Bulletin
de la SOCIÉTÉ MATHÉMATIQUE DE FRANCE

ON SETS WITH SMALL SUMSET AND m-SUM-FREE SETS IN $\mathbb{Z}/p\mathbb{Z}$

Pablo Candela, Diego González-Sánchez & David J. Grynkiewicz

Tome 149
Fascicule 1

2021

SOCIÉTÉ MATHÉMATIQUE DE FRANCE

pages 155-177

Le *Bulletin de la Société Mathématique de France* est un périodique trimestriel de la Société Mathématique de France.

Fascicule 1, tome 149, mars 2021

Diffusion

Maison de la SMF
Case 916 - Luminy
13288 Marseille Cedex 9
France
commandes@smf.emath.fr

AMS
P.O. Box 6248
Providence RI 02940
USA
www.ams.org

Tarifs

Vente au numéro : 43 € ($ 64)
Abonnement électronique : 135 € ($ 202),
avec supplément papier : Europe 179 €, hors Europe 197 € ($ 296)
Des conditions spéciales sont accordées aux membres de la SMF.

Secrétariat : Bulletin de la SMF

Bulletin de la Société Mathématique de France
Société Mathématique de France
Institut Henri Poincaré, 11, rue Pierre et Marie Curie
75231 Paris Cedex 05, France
Tél : (33) 1 44 27 67 99 • Fax : (33) 1 40 46 90 96
bulletin@smf.emath.fr • smf.emath.fr

ISSN 0037-9484 (print) 2102-622X (electronic)

Directeur de la publication : Fabien DURAND

Bull. Soc. Math. France
149 (1), 2021, p. 155-177

ON SETS WITH SMALL SUMSET AND m-SUM-FREE SETS IN $\mathbb{Z}/p\mathbb{Z}$

BY PABLO CANDELA, DIEGO GONZÁLEZ-SÁNCHEZ & DAVID J. GRYNKIEWICZ

ABSTRACT. — The $3k-4$ conjecture in groups $\mathbb{Z}/p\mathbb{Z}$ for p prime states that if A is a nonempty subset of $\mathbb{Z}/p\mathbb{Z}$ satisfying $2A \neq \mathbb{Z}/p\mathbb{Z}$ and $|2A| = 2|A| + r \leq \min\{3|A| - 4,\ p - r - 4\}$, then A is covered by an arithmetic progression of size at most $|A| + r + 1$. Previously, the best result toward this conjecture, without any additional constraint on $|A|$, was a theorem of Serra and Zémor proving the conjecture provided $r \leq 0.0001|A|$. Subject to the mild additional constraint $|2A| \leq 3p/4$, which is optimal in the sense explained in the paper, our first main result improves the bound on r, allowing $r \leq 0.1368|A|$. We also prove a variant that further improves this bound on r provided that A is sufficiently dense. We then give several applications. First, we apply the above variant to give a new upper bound for the maximal density of m-sum-free sets in $\mathbb{Z}/p\mathbb{Z}$, i.e., sets A having no solution $(x, y, z) \in A^3$ to the equation $x + y = mz$, where $m \geq 3$ is a fixed integer. The previous best upper bound for this maximal density was $1/3.0001$ (using the Serra-Zémor theorem). We improve this to $1/3.1955$. We also present a construction following an idea of Schoen, which yields a lower bound for this maximal density of the form $1/8 + o(1)_{p\to\infty}$. Another application of our main results concerns sets of the form $\frac{A+A}{A}$ in $\mathbb{F}_p$, and we also improve the structural description of large sum-free sets in $\mathbb{Z}/p\mathbb{Z}$.

Texte reçu le 11 septembre 2019, modifié le 12 mars 2020, accepté le 20 octobre 2020.

PABLO CANDELA, Universidad Autónoma de Madrid, and ICMAT, Madrid 28049, Spain • *E-mail :* pablo.candela@uam.es

DIEGO GONZÁLEZ-SÁNCHEZ, Universidad Autónoma de Madrid, and ICMAT, Madrid 28049, Spain • *E-mail :* diego.gonzalezs@predoc.uam.es

DAVID J. GRYNKIEWICZ, University of Memphis, Department of Mathematical Sciences, Memphis, TN 38152 • *E-mail :* diambri@hotmail.com

Mathematical subject classification (2010). — 11P70, 11B13, 05B10.

Key words and phrases. — Additive combinatorics, Small sumset, m-sum-free set, Freiman's $3k-4$ theorem, $3k-4$ conjecture.

This work has benefited from support from the Spanish Ministerio de Ciencia e Innovación project MTM2017-83496-P and from the La Caixa Foundation (ID 100010434) under agreement LCF/BQ/SO16/52270027.

0037-9484/2021/155/$ 5.00
doi:10.24033/bsmf.2827

RÉSUMÉ (*Sur les ensembles de petite somme et les ensembles sans m-somme dans $\mathbb{Z}/p\mathbb{Z}$*). — La conjecture $3k-4$ dans les groupes $\mathbb{Z}/p\mathbb{Z}$, pour p premier, affirme que si A est un sous-ensemble non vide de $\mathbb{Z}/p\mathbb{Z}$ vérifiant $2A \neq \mathbb{Z}/p\mathbb{Z}$ et $|2A| = 2|A| + r \leq \min\{3|A| - 4,\ p - r - 4\}$, alors A est inclus dans une suite arithmétique de cardinalité au plus $|A|+r+1$. Le meilleur résultat précédent vers cette conjecture, sans contraintes supplémentaires sur $|A|$, est un théorème de Serra et Zémor qui confirme la conjecture pour $r \leq 0.0001|A|$. Sous la faible contrainte additionnelle $|2A| \leq 3p/4$, qui est optimale en un sens détaillé dans l'article, notre premier résultat principal améliore la borne supérieure sur r, permettant de prendre $r \leq 0.1368|A|$. Nous démontrons aussi une variante qui améliore davantage la borne sur r pour tout ensemble A suffisamment dense. Nous présentons ensuite plusieurs applications. Premièrement, la variante en question est employée pour obtenir une nouvelle borne supérieure pour la densité maximale des ensembles sans m-somme dans $\mathbb{Z}/p\mathbb{Z}$, i.e., les ensembles A tels qu'il n'existe aucune solution $(x, y, z) \in A^3$ de l'équation $x + y = mz$, où $m \geq 3$ est un entier fixé. Précédemment, la meilleure borne supérieure pour cette densité maximale était 1/3.0001 (comme conséquence du théorème de Serra–Zémor). Nous obtenons ici la borne améliorée 1/3.1955. Nous présentons aussi une construction suivant une idée de Schoen, qui fournit une borne inférieure $1/8 + o(1)_{p\to\infty}$ pour la densité maximale en question. Une autre application de nos résultats concerne les ensembles de la forme $\frac{A+A}{A}$ dans $\mathbb{F}_p$. Nous donnons aussi une description améliorée de la structure des grands ensembles sans somme dans $\mathbb{Z}/p\mathbb{Z}$.

1. Introduction

Given a subset A of an abelian group G, we often denote the sumset $A+A = \{x + y : x, y \in A\}$ by $2A$ and we denote the complement $G \setminus A$ by $\overline{A}$.

One of the central topics in additive number theory is the study of the structure of a finite subset A of an abelian group under the assumption that the sumset $2A$ is small. In this paper, we focus on groups $\mathbb{Z}/p\mathbb{Z}$ of integers modulo a prime p and on the regime in which the *doubling constant* $|2A|/|A|$ is within a small additive constant of the minimum possible value.

To put this into context, let us recall the basic fact that a finite set A of integers always satisfies $|2A| \geq 2|A| - 1$ and that this minimum is attained only if A is an arithmetic progression (see [12, Theorem 3.1]). This description of extremal sets is extended by a result of Freiman, known as the $3k-4$ theorem, which tells us that A is still efficiently covered by an arithmetic progression even when $|2A|$ is as large as $3|A| - 4$.

THEOREM 1.1 (Freiman's $3k-4$ theorem). — *Let $A \subseteq \mathbb{Z}$ be a finite set satisfying $|2A| \leq 3|A| - 4$. Then there is an arithmetic progression $P \subseteq \mathbb{Z}$, such that $A \subseteq P$ and $|P| \leq |2A| - |A| + 1$.*

For sets A in $\mathbb{Z}/p\mathbb{Z}$ with $2A \neq \mathbb{Z}/p\mathbb{Z}$, the Cauchy–Davenport theorem [12, Theorem 6.2] gives the lower bound analogous to the one for $\mathbb{Z}$ mentioned above, namely $|2A| \geq 2|A| - 1$, and the description of extremal sets as arithmetic

progressions (when $|2A| < p-1$) is given by Vosper's theorem [12, Theorem 8.1].

It is widely believed that an analogue of Freiman's $3k-4$ theorem holds for subsets of $\mathbb{Z}/p\mathbb{Z}$ under some mild additional upper bound on $|2A|$ (or on $|A|$). More precisely, the following conjecture is believed to be true (see [12, Conjecture 19.2]), describing efficiently not just A but also $2A$, in terms of progressions.

CONJECTURE 1.2. — *Let p be a prime and let $A \subset \mathbb{Z}/p\mathbb{Z}$ be a nonempty subset satisfying $2A \neq \mathbb{Z}/p\mathbb{Z}$ and $|2A| = 2|A| + r \leq \min\{3|A| - 4,\ p - r - 4\}$. Then there exist arithmetic progressions $P_A, P_{2A} \subseteq \mathbb{Z}/p\mathbb{Z}$ with the same difference, such that $A \subseteq P_A$, $|P_A| \leq |A| + r + 1$, $P_{2A} \subseteq 2A$, and $|P_{2A}| \geq 2|A| - 1$.*

Progress toward this conjecture was initiated by Freiman himself, who proved in [10] that the conclusion concerning P_A holds provided that $|2A| \leq 2.4|A| - 3$ and $|A| < p/35$. Since then, there has been much work improving Freiman's result in various ways. For instance, Rødseth showed in [17] that the constraint $|A| < p/35$ can be weakened to $|A| < p/10.7$ while maintaining the doubling constant 2.4. In [11], Green and Ruzsa pushed the doubling constant up to 3, at the cost of a stronger constraint $|A| < p/10^{215}$. In [20], Serra and Zémor obtained a result with no constraint on $|A|$ other than the bounds on $|2A|$ in the conjecture, with the same conclusion concerning P_A but at the cost of reducing the doubling constant, namely, assuming that $|2A| \leq (2+\alpha)|A|$ with $\alpha < 0.0001$. See also [5, 14] for recent improvements on the doubling constant 2.4 in Freiman's result. The book [12] presents various other results towards Conjecture 1.2, in a treatment covering many of the methods from the works mentioned above.

In this paper, we establish the following new result regarding Conjecture 1.2, which noticeably improves the doubling constant obtained by Serra and Zémor in [20] at the cost of only adding the constraint $|2A| \leq \frac{3}{4}p$.

THEOREM 1.3. — *Let p be prime, let $A \subseteq \mathbb{Z}/p\mathbb{Z}$ be a nonempty subset with $|2A| = 2|A| + r$, and let $\alpha \approx 0.136861$ be the unique real root of the cubic $4x^3 + 9x^2 + 6x - 1$. Suppose*

$$|2A| \leq (2+\alpha)|A| - 3 \quad \text{and} \quad |2A| \leq \frac{3}{4}p.$$

Then there exist arithmetic progressions $P_A, P_{2A} \subseteq \mathbb{Z}/p\mathbb{Z}$ with the same difference, such that $A \subseteq P_A$, $|P_A| \leq |A| + r + 1$, $P_{2A} \subseteq 2A$, and $|P_{2A}| \geq 2|A| - 1$.

Unlike in [20], here we do have a constraint on $|A|$ in the form of the upper bound $|2A| \leq \frac{3}{4}p$. However, this upper bound is still optimal in the following weak sense. The conjectured upper bound on $|2A|$ (given by Conjecture 1.2) is $p - r - 4$. However, in the extremal case where $r = |A| - 4$ (the largest value of r allowed in Conjecture 1.2), the conjectured bound implies $3|A| - 4 = |2A| \leq$

$p - |A|$, whence $|A| \le \frac{p+4}{4}$ and $|2A| = 3|A| - 4 \le \frac{3p}{4} - 1$. Thus, the bound $p - r - 4$ becomes as small as $\frac{3p}{4} - 1$, as we *range* over all allowed values for α and $|A|$, making $\frac{3}{4}p$ the optimal bound independent of α and r.

Let us emphasize that our improvement upon the Serra–Zémor result (i.e., our weakening of the constraint on α) is valid for $|A| \le \frac{0.75p+3}{2+\alpha}$, whereas the natural upper bound on $|A|$ given by Conjecture 1.2 is larger, namely $|A| \le \frac{p+2}{2+2\alpha}$. Therefore, in the regime $\frac{0.75p+3}{2+\alpha} < |A| \le \frac{p+2}{2+2\alpha}$, our result does not improve on that of Serra and Zémor.

We also prove the following variant of Theorem 1.3, which is optimized for sets A whose density is large but at most $1/3$. This optimization is designed for an application concerning m-sum-free sets, which we discuss below.

THEOREM 1.4. — *Let p be prime, let $\eta \in (0,1)$, let $A \subseteq \mathbb{Z}/p\mathbb{Z}$ be a set with $|A| \ge \eta\, p > 0$ and $|2A| = 2|A| + r < p$, and let*

$$\alpha = -\frac{5}{4} + \frac{1}{4}\sqrt{9 + 8\,\eta\, p \sin(\pi/p)/\sin(\pi\eta/3)}.$$

Suppose

$$|2A| \le (2+\alpha)|A| - 3 \quad \textit{and} \quad |A| \le \frac{p-r}{3}.$$

Then there exist arithmetic progressions $P_A, P_{2A} \subseteq \mathbb{Z}/p\mathbb{Z}$ with the same difference such that $A \subseteq P_A$, $|P_A| \le |A| + r + 1$, $P_{2A} \subseteq 2A$, and $|P_{2A}| \ge 2|A| - 1$.

We apply this result to obtain new upper bounds for the size of m-sum-free sets in $\mathbb{Z}/p\mathbb{Z}$. For a positive integer m, a subset A of an abelian group is said to be *m-sum-free* if there is no triple $(x, y, z) \in A^3$ satisfying $x + y = mz$. These sets have been studied in numerous works on arithmetic combinatorics, including various types of abelian group settings [1, 8, 7, 16, 15] (see also [4, Section 3] for an overview of this topic). In $\mathbb{Z}/p\mathbb{Z}$, a central goal concerning these sets is to estimate the quantity

$$d_m(\mathbb{Z}/p\mathbb{Z}) = \max\big\{\tfrac{|A|}{p} : A \subseteq \mathbb{Z}/p\mathbb{Z} \text{ } m\text{-sum-free}\big\}. \tag{1}$$

This goal splits naturally into two problems of different nature. On the one hand, we have the case $m = 2$, which is the only one in which the solutions of the linear equation in question (i.e., three-term arithmetic progressions) form a translation invariant set. Roth's theorem [18] tells us that $d_2(\mathbb{Z}/p\mathbb{Z}) \to 0$ as $p \to \infty$, and the problem in this case is then the well-known one of determining the optimal bounds for Roth's theorem, i.e., how fast $d_2(\mathbb{Z}/p\mathbb{Z})$ vanishes as p increases (recent developments in this direction include [3, 19]). On the other hand, we have the cases $m \ge 3$. For each of these, the above-mentioned translation invariance fails, and it is known that $d_m(\mathbb{Z}/p\mathbb{Z})$ converges, as $p \to \infty$ through primes, to a positive constant d_m that can be modeled on the circle group (see [6]), the problem then being to determine this constant. Our application of Theorem 1.4 makes progress on the latter problem.

Note that, if A is m-sum-free, then the *dilate* $m\cdot A = \{mx : x \in A\} \subseteq \mathbb{Z}/p\mathbb{Z}$ satisfies $2A \cap m\cdot A = \emptyset$, whence, if m and p are coprime, we have $|2A|+|m\cdot A| = |2A| + |A| \leq p$. Combining this with the bound $|2A| \geq 2|A| - 1$ given by the Cauchy–Davenport Theorem, we deduce the simple bound $|A| \leq \frac{p+1}{3}$, which implies in particular that $d_m \leq 1/3$. It was noted in [4] that partial versions of Conjecture 1.2 can be used to improve on this bound, provided that these versions are applicable to sets of density up to $1/3$. The best version available for that purpose in [4] was given by the theorem of Serra and Zémor mentioned above, and this resulted in the first upper bound for d_m below $1/3$, namely $1/3.0001$ (see [4, Theorem 3.1]). In this paper, using Theorem 1.4 we obtain the following improvement.

THEOREM 1.5. — *Let $p \geq 80$ be a prime, let m be an integer in $[2, p-2]$, and let $c = c(p)$ be the solution to the equation $\left(7+\sqrt{8\,c\,p\sin(\pi/p)/\sin(\pi c/3)+9}\right)c = 4 + \frac{12}{p}$. Then $d_m(\mathbb{Z}/p\mathbb{Z}) < c$. In particular, $d_m \leq \frac{1}{3.1955}$.*

The following observation, relating this theorem to the study of sum-products in the field $\mathbb{F}_p$, was made by the anonymous referee: if $(A+A)\cap m\cdot A$ contains a nonzero element and $0 \notin A$, then m is in the set $\frac{A+A}{A} := \{(a_1+a_2)a_3^{-1} : a_1, a_2, a_3 \in A\} \subset \mathbb{F}_p$, and, therefore, Theorem 1.5 has the following consequence.

COROLLARY 1.6. — *If $A \subset \mathbb{F}_p \setminus \{0\}$ satisfies $|A| \geq 0.313\,p$, then for p sufficiently large we have $\mathbb{F}_p \setminus \{-1, 0, 1\} \subseteq \frac{A+A}{A}$.*

This result is an analogue, for sets $\frac{A+A}{A}$, of Theorem 1.1 in [2], which says that if $A \subset \mathbb{F}_p$ has $|A| \geq 0.3051\,p$, then for p sufficiently large, we have $\mathbb{F}_p \setminus \{0\} \subseteq (A+A)A := \{(a_1+a_2)a_3 : a_i \in A\}$.

Regarding lower bounds for $d_m(\mathbb{Z}/p\mathbb{Z})$, note that, identifying $\mathbb{Z}/p\mathbb{Z}$ with the integers $[0, p-1]$, the interval $(\frac{2}{m^2-4}p, \frac{m}{m^2-4}p)$ is an m-sum-free set. This set has asymptotic density $\frac{1}{m+2}$ and is still the greatest known example for $m \leq 6$. However, for larger values of m, a construction of Tomasz Schoen (personal communication), presented in this paper in Lemma 3.1 in an optimized form thanks to indications of the anonymous referee, yields the improved lower bound $d_m \geq \frac{1}{8}$. The following theorem summarizes these results.

THEOREM 1.7. — *For $m \leq 6$, we have $d_m \geq \frac{1}{m+2}$. For $m \geq 7$, we have $d_m \geq \frac{1}{8}$.*

Our final application concerns the study of large sum-free sets in $\mathbb{Z}/p\mathbb{Z}$ (i.e. the case $m = 1$ of m-sum-free sets as defined above). It is well-known, by the argument using the Cauchy–Davenport theorem mentioned above, that a sum-free set in $\mathbb{Z}/p\mathbb{Z}$ has size at most $\lfloor (p+1)/3 \rfloor$ and that this bound is attained by the interval $I = (p/3, 2p/3) \subset \mathbb{Z}/p\mathbb{Z}$ and by any nonzero dilate

of I. Several works have studied the question of the robustness of this structural description, namely, whether every sum-free set in $\mathbb{Z}/p\mathbb{Z}$ of density close to $1/3$ must resemble a dilate of I. In this direction, the following theorem was proved by Deshouillers and Lev in [9].

THEOREM 1.8. — *Let p be a sufficiently large prime and suppose that $A \subset \mathbb{Z}/p\mathbb{Z}$ is sum-free. If $|A| > 0.318\,p$, then there exists $d \in \mathbb{Z}$, such that $A \subset d \cdot [\,|A|, p - |A|\,]$.*

Applying Theorem 1.4, we improve the constant 0.318 to 0.313.

The paper is laid out as follows. In Section 2, we prove Theorems 1.3 and 1.4. Our results on m-sum-free sets are proved in Section 3. In Section 3.1, we present the above construction and deduce Theorem 1.7. In Section 3.2, we apply Theorem 1.4 to obtain Theorem 1.5. Finally, in Section 3.3, we obtain the above-mentioned improvement of Theorem 1.8.

2. New bounds toward the $3k-4$ conjecture in $\mathbb{Z}/p\mathbb{Z}$

Our first task in this section is to prove Theorem 1.3. We shall obtain this result as the special case $\varepsilon = 3/4$ of the following theorem.

THEOREM 2.1. — *Let p be prime, let $0 < \varepsilon \leq \frac{3}{4}$ be a real number, let α be the unique positive root of the cubic $4x^3 + (12 - 4\varepsilon)x^2 + (9 - 4\varepsilon)x + (8\varepsilon - 7)$, and let $A \subseteq \mathbb{Z}/p\mathbb{Z}$ be a nonempty subset with $|2A| = 2|A| + r$. Suppose*

$$|2A| \leq (2+\alpha)|A| - 3 \quad \textit{and} \quad |2A| \leq \varepsilon\, p.$$

Then there exist arithmetic progressions $P_A, P_{2A} \subseteq \mathbb{Z}/p\mathbb{Z}$ with the same difference, such that $A \subseteq P_A$, $|P_A| \leq |A| + r + 1$, $P_{2A} \subseteq 2A$, and $|P_{2A}| \geq 2|A| - 1$.

The proof is a modification of the argument used to prove [12, Theorem 19.3], itself based on the original work of Freiman [10] and incorporating improvements to the calculations noted by Rødseth [17]. The main new contribution is an argument to allow the restriction $|2A| \leq \frac{1}{2}(p+3)$ from [12, Theorem 19.3] to be replaced by the above condition $|2A| \leq \varepsilon p$. For $\varepsilon = 3/4$, this is optimal in the sense explained in the Introduction.

In the proof of Theorem 2.1, we use the following version of the $3k-4$ theorem for $\mathbb{Z}$. Here, for $X \subseteq \mathbb{Z}$, we denote the greatest common divisor $\gcd(X - X)$ by $\gcd^*(X)$. Note, for $|X| \geq 2$, that $d = \gcd^*(X)$ is the minimal $d \geq 1$, such that X is contained in an arithmetic progression with difference d. We remark that, when $B = -A$, we have $P_{A-A} \subseteq A - A$ and $-P_{A-A} \subseteq -(A-A) = A - A$. Since $2|P_{A-A}| \geq 4|A| - 2 > |A - A|$, the progressions P_{A-A} and $-P_{A-A}$ intersect, ensuring that $P = P_{A-A} \cup -P_{A-A} \subseteq A - A$ is a progression contained in $A - A$ with $|P| \geq 2|A| - 1$ and $-P = P$. Thus, the progression P_{A-A} in Theorem 2.2 can be assumed to be symmetric (i.e., centered at the origin) when $B = -A$.

THEOREM 2.2. — *Let A, $B \subseteq \mathbb{Z}$ be finite, nonempty subsets with* $\gcd^*(A+B) = 1$ *and*

$$|A+B| = |A| + |B| + r \leq |A| + |B| + \min\{|A|, |B|\} - 3 - \delta,$$

where $\delta = 1$ if $x + A = B$ for some $x \in \mathbb{Z}$, and otherwise $\delta = 0$. Then there are arithmetic progressions P_A, P_B, $P_{A+B} \subseteq \mathbb{Z}$ with common difference 1*, such that $A \subseteq P_A$, $B \subseteq P_B$, $P_{A+B} \subseteq A + B$, $|P_A| \leq |A| + r + 1$, $|P_B| \leq |B| + r + 1$ and $|P_{A+B}| \geq |A| + |B| - 1$.*

Let G and G' be abelian groups and let A, $B \subseteq G$. A *Freiman isomorphism* is a well-defined map $\psi : A + B \to G'$ defined by two coordinate maps $\psi_A : A \to G'$ and $\psi_B : B \to G'$, such that $\psi(x + y) = \psi_A(x) + \psi_B(y)$ for all $x \in A$ and $y \in B$. That ψ is well-defined is equivalent to the statement that $\psi_A(x_1) + \psi_B(y_1) = \psi_A(x_2) + \psi_B(y_2)$ whenever $x_1 + y_1 = x_2 + y_2$, for x_1, $x_2 \in A$ and y_1, $y_2 \in B$, and $\psi_A(A)+\psi_B(B)$ is then the homomorphic image of $A + B$. It is an isomorphism if ψ is injective on $A + B$, which is equivalent to $\psi_A(x_1)+\psi_B(y_1) = \psi_A(x_2)+\psi_B(y_2)$ holding if and only if $x_1+y_1 = x_2+y_2$, for x_1, $x_2 \in A$ and y_1, $y_2 \in B$. We denote this by $A + B \cong \psi_A(A) + \psi_B(B)$. A Freiman homomorphism $\psi : A + B \to G'$ on the sumset defines a Freiman homomorphism $\psi' : A - B \to G'$ on the difference set given by $\psi'(x - y) = \psi_A(x) - \psi_B(y)$, for $x \in A$ and $y \in B$, which is an isomorphism when ψ is. In the special case when $A = B$, we find that $\psi_A(x) + \psi_B(y) = \psi_A(y) + \psi_B(x)$ for all x, $y \in A = B$, implying $\psi_B(x) = \psi_A(x) + (\psi_B(y) - \psi_A(y))$ for any x, $y \in A = B$. Fixing $y \in A$ and letting x range over all possible $x \in A$ shows that the map ψ_B is simply a translate of the map ψ_A. This means it can (and generally will) be assumed that $\psi_A = \psi_B$ for a Freiman homomorphism ψ when $A = B$. See [12, Chapter 20] for a fuller discussion regarding Freiman homomorphisms.

For a prime p, nonzero $g \in \mathbb{Z}/p\mathbb{Z}$ (which is then a generator of $\mathbb{Z}/p\mathbb{Z}$), and integers $m \leq n$, let

$$[m, n]_g = \{mg, (m + 1)g, \ldots, ng\}$$

denote the corresponding interval in $\mathbb{Z}/p\mathbb{Z}$. If $m > n$, then $[m, n]_g = \emptyset$. We define (for each $g \in \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$) a function ℓ_g from the set of subsets $X \subset \mathbb{Z}/p\mathbb{Z}$ to $\mathbb{Z}_{\geq 0}$, by

$$\ell_g(X) := \min\{|P| : P \text{ is an arithmetic progression of difference } g \text{ with } X \subset P\}.$$

We let $\overline{X} = (\mathbb{Z}/p\mathbb{Z}) \setminus X$ denote the complement of X in $\mathbb{Z}/p\mathbb{Z}$. We say that a sumset $A + B \subseteq \mathbb{Z}/p\mathbb{Z}$ *is rectifiable*, if $\ell_g(A) + \ell_g(B) \leq p + 1$ for some nonzero $g \in \mathbb{Z}/p\mathbb{Z}$. In such a case, $A \subseteq a_0 + [0, m]_g$ and $B \subseteq b_0 + [0, n]_g$ with $m + n = \ell_g(A) + \ell_g(B) - 2 \leq p - 1$, for some a_0, $b_0 \in \mathbb{Z}/p\mathbb{Z}$, in which case the maps $a_0 + sg \mapsto s$ and $b_0 + tg \mapsto t$, for s, $t \in \mathbb{Z}$, when restricted to A and B, respectively, show that the sumset $A + B$ is Freiman isomorphic (see

[12, Section 2.8]) to an integer sumset. This allows us to canonically apply results from $\mathbb{Z}$ to the sumset $A+B$.

If G is an abelian group and $A, B \subseteq G$ are subsets, then we say that A is *saturated* with respect to B, if $(A \cup \{x\}) + B \neq A + B$ for all $x \in \overline{A}$. In the proof of Theorem 2.1, we shall also use the following basic result regarding saturation [12, Lemma 7.2], whose earlier form dates back to Vosper [21]. We include the short proof for completeness.

LEMMA 2.3. — *Let G be an abelian group and let $A, B \subseteq G$ be subsets. Then*

$$-B + \overline{A+B} \subseteq \overline{A}$$

with equality holding if and only if A is saturated with respect to B.

Proof. — First observe that $-B + \overline{A+B} \subseteq \overline{A}$, for if $b \in B$, $z \in \overline{A+B}$, and by contradiction $-b+z = a$ for some $a \in A$, then $z = a+b \in A+B$, contrary to its definition. If A is saturated with respect to B, then given any $x \in \overline{A}$, there exists some $b \in B$ and $z \in \overline{A+B}$ with $x+b = z$, whence $x = -b+z \in -B+\overline{A+B}$. This shows that $\overline{A} \subseteq -B+\overline{A+B}$, and as the reverse inclusion always holds (as was just shown), it follows that $\overline{A} = -B + \overline{A+B}$. Conversely, if $\overline{A} = -B+\overline{A+B}$, then given any $x \in \overline{A}$, there exists some $b \in B$ and $z \in \overline{A+B}$ with $x = -b+z$, implying $x+b = z \notin A+B$. Since $x \in \overline{A}$ is arbitrary, this shows that A is saturated with respect to B. □

Proof of Theorem 2.1. — Let $f(x) = 4x^3 + (12-4\varepsilon)x^2 + (9-4\varepsilon)x + (8\varepsilon - 7)$, so that $f'(x) = 12x^2 + (24-8\varepsilon)x + (9-4\varepsilon)$. Then $f'(x) > 0$ for $x \geq 0$ (in view of $\varepsilon \leq 3/4$), meaning that $f(x)$ is an increasing function for $x \geq 0$ with $f(0) = 8\varepsilon - 7 < 0$ and $f(1/2) = 1 + 5\varepsilon > 0$. Consequently, $f(x)$ has a unique positive root $0 < \alpha < \frac{1}{2}$.

Since $|2A| \leq \varepsilon p < p$, the Cauchy–Davenport theorem implies $r \geq -1$. Let

$$\beta = \frac{r+3}{|A|} > 0, \tag{2}$$

so that

$$r = \beta|A| - 3, \quad |2A| = 2|A| + r = (2+\beta)|A| - 3 \quad \text{and} \quad \beta \leq \alpha < \frac{1}{2}. \tag{3}$$

Since $2|A| + r = |2A| \leq \varepsilon p \leq \frac{3}{4}p$, it follows that $|A| \leq \frac{3}{8}p - \frac{1}{2}r$, and since $r \geq -1$, we deduce that

$$|A| \leq \frac{3p+4}{8}. \tag{4}$$

The proof naturally breaks into two parts: a first case where there is a large rectifiable subsumset and a second case where there is not. The latter case will lead to a contradiction.

Case 1. — Suppose there exist subsets $A' \subseteq A$ and $B' \subseteq A$ with $|B'| \le |A'|$ and

$$|A'| + 2|B'| - 4 \ge |2A| \tag{5}$$

such that $A' + B'$ is rectifiable. Furthermore, choose a pair of subsets $A' \subseteq A$ and $B' \subseteq A$ with these properties, such that $|A'|+|B'|$ is maximal, and for these subsets A' and B', let $g \in \mathbb{Z}/p\mathbb{Z}$ be a nonzero difference with $\ell_g(A') + \ell_g(B') \le p+1$ minimal. Note that $|A'| \ge |B'| \ge 2$; indeed, if $|B'| \le 1$, then combining this with the hypotheses $|B'| \le |A'| \le |A|$ and (5) yields the contradiction $|A| - 2 \ge |2A| \ge |A|$. Since $A' + B'$ is rectifiable, the Cauchy–Davenport theorem for $\mathbb{Z}$ [12, Theorem 3.1] ensures

$$|A' + B'| = |A'| + |B'| + r' \quad \text{with } r' \ge -1.$$

Moreover, we have

$$\begin{aligned} &A' \subseteq P_A := a_0 + [0,m]_g, \quad B' \subseteq P_B := b_0 + [0,n]_g, \quad \text{and} \\ &A' + B' \subseteq a_0 + b_0 + [0, m+n]_g, \end{aligned} \tag{6}$$

with $a_0,\, a_0 + mg \in A'$, $b_0,\, b_0 + ng \in B'$ and $m + n \le p - 1$, for some $a_0,\, b_0 \in \mathbb{Z}/p\mathbb{Z}$. Then, since $A' + B'$ is rectifiable, it follows that the map $\psi : \mathbb{Z}/p\mathbb{Z} \to [0, p-1] \subseteq \mathbb{Z}$ defined by $\psi(sg) = s$ for $s \in [0, p-1]$ gives a Freiman isomorphism of $A'+B'$ with the integer sumset $\psi(-a_0+A')+\psi(-b_0+B') \subseteq \mathbb{Z}$. Observe that

$$\gcd^*(\psi(-a_0 + A') + \psi(-b_0 + B')) = 1,$$

since if $\psi(-a_0+A')+\psi(-b_0+B')$ were contained in an arithmetic progression with difference $d \ge 2$, then this would also be the case for $\psi(-a_0 + A')$ and $\psi(-b_0+B')$, and then $\ell_{dg}(A')+\ell_{dg}(B') < \ell_g(A')+\ell_g(B')$ would follow in view of $|A'| \ge |B'| \ge 2$, contradicting the minimality of $\ell_g(A') + \ell_g(B')$ for g.

In view of (5) and $|B'| \le |A'|$, we have $|A' + B'| \le |2A| \le |A'| + |B'| + \min\{|A'|, |B'|\} - 4$. Thus, since $\gcd^*(\psi(-a_0 + A') + \psi(-b_0 + B')) = 1$, we can apply the $3k-4$ theorem (Theorem 2.2) to the isomorphic sumset $\psi(-a_0 + A') + \psi(-b_0 + B')$. Then, letting $P_A = a_0 + [0,m]_g$, $P_B = b_0 + [0,n]_g$ and letting $P_{A+B} \subseteq A' + B'$ be the resulting arithmetic progressions with common difference g, we conclude that

$$|P_A \setminus A'| \le r' + 1 \quad \text{und} \quad |P_B \setminus B'| \le r' + 1. \tag{7}$$

If $A' = A$ and $B' = A$, then the original sumset $2A$ is rectifiable, we have $r' = r$, and the theorem follows with $P_A = P_B$ and $P_{2A} = P_{A+B}$ as just defined. Therefore, we can assume otherwise, which in view of $|B'| \le |A'|$ means

$$A \setminus B' \ne \emptyset. \tag{8}$$

Let $\Delta = |2A| - |A' + B'| \geq 0$. Then

$$r' = |A \setminus A'| + |A \setminus B'| + r - \Delta. \tag{9}$$

Since $|A'| + |B'| + r' = |A' + B'| = |2A| - \Delta$, it follows from (5) and $|B'| \leq |A'|$ that

$$r' \leq |B'| - 4 - \Delta \quad \text{and} \quad r' \leq |A'| - 4 - \Delta. \tag{10}$$

Averaging both bounds in (10), using (9), and recalling that $|2A| = 2|A| + r$, we obtain

$$r' \leq \frac{1}{3}|2A| - \frac{8}{3} - \Delta. \tag{11}$$

Step A. — $|-A' + \overline{A' + A}| \leq |\overline{A' + A}| + 2|A'| - 4$.

Proof. — If Step A fails, then combining its failure with $p - |2A| = |\overline{2A}| \leq |\overline{A' + A}|$ and Lemma 2.3 yields

$$p - |2A| + 2|A'| - 3 \leq |\overline{A' + A}| + 2|A'| - 3 \leq |-A' + \overline{A' + A}| \leq |\overline{A}| = p - |A|,$$

which implies that $|A| + 2|A'| - 3 \leq |2A|$. This together with (5) and $|B'| \leq |A'| \leq |A|$ implies $|A| + 2|A'| - 3 \leq |A'| + 2|B'| - 4 \leq |A| + 2|A'| - 4$, which is not possible. □

Step B. — $|-A' + \overline{A' + A}| \leq |A'| + 2|\overline{A' + A}| - 3$.

Proof. — If Step B fails, then combining its failure with $2p - 4|A| - 2r = 2|\overline{2A}| \leq 2|\overline{A' + A}|$ and Lemma 2.3 yields

$$\begin{aligned} |A'| + 2p - 4|A| - 2r - 2 &\leq |A'| + 2|\overline{A' + A}| - 2 \\ &\leq |-A' + \overline{A' + A}| \leq |\overline{A}| = p - |A|. \end{aligned}$$

Collecting terms in the above inequality, multiplying by 2, and applying the estimates $|B'| \leq |A'|$ and (11) yields

$$\begin{aligned} 2p &\leq 6|A| + 4r - 2|A'| + 4 \leq 3|2A| + r - |A'| - |B'| + 4 \\ &= 3|2A| - |A' + B'| + r + r' + 4 = 2|2A| + \Delta + r + r' + 4 \\ &\leq \frac{7}{3}|2A| + r + \frac{4}{3}. \end{aligned}$$

Hence, $|2A| \geq \frac{6}{7}p - \frac{3}{7}r - \frac{4}{7}$. Combined with (3) and (4), we conclude that

$$\frac{6}{7}p - \frac{3}{7}\alpha\Big(\frac{3p+5}{8}\Big) + \frac{5}{7} < \frac{6}{7}p - \frac{3}{7}\beta|A| + \frac{5}{7} = \frac{6}{7}p - \frac{3}{7}r - \frac{4}{7} \leq |2A| \leq \varepsilon p \leq \frac{3}{4}p,$$

which yields the contradiction $0 < (\frac{6}{7} - \frac{3}{4} - \frac{9}{56}\alpha)p < \frac{15}{56}\alpha - \frac{5}{7} < 0$ (in view of $\alpha < \frac{1}{2}$), completing Step B. □

By our application of the $3k-4$ theorem (Theorem 2.2) to $\psi(-a_0+A')+\psi(-b_0+B')$, we know that $A'+B'$ contains an arithmetic progression P_{A+B} with difference g and length $|P_{A+B}| \geq |A'|+|B'|-1$, which implies

$$\ell_g(\overline{A'+B'}) \leq p-|A'|-|B'|+1.$$

By (7) and (10), we obtain

$$\ell_g(-A') = \ell_g(A') \leq |A'|+r'+1 \leq |A'|+|B'|-3, \tag{12}$$

whence $\ell_g(-A')+\ell_g(\overline{A'+B'}) \leq p-2$, ensuring that $-A'+\overline{A'+B'}$ is rectifiable via the difference g. Since $\overline{A'+A} \subseteq \overline{A'+B'}$, it follows that $-A'+\overline{A'+A}$ is also rectifiable via the difference g.

By our application of the $3k-4$ theorem (Theorem 2.2) to $\psi(-a_0+A')+\psi(-b_0+B')$ we know that $\psi(-a_0+A')$ is contained in the arithmetic progression $\psi(-a_0+P_A)=[0,m]$ with difference 1 and length $|P_A| \leq |A'|+r'+1$, with the latter inequality by (7). Moreover, $r'+1 \leq |B'|-3 \leq |A'|-3$ (by (10)), so that $|A'| > \lceil \frac{1}{2}|P_A| \rceil$, meaning that $\psi(-a_0+A')$ must contain at least two consecutive elements. Hence,

$$\gcd^*(\psi(-a_0+A')) = 1. \tag{13}$$

Since $-A'+\overline{A'+A}$ is rectifiable via the difference g, it is then isomorphic to the integer sumset $\psi(a_0+mg-A')+\psi(x+\overline{A'+A})$ for an appropriate $x \in \mathbb{Z}/p\mathbb{Z}$. Hence, in view of (13), Step A, and Step B, we can apply the $3k-4$ theorem (Theorem 2.2) to the isomorphic sumset $\psi(a_0+mg-A')+\psi(x+\overline{A'+A})$ and thereby conclude that there is an arithmetic progression $P \subseteq -A'+\overline{A'+A}$ with difference g and length $|P| \geq |A'|+|\overline{A'+A}|-1 \geq |A'|+|\overline{2A}|-1 = p-|2A|+|A'|-1$. Consequently, since Lemma 2.3 ensures that $P \subseteq -A'+\overline{A'+A} \subseteq \overline{A}$, it follows that $\ell_g(A) \leq |2A|-|A'|+1$. Combined with (12), we find that

$$\ell_g(A')+\ell_g(A) \leq |2A|+r'+2. \tag{14}$$

If $A'+A$ is not rectifiable, then $\ell_g(A')+\ell_g(A) \geq p+2$, and, hence, by (11) and (14) we have $p \leq |2A|+r' \leq \frac{4}{3}|2A|-\frac{8}{3}$, whence $|2A| \geq \frac{3}{4}p+2 > \varepsilon p$, contrary to the hypothesis. Therefore, $A'+A$ is rectifiable. This contradicts the maximality of $|A'|+|B'|$, since by (8) we have $|A| > |B'|$, which completes Case 1.

Case 2. — Every pair of subsets $A' \subseteq A$ and $B' \subseteq A$ with $|B'| \leq |A'|$, whose sumset $A'+B'$ is rectifiable, has

$$|A'|+2|B'| \leq |2A|+3. \tag{15}$$

Let $\ell := |2A| = 2|A|+r$. For the rest of this proof, let us identify $\mathbb{Z}/p\mathbb{Z}$ with the set of integers $[0,p-1]$ with addition mod p. Then, for every $X \subseteq \mathbb{Z}/p\mathbb{Z}$ and $d \in \mathbb{Z}/p\mathbb{Z}$, we define the exponential sum $S_X(d) = \sum_{x \in X} e^{\frac{2\pi i}{p}dx} \in \mathbb{C}$.

The idea is to use Freiman's estimate [13, Theorem 1] for such sums to show that the assumption (15) implies

$$|S_A(d)| \le \tfrac{1}{3}|A| + \tfrac{2}{3}r + 2 \quad \text{for all nonzero } \ d \in \mathbb{Z}/p\mathbb{Z}. \tag{16}$$

For any $u \in [0, 2\pi)$, consider the open arc $C_u = \{e^{ix} : \ x \in (u, u+\pi)\}$ of length π in the unit circle in $\mathbb{C}$. Let $A' = \{x \in A : e^{\frac{2\pi i}{p}dx} \in C_u\}$. Since the set of p-th roots of unity contained in C_u correspond to an arithmetic progression of difference 1 in $\mathbb{Z}/p\mathbb{Z}$, it is clear that for d^*, the multiplicative inverse of d modulo p, we have $\ell_{d^*}(A') \le \frac{p+1}{2}$. Hence, the sumset $A' + A'$ is rectifiable. Then the assumption (15) implies that $3|A'| \le |2A| + 3$. This shows that every open half-arc of the unit circle contains at most $n = \frac{1}{3}|2A| + 1$ of the $|A|$ terms involved in the sum $S_A(d)$. By [13, Theorem 1] applied with this n, $N = |A|$, and $\varphi = \pi$, we obtain $|S_A(d)| \le 2n - N = \frac{2}{3}|2A| + 2 - |A|$, and (16) follows.

To complete the proof, we now exploit (16) to obtain a contradiction, using in particular the following manipulations, which are standard in the additive combinatorial use of Fourier analysis (e.g. [12, pp. 290–291])

By Fourier inversion and the fact that $S_A(0) = |A|$ and $S_{2A}(0) = \ell$, we have

$$\begin{aligned}
|A|^2 p &= \sum_{x \in \mathbb{Z}/p\mathbb{Z}} S_A(x) S_A(x) \overline{S_{2A}(x)} \\
&= S_A(0) S_A(0) \overline{S_{2A}(0)} + \sum_{x \in (\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}} S_A(x) S_A(x) \overline{S_{2A}(x)} \\
&= |A|^2 \ell + \sum_{x \in (\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}} S_A(x) S_A(x) \overline{S_{2A}(x)} \\
&\le |A|^2 \ell + \sum_{x \in (\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}} |S_A(x)||S_A(x)||S_{2A}(x)| \\
&\le |A|^2 \ell + (\tfrac{1}{3}|A| + \tfrac{2}{3}r + 2) \sum_{x \in (\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}} |S_A(x)||S_{2A}(x)|.
\end{aligned}$$

This last sum is at most $\big(\sum_{x \in \mathbb{Z}/p\mathbb{Z} \setminus \{0\}} |S_A(x)|^2\big)^{1/2} \big(\sum_{x \in \mathbb{Z}/p\mathbb{Z} \setminus \{0\}} |S_{2A}(x)|^2\big)^{1/2}$ by the Cauchy–Schwarz inequality. We thus conclude that

$$|A|^2 p \le |A|^2 \ell + \frac{|A| + 2r + 6}{3} (|A|p - |A|^2)^{1/2} (\ell p - \ell^2)^{1/2}.$$

Rearranging this inequality, we obtain

$$\frac{|A| + 2r + 6}{3|A|} \ge \frac{|A|(p-\ell)}{|A|^{1/2}(p-|A|)^{1/2} \ell^{1/2} (p-\ell)^{1/2}} = \left(\frac{\frac{p}{\ell} - 1}{\frac{p}{|A|} - 1} \right)^{1/2}. \tag{17}$$

By hypothesis $r = \beta|A| - 3$ and $\ell = |2A| = (2+\beta)|A| - 3$, so $|A| = \frac{\ell+3}{2+\beta} > \frac{\ell}{2+\beta}$. Using these estimates in (17) yields

$$\frac{1+2\beta}{3} = \frac{|A| + 2(\beta|A| - 3) + 6}{3|A|} = \frac{|A| + 2r + 6}{3|A|}$$
$$\geq \left(\frac{\frac{p}{\ell} - 1}{\frac{p}{|A|} - 1}\right)^{1/2} > \left(\frac{\frac{p}{\ell} - 1}{(2+\beta)\frac{p}{\ell} - 1}\right)^{1/2}.$$

Rearranging the above inequality yields (in view of $0 < \beta \leq \alpha < 1$)

$$\varepsilon p \geq \ell > \frac{1 - (\frac{1+2\beta}{3})^2(2+\beta)}{1 - (\frac{1+2\beta}{3})^2} p. \tag{18}$$

Since $\beta \leq \alpha < 1$, rearranging the above inequality yields

$$4\beta^3 + (12 - 4\varepsilon)\beta^2 + (9 - 4\varepsilon)\beta + 8\varepsilon - 7 > 0. \tag{19}$$

Thus, $f(\beta) > 0$, with $f(x) = 4x^3 + (12 - 4\varepsilon)x^2 + (9 - 4\varepsilon)x + 8\varepsilon - 7$. As noted at the start of the proof, $f(x)$ is increasing for $x \geq 0$ with a unique positive root α. As a result, (19) ensures that $\beta > \alpha$, which is contrary to the hypothesis, completing the proof. □

Remark 2.4. — Our restriction $|2A| \leq \frac{3}{4}p$ in Theorem 2.1 could be relaxed somewhat further, but at increasingly greater cost to the resulting constant α. One simply needs to strengthen the hypothesis of (5) and appropriately adjust the Fourier analytic calculation in Case 2 in the above proof, using the correspondingly weakened inequality for (15).

Proof of Theorem 1.3. — As mentioned earlier, Theorem 1.3 is just the special case of Theorem 2.1 with $\varepsilon = \frac{3}{4}$. □

We now proceed to prove the variant that we shall apply in the next section.

Proof of Theorem 1.4. — The proof is very close to that of Theorem 2.1, with the most significant difference occurring in Case 2. We only highlight the few differences in the argument.

First observe that, if $p = 2$, then $|2A| < p$ forces $|A| = 1$, in which case, the theorem holds trivially. Therefore, we can assume $p \geq 3$. Next, observe (via Taylor series expansion) that $p\sin(\pi/p)$ is an increasing function for $p > 1$ with limit π. The function $\eta/\sin(\pi\eta/3)$ is also an increasing function for $\eta \in (0, 1)$. Thus, $\alpha \leq -\frac{5}{4} + \frac{1}{4}\sqrt{9 + 8\pi/\sin(\pi/3)} < 0.3$. By hypothesis, $|A| \leq \frac{p-r}{3} = \frac{1}{3}p - \frac{1}{3}\beta|A| + 1$, implying

$$|A| \leq \frac{p+3}{\beta+3} < \frac{p+3}{3}, \tag{20}$$

which replaces (4) for the proof. Also, $|2A| = 2|A| + r \leq 2(\frac{p-r}{3}) + r = \frac{2p+r}{3}$.

At the end of Step B in Case 1, we instead obtain $\frac{6}{7}p-\frac{3}{7}r-\frac{4}{7} \le |2A| \le \frac{2p+r}{3}$, which implies

$$\frac{2}{3}p \ge \frac{6}{7}p-\frac{16}{21}r-\frac{4}{7} \ge \frac{6}{7}p-\frac{16}{21}\alpha|A|+\frac{16}{7}-\frac{4}{7} > \frac{6}{7}p-\frac{16}{21}\alpha\Big(\frac{p+3}{3}\Big)+\frac{16}{7}-\frac{4}{7},$$

with the final inequality above in view of (20). Thus, $0 < (\frac{6}{7}-\frac{2}{3}-\frac{16}{63}\alpha)p < \frac{16}{21}\alpha-\frac{12}{7} < 0$ (in view of $0<\alpha<0.3$), which is the contradiction that instead completes Step B.

At the end of Case 1, we instead likewise obtain

$$\frac{3}{4}p+2 \le |2A| \le \frac{2p+r}{3} \le \frac{2}{3}p+\frac{1}{3}\alpha|A|-1 < \frac{2}{3}p+\frac{1}{3}\alpha\Big(\frac{p+3}{3}\Big)-1.$$

This yields the contradiction $0 < (\frac{3}{4}-\frac{2}{3}-\frac{\alpha}{9})p < \frac{\alpha}{3}-3 < 0$ (in view of $0<\alpha<0.3$) in order to complete Case 1.

For Case 2, we begin by following the argument that proves (16), except that we use Lev's sharper estimate [13, Theorem 2] instead of [13, Theorem 1]. Thus, using that any two distinct terms in S_A have the shortest arc between them of length at least $\delta = 2\pi/p$, we obtain by [13, Theorem 2] applied with $n = \frac{1}{3}|2A|+1 \le p/2$ (so $\delta n \le \pi$) that for every such nonzero d, we have

$$|S_A(d)| \le \frac{\sin\Big(\big(\frac{1}{3}|2A|+1-\frac{1}{2}|A|\big)\frac{2\pi}{p}\Big)}{\sin(\frac{\pi}{p})} = \frac{\sin\big((\frac{1}{3}|A|+\frac{2}{3}r+2)\frac{\pi}{p}\big)}{\sin(\frac{\pi}{p})}. \tag{21}$$

Let $M = \frac{1}{3}|A|+\frac{2}{3}r+2$ and let $y = M/p$. Note $M \le (\frac{1}{3}+\frac{2}{3}\alpha)|A| < (\frac{1}{3}+\frac{2}{3}(0.3))\frac{p+3}{3} < \frac{p}{2}$ in view of $r \le \alpha|A|-3$ and (20), ensuring $y \in (\frac{\eta}{3},\frac{1}{2})$. Then the inequality in (21) becomes $|S_A(d)| \le \frac{\sin(y\pi)}{yp\sin(\frac{\pi}{p})}\,M$. The function $f(p,y) = \frac{\sin(y\pi)}{yp\sin(\frac{\pi}{p})}$ is decreasing in $y \in (0,1/2)$ for any fixed $p \ge 3$, as can be seen by considering the Taylor series expansion of its partial derivative. It is also decreasing in p for every fixed $y \in (0,1/2)$ by a similar analysis. Letting $\gamma = f(p,\frac{\eta}{3}) > 0$, we can, therefore, replace (16) by the bound

$$|S_A(d)| \le \gamma(\tfrac{1}{3}|A|+\tfrac{2}{3}r+2). \tag{22}$$

Since $M\frac{\pi}{p} < \frac{\pi}{2}$, $M>1$ and $p \ge 3$, it follows that $\sin(M\frac{\pi}{p}) - M\sin(\frac{\pi}{p}) \le 0$ (as can be seen by considering derivatives with respect to M and using the Taylor series expansion of $\tan(\frac{\pi}{p})$ to note $\tan(\frac{\pi}{p}) > \frac{\pi}{p}$). Consequently, we see that the bound in (21) is at most M, ensuring $\gamma \le 1$. We now obtain the following inequality instead of (17):

$$\begin{aligned}\gamma\frac{1+2\beta}{3} &= \frac{\gamma(\frac{1}{3}|A|+\frac{2}{3}r+2)}{|A|} \\ &\ge \frac{|A|(p-\ell)}{|A|^{1/2}(p-|A|)^{1/2}\ell^{1/2}(p-\ell)^{1/2}} = \left(\frac{\frac{p}{\ell}-1}{\frac{p}{|A|}-1}\right)^{1/2}.\end{aligned} \tag{23}$$

A similar rearrangement to the one that yielded (18) now leads to

$$\frac{2p+\frac{\beta}{3+\beta}(p+3)-3}{3} \geq \frac{2p+\beta|A|-3}{3} = \frac{2p+r}{3} \geq |2A| > \frac{1-\gamma^2(\frac{1+2\beta}{3})^2(2+\beta)}{1-\gamma^2(\frac{1+2\beta}{3})^2}p, \tag{24}$$

with the first inequality following from (20). Since $0 \leq \beta < 1$ and $0 < \gamma \leq 1$, we have $\frac{\beta}{3+\beta} < 1$ and also $1-\gamma^2(\frac{1+2\beta}{3})^2 > 0$, so (24) implies $\big(\frac{\beta+2}{\beta+3}\big)\big(1-\gamma^2\big(\frac{1+2\beta}{3}\big)^2\big) > 1-\gamma^2\big(\frac{1+2\beta}{3}\big)^2(2+\beta)$. Multiplying both sides by $\beta+3>0$ and grouping on the left-hand side the terms involving γ, we obtain $(\beta+2)^2\gamma^2\big(\frac{1+2\beta}{3}\big)^2 > 1$. Taking square roots and expanding, we deduce $2\beta^2+5\beta+2-3\gamma^{-1} > 0$. The quadratic formula thus implies that either $\beta < \frac{-5-\sqrt{9+24\gamma^{-1}}}{4} < 0$ or $\beta > \frac{-5+\sqrt{9+24\gamma^{-1}}}{4} = \alpha$. Since $\beta > 0$, this contradicts the hypothesis $\beta \leq \alpha$, completing the proof. □

3. Bounds for m-sum-free sets in $\mathbb{Z}/p\mathbb{Z}$

In this section, we give new bounds for the quantity $d_m(\mathbb{Z}/p\mathbb{Z})$ defined in formula (1) and for the associated limit

$$d_m = \lim_{\substack{p\to\infty \\ p \text{ prime}}} d_m(\mathbb{Z}/p\mathbb{Z}).$$

In Section 3.1, we present some examples of large m-sum-free sets and in Section 3.2, we apply Theorem 1.4 to give a new upper bound for $d_m(\mathbb{Z}/p\mathbb{Z})$. In Section 3.3 we obtain an improvement of Theorem 1.8.

3.1. Lower bounds for $d_m(\mathbb{Z}/p\mathbb{Z})$. — As mentioned in the Introduction, a simple example of a large m-sum-free set is the interval $(\frac{2}{m^2-4}p, \frac{m}{m^2-4}p)$, having the asymptotic density $\frac{1}{m+2}$ as $p\to\infty$. This gives the largest known size of m-sum-free sets for $m \leq 6$ but not for greater values of m. Indeed, there is the following construction, following an idea due to Tomasz Schoen. The version given below incorporates a suggestion of the anonymous referee that, with some additional modification, yielded the result as stated below. As noted in the proof, for fixed m, the constant $\frac{1}{8}$ can be improved by a small factor tending to 0 as $m\to\infty$.

LEMMA 3.1. — *For each integer $m \geq 7$, we have $d_m(\mathbb{Z}/p\mathbb{Z}) \geq \frac{1}{8}(1-\frac{1}{p})$ for every prime p of the form $p = 4m^2n+1$. In particular, $d_m \geq \frac{1}{8}$.*

Proof. — We identify $\mathbb{Z}/p\mathbb{Z}$ with the interval of integers $[0, p-1]$ with addition mod p. Let $\lambda \in [3, m]$ and $\mu \in [0, m-1]$ be integer parameters to be fixed later

and consider the interval

$$J = \{4mn + 1, 4mn + 2, \dots, 2\lambda mn\} \subset [0, p - 1].$$

We define an m-sum-free set A by picking elements from J in appropriate congruence classes mod m:

$$A := \{x \in J : x \bmod m \in [0, \mu]\}.$$

Note that the sumset $A + A$ taken in $\mathbb{Z}$ is a subset of $[0, p - 1]$ because $\lambda \leq m$ guarantees $2 \max A = 4mn\lambda \leq 4m^2 n = p - 1$. We therefore have $y \in 2A \Rightarrow y \bmod m \in [0, 2\mu]$.

Now,

$$\begin{aligned} J &= \bigcup_{i=1}^{\lceil \frac{\lambda}{2} \rceil - 2} [(4i)mn + 1, 4(i + 1)mn] \cup [(4(\lceil \tfrac{\lambda}{2} \rceil - 1)mn + 1, 2\lambda mn] \\ &\subseteq \bigcup_{i=1}^{\lceil \frac{\lambda}{2} \rceil - 1} [(4i)mn + 1, 4(i + 1)mn]. \end{aligned}$$

Since $p = 4m^2 n + 1$, we have $m \cdot [(4i)mn + 1, 4(i + 1)mn] = \{m - i, 2m - i, \dots, 4m^2 n - i\}$ for $i \in [1, \lceil \frac{\lambda}{2} \rceil - 1]$, meaning that $m \cdot J$ is covered by the progressions

$$U_i = \{m - i, 2m - i, \dots, 4m^2 n - i\}, \quad i \in [1, \lceil \tfrac{\lambda}{2} \rceil - 1].$$

For A to be m-sum-free it suffices to ensure that $2A \cap (m \cdot J) = \emptyset$, and for this, it suffices for λ and μ to satisfy $2\mu \leq m - (\lceil \frac{\lambda}{2} \rceil - 1) - 1$, that is,

$$2\mu + \lceil \tfrac{\lambda}{2} \rceil \leq m.$$

We also have $|A| = (\mu + 1) \frac{|J|}{m} = 2n(\mu + 1)(\lambda - 2)$, so

$$\frac{|A|}{p - 1} = \frac{(\mu + 1)(\lambda - 2)}{2m^2}.$$

Suppose $m \equiv 0 \bmod 4$, so $m \geq 8$. Considering $\lambda = m$ and $\mu = \frac{m}{4}$ yields $\frac{|A|}{p-1} = \frac{(\mu+1)(\lambda-2)}{2m^2} = \frac{m^2+2m-8}{8m^2}$, which is at least $\frac{1}{8}$ for $m \geq 4$.

Suppose $m \equiv 1 \bmod 4$, so $m \geq 9$. Considering $\lambda = m$ and $\mu = \frac{m-1}{4}$ yields $\frac{|A|}{p-1} = \frac{(\mu+1)(\lambda-2)}{2m^2} = \frac{m^2+m-6}{8m^2}$, which is at least $\frac{1}{8}$ for $m \geq 6$. We remark that taking $\lambda = m - 3$ and $\mu = \frac{m+3}{4}$ instead yields $\frac{|A|}{p-1} = \frac{(\mu+1)(\lambda-2)}{2m^2} = \frac{m^2+2m-35}{8m^2}$, which is slightly better for larger values of m.

Suppose $m \equiv 2 \bmod 4$, so $m \geq 10$. In this case, we will modify the above construction with $\lambda = m - 1$ and $\mu = \frac{m-2}{4}$. For these parameters, we have

$\lceil \frac{\lambda}{2} \rceil - 1 = \frac{m-2}{2}$, $2(\mu+1) = \frac{m+2}{2} = m - \frac{m-2}{2}$, and

$$m \cdot [(4(\lceil \tfrac{\lambda}{2} \rceil - 1)mn + 1, 2\lambda mn] = m \cdot [2(m-2)mn + 1, 2(m-1)mn]$$
$$= \{m - \tfrac{m-2}{2}, 2m - \tfrac{m-2}{2}, \dots, 2m^2 n - \tfrac{m-2}{2}\}, \tag{25}$$

which is the subset of $m \cdot J \subseteq [0, p-1]$ congruent to $m - \frac{m-2}{2}$ modulo m. Let $B = \{tm + \frac{m+2}{4} : \ mn \le t \le 2(m-1)n - 1\}$ and set $A' = A \cup B$. Since $mn \le t \le 2(m-1)n-1$, we have $B \subseteq J$, while $2B = \{2m^2 n + m - \frac{m-2}{2}, 2m^2 n + 2m - \frac{m-2}{2}, \dots, 4(m-1)mn - m - \frac{m-2}{2}\}$, which is disjoint from the set in (25). Since $A + B$ is also disjoint from $m \cdot J$, it follows that $2A' \cap (m \cdot J) = \emptyset$, so A' is m-sum-free. We have $\frac{|A'|}{p-1} = \frac{|A|+|B|}{p-1} = \frac{2n(\mu+1)(\lambda-2)+(m-2)n}{p-1} = \frac{m^2+m-10}{8m^2}$, which is at least $\frac{1}{8}$ for $m \ge 10$. We remark that taking $\lambda = m-2$ and $\mu = \frac{m+2}{4}$ in the original construction instead yields $\frac{|A|}{p-1} = \frac{(\mu+1)(\lambda-2)}{2m^2} = \frac{m^2+2m-24}{8m^2}$, which is slightly better for larger values of m.

Suppose $m \equiv 3 \bmod 4$, so $m \ge 7$. We modify the original construction with $\lambda = m$ and $\mu = \frac{m-3}{4}$. For these parameters, we have $\lceil \frac{\lambda}{2} \rceil - 1 = \frac{m-1}{2}$, $2(\mu+1) = \frac{m+1}{2} = m - \frac{m-1}{2}$, and

$$m \cdot [(4(\lceil \tfrac{\lambda}{2} \rceil - 1)mn + 1, 2\lambda mn] = m \cdot [2(m-1)mn + 1, 2m^2 n]$$
$$= \{m - \tfrac{m-1}{2}, 2m - \tfrac{m-1}{2}, \dots, 2m^2 n - \tfrac{m-1}{2}\},$$

which is the subset of $m \cdot J \subseteq [0, p-1]$ congruent to $m - \frac{m-1}{2}$ modulo m. Let $B = \{tm + \frac{m+1}{4} : \ mn \le t \le 2mn - 1\}$ and set $A' = A \cup B$. Since $mn \le t \le 2mn-1$, we have $B \subseteq J$, while $2B = \{2m^2 n + m - \frac{m-1}{2}, 2m^2 n + 2m - \frac{m-1}{2}, \dots, 4m^2 n - m - \frac{m-1}{2}\}$. Thus, similarly to the previous case, $2A' \cap (m \cdot J) = \emptyset$, so A' is m-sum-free. We have $\frac{|A'|}{p-1} = \frac{|A|+|B|}{p-1} = \frac{2n(\mu+1)(\lambda-2)+mn}{p-1} = \frac{m^2+m-2}{8m^2}$, which is at least $\frac{1}{8}$ for $m \ge 2$. We remark that taking $\lambda = m-1$ and $\mu = \frac{m+1}{4}$ in the original construction instead yields $\frac{|A|}{p-1} = \frac{(\mu+1)(\lambda-2)}{2m^2} = \frac{m^2+2m-15}{8m^2}$, which is slightly better for larger m.

In all four cases above, we obtain a set A, such that $d_m(\mathbb{Z}/p\mathbb{Z}) \ge \frac{|A|}{p} \ge \frac{|A|}{p-1}(1 - \frac{1}{p}) \ge \frac{1}{8}(1 - \frac{1}{p})$, and now the claim about the limit follows from the fact that by Dirichlet's theorem there exist infinitely many primes in the arithmetic progression $\{4m^2 n + 1 : n \ge 1\}$. □

3.2. Upper bound for $d_m(\mathbb{Z}/p\mathbb{Z})$. — In this section we prove Theorem 1.5, which we restate here for convenience.

THEOREM 3.2. — *Let $p \ge 80$ be a prime, m be an integer in $[2, p-2]$, and $c = c(p)$ be the solution to the equation $c = \frac{1+3/p}{3+\alpha(c,p)}$, where $\alpha = \alpha(c,p)$ is the parameter in Theorem 1.4 with $\eta = c$. Then, $d_m(\mathbb{Z}/p\mathbb{Z}) < c$. In particular, $d_m \le \frac{1}{3.1955}$.*

The idea of the proof is roughly the following: either an m-sum-free set A has a doubling constant at least $2+\alpha$, in which case, since $(m\cdot A)\cap 2A=\emptyset$, we have $(3+\alpha)|A|\le |(m\cdot A)|+|2A|\le p$ and we are done; or we can apply Theorem 1.4, and thus, working with the two arithmetic progressions provided by the theorem, we reduce the problem essentially to bounding the size that two progressions I and J of equal difference can have if the dilate $m\cdot J$ has small intersection with I. Let us begin by establishing this result about progressions.

LEMMA 3.3. — *Let $p\ge 80$ be prime, $0<\alpha\le 1/5$, $d\in[2,p-2]$, and $N\in\mathbb{N}$. Let I and J be progressions in $\mathbb{Z}/p\mathbb{Z}$ having the same difference and satisfying $|I|=2N-1$, $|J|>(1+\alpha)N-3$, and $|I\cap(d\cdot J)|\le \alpha N-2$. Then, $N<\frac{p+3}{3+\alpha}$.*

Proof. — First note that without loss of generality, we can assume $d\le\frac{p-1}{2}$, since if the lemma is proved with this assumption, then, given $d>\frac{p-1}{2}$, we can multiply by -1 and apply the lemma with the intervals $-I$ and J. Let us proceed by contradiction supposing that there exists some N (along with p, d, α, I, and J), such that the hypotheses of the lemma are satisfied, but $N\ge\frac{p+3}{3+\alpha}$. Note that the supposed properties of I and J are conserved, if we dilate by the inverse of their difference mod p and if we translate, replacing I by $I+dz$ and J by $J+z$. It follows that identifying $\mathbb{Z}/p\mathbb{Z}$ with the integers $[0,p-1]$ with addition mod p, we can assume that $I=[p-|I|,p-1]$ and $J=x+[0,|J|-1]\bmod p$, for some $x\in[0,p-1]$.

We claim that we can assume without loss of generality that

$$d\cdot x\in[0,d-1]\bmod p. \tag{26}$$

Indeed, if this does not hold, then either $d\cdot x\in[d,p-|I|+d-1]\bmod p$ or $d\cdot x\in[p-|I|,p-1]$. If the former holds, then $d\cdot(x-1)\notin I\bmod p$, so the interval $J'=(x-1)+[0,|J|-1]$ satisfies the hypotheses with $|I\cap(d\cdot J')|\le|I\cap(d\cdot J)|$. On the other hand, if $d\cdot x\in[p-|I|,p-1]$, then letting $J'=(x+1)+[0,|J|-1]$ we have $d\cdot x\in I\cap(d\cdot J)$ and $d\cdot x\notin I\cap(d\cdot J')$, so this interval J' satisfies the hypotheses with $|I\cap(d\cdot J')|\le|I\cap(d\cdot J)|$. In either case, by repeatedly shifting the interval J, we eventually obtain (26).

Given (26), we may partition $d\cdot J$ into successive progressions U_i (with difference d) for $i\in[1,s+1]$, such that $U_i=(\min U_i+d\mathbb{Z})\cap[0,p-1]$ with $\min U_i\in[0,d-1]$ for $i\in[1,s]$, and U_{s+1} is either empty or consists of an initial portion of $(\min U_{s+1}+d\mathbb{Z})\cap[0,p-1]$ with $\min U_{s+1}\in[0,d-1]$. Then, $|U_i\cap I|\ge\left\lfloor\frac{|I|}{d}\right\rfloor$ for $i\in[1,s]$. It follows that $|(d\cdot J)\cap I|\ge s\left\lfloor\frac{|I|}{d}\right\rfloor$, whence

$$\alpha N-2\ge s\left\lfloor\frac{|I|}{d}\right\rfloor. \tag{27}$$

Now, as $d\cdot x\in[0,d-1]\bmod p$, each U_i with $i\le s$ starts in $[0,d-1]$ and ends in $[p-d,p-1]$, so s is at least the number of consecutive intervals of length p

that fit inside $[0, |J|d-1]$:

$$s \geq \left\lfloor \frac{|J|d}{p} \right\rfloor > \frac{((1+\alpha)N-3)d}{p} - 1. \tag{28}$$

Substituting this lower bound for s in (27), as well as the bound $\lfloor \frac{|I|}{d} \rfloor \geq \frac{|I|}{d} - \frac{d-1}{d} = \frac{2N}{d} - 1$, and expanding the resulting product, we obtain $\alpha N - 2 > \frac{2(1+\alpha)}{p} N^2 - \big(\frac{(1+\alpha)d}{p} + \frac{6}{p} + \frac{2}{d}\big)N + 1 + \frac{3d}{p}$. We group all terms involving N on the right-hand side, note that the other terms grouped on the left-hand side amount to a negative number, and multiply through by $\frac{p}{2(1+\alpha)N}$ to deduce that

$$N < \frac{1}{2(1+\alpha)} \left(d(1+\alpha) + 6 + \frac{2p}{d} + \alpha p \right). \tag{29}$$

We want to obtain a contradiction from this, using that $N \geq \frac{p+3}{3+\alpha}$. To this end, using the bounds $2 \leq d \leq \frac{p-1}{2}$ on the right-hand side of (29) is not enough. However, we shall now show that we can assume $11 \leq d < p/6$, which will be enough.

First, we claim that $s \geq 1$. Indeed, otherwise $|J| \leq |(d \cdot J) \cap I| + |(d \cdot J) \cap [0, p - |I| - 1]| \leq \alpha N - 2 + \lceil \frac{p-|I|}{d} \rceil$. Using the assumptions on $|I|, |J|$, and $d \geq 2$, we deduce that $N < \frac{p+2d}{d+2} \leq \frac{p}{4} + 2$. This, combined with our assumptions $N \geq (p+3)/(3+\alpha)$ and $\alpha < 1/5$, contradicts $p \geq 80$.

Since $s \geq 1$, (27) yields $\alpha N - 2 \geq \lfloor |I|/d \rfloor \geq \frac{2N}{d} - 1$. It follows that $(\alpha N - 1)d \geq 2N > 0$. Hence, $\alpha N - 1 > 0$ and $d \geq \frac{2N}{\alpha N - 1} > \frac{2}{\alpha}$, whence $d \geq 11$ follows in view of $\alpha \leq \frac{1}{5}$.

Note that $\lfloor |I|/d \rfloor \geq 1$, for otherwise $2N = |I| + 1 < d + 1 \leq \frac{p+1}{2}$, contradicting our assumptions $N \geq \frac{p+3}{3+\alpha}$ and $\alpha \leq 1/5$. Combining this with (27) and (28), we obtain $\alpha N - 2 > \frac{((1+\alpha)N-3)d}{p} - 1$, which means $d \leq \big(\frac{\alpha N - 1}{(1+\alpha)N - 3}\big)p < \frac{\alpha}{1+\alpha} p$. As $\alpha \leq 1/5$, we conclude that $d < p/6$.

Now using the bounds $11 \leq d < p/6$ in (29) and the assumption that $N \geq \frac{p+3}{3+\alpha}$, we deduce that $\frac{p+3}{3+\alpha} < \frac{p}{12} + \frac{p}{11(1+\alpha)} + \frac{\alpha p}{2(1+\alpha)} + \frac{3}{1+\alpha}$, implying $\frac{1}{3.2} < \frac{1}{12} + \frac{1}{11} + \frac{1}{10} + \frac{3}{p}$, contradicting $p \geq 80$. □

Remark 3.4. — It is possible to extend the validity of Lemma 3.3 to all primes $p \geq 5$, at the cost of lengthening the proof with several technicalities. The lemma has potential generalizations that seem of independent interest, although we do not need to pursue them for our purposes in this paper. For instance, the anonymous referee raised the question of which values of coefficients α, β and which functions $f(\alpha, \beta), g(\alpha, \beta) > 0$ ensure that the following statement holds: if I, J are arithmetic progressions in $\mathbb{Z}/p\mathbb{Z}$ with common difference and respective sizes $\alpha N + a$, $\beta N + b$, then $N > f(\alpha, \beta)p$ implies $|I \cap (d \cdot J)| > g(\alpha, \beta)N$.

We can now prove the main result.

Proof of Theorem 3.2. — Let $A \subseteq \mathbb{Z}/p\mathbb{Z}$ be an m-sum-free subset of maximum size, with $|A| = \eta p$, and let $\alpha = \alpha(\eta, p) = -\frac{5}{4} + \frac{1}{4}\sqrt{9 + 8\,\eta\, p \sin(\pi/p)/\sin(\pi\eta/3)}$. Assume by contradiction that $\eta \geq c$. Then, since $x \mapsto \frac{1+3/p}{3+\alpha(x,p)}$ is decreasing in $x \in (0,1)$, and $c = \frac{1+3/p}{3+\alpha(c,p)}$, we deduce that $\eta \geq c \geq \frac{1+3/p}{3+\alpha}$, whence

$$|A| \geq \frac{p+3}{3+\alpha} > 1. \tag{30}$$

As noted at the start of the proof of Theorem 1.4, $\alpha(\eta, p)$ is increasing for $\eta \in (0,1)$ with $p\sin(\pi/p) \to \pi$ monotonically. Since $2A$ and $m \cdot A$ are disjoint, we have $|2A| \leq p - |A|$, while $|2A| \geq 2|A| - 1$ by the Cauchy–Davenport theorem. Thus, $2|A| - 1 \leq |2A| \leq p - |A|$, implying $|A| \leq \frac{p+1}{3}$ and $\eta \leq \frac{p+1}{3p}$. Since $p \geq 80$, we have $\eta \leq \frac{3}{8}$ and $\alpha \leq -\frac{5}{4} + \frac{1}{4}\sqrt{9 + 3\pi/\sin(\pi/8)} < 0.2$.

Let $|2A| = 2|A| + r$. Since A is m-sum-free, the sets $2A$ and $m \cdot A$ are disjoint, which implies that $|2A| < p$ (as A is nonempty) and that $p \geq |2A| + |m \cdot A| = 3|A| + r$. Thus,

$$|A| \leq \frac{p-r}{3} \quad \text{and} \quad |2A| = 2|A| + r \leq \frac{2p+r}{3}.$$

Since $|2A| < p$, the Cauchy–Davenport theorem implies $r \geq -1$.

If $|2A| = 2|A| + r > (2+\alpha)|A| - 3$, then $r > \alpha|A| - 3$, in which case $|A| \leq \frac{p-r}{3} < \frac{p-\alpha|A|+3}{3}$, which contradicts (30). Therefore, $|2A| \leq (2+\alpha)|A| - 3$ and $r \leq \lfloor \alpha|A| - 3 \rfloor$. We can now apply Theorem 1.4. As a result, there are arithmetic progressions P_A and P_{2A} with common difference g such that $A \subseteq P_A$, $P_{2A} \subseteq 2A$, $|P_A| = \lfloor (1+\alpha)|A| - 2 \rfloor \leq p$, and $|P_{2A}| = 2|A| - 1$. It follows that $P := m \cdot P_A$ is an arithmetic progression with difference $mg \neq \pm g$, such that

$$|P \cap P_{2A}| \leq |P \cap 2A| \leq |P_A \setminus A| \leq \alpha|A| - 2.$$

We can, therefore, apply Lemma 3.3 with $N = |A|$ (as $\alpha < 0.2$), deducing that $|A| < \frac{p+3}{3+\alpha}$, which is a contradiction. Therefore, we must have $\eta < c$, so $d_m(\mathbb{Z}/p\mathbb{Z}) < c$, which proves the first claim in the theorem. Taking the limit of c as $p \to \infty$, we deduce that $d_m \leq t$, where t is defined by the equation $t = F(t)$ for the function $F(t) = (\frac{7}{4} + \frac{1}{4}\sqrt{9 + 8\,t\,\pi/\sin(\pi t/3)})^{-1}$. Since F is monotonically decreasing and satisfies $F(3.1955^{-1}) < 3.1955^{-1}$, we must have $t < 3.1955^{-1}$, which proves the second claim in the theorem. □

3.3. The structure of large sum-free sets in $\mathbb{Z}/p\mathbb{Z}$. — In this final part of the paper, we apply Theorem 1.4 to obtain the following improvement of Theorem 1.8.

THEOREM 3.5. — *Let $p \geq 14\,000$ be prime and let $A \subseteq \mathbb{Z}/p\mathbb{Z}$ be sum-free with $|A| \geq (0.313)p$. Then, $m \cdot A \subseteq [\,|A|, p - |A|\,] \subseteq \mathbb{Z}/p\mathbb{Z}$, for some $m \in [1, p-1]$.*

Proof. — By hypothesis, $|A| = \eta p > 0$ with $\eta \geq 0.313$. Set $|2A| = 2|A| + r$. Since A is sum-free, we have $(2A) \cap A = \emptyset$, implying $2|A| + r = |2A| \leq p - |A| < p$, whence $|A| \leq \frac{p-r}{3}$. As in the proof of Theorem 3.2, let $\alpha = \alpha(\eta, p) = -\frac{5}{4} + \frac{1}{4}\sqrt{9 + 8\,\eta\, p \sin(\pi/p)/\sin(\pi\eta/3)}$. Observe that $\alpha(\eta, p)$ is increasing as a function of $p \geq 2$ and $\eta \in (0, 1)$, so $\alpha = \alpha(\eta, p) \geq \alpha(0.313, 14000) \geq \beta := 0.195579$. If $|2A| > (2+\beta)|A| - 3$, then we have $(2+\beta)|A| - 3 < |2A| \leq p - |A|$, implying $(0.313)p \leq |A| < \frac{p+3}{3+\beta}$, and, thus, $p \leq 13\,875$, which is contrary to the hypothesis. Therefore, we instead conclude that $|2A| \leq (2 + \beta)|A| - 3 \leq (2 + \alpha)|A| - 3$, allowing us to apply Theorem 1.4 to conclude that there is an arithmetic progression $P \subseteq \mathbb{Z}/p\mathbb{Z}$ with $A \subseteq P$ and $|P| \leq |A| + r + 1$. By dilating A by the inverse of the difference of the progression P, we can assume without loss of generality that P has difference 1. Since $2|A| + r = |2A| \leq (2+\beta)|A| - 3$, we have $r \leq \beta|A| - 3$, and, thus, $|P| \leq |A| + r + 1 \leq (1 + \beta)|A| - 2$. The bound $|A| \leq (p + 1)/3$ given by the Cauchy–Davenport theorem then implies $|P| \leq (1 + \beta)(p + 1)/3 < \frac{p+1}{2}$. It follows that the sumset $A + A$ is rectifiable.

Let $\psi : A + A \to \mathbb{Z}$ be the associated Freiman isomorphism, with coordinate map $\psi_A : A \to \mathbb{Z}$. Note that the map of the form $a_0 + sg \mapsto s$ involved in the definition of ψ_A (see the remarks before Lemma 2.3) can be assumed to be just a translation (since the element g here, being the difference of P, is assumed to be 1). By slight abuse of notation, we drop the subscript from ψ_A, denoting this map also by ψ. Let $\psi' : A - A \to \mathbb{Z}$ be the Freiman isomorphism defined by $\psi'(x - y) = \psi(x) - \psi(y)$, for $x, y \in A$ (see the remarks after Theorem 2.2). Since $|P| \leq |A| + r + 1 \leq 2|A| - 2$ implies $|A| > \frac{|P|+1}{2}$, we are assured that A contains two consecutive elements in P, whence $\gcd^*(\psi(A)) = 1$. Since A is sum-free, we have $(A - A) \cap A = \emptyset$, and, thus, $|A - A| \leq p - |A|$. Since $A - A \cong \psi(A) - \psi(A)$, we have $|\psi(A) - \psi(A)| = |A - A|$ and $|\psi(A)| = |A|$. As a result, if $|\psi(A) - \psi(A)| \geq 3|\psi(A)| - 3$, then $p - |A| \geq |A - A| = |\psi(A) - \psi(A)| \geq 3|\psi(A)| - 3 = 3|A| - 3$, implying $(0.313)p \leq |A| \leq \frac{p+3}{4}$, contradicting that $p \geq 14\,000$. Therefore, $|\psi(A) - \psi(A)| \leq 3|\psi(A)| - 4$, allowing us to apply the $3k - 4$ theorem (Theorem 2.2) with the sets $\psi(A)$, $-\psi(A)$. This, together with the remarks in the paragraph above Theorem 2.2, implies that $[-(|A|-1), (|A|-1)] \subseteq \psi(A) - \psi(A)$. Hence, $[-(|A|-1), (|A|-1)] \subseteq \psi'(A - A)$ and given the form of ψ', it follows that in $\mathbb{Z}/p\mathbb{Z}$, we have $[-(|A| - 1), (|A| - 1)] \subseteq A - A$. Since A being sum-free implies $(A - A) \cap A = \emptyset$, this forces $A \cap [-(|A|-1), (|A|-1)] = \emptyset$, i.e., $A \subseteq [\,|A|, p - |A|\,]$, which completes the proof. □

Acknowledgements. — The authors are very grateful to Tomasz Schoen for providing the original idea of the construction in Lemma 3.1 and for useful remarks. We also thank the anonymous referee very much for the insightful comments that helped us to improve this paper.

BIBLIOGRAPHY

[1] A. Baltz, P. Hegarty, J. Knape, U. Larsson & T. Schoen – "The structure of maximum subsets of $\{1,\dots,n\}$ with no solutions to $a+b=kc$", *Electron. J. Combin.* (2005), no. 12, Paper No. R19.

[2] P.-Y. Bienvenu, F. Hennecart & I. Shkredov – "A note on the set $A(A+A)$", *Mosc. J. Comb. Number Theory* **8** (2019), no. 2, p. 179–188.

[3] T. F. Bloom – "A quantitative improvement for Roth's theorem on arithmetic progressions", *J. Lond. Math. Soc. (2)* (2016), no. 93, p. 643–663.

[4] P. Candela & A. de Roton – "On sets with small sumset in the circle", *Q. J. Math.* **70** (2019), no. 1, p. 49–69.

[5] P. Candela, O. Serra & C. Spiegel – "A step beyond Freiman's theorem for set addition modulo a prime", *J. Théor. Nombres Bordeaux* **32** (2020), no. 1, p. 275–289.

[6] P. Candela & O. Sisask – "On the asymptotic maximal density of a set avoiding solutions to linear equations modulo a prime", *Acta Math. Hungar.* **132** (2011), no. 3, p. 223–243.

[7] F. R. K. Chung & J. L. Goldwasser – "Maximum subsets of $(0,1]$ with no solutions to $x+y=kz$", *Electron. J. Combin.* (1996), no. 1, p. 3, Research Paper 1.

[8] ———, "Integer sets containing no solutions to $x+y=3z$", in *The Mathematics of Paul Erdős* (R. Graham & J. Nesetřil, eds.), Springer, Berlin, 1997, p. 218–227.

[9] J.-M. Deshouillers & V. F. Lev – "A refined bound for sum-free sets in groups of prime order", *Bull. Lond. Math. Soc.* **40** (2008), no. 5, p. 863–875.

[10] G. Freiman – "Inverse problems in additive number theory. Addition of sets of residues modulo a prime", *Dokl. Akad. Nauk SSSR* **141** (1961), no. 3, p. 571–573.

[11] B. Green & I. Z. Ruzsa – "Sets with small sumset and rectification", *Bull. Lond. Math. Soc. (1)* **38** (2006), p. 43–52.

[12] D. J. Grynkiewicz – *Structural additive theory*, Developments in Mathematics, no. 30, Springer, Cham, 2013.

[13] V. F. Lev – "Distribution of points on arcs", *Integers* **5** (2005), no. 2, electronic.

[14] V. F. Lev & I. Shkredov – "Small doubling in prime-order groups: from 2.4 to 2.6", *J. Number Theory* **217** (2020), p. 278–291.

[15] M. Matolcsi & I. Z. Ruzsa – "Sets with no solutions to $x+y=3z$", *European J. Combin.* **34** (2013), no. 8, p. 1411–1414.

[16] A. Plagne & A. de Roton – "Maximal sets with no solution to $x+y=3z$", *Combinatorica* **36** (2016), no. 2, p. 229–248.

[17] Ø. J. Rødseth – "On Freiman's 2.4-theorem", *Skr. K. Nor. Vidensk. Selsk* (2006), no. 4, p. 11–18.

[18] K. F. Roth – "On certain sets of integers", *J. London Math. Soc.* **28** (1953), p. 104–109.
[19] T. Sanders – "On Roth's theorem on progressions", *Ann. of Math.* **174** (2011), p. 619–636.
[20] O. Serra & G. Zémor – "Large sets with small doubling modulo p are well covered by an arithmetic progression", *Ann. Inst. Fourier (Grenoble)* **59** (2009), no. 5, p. 2043–2060.
[21] G. Vosper – "The critical pairs of subsets of a group of prime order", *J. London Math. Soc.* **31** (1956), p. 200–205.