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

Ernie Croot *

October 6, 2005

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 $f : \mathbb{Z}_N \to [0, 1]$ define

$$ T_3(f) = T_3(f; N) := \sum_{a+b=2c \pmod{N}} f(a)f(b)f(c). $$

Thus, 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 $T_3(S)$ is the number of three-term arithmetic progressions $a, a+d, a+2d$ in the set $S$, including trivial progressions $a, a, a$.

Given $v \in (0, 1]$, define

$$ \rho(v, N) = \frac{1}{N^2} \min_{S \subseteq \mathbb{Z}_N} \min_{|S| \geq vN} T_3(S). $$

---

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

In this paper we answer this question in the affirmative:

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

The harder, and more interesting question, also asked by B. Green, which we do not answer in this paper, is to give a formula for this limit as a function of \( v \).

We will also prove the following:

**Theorem 2** For \( v = 2/3 \) we have
\[ \lim_{N \to \infty \text{ odd}} N \rho(v, N) \text{ does not exist,} \]
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 \( f : \mathbb{Z}_N \to \mathbb{C} \), we define the Fourier transform
\[
\hat{f}(a) = \sum_{n=0}^{N-1} f(n)e^{2\pi i an/N}.
\]

Thus, the Fourier transform of an indicator function \( C(n) \) for a set \( C \subseteq \mathbb{Z}_N \) is:
\[
\hat{C}(a) = \sum_{n=0}^{N-1} C(n)e^{2\pi i an/N} = \sum_{n \in C} e^{2\pi i an/N}.
\]
We also define the usual norms
\[ ||f||_t = \left( \sum_{a=0}^{N-1} |f(a)|^t \right)^{1/t}. \]

In our proofs we will make use of Parseval’s identity, which says that
\[ ||\hat{f}||_2^2 = N||f||_2^2; \]

in other words,
\[ \sum_{a=0}^{N-1} |\hat{f}(a)|^2 = N \sum_{n=0}^{N-1} |f(n)|^2. \]

This implies that
\[ ||\hat{C}||_2^2 = N|C|. \]

Another basic fact we will use is that
\[ T_3(f) = \frac{1}{N} \sum_{a=0}^{N-1} \hat{f}(a)^2 \hat{f}(-2a). \]

3 Key Lemmas

Here we list out 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 \( C \) denote the set of all values \( a \in \mathbb{Z}_N \) for which
\[ |\hat{h}(a)| \geq \beta \hat{h}(0). \]

Then,
\[ |C| \leq \beta^{-2}(N/\hat{h}(0))^2. \]

**Proof of the Lemma.** This is an easy consequence of Parseval:
\[ |C|(\beta\hat{h}(0))^2 \leq ||\hat{h}||_2^2 = N||h||_2^2 \leq N^2. \]
Lemma 2 Suppose that \(f, g : \mathbb{Z}_N \to [-2, 2]\) have the property
\[
||\hat{f} - \hat{g}||_\infty < \beta N.
\]
Then,
\[
|T_3(f) - T_3(g)| < 12\beta N^2.
\]

Proof of the Lemma. The proof is an exercise in multiple uses of Cauchy-Schwarz and Parseval.

First, let \(\delta(a) = \hat{f}(a) - \hat{g}(a)\). We have that
\[
T_3(f) = \frac{1}{N} \sum_{a \in \mathbb{Z}_N} \hat{f}(a)^2(\hat{g}(-2a) + \delta(-2a))
= \left(\frac{1}{N} \sum_{a \in \mathbb{Z}_N} \hat{f}(a)^2\hat{g}(-2a)\right) + E_1,
\]
where by Parseval’s identity we have that the error \(E_1\) satisfies
\[
|E_1| \leq \frac{1}{N} ||\delta||_\infty ||\hat{f}||_2^2 < 4\beta N^2.
\]

Next, we have that
\[
\frac{1}{N} \sum_{a \in \mathbb{Z}_N} \hat{f}(a)^2\hat{g}(-2a) = \frac{1}{N} \sum_{a \in \mathbb{Z}_N} \hat{f}(a)(\hat{g}(a) + \delta(a))\hat{g}(-2a)
= \left(\frac{1}{N} \sum_{a \in \mathbb{Z}_N} \hat{f}(a)\hat{g}(a)\hat{g}(-2a)\right) + E_2,
\]
where by Parseval again, along with Cauchy-Schwarz, we have that the error \(E_2\) satisfies
\[
|E_2| \leq \frac{1}{N} ||\hat{f}(a)\hat{g}(-2a)||_1 ||\delta||_\infty < \beta ||\hat{f}||_2 ||\hat{g}||_2 \leq 4\beta N^2.
\]

Finally,
\[
\frac{1}{N} \sum_{a \in \mathbb{Z}_N} \hat{f}(a)\hat{g}(a)\hat{g}(-2a) = \frac{1}{N} \sum_{a \in \mathbb{Z}_N} (\hat{g}(a) + \delta(a))\hat{g}(a)\hat{g}(-2a)
= T_3(g) + E_3,
\]
where by Parseval again, along with Cauchy-Schwarz, we have that the error $E_3$ satisfies

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

Thus, we deduce

$$|T_3(f) - T_3(g)| < 12\beta N^2.$$

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 $\{b_1, \ldots, b_t\} \subset \mathbb{Z}_p$, there exists a weight function $\mu : \mathbb{Z}_p \rightarrow [0, 1]$ such that

- $||\mu||_1 = 1$;
- $|\hat{\mu}(b_i) - 1| < \epsilon^2$, for all $i = 1, 2, \ldots, t$; and,  
- $||\hat{\mu}||_1 \leq (6\epsilon)^t$.

**Proof.** We first define the functions $y_1, \ldots, y_t : \mathbb{Z}_p \rightarrow [0, 1]$, by defining their Fourier transforms: Let $c_i \equiv b_i^{-1} \pmod{p}$. Let $L = \lfloor ep/10 \rfloor$, and set

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

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

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

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

$$\hat{v}(a) = \frac{(\hat{y}_1 * \hat{y}_2 * \cdots * \hat{y}_t)(a)}{p^{t-1}}$$

$$= \frac{1}{p^{t-1}} \sum_{r_1 + r_2 + \cdots + r_t \equiv a \pmod{p}} \hat{y}_1(r_1)\hat{y}_2(r_2) \cdots \hat{y}_t(r_t). \quad (2)$$

Now, as all the terms in the sum are non-negative reals we deduce that for $p$ sufficiently large,

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

5
We now let $\mu(a)$ be the weight whose Fourier transform is defined by

$$\hat{\mu}(a) = \frac{\hat{v}(a)}{\hat{v}(0)} \tag{4}$$

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 (1) we deduce that if $\mu(n) \neq 0$, then for some $|j| \leq 2L$,

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

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

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

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

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

$$\sum_{a=0}^{p-1} |\hat{\mu}(a)| = \frac{1}{\hat{v}(0)}p^{\ell-1} \sum_{a=0}^{p-1} \sum_{r_1, r_i \equiv a \pmod{p}} \hat{y}_1(r_1)\hat{y}_2(r_2) \cdots \hat{y}_t(r_t)$$

$$= \frac{1}{\hat{v}(0)}p^{\ell-1} \prod_{i=1}^{t} \left( \sum_{r=0}^{p-1} \hat{y}_i(r) \right)$$

$$= \frac{p y_1(0)y_2(0) \cdots y_t(0)}{\hat{v}(0)}$$

$$= \frac{p}{\hat{v}(0)}$$

$$< (6\epsilon^{-1})^{\ell}.$$  

Next we have the following Proposition, which is an extended corollary of Lemma 3

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

- $\hat{g}(0) = \hat{f}(0)$.
- $g : \mathbb{R} \to [-2\epsilon, 1 + 2\epsilon]$. 

6
• \( \hat{g} \) has “small” support. That is, there is a set of residues \( c_1, \ldots, c_m \in \mathbb{Z}_p \), \( m < m_0(\epsilon) \), satisfying

\[
g(n) = \frac{1}{p} \sum_{i=1}^{m} e^{-2\pi i c_i n/p} \hat{g}(c_i).
\]

• The \( c_i \) satisfy \( |c_i| < p^{1/m} \).
• \( |T_3(g) - T_3(f)| < 25ep^2 \).

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

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

and let \( t = |B| \). Define

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

and let \( m = |B'| \). Note that \( B \subseteq B' \) 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 \( \{b_1, \ldots, b_t\} = B \).

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

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

such \( s \) exists by the Dirichlet Box Principle. Let \( c_1, \ldots, c_m \) be the values \( c \) so produced. \(^1\)

Define

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

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

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

\(^1\)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 \( b \equiv sc \pmod{p} \).
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
\[
|g(\alpha) - g(\beta)| < \frac{m \sup_i |\hat{h}(c_i)|}{p} |e^{2\pi i (\alpha - \beta)p^{-1/m}} - 1| < \epsilon,
\tag{5}
\]
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,
\[
g(n) = h(n) - \frac{1}{p} \sum_{c \in \mathbb{Z}_p \setminus \{c_1, \ldots, c_m\}} e^{-2\pi i cn/p} \hat{\mu}(sc) \hat{f}(sc) = h(n) - \delta,
\]
where
\[
|\delta| \leq \frac{1}{p} ||\hat{\mu}||_1 \sup_{c \in \mathbb{Z}_p \setminus \{c_1, \ldots, c_m\}} |\hat{f}(sc)| = \frac{1}{p} ||\hat{\mu}||_1 \sup_{b \in \mathbb{Z}_p \setminus B'} |\hat{f}(b)| < \epsilon.
\]

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
\[
T_3(g) = T_3(h) - E,
\]
where
\[
|E| = \frac{1}{p} \sum_{c \in \mathbb{Z}_p \setminus \{c_1, \ldots, c_m\}} |\hat{h}(c)|^2 |\hat{h}(-2c)| < \epsilon(\epsilon/6)^2 ||\hat{h}||_2^2 
\leq \epsilon^2 p^2/6.
\]

To complete the proof of the Proposition, we must relate $T_3(h)$ to $T_3(f)$: 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\[ |T_3(f) - T_3(h)| < 24\epsilon p^2.\]

So,\[ |T_3(f) - T_3(g)| < 25\epsilon p^2. \]

**Lemma 4** Given a weight $\theta : \mathbb{Z}_N \rightarrow [0, 1]$, there exists a set $B \subseteq \mathbb{Z}_N$ such that\[ |T_3(B) - T_3(\theta)| = O(N^{3/2}), \] and such that\[ \hat{\theta}(0) \leq |B| < \hat{\theta}(0) + 1. \]

**Proof.** Suppose that $T(0), ..., T(N - 1)$ are independent random variables indexed by the residue classes modulo $N$, such that $T(a)$ takes on the value 1 with probability $\theta(a)$, and takes on the value 0 with probability $1 - \theta(a)$.

Let\[ Y = \sum_{a=0}^{N-1} T(a), \]

and let\[ Z = \sum_{a+b=2c \mod N} T(a)T(b)T(c). \]

Then, we have that\[ \mathbb{E}(Y) = \sum_{a=0}^{N-1} \theta(a) = \hat{\theta}(0), \]

and\[ V(Y) = \sum_{a=0}^{N-1} \theta(a)(1 - \theta(a)) < N. \]

So, by Chebychev’s inequality, we have that\[ |Y - \mathbb{E}(Y)| \leq 2N^{1/2} \]
occurs with probability greater than 3/4.

Next, we observe that
\[ \mathbb{E}(Z) = T_3(\theta) \]

We also have that
\[ \mathbb{E}(Z^2) \leq T_3(\theta)^2 + 2 \sum_{a+b \equiv 2c \pmod{N}} 1 + \sum_{a+b \equiv 2c \pmod{N}} 1 \]
\[ + O(N^2) \]
\[ < \mathbb{E}(Z)^2 + 4N^3, \]
for \( N \) sufficiently large.

So, the variance of \( Z \) is
\[ V(Z) = \mathbb{E}(Z^2) - \mathbb{E}(Z)^2 < 4N^3. \]

It follows from Chebychev’s inequality that
\[ |Z - \mathbb{E}(Z)| \leq 3N^{3/2} \] (10)
with probability more than 5/9.

Thus, since both (9) and (10) occur simultaneously with positive probability, it is easy to see that there exists a subset \( B' \subseteq \{0,1,...,N-1\} \) satisfying
\[ ||B'| - \hat{\theta}(0)|| \leq 4N^{1/2}, \]
and
\[ |T_3(B') - T_3(\theta)| \leq 3N^{3/2} \] (11)

By adding or deleting at most \( 4N^{1/2} \) elements from \( B' \) we can produce a set \( B \) satisfying (8). Each of these elements we add or delete from \( B' \) to produce \( B \) alters the number of solutions \( a+b \equiv 2c \pmod{N} \), \( a,b,c \in B' \) by at most \( N \). So, the number solutions \( a+b \equiv 2c \pmod{N} \), \( a,b,c \in B' \) is within \( O(N^{3/2}) \) of the number of solutions with \( a,b,c \in B \). Combining this observation with (11), (7) follows, and the lemma is proved. \( \blacksquare \)

Finally, we will require the following technical lemma, which is used in the proof of Theorem 2:

**Lemma 5** 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 \( 1 < a \leq p - 1 \), 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 above 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,

\[
||S \ast S||_2^2 = \frac{1}{p} ||\hat{S}||_4^4 \leq \frac{|S|^4}{p} + \frac{1}{p}(||\hat{S}||_2^2 - |S|^2) \sup_{a \neq 0} |\hat{S}(a)|^2 < 0.856|S|^3,
\]

for \( p \) sufficiently large.

By Cauchy-Schwarz we have that

\[
\sum_{n \in T} r(n) \leq \left( \sum_{n=0}^{p-1} r(n)^2 \right)^{1/2} |T|^{1/2} = ||S \ast S||_2 |T|^{1/2} < 0.93|S|(|S|T|)^{1/2}.
\]
4 Proof of Theorem 1

To prove the theorem it suffices to show that for every $0 < \epsilon, \nu < 1$, every pair of primes $p, r$ with $r > p^3 > p_0(\epsilon)$, and every set $A \subseteq \mathbb{Z}_p$ satisfying $|A| \geq \nu p$, there exists a set $B \subseteq \mathbb{Z}_r$, $|B| \geq \nu r$, such that

\[
\frac{T_3(B)}{r^2} < \frac{T_3(A)}{p^2} + \epsilon. \tag{12}
\]

This then implies

\[
\rho(r, \nu) < \rho(p, \nu) + \epsilon,
\]

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

To prove (12), let $A \subseteq \mathbb{Z}_p$, where $|A| \geq \nu p$. Then, applying Proposition 1 with $f(n) = A(n)$, the indicator function for the set $A$, we deduce that there is a map $g: \mathbb{R} \to \mathbb{R}$ satisfying the conclusion of that proposition. Let $c_1, \ldots, c_m, |c_i| < p^{1-1/m}$ be as in the proposition.

Define

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

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

- $h: \mathbb{Z}_r \to [-2\epsilon, 1 + 2\epsilon]$.
- $\hat{h}(0) = r \hat{g}(0)/p = r|A|/p \geq \nu r$. (Here, the Fourier transform of $h$ is with respect to $\mathbb{Z}_r$, while the Fourier transform of $g$ is with respect to $\mathbb{Z}_p$.)
- 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 $h(c_i) = r \hat{g}(c_i)/p$.

From the third conclusion we get that

\[
T_3(h) = \frac{1}{r} \sum_{i=1}^{m} \frac{r^3}{p^2} \hat{g}(c_i)^2 \hat{g}(-2c_i) = \frac{r^2 T_3(g)}{p^2}.
\]

Then, from the final conclusion in Proposition 1 we have that

\[
\frac{T_3(h)}{r^2} < \frac{T_3(f)}{p^2} + 25\epsilon. \tag{13}
\]
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

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

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 \(^{2}\)

\[
\hat{\ell}(0) = \hat{h}(0), \quad \text{and } ||\hat{\ell} - \hat{h}||_{\infty} < 4\epsilon r.
\]

From Lemma 2 we then deduce

\[
|T_3(\ell) - T_3(h)| < 48\epsilon r^2.
\]

Then, from Lemma 4 applied with \( \theta = \ell \), there exits a subset \( B \subseteq \mathbb{Z}_r \) such that for some \( 0 \leq \delta < 1 \) we have

\[
|B| = \hat{\ell}(0) + \delta = \hat{h}(0) + \delta = \frac{r\hat{g}(0)}{p} + \delta = \frac{r|A|}{p} + \delta \\
\geq vr.
\]

Also,

\[
T_3(B) = T_3(\ell) + O(r^{3/2});
\]

and so,

\[
|T_3(B) - T_3(h)| \leq |T_3(B) - T_3(\ell)| + |T_3(\ell) - T_3(h)| \leq 49\epsilon r^2,
\]

for \( r \) sufficiently large. It follows then from (13) that

\[
\frac{T_3(B)}{r^2} < \frac{T_3(h)}{r^2} + 49\epsilon < \frac{T_3(f)}{p^2} + 74\epsilon.
\]

This then proves (12) on rescaling our 74\( \epsilon \) to \( \epsilon \), and our theorem follows.

---

\(^{2}\)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 \( \hat{h}(0) \leq \hat{\ell}_0(n) < \hat{h}(0) + 1 \), 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 \( \hat{\ell}_0(0) < \hat{h}(0) \), we reassign some values where \( \ell_0(n) = 0 \) to 1.
5 Proof of Theorem 2

We begin with a simple lemma:

**Lemma 6** Suppose \(N \geq 3\) is odd, and suppose \(A \subseteq \mathbb{Z}_N\), \(|A| = vN\). Let \(A'\) denote the complement of \(A\). Then,

\[
T_3(A) + T_3(A') = (3v^2 - 3v + 1)N^2.
\]

**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

\[
T_3(A) + T_3(A') = \frac{1}{N} \sum_{a=0}^{N-1} \hat{A}(a)^2 \hat{A}(-2a) + \hat{A}'(a)\hat{A}'(-2a)
\]

\[
= (v^3 + (1 - v)^3)N^2
\]

\[
= (3v^2 - 3v + 1)N^2. \qed
\]

A consequence of this lemma is that for a given density \(v\), the sets \(A \subseteq \mathbb{Z}_N\) which minimize \(T_3(A)\) are exactly those which maximize \(T_3(A')\). If \(3|N\) and \(v = 2/3\), clearly if we let \(A'\) be the multiplies of 3 modulo \(N\), then \(T_3(A')\) is maximized and therefore \(T_3(A)\) is minimized. In this case, for every pair \(m, m + d \in A'\) we have \(m + 2d \in A'\), and so \(T_3(A') = (1 - v)^2 N^2\). By the above lemma,

\[
T_3(A) = N^2(3v^2 - 3v + 1 - (1 - v)^2) = N^2(2v^2 - v) = \frac{2N^2}{9}.
\]

So,

\[
\rho(2/3, N) = \frac{2}{9}.
\]

The idea now is to show that

\[
\lim_{p \to \infty, p \text{ prime}} \rho(2/3, p) \neq \frac{2}{9}.
\]

Suppose \(p \equiv 1 \pmod{3}\) and that \(A \subseteq \mathbb{Z}_p\) minimizes \(T_3(A)\) subject to \(|A| = (2p + 1)/3\). Let \(S = \mathbb{Z}_p \setminus A\), and note that \(|S| = (p - 1)/3\). Let \(T = 2 \ast S = \{2s : s \in S\}\).
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 5 we have

\[
T_3(T) = \sum_{n \in T} r(n) < 0.93|S|(|S||T|)^{1/2} \leq 0.93p^2/9,
\]

for all \( p \) sufficiently large. So, by Lemma 6 we have that

\[
T_3(A) > 0.23p^2,
\]

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


