Canad. Math. Bull. Vol. **51** (1), 2008 pp. 47–56

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

Ernie Croot

Abstract. How few three-term arithmetic progressions can a subset $S \subseteq \mathbb{Z}_N := \mathbb{Z}/N\mathbb{Z}$ have if $|S| \geq \upsilon N$ (that is, S has density at least υ)? Varnavides showed that this number of arithmetic progressions is at least $c(\upsilon)N^2$ for sufficiently large integers N. It is well known that determining good lower bounds for $c(\upsilon) > 0$ is at the same level of depth as Erdös'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).

We answer a question posed by B. Green about how this minimial number of progressions oscillates for a fixed density υ 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 $f\colon \mathbb{Z}_N \to \mathbb{C}$ 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 $g\colon \mathbb{Z}_N \to \mathbb{C}$ to be

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

If $S \subseteq \mathbb{Z}_N$, and if we identify S with its indicator function $S(n)$, which is 0 if $n \notin S$ 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 $\upsilon \in (0,1]$, consider the family $\mathcal{F}(\upsilon)$ of all functions $f\colon \mathbb{Z}_N \to [0,1]$, such that $\mathbb{E}(f) \geq \upsilon$. Then define $\rho(\upsilon, N) := \min_{f\in\mathcal{F}(\upsilon)} \Lambda_3(f)$. From an old result of Varnavides [3], we know that $\Lambda_3(f) \geq c(\upsilon) > 0$, where $c(\upsilon)$ does not depend on N. A natural and interesting question (posed by B. Green[1]) is to determine whether

$$\lim_{\substack{p\to\infty \\ p \text{ prime}}} \rho(\upsilon, p)$$

Received by the editors November 1, 2005; revised May 2, 2006.
The author was supported by NSF grants DMS-0500863 and DMS-0301282
AMS subject classification: 05D99.

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

exists for fixed υ.

In this paper we answer this question in the affirmative.[2]

Theorem 1.1 *For a fixed $\upsilon \in (0,1]$,*

$$\lim_{\substack{p\to\infty \\ p \text{ prime}}} \rho(\upsilon, p)$$

exists.

Call the limit in this theorem $\rho(\upsilon)$. Then this theorem has the following immediate corollary.

Corollary 1.2 *For a fixed $\upsilon \in (0,1]$, let S be any subset of $\mathbb{Z}_N$ such that $\Lambda_3(S)$ is minimal subject to the constraint $|S| \geq \upsilon N$. Let $\rho_2(\upsilon, N) = \Lambda_3(S)$. Then*

$$\lim_{\substack{p\to\infty \\ p \text{ prime}}} \rho_2(\upsilon, p) = \rho(\upsilon).$$

Given Theorem 1.1, the proof of the corollary is standard, and just amounts to applying a functions-to-sets lemma, which works as follows: given $f\colon \mathbb{Z}_N \to [0,1]$, $\mathbb{E}(f) = \upsilon$, 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 $1 - o_\upsilon(1)$,

$$\mathbb{E}(S_0) \sim \mathbb{E}(f), \quad \text{and} \quad \Lambda_3(S_0) \sim \Lambda_3(f).$$

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 $|S| \geq \upsilon N$ and $\Lambda_3(S) \sim \Lambda_3(f)$.

We will also prove the following.

Theorem 1.3 *For $\upsilon = 2/3$,*

$$\lim_{\substack{N\to\infty \\ N \text{ odd}}} \rho(\upsilon, N)$$

does not exist, where here we consider all odd N, not just primes.

Thus, in our proof of Theorem 1.1, we will make special use of the fact that our moduli are prime.

[2]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.

https://doi.org/10.4153/CMB-2008-006-9 Published online by Cambridge University Press

2 Basic Notation on Fourier Analysis

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

$$\widehat{f}(a) = \sum_{n \in \mathbb{Z}_N} f(n) e^{2\pi i a n/N}.$$

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

$$\widehat{C}(a) = \sum_{n=0}^{N-1} C(n) e^{2\pi i a n/N} = \sum_{n \in C} e^{2\pi i a n/N}.$$

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

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

We also define 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

$$\|f_1 f_2 \cdots f_n\|_b \leq \|f_1\|_{b_1} \|f_2\|_{b_2} \cdots \|f_n\|_{b_n}, \quad \text{if } \frac{1}{b} = \frac{1}{b_1} + \cdots + \frac{1}{b_n},$$

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

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

This implies that $\|\widehat{C}\|_2^2 = N|C|$. We will also use Fourier inversion, which says

$$f(n) = N^{-1}\Sigma_a e^{-2\pi a n/N} \widehat{f}(a).$$

Another basic fact we will use is that

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

3 Key Lemmas

Here we list some key lemmas we will need in the course of our proof of Theorems 1.1 and 1.3.

Lemma 3.1 *Suppose $h\colon \mathbb{Z}_N \to [0,1]$, and let $\mathcal{C}$ denote the set of all values $a \in \mathbb{Z}_N$ for which $|\widehat{h}(a)| \geq \beta \widehat{h}(0)$. Then $|\mathcal{C}| \leq (\beta \widehat{h}(0))^{-2} N^2$.*

https://doi.org/10.4153/CMB-2008-006-9 Published online by Cambridge University Press

Proof This is an easy consequence of Parseval's identity:

$$|\mathcal{C}|(\beta\widehat{h}(0))^2 \le N\|\widehat{h}\|_2^2 = N^2\|h\|_2^2 \le N^2. \qquad \blacksquare$$

Lemma 3.2 *Suppose that $f, g\colon \to [-2,2]$ have the property $\|\widehat{f}-\widehat{g}\|_\infty < \beta N$. Then $|\Lambda_3(f) - \Lambda_3(g)| < 12\beta$.*

Proof The proof is an exercise in multiple uses of Cauchy–Schwarz (or Hölder's inequality) and Parseval's identity.

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

$$\begin{aligned}\Lambda_3(f) &= N^{-3}\Sigma_a \widehat{f}(a)^2(\widehat{g}(-2a) + \delta(-2a))\\ &= N^{-3}\Sigma_a \widehat{f}(a)^2\widehat{g}(-2a) \;+\; E_1,\end{aligned}$$

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

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

Next, we have that

$$\begin{aligned}N^{-3}\Sigma_a \widehat{f}(a)^2\widehat{g}(-2a) &= N^{-3}\Sigma_a \widehat{f}(a)(\widehat{g}(a) + \delta(a))\widehat{g}(-2a)\\ &= N^{-3}\Sigma_a \widehat{f}(a)\widehat{g}(a)\widehat{g}(-2a) + E_2,\end{aligned}$$

where by Parseval's identity again, along with Cauchy–Schwarz (or Hölder's inequality), we have that the error E_2 satisfies

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

Finally,

$$N^{-3}\Sigma_a \widehat{f}(a)\widehat{g}(a)\widehat{g}(-2a) = N^{-3}\Sigma_a(\widehat{g}(a) + \delta(a))\widehat{g}(a)\widehat{g}(-2a) = \Lambda_3(g) + E_3,$$

where by Parseval's identity again, along with Cauchy–Schwarz (Hölder), we have that the error E_3 satisfies

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

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 [1, 2].

Lemma 3.3 *For every $t \ge 1$, $0 < \epsilon < 1$, 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 $\mu\colon \mathbb{Z}_p \to [0,1]$ such that*

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

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

$$\widehat{y}_i(a) = (2L+1)^{-1} \big(\Sigma_{|j| \leq L} e^{2\pi i a c_i j/p} \big)^2 \in \mathbb{R}_{\geq 0}.$$

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

$$y_i(n) \neq 0 \text{ implies } b_i n \equiv j \pmod{p}, \text{ where } |j| \leq 2L. \tag{3.1}$$

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

$$\begin{aligned} \widehat{\nu}(a) &= p^{-t+1} (\widehat{y}_1 * \widehat{y}_2 * \cdots * \widehat{y}_t)(a) \\ &= p^{-t+1} \Sigma_{r_1 + \cdots + r_t \equiv a} \widehat{y}_1(r_1) \widehat{y}_2(r_2) \cdots \widehat{y}_t(r_t). \end{aligned} \tag{3.2}$$

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

$$p > \widehat{\nu}(0) \geq p^{-t+1} \widehat{y}_1(0) \cdots \widehat{y}_t(0) = p^{-t+1}(2L+1)^t > (\epsilon/6)^t p. \tag{3.3}$$

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

$$\widehat{\mu}(a) = \widehat{\nu}(0)^{-1} \widehat{\nu}(a). \tag{3.4}$$

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

Consider now the value $\widehat{\mu}(b_i)$. As $\mu(n) \neq 0$ implies $y_i(n) \neq 0$, from (3.1) we deduce that if $\mu(n) \neq 0$, then for some $|j| \leq 2L$,

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

So, since $\widehat{\mu}(b_i)$ is real, we deduce that $\widehat{\mu}(b_i) = \widehat{\nu}(0)^{-1} \Sigma_n \nu(n) e^{2\pi i b_i n/p} > 1 - \epsilon^2$. So our weight $\mu(n)$ satisfies (ii).

Now from (3.2), (3.4), and (3.3) we have that

$$\begin{aligned} \|\widehat{u}\|_1 &= p^{-t} \widehat{\nu}(0)^{-1} \Sigma_a \, \Sigma_{r_1 + \cdots + r_t \equiv a} \widehat{y}_1(r_1) \widehat{y}_2(r_2) \cdots \widehat{y}_t(r_t) \\ &= p^{-t} \nu(0)^{-1} \prod_{i=1}^{t} \Sigma_r \widehat{y}_i(r) = \widehat{\nu}(0)^{-1} y_1(0) y_2(0) \cdots y_t(0) = \widehat{\nu}(0)^{-1} \\ &< p^{-1}(6\epsilon^{-1})^t. \end{aligned}$$

■

Next we have the following proposition, which is an extended corollary of Lemmas 3.2 and 3.3.

https://doi.org/10.4153/CMB-2008-006-9 Published online by Cambridge University Press

Proposition 3.4 *For every $\epsilon > 0$, $p > p_0(\epsilon)$ prime, and every $f\colon \mathbb{Z}_p \to [0,1]$, there exists a periodic function $g\colon \mathbb{R} \to \mathbb{R}$ with period p satisfying:*

(i) $\mathbb{E}(g) = \mathbb{E}(f)$. *(Here we restrict to $g\colon \mathbb{Z}_p \to \mathbb{R}$ when we compute the expectation of g.)*

(ii) $g\colon \mathbb{R} \to [-2\epsilon, 1+2\epsilon]$.

(iii) *There is a set of integers $c_1, \dots, c_m$, $m < m_0(\epsilon)$, such that for $\alpha \in \mathbb{R}$,*

$$g(\alpha) = p^{-1}\Sigma_{1\le i\le m} e^{-2\pi i c_i \alpha/p}\widehat{g}(c_i),$$

where we get the Fourier transforms $\widehat{g}(c_i)$ by restricting $g\colon \mathbb{Z}_p \to \mathbb{R}$, which is possible by the periodicity of g.

(iv) *The c_i satisfy $|c_i| < p^{1-1/m}$.*

(v) $|\Lambda_3(g) - \Lambda_3(f)| < 25\epsilon$.

Proof We will need to define a number of sets and functions in order to begin the proof. Define $\mathcal{B} = \{a \in \mathbb{Z}_p : |\widehat{f}(a)| > \epsilon \widehat{f}(0)\}$, and let $t = |\mathcal{B}|$. Define

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

and let $m = |\mathcal{B}'|$. Note that $\mathcal{B} \subseteq \mathcal{B}'$ implies $t \le m$. Lemma 3.1 implies that $m < m_0(\epsilon)$, where $m_0(\epsilon)$ depends only on ϵ.

Let $\mu\colon \mathbb{Z}_p \to [0,1]$ be as in Lemma 3.3 with parameter ϵ and $\{b_1, \dots, b_t\} = \mathcal{B}$.

Let $1 \le s \le p-1$ be such that for every $b \in \mathcal{B}'$, if $c \equiv sb \pmod p$, $|c| < p/2$, then $|c| < p^{1-1/m}$. Such s exists by the Dirichlet Box Principle. Let $c_1, \dots, c_m$ be the values c so produced.[3]

Define $h(n) = (\mu * f)(sn) = \Sigma_{a+b\equiv n}\mu(sa)f(sb)$. We have that $h\colon \mathbb{Z}_p \to [0,1]$ and $\widehat{h}(a) = \widehat{\mu}(s^{-1}a)\widehat{f}(s^{-1}a)$. Note that $\widehat{h}(c_i) = \widehat{\mu}(b)\widehat{f}(b)$, for some $b \in \mathcal{B}'$.

Finally, define $g\colon \mathbb{R} \to \mathbb{R}$ to be $g(\alpha) = p^{-1}\Sigma_{1\le i\le m} e^{-2\pi i c_i\alpha/p}\widehat{h}(c_i)$, which is a truncated inverse Fourier transform of $\widehat{h}$. We note that if $|\alpha - \beta| < 1$, then since $|c_i| < p^{1-1/m}$, we deduce that

$$|g(\alpha) - g(\beta)| < p^{-1}m\left|e^{2\pi i(\alpha-\beta)p^{-1/m}} - 1\right| \sup_i |\widehat{h}(c_i)| < \epsilon, \tag{3.5}$$

for p sufficiently large.

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

Next, suppose that $n \in \mathbb{Z}_p$. Then,

$$g(n) = h(n) - p^{-1}\Sigma_{c\ne c_1,\dots,c_m} e^{-2\pi i c n/p}\widehat{\mu}(s^{-1}c)\widehat{f}(s^{-1}c) = h(n) - \delta,$$

where

$$|\delta| \le \|\widehat{\mu}\|_1 \sup_{c\ne c_1,\dots,c_m} |\widehat{f}(s^{-1}c)| = \|\widehat{\mu}\|_1 \sup_{b\in\mathbb{Z}_p\setminus\mathcal{B}'} |\widehat{f}(b)| < \epsilon.$$

[3] Here is where we are using the fact that p is prime: we need it in order that $c_1, \dots, c_m$ are distinct.

From this, together with (3.5), 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

$$|E| \leq p^{-3}\Sigma_{c \neq c_1,\ldots,c_m}|\widehat{h}(c)|^2|\widehat{h}(-2c)| < \epsilon(\epsilon/6)^t p^{-1}\|\widehat{h}\|_2^2 \leq \epsilon^2/6.$$

To complete the proof of the proposition, we must relate $\Lambda_3(h)$ to $\Lambda_3(f)$. We begin by observing that if $b \in \mathcal{B}$, then $|\widehat{f}(b) - \widehat{h}(sb)| = |\widehat{f}(b)||1 - \widehat{\mu}(b)| < \epsilon^2 p$. Also, if $b \in \mathbb{Z}_p \setminus \mathcal{B}$, then $|\widehat{f}(b) - \widehat{h}(sb)| < 2|\widehat{f}(b)| < 2\epsilon p$. Thus, $\|\widehat{f}(a) - \widehat{h}(sa)\|_\infty < 2\epsilon p$.

From Lemma 3.2 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 1.3.

Lemma 3.5 *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 $\Sigma_{n\in T} r(n) < 0.93|S|(|S||T|)^{1/2}$.*

Proof 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 $|\widehat{S}(a)|$ satisfies

$$|\widehat{S}(a)| = |1 + e^{2\pi i/p} + e^{4\pi i/p} + \cdots + e^{2\pi i(|S|-1)/p}| = \frac{|e^{2\pi i|S|/p} - 1|}{|e^{2\pi i/p} - 1|} = \frac{|\sin(\pi|S|/p)|}{|\sin(\pi/p)|}.$$

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 $a \neq 0$,

$$|\widehat{S}(a)| < \frac{3\sqrt{3}|S|}{2p|\sin(\pi/p)|} \sim \frac{3\sqrt{3}|S|}{2\pi}.$$

Thus, by Parseval's identity,

$$\|S * S\|_2^2 = p^{-1}\|\widehat{S}\|_4^4 \leq p^{-2}|S|^4 + p^{-1}(\|\widehat{S}\|_2^2 - p^{-1}|S|^2)\sup_{a\neq 0}|\widehat{S}(a)|^2 < 0.856p^{-1}|S|^3,$$

for p sufficiently large.

By Cauchy–Schwarz we have that

$$\Sigma_{n\in T} r(n) \leq |T|^{1/2}\big(\Sigma_n r(n)^2\big)^{1/2} = |T|^{1/2}p^{1/2}\|S * S\|_2 < 0.93|S|(|S||T|)^{1/2}. \quad ■$$

Lemma 3.6 *Suppose $N \geq 3$ is odd, and suppose $A \subseteq \mathbb{Z}_N$, $|A| = \upsilon N$. Let A' denote the complement of A. Then $\Lambda_3(A) + \Lambda_3(A') = 3\upsilon^2 - 3\upsilon + 1$.*

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

$$\begin{aligned}\Lambda_3(A) + \Lambda_3(A') &= N^{-3}\Sigma_a \widehat{A}(a)^2\widehat{A}(-2a) + \widehat{A}'(a)\widehat{A}'(-2a)\\ &= \upsilon^3 + (1-\upsilon)^3\\ &= 3\upsilon^2 - 3\upsilon + 1.\end{aligned}$$

■

4 Proof of Theorem 1.1

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

$$\Lambda_3(\ell) < \Lambda_3(f) + \epsilon. \tag{4.1}$$

This then implies $\rho(\upsilon, r) < \rho(\upsilon, p) + \epsilon$, and then our theorem follows (because then $\rho(r, \upsilon)$ is approximately decreasing as r runs through the primes.)

To prove (4.1), let $f\colon \mathbb{Z}_p \to [0,1]$ satisfy $\mathbb{E}(f) \geq \upsilon$. Then, applying Proposition 3.4, we deduce that there is a map $g\colon \mathbb{R} \to \mathbb{R}$ satisfying the conclusion of that proposition. Let $c_1, \ldots, c_m$, $|c_i| < p^{1-1/m}$ be as in the proposition.

Define

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

(The Fourier transforms $\widehat{g}(c_i)$ are computed with respect to $\mathbb{Z}_p$.) If we restrict to integer values of α, then h has the following properties:

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

From the third conclusion we get that

$$\Lambda_3(h) = r^{-3}\Sigma_{1\leq i\leq m}\widehat{h}(c_i)^2\widehat{h}(-2c_i) = \Lambda_3(g).$$

Then from the final conclusion in Proposition 3.4 we have that $\Lambda_3(h) < \Lambda_3(f) + 25\epsilon$.

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

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

https://doi.org/10.4153/CMB-2008-006-9 Published online by Cambridge University Press

We have that $|\ell_0(n) - h(n)| \leq 2\epsilon$, and therefore $\|\widehat{\ell_0} - \widehat{h}\|_\infty < 2\epsilon r$. It is clear that by reassigning some of the values of $\ell_0(n)$ we can produce a map $\ell \colon \mathbb{Z}_r \to [0,1]$ such that[4] $\mathbb{E}(\ell) = \mathbb{E}(h)$, and $\|\widehat{\ell} - \widehat{h}\|_\infty < 4\epsilon r$. From Lemma 3.2 we then deduce

$$|\Lambda_3(\ell) - \Lambda_3(h)| < 48\epsilon;$$

and so $\mathbb{E}(\ell) = \mathbb{E}(f)$ and $\Lambda_3(\ell) < \Lambda_3(f) + 73\epsilon$. Our theorem is now proved on rescaling the 73ϵ to ϵ. ∎

5 Proof of Theorem 1.3

A consequence of Lemma 3.6 is that for a given density υ, 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 multiples 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 Lemma 3.6

$$\Lambda_3(A) = 3\upsilon^2 - 3\upsilon + 1 - (1-\upsilon)^2 = 2\upsilon^2 - \upsilon = 2/9.$$

So, $\rho(2/3, N) = 2/9$.

The idea now is to show that

$$\lim_{\substack{p \to \infty \\ p \text{ prime}}} \rho(2/3, p) \neq 2/9.$$

Suppose $p \equiv 1 \pmod 3$ and that $A \subseteq Z_p$ minimizes $\Lambda_3(A)$ subject to $|A| = (2p+1)/3$. Let $S = \mathbb{Z}_p \backslash A$, 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 3.5 we have

$$\Lambda_3(S) = p^{-2} \sum_{n \in T} r(n) < 0.93 p^{-2} |S| (|S||T|)^{1/2} < 0.93/9$$

for all p sufficiently large. So, by Lemma 3.6 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. ∎

[4] If $\widehat{\ell_0}(0) > \widehat{h}(0)$, then we reassign some of values of $\ell_0(n)$ from 1 to 0, so that we then get $\widehat{h}(0) \leq \widehat{\ell_0}(0) < \widehat{h}(0) + 1$, and then we change one more value of $\ell_0(n)$ from 1 to some $0 < \delta \leq 1$ to produce $\ell \colon \mathbb{Z}_r \to [0,1]$ satisfying $\widehat{\ell}(0) = \widehat{h}(0)$; likewise, if $\widehat{\ell_0}(0) < \widehat{h}(0)$, we reassign some values $\widehat{\ell_0}(n)$ from 0 to 1.

Acknowledgements I would like to thank Ben Green for the question, as well as for suggesting the proof of Theorem 1.1, which was a modification of an earlier proof of the author.

References

[1] B. Green, *Roth's theorem in the primes*. Ann. of Math. **161**(2005), no. 3, 1609–1636.
[2] B. Green and I. Ruzsa, *Counting sumsets and sum-free sets modulo a prime*. Studia Sci. Math. Hungar. **41**(2004), no. 3, 285–293.
[3] P. Varnavides, *On certain sets of positive density.* J. London Math. Soc. **34**(1959), 358–360.

Department of Mathematics
Georgia Institute of Technology
Atlanta, GA 30332-0160
U.S.A.
e-mail: ecroot@math.gatech.edu