Long Arithmetic Progressions in Critical Sets

Ernie Croot *

September 5, 2005

Abstract

Given a density $0 < \sigma \leq 1$, we show for all sufficiently large primes p that if $S \subseteq \mathbb{Z}/p\mathbb{Z}$ has the least number of three-term arithmetic progressions among all sets with at least σp elements, then S contains an arithmetic progression of length at least $\log^{1/4+o(1)} p$.

1 Introduction

Given a prime p, we say that $S \subseteq \mathbb{Z}/p\mathbb{Z}$ is a critical set for the density σ if $|S| \geq \sigma p$ and S has the least number of three-term arithmetic progressions among all the subsets of $\mathbb{Z}/p\mathbb{Z}$ having at least σp elements. In this context, an arithmetic progression of length k is a sequence of residue classes $(n, n+m, n+2m, ..., n+(k-1)m)$ modulo p. Note that this includes "trivial" progressions, which are ones where $m \equiv 0 \pmod{p}$, as well as "non-trivial" progressions, which are ones where $m \not\equiv 0 \pmod{p}$. Also notice that the progression $(1, 2, 3)$, say, is distinct from $(3, 2, 1)$; that is, in our definition, it matters how the progression is ordered.

The main result of this paper is the following theorem, which basically says that critical sets of positive density must have long arithmetic progressions.

Theorem 1 *For every $0 < \sigma \leq 1$ and any sufficiently large prime p, if $S \subseteq \mathbb{Z}/p\mathbb{Z}$ is critical for the density σ, then S contains an arithmetic progression of length at least $\log^{1/4+o(1)} p$.* [1]

*Supported in part by an NSF grant.

[1] One might would think that this gives a new proof of Roth's theorem on three-term arithmetic progressions; however, in our proof, we use a theorem of Varnavides, which implicitly makes use of Roth's result.

Moreover, for every $0 < \sigma \leq 1$, $L > 0$, and p sufficiently large, there exists an arithmetic progression $P \subseteq \mathbb{Z}/p\mathbb{Z}$ of length at least $\log^L p$, such that

$$|S \cap P| \ > \ |P| \left(1 - \frac{1}{\log^{1/4+o(1)} p}\right).$$

It is easily seen that the second assertion of the theorem for the case $L = 1$ implies the first one. For, if $|S \cap P| > |P|(1 - \log^{-1/4+o(1)} p)$, then $|P \setminus S| < |P| \log^{-1/4+o(1)} p$, whence $S \cap P$ contains an arithmetic progression of length at least $(1 - \log^{-1/4+o(1)} p)/\log^{-1/4+o(1)} p = \log^{1/4+o(1)} p$. For this reason we will only be concerned below with the proof of the second assertion.

We now compare this theorem with the state-of-the-art on long progressions in arbitrary sets of integers. As a consequence of Gowers' deep and beautiful proof of Szemerédi's Theorem [3, Theorem 18.6], one can show that for $0 < \delta \leq 1$, and all x sufficiently large, any set $S \subseteq \{1, 2, ..., x\}$ having at least δx elements contains an arithmetic progression of length at least $\log\log\log\log\log(x) + c(\delta)$, for some constant $c(\delta)$. This is a considerably shorter arithmetic progression than the one given for critical sets in our theorem above.

There are also some results for sumsets, which give much longer arithmetic progressions. For example, Bourgain [1] proved the interesting result that if $A, B \subseteq \{1, ..., x\}$, where $|A| > \delta x$, $|B| > \gamma x$, then the sumset $A + B$ contains an arithmetic progression of length at least $\exp(c(\delta\gamma \log x)^{1/3} - \log\log x)$ (for some $c > 0$). Ruzsa [9] gave an ingenious construction, which shows that for every $0 < \epsilon < 1/3$, and all x sufficiently large, there exists a set A having at least $b(\epsilon)x$ elements (for some function $b(\epsilon) > 0$ that depends only on ϵ), such that $A + A$ has no arithmetic progressions longer than $\exp(\log^{2/3-\epsilon} x)$. Then, Green [4] improved Bourgain's result, and showed that $A + B$ contains an arithmetic progression of length at least $\exp(c'(\delta\gamma \log x)^{1/2} - \log\log x)$. We note that the length of the progressions in these sumsets is much larger than the ones we give for critical sets; and so, if we could somehow prove that critical sets are sumsets of two large sets A and B, then our result could possibly be improved.

There are also some impressive results on long arithmetic progressions in repeated sumsets $A + A + \cdots + A$ and subset sums, notably those of Freiman [2]; Sárkőzy [10], [11], and [12]; Lev [6], and [7]; Vu and Szemerédi [14] and [15]; and Solymosi [13].

It is worth pointing out that our argument has many common features

with that of Green [4]. In particular, we both make use of large deviation (or concentration of measure) results from probability theory; and we both use techniques involving Bohr neighborhoods. However, the combinatorial aspects of our results are different, which reflects the fact that sumsets and critical sets have different properties that must be exploited in different ways.

It might be possible to refine the proof of Theorem 1 to show that critical sets $S \subseteq \mathbb{Z}/p\mathbb{Z}$ of density σ have a long arithmetic progression for any $\sigma > (\log\log p)^{-1}$, say. It should also be possible to prove that if S is "nearly" critical, meaning that the number of three-term progressions in S is at most $1+\epsilon$ times the number in a critical set with the same density as S, then S should have a long arithmetic progression, where the smaller we take ϵ, the longer will be the length of the arithmetic progression.

2 Proof of Theorem 1

We note that $L > 1$ can be assumed without loss of generality.

We identify subsets of $\mathbb{Z}/p\mathbb{Z}$ with their indicator functions; say,

$$S(n) \ = \ \begin{cases} 1, & \text{if } n \in S; \\ 0, & \text{otherwise.} \end{cases}$$

Now, for a function $f : \mathbb{F}_p \to \mathbb{C}$ we define the discrete Fourier transform of f to be

$$\hat{f}(a) \ = \ \sum_{0 \le n \le p-1} f(n) e^{2\pi i a n/p}.$$

Then the number of three-term arithmetic progressions in the set S is

$$\sum_{r+s \equiv 2t \pmod p} S(r)S(s)S(t) \ = \ \frac{1}{p} \sum_{0 \le a \le p-1} \hat{S}(a)^2 \hat{S}(-2a).$$

We write this last sum as $\Sigma_1 + \Sigma_2$, where Σ_1 is the sum over all those a with

$$|\hat{S}(-2a)| \ > \ \frac{p \log\log p}{\sqrt{\log p}}, \tag{1}$$

and where Σ_2 is the sum over the remaining values of a. ¿From Parseval's identity we deduce the estimate

$$|\Sigma_2| \ \le \ \frac{p \log\log p}{\sqrt{\log p}} \sum_{0 \le a \le p-1} |\hat{S}(a)|^2 \ \le \ \frac{\sigma p^3 \log\log p}{\sqrt{\log p}}. \tag{2}$$

We now bound the number of terms in Σ_1 from above. Denote this number of terms by M. Then, by Parseval's identity we get that

$$\frac{p^2(\log\log p)^2}{\log p}M \ < \ \sum_{0\le a\le p-1}|\hat{S}(a)|^2 \ = \ \sigma p^2,$$

which implies

$$M \ < \ \frac{\sigma\log p}{(\log\log p)^2}. \tag{3}$$

We next require the following basic lemma.

Lemma 1 *Suppose that* $0 \le a_1, ..., a_k \le p-1$, $K > 0$ *and*

$$k \ \le \ \frac{\log p}{K\log\log p}.$$

Then, for p *sufficiently large there is an integer* $1 \le n \le p-1$ *such that*

$$\left|\left|\frac{a_i n}{p}\right|\right| \ \le \ \frac{1}{\log^K p}; \quad i = 1, 2, \ldots, k, \tag{4}$$

where $||x||$ *denote the distance from* x *to the nearest integer.*

Proof of the Lemma. Draw a k-dimensional cube with edge length $1/\log^K p$ around each point of the form

$$(\{a_1 y/p\}, ..., \{a_k y/p\}),$$

where y runs through the integers $0, 1, ..., p-1$, and where $\{t\} = t - \lfloor t\rfloor$ denotes the fractional part of t. If $p/\log^{kK} p \ge 1$ then two of these cubes (considered as torus subsets) will intersect, and the assertion follows. ■

Let $a_1, ..., a_M$ be the values of a satisfying (1), which are the indices of the terms in Σ_1. For $k = M$ and $K = 2L$, we have that since M satisfies (3), the hypotheses of Lemma 1 hold; and so, there is an integer n_0 satisfying (4) for $n = n_0$. Now, let P_0 be the arithmetic progression

$$P_0 \ = \ \{in_0 \pmod p \ : \ 0 \le i < \log^L p\}. \tag{5}$$

The proof of the main theorem of the paper will amount to showing that S is saturated on some translate of $-P_0$; that is, $S \cap (j - P_0)$ contains "almost" $|P_0|$ elements for some $j \in \mathbb{Z}/p\mathbb{Z}$. We prove this by showing that

if $|S \cap (j - P_0)|$ is not close to $|P_0|$ for any j, then we can produce a new set S', where $|S'|$ is slightly larger than $|S|$, such that this set S' has an anomalously small number of three-term arithmetic progressions, relative to other sets with $|S'|$ elements. We will then intersect S' with another set having few three-term arithmetic progressions, to produce a new set S'', such that $|S''| = |S|$, and S'' has fewer three-term arithmetic progressions than S. This contradicts the fact that S' is critical, and so we must have had that S is saturated on some translate of $-P_0$.

For $m \in \mathbb{Z}/p\mathbb{Z}$ we denote by $(S * P_0)(m)$ the number of representations of m as a sum of an element of S and an element of P_0. Our notation is explained by the fact that $S * P_0$ is the convolution of the indicator functions S and P_0:

$$(S * P_0)(m) \ = \sum_{a+b \equiv m \pmod p} S(a)P_0(b).$$

Observe that

$$0 \ \leq \ (S * P_0)(m) \ \leq \ \min\{|S|, |P_0|\}.$$

We now show that if S is a critical set, then

$$(S * P_0)(m) \ > \ |P_0| \left(1 - \frac{\log\log p}{\log^{1/4} p}\right), \tag{6}$$

for some m; Theorem 1 will then follow as $|(S * P_0)(m)| = |S \cap (m - P_0)|$.

Assuming, for proof by contradiction, that (6) fails to hold for every $0 \leq m \leq p-1$, let

$$\kappa \ = \ 1 - \frac{\log\log p}{\log^{1/4} p}.$$

Then, define the weighting function $w(m)$ for $0 \leq m \leq p-1$ to be

$$w(m) \ = \ \frac{(S * P_0)(m)}{\kappa |P_0|},$$

so that

$$\hat{w}(0) \ = \ \frac{\widehat{(S * P_0)}(0)}{\kappa |P_0|} \ = \ \frac{\hat{S}(0)\hat{P}_0(0)}{\kappa |P_0|} \ = \ \kappa^{-1}|S| \tag{7}$$

and

$$\hat{w}(a) \ = \ \frac{\widehat{(S * P_0)}(a)}{\kappa |P_0|} \ = \ \frac{\hat{S}(a)\hat{P}_0(a)}{\kappa |P_0|}. \tag{8}$$

From the assumption that (6) fails for holds for every m, we deduce

$$0 \ \leq \ w(m) \ \leq \ 1.$$

Lemma 2 *For any function $w : \mathbb{Z}/p\mathbb{Z} \to [0,1]$ there exists another function $u : \mathbb{Z}/p\mathbb{Z} \to \{0,1\}$ such that $\hat{u}(a) = \hat{w}(a) + O(\sqrt{p}\log p)$ for all $a \in \mathbb{Z}/p\mathbb{Z}$, and in addition, $\hat{u}(0) = \hat{w}(0) + \delta$ with $0 \leq \delta < 1$.*

Before we can prove this lemma we require the following concentration of measure result due to Hoeffding [5] (also see [8], Theorem 5.7).

Proposition 1 *Suppose that $z_1, ..., z_r$ are independent real random variables with $|z_i| \leq 1$. Let $\mu = E(z_1 + \cdots + z_r)$, and let $\Sigma = z_1 + \cdots + z_r$. Then,*

$$\text{Prob}\left(|\Sigma - \mu| \ > \ rt\right) \ \leq \ 2\exp(-rt^2/2),$$

for any $t > 0$.

From this proposition we deduce the following corollary, which is the version of this result that we actually use.

Corollary 1 *Suppose that $v_1, ..., v_r$ are independent complex random variables with $|v_i| \leq 1$. Let $\nu \ = \ E(v_1 + \cdots + v_r)$, and let $\Sigma = v_1 + \cdots + v_r$. Then,*

$$\text{Prob}\left(|\Sigma - \nu| \ > \ rt\right) \ \leq \ 4\exp(-rt^2/4),$$

for any $t > 0$.

Proof of the Corollary. Let

$$\nu_x \ = \ \text{Re}(\nu), \text{ and } \nu_y \ = \ \text{Im}(\nu).$$

Then, for $j = 1, 2, ..., r$ define the random variables

$$x_j \ = \ \text{Re}(v_j), \text{ and } y_j \ = \ \text{Im}(v_j).$$

We note that these random variables x_j, y_j are bounded from above by 1 in absolute value, because $|v_j| \leq 1$. Therefore, $|\nu_x| \leq r$ and $|\nu_y| \leq r$. Finally, let

$$\Sigma_x \ = \ x_1 + \cdots + x_r, \text{ and } \Sigma_y \ = \ y_1 + \cdots + y_r.$$

Observe that if the event $|\Sigma - \nu| > rt$ occurs, then either we have that

$$|\Sigma_x - \nu_x| \ > \ \frac{rt}{\sqrt{2}},$$

or that

$$|\Sigma_y - \nu_y| \ > \ \frac{rt}{\sqrt{2}}.$$

To bound the probability of the first of these events, we apply Hoeffding's theorem with $z_j = x_j$, and deduce that

$$\text{Prob}(|\Sigma_x - \nu_x| > rt/\sqrt{2}) \ \leq \ 2\exp(-rt^2/4);$$

likewise,

$$\text{Prob}(|\Sigma_y - \nu_y| > rt/\sqrt{2}) \ \leq \ 2\exp(-rt^2/4).$$

Thus,

$$\text{Prob}(|\Sigma - \nu| > rt) \ \leq \ 4\exp(-rt^2/4),$$

as claimed. ■

Proof of Lemma 2. Let $x_0, ..., x_{p-1}$ be independent Bernoulli random variables with

$$\text{Prob}(x_m = 1) \ = \ w(m).$$

Then, for each integer a satisfying $0 \leq a \leq p-1$, we define

$$X(a) \ = \ \sum_{j=0}^{p-1} x_j e^{2\pi i j a/p},$$

which is the sum of independent random variables $v_j = x_j e^{2\pi i j a/p}$.

Now,

$$E(X(a)) \ = \ E(v_0) + \cdots + E(v_{p-1}) \ = \ \sum_{j=0}^{p-1} E(x_j) e^{2\pi i j a/p} \ = \ \hat{w}(a)$$

and applying Corollary 1, we deduce that

$$\text{Prob}(|X(a) - \hat{w}(a)| > \sqrt{p}\log p) \ \leq \ 4\exp(-(\log^2 p)/4).$$

Thus, the probability that

$$\text{For all } a = 0, 1, ..., p-1, \ \ |X(a) - \hat{w}(a)| \ \leq \ \sqrt{p}\log p \tag{9}$$

is at least

$$1 - 4p \ \exp\left(-(\log^2 p)/4\right),$$

which is positive for p sufficiently large.

Since (9) holds with positive probability, there exists a function $u : \mathbb{Z}/p\mathbb{Z} \to \{0, 1\}$, such that

$$\text{For all } a = 0, 1, ..., p-1, \ \ |\hat{u}(a) - \hat{w}(a)| \ < \ \sqrt{p}\log p.$$

We know that since $w(n) \in [0,1]$, $\hat{w}(0) \in [0,p]$; likewise, $\hat{u}(0) \in [0,p]$. Thus, we either have $\hat{u}(0) \geq \hat{w}(0) \geq 0$ or $\hat{u}(0) < \hat{w}(0) \leq p$. If $\hat{u}(0) \geq \hat{w}(0) \geq 0$, then we can reassign at most $\sqrt{p}\log p$ of the values of $u(m)$ from 1 to 0 until we get

$$\hat{u}(0) \ = \ \hat{w}(0) + \delta, \ 0 \leq \delta < 1, \tag{10}$$

and

$$\hat{u}(a) \ = \ \hat{w}(a) + O(\sqrt{p}\log p) \tag{11}$$

for all the other values $a = 1, 2, ..., p-1$. If $\hat{u}(0) < \hat{w}(0) \leq p$, then we can likewise reassign at most $\sqrt{p}\log p$ of the values of $u(m)$ from 0 to 1 until we get (10) and (11) to hold.

Thus, we have constructed a function $u(m)$ which satisfies the conclusion of our lemma. ■

Now let S' denote the set for which $u(m)$ is the indicator function. Then, from the conclusion of Lemma 2 and (7) we have that for some $0 \leq \delta < 1$,

$$|S'| \ = \ \hat{u}(0) \ = \ \hat{w}(0) + \delta \ = \ \kappa^{-1}|S| + \delta, \quad \text{where} \ \ 0 \leq \delta < 1. \tag{12}$$

We now estimate the number of three-term arithmetic progressions contained in S' modulo p; this number is

$$\begin{aligned} \frac{1}{p}\sum_{a=0}^{p-1} \hat{u}(a)^2\hat{u}(-2a) \ &= \ \frac{1}{p}\sum_{a=0}^{p-1}\Big(\hat{w}(a) + O(\sqrt{p}\log p))^2(\hat{w}(-2a) + O(\sqrt{p}\log p)\Big) \\ &= \ \frac{1}{p}\sum_{a=0}^{p-1} \hat{w}(a)^2\hat{w}(-2a) \ + \ E, \end{aligned} \tag{13}$$

where

$$\begin{aligned} E \ll \frac{\log p}{\sqrt{p}}\sum_{a=0}^{p-1}\Big(p\log^2 p + |\hat{w}(a)|\sqrt{p}\log p + |\hat{w}(a)|^2 \\ + |\hat{w}(a)\hat{w}(-2a)| + |\hat{w}(-2a)|\sqrt{p}\log p\Big). \end{aligned}$$

From Parseval's identity we know that

$$\sum_{a=0}^{p-1} |\hat{w}(a)|^2 \ = \ p\sum_{n=0}^{p-1} w(n)^2 \ \leq \ p^2.$$

From this and the Cauchy-Schwarz inequality we then deduce that

$$E \ = \ O\left(p\sqrt{p}\log^3 p\right);$$

and so it follows from this and (8) that the number of three-term arithmetic progressions in S' modulo p is

$$\begin{aligned}&\frac{1}{p}\sum_{a=0}^{p-1}\hat{w}(a)^2\hat{w}(-2a) \;+\; O\left(p\sqrt{p}\log^3 p\right)\\ &\qquad = \;\frac{1}{\kappa^3 p}\sum_{a=0}^{p-1}\hat{S}(a)^2\hat{S}(-2a)\frac{\hat{P}_0^2(a)\hat{P}_0(-2a)}{|P_0|^3} \;+\; O(p\sqrt{p}\log^3 p).\end{aligned} \tag{14}$$

We now write this last sum as $\Sigma_1' + \Sigma_2'$, where Σ_1' is the sum over $0 \le a \le p-1$ satisfying (1), and Σ_2' is the sum over the remaining values of a. Now, for each a satisfying (1) and for each $n \in P_0$ we have from (5) and (4) with $K = 2L$ that

$$\left|\left|\frac{-2an}{p}\right|\right| \;\le\; 2\left|\left|\frac{an}{p}\right|\right| \;<\; \frac{2}{\log^L p}.$$

for p sufficiently large. Thus,

$$\begin{aligned}\frac{\hat{P}_0(-2a)}{|P_0|} &= \frac{1}{|P_0|}\sum_{n\in P_0} e^{2\pi i(-2an)/p}\\ &= \frac{1}{|P_0|}\sum_{n\in P_0}\left(1+O\left(\frac{1}{\log^L p}\right)\right)\\ &= 1+O\left(\frac{1}{\log^L p}\right)\end{aligned}$$

and the same estimate holds for $\hat{P}_0(a)/|P_0|$. Thus, we conclude that

$$\begin{aligned}\Sigma_1' &= \Sigma_1 \;+\; O\left(\frac{1}{\log^L p}\right)\sum_{a=0}^{p-1}|\hat{S}(a)|^2|\hat{S}(-2a)|\\ &= \Sigma_1 \;+\; O\left(\frac{p}{\log^L p}\sum_{a=0}^{p-1}|\hat{S}(a)|^2\right)\\ &= \Sigma_1 \;+\; O\left(\frac{p^3}{\log^L p}\right).\end{aligned}$$

The last line here follows from Parseval's identity.

We also have the estimate

$$|\Sigma_2'| \;\le\; \frac{p\log\log p}{\sqrt{\log p}}\sum_{0\le a\le p-1}|\hat{S}(a)|^2 \;\le\; \frac{p^3\log\log p}{\sqrt{\log p}},$$

the second inequality following from Parseval's identity.

Combining our estimates for Σ_1' and Σ_2' together with (14) and (2), we deduce that the number of three-term arithmetic progressions in S' modulo p is

$$\frac{1}{\kappa^3 p}\left(\Sigma_1' + \Sigma_2'\right) + O(p\sqrt{p}\log^3 p) \;=\; \frac{1}{\kappa^3 p}\left(\Sigma_1 + \Sigma_2\right) + O\left(\frac{p^2 \log\log p}{\sqrt{\log p}}\right).$$

Thus, if we let $\mathcal{P}(A)$ denote the number of three-term arithmetic progressions modulo p in a set A, then we have that

$$\mathcal{P}(S') \;=\; \frac{1}{\kappa^3}\mathcal{P}(S) + O\left(\frac{p^2 \log\log p}{\sqrt{\log p}}\right). \tag{15}$$

We now proceed to show that this is impossible, and from our chain of reasoning above, this would mean that (6) holds for some m, which would prove our theorem.

To show that (15) cannot hold, we require the following combinatorial lemma, which is proved using the probabilistic method, in combination with the second moment method.

Lemma 3 *Suppose $A, B \subset \mathbb{Z}/p\mathbb{Z}$ have densities γ and δ, respectively; and, suppose that A and B contain $\alpha\gamma^3 p^2$ and $\beta\delta^3 p^2$ non-trivial three-term arithmetic progressions [2], respectively. Then, there exists a subset C of $\mathbb{Z}/p\mathbb{Z}$ having density at least*

$$\gamma\delta + O(p^{-1/4}),$$

such that the number of non-trivial three-term arithmetic progressions lying in C modulo p is at most

$$\alpha\beta(\gamma\delta)^3 p^2 \;+\; O(p^{3/2}).$$

Here the implicit constants depend on α, β, γ and δ only.

Remark. The same result holds if we add in trivial three-term arithmetic progressions, since a subset D of $\mathbb{Z}/p\mathbb{Z}$ can have only $O(p)$ trivial three-term arithmetic progressions, which is well within the remainder term $O(p^{3/2})$.

Proof of Lemma 3. We will find a pair of integers u, v such that $A \cap (uB + v)$ has the desired properties. First, we show that this intersection

[2] The condition on the number of three-term arithmetic progressions in A and B is saying the following. A "typical" subset A (or B) of the integers modulo p having density γ (or δ) should have $\gamma^3 p^2$ (or $\delta^3 p^2$) three-term arithmetic progressions. Thus, the factors α and β gauge how far away from this expected number the sets A and B stray.

has density very close to $\gamma\delta$ for almost all $0 \leq u, v \leq p-1$, by using a second moment argument. Let u and v be independent random variables, with u taking values from $\{1, 2, ..., p-1\}$, each value attained with probability $1/(p-1)$, and with v taking values from $\{0, 1, ..., p-1\}$, where each value is attained with probability $1/p$. Then, the variance $V(|A \cap (uB+v)|)$ is

$$E(|A \cap (uB+v)|^2) \ - \ E(|A \cap (uB+v)|)^2.$$

To compute the first expectation we express the intersection as a sum of indicator functions:

$$|A \cap (uB+v)| \ = \ \sum_{b \in B} A(ub+v).$$

So, we have that

$$\begin{aligned} E(|A \cap (uB+v)|^2) \quad &= \quad \sum_{(b,b') \in B \times B} E(A(ub+v)A(ub'+v)) \\ &= \quad \frac{1}{p(p-1)} \sum_{(b,b') \in B \times B} \sum_{\substack{1 \leq u' \leq p-1 \\ 0 \leq v' \leq p-1}} A(u'b+v')A(u'b'+v'). \end{aligned}$$

Now, given an ordered pair (b, b') of unequal elements of B, and given an ordered pair $(a, a') \in A \times A$ of unequal elements of A, there is exactly one pair of numbers $u', v' \pmod p$, $1 \leq u' \leq p-1$, $0 \leq v' \leq p-1$, satisfying $u'b+v' \equiv a \pmod p$ and $u'b'+v' \equiv a' \pmod p$. If we allow $a = a'$ here, then for this case we would have to have $u' = 0$ in order that $u'b+v' = a = a' = u'b'+v'$. We conclude that if $b' \neq b$, then there are exactly $|A|(|A|-1)$ pairs u', v', $1 \leq u' \leq p-1$, $0 \leq v' \leq p-1$, which make $A(u'b+v')A(u'b'+v') \neq 0$ (and therefore equal to 1). Thus,

$$E(|A \cap (uB+v)|^2) \ \leq \ \frac{\gamma p(\gamma p-1)\delta p(\delta p-1)}{p(p-1)} \ + \ |B| \ = \ \gamma^2\delta^2 p^2 + O(p).$$

(The term $|B|$ comes from those pairs b, b' with $b = b'$.)

To estimate $E(|A \cap (uB+v)|)$, we note that for any fixed $b \in B$ and $1 \leq u \leq p-1$, the probability that $ub+v$ lies in A is γ. Thus, the expected size of this intersection is $\gamma\delta p$.

We now conclude that

$$V(|A \cap (uB+v)|) \ = \ O(p);$$

and so, by an application of Chebychev's inequality we conclude that

$$\text{Prob}(|A \cap (uB+v)| < (1-\epsilon)\gamma\delta p) \;=\; O\left(\frac{1}{\epsilon^2\gamma^2\delta^2 p}\right).$$

Next, we compute the expected number of three-term arithmetic progressions in the intersection $A \cap (uB+v)$: Let $Q = Q(u,v)$ be the number of non-trivial three-term arithmetic progressions lying in $A \cap (uB+v)$. Now, suppose that x_1, x_2, x_3 is a non-trivial three-term arithmetic progression in A, so that $x_2 \equiv x_1 + d, x_3 \equiv x_1 + 2d \pmod p$, for some $d \not\equiv 0 \pmod p$; and, suppose that y_1, y_2, y_3 is a non-trivial three-term arithmetic progression in B. Then, there is exactly one pair (u', v'), $u' \in \{1, ..., p-1\}$, $v' \in \{0, ..., p-1\}$ such that

$$\text{For } i = 1, 2, 3, \quad u'x_i + v' \equiv y_i \pmod p.$$

Thus, the probability that a particular non-trivial three-term arithmetic progression in A also lies in $uB + v$ is

$$\frac{\beta\delta^3 p^2}{p(p-1)} \;=\; \beta\delta^3 + O(1/p);$$

and so, the expected size of Q is $\alpha\beta(\gamma\delta)^3 p^2 + O(p)$. So, there can be at most $p^2 - p^{3/2}$ of the choices for u' and v' such that the intersection $A \cap (u'B + v')$ has more than $\alpha\beta(\gamma\delta)^3(p^2 + 2p^{3/2})$ three-term arithmetic progressions; for otherwise, the expectation of Q would exceed

$$\frac{(p^2 - p^{3/2})(p^2 + 2p^{3/2})}{p(p-1)}\alpha\beta(\gamma\delta)^3 \;=\; \alpha\beta(\gamma\delta)^3(p^2 + p^{3/2} + O(p)),$$

which we know is not the case. Thus, the probability that $Q < \alpha\beta(\gamma\delta)^3(p^2 + 2p^{3/2})$ is at least $1 - (p^2 - p^{3/2})/(p(p-1)) = p^{-1/2} + O(1/p)$. So, for $\epsilon = cp^{-1/4}$, for a certain constant $c > 0$ depending on γ and δ, we get that with a positive probability, both

$$|A \cap (uB+v)| \;\geq\; (1-\epsilon)\gamma\delta p \;\text{ and }\; Q \;<\; \alpha\beta(\gamma\delta)^3(p^2 + 2p^{3/2})$$

hold. So, there is a choice for u and v so that both these events occur, which proves the lemma. ■

We require one more lemma and a corollary of a result of Varnavides [16] before we can prove that (15) is impossible.

Lemma 4 *Given $0 < \theta < 1/2$, for any sufficiently large prime p there exists a subset $U \subset \mathbb{Z}/p\mathbb{Z}$ having density $1 - \theta + O(1/p)$ such that the number of*

three-term arithmetic progressions in U, both trivial and non-trivial, is at most

$$p^2(1-3\theta+2.5\theta^2)+O(p) \ < \ p^2(1-\theta)^3(1-\theta^2/2).$$

Proof. In fact, we just let U be the integers in the interval $[0,(1-\theta)p]$. [3] Then, U will have density $1-\theta+O(1/p)$. Now, let $U' = (\mathbb{Z}/p\mathbb{Z}) \setminus U$, and observe that for $a \not\equiv 0 \pmod p$, $\hat{U}(a) = -\hat{U}'(a)$, and $\hat{U}(0) = p - \hat{U}'(0)$. Thus, the number of triples (u,v,w) that lie in either U^3 or in $(U')^3$, satisfying $u+v \equiv 2w \pmod p$, is

$$\begin{aligned}\frac{1}{p}\sum_{a=0}^{p-1}\Big(\hat{U}(a)^2\hat{U}(-2a)+\hat{U}'(a)^2\hat{U}'(-2a)\Big) &= \frac{\hat{U}(0)^3+\hat{U}'(0)^3}{p} \\ &= (1-3\theta+3\theta^2)p^2+O(p).\end{aligned}$$

Now, for $0<\theta<1/2$, the number of triples $(u,v,w) \in (U')^3$ satisfying $u+v \equiv 2w \pmod p$ is just the number of pairs $(u,v) \in (U')^2$ of the same parity. There are $\theta^2p^2/2+O(p)$ such pairs; and so, the number of triples $(u,v,w) \in U^3$ satisfying $u+v \equiv 2w \pmod p$ is $(1-3\theta+2.5\theta^2)p^2+O(p)$. Up to an error of $O(p)$ this will also equal the number of non-trivial three-term arithmetic progressions in U. ■

The result of Varnavides is as follows.

Theorem 2 *Given $0<\alpha\le 1$, there exists $0<c\le 1$ such that for any integer $x \ge 1$ and any set $T \subseteq \{1,2,...,x\}$ having $|T| \ge \alpha x$,*

$$\#\{(u,v,w) \in T^3 \ : \ u+v=2w\} \ > \ cx^2.$$

Corollary 2 *There exists $0<c\le 1$, depending only on σ (the lower bound for the density of S), such that $\mathcal{P}(S) > cp^2$.*

The proof of this corollary is immediate, since if we think of S as a set of integers, say $S \subseteq \{0,1,...,p-1\}$ (instead of as a set of residue classes modulo p), then every solution to $a+b=2c$, $a,b,c \in S$ in the integers gives a solution $a+b \equiv 2c \pmod p$. So, the number of three-term arithmetic progressions in S modulo p is at least the number of three-term arithmetic progressions in S, when we think of it as a subset of the integers.

[3] This is a little counterintuitive, since we know that short intervals $[0,\epsilon p]$ contain more arithmetic progressions that a "typical" subset of $\mathbb{Z}/p\mathbb{Z}$ of density ϵ; but, when ϵ is near to 1, this is not the case!

Now we let $\theta = 1 - \kappa$, and let U be the set given by Lemma 4. Then, we apply Lemma 3 with $A = U$, and $B = S'$, and we deduce from (12) and our assumption (15) that there is a set C with

$$\begin{aligned} |C| &\geq |U||S'|p^{-1} + O(p^{3/4}) \\ &= (\kappa p + O(1))(\kappa^{-1}|S| + O(1))p^{-1} + O(p^{3/4}) \\ &= |S| + O(p^{3/4}), \end{aligned}$$

such that the number of three-term arithmetic progressions in C is at most

$$\begin{aligned} &\kappa^3 \left(1 - \frac{(1-\kappa)^2}{2}\right)\left(\frac{\mathcal{P}(S)}{\kappa^3} + O\left(\frac{p^2 \log\log p}{\sqrt{\log p}}\right)\right) + O(p^{3/2}) \\ &\quad = \mathcal{P}(S)\left(1 - \frac{(\log\log p)^2}{2\sqrt{\log p}}\right)\left(1 + O\left(\frac{\log\log p}{\sqrt{\log p}}\right)\right) \\ &\quad = \mathcal{P}(S)\left(1 - \frac{(\log\log p)^2}{2\sqrt{\log p}} + O\left(\frac{\log\log p}{\sqrt{\log p}}\right)\right). \end{aligned}$$

Note that Corollary 2 is what allowed us to absorb the error terms.

To show that this is impossible for sufficiently large p, we let C' be any set obtained from C by adding at most $O(p^{3/4})$ elements so that

$$|C'| \geq |S|.$$

Then, in the worst case, each element we add to C (to produce C') adds at most $O(p)$ new three-term arithmetic progressions. Thus,

$$\begin{aligned} \mathcal{P}(C') &= \mathcal{P}(C) + O(p^{1.75}) \\ &< \mathcal{P}(S)\left(1 - \frac{(\log\log p)^2}{2\sqrt{\log p}} + O\left(\frac{\log\log p}{\sqrt{\log p}}\right)\right). \end{aligned} \tag{16}$$

Finally, (16) contradicts the fact that S is a critical set: we have constructed a set C' having at least as many elements as S, but having fewer three-term arithmetic progressions than S. ■

3 Acknowledgements

I would like to thank the referees for their extensive comments, which have greatly improved the presentation of the results.

References

[1] J. Bourgain, *On Arithmetic Progressions in Sums of Sets of Integers*, A Tribute to Paul Erdős, 105-109, Cambridge University Press, Cambridge, 1990.

[2] G. A. Freiman, H. Halberstam, and I. Ruzsa, *Integer Sums sets Containing Long Arithmetic Progressions*, J. London Math. Soc. (2) **46** (1992), 193-201.

[3] W. T. Gowers, *A New Proof of Szemerédi's Theorem*, Geom. Funct. Anal. **11** (2001), no. 3, 465-588.

[4] B. Green, *Arithmetic Progressions in Sumsets*, Geom. Funct. Anal. **12** (2002), 584-597.

[5] W. Hoeffding, *Probability Inequalities for Sums of Independent Random Variables*, J. Amer. Statist. Assoc. **58** (1963), 13-30.

[6] V. F. Lev, *Optimal Representations by Sumsets and Subset Sums*, J. Number Theory **62** (1997), 127-143.

[7] ———-, *Blocks and Progressions in Subset Sums Sets*, Acta Arith. **106** (2003), 123-142.

[8] C. McDiarmid, *On the Method of Bounded Differences*, London Math. Soc. Lecture Note Ser. 14, Cambridge Univ. press, Cambridge, 1989.

[9] I. Ruzsa, *Arithmetic Progressions in Sumsets*, Acta Arith. **60** (1991), no. 2, 191-202.

[10] A. Sárkőzy, *Finite Addition Theorems. I*, J. Number Theory **32** (1989), 114-130.

[11] ————, *Finite Addition Theorems. II*, J. Number Theory **48** (1994), 197-218.

[12] ————, *Finite Addition Theorems. III*, Groupe de Travail en Théorie Analytique et Élémentaire des Nombres, 1989-1990, 105-122, Publ. Math. Orsay, 92-01, Univ. Paris XI, Orsay, 1992.

[13] J. Solymosi, *Arithmetic Progressions in Sets with Small Sumsets*, Manuscript.

[14] E. Szemerédi and V. Vu, *Long Arithmetic Progressions in Sum-Sets and the Number of x-sum-free Sets*, submitted.

[15] ———————————, *Finite and Infinite Arithmetic Progressions in Sumsets*, submitted.

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