INTEGERS: ELECTRONIC JOURNAL OF COMBINATORIAL NUMBER THEORY 8 (2008), #A04

ARITHMETIC STRUCTURES IN RANDOM SETS

Mariah Hamel
Department of Mathematics, University of British Columbia, Vancouver, B.C. V6T 1Z2, Canada
mehamel@math.ubc.ca

Izabella Łaba
Department of Mathematics, University of British Columbia, Vancouver, B.C. V6T 1Z2, Canada
ilaba@math.ubc.ca

Received: 3/25/07, Accepted: 1/23/08, Published: 1/29/08

Abstract

We extend two well-known results in additive number theory, Sárközy's theorem on square differences in dense sets and a theorem of Green on long arithmetic progressions in sumsets, to subsets of random sets of asymptotic density 0. Our proofs rely on a restriction-type Fourier analytic argument of Green and Green-Tao.

1. Introduction

The purpose of this paper is to extend several basic results in additive number theory, known for sets of positive density in $\mathbb{Z}_N$, to the setting of random sets of asymptotic density 0. This line of work originated in the paper of Kohayakawa-Łuczak-Rödl [12], who proved a random-set analogue of Roth's theorem on 3-term arithmetic progressions. Roth's theorem [15] asserts that for any fixed $\delta > 0$ there is a large integer N_0 such that if $N > N_0$ and if A is a subset of $\{1, \ldots, N\}$ with $|A| \geq \delta N$, then A contains a non-trivial 3-term arithmetic progression $a, a+r, a+2r$ with $r \neq 0$. The article [12] raises the following question: are there any sets W, sparse in $\{1, \ldots, N\}$, with the property that any set A containing a positive proportion of the elements of W must contain a 3-term arithmetic progression? The authors proceed to answer it in the affirmative for random sets:

Theorem 1.1. *[12] Suppose that W is a random subset of $\mathbb{Z}_N$ such that the events $x \in W$, where x ranges over $\mathbb{Z}_N$, are independent and have probability $p = p(N) \in (CN^{-1/2}, 1]$. Fix $\alpha > 0$. Then the statement*

every set $A \subset W$ with $|A| \geq \alpha |W|$ contains a 3-term arithmetic progression

is true with probability $1 - o_\alpha(1)$ *as* $N \to \infty$.

The current interest in questions of this type is motivated by the work of Green [8] and Green-Tao [9], [10] on arithmetic progressions in the primes, where the "pseudorandomness" of the almost-primes plays a key role. For example, Tao-Vu [22, Section 10.2] give an alternative (and simpler) proof of Theorem 1.1 under the stronger assumption that $p \geq CN^{-\theta}$ with θ small enough. While the argument in [12] is combinatorial and uses Szemerédi's regularity lemma, the proof in [22] is Fourier-analytic and relies in particular on a restriction-type estimate from [8], [10].

It is natural to ask which other results from additive number theory can be extended to the random set setting. While the methods of [12] do not seem to extend to other questions, the decomposition technique in [10] turns out to be more robust. We are able to use it to prove random set analogues of two well-known results: Sárközy's theorem on square differences, and a theorem of Green on long arithmetic progressions in sumsets.

We note that the concept of pseudorandomness has played a major role in many of the basic extremal results in additive number theory, such as Szemerédi's theorem on arithmetic progressions. Specifically, in order to find a certain type of an arithmetic structure (such as an arithmetic progression) in sets of positive density, one often begins by showing that such structures are common in appropriately defined pseudorandom sets. It is not clear whether our results will have applications of this type, as the corresponding extremal results for sets of positive density are already known. On the other hand, we expect that the methods developed here will be useful in proving similar results in settings where the background set W is a given set of density zero with sufficiently good pseudorandom properties (e.g. the primes, the Chen primes). For example, one could inquire about the arithmetic properties of sets of the form $A + B$, where A and B are subsets of the primes with relative positive density.

We now give the precise statement of our results. Throughout the paper, W is a random subset of $\mathbb{Z}_N$, with each $x \in \mathbb{Z}_N$ belonging to W independently with probability $p \in (0, 1]$. We will assume that $p \geq N^{-\theta}$, where θ is a sufficiently small positive number. In particular, we allow p to go to 0 as $N \to \infty$. We also fix $\delta > 0$ and let $A \subset W$, $|A| = \delta|W|$.

Sárközy's theorem (proved also independently by Furstenberg) states that for any fixed positive number δ there is a large integer N_0 such that if $N > N_0$ and if A is a subset of $\{1, \ldots, N\}$ with $|A| \geq \delta N$, then A contains two distinct elements x, y such that $x - y$ is a perfect square. The best known quantitative bound, due to Pintz, Steiger and Szemerédi [14], is that one may take $N_0 = (\log N)^{-c \log\log\log\log N}$. In the converse direction, Ruzsa [16] constructed a set of size $N^{1-0.267}$ which contains no square difference.

We are able to prove the following.

Theorem 1.2. *Suppose that* W *is a random subset of* $\mathbb{Z}_N$ *such that the events* $x \in W$, *where* x *ranges over* $\mathbb{Z}_N$, *are independent and have probability* $p = p(N) \in (cN^{-\theta}, 1]$ *where* $0 < \theta < 1/110$. *Let* $\alpha > 0$. *Then the statement*

for every set $A \subset W$ with $|A| \geq \alpha W$, there are $x, y \in A$ such that $x - y$ is a non-zero perfect square

is true with probability $1 - o_\alpha(1)$ as $N \to \infty$.

We also have an analogous result for higher power differences (see Section 5).

If A, B are two sets of integers, we will write $A + B = \{a + b : \ a \in A, b \in B\}$. Let W be a random set as described above, but with $\theta \in (0, 1/2]$. One can show using a probabilistic argument that it holds with probability $1 - o(1)$ that the sumset $A + A$ of every subset $A \subset W$ with $|A| > \alpha|W|$ has density at least α^2 in $\mathbb{Z}_N$[1]. If θ is close enough to 0, then we can prove the following stronger result using Fourier-analytic methods.

Proposition 1.3. *Suppose that W is a random subset of $\mathbb{Z}_N$ such that the events $x \in W$, where x ranges over $\mathbb{Z}_N$, are independent and have probability $p = p(N) \in (CN^{-\theta}, 1]$, where $0 < \theta < 1/140$. Then for every $\beta < \alpha$, the statement*

for every set $A \subset W$ with $|A| \geq \alpha|W|$, we have $|A + A| \geq \beta N$

is true with probability $1 - o_{\alpha,\beta}(1)$ as $N \to \infty$.

It is easy to see that one can have $|A + A| \approx \alpha N$ in the setting of the proposition: let $A_x = W \cap (P + x)$, where P is an arithmetic progression in $\mathbb{Z}_N$ of step about α^{-1} and length about αN. An averaging argument shows that $|A_x| \gg \alpha|W|$ for some x, while $|A_x + A_x| \leq 2|P| \approx \alpha N$.

Our second main result concerns the existence of long arithmetic progressions in sumsets. Bourgain [1] proved that if A, B are sumsets of $\{1, \ldots, N\}$ with $|A| > \alpha N$, $|B| > \beta N$, then $A + B$ contains a k-term arithmetic progression with

$$k > \exp(c(\alpha\beta \log N)^{1/3} - \log\log N). \tag{1.1}$$

The point here is that a sumset has much more arithmetic structure, and therefore contains much longer arithmetic progressions, than would be normally expected in a set of a similar size (based on Szemerédi's theorem, for example). Bourgain's bound was improved by Green [6] to

$$k > \exp(c(\alpha\beta \log N)^{1/2} - \log\log N), \tag{1.2}$$

which is the best known result in this direction so far. An alternative proof of essentially the same bound was given more recently by Sanders [18]. On the other hand, Ruzsa [17] gave a construction showing that the exponent $1/2$ in (1.2) cannot be improved beyond $2/3$. Note that if $A = B$, the estimate (1.2) gives a non-trivial result only when $\alpha > (\log N)^{-1/2}$, and in particular sets with density $N^{-\epsilon}$ are not allowed.

[1] We are grateful to Mihalis Kolountzakis for pointing this out to us and communicating a short proof.

The case of sparse sets was considered more recently by Croot-Ruzsa-Schoen [4]. The authors proved that if $A, B \subset \mathbb{Z}_N$ obey $|A||B| \geq (6N)^{2-\frac{2}{k-1}}$, then $A+B$ contains a k-term arithmetic progression. They also gave a construction of sets $A \subset \mathbb{Z}_N$ with $|A| \geq N^{1-\theta}$, where θ is small enough depending on $\epsilon > 0$, such that $A+A$ does not contain an arithmetic progression longer than $\exp(c\theta^{-\frac{2}{3}-\epsilon})$.

Our result is the following.

Theorem 1.4. *Suppose that W is a random subset of $\mathbb{Z}_N$ such that the events $x \in W$, where x ranges over $\mathbb{Z}_N$, are independent and have probability $p = p(N) \in (CN^{-\theta}, 1]$, where $0 < \theta < 1/140$. Assume that α and k obey*

$$\alpha \geq \frac{C_1 \log\log N}{\sqrt{\log N}}, \tag{1.3}$$

$$k \leq \exp\left(\frac{\alpha^2 \log\log N}{C_2 \log\frac{1}{\alpha}(\log\log\log N + \log\frac{1}{\alpha})}\right), \tag{1.4}$$

where C_1, C_2 are sufficiently large constants. Then the statement

> *for every set $A \subset W$ with $|A| \geq \alpha|W|$, the sumset $A+A$ contains a k-term arithmetic progression*

is true with probability $1 - o_{k,\alpha}(1)$ as $N \to \infty$.

A non-quantitative version of the result, namely that the displayed statement in the theorem is true with probability $1 - o(1)$ as $N \to \infty$ if α and k are fixed, can be obtained by applying Szemerédi's theorem to the positive density set $A+A$. Our point, as in [1] or [6], is that the arithmetic progressions indicated by Theorem 1.4 are much longer than those in Szemerédi's theorem, and that they can be found using a much easier argument. For comparison, the current best bounds in Szemerédi's theorem [5] imply that a set of relative density α in $\mathbb{Z}_N$ should contain k-term arithmetic progressions with

$$k \leq \log\log\left(\frac{\log\log N}{\log\frac{1}{\alpha}}\right),$$

which is much weaker than (1.4).

The bounds on θ in Theorems 1.2 and 1.4 are due to our choices of exponents in the proofs and are probably not optimal. The natural threshold would be $1/2$, as in [12]. However, it does not seem possible to extend our results to all $\theta < 1/2$ using the same type of arguments as in this paper.

The article is organized as follows. In the next section we explain the notation and summarize the known results that will be used repeatedly. Theorem 1.2 is proved in Sections 3 and 4. Its analogue for higher power differences, Theorem 5.1, is stated and proved in Section 5. The proof of Theorem 1.4 is given in Section 6, with the proofs of the main estimates postponed to Sections 7 and 8. The proof of Proposition 1.3, which involves a simplified version of the argument in the proof of Theorem 1.4, concludes the paper.

2. Preliminaries

We first explain the notation. We use $|A|$ to denote the cardinality of a set $A \subset \mathbb{Z}_N$. The *probability* of a set A is $\mathbb{P}(A) = N^{-1}|A|$, and the *expectation* of a function $f : \mathbb{Z}_N \to \mathbb{C}$ is defined as

$$\mathbb{E}f = \mathbb{E}_x f = N^{-1} \sum_{x \in \mathbb{Z}_N} f(x).$$

We will also sometimes use conditional probability and expectation

$$\mathbb{P}(A|X) = \frac{|A \cap X|}{|X|}, \ \mathbb{E}(f|X) = \mathbb{E}_{x \in X} f(x) = \frac{1}{|X|} \sum_{x \in X} f(x).$$

Whenever the range of a variable (in a sum, expectation, etc.) is not indicated, it is assumed to be all of $\mathbb{Z}_N$. We will also use the notation $\|f\|_p = (\sum_x |f(x)|^p)^{1/p}$ and $\|f\|_{L^p(X)} = (\sum_{x \in X} |f(x)|^p)^{1/p}$. All constants throughout the paper will be independent of N, α, and k.

The discrete Fourier transform of f is defined by

$$\widehat{f}(\xi) = \mathbb{E}_x f(x) e^{-2\pi i x\xi/N}.$$

We have the usual Plancherel identity $\sum \widehat{f}\overline{\widehat{g}} = N^{-1} \sum f\bar{g}$ and the inversion formula $f(x) = \sum_{\xi \in \mathbb{Z}_N} \widehat{f}(\xi) e^{-2\pi i x\xi/N}$.

We define the convolution of two functions $f, g : \mathbb{Z}_N \to \mathbb{C}$ by the formula

$$(f * g)(x) = \sum_y f(y)g(x-y) = \sum_{t,s: t+s=x} f(t)g(s).$$

We have the identity $N\widehat{f}\widehat{g} = \widehat{f * g}$.

We recall a few basic results about Bohr sets, all of which are standard in the literature and can be found e.g. in [11], [22], or in [2] where regular Bohr sets were first introduced.

Definition 2.1. *A* Bohr set *is a set of the form $B = b + B(\Lambda, \delta)$, where $b \in \mathbb{Z}_N$, $\Lambda \subset \mathbb{Z}_N$, $\delta \in (0, 2)$, and*

$$B(\Lambda, \delta) = \{x \in \mathbb{Z}_N : \ |e^{2\pi i x\xi/N} - 1| \leq \delta \text{ for all } \xi \in \Lambda\}.$$

We will often refer to $|\Lambda|$ and δ as the rank and radius of B, respectively.

Definition 2.2. *Let c_0 be a small positive constant which will remain fixed throughout the paper. We will say that a Bohr set $B(\Lambda, \delta)$ is* regular *if*

$$\mathbb{P}(B(\Lambda, (1 + c_0^2)\delta) \setminus B(\Lambda, (1 - c_0^2)\delta)) \leq c_0 \mathbb{P}(B(\Lambda, \delta)).$$

We will also say that $B = b + B(\Lambda, \delta)$ is regular if $B(\Lambda, \delta)$ is regular.

Lemma 2.3. *If $B = B(\Lambda, \delta)$ is a regular Bohr set, then $\mathbb{P}(B) \geq (cc_0^2\delta)^{|\Lambda|}$.*

Lemma 2.4. *Assume that c_0 is small enough. Then for any $\Lambda \subset \mathbb{Z}_N$ with $|\Lambda| \leq \sqrt{c_0}N$ and any $\delta_0 > 0$ there is a $\delta \in (\frac{\delta_0}{2}, \delta_0)$ such that $B(\Lambda, \delta)$ is regular.*

We will need a Fourier-analytic argument which first appeared in [8] in a slightly different formulation and in [10] as stated, and was adapted in [22] to a random set setting. Specifically, [8] and [10] introduced the decomposition $f = f_1 + f_2$ defined below, where f_1 is the "structured" bounded part, and f_2 is unbounded but random. We will need several results concerning the properties of f_1 and f_2, which we collect in the next two lemmas. The first one is contained in the proofs of [10, Proposition 5.1] or [22, Theorem 10.20].

Lemma 2.5. *Assume that $f : \mathbb{Z}_N \to [0, \infty)$ satisfies $\mathbb{E}(f) \geq \delta > 0$ and*

$$\|\widehat{f}\|_q \leq M \tag{2.1}$$

for some $2 < q < 3$. Assume also that $f \leq \nu$, where $\nu : \mathbb{Z}_N \to [0, \infty)$ obeys the pseudorandom condition

$$\|\hat{\nu}(\xi) - \mathbf{1}_{\xi=0}\|_\infty \leq \eta \tag{2.2}$$

for some $0 < \eta \leq 1$. Let

$$f_1(x) = \mathbb{E}(f(x + y_1 - y_2) : \ y_1, y_2 \in B_0),$$

where

$$B_0 = \{x : \ |e^{-2\pi i \xi x/N} - 1| \leq \epsilon_0, \ \xi \in \Lambda_0\}, \ \Lambda_0 = \{\xi : \ |\widehat{f}(\xi)| \geq \epsilon_0\}$$

for some ϵ_0 to be fixed later. Let also $f_2(x) = f(x) - f_1(x)$. Then

(i) $0 \leq f_1 \leq 1 + (1 + \mathbb{P}(B_0)^{-1})\eta$,

(ii) $\mathbb{E}f_1 = \mathbb{E}f$,

(iii) $\|\widehat{f_2}\|_\infty \leq 3(1 + \eta)\epsilon_0$,

(iv) $|\widehat{f_i}(\xi)| \leq |\widehat{f}(\xi)|$ *for all $\xi \in \mathbb{Z}_N$ and $i = 1, 2$. In particular, (2.1) holds with f replaced by f_2.*

In order to be able to apply Lemma 2.5, we need to have the estimate (2.1) for some $2 < q < 3$. To this end we have the following result, based on the Stein-Tomas argument as used in [8], [10], and contained in the form we need in [22, Lemma 10.22 and proof of Theorem 10.18].

Lemma 2.6. *Let f and ν be as in Lemma 2.5, except that instead of (2.1) we assume that*

$$\|\widehat{f}\|_2 \leq C\eta^{-\epsilon/4}$$

for some $\epsilon > 0$. Then (2.1) holds with $q = 2 + \epsilon$.

We adapt this argument to the random setting as in [22, Section 10.2]. Suppose that W is a random subset of $\mathbb{Z}_N$ such that each $x \in \mathbb{Z}_N$ belongs to W independently with probability $p \in (0,1)$. We will assume that $p \geq N^{-\theta}$, where $0 < \theta < 1/100$. We also fix $\delta > 0$ and let $A \subset W$, $|A| = \delta|W|$. We let

$$\nu(x) = p^{-1}W(x), \ f(x) = p^{-1}A(x).$$

Lemma 2.7. *Let ν and f be the random variables defined above. Then*

(i) $\|\widehat{\nu(\xi)} - \mathbf{1}_{\xi=0}\|_\infty = O(N^{-1/5})$ *with probability* $1 - o(1)$,

(ii) $\|\widehat{f}\|_2^2 = N^{-1}\|f\|_2^2 = O(p^{-1}) \leq N^\theta$ *with probability* $1 - o(1)$.

Part (i) of the lemma follows from well-known probabilistic arguments. It can be found e.g. in [22, Corollary 1.9 and Lemma 4.15], or extracted from the proof of Lemma 14 in [6]. Observe in particular that (i) with $\xi = 0$ says that $\mathbb{P}(W) = p(1+O(N^{-1/5}))$ with probability $1 - o(1)$. Part (ii) follows from this and the Plancherel identity.

3. A Varnavides-type Theorem for Square Differences

The purpose of this section is to prove the following theorem.

Theorem 3.1. *Let $0 < \delta \leq 1$ and $N \geq 1$ be a prime integer. Let $f : \mathbb{Z}_N \to [0,1]$ be a bounded function such that $\mathbb{E}f \geq \delta$. Then we have*

$$\mathbb{E}(f(n)f(n+r^2)|n, r \in \mathbb{Z}_N, \ 1 \leq r \leq \lfloor\sqrt{N/3}\rfloor) \geq c(\delta) - o_\delta(1).$$

Theorem 3.1 strengthens Sárközy's theorem (stated in the introduction) in the same way in which a theorem of Varnavides [23] strengthens Roth's theorem on 3-term arithmetic progressions. It guarantees the existence of "many" square differences in a set of positive density, instead of just one.

Proof. The proof combines Sárközy's theorem with a modification of Varnavides's combinatorial argument [23]. We first note that it suffices to prove the result for characteristic functions. To see this, let f be as in the theorem, and define $A := \{n \in \mathbb{Z}_N : f(n) \geq \delta/2\}$. Then $|A| \geq \delta N/2$ and $f \geq \frac{\delta}{2}$ on A. Hence, assuming the result for characteristic functions, we have

$$\mathbb{E}(f(n)f(n+r^2)) \geq \frac{\delta^2}{4}\mathbb{E}(A(n)A(n+r^2)) \geq \frac{\delta^2}{4}c(\delta/2).$$

We now turn to the proof of the result for characteristic functions. Let $A \subset \mathbb{Z}_N$ such that $|A| \geq \delta N$ and N is sufficiently large. We will consider arithmetic progressions

$$P_{x,r} = \{x, x+r^2, \ldots, x+(k-1)r^2\}, \ 1 \leq x \leq x+(k-1)r^2 \leq N \tag{3.1}$$

where $x, r \in \mathbb{Z}_N$, $r \leq \sqrt{3N}$, and where $k \in \mathbb{N}$ is chosen so that the conclusion of Sárközy's theorem holds for subsets of $\{1, ..., k\}$ which have size at least $\frac{1}{2}\delta k$.

Suppose that

$$r^2 < \frac{\delta N}{k^2}. \tag{3.2}$$

We say that a progression $P_{x,r}$ as in (3.1) is *good* if

$$|P_{x,r} \cap A| \geq \frac{1}{2}\delta k. \tag{3.3}$$

Let $G_r(N)$ denote the set of good progressions $P_{x,r}(N)$ for a fixed r. We claim that

$$|G_r(N)| > \frac{1}{4}\delta N. \tag{3.4}$$

Indeed, we have

$$|A \cap (kr^2, N - kr^2)| \geq |A| - 2kr^2 \geq \delta N - 2kr^2 \geq \delta(1 - \frac{2}{k})N,$$

where at the last step we used (3.2). Each $a \in A \cap (kr^2, N - kr^2)$ is contained in exactly k progressions $P_{x,r}$. Hence

$$\sum_{x:1 \leq x < x+(k-1)r^2 \leq N} |A \cap P_{x,r}| \geq k\delta(1 - \frac{2}{k})N > \frac{3}{4}\delta kN \quad (k > 8).$$

On the other hand, the number of progressions $P_{x,r}$ for a fixed r is clearly bounded by N, and hence we have an upper bound

$$\sum_{x:1 \leq x < x+(k-1)r^2 \leq N} |A \cap P_{x,r}| < N \cdot \frac{1}{2}\delta k + G_r(N)k.$$

Combining these bounds yields (3.4) as claimed.

Let $G(N) := \sum_{r:r^2 < \frac{\delta N}{k^2}} G_r(N)$. Then

$$G(N) \geq \frac{\sqrt{\delta N}}{k}\frac{\delta N}{4} = c_1(\delta)N^{3/2}, \tag{3.5}$$

since k depends only on δ.

By Sárközy's theorem, each good progression $P_{x,r}$ contains a square difference. We now count the number of good progressions which may contain a fixed square difference pair $x, x + r^2$. Clearly, $x, x + r^2$ can be contained in at most $k - 1$ progressions with step size r^2 and at most $\frac{1}{2}k(k - 1)$ progressions with step size r^2/t for integers $t > 1$. Since k depends only on δ, the total number of progressions containing $x, x + r^2$ is bounded by $c_2(\delta)$. Thus the total number of square differences in A must be at least

$$\frac{c_1(\delta)}{c_2(\delta)}N^{3/2} = c(\delta)N^{3/2}.$$

Subtracting off the trivial progressions (with $r^2 = 0$) gives the desired result. □

4. Proof of Theorem 1.2

Let W, A be as in Theorem 1.2. At least one of the sets $A_1 = A \cap [0, N/3)$, $A_2 = A \cap [N/3, 2N/3)$, $A_3 = A \cap [2N/3, N)$, say A_1 (the other two cases are identical), has size at least $|A|/3$. Define ν, f as in Lemma 2.7, but with A replaced by A_1. By Lemma 2.7, the assumptions of Lemma 2.6 with $\eta = N^{-1/5}$ and $\epsilon = 1/11$ are satisfied with probability $1 - o(1)$, and thus (2.1) holds with $q = 23/11$. We will henceforth assume this is the case. Let $f = f_1 + f_2$ as in Lemma 2.5, with $\epsilon_0 = \epsilon_0(\alpha)$ small enough to be fixed later. We would like to ensure that

$$\|f_1\|_\infty \leq 2. \tag{4.1}$$

By Lemma 2.5, this will follow if

$$N^{-1/5}(1 + \mathbb{P}(B_0))^{-1} < 1. \tag{4.2}$$

By Lemma 2.3, we can estimate $\mathbb{P}(B_0) \gg (c\epsilon_0)^{|\Lambda_0|}$, while by (2.1) and Chebyshev's inequality we have $|\Lambda_0| \leq (M/\epsilon_0)^{23/11}$. Now a short calculation shows that if

$$\log \frac{1}{\epsilon_0} < c_1 \log\log N \tag{4.3}$$

with c_1 small enough, which we will assume henceforth, then (4.2) and (4.1) hold.

It suffices to prove that

$$\mathbb{E}(f(x)f(x + r^2)|x, r \in \mathbb{Z}_N, 1 \leq r \leq \sqrt{N/3}) \geq c(\delta) - o_\delta(1). \tag{4.4}$$

Indeed, since $A_1 \subset [0, N/3)$, any square difference $a - a' = r^2$ with $a, a' \in A_1$ and $1 \leq r^2 \leq N/3$ must be an actual square difference in $\mathbb{Z}$, not just a square difference mod N.

We write $f(x)f(x + r^2) = \sum_{i,j=1}^2 f_i(x)f_j(x + r^2)$, and estimate the expectation of each term. Applying Theorem 3.1 to f_1, we get a lower bound on the main term

$$\mathbb{E}(f_1(x)f_1(x + r^2)|x, r \in \mathbb{Z}_N, 1 \leq r \leq \sqrt{N/3}) \geq c_1(\delta) - o_\delta(1), \tag{4.5}$$

if N is large enough so that (4.3) holds. We now turn to the error estimates. We write

$$\mathbb{E}(f_2(x)f_2(x+r^2)|x, r \in \mathbb{Z}_N, 1 \leq r \leq \sqrt{N/3}) = \sqrt{3N}\,\mathbb{E}(f_2(x)f_2(x+t)S(t)|x, t \in \mathbb{Z}_N), \tag{4.6}$$

where $S(\cdot)$ denotes the characteristic function of the squares less than $N/3$. From Green [7] we have the estimate

$$\|\hat{S}\|_{12} \leq 2^{19/12} N^{-1/2},$$

based on a number theoretic bound on the number of representations of an integer as the

sum of six squares. Using also Parseval's identity and Hölder's inequality, we have

$$\begin{aligned}\mathbb{E}(f_2(x)f_2(x+t)S(t)|x,t\in\mathbb{Z}_N)&\\ &=\sum_{\xi\in\mathbb{Z}_N}|\hat{f}_2(\xi)|^2|\hat{S}(\xi)|\\ &\leq\big(\sum_{\xi\in\mathbb{Z}_N}|\hat{S}(\xi)|^{12}\big)^{1/12}\big(\sum_{\xi\in\mathbb{Z}_N}|\hat{f}_2(\xi)|^{24/11}\big)^{11/12}\\ &\leq 2^{19/12}N^{-1/2}\|\hat{f}_2\|_{23/11}^{23/12}\|\hat{f}_2\|_\infty^{1/12}\\ &\leq CN^{-1/2}\epsilon_0^{1/12}.\end{aligned}$$

Plugging this into (4.6), we see that

$$\mathbb{E}(f_2(x)f_2(x+r^2)|x,r\in\mathbb{Z}_N,1\leq r\leq\sqrt{N/3})\leq c_1(\delta)/4$$

if ϵ_0 was chosen sufficiently small depending on δ. The "mixed" error terms are estimated similarly. Combining the error estimates with (4.5) yields (4.4) as desired.

5. Power Differences

In this section we show that a modification of the proof of Theorem 1.2 yields an analogous result for higher power differences.

Theorem 5.1. *Suppose that W is a random subset of $\mathbb{Z}_N$ such that the events $x\in W$, where x ranges over $\mathbb{Z}_N$, are independent and have probability $p=p(N)\in(cN^{-\theta},1]$ with $0<\theta<\theta_k$, where θ_k is small enough depending on $k\in\mathbb{N}$. Let $\alpha>0$. Then the statement*

> *for every set $A\subset W$ with $|A|\geq\alpha W$, $\exists\ x,y\in A$ such that $x-y=n^k$ for some $n\in\mathbb{N}$*

is true with probability $o_{k,\alpha}(1)$ as $N\to\infty$.

Since the proof is very similar to that of Theorem 1.2, we only sketch the main steps. Instead of Theorem 3.1, we will need a similar result for higher powers, which can be proved by exactly the same argument.

Theorem 5.2. *Let $0<\delta\leq 1$, and let $N\geq 1$ be a prime integer. Let $f:\mathbb{Z}_N\to[0,1]$ be a bounded function such that $\mathbb{E}f\geq\delta$. Then we have*

$$\mathbb{E}(f(n)f(n+r^k)|n,r\in\mathbb{Z}_N,\ 1\leq r\leq\lfloor\sqrt[k]{N/3}\rfloor)\geq c(\delta)-o_\delta(1).$$

We now follow the argument in Section 4. Define ν, f, f_1, f_2 as in the proof of Theorem 1.2. Applying Theorem 5.2 to f_1, we see that

$$\mathbb{E}(f_1(x)f_1(x+r^k)|x, r \in \mathbb{Z}_N, 1 \leq r \leq \sqrt[k]{N/3}) \geq c(\delta) - o_{\delta,\epsilon_0,M}(\eta).$$

To estimate the error terms, we invoke the asymptotic formula for Waring's problem (see e.g. [13]), which implies that

$$R_{k,3k}(x) := |\{(a_1, \ldots, a_{3k}) \in \mathbb{Z}_N | a_1^k + \cdots + a_{3k}^k \equiv x(\mod N)\}| \leq cN^2.$$

By convolution and Parseval identities, this translates to

$$\|\widehat{P_k}\|_{6k} \leq c_1 N^{1/k-1},$$

where P_k denotes the characteristic function of the set of k-th powers smaller than $N/3$, and c, c_1 are constants depending on k. Now we are able to estimate the error terms as in Section 4; for example, we have

$$\begin{aligned}\mathbb{E}(f_2(x)f_2(x+r)P_k(r)) &\leq \|\hat{P}_k\|_{6k}\|\hat{f}_2\|_{(12k-1)/(6k-1)}^{(12k-2)/(12k)}\|\hat{f}_2\|_\infty^{1/6k} \\ &\leq c_1 C N^{1/k-1}\epsilon_0^{1/6k}.\end{aligned}$$

At the last step we used that (2.1) holds with $q = \frac{12k-1}{6k-1}$ if θ_k is small enough. The proof is finished as in Section 4.

6. Long Arithmetic Progressions in Sumsets

We now turn to Theorem 1.4. In this section we prove the theorem, modulo the two main estimates (6.1), (6.7) which will be proved in the next two sections.

Our proof will combine the arguments of Sanders [18] with those of Green-Tao [10]. Let W, A be as in Theorem 1.4, and define ν, f as in Lemma 2.7. We will show that, with high probability, there is a reasonably large Bohr set B on which we have $f * f(x) > 0$ for all but a few values of x. But $f * f$ is supported on $A + A$. Hence, all but a small fraction of B is contained in $A + A$. The proof is concluded by invoking a pigeonholing argument from [18], which says that the portion of B contained in $A + A$ contains a long arithmetic progression.

The details are as follows. Fix k (the length of the progression), and let $\sigma = (16k)^{-1}$. We will also assume that $k > k_0$ and $\alpha < \alpha_0$, where $k_0 \in \mathbb{N}$ is a sufficiently large absolute constant and $\alpha_0 > 0$ is a sufficiently small absolute constant.

By Lemma 2.7, the assumptions of Lemma 2.6 with $\eta = N^{-1/5}$ and $\epsilon = 1/9$ are satisfied with probability $1 - o(1)$, and thus (2.1) holds with $q = 19/9$. Let $f = f_1 + f_2$ as in Lemma 2.5, with $\epsilon_0 = \epsilon_0(\alpha, \sigma)$ small enough to be fixed later. We will assume that (4.3) holds with c_1 sufficiently small; as in Section 4, it follows that $\|f_1\|_\infty \leq 2$.

We need an extension of a result of Sanders [18]: there are regular Bohr sets $B := b + B(\Gamma, \delta)$ and $B' := b + B(\Gamma, \delta')$ such that

$$\Big|\{x \in B' : \ f_1 * f_1(x) \geq \frac{\alpha^2}{2}|B|\}\Big| > (1-\sigma)|B'|, \tag{6.1}$$

and

$$\delta' \gg \frac{\alpha^2 \delta}{|\Gamma|}, \tag{6.2}$$

$$\delta \gg \big(\frac{\alpha}{\log(\sigma^{-1})}\big)^{C\log(\alpha^{-1})}, \tag{6.3}$$

$$|\Gamma| \ll \alpha^{-2}\log(\sigma^{-1}). \tag{6.4}$$

We establish this in Proposition 7.2. We then verify in Section 8, via a restriction-type argument, that if

$$\log\frac{1}{\epsilon_0} \gg \alpha^{-2}\log\frac{1}{\alpha}\log k(\log\log k + \log\frac{1}{\alpha}), \tag{6.5}$$

with a large enough implicit constant, then

$$\Big|\{x \in B' : \ |f_2 * f_i(x)| \geq \frac{\alpha^2}{10}|B|\}\Big| < \sigma|B'|, \ i = 1, 2. \tag{6.6}$$

It follows that

$$\Big|\{x \in B' : \ f * f(x) \geq \frac{\alpha^2}{10}|B|\}\Big| > (1-4\sigma)|B'|, \tag{6.7}$$

provided that both (4.3) and (6.5) hold. A somewhat cumbersome calculation shows that ϵ_0 can be chosen so as to satisfy both (4.3) and (6.5), provided that

$$\log k \ll \frac{\alpha^2 \log\log N}{\log\frac{1}{\alpha}(\log\log\log N + \log\frac{1}{\alpha})}, \tag{6.8}$$

which is equivalent to (1.4).

We now invoke Lemma 6.5 in [18], which says that if

$$(4\sigma)^{-1} \ll |\Gamma|^{-1}\delta' N^{1/|\Gamma|}, \tag{6.9}$$

then the set on the left side of (6.7) contains an arithmetic progression of length $(16\sigma)^{-1} = k$. Plugging in (6.2)–(6.4) and solving for N, we see that (6.9) holds if

$$\log N \gg \alpha^{-2}(\log^2 k + \log^2(\frac{1}{\alpha}) + \log\frac{1}{\alpha}\log\log k). \tag{6.10}$$

Another cumbersome calculation shows that if we assume (6.8), then the additional condition (1.3) suffices to guarantee that (6.10) holds. Thus, assuming both (1.3) and (1.4), the set on the left side of (6.7) contains a k-term arithmetic progression. Since that set is contained in $A + A$, the conclusion of the theorem follows.

In the next two sections we complete the proof by verifying the inequalities (6.1), (6.6).

7. The Main Term Estimate

Proposition 7.1. *Let $B = b + B(\Gamma, \delta)$ be a regular Bohr set. Let $f : \mathbb{Z}_N \to \mathbb{R}$ be a function such that $supp(f) \subset B$, $0 \leq f \leq 1$ and $\mathbb{E}_B f = \alpha > 0$. Fix $\sigma \in (0, 1]$ and let $d = |\Gamma|$. Then one of the following must be true:*

(i) There is a $\delta' \gg \frac{\alpha^2 \delta}{d}$ such that $B' = b + B(\Gamma, \delta')$ is regular and

$$\Big|\{x \in B' : (f * f)(x) \geq \frac{\alpha^2}{2}|B|\}\Big| \geq (1 - \sigma)|B'|, \tag{7.1}$$

or

(ii) There is a regular Bohr set $B'' = b'' + B(\Gamma \cup \Lambda, \delta'')$ such that

$$\mathbb{E}(f|B'') \geq \alpha\big(1 + 2^{-5}\big), \tag{7.2}$$

where $|\Lambda| \ll \alpha^{-2} \log \sigma^{-1}$ and $\delta'' \gg \frac{\alpha^4 \delta}{d^3 \log \sigma^{-1}}$.

Proof. We essentially follow the argument of Sanders [18]; however, some care must be taken to get the right quantitative version. Replacing f by $f(\cdot + b)$ if necessary, we may assume that $b = 0$. Let c_0 be a small enough constant which will be fixed later. By [11], Lemma 8.2, we can find δ' such that

$$\delta' \in (c_0 \alpha^2 \delta d^{-1}, 2c_0 \alpha^2 \delta d^{-1}) \tag{7.3}$$

and that the set B' defined in (i) is regular. Suppose that (7.1) fails for this choice of δ'; we have to prove that this implies (ii).

The failure of (7.1) means that we can find a set $S \subset B' \cap \{x : (f * f)(x) < \frac{\alpha^2}{2}|B|\}$ such that $|S| = \sigma|B'|$. Let $g = f - \alpha B$ be the "balanced function" of f. We first claim that

$$\frac{1}{|B||B'|} \sum_{x \in S} g * g(x) \leq -\frac{\alpha^2 \sigma}{2} + O(d\delta' \delta^{-1} \sigma). \tag{7.4}$$

To prove this, we write

$$\frac{1}{|B||B'|} \sum_{x \in S} (g * g)(x) = \frac{1}{|B||B'|} \big(\sum_{x \in S} (f * f)(x) - 2\alpha \sum_{x \in S} (B * f)(x) + \alpha^2 \sum_{x \in S} (B * B)(x) \big).$$

The first term obeys

$$\frac{1}{|B||B'|} \sum_{x \in S} (f * f)(x) \leq \frac{\alpha^2 |B|}{2|B||B'|} |S| = \frac{\alpha^2 \sigma}{2}, \tag{7.5}$$

by the choice of S. The second term is estimated as in [18]. By [18], Corollary 3.4, we have for $x \in B'$

$$|f * \frac{B}{|B|}(x) - f * \frac{B}{|B|}(0)| \ll d\delta' \delta^{-1}.$$

But $f * \frac{B}{|B|}(0) = \alpha$, so that $f * \frac{B}{|B|}(x) = \alpha + O(d\delta'\delta^{-1})$ for $x \in B'$. Hence,

$$\frac{1}{|B'|}\sum_{x\in S}\frac{B}{|B|} * f(x) = \frac{|S|}{|B'|}(\alpha + O(d\delta'\delta^{-1})) = \alpha\sigma + O(d\delta'\delta^{-1}\sigma). \tag{7.6}$$

Finally, we trivially have $B * B(x) \leq |B|$ for all x. Hence,

$$\frac{1}{|B||B'|}\sum_{x\in S} B * B(x) \leq \sigma + O(d\delta'\delta^{-1}\sigma). \tag{7.7}$$

Combining (7.5), (7.6), (7.7), we get (7.4).

We now convert this to a Fourier analytic statement. We have

$$\begin{aligned}\sum_{x\in S} g * g(x) &= \sum_{x\in\mathbb{Z}_N} g * g(x)S(x)\\ &= N\sum_{\xi\in\mathbb{Z}_N}\widehat{g * g}(\xi)\widehat{S}(\xi)\\ &= N^2\sum_{\xi\in\mathbb{Z}_N}|\widehat{g}(\xi)|^2\widehat{S}(\xi).\end{aligned}$$

Hence, by the triangle inequality, (7.4) implies that

$$\frac{N^2}{|B||B'|}\sum_{\xi}|\widehat{g}(\xi)|^2|\widehat{S}(\xi)| \geq \frac{\alpha^2\sigma}{2} + O(d\delta'\delta^{-1}\sigma). \tag{7.8}$$

Define

$$\mathcal{L} := \{\xi \in \mathbb{Z}_N : |\widehat{S}(\xi)| \geq \frac{\alpha\sigma|B'|}{4N}\}.$$

We claim that the main contribution to the sum in (7.8) comes from $\mathcal{L}$. In fact

$$\begin{aligned}\frac{N^2}{|B||B'|}\sum_{\xi\notin\mathcal{L}}|\widehat{g}(\xi)|^2|\widehat{S}(\xi)| &\leq \frac{\alpha\sigma N}{4|B|}\sum_{\xi\notin\mathcal{L}}|\widehat{g}(\xi)|^2\\ &\leq \frac{\alpha\sigma N}{4|B|}\sum_{\xi\in\mathbb{Z}_N}|\widehat{g}(\xi)|^2\\ &= \frac{\alpha\sigma}{4|B|}\sum_{x\in\mathbb{Z}_N}|g(x)|^2\\ &= \frac{\alpha\sigma}{4|B|}\sum_{x\in\mathbb{Z}_N}|f(x)-\alpha B(x)|^2\\ &= \frac{\alpha\sigma}{4|B|}\sum_{x\in\mathbb{Z}_N}f(x)^2 - 2\frac{\alpha^2\sigma}{4|B|}\sum_{x\in\mathbb{Z}_N}f(x)B(x) + \frac{\alpha^3\sigma}{4|B|}\sum_{x\in\mathbb{Z}_N}B(x)^2\\ &\leq \frac{\alpha^2\sigma}{4} - \frac{2\alpha^3\sigma}{4} + \frac{\alpha^3\sigma}{4}\\ &= \frac{\alpha\sigma}{4}(\alpha-\alpha^2)\\ &\leq \frac{\alpha^2\sigma}{4}\end{aligned}$$

Hence

$$\frac{N^2}{|B||B'|}\sum_{\xi\in\mathcal{L}}|\widehat{g}(\xi)|^2|\widehat{S}(\xi)| \geq \frac{\alpha^2\sigma}{4} + O(d\delta'\delta^{-1}).$$

Since $\frac{N}{|B'|}|\widehat{S}(\xi)|$ is trivially bounded by σ, we have

$$\frac{N}{|B|}\sum_{\xi\in\mathcal{L}}|\widehat{g}(\xi)|^2 \geq \frac{\alpha^2}{4} + O(d\delta'\delta^{-1}\sigma). \tag{7.9}$$

We now apply the localized version of Chang's theorem proved in [18] (Proposition 4.2) to $S \subset B'$, with $\epsilon = \alpha/4$ and $\eta = 1/2$. We conclude that there is a set $\Lambda \subset \mathbb{Z}_N$ and a $\delta_0'' > 0$ such that

$$|\Lambda| \ll \frac{2^4}{\alpha^2}\log\sigma^{-1},$$

$$\delta_0'' \gg \frac{\delta'\alpha^2 4}{d^2\log\sigma^{-1}},$$

and

$$\mathcal{L} \subset \{\xi \in \mathbb{Z}_N : |1 - e^{-2\pi i x\xi/N}| \leq 1/2 \ \forall\ x \in B(\Gamma\cup\Lambda, \delta_0'')\}.$$

Choose $\delta'' \in (\delta_0'', 2\delta_0'')$ such that $B'' := B(\Gamma\cup\Lambda, \delta'')$ is regular. Note that this together with (7.3) implies that δ'' obeys the condition in (ii). We may also assume that $\delta'' < \delta'$. Our goal is to get the L^2 density increment as in (7.2) on a translate of B''.

By the definition of $\mathcal{L}$, we have $\frac{N}{|B''|}|\widehat{B''}(\xi)| \geq 1/2$ for all $\xi \in \mathcal{L}$. Hence

$$\frac{N^3}{|B||B''|^2}\sum_{\xi\in\mathcal{L}}|\widehat{g}(\xi)|^2|\widehat{B''}(\xi)|^2 \geq \frac{\alpha^2}{16} + O(d\delta'\delta^{-1}).$$

Again using Plancherel's identity and the convolution identity we have

$$\begin{aligned}\alpha^2\big(\frac{1}{16} + O(\alpha^{-2}d\delta'\delta^{-1})\big) &\leq \frac{N^3}{|B||B''|^2}\sum_{\xi\in\mathbb{Z}_N}|\widehat{g}(\xi)|^2|\widehat{B''}(\xi)|^2 \\ &= \frac{N^3}{|B||B''|^2}\sum_{\xi\in\mathbb{Z}_N}|N^{-1}\widehat{g * B''}(\xi)|^2 \\ &= \frac{1}{|B||B''|^2}\sum_{x\in\mathbb{Z}_N}|g * B''(x)|^2.\end{aligned}$$

We now apply Lemma 5.2 from [18] and conclude that

$$\begin{aligned}\frac{1}{|B''|}\sup_{x\in\mathbb{Z}_N}|f * B''(x)| &\geq \alpha\big(1 + 2^{-4} + O(\alpha^{-2}d\delta'\delta^{-1})\big) + O(d\delta''\delta^{-1}) \\ &\geq \alpha\big(1 + 2^{-4}\big) + O(d\alpha^{-1}\delta'\delta^{-1}).\end{aligned}$$

We now let the constant c_0 in (7.3) be small enough, so that the error term is bounded by $\alpha 2^{-5}$. The conclusion (ii) follows if we choose b'' to maximize $|f * B''(b'')|$.

Proposition 7.2. *Let $f : \mathbb{Z}_N \to [0,1]$ be defined such that*

$$\mathbb{E}_{x\in\mathbb{Z}_N} f(x) = \alpha > 0.$$

Let $\sigma \in (0,1]$. Then there exist Bohr sets $B := b + B(\Gamma,\delta)$ and $B' := b + B(\Gamma,\delta')$ such that

$$\Big|\{x \in B' :\ f * f(x) \geq \frac{\alpha^2}{2}|B|\}\Big| > (1-\sigma)|B'|,$$

and

$$\delta' \gg \frac{\alpha^2\delta}{|\Gamma|},$$

$$\delta \gg \big(\frac{\alpha}{\log(\sigma^{-1})}\big)^{C\log(\alpha^{-1})},$$

and

$$|\Gamma| \ll \alpha^{-2}\log(\sigma^{-1}).$$

Proof of Proposition 7.2. We construct the Bohr sets B and B' by iterating Proposition 7.1. Let $\Gamma_0 := \{0\}$, and pick $\delta_0 \gg 1$ so that $B(\Gamma_0,\delta_0)$ is regular. Define $\alpha_0 := \alpha$. Averaging over translates of $B(\Gamma_0,\delta_0)$, we see that there is a b_0 such that $\mathbb{E}(f|B_0) \geq \alpha_0$ for $B_0 = b_0 + B(\Gamma_0,\delta_0)$. By Proposition 7.1, one of the following must hold:

(i) There is a $\delta_0' \gg \frac{\alpha_0^2\delta_0}{|\Gamma_0|}$ such that $B_0' := b_0 + B(\Gamma_0,\delta_0')$ is regular and

$$\Big|\{x \in B_0' : (f*f)(x) \geq \frac{\alpha_0^2}{2}|B_0|\}\Big| \geq (1-\sigma)|B_0'|, \tag{7.10}$$

(ii) There is a regular Bohr set $B_1 := b_1 + B(\Gamma_0 \cup \Lambda_0, \delta_1)$ such that

$$\mathbb{E}(f|B_1) \geq \alpha_0(1+2^{-5}), \tag{7.11}$$

where $|\Gamma_0| \ll \alpha_0^{-2}\log(\sigma^{-1})$ and $\delta_1 \gg \frac{\alpha_0^4\delta_0}{|\Gamma_0|^3\log(\sigma^{-1})}$.

If (i) holds, we let $B' = B_0'$ and we are done. If on the other hand (ii) holds, we repeat the procedure with B_0 replaced by B_1, and continue by induction. If we have not satisfied (i) by the end of the kth step, we have found a regular Bohr set $B_k := b_k + B(\Gamma_k,\delta_k)$ such that

$$\mathbb{E}(f|B_k) = \alpha_k|B_k|,$$

where

$$\alpha_k \geq \alpha_{k-1}(1+2^{-5}), \tag{7.12}$$

$$\delta_k \gg \frac{\alpha_{k-1}^4\delta_{k-1}}{|\Gamma_{k-1}|^3\log(\sigma^{-1})}, \tag{7.13}$$

and

$$|\Gamma_k| - |\Gamma_{k-1}| \ll \alpha_{k-1}\log(\sigma^{-1}). \tag{7.14}$$

The iteration must terminate (upon reaching density 1 on a large enough Bohr set) after at most

$$k \ll \log(\alpha^{-1})$$

steps, since from (7.12) we have

$$\alpha_k^2 \geq \alpha^2(1+2^{-5})^{k-1}.$$

By (7.14) we have

$$\begin{aligned}|\Gamma_k| &\ll \alpha_{k-1}^{-2}\log(\sigma-1) + \alpha_{k-2}^{-2}\log(\sigma^{-1}) + \cdots + \alpha_0^{-2}\log(\sigma^{-1}) \\ &\leq \alpha^{-2}\log(\sigma^{-1})\sum_{j=0}^{\infty}(1+2^{-5})^{-j} \ll \alpha^{-2}\log(\sigma^{-1}).\end{aligned}$$

Finally, using our bounds for α_k and $|\Gamma_k|$, we have

$$\delta_k \gg \big(\frac{\alpha}{\log(\sigma^{-1})}\big)^{C\log(\alpha^{-1})},$$

for some absolute constant $C > 0$.

8. The Restriction Argument

Assume that the hypotheses of Theorem 1.4 hold. We need to show that if f_1, f_2 are as in Lemma 2.5 and B, B' are the Bohr sets chosen in Proposition 7.2, then (6.6) holds, i.e.

$$\Big|\{x \in B' : \ |f_2 * f_i(x)| \geq \frac{\alpha^2}{10}|B|\}\Big| \leq \sigma|B'|, \ i = 1, 2. \tag{8.15}$$

It suffices to prove that

$$\|f_i * f_2\|_{L^2(B')}^2 \leq \frac{\alpha^4}{200}\sigma|B|^2|B'|. \tag{8.16}$$

We have

$$\begin{aligned}\|f_i * f_2\|_{L^2(B')}^2 &= \sum_{x\in B'}(f_i * f_2)^2(x) = \sum_{x\in B'}\Big(\sum_y f_i(y)f_2(x-y)\Big)\Big(\sum_z f_i(z)f_2(x-z)\Big) \\ &= \sum_{x,y,z,u,v} B'(x)f_i(y)f_2(z)\frac{1}{N}\sum_{\xi} e^{-2\pi i(y+z-x)\xi/N} \\ &\qquad \cdot f_i(u)f_2(v)\frac{1}{N}\sum_{\eta} e^{-2\pi i(u+v-x)\eta/N} \\ &= N^3\sum_{\xi,\eta}\widehat{B'}(-\eta-\xi)\widehat{f_i}(\xi)\widehat{f_2}(\xi)\widehat{f_i}(\eta)\widehat{f_2}(\eta) \\ &= N^3\sum_{\xi}(\widehat{B'} * \widehat{f_i}\widehat{f_2})(-\xi)\widehat{f_i}(\xi)\widehat{f_2}(\xi).\end{aligned}$$

By Hölder's inequality,

$$\|f_i * f_2\|^2_{L^2(B')} \leq N^3 \|\widehat{B'} * \widehat{f}_i\widehat{f}_2\|_{10} \, \|\widehat{f}_i\widehat{f}_2\|_{10/9}. \tag{8.17}$$

Applying Young's inequality, we get

$$\|\widehat{B'} * \widehat{f}_i\widehat{f}_2\|_{10} \leq \|\widehat{B'}\|_5 \, \|\widehat{f}_i\widehat{f}_2\|_{10/9}. \tag{8.18}$$

Furthermore,

$$\begin{aligned} \|\widehat{f}_i\widehat{f}_2\|^{10/9}_{10/9} &\leq \|\widehat{f}_2\|^{1/9}_\infty \sum_\xi |\widehat{f}_2(\xi)| \, |\widehat{f}_i(\xi)|^{10/9} \\ &\leq \|\widehat{f}_2\|^{1/9}_\infty \, \|\widehat{f}_2\|_{19/9} \, \|\widehat{f}_i\|^{10/9}_{19/9}, \end{aligned}$$

where at the last step we used Hölder's inequality again. Plugging this together with (8.18) in (8.17), we see that

$$\begin{aligned} \|f_i * f_2\|^2_{L^2(B')} &\leq N^3 \|\widehat{B'}\|_5 \, \|\widehat{f}_i\widehat{f}_2\|^2_{10/9} \\ &\leq N^3 \|\widehat{B'}\|_5 \left(\|\widehat{f}_2\|^{1/9}_\infty \, \|\widehat{f}_2\|_{19/9} \, \|\widehat{f}_i\|^{10/9}_{19/9} \right)^{9/5} \\ &\leq N^3 \|\widehat{B'}\|_5 \, \|\widehat{f}_2\|^{1/5}_\infty \, \|\widehat{f}_2\|^{9/5}_{19/9} \, \|\widehat{f}_i\|^2_{19/9}. \end{aligned}$$

By Plancherel's theorem and Lemma 2.5(iv), we have

$$\|\widehat{f}_i\|_2^2 \leq \|\widehat{f}\|_2^2 = N^{-1}\|f\|_2^2 \ll \alpha p^{-1} = \alpha N^\theta.$$

Since $\theta < 1/20$, it follows from Lemma 2.6 that

$$\|\widehat{f}\|_{19/9} = O(1) \text{ and } \|\widehat{f}_i\|_{19/9} = O(1), \ i = 1, 2.$$

By Lemma 2.5(iii), we have

$$\|\widehat{f}_2\|_\infty \leq C\epsilon_0.$$

Finally,

$$\|\widehat{B'}\|_5^5 \leq \|\widehat{B'}\|_\infty^3 \, \|\widehat{B'}\|_2^2 \leq \frac{|B'|^3}{N^3}\|\widehat{B'}\|_2^2 = \frac{|B'|^4}{N^4}.$$

Combining these estimates, we get

$$\|f_i * f_2\|^2_{L^2(B')} \ll N^3 \epsilon_0^{1/5} \frac{|B'|^{4/5}}{N^{4/5}}. \tag{8.19}$$

We need the right side of this to be smaller than $\frac{\alpha^4}{200}\sigma|B|^2|B'|$, i.e. we need to have

$$\epsilon_0^{1/5} \leq c\alpha^4\sigma \frac{|B|^2}{N^2}\frac{|B'|^{1/5}}{N^{1/5}} = c\alpha^4\sigma\mathbb{P}(B)^2\mathbb{P}(B')^{1/5}. \tag{8.20}$$

But by Lemma 2.3 and (6.2)–(6.4), $\mathbb{P}(B)$ and $\mathbb{P}(B')$ are bounded from below by

$$\mathbb{P}(B) \geq \mathbb{P}(B') \gg (c\delta'')^{|\Gamma|} \gg \Big(\frac{c\alpha}{\log k}\Big)^{c\alpha^{-2}\log\frac{1}{\alpha}\log k},$$

where we plugged in $\sigma = (16k)^{-1}$. Hence (8.20) holds if

$$\epsilon_0 \ll \alpha^{28}k^{-9}\Big(\frac{c\alpha}{\log k}\Big)^{c\alpha^{-2}\log\frac{1}{\alpha}\log k}. \tag{8.21}$$

A short calculation shows that (6.5) is sufficient to guarantee that (8.21) is satisfied.

9. Proof of Proposition 1.3

Let $0 < \sigma < (\alpha - \beta)/10$. Define ν, f, f_1, f_2 as in Section 6, except that instead of (4.1) we will require

$$\|f_1\|_\infty \leq 1 + \sigma, \tag{9.1}$$

which holds for large enough N (depending on σ and on the ϵ_0 in the definition of f_i) by the same argument as in Section 4.

It clearly suffices to prove that

$$\Big|\{x \in \mathbb{Z}_N : \ f * f(x) > 0\}\Big| \geq (\alpha - 10\sigma)N. \tag{9.2}$$

Indeed, (9.2) shows that the sumset $A + A$ in $\mathbb{Z}_N$ has size at least βN, and hence so does the sumset $A + A$ in $\mathbb{Z}$.

We first claim that if N is large enough, then

$$\Big|\{x \in \mathbb{Z}_N : \ f_1 * f_1(x) \geq \sigma\alpha N\}\Big| \geq (\alpha - 3\sigma)N. \tag{9.3}$$

To see this, we first note that

$$\|f_1 * f_1\|_1 = \|f_1\|_1^2 = \alpha^2N^2(1 + O(N^{-1/5})). \tag{9.4}$$

On the other hand, if (9.3) failed, we would have

$$\begin{aligned}\|f_1 * f_1\|_1 &\leq \sigma\alpha N \cdot N + \alpha N(1 + \sigma + O(N^{-1/5})) \cdot (\alpha - 3\sigma)N \\ &= \alpha^2N^2(1 + O(N^{-1/5})) - \sigma\alpha N^2,\end{aligned}$$

which contradicts (9.4). This proves (9.3).

The proof of (9.2) will be complete if we can show that

$$\Big|\{x \in \mathbb{Z}_N : |\ f_i * f_2(x)| \geq \frac{\sigma\alpha}{10}N\}\Big| \leq \sigma N. \tag{9.5}$$

To this end, we repeat the argument in Section 8. It suffices to prove that

$$\|f_i * f_2\|_2^2 \leq \frac{\sigma^2\alpha^2}{200}\sigma N^3. \tag{9.6}$$

As in Section 8 (with $B = B' = \mathbb{Z}_N$), we have

$$\|f_i * f_2\|_2^2 \ll \epsilon_0^{1/5} N^3, \tag{9.7}$$

and the right side is smaller than the right side of (9.6) if $\epsilon_0 \ll \sigma^{15}\alpha^{10}$, with a small enough implicit constant. Thus (9.5) holds for large enough N if ϵ_0 was chosen small enough.

10. Acknowledgements

The authors were supported in part by an NSERC Discovery Grant. We are grateful to Ben Green for suggesting the feasibility of Theorem 1.2, and to Ernie Croot and Mihalis Kolountzakis for helpful discussions and suggestions.

References

[1] J. Bourgain, *On arithmetic progressions in sums of sets of integers*, in *A tribute to Paul Erdős*, pp. 105-109, Cambridge University Press, 1990.

[2] J. Bourgain, *On triples in arithmetic progressions*, Geom. Funct. Anal. **9** (1999), 968–984.

[3] M.-C. Chang, *A polynomial bound in Freiman's theorem*, Duke Math. J. **113** (2002), 399–419.

[4] E. Croot, I.Ruzsa, T. Schoen, *Long arithmetic progressions in sparse sumsets*, Integers: The Electronic Journal of Combinatorial Number Theory, **7**(2) (2007), #A10.

[5] W.T. Gowers, *A new proof of Szemerédi's theorem*, Geom. Funct. Anal. **11** (2001), 465–588.

[6] B.J. Green, *Arithmetic progressions in sumsets*, Geom. Funct. Anal. **12** (2002), 584–597.

[7] B.J. Green, *On arithmetic structures in dense sets of integers*, Duke Math. Jour., **114** (2002), 215-238.

[8] B.J. Green, *Roth's Theorem in the primes*, Annals of Math. 161 (2005), 1609-1636.

[9] B.J. Green, T. Tao, *The primes contain arbitrarily long arithmetic progressions*, Annals of Math., to appear.

[10] B.J. Green, T. Tao, *Restriction theory of the Selberg Sieve, with applications*, Journal de Théorie des Nombers de Bordeaux, **18** (2006), 137–172.

[11] B.J. Green, T. Tao, *An inverse theorem for the Gowers $U^3(G)$ norm*, Proc. Edinburgh Math. Soc., to appear.

[12] Y. Kohayakawa, T. Łuczak, V. Rödl, *Arithmetic progressions of length three in subsets of a random set*, Acta Arith. **75** (1996), 133–163.

[13] M. B. Nathanson, *Additive Number Theory: The Classical Bases*, Springer, New York, 1996.

[14] J. Pintz, W.L. Steiger, E. Szemerédi, *On sets of natural numbers whose difference set contains no squares*, J. London Math. Soc. **37** (1988), 219-231.

[15] K. Roth, *On certain sets of integers*, J. London Math. Soc. **28** (1953), 245–252.

[16] I. Ruzsa, *Difference sets without squares*, Period. Math. Hungar. **15** (1984), no. 3, 205-209.

[17] I. Ruzsa, *Arithmetic progressions in sumsets*, Acta Arith. **60** (1991), 191–202.

[18] T. Sanders, *Additive structures in sumsets*, to appear in Math. Proc. Cambridge Philos. Soc.

[19] E. Szemerédi, *On sets of integers containing no four elements in arithmetic progression*, Acta Math. Acad. Sci. Hungar. **20** (1969), 89–104.

[20] E. Szemerédi, *On sets of integers containing no k elements in arithmetic progression*, Acta Arith. **27** (1975), 299–345.

[21] T. Tao, *Arithmetic progressions and the primes*, Collect. Math. (2006), Vol. Extra, 37-88.

[22] T. Tao, V. Vu, *Additive combinatorics*, Cambridge Univ. Press, 2006.

[23] P. Varnavides, *On certain sets of positive density*, Journal London Math. Soc., **34** (1959), 358–360