The Minimal Number of Three-Term Arithmetic Progressions Modulo a Prime Converges to a Limit

Ernie Croot *

October 22, 2018

Abstract

How few three-term arithmetic progressions can a subset $S \subseteq \mathbb{Z}_N := \mathbb{Z}/N\mathbb{Z}$ have if $|S| \geq vN$? (that is, $S$ has density at least $v$). Varnavides [4] showed that this number of arithmetic-progressions is at least $c(v)N^2$ for sufficiently large integers $N$; and, it is well-known that determining good lower bounds for $c(v) > 0$ is at the same level of depth as Erdős's famous conjecture about whether a subset $T$ of the naturals where $\sum_{n \in T} 1/n$ diverges, has a $k$-term arithmetic progression for $k = 3$ (that is, a three-term arithmetic progression).

The author answers a question of B. Green [1] about how this minimal number of progressions oscillates for a fixed density $v$ as $N$ runs through the primes, and as $N$ runs through the odd positive integers.

1 Introduction

Given an integer $N \geq 2$ and a mapping $f : \mathbb{Z}_N \to \mathbb{C}$ define

$$\Lambda_3(f) = \Lambda_3(f; N) := \mathbb{E}_{n,d \in \mathbb{Z}_N} (f(n)f(n + d)f(n + 2d)) = \frac{1}{N^2} \sum_{n,d \in \mathbb{Z}_N} f(n)f(n + d)f(n + 2d),$$

where $\mathbb{E}$ is the expectation operator, defined for a function $g : \mathbb{Z}_N \to \mathbb{C}$ to be

$$\mathbb{E}(g) = \mathbb{E}_n(g) := \frac{1}{N} \sum_{n \in \mathbb{Z}_N} g(n).$$

*Supported by an NSF grant
If \( S \subseteq \mathbb{Z}_N \), and if we identify \( S \) with its indicator function \( S(n) \), which is 0 if \( n \not\in S \) and is 1 if \( n \in S \), then \( \Lambda_3(S) \) is a normalized count of the number of three-term arithmetic progressions \( a, a + d, a + 2d \) in the set \( S \), including trivial progressions \( a, a, a \).

Given \( v \in (0, 1] \), consider the family \( \mathcal{F}(v) \) of all functions \( f : \mathbb{Z}_N \to [0, 1] \), such that \( \mathbb{E}(f) \geq v \).

Then, define
\[
\rho(v, N) := \min_{f \in \mathcal{F}(v)} \Lambda_3(f).
\]

From an old result of Varnavides [4] we know that
\[
\Lambda_3(f) \geq c(v) > 0,
\]
where \( c(v) \) does not depend on \( N \). A natural and interesting question (posed by B. Green [1]) is to determine whether for fixed \( v \)
\[
\lim_{p \to \infty, p \text{ prime}} \rho(v, p) \text{ exists?}
\]

In this paper we answer this question in the affirmative: \(^1\)

**Theorem 1** For a fixed \( v \in (0, 1] \) we have
\[
\lim_{p \to \infty, p \text{ prime}} \rho(v, p) \text{ exists.}
\]

Call the limit in this theorem \( \rho(v) \). Then, this theorem has the following immediate corollary:

**Corollary 1** For a fixed \( v \in (0, 1] \), let \( S \) be any subset of \( \mathbb{Z}_N \) such that \( \Lambda_3(S) \) is minimal subject to the constraint \( |S| \geq vN \). Let \( \rho_2(v, N) = \Lambda_3(S) \). Then,
\[
\lim_{p \to \infty, p \text{ prime}} \rho_2(v, p) = \rho(v).
\]

\(^1\)The harder, and more interesting question, also asked by B. Green, which we do not answer in this paper, is to give a simple formula for this limit.
Given Theorem 1, the proof of the corollary is standard, and just amounts to applying a functions-to-sets lemma, which works as follows: Given \( f : \mathbb{Z}_N \rightarrow [0,1] \), we let \( S_0 \) be a random subset of \( \mathbb{Z}_N \) where \( \mathbb{P}(s \in S_0) = f(s) \). It is then easy to show that with probability \( 1 - o(1) \),

\[
\mathbb{E}(S_0) \sim \mathbb{E}(f), \text{ and } \Lambda_3(S_0) \sim \Lambda_3(f).
\]

So, there will exist a set \( S_1 \) with these two properties (an instantiation of the random set \( S_0 \)). Then, by adding only a small number of elements to \( S_1 \) as needed, we will have a set \( S \) satisfying

\[
|S| \geq \nu N, \text{ and } \Lambda_3(S) \sim \Lambda_3(f).
\]

We will also prove the following:

**Theorem 2** For \( \nu = 2/3 \) we have that

\[
\lim_{N \to \infty} \rho(\nu, N) \text{ does not exist,}
\]

where here we consider all odd \( N \), not just primes.

Thus, in our proof of Theorem 1, we will make special use of the fact that our moduli are prime.

### 2 Basic Notation on Fourier Analysis

Given an integer \( N \geq 2 \) (not necessarily prime), and a function \( f : \mathbb{Z}_N \rightarrow \mathbb{C} \), we define the Fourier transform

\[
\hat{f}(a) = \sum_{n \in \mathbb{Z}_N} f(n) e^{2\pi i an/N}.
\]

Thus, the Fourier transform of an indicator function \( C(n) \) for a set \( C \subseteq \mathbb{Z}_N \) is:

\[
\hat{C}(a) = \sum_{n=0}^{N-1} C(n) e^{2\pi i an/N} = \sum_{n \in C} e^{2\pi i an/N}.
\]
Throughout the paper, when working with Fourier transforms, we will use a slightly compressed form of summation notation, by introducing the sigma operator, defined by

$$\sum_n f(n) = \sum_{n \in \mathbb{Z}_N} f(n).$$

We also define the norms

$$||f||_t = (\mathbb{E}|f(n)|^t)^{1/t},$$

which is the usual $t$-norm where we take our measure to be the uniform measure on $\mathbb{Z}_N$.

With our definition of norms, Hölder’s inequality takes the form

$$||f_1 f_2 \cdots f_n||_b \leq ||f_1||_{b_1} ||f_2||_{b_2} \cdots ||f_n||_{b_n},$$

if $\frac{1}{b} = \frac{1}{b_1} + \cdots + \frac{1}{b_n}$, although we will ever only need this for the product of two functions, and where the $a_i$ and $b_i$ are 1 or 2 (i.e. Cauchy-Schwarz).

In our proofs we will make use of Parseval’s identity, which says that

$$||\hat{f}||_2^2 = N||f||_2^2.$$  

This implies that

$$||\hat{C}||_2^2 = N|C|.$$  

We will also use Fourier inversion, which says

$$f(n) = N^{-1} \sum_a e^{-2\pi an/N} \hat{f}(a).$$

Another basic fact we will use is that

$$\Lambda_3(f) = N^{-3} \sum_a \hat{f}(a)^2 \hat{f}(-2a).$$

### 3 Key Lemmas

Here we list some key lemmas we will need in the course of our proof of Theorems 1 and 2.
Lemma 1 Suppose $h : \mathbb{Z}_N \to [0, 1]$, and let $\mathcal{C}$ denote the set of all values $a \in \mathbb{Z}_N$ for which

$$|\hat{h}(a)| \geq \beta \hat{h}(0).$$

Then,

$$|\mathcal{C}| \leq (\beta \hat{h}(0))^{-2}N^2.$$ 

Proof of the Lemma. This is an easy consequence of Parseval:

$$|\mathcal{C}|(\beta \hat{h}(0))^2 \leq N||\hat{h}||_2^2 = N^2||\hat{h}||_2^2 \leq N^2.$$ 

Lemma 2 Suppose that $f, g : \mathbb{Z}_N \to [-2, 2]$ have the property

$$||\hat{f} - \hat{g}||_{\infty} < \beta N.$$ 

Then,

$$|\Lambda_3(f) - \Lambda_3(g)| < 12\beta.$$ 

Proof of the Lemma. The proof is an exercise in multiple uses of Cauchy-Schwarz (or Hölder’s inequality) and Parseval.

First, let $\delta(a) = \hat{f}(a) - \hat{g}(a)$. We have that

$$\Lambda_3(f) = N^{-3}\sum_a \hat{f}(a)^2(\hat{g}(-2a) + \delta(-2a)) = N^{-3}\sum_a \hat{f}(a)^2\hat{g}(-2a) + E_1,$$

where by Parseval’s identity we have that the error $E_1$ satisfies

$$|E_1| \leq N^{-2}||\delta||_{\infty}||\hat{f}||_2^2 = N^{-1}||\delta||_{\infty}||f||_2^2 < 4\beta.$$ 

Next, we have that

$$N^{-3}\sum_a \hat{f}(a)^2\hat{g}(-2a) = N^{-3}\sum_a \hat{f}(a)(\hat{g}(a) + \delta(a))\hat{g}(-2a) = N^{-3}\sum_a \hat{f}(a)\hat{g}(a)\hat{g}(-2a) + E_2,$$

where by Parseval again, along with Cauchy-Schwarz (or Hölder’s inequality), we have that the error $E_2$ satisfies

$$|E_2| \leq N^{-2}||\hat{f}(a)\hat{g}(-2a)||_1||\delta||_{\infty} < \beta N^{-1}||\hat{f}||_2||\hat{g}||_2 \leq 4\beta.$$
Finally,

\[ N^{-3} \sum_a \hat{f}(a) \hat{g}(a) \hat{g}(-2a) = N^{-3} \sum_a (\hat{g}(a) + \delta(a)) \hat{g}(a) \hat{g}(-2a) = \Lambda_3(g) + E_3, \]

where by Parseval again, along with Cauchy-Schwarz (Hölder), we have that the error \( E_3 \) satisfies

\[ |E_3| \leq N^{-2} ||\delta||_\infty ||\hat{g}(a)\hat{g}(-2a)||_1 < \beta N^{-1} ||\hat{g}||^2_2 \leq 4\beta. \]

Thus, we deduce

\[ |\Lambda_3(f) - \Lambda_3(g)| < 12\beta. \]

\[ \blacksquare \]

The following Lemma and the Proposition after it make use of ideas similar to the “granularization” methods from \[2\] and \[3\].

**Lemma 3** For every \( t \geq 1 \), \( 0 < \epsilon < 1 \), the following holds for all primes \( p \) sufficiently large: Given any set of residues \( \{b_1, ..., b_t\} \subset \mathbb{Z}_p \), there exists a weight function \( \mu : \mathbb{Z}_p \to [0, 1] \) such that

- \( \hat{\mu}(0) = 1 \) (in other words, \( \mathbb{E}(\mu) = p^{-1} \));
- \( |\hat{\mu}(b_i) - 1| < \epsilon^2 \), for all \( i = 1, 2, ..., t \); and,
- \( ||\hat{\mu}||_1 \leq p^{-1}(6\epsilon^{-1})^t \).

**Proof.** We begin by defining the functions \( y_1, ..., y_t : \mathbb{Z}_p \to [0, 1] \) by defining their Fourier transforms: Let \( c_i \equiv b_i^{-1} \pmod{p} \), \( L = [\epsilon p/10] \), and define

\[ \tilde{y}_i(a) = (2L + 1)^{-1} \left( \sum_{|j| \leq L} e^{2\pi i ac_i j/p} \right)^2 \in \mathbb{R}_{\geq 0}. \]

It is obvious that \( 0 \leq y_i(n) \leq 1 \), and \( y_i(0) = 1 \). Also note that

\[ y_i(n) \neq 0 \text{ implies } b_i n \equiv j \pmod{p}, \text{ where } |j| \leq 2L. \] \hspace{1cm} (1)

Now we let \( v(n) = y_1(n)y_2(n) \cdots y_t(n) \). Then,

\[ \hat{v}(a) = p^{-t+1}(\hat{y}_1 * \hat{y}_2 * \cdots * \hat{y}_t)(a) = p^{-t+1} \sum_{r_1 + \cdots + r_t = a} \hat{y}_1(r_1)\hat{y}_2(r_2) \cdots \hat{y}_t(r_t). \] \hspace{1cm} (2)
Now, as all the terms in the sum are non-negative reals we deduce that for $p$ sufficiently large,

$$p > \hat{v}(0) \geq p^{-t+1} \hat{y}_1(0) \cdots \hat{y}_t(0) = p^{-t+1}(2L + 1)^t > (\epsilon/6)^t p. \quad (3)$$

We now let $\mu(a)$ be the weight whose Fourier transform is defined by

$$\hat{\mu}(a) = \hat{v}(0)^{-1} \hat{v}(a). \quad (4)$$

Clearly, $\mu(a)$ satisfies conclusion 1 of the lemma.

Consider now the value $\hat{\mu}(b_i)$. As $\mu(n) \neq 0$ implies $y_i(n) \neq 0$, from (4) we deduce that if $\mu(n) \neq 0$, then for some $|j| \leq 2L$,

$$\text{Re}(e^{2\pi i b_i n/p}) = \text{Re}(e^{2\pi j/p}) = \cos(2\pi j/p) \geq 1 - \frac{1}{2}(2\pi \epsilon / 5)^2 > 1 - \epsilon^2.$$ 

So, since $\hat{\mu}(b_i)$ is real, we deduce that

$$\hat{\mu}(b_i) = \hat{v}(0)^{-1} \sum_n v(n) e^{2\pi i b_i n/p} > 1 - \epsilon^2.$$ 

So, our weight $\mu(n)$ satisfies the second conclusion of our Lemma.

Now, then, from (2), (4), and (3) we have that

$$||\tilde{u}||_1 = p^{-t} \hat{v}(0)^{-1} \sum_a \sum_{r_1+\cdots+r_t = a} \hat{y}_1(r_1) \hat{y}_2(r_2) \cdots \hat{y}_t(r_t)$$

$$= p^{-t} \hat{v}(0)^{-1} \prod_{i=1}^t \sum_r \hat{y}_i(r)$$

$$= \hat{v}(0)^{-1} y_1(0) y_2(0) \cdots y_t(0)$$

$$= \hat{v}(0)^{-1}$$

$$< p^{-1} (6\epsilon^{-1})^t. \quad \blacksquare$$

Next we have the following Proposition, which is an extended corollary of Lemmas 2 and 3.

**Proposition 1** For every $\epsilon > 0$, $p > p_0(\epsilon)$ prime, and every $f: \mathbb{Z}_p \to [0, 1]$,

there exists a periodic function $g: \mathbb{R} \to \mathbb{R}$ with period $p$ satisfying:

- $E(g) = E(f)$ (Here when we compute the expectation of $g$ we restrict to $g: \{0, \ldots, p-1\} \to \mathbb{R}$, and treat it as a mapping from $\mathbb{Z}_p.$)

- $g: \mathbb{R} \to [-2\epsilon, 1 + 2\epsilon].$
\[ g(n) = p^{-1} \sum_{1 \leq i \leq m} e^{-2\pi i c_i n/p} \hat{g}(c_i). \]

- \( \hat{g} \) has “small” (approximate) support, when treated as a function from \( \mathbb{Z}_p \to \mathbb{R} \). That is, there is a set of residues \( c_1, ..., c_m \in \mathbb{Z}_p, m < m_0(\epsilon), \)
satisfying

- The \( c_i \) satisfy \( |c_i| < p^{1-1/m} \).
- \( |\Lambda_3(g) - \Lambda_3(f)| < 25\epsilon \).

**Proof of the Proposition.** We will need to define a number of sets and functions in order to begin the proof: Define

\[ \mathcal{B} = \{ a \in \mathbb{Z}_p : |\hat{f}(a)| > \epsilon \hat{f}(0) \}, \]

and let \( t = |\mathcal{B}| \). Define

\[ \mathcal{B}' = \{ a \in \mathbb{Z}_p : |\hat{f}(-2a)| > \epsilon |\hat{f}(a)| > \epsilon(\epsilon/6)^t \hat{f}(0) \}, \]

and let \( m = |\mathcal{B}'| \). Note that \( \mathcal{B} \subseteq \mathcal{B}' \) implies \( t \leq m \). Lemma 1 implies that \( m < m_0(\epsilon) \), where \( m_0(\epsilon) \) depends only on \( \epsilon \).

Let \( \mu : \mathbb{Z}_p \to [0, 1] \) be as in Lemma 3 with parameter \( \epsilon \) and with \( \{b_1, ..., b_t\} = \mathcal{B} \).

Let \( 1 \leq s \leq p - 1 \) be such that for every \( b \in \mathcal{B}' \),

\[ b \equiv sc \pmod{p}, \text{ where } |c| < p^{1-1/m}; \]

such \( s \) exists by the Dirichlet Box Principle. Let \( c_1, ..., c_m \) be the values \( c \) so produced. \(^2\)

Define

\[ h(n) = (\mu * f)(sn) = \sum_{a+b \equiv n} \mu(sa)f(sb). \]

We have that \( h : \mathbb{Z}_p \to [0, 1] \) and

\[ \hat{h}(a) = \hat{\mu}(sa) \hat{f}(sa). \]

Finally, define \( g : \mathbb{R} \to \mathbb{R} \) to be

\[ g(\alpha) = p^{-1} \sum_{1 \leq i \leq m} e^{-2\pi i c_i \alpha / p} \hat{h}(c_i), \]

which is a truncated inverse Fourier transform of \( \hat{h} \). We note that if \( |\alpha - \beta| < 1 \), then since \( |c_i| < p^{1-1/m} \) we deduce that

\[ |g(\alpha) - g(\beta)| < p^{-1} m \left| e^{2\pi i (\alpha - \beta) p^{-1/m}} - 1 \right| \sup_i |\hat{h}(c_i)| < \epsilon, \quad (5) \]

\(^2\)Here is where we are using the fact that \( p \) is prime: We need it to prove that such \( s \) exists, and to extract the values of \( c \) from congruences \( b \equiv sc \pmod{p} \).
for \( p \) sufficiently large.

This function \( g \) clearly satisfies the first property
\[
\hat{g}(0) = \hat{h}(0) = \hat{\mu}(0)\hat{f}(0) = \hat{f}(0).
\]
(Fourier transforms are with respect to \( \mathbb{Z}_p \)).

Next, suppose that \( n \in \mathbb{Z}_p \). Then,
\[
g(n) = h(n) - p^{-1}\sum_{c \neq c_1, \ldots, c_m} e^{-2\pi icn/p}\hat{\mu}(sc)\hat{f}(sc) = h(n) - \delta,
\]
where
\[
|\delta| \leq ||\hat{\mu}||_1 \sup_{c \neq c_1, \ldots, c_m} |\hat{f}(sc)| = ||\hat{\mu}||_1 \sup_{b \in \mathbb{Z}_p \setminus B'} |\hat{f}(b)| < \epsilon.
\]

From this, together with (5) we have that for \( \alpha \in \mathbb{R} \), \( g(\alpha) \in [-2\epsilon, 1+2\epsilon] \), as claimed by the second property in the conclusion of the proposition.

Next, we observe that
\[
\Lambda_3(g) = \Lambda_3(h) - E,
\]
where
\[
|E| \leq p^{-3}\sum_{c \neq c_1, \ldots, c_m} |\hat{h}(c)|^2|\hat{h}(-2c)| < \epsilon(\epsilon/6)^4 p^{-1}||\hat{h}||_2^2 \leq \epsilon^2/6.
\]

To complete the proof of the Proposition, we must relate \( \Lambda_3(h) \) to \( \Lambda_3(f) \): We begin by observing that if \( b \in B \), then
\[
|\hat{f}(b) - \hat{h}(s^{-1}b)| = |\hat{f}(b)||1 - \hat{\mu}(b)| < \epsilon^2 p. \tag{6}
\]
Also, if \( b \in \mathbb{Z}_p \setminus B \), then
\[
|\hat{f}(b) - \hat{h}(s^{-1}b)| < 2|\hat{f}(b)| < 2\epsilon p.
\]
Thus,
\[
||\hat{f}(sa) - \hat{h}(a)||_\infty < 2\epsilon p.
\]

From Lemma 2 with \( \beta = 2\epsilon \) we conclude that
\[
|\Lambda_3(f) - \Lambda_3(h)| < 24\epsilon.
\]
So,

\[ |\Lambda_3(f) - \Lambda_3(g)| < 25\epsilon. \]

Finally, we will require the following two technical lemmas, which are used in the proof of Theorem 2:

**Lemma 4** Suppose \( p \) is prime, and suppose that \( S \subseteq \mathbb{Z}_p \) satisfies

\[ p/3 < |S| < 2p/5. \]

Let \( r(n) \) be the number of pairs \((s_1, s_2) \in S \times S\) such that \( n = s_1 + s_2 \). Then, if \( T \subseteq \mathbb{Z}_p \), and \( p \) is sufficiently large, we have

\[ \sum_{n \in T} r(n) < 0.93|S|(|S||T|)^{1/2}. \]

**Proof of the Lemma.** First, observe that if \( 1 \leq a \leq p - 1 \), then among all subsets \( S \subseteq \mathbb{Z}_p \) of cardinality at most \( p/2 \), the one which maximizes \( |\hat{S}(a)| \) satisfies

\[ |\hat{S}(a)| = \left| 1 + e^{2\pi i/p} + e^{4\pi i/p} + \cdots + e^{2\pi i(|S|-1)/p} \right| = \frac{|e^{2\pi i|S|/p} - 1|}{|e^{2\pi i/p} - 1|} \frac{|\sin(\pi|S|/p)|}{|\sin(\pi/p)|}. \]

Since \( |\theta| > \pi/3 \) we have that

\[ |\sin(\theta)| < \frac{\sin(\pi/3)|\theta|}{\pi/3} = \frac{3\sqrt{3}|\theta|}{2\pi}. \]

This can be seen by drawing a line passing through \((0, 0)\) and \((\pi/3, \sin(\pi/3))\), and realizing that for \( \theta > \pi/3 \) we have \( \sin(\theta) \) lies below the line. Thus, since \( p/3 < |S| < 2p/5 \) we deduce that for \( a \neq 0 \),

\[ |\hat{S}(a)| < \frac{3\sqrt{3}|S|}{2p|\sin(\pi/p)|} \sim \frac{3\sqrt{3}|S|}{2\pi}. \]

Thus, by Parseval,

\[ ||S * S||_2^2 = p^{-1}||\hat{S}||_4^4 \leq p^{-2}|S|^4 + p^{-1}(||\hat{S}||_2^2 - p^{-1}|S|^2) \sup_{a \neq 0} |\hat{S}(a)|^2 \]

\[ < 0.856p^{-1}|S|^3, \]
for $p$ sufficiently large.

By Cauchy-Schwarz we have that

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

$$= |T|^{1/2} p^{1/2} \|SS\|_2$$

$$< 0.93 |S| (|S||T|)^{1/2}.$$  ■

**Lemma 5** Suppose $N \geq 3$ is odd, and suppose $A \subseteq \mathbb{Z}_N$, $|A| = vN$. Let $A'$ denote the complement of $A$. Then,

$$\Lambda_3(A) + \Lambda_3(A') = 3v^2 - 3v + 1$$

**Proof.** The proof is an immediate consequence of the fact that $\hat{A}(0) = (1 - v)N$, together with $\hat{A}(a) = -\hat{A}'(a)$ for $1 \leq a \leq N - 1$. For then, we have

$$\Lambda_3(A) + \Lambda_3(A') = N^{-3} \sum_a \hat{A}(a)^2 \hat{A}(-2a) + \hat{A}'(a) \hat{A}'(-2a)$$

$$= v^3 + (1 - v)^3$$

$$= 3v^2 - 3v + 1.$$  ■

**4 Proof of Theorem 1**

To prove the theorem it suffices to show that for every $0 < \epsilon, v < 1$, every pair of primes $p, r$ with $r > p^3 > p_0(\epsilon)$, and every function $f : \mathbb{Z}_p \to [0, 1]$ satisfying $E(f) \geq v$, there exists a function $\ell : \mathbb{Z}_r \to [0, 1]$ satisfying $E(\ell) \geq v$, such that

$$\Lambda_3(\ell) < \Lambda_3(f) + \epsilon$$  (7)

This then implies

$$\rho(v, r) < \rho(v, p) + \epsilon,$$

and then our theorem follows (because then $\rho(r, v)$ is approximately decreasing as $r$ runs through the primes.)

To prove (7), let $f : \mathbb{Z}_p \to [0, 1]$ satisfy $E(f) \geq v$. Then, applying Proposition 1 we deduce that there is a map $g : \mathbb{R} \to \mathbb{R}$ satisfying the
conclusion of that proposition. Let \(c_1, ..., c_m, |c_i| < p^{1-1/m}\) be as in the proposition.

Define

\[
h(\alpha) = p^{-1} \sum_{1 \leq i \leq m} e^{-2\pi i a c_i} \hat{g}(c_i) = g(\alpha p/r) \in [-2\epsilon, 1 + 2\epsilon].
\]

If we restrict to integer values of \(\alpha\), then we have that \(h\) has the following properties

- \(h : \mathbb{Z}_r \to [-2\epsilon, 1 + 2\epsilon]\).
- \(\mathbb{E}(h) = \mathbb{E}(g) \geq vr\). (Here, \(\mathbb{E}(g)\) is computed by restricting to \(g : \{0, ..., p-1\} \to \mathbb{R}\).)
- For \(|a| < r/2\) we have \(\hat{h}(a) \neq 0\) if and only if \(a = c_i\) for some \(i\), where \(|c_i| < p^{1-1/m}\), in which case \(\hat{h}(c_i) = r \hat{g}(c_i)/p\).

From the third conclusion we get that

\[
\Lambda_3(h) = r^{-3} \sum_{1 \leq i \leq m} \hat{h}(c_i)^2 \hat{h}(-2c_i) = \Lambda_3(g).
\]

Then, from the final conclusion in Proposition \(\Pi\) we have that

\[
\Lambda_3(h) < \Lambda_3(f) + 25\epsilon. \tag{8}
\]

This would be the end of the proof of our theorem were it not for the fact that \(h : \mathbb{Z}_r \to [-2\epsilon, 1 + 2\epsilon]\), instead of \(\mathbb{Z}_r \to \{0, 1\}\). This is easily fixed: First, we let \(\ell_0 : \mathbb{Z}_r \to [0, 1]\) be defined by

\[
\ell_0(n) = \begin{cases} h(n), & \text{if } h(n) \in [0, 1]; \\ 0, & \text{if } h(n) < 0; \\ 1, & \text{if } h(n) > 1. \end{cases}
\]

We have that

\[
|\ell_0(n) - h(n)| \leq 2\epsilon, \text{ and therefore } ||\hat{\ell}_0 - \hat{h}||_\infty < 2\epsilon r.
\]

It is clear that by reassigning some of the values of \(\ell_0(n)\) we can produce a map \(\ell : \mathbb{Z}_r \to [0, 1]\) such that \(^3\)

\[
\mathbb{E}(\ell) = \mathbb{E}(h), \text{ and } ||\hat{\ell} - \hat{h}||_\infty < 4\epsilon r.
\]

\(^3\)If \(\hat{\ell}_0(0) > \hat{h}(0)\), then we reassign some of the \(n\) where \(\ell_0(n) = 1\) to 0, so that we then get \(\hat{h}(0) - \hat{\ell}_0(0) < \hat{h}(0) + 1\), and then we change one more \(n\) where \(\ell_0(n) = 0\) to produce \(\ell : \mathbb{Z}_r \to [0, 1]\) satisfying \(\ell(0) = h(0)\); likewise, if \(\ell_0(0) < \hat{h}(0)\), we reassign some values where \(\ell_0(n) = 0\) to 1.
From Lemma 2 we then deduce
\[ |\Lambda_3(\ell) - \Lambda_3(h)| < 48\epsilon; \]
and so,
\[ E(\ell) = E(f), \quad \text{and} \quad \Lambda_3(\ell) < \Lambda_3(f) + 73\epsilon. \]
Our theorem is now proved on rescaling the $73\epsilon$ to $\epsilon$. ■

5 Proof of Theorem 2

A consequence of Lemma 5 is that for a given density $\upsilon$, the sets $A \subseteq \mathbb{Z}_N$ which minimize $\Lambda_3(A)$ are exactly those which maximize $\Lambda_3(A')$. If $3|N$ and $\upsilon = 2/3$, clearly if we let $A'$ be the multiplies of 3 modulo $N$, then $\Lambda_3(A')$ is maximized and therefore $\Lambda_3(A)$ is minimized. In this case, for every pair $m, m + d \in A'$ we have $m + 2d \in A'$, and so $\Lambda_3(A') = (1 - \upsilon)^2$. By the above lemma,
\[ \Lambda_3(A) = 3\upsilon^2 - 3\upsilon + 1 - (1 - \upsilon)^2 = 2\upsilon^2 - \upsilon = 2/9. \]
So,
\[ \rho(2/3, N) = 2/9. \]

The idea now is to show that
\[ \lim_{p \to \infty} \rho(2/3, p) \neq 2/9. \]

Suppose $p \equiv 1 \pmod{3}$ and that $A \subseteq \mathbb{Z}_p$ minimizes $\Lambda_3(A)$ subject to $|A| = (2p + 1)/3$. Let $S = \mathbb{Z}_p \setminus A$, and note that $|S| = (p - 1)/3$. Let $T = 2 * S = \{2s : s \in S\}$.

Now, if $r(n)$ is the number of pairs $(s_1, s_2) \in S \times S$ satisfying $s_1 + s_2 = n$, then by Lemma 4 we have
\[ \Lambda_3(T) = p^{-2} \sum_{n \in T} r(n) < 0.93p^{-2}|S||S|^{1/2} \leq 0.93/9, \]
for all $p$ sufficiently large. So, by Lemma 5 we have that
\[ \Lambda_3(A) > 0.23, \]
and therefore
\[ \rho(2/3, p) > 0.23 > 2/9 \]
for all sufficiently large primes $p \equiv 1 \pmod{3}$. This finishes the proof of the theorem. ■
6 Acknowledgements

I would like to thank Ben Green for the question, as well as for suggesting the proof of Theorem 1, which was a modification of an earlier proof of the author.

References

[1] Some Problems in Additive Combinatorics, AIM ARCC Workshop, compiled by E. Croot and S. Lev.

[2] B. Green, Roth’s Theorem in the Primes. Annals of Math. 161 (2005), 1609-1636.

[3] B. Green, I. Ruzsa, Counting Sumsets and Sumfree Sets Modulo a Prime. Studia Sci. Math. Hungar. 41 (2004), 285-293.

[4] P. Varavides, On Certain Sets of Positive Density, J. London Math. Soc. 34 (1959), 358-360.