Towards $3n - 4$ in groups of prime order

Vsevolod F. Lev

Department of Mathematics
The University of Haifa at Oranim
Tivon 36006, Israel

seva@math.haifa.ac.il

Oriol Serra

Department of Mathematics and Institute of Mathematics Barcelona-Tech*
Universitat Politècnica de Catalunya
oriol.serra@upc.edu

Submitted: Apr 2, 2023; Accepted: May 3, 2023; Published: Jun 16, 2023

Abstract

We show that if $\mathcal{A}$ is a subset of a group of prime order p such that $|2\mathcal{A}| < 2.7652|\mathcal{A}|$ and $10 \leqslant |\mathcal{A}| < 1.25 \cdot 10^{-6}p$, then $\mathcal{A}$ is contained in an arithmetic progression with at most $|2\mathcal{A}| - |\mathcal{A}| + 1$ terms, and $2\mathcal{A}$ contains an arithmetic progression with the same difference and at least $2|\mathcal{A}| - 1$ terms. This improves a number of previously known results.

Mathematics Subject Classifications: 11P70, 11B25

1 Introduction

A classical result in additive combinatorics, Freiman's $(3n - 4)$-theorem, says that if A is a finite set of integers satisfying $|2A| \leqslant 3|A| - 4$, then A is contained in an arithmetic progression of length $|2A| - |A| + 1$.

It is believed that an analogue of Freiman's theorem holds for the "not-too-large" subsets of the prime-order groups; that is, if $\mathcal{A}$ is a subset of a group of prime order such that $|2\mathcal{A}| \leqslant 3|\mathcal{A}| - 4$ then, subject to some mild density restrictions, $\mathcal{A}$ is contained in an arithmetic progression with at most $|2\mathcal{A}| - |\mathcal{A}| + 1$ terms. The precise form of this (and indeed, somewhat more general) conjecture can be found in [7, Conjecture 19.2].

*Supported by the Spanish Agencia Estatal de Investigación under projects PID2020-113082GBI00 and the Severo Ochoa and Mara de Maeztu Program for Centers and Units of Excellence in R&D (CEX2020-001084-M)

For an integer $m \geqslant 1$, we denote by $\mathbb{C}_m$ the cyclic group of order m. Let p be a prime. Over sixty years ago, Freiman himself showed [4] that a subset $\mathcal{A} \subseteq \mathbb{C}_p$ is contained in a progression with at most $|2\mathcal{A}| - |\mathcal{A}| + 1$ terms provided that $|2\mathcal{A}| < 2.4|\mathcal{A}| - 3$ and $|\mathcal{A}| < p/35$. Much work has been done to improve Freiman's result in various directions; we list just a few results of this kind.

Rødseth [10] showed that the assumption $|\mathcal{A}| < p/35$ can be relaxed to $|\mathcal{A}| < p/10.7$. Green and Ruzsa [6] pushed the doubling constant from 2.4 up to 3, at the cost of a stronger density assumption $|\mathcal{A}| < p/10^{215}$. In [11], Serra and Zémor obtained a result without any density assumption other than the conjectural one, but at the cost of reducing essentially the doubling coefficient; namely, assuming that $|2\mathcal{A}| \leqslant (2+\varepsilon)|\mathcal{A}|$ with $\varepsilon < 0.0001$. An improvement, allowing in particular $\varepsilon < 0.1368$, was obtained by Candela, González-Sánchez, and Grynkiewicz [1]. Candela, Serra, and Spiegel [2] improved the doubling coefficient to 2.48 under the assumption $|\mathcal{A}| < p/10^{10}$, and this was further improved by Lev and Shkredov [9] to 2.59 and $|\mathcal{A}| < 0.0045p$, respectively.

We have mentioned only several most relevant results; variations and extensions, such as the results on the asymmetric sumset $\mathcal{A} + \mathcal{B}$ and restricted sumset $\mathcal{A}\dot{+}\mathcal{A}$, are intentionally left out. A systematic coverage of the topic can be found in [7, Chapter 19].

In this paper, we prove the following result.

Theorem 1. *Let p be a prime, and suppose that a set $\mathcal{A} \subseteq \mathbb{C}_p$ satisfies $|2\mathcal{A}| < 2.7652|\mathcal{A}| - 3$. If $10 \leqslant |\mathcal{A}| < 1.25 \cdot 10^{-6}p$, then $\mathcal{A}$ is contained in an arithmetic progression with at most $|2\mathcal{A}| - |\mathcal{A}| + 1$ terms, and $2\mathcal{A}$ contains an arithmetic progression with the same difference and at least $2|\mathcal{A}| - 1$ terms.*

Our argument follows closely that in [2]. The improvements come primarily from applying a result of Lev [8] that establishes the structure of small-doubling sets in cyclic groups (instead of an earlier result of Deshouillers and Freiman [3]), and also from using an estimate from a recent paper of Lev and Shkredov [9].

In the next section we collect the results needed for the proof of Theorem 1. The proof itself is presented in the concluding Section 3.

2 Preparations

This paper is intended for the reader familiar with the basic notions and results from the area of additive combinatorics, such as the sumsets, additive energy, Freiman's isomorphism, Cauchy–Davenport and Vosper's theorems, the Plünnecke–Ruzsa inequality etc; they will be used without any further explanations. Our notation and terminology are also quite standard. It may be worth recalling, nevertheless, that a subset of an abelian group is called *rectifiable* if it is Freiman-isomorphic to a set of integers, and that the *additive dimension* of a subset $A \subseteq \mathbb{Z}$, denoted $\dim(A)$, is the largest integer d such that A is Freiman-isomorphic to a subset of $\mathbb{Z}^d$ not contained in a hyperplane. By φ_m we denote the canonical homomorphism from $\mathbb{Z}$ onto the quotient group $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{C}_m$. The *size* of an arithmetic progression is the number of its (distinct) elements.

The core new component used in the proof of Theorem 1 is the following result.

Theorem 2 (Lev [8, Theorem 1.1]). *Let m be a positive integer. If a set $\mathcal{A} \subseteq \mathbb{C}_m$ satisfies $|2\mathcal{A}| < \frac{9}{4}|\mathcal{A}|$, then one of the following holds:*

(i) There is a subgroup $\mathcal{H} \leqslant \mathbb{C}_m$ such that $\mathcal{A}$ is contained in an $\mathcal{H}$-coset and $|\mathcal{A}| > C^{-1}|\mathcal{H}|$, where $C = 2 \cdot 10^5$.

(ii) There is a proper subgroup $\mathcal{H} < \mathbb{C}_m$ and an arithmetic progression $\mathcal{P}$ of size $|\mathcal{P}| > 1$ such that $|\mathcal{P} + \mathcal{H}| = |\mathcal{P}||\mathcal{H}|$, $\mathcal{A} \subseteq \mathcal{P} + \mathcal{H}$, and

$$(|\mathcal{P}| - 1)|\mathcal{H}| \leqslant |2\mathcal{A}| - |\mathcal{A}|.$$

(iii) There is a proper subgroup $\mathcal{H} < \mathbb{C}_m$ such that $\mathcal{A}$ meets exactly three $\mathcal{H}$-cosets, the cosets are not in an arithmetic progression, and

$$3|\mathcal{H}| \leqslant |2\mathcal{A}| - |\mathcal{A}|.$$

The following lemma originating from [2] relates the additive dimension of a set with the rectifiability of its image under a quotient map.

Lemma 3 (Candela–Serra–Spiegel [2, Lemma 2.2]). *Let l be a positive integer, and suppose that A is a set of integers satisfying $\{0, l\} \subseteq A \subseteq [0, l]$ and $\gcd(A) = 1$. If there is a proper subgroup $H < \mathbb{C}_l$ such that the image of A under the composite homomorphism $\mathbb{Z} \to \mathbb{C}_l \to \mathbb{C}_l/H$ is rectifiable, then $\dim(A) \geqslant 2$.*

Since the proof is just several lines long, we reproduce it here for the convenience of the reader.

Proof. Writing $m := l/|H|$, we identify the quotient group $\mathbb{C}_l/H$ with the group $\mathbb{C}_m$, and the map $\mathbb{Z} \to \mathbb{C}_l \to \mathbb{C}_l/H$ with φ_m. Let $f\colon \varphi_m(A) \to \mathbb{Z}$ be Freiman's isomorphism of $\varphi_m(A)$ into the integers. The set $\{(a, f(\varphi_m(a)))\colon a \in A\} \subseteq \mathbb{Z}^2$ is easily seen to be isomorphic to A, and to complete the proof we show that this set is not contained in a line. Assuming the opposite, from $f(\varphi_m(0)) = f(\varphi_m(l))$ we derive that $f(\varphi_m(a))$ attains the same common value for all $a \in A$. The same is then true for $\varphi_m(a)$, showing that $\varphi_m(a) = \varphi_m(0) = 0$ for any $a \in A$; that is, all elements of A are divisible by m, contradicting the assumption $\gcd(A) = 1$, except if $m = 1$ in which case $H = \mathbb{C}_l$. □

From Theorem 2 and Lemma 3 we deduce the key proposition used in the proof of Theorem 1.

Proposition 4. *Let A be a finite set of integers satisfying $|2A| < \frac{13}{4}|A| - \frac{9}{4}$. If $\dim(A) = 1$, then A is contained in an arithmetic progression with at most $2 \cdot 10^5|A|$ terms.*

The proof essentially follows that of [2, Proposition 2.3], with some simplifications, and with Theorem 2 replacing [3, Theorem 1].

Proof of Proposition 4. Without loss of generality we assume that $\{0, l\} \subseteq A \subseteq [0, l]$ with an integer $l > 0$, and that $\gcd(A) = 1$. We want to show that $l < 2 \cdot 10^5 |A|$.

Aiming at a contradiction, assume that $l \geqslant 2 \cdot 10^5 |A|$. Let $\mathcal{A} := \varphi_l(A) \subseteq \mathbb{C}_l$; thus, $|\mathcal{A}| = |A| - 1$. Since $\varphi_l(a) = \varphi_l(a + l)$ for any $a \in A \setminus \{0, l\}$, and $\varphi_l(0) = \varphi_l(l) = \varphi_l(2l)$, we have $|2A| \geqslant |2\mathcal{A}| + |A|$. It follows that

$$|2\mathcal{A}| \leqslant |2A| - |A| < \frac{9}{4}|A| - \frac{9}{4} = \frac{9}{4}|\mathcal{A}|,$$

allowing us to apply Theorem 2. We consider three possible cases corresponding to the three cases in the conclusion of the theorem.

Case (i): There is a subgroup $\mathcal{H} \leqslant \mathbb{C}_l$ such that $\mathcal{A}$ is contained in an $\mathcal{H}$-coset and $|\mathcal{A}| > C^{-1}|\mathcal{H}|$, where $C = 2 \cdot 10^5$. Since $0 \in A$ and $\gcd(A) = 1$, the subgroup $\mathcal{H}$ is not proper. Therefore $l = |\mathcal{H}| < 2 \cdot 10^5 |\mathcal{A}| < 2 \cdot 10^5 |A|$, as wanted.

Case (ii): There is a proper subgroup $\mathcal{H} < \mathbb{C}_l$ and an arithmetic progression $\mathcal{P} \subseteq \mathbb{C}_l$ of size $|\mathcal{P}| > 1$ such that $|\mathcal{P} + \mathcal{H}| = |\mathcal{P}||\mathcal{H}|$, $\mathcal{A} \subseteq \mathcal{P} + \mathcal{H}$, and $(|\mathcal{P}| - 1)|\mathcal{H}| \leqslant |2\mathcal{A}| - |\mathcal{A}|$. The image of $\mathcal{A}$ under the quotient map $\mathbb{C}_l \to \mathbb{C}_l/\mathcal{H}$ is contained in an arithmetic progression of size

$$\begin{aligned}|\mathcal{P}| \leqslant 1 + (|2\mathcal{A}| - |\mathcal{A}|)/|\mathcal{H}| &\leqslant 1 + \frac{5}{4}|\mathcal{A}|/|\mathcal{H}| \\ &< 1 + \frac{5}{4}|A|/|\mathcal{H}| \leqslant 1 + \frac{5}{8}10^{-5} l/|\mathcal{H}| < \frac{1}{2} l/|\mathcal{H}| = \frac{1}{2}|\mathbb{C}_l/\mathcal{H}|.\end{aligned}$$

The difference of this progression is coprime with $|\mathbb{C}_l/\mathcal{H}|$ in view of the assumptions $0 \in A$ and $\gcd(A) = 1$. Hence, the progression is rectifiable, and so is the image of A contained therein. The result now follows by applying Lemma 3.

Case (iii): There is a proper subgroup $\mathcal{H} < \mathbb{C}_l$ such that $\mathcal{A}$ meets exactly three $\mathcal{H}$-cosets, the cosets are not in an arithmetic progression, and $3|\mathcal{H}| \leqslant |2\mathcal{A}| - |\mathcal{A}|$. In this case the image of A in $\mathbb{C}_l/\mathcal{H}$ consists of three elements not in an arithmetic progression; therefore the image is isomorphic, say, to the set $\{0, 1, 3\} \subseteq \mathbb{Z}$, and an application of Lemma 3 completes the proof. □

Lemma 5 (Freiman [5, Lemma 1.14])**.** *For any finite, nonempty set A of integers, writing $d := \dim(A)$, we have*

$$|2A| \geqslant (d + 1)|A| - \binom{d+1}{2}.$$

Lemma 6 (Candela–Serra–Spiegel [2, Corollary 2.6])**.** *Let $A \subseteq \mathbb{Z}$ be a finite set with $\dim A = 2$. If $|2A| \leqslant \frac{10}{3}|A| - 7$, then A is contained in the union of two arithmetic progressions, P_1 and P_2, with the same difference, such that $|P_1 \cup P_2| \leqslant |2A| - 2|A| + 3$ and the sumsets $2P_1$, $P_1 + P_2$ and $2P_2$ are pairwise disjoint.*

The following result is, essentially, extracted from [9, Proof of Theorem 3], with a little twist that will help us keep the remainder terms under better control.

For a prime p and a subset $\mathcal{A} \subseteq \mathbb{C}_p$, by $\widehat{\mathcal{A}}$ we denote the non-normalized Fourier transform of the indicator function of $\mathcal{A}$:

$$\widehat{\mathcal{A}}(\chi) = \sum_{a \in \mathcal{A}} \chi(a); \quad \chi \in \widehat{\mathbb{C}_p}.$$

The principal character is denoted by 1. We let

$$\eta_{\mathcal{A}} := \max\{|\widehat{\mathcal{A}}(\chi)|/|\mathcal{A}| \colon \chi \neq 1\}.$$

Proposition 7. *Suppose that p is a prime, and $\mathcal{A} \subseteq \mathbb{C}_p$ is a nonempty subset of density $\alpha := |\mathcal{A}|/p < 1/2$. If $|2\mathcal{A}| = K|\mathcal{A}|$ and $\mathcal{A}$ is not an arithmetic progression, then*

$$(1 - \alpha K)(1 - \eta_{\mathcal{A}}^2) \leqslant 1 - K^{-1} - K^{-2} + (K - (1 - 2K^{-1})|\mathcal{A}|)/|\mathcal{A}|^2.$$

Proof. Let $\mathcal{S} := 2\mathcal{A}$ and $\mathcal{D} := \mathcal{A} - \mathcal{A}$. For a set $\mathcal{T} \subseteq \mathbb{C}_p$ and element $x \in \mathbb{C}_p$, we write $\mathcal{T}_x := \mathcal{T} \cap (x + \mathcal{T})$; thus, $|\mathcal{T}_x|$ is the number of representations of x as a difference of two elements of $\mathcal{T}$, and in particular $|\mathcal{T}_0| = |\mathcal{T}|$.

Consider the easily-verified identity

$$\frac{1}{p} \sum_{\chi \in \widehat{\mathbb{C}_p}} |\widehat{\mathcal{A}}(\chi)|^2 |\widehat{\mathcal{S}}(\chi)|^2 = \sum_{x \in \mathcal{D}} |\mathcal{A}_x||\mathcal{S}_x|. \tag{1}$$

For the left-hand side using the Parseval identity we obtain the estimate

$$\begin{aligned} \frac{1}{p} \sum_{\chi \in \widehat{\mathbb{C}_p}} |\widehat{\mathcal{A}}(\chi)|^2 |\widehat{\mathcal{S}}(\chi)|^2 &\leqslant \frac{1}{p} |\mathcal{A}|^2 |\mathcal{S}|^2 + \frac{1}{p} \eta_{\mathcal{A}}^2 |\mathcal{A}|^2 |\mathcal{S}|(p - |\mathcal{S}|) \\ &\leqslant \alpha K^2 |\mathcal{A}|^3 + \eta_{\mathcal{A}}^2 K |\mathcal{A}|^3 (1 - \alpha K). \end{aligned} \tag{2}$$

To estimate the right-hand side we recall the *Katz–Koester observation* $\mathcal{A} + \mathcal{A}_x \subseteq \mathcal{S}_x$, $x \in \mathbb{C}_p$. Let N be the number of elements $x \in \mathcal{D}$ with $|\mathcal{A}_x| = 1$. Notice that $N \leqslant |\mathcal{D}| \leqslant K^2|\mathcal{A}|$; here the first estimate is trivial, and the second is the Plünnecke–Ruzsa inequality. From the assumption $\alpha < 1/2$ and the theorems of Cauchy–Davenport and Vosper, we get

$$\begin{aligned} \sum_{x \in \mathcal{D}} |\mathcal{A}_x||\mathcal{S}_x| &\geqslant \sum_{x \in \mathcal{D} \setminus \{0\}} |\mathcal{A}_x||\mathcal{S}_x| + |\mathcal{A}||\mathcal{S}| \\ &\geqslant \sum_{x \in \mathcal{D} \setminus \{0\}} |\mathcal{A}_x||\mathcal{A} + \mathcal{A}_x| + |\mathcal{A}||\mathcal{S}| \\ &\geqslant \sum_{x \in \mathcal{D} \setminus \{0\}} |\mathcal{A}_x|(|\mathcal{A}| + |\mathcal{A}_x|) - N + |\mathcal{A}||\mathcal{S}| \\ &\geqslant \sum_{x \in \mathcal{D}} |\mathcal{A}_x|(|\mathcal{A}| + |\mathcal{A}_x|) - N + |\mathcal{A}||\mathcal{S}| - 2|\mathcal{A}|^2 \\ &\geqslant |\mathcal{A}|^3 + \mathsf{E}(\mathcal{A}) - K^2|\mathcal{A}| + (K - 2)|\mathcal{A}|^2 \end{aligned} \tag{3}$$

where $\mathsf{E}(\mathcal{A}) = \sum_{x\in\mathcal{D}} |\mathcal{A}_x|^2$ is the additive energy of $\mathcal{A}$, and where the third estimate follows from Vosper's theorem if $|A + A_x| \leqslant p - 2$, and otherwise from $|\mathcal{A} + \mathcal{A}_x| \geqslant p - 1 > 2\alpha p - 1 = 2|\mathcal{A}| - 1 \geqslant |\mathcal{A}| + |\mathcal{A}_x| - 1$.

Combining (1), (2), and (3), and using the basic bound $\mathsf{E}(\mathcal{A}) \geqslant |\mathcal{A}|^3/K$, we get

$$\alpha K^2|\mathcal{A}|^3 + \eta_{\mathcal{A}}^2 K|\mathcal{A}|^3(1-\alpha K) \geqslant (1+K^{-1})|\mathcal{A}|^3 - (K^2 - (K-2)|\mathcal{A}|)|\mathcal{A}|$$

whence

$$\begin{gathered}\alpha K + \eta_{\mathcal{A}}^2(1-\alpha K) \geqslant K^{-1} + K^{-2} - (K - (1-2K^{-1})|\mathcal{A}|)/|\mathcal{A}|^2, \\ (\eta_{\mathcal{A}}^2 - 1)(1-\alpha K) \geqslant K^{-1} + K^{-2} - 1 - (K - (1-2K^{-1})|\mathcal{A}|)/|\mathcal{A}|^2\end{gathered}$$

which is equivalent to the inequality sought. □

Corollary 8. *Let $\mathcal{A}$, α, and K be as in Proposition 7. If $\alpha < 10^{-5}$, $K < 2.7652$, and $|\mathcal{A}| \geqslant 10$, then $\eta_{\mathcal{A}} > \frac{8}{13}K - 1$.*

Proof. Assuming $\eta_{\mathcal{A}} \leqslant \frac{8}{13}K - 1$ we get

$$1 - \eta_{\mathcal{A}}^2 \geqslant \frac{16}{13}K - \frac{64}{169}K^2 = \frac{16}{169}K(13-4K)$$

whence, by Proposition 7,

$$(1-\alpha K)\frac{16}{169}K(13-4K) \leqslant 1 - K^{-1} - K^{-2} + (K - (1-2K^{-1})|\mathcal{A}|)/|\mathcal{A}|^2. \tag{4}$$

The left-hand side is decreasing both as a function of K (since $K > 13/8$) and as a function of α, while the right-hand side is an increasing function of K. Therefore (4) stays true with K substituted by 2.7652 and α by 10^{-5}; this results in a quadratic inequality in $|\mathcal{A}|$ which is false for $|\mathcal{A}| \geqslant 10$. □

The following lemma is standardly used to convert the "Fourier bias" (established in Corollary 8) into the "combinatorial bias".

Lemma 9 (Freiman [5])**.** *Suppose that p is a prime, and $\mathcal{A} \subseteq \mathbb{C}_p$ is a nonempty subset. There is an arithmetic progression $\mathcal{P} \subset \mathbb{C}_p$ with $|\mathcal{P}| \leqslant (p+1)/2$ terms such that*

$$|\mathcal{A} \cap \mathcal{P}| > \frac{1}{2}(1+\eta_{\mathcal{A}})|\mathcal{A}|.$$

Finally, we need the symmetric case of a version of the $(3n-4)$-theorem due to Grynkiewicz.

Theorem 10 (Special case of [7, Theorem 7.1])**.** *Let A be a finite set of integers. If $|2A| \leqslant 3|A| - 4$, then A is contained in an arithmetic progression with at most $|2A| - |A| + 1$ terms, and $2A$ contains an arithmetic progression with the same difference and at least $2|A| - 1$ terms.*

3 Proof of Theorem 1

Throughout the proof, we identify $\mathbb{C}_p$ with the additive group of the p-element field; accordingly, the automorphisms of $\mathbb{C}_p$ are identified with the dilates. We write $d * \mathcal{A} := \{da \colon a \in \mathcal{A}\}$ where d is an integer or an element of $\mathbb{C}_p$.

For $u \leqslant v$, by $[u, v]$ we denote both the set of all integers $u \leqslant z \leqslant v$ and the image of this set in $\mathbb{C}_p$ under the homomorphism φ_p. We may also occasionally identify integers with their images under φ_p. For brevity, we write $p' := (p-1)/2$.

Assuming that $\mathcal{A} \subseteq \mathbb{C}_p$ satisfies $|2\mathcal{A}| \leqslant K|\mathcal{A}| - 3$ with $K < 2.7652$ and $10 \leqslant |\mathcal{A}| < 1.25 \cdot 10^{-6}p$, we prove that $\mathcal{A}$ is contained in an arithmetic progression with at most $(p+1)/2$ terms; equivalently, there is an affine transformation that maps $\mathcal{A}$ into a subset of an interval of length at most p'. This will show that $\mathcal{A}$ is rectifiable and imply the result in view of Theorem 10.

Let $\mathcal{A}_0$ be a subset of $\mathcal{A}$ of the largest possible size such that $\mathcal{A}_0$ is contained in an arithmetic progression with at most $(p+1)/2$ terms. We observe that, by the maximality of $|\mathcal{A}_0|$, if $\mathcal{A}_0 \subseteq [0, l]$ with an integer $0 \leqslant l \leqslant p'$, then the two intervals of length $p' - l - 1$ adjacent to $[0, l]$ "from the left" and "from the right" do not contain any elements of $\mathcal{A}$; that is,

$$[l + p' + 1, p - 1] \cap \mathcal{A} = [l + 1, p'] \cap \mathcal{A} = \varnothing.$$

Therefore

$$\mathcal{A} \setminus \mathcal{A}_0 \subseteq [p' + 1, p' + l] = p' + [1, l]. \tag{5}$$

Suppose first that $\mathcal{A}_0$ is contained in an arithmetic progression with at most $2 \cdot 10^5|\mathcal{A}_0|$ terms. Having applied a suitable affine transformation, we assume that $\mathcal{A}_0 \subseteq [0, l]$ with $l < 2 \cdot 10^5|\mathcal{A}_0|$. By (5), we have

$$2 * \mathcal{A} \subseteq (2 * \mathcal{A}_0) \cup [1, 2l - 1] \subseteq [0, 2l].$$

In view of $2l + 1 < 4 \cdot 10^5|\mathcal{A}_0| \leqslant 4 \cdot 10^5|\mathcal{A}| \leqslant p'$, this shows that the affine transformation $z \mapsto 2z$ maps $\mathcal{A}$ into an interval of length at most p', which is shown above to imply the result.

We therefore assume from now on that $\mathcal{A}_0$ is not contained in an arithmetic progression with $2 \cdot 10^5|\mathcal{A}_0|$ or fewer terms; in particular, the set $\mathcal{A}_0$ itself is not an arithmetic progression.

In view of $10 \leqslant |\mathcal{A}| < 1.25 \cdot 10^{-6}p < 10^{-5}p$, we can apply Corollary 8, and then Lemma 9, to get

$$|\mathcal{A}_0| > \frac{4}{13}K|\mathcal{A}|; \tag{6}$$

it follows that

$$|2\mathcal{A}_0| \leqslant |2\mathcal{A}| \leqslant K|\mathcal{A}| - 3 < \frac{13}{4}|\mathcal{A}_0| - \frac{9}{4}. \tag{7}$$

Recalling the way the set $\mathcal{A}_0$ has been chosen, we find a set $A_0 \subseteq \mathbb{Z}$ such that $\mathcal{A}_0 = \varphi_p(A_0)$, $|A_0| = |\mathcal{A}_0|$, and A_0 is contained in an arithmetic progression with at most $p' + 1$ terms;

thus, A_0 is Freiman-isomorphic to $\mathcal{A}_0$, and as a result,

$$|2A_0| < \frac{13}{4}\,|A_0| - \frac{9}{4}.$$

Since $\mathcal{A}_0$ is not contained in an arithmetic progression with $2 \cdot 10^5|\mathcal{A}_0|$ or fewer terms, neither is A_0. (This does not follow from the mere fact that A_0 and $\mathcal{A}_0$ are Freiman-isomorphic, but does follow immediately by observing that $\mathcal{A}_0$ is the image of A_0 under a group homomorphism.) Consequently, by Proposition 4, we conclude that $\dim(A_0) \geqslant 2$, and then, indeed, $\dim(A_0) = 2$ by Lemma 5. Applying Lemma 6, we derive that A_0 is contained in the union of two arithmetic progressions, say P_1 and P_2, with the same difference, such that $|P_1 \cup P_2| \leqslant |2A_0| - 2|A_0| + 3$ and the sumsets $2P_1$, $P_1 + P_2$ and $2P_2$ are pairwise disjoint. Hence, $\mathcal{A}_0$ is contained in the union of the disjoint progressions $\mathcal{P}_1 := \varphi_p(P_1)$ and $\mathcal{P}_2 := \varphi_p(P_2)$. Let $\mathcal{A}_1 = \mathcal{A}_0 \cap \mathcal{P}_1$ and $\mathcal{A}_2 = \mathcal{A}_0 \cap \mathcal{P}_2$. Without loss of generality, we assume that $|\mathcal{A}_1| \geqslant |\mathcal{A}_0|/2$.

Applying a suitable affine transformation, we can arrange that $\mathcal{P}_1 = [0, b]$ and $\mathcal{P}_2 = [c, d]$, where $0 \leqslant b < c \leqslant d < p$ are integers such that

$$c - b \leqslant p - d. \tag{8}$$

Recalling (6), we obtain

$$\begin{aligned} b + d - c = |\mathcal{P}_1| + |\mathcal{P}_2| - 2 &\leqslant |2\mathcal{A}_0| - 2|\mathcal{A}_0| + 1 \\ &\leqslant |2\mathcal{A}| - 2|\mathcal{A}_0| + 1 < K|\mathcal{A}| - \frac{8}{13}K|\mathcal{A}| = \frac{5}{13}K|\mathcal{A}| < 2|\mathcal{A}|, \end{aligned}$$

whence

$$b + (d - c) < 2|\mathcal{A}|. \tag{9}$$

Writing $n := |\mathcal{A}|$, we therefore have

$$\mathcal{A}_1 \subseteq [0, b] \subseteq [0, 2n], \quad \mathcal{A}_2 \subseteq c + [0, d - c] \subseteq c + [0, 2n], \tag{10}$$

and also

$$(c - b) + (p - d) = p - (d - c) - b > p - 2n.$$

Along with (8), the last estimate gives $p - d \geqslant p' - n + 1$ and, consequently, $d \leqslant p' + n$. In fact, we have

$$4n < d < p' - 4n; \tag{11}$$

here the lower bound follows immediately from the assumption that $\mathcal{A}_0$ is not contained in a progression with $2 \cdot 10^5|\mathcal{A}_0|$ or fewer terms, and the upper bound follows by observing that if we had $p' - 4n \leqslant d \leqslant p' + n$, in view of (9) this would imply $[c, d] = [d - (d - c), d] \subseteq [d - 2n, d] \subseteq p' + [-6n, n]$ and, consequently, $2 * \mathcal{A}_0 \subseteq [0, 2b] \cup [-12n - 1, 2n - 1] \subseteq [-12n - 1, 4n]$, in a contradiction with the same assumption.

We have $2\mathcal{A}_0 = 2\mathcal{A}_1 \cup (\mathcal{A}_1 + \mathcal{A}_2) \cup 2\mathcal{A}_2$ where the union is disjoint; therefore, by the Cauchy–Davenport theorem,

$$|2\mathcal{A}_0| \geqslant (2|\mathcal{A}_1| - 1) + (|\mathcal{A}_1| + |\mathcal{A}_2| - 1) + (2|\mathcal{A}_2| - 1) = 3|\mathcal{A}_0| - 3. \tag{12}$$

It follows that for any $a \in \mathcal{A}\setminus\mathcal{A}_0$ we have $(a+\mathcal{A}_1)\cap(2\mathcal{A}_0) \neq \varnothing$, as assuming the opposite,

$$|2\mathcal{A}| \geqslant |2\mathcal{A}_0| + |a+\mathcal{A}_1| \geqslant 3|\mathcal{A}_0| - 3 + \frac{1}{2}|\mathcal{A}_0| > \frac{7}{2}\cdot\frac{4}{13}K|\mathcal{A}| - 3 = \frac{14}{13}K|\mathcal{A}| - 3,$$

a contradiction. Therefore, recalling (10),

$$\mathcal{A}\setminus\mathcal{A}_0 \subseteq 2\mathcal{A}_0 - \mathcal{A}_1 \subseteq \{0, c, 2c\} + [-2n, 4n]. \tag{13}$$

On the other hand, since $d < p'$, we can apply (5) with $l = d$ to get

$$\mathcal{A}\setminus\mathcal{A}_0 \subseteq p' + [1, d]. \tag{14}$$

Comparing (13) and (14), and observing that, in view of (11), both intervals $[-2n, 4n]$ and $c + [-2n, 4n]$ are disjoint from the interval $p' + [1, d]$, we conclude that

$$\mathcal{A}\setminus\mathcal{A}_0 \subseteq 2c + [-2n, 4n] \tag{15}$$

and, consequently, using (10) once again,

$$\mathcal{A} \subseteq \{0, c, 2c\} + [-2n, 4n].$$

We notice that the set $2(\mathcal{A}\setminus\mathcal{A}_0)$ is not disjoint from the set $2\mathcal{A}_0$ as otherwise using (12) we would get

$$\begin{aligned}|2\mathcal{A}| &\geqslant |2(\mathcal{A}\setminus\mathcal{A}_0)| + |2\mathcal{A}_0| \geqslant 2|\mathcal{A}\setminus\mathcal{A}_0| - 1 + 3|\mathcal{A}_0| - 3\\ &= 2|\mathcal{A}| + |\mathcal{A}_0| - 4 \geqslant \left(2 + \frac{4}{13}K\right)|\mathcal{A}| - 4 > K|\mathcal{A}| - 3.\end{aligned}$$

Since $2(\mathcal{A}\setminus\mathcal{A}_0) \subseteq 4c + [-4n, 8n]$ by (15), and $2\mathcal{A}_0 \subseteq \{0, c, 2c\} + [0, 4n]$ in view of (10), we conclude that $kc \in [-8n, 8n]$ for some $k \in \{2, 3, 4\}$. Therefore $k*\mathcal{A}_0 \subseteq \{0, kc\} + [0, 2kn] \subseteq [-8n, (8+2k)n]$. Hence, $\mathcal{A}_0$ is contained in an arithmetic progression with at most $(16+2k)n + 1 < 25n < 2\cdot 10^5|\mathcal{A}_0|$ terms, a contradiction.

References

[1] P. Candela, D. González-Sánchez, and D. Grynkiewicz, On sets with small sumset and m-sum-free sets in Z/pZ, *Bull. Soc. Math. France* 149 (1): 155–177, 2021).

[2] P. Candela, O. Serra, and C. Spiegel. A step beyond Freiman's theorem for set addition modulo a prime. *J. Theor. Nombres Bordeaux*, 32: 275–289, 2020.

[3] J.-M. Deshouillers and G. A. Freiman. A step beyond Kneser's theorem for abelian finite groups. *Proceedings of the London Mathematical Society* 86 (1): 1–28, 2003.

[4] G. Freiman. Inverse problems in additive number theory. Addition of sets of residues modulo a prime. *Dokl. Akad. Nauk SSSR* 141: 571–573, 1961.

[5] G. Freiman. Foundations of a structural theory of set addition. Translated from the Russian. Translations of mathematical monographs. *American Mathematical Society, Providence, RI*, 1973.

[6] B. Green and I. Z. Ruzsa. Sets with small sumset and rectification. *Bulletin of the London Mathematical Society*, 38(1):43–52, 2006.

[7] D. J. Grynkiewicz. *Structural additive theory.* Springer Science & Business Media 30, 2013.

[8] V. F. Lev. Small doubling in cyclic groups. *J. Number Theory* 243:561–614, 2023.

[9] V. F. Lev and I. D. Shkredov. Small doubling in prime-order groups: from 2.4 to 2.6. *Journal of Number Theory* 217:278–291, 2020.

[10] Ø. J. Rødseth. On Freiman's 2.4-theorem. *Skr. K. Nor. Vidensk. Selsk* 4:11–18, 2006.

[11] O. Serra and G. Zémor. Large sets with small doubling modulo p are well covered by an arithmetic progression. *Annales de l'institut Fourier* 59:2043–2060, 2009.