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

PABLO CANDELA, DIEGO GONZÁLEZ-SÁNCHEZ, AND DAVID J. GRYNKIEWICZ

ABSTRACT. This paper makes progress toward the $3k-4$ conjecture in groups $\mathbb{Z}/p\mathbb{Z}$ for p prime. The conjecture states that if A is a nonempty subset of $\mathbb{Z}/p\mathbb{Z}$ satisfying $2A \neq \mathbb{Z}/p\mathbb{Z}$ and $|2A| = 2|A|+r \leq \min\{3|A|-4,\ p-r-3\}$, 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 a 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 which further improves this bound on r provided A is sufficiently dense. We then apply this 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 of Schoen that yields a lower bound independent of m for this maximal density, of the form $1/8 - o_{m,p\to\infty}(1)$.

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 in 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 [11, 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 [11, 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 [11, 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 [11, 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 $|2A| = 2|A| + r \leq \min\{3|A| - 4,\ p - r - 3\}$. Then there exist arithmetic progressions $P_A, P_{2A} \subseteq \mathbb{Z}/p\mathbb{Z}$ with the same difference such that $A \subseteq P_A$, $|P_A| \leq |A| + r + 1$, $P_{2A} \subseteq 2A$, and $|P_{2A}| \geq 2|A| - 1$.*

Progress toward this conjecture was initiated by Freiman himself, who proved in [9] 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 [14] that the constraint $|A| < p/35$ can be weakened to $|A| < p/10.7$ while maintaining the doubling constant 2.4. In [10], Green and Ruzsa pushed the doubling constant up to 3, at the cost of a stronger constraint $|A| < p/10^{215}$. In [17], 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 [3], where the doubling constant 2.4 in Freiman's result is improved to 2.48 while keeping the hypothesis on $|A|$ markedly less constraining than the one from [10]. The book [11] 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 [17] at the cost of only adding the mild 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*

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

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 [17], 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 $p - r - 3$. However, in the extremal case where $r = |A| - 4$ (the largest value of r allowed in Conjecture 1.2), the conjectured bound implies $3|A| - 4 = |2A| \leq p - |A| + 1$, whence $|A| \leq \frac{p+5}{4}$ and $|2A| = 3|A| - 4 \leq \frac{3p-1}{4}$. Thus, the bound $p - r - 3$ becomes as small as $\frac{3p-1}{4}$ as we *range* over all allowed values for α and $|A|$, making $\frac{3}{4}p$ the optimal bound independent of α and r.

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 $|A| \geq \eta\, p > 0$ 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*

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

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

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 in arithmetic combinatorics, including various types of abelian group settings [1, 6, 7, 8, 13] (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

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

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., 3-term arithmetic progressions) form a translation invariant set. Roth's Theorem [15] 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 [2, 16]). On the other hand, we have the cases $m \geq 3$. 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 which can be modeled on the circle group (see [5]), 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 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 $p \geq 5$ 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, $d_m \leq \frac{1}{3.1955}$.*

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 $m \leq 7$. However, for larger values of m, a construction of Tomasz Schoen (personal communication), presented in this paper in Lemma 3.1 with his kind permission, yields an improved lower bound of the form $d_m \geq \frac{1}{8} - o_{m\to\infty}(1)$. We summarize these results as follows.

Theorem 1.6. *For $m \leq 7$, we have $d_m \geq \frac{1}{m+2}$. For $m \geq 8$, we have $d_m \geq \frac{1}{2m}\lfloor \frac{m}{4} \rfloor$.*

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. There, in Subsection 3.1, we present Schoen's construction and deduce Theorem 1.6. Then, in Subsection 3.2, we apply Theorem 1.4 to obtain Theorem 1.5.

Acknowledgements. We are very grateful to Tomasz Schoen for providing the construction in Lemma 3.1 and for some useful remarks.

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*

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

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 [11, Theorem 19.3], itself based on the original work of Freiman [9] and incorporating improvements to the calculations noted by Rødseth [14]. The main new contribution is an argument to allow the restriction $|2A| \leq \frac{1}{2}(p+3)$ from [11, 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.

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 $|P_{A+B}| \geq |A| + |B| - 1$.

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 $[m, n]_g = \emptyset$. For $X \subseteq \mathbb{Z}/p\mathbb{Z}$, we let $\ell_g(X)$ denote the length of the shortest arithmetic progression with difference g which contains X, and 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 $A + B \subseteq \mathbb{Z}/p\mathbb{Z}$ *rectifies* if $\ell_g(A) + \ell_g(B) \leq p + 1$ for some nonzero $g \in \mathbb{Z}/p\mathbb{Z}$. In such 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 [11, 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 [11, Lemma 7.2], whose earlier form dates back to Vosper [18]. 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 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 $f(x)$ 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 $|2A| \le \epsilon p < p$, the Cauchy-Davenport Theorem implies $r \ge -1$. Let

$$\beta = \frac{r+3}{|A|} > 0, \tag{1}$$

so that

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

Since $2|A| + r = |2A| \le \varepsilon p \le \frac{3}{4}p$, it follows that $|A| \le \frac{3}{8}p - \frac{1}{2}r = \frac{3}{8}p - \frac{1}{2}\beta|A| + \frac{3}{2}$, which implies (in view of $\beta > 0$) that

$$|A| \le \frac{3p+12}{4(2+\beta)} < \frac{3p+12}{8}. \tag{3}$$

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.

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

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

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 $|A'| \ge |B'| \ge 2$; indeed, if $|B'| \le 1$, then combining this with the hypotheses $|B'| \le |A'| \le |A|$ and (4) yields the contradiction $|A| - 2 \ge |2A| \ge |A|$. Since $A' + B'$ rectifies, the Cauchy-Davenport Theorem for $\mathbb{Z}$ [11, Theorem 3.1] ensures

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

Moreover, we have

$$A' \subseteq P_A := a_0 + [0,m]_g, \quad B' \subseteq P_B := b_0 + [0,n]_g, \quad \text{and} \quad A' + B' \subseteq a_0 + b_0 + [0, m+n]_g \tag{5}$$

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 $A' + B'$ rectifies, 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 (4) 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 $P_{A+B} \subseteq A' + B'$ be the resulting arithmetic progressions with common difference g, we conclude that

$$|P_A \setminus A'| \le r' + 1 \qquad \text{and} \qquad |P_B \setminus B'| \le r' + 1. \tag{6}$$

If $A' = A$ and $B' = A$, then the original sumset $2A$ rectifies, 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

$$A \setminus B' \neq \emptyset. \tag{7}$$

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

$$r' = |A \setminus A'| + |A \setminus B'| + r - \Delta. \tag{8}$$

Since $|A'| + |B'| + r' = |A' + B'| = |2A| - \Delta$, it follows from (4) and $|B'| \le |A'|$ that

$$r' \le |B'| - 4 - \Delta \qquad \text{and} \qquad r' \le |A'| - 4 - \Delta. \tag{9}$$

Averaging both bounds in (9) along with the bound (8), and recalling that $|2A| = 2|A| + r$, we obtain

$$r' \le \frac{1}{3}|2A| - \frac{8}{3} - \Delta. \tag{10}$$

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

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

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

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

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

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

$$|A'| + 2p - 4|A| - 2r - 2 \le |A'| + 2|\overline{A' + A}| - 2 \le | - A' + \overline{A' + A}| \le |\overline{A}| = p - |A|.$$

Collecting terms in the above inequality, multiplying by 2, and applying the estimates $|B'| \le |A'|$ and (10) yields

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

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

$$\frac{6}{7}p - \frac{3}{7}\alpha(\frac{3p+12}{8}) + \frac{5}{7} < \frac{6}{7}p - \frac{3}{7}\beta|A| + \frac{5}{7} = \frac{6}{7}p - \frac{3}{7}r - \frac{4}{7} \le |2A| \le \varepsilon p \le \frac{3}{4}p,$$

which yields the contradiction $0 < (\frac{6}{7} - \frac{3}{4} - \frac{9}{56}\alpha)p < \frac{36}{56}\alpha - \frac{5}{7} < 0$ (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 (6) and (9), we obtain

$$\ell_g(-A') = \ell_g(A') \leq |A'| + r' + 1 \leq |A'| + |B'| - 3, \tag{11}$$

whence $\ell_g(-A') + \ell_g(\overline{A' + B'}) \leq p-2$, ensuring $-A' + \overline{A' + B'}$ rectifies via the difference g. Since $\overline{A' + A} \subseteq \overline{A' + B'}$, it follows that $-A' + \overline{A' + A}$ also rectifies 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 $\psi(-a_0+A')$ 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 (6). Moreover, $r'+1 \leq |B'|-3 \leq |A'|-3$ (by (9)), so that $|A'| > \lceil \frac{1}{2}|P_A| \rceil$, meaning $\psi(-a_0 + A')$ must contain at least 2 consecutive elements. Hence

$$\gcd^*(\psi(-a_0 + A')) = 1. \tag{12}$$

Since $-A' + \overline{A' + A}$ rectifies 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 (12), 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 (11), we find that

$$\ell_g(A') + \ell_g(A) \leq |2A| + r' + 2. \tag{13}$$

If $A' + A$ does not rectify, then (13) and (10) imply $p \leq |2A| + r' \leq \frac{4}{3}|2A| - \frac{8}{3}$, whence $|2A| \geq \frac{3}{4}p + 2 > \varepsilon p$, contrary to hypothesis. Therefore $A' + A$ rectifies. This contradicts the maximality of $|A'| + |B'|$ since by (7) 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 $A' + B'$ rectifies has

$$|A'| + 2|B'| \leq |2A| + 3. \tag{14}$$

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 [12, Theorem 1] for such sums to show that the assumption (14) implies

$$|S_A(d)| \le \tfrac{1}{3}|A| + \tfrac{2}{3}r + 2 \quad \text{for all nonzero } \ d \in \mathbb{Z}/p\mathbb{Z}. \tag{15}$$

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 $A'+A'$ rectifies. Then the assumption (14) 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 [12, 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 (15) follows.

To complete the proof, we now exploit (15) to obtain a contradiction, using in particular the following manipulations which are standard in the additive combinatorial use of Fourier analysis (e.g. [11, pp. 290–291])

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

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

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

$$\frac{|A| + 2r + 6}{3|A|} \ge \frac{|A|(p-\ell)}{|A|^{1/2}(p-|A|)^{1/2}\ell^{1/2}(p-\ell)^{1/2}} = \left(\frac{\frac{p}{\ell} - 1}{\frac{p}{|A|} - 1}\right)^{1/2}. \tag{16}$$

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 (16) yields

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

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

$$\varepsilon p \ge \ell > \frac{1-(\frac{1+2\beta}{3})^2(2+\beta)}{1-(\frac{1+2\beta}{3})^2}p. \tag{17}$$

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

$$4\beta^3 + (12-4\varepsilon)\beta^2 + (9-4\varepsilon)\beta + 8\varepsilon - 7 > 0. \tag{18}$$

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 $x \ge 0$ with a unique positive root α. As a result, (18) ensures that $\beta > \alpha$, which is contrary to hypothesis, completing the proof. □

Remark 2.4. *Our restriction $|2A| \le \frac{3}{4}p$ 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* (4) *and appropriately adjust the Fourier analytic calculation in Case 2 in the above proof, using the correspondingly weakened inequality for* (14)*.*

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 $p \ge 3$. 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 $\alpha \le -\frac{5}{4} + \frac{1}{4}\sqrt{9 + 8\pi/\sin(\pi/3)} < 0.3$. By hypothesis, $|A| \le \frac{p-r}{3} = \frac{1}{3}p - \frac{1}{3}\beta|A| + 1$, implying

$$|A| \le \frac{p+3}{\beta+3} < \frac{p+3}{3}, \tag{19}$$

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

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

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

with the final inequality above in view of (19). 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

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

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 (15), except that we use Lev's sharper estimate [12, Theorem 2] instead of [12, 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 [12, 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

$$|S_A(d)| \le \frac{\sin\Big(\big(\frac{1}{3}|2A|+1-\frac{1}{2}|A|\big)\frac{2\pi}{p}\Big)}{\sin(\frac{\pi}{p})} = \frac{\sin\big((\frac{1}{3}|A|+\frac{2}{3}r+2)\frac{\pi}{p}\big)}{\sin(\frac{\pi}{p})}. \tag{20}$$

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 (19), ensuring $y \in (\frac{\eta}{3}, \frac{1}{2})$. Then the inequality in (20) 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 (15) by the bound

$$|S_A(d)| \le \gamma(\tfrac{1}{3}|A|+\tfrac{2}{3}r+2). \tag{21}$$

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 (20) is at most M, ensuring $\gamma \le 1$. We now obtain the following inequality instead of (16):

$$\gamma\frac{1+2\beta}{3} = \frac{\gamma(\frac{1}{3}|A|+\frac{2}{3}r+2)}{|A|} \ge \frac{|A|(p-\ell)}{|A|^{1/2}(p-|A|)^{1/2}\ell^{1/2}(p-\ell)^{1/2}} = \left(\frac{\frac{p}{\ell}-1}{\frac{p}{|A|}-1}\right)^{1/2}. \tag{22}$$

A similar rearrangement as the one that yielded (17) now leads to

$$\frac{2p+\frac{\beta}{3+\beta}(p+3)-3}{3} \ge \frac{2p+\beta|A|-3}{3} = \frac{2p+r}{3} \ge |2A| > \frac{1-\gamma^2(\frac{1+2\beta}{3})^2(2+\beta)}{1-\gamma^2(\frac{1+2\beta}{3})^2}p, \tag{23}$$

with the first inequality following from (19). Since $0 \le \beta < 1$ and $0 < \gamma \le 1$, we have $\frac{\beta}{3+\beta} < 1$ and also $1-\gamma^2(\frac{1+2\beta}{3})^2 > 0$, whence (23) 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 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 $\beta \le \alpha$, 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

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

In the first subsection below, we present some examples of large m-sum-free sets, and in Subsection 3.2, we apply Theorem 1.4 to give a new upper bound for $d_m(\mathbb{Z}/p\mathbb{Z})$.

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 asymptotic density $\frac{1}{m+2}$ as $p \to \infty$. This gives the largest known example for $m \leq 7$, but not for greater values of m. Indeed, there is the following construction, due to Tomasz Schoen.

Lemma 3.1 (T. Schoen). *For each integer $m \geq 3$, we have $d_m(\mathbb{Z}/p\mathbb{Z}) \geq \frac{\lfloor m/4 \rfloor}{m}\frac{p-1}{2p}$ for every prime p of the form $p = 2mn+1$. In particular, $\lim\limits_{p\ prime \to \infty} d_m(\mathbb{Z}/p\mathbb{Z}) \geq \frac{1}{2m}\lfloor \frac{m}{4} \rfloor$.*

Proof. We identify $\mathbb{Z}/p\mathbb{Z}$ with the interval of integers $[0, p-1]$ with addition mod p. Let J be the interval $[1, (p-1)/2] = [1, mn]$ in $\mathbb{Z}/p\mathbb{Z}$. We construct an m-sum-free set A by picking appropriate elements from J. We need to ensure that $2A \cap (m \cdot A) = \emptyset$, and for this it suffices to have $2A \cap (m \cdot J) = \emptyset$.

Now $m \cdot J$ is an arithmetic progression of difference m. Taking blocks of $2n$ consecutive terms, we partition $m \cdot J$ into progressions $U_1, U_2, \ldots, U_s$, $s = \lfloor \frac{m}{2} \rfloor$, together with a final remainder progression U_{s+1} of length 0 if m is even and length n if m is odd. More precisely, we have $U_1 = \{m, 2m, \ldots, 2mn\}$, then $U_2 = \{m-1, 2m-1, \ldots, 2mn-1\}$, and so on, up to $U_s = \{m-(s-1), \ldots, 2mn-(s-1)\}$, with $U_{s+1} = \emptyset$ or $\{m-s, \ldots, mn-s\}$.

Looking at this modulo m, we see $m \cdot J$ is confined to the congruence classes $0, -1, \ldots, -\lfloor \frac{m-1}{2} \rfloor$ mod m. Therefore, it suffices to ensure that $2A$ occupies the other congruence classes mod m. For example, the following set in $\mathbb{Z}/p\mathbb{Z}$ is m-sum-free:

$$A = \{x \in J : x \in [1, \lfloor m/4 \rfloor] \mod m\},$$

since $2A \mod m$ is included in $[1, \lfloor \frac{m}{2} \rfloor]$ which is the complement of $[\lceil \frac{m+1}{2} \rceil, m]$ mod m with $m \cdot J \subseteq [\lceil \frac{m+1}{2} \rceil, m]$ mod m. We have $|A| = n\lfloor m/4 \rfloor = \frac{\lfloor m/4 \rfloor}{m}\frac{p-1}{2}$, and the result follows as there are an infinite number of primes of the form $2mn+1$ for fixed m. □

3.2. Upper bound for $d_m(\mathbb{Z}/p\mathbb{Z})$.

In this final part of the paper, we prove Theorem 1.5, which we restate here for convenience.

Theorem 3.2. *Let $p \geq 5$ be a prime, let m be an integer in $[2, p-2]$, and let $c = c(p)$ 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, $d_m \leq \frac{1}{3.1955}$.*

The idea of the proof is roughly the following: either an m-sum-free set A has doubling constant at least $2+\alpha$, in which case, since $(m \cdot A) \cap 2A = \emptyset$, we have $(3+\alpha)p = |(m \cdot A)| + |2A| \leq p$ 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 $p \geq 5$ be prime, let $0 < \alpha \leq 1/5$, and let $d \in [2, p-2]$ and N be natural numbers with $N \leq \frac{p+1}{3}$. Let I and J be progressions in $\mathbb{Z}/p\mathbb{Z}$ having the same difference and satisfying $|I| = 2N-1$, $|J| = \lfloor (1+\alpha)N - 2 \rfloor$, and $|I \cap (d \cdot J)| \leq \alpha N - 2$. Then $N < \frac{p+3}{3+\alpha}$.*

Proof. First note that, without loss of generality, we can assume $d \leq \frac{p-1}{2}$, 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 $N \geq \frac{p+3}{3+\alpha}$. 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 $J = x + [0, |J| - 1] \mod p$ for some $x \in [0, p-1]$.

If $d \cdot x \in [d, p - |I| + d - 1] \mod p$, then $d \cdot (x-1) \notin I \mod p$, ensuring that the interval $J' = (x-1) + [0, |J| - 1]$ satisfies the hypotheses with $|I \cap (d \cdot J')| \leq |I \cap (d \cdot J)|$. On the other hand, if $d \cdot x \in [p - |I|, p-1]$, then $d \cdot x$ is an element from the intersection $I \cap (d \cdot J)$ not contained in $I \cap (d \cdot J')$, where $J' = (x+1) + [0, |J| - 1]$, whence the interval $J' = (x+1) + [0, |J| - 1]$ satisfies the hypotheses with $|I \cap (d \cdot J')| \leq |I \cap (d \cdot J)|$. In either case, by repeatedly shifting the interval J, we can w.l.o.g assume

$$d \cdot x \in [0, d-1] \mod p. \tag{24}$$

In view of (24), we may partition $d \cdot J$ into successive progressions U_i (with difference d) for $i = 1, 2 \ldots, s+1$ 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

$$|U_i \cap I| \geq \left\lfloor \frac{|I|}{d} \right\rfloor \quad \text{for } i \in [1, s]. \tag{25}$$

In view of (25), we have

$$\alpha N - 2 \geq |(d \cdot J) \cap I| \geq s \left\lfloor \frac{|I|}{d} \right\rfloor. \tag{26}$$

Note first that, since the intersection of $y + d\mathbb{Z}$ with an interval of length p has size at most $\lceil p/d \rceil$, we have

$$s \geq \left\lfloor \frac{|J|}{\lceil p/d \rceil} \right\rfloor \geq \left\lfloor \frac{|J|d}{p+d-1} \right\rfloor \geq \frac{|J|d+1}{p+d-1} - 1 > \frac{((1+\alpha)N-3)d+1}{p+d-1} - 1. \tag{27}$$

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 that $|J| > (1+\alpha)N - 3$, $|I| = 2N-1$, $d \geq 2$ and $p \geq 5$, we conclude that $N < \frac{p+2d}{d+2} \leq (p+4)/4$. Thus $N \leq \frac{p+3}{4}$, which combined with our assumption $N \geq (p+3)/(3+\alpha)$ yields $(1-\alpha)(p+3) \leq 0$, contradicting that $\alpha < 1$, which proves our claim.

Since $s \geq 1$, (26) yields

$$|(d \cdot J) \cap I| \geq \lfloor |I|/d \rfloor \geq \frac{2N}{d} - 1. \tag{28}$$

Using again the hypothesis $|(d \cdot J) \cap I| \leq \alpha N - 2$, 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 $\alpha \leq \frac{1}{5}$. Thus $11 \leq d \leq \frac{p-1}{2}$, implying $p \geq 23$ and $N \geq \frac{p+3}{3+\alpha} > 6$ (in view of $\alpha \leq 1$).

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 $\alpha \leq 1$. Combining this with (26) and (27), we obtain $\alpha N - 2 > \frac{((1+\alpha)N-3)d+1}{p+d-1} - 1$, which means $d \leq \left(\alpha - \frac{1-2\alpha}{N-2}\right)(p-1) < \alpha p$ (in view of $\alpha \leq \frac{1}{2}$ and $N \geq 3$).

So far we have that, if $N \geq \frac{p+3}{3+\alpha}$ holds, then $11 \leq d < \alpha p \leq p/5$, and therefore

$$p > 55.$$

Also, we have $\frac{2N}{d} - 1 > 0$, for otherwise we obtain the contradiction $\frac{p}{4} \leq \frac{p+3}{3+\alpha} \leq N \leq \frac{d}{2} < \frac{1}{2}\alpha p \leq \frac{p}{10}$. The final part of the proof is a calculation involving (26) which will yield a contradiction. Combining (26) with (28) and (27), we obtain

$$\begin{aligned} \alpha N - 2 &> \left(\frac{((1+\alpha)N-3)d+1}{p+d-1} - 1\right)\left(\frac{2N}{d} - 1\right) \\ &= \frac{2d(1+\alpha)}{d(p+d-1)}N^2 - \left(\frac{(1+\alpha)d}{p+d-1} + \frac{6d-2}{d(p+d-1)} + \frac{2}{d}\right)N + 1 + \frac{3d-1}{p+d-1}. \end{aligned}$$

We group all terms involving N on the right side, we note that the other terms grouped on the left side amount to a negative number, and we multiply through by $\frac{p+d-1}{2(1+\alpha)N}$, to deduce that

$$N < \frac{1}{2(1+\alpha)}\left((1+2\alpha)d + (\frac{2}{d} + \alpha)p + 8 - \frac{4}{d} - \alpha\right). \tag{29}$$

Using that $11 \leq d < p/5$ and the assumption $N \geq \frac{p+3}{3+\alpha}$, we see that (29) implies

$$\frac{p+3}{3+\alpha} < \frac{1}{2(1+\alpha)}\left((1+2\alpha)\frac{p}{5} + (\frac{2}{11} + \alpha)p + 8 - \frac{4}{11} - \alpha\right).$$

Grouping terms involving p to the left side and multiplying through by $110(1+\alpha)(3+\alpha)$ yields

$$p(47 - 142\alpha - 77\alpha^2) < 930 - 75\alpha - 55\alpha^2.$$

The polynomial in α on the left side is positive for $\alpha \in [0, 1/5]$, whence

$$p \leq \frac{55\alpha^2 + 75\alpha - 930}{77\alpha^2 + 142\alpha - 47},$$

which is a bound increasing for $\alpha \geq 0$, thus maximized for $\alpha = \frac{1}{5}$, yielding $p < 59$. Since p is prime, this forces $p \leq 53$, contradicting that $p > 55$, which completes the proof. □

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 $\eta \leq \frac{p+1}{3p}$. If $p = 5$, then $1 < |A| \leq \frac{p+1}{3} = 2$ forces $|A| = 2$ and $\eta = \frac{2}{5}$, whence $\alpha < 0.167$. If $p = 7$, then $\eta \leq \frac{p+1}{3p} = \frac{8}{21}$ and $\alpha \leq -\frac{5}{4} + \frac{1}{4}\sqrt{9 + 8(8/21)7\sin(\pi/7)/\sin(\pi(8/21)/3)} < .183$. For $p \geq 11$, we have $\eta \leq \frac{p+1}{3p} \leq \frac{12}{33}$ and $\alpha \leq -\frac{5}{4} + \frac{1}{4}\sqrt{9 + 8(12/33)\pi/\sin(\pi(12/33)/3)} < 0.199$. Thus

$$\alpha < 0.2$$

in all cases.

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

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

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 $A \subseteq P_A$, $P_{2A} \subseteq 2A$,

$$|P_A| = \lfloor (1 + \alpha)|A| - 2 \rfloor \leq p \qquad \text{and} \qquad |P_{2A}| = 2|A| - 1. \tag{31}$$

It follows that $P := m \cdot P_A$ is an arithmetic progression with difference $mg \neq \pm g$ such that

$$|P \cap P_{2A}| \leq |P \cap 2A| \leq |P_A \setminus A| \leq \alpha|A| - 2. \tag{32}$$

We can therefore apply Lemma 3.3 with $N = |A|$ (as $\alpha < 0.2$), deducing that $|A| < \frac{p+3}{3+\alpha}$, 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 $t =$

$\left(\frac{7}{4}+\frac{1}{4}\sqrt{9+8\,t\,\pi/\sin(\pi t/3)}\right)^{-1}$, and the second claim in the theorem follows from solving for t numerically. □

References

[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. **12** (2005), Paper No. R19, 16pp.

[2] T. F. Bloom, *A quantitative improvement for Roth's theorem on arithmetic progressions*, J. Lond. Math. Soc. (2) **93** (2016), 643–663.

[3] P. Candela, O. Serra, C. Spiegel, *A step beyond Freiman's theorem for set addition modulo a prime*, preprint (2018). arXiv:1805.12374

[4] P. Candela, A. de Roton, *On sets with small sumset in the circle*, to appear in Q. J. Math.

[5] 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, 223–243.

[6] F. R. K. Chung, J. L. Goldwasser, *Integer sets containing no solutions to* $x+y=3z$, in: R.L. Graham and J. Nesetil eds., The Mathematics of Paul Erdős, Springer, Berlin (1997), 218–227.

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

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

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

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

[11] D. J. Grynkiewicz, *Structural additive theory*, Developments in Mathematics, **30**. Springer, Cham, 2013. xii+426 pp.

[12] V. F. Lev, *Distribution of points on arcs*, Integers 5(2)(2005)(electronic)

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

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

[15] K. F. Roth, *On certain sets of integers* J. London Math. Soc. **28** (1953), 104–109.

[16] T. Sanders, *On Roth's theorem on progressions*, Ann. of Math. **174** (2011), 619–636.

[17] 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, 2043–2060.

[18] G. Vosper, *The critical pairs of subsets of a group of prime order*, J. London Math. Soc. **31** (1956), 200-205.

Universidad Autónoma de Madrid, and ICMAT, Ciudad Universitaria de Cantoblanco, Madrid 28049, Spain

E-mail address: pablo.candela@uam.es

Universidad Autónoma de Madrid, and ICMAT, Ciudad Universitaria de Cantoblanco, Madrid 28049, Spain

E-mail address: diego.gonzalezs@predoc.uam.es

University of Memphis, Department of Mathematical Sciences, Memphis, TN 38152, USA

E-mail address: diambri@hotmail.com