Acta Math. Univ. Comenianae
Vol. LXXXVIII, 3 (2019), pp. 521–525

A STEP TOWARDS THE $3k-4$ CONJECTURE IN $\mathbb{Z}/p\mathbb{Z}$ AND AN APPLICATION TO m-SUM-FREE SETS

P. CANDELA, D. GONZÁLEZ-SÁNCHEZ and D. J. GRYNKIEWICZ

Abstract. The $3k-4$ conjecture in $\mathbb{Z}/p\mathbb{Z}$ 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 $|A| + r + 1$. In this paper we summarize progress made towards this conjecture in a recent joint paper of the same authors. In that paper we prove first that if $|2A| \leq (2+\alpha)|A| - 3$ for $\alpha \approx 0.136861$ and $|2A| \leq 3p/4$, then A is efficiently covered by an arithmetic progression, as in the conclusion of the conjecture. With a refined argument we prove that we can go up to $\alpha = (\sqrt{33} - 5)/4 + o_{|A|,p\to\infty}(1)$ at the cost of restricting $|A| \leq (p-r)/3$. We then use this to investigate the maximum size of m-sum-free sets for $m \geq 3$, i.e., sets $A \subseteq \mathbb{Z}/p\mathbb{Z}$ such that the equation $x + y = mz$ has no solution in A. We obtain that for m fixed, $\lim_{p\to\infty} \max\{|A|/p : A \subseteq \mathbb{Z}/p\mathbb{Z}\ m\text{-sum-free}\} \leq 1/3.1955$ (previously, the best known upper bound was $1/3.0001$).

1. Introduction

This article is a short version of the paper [**3**].

Let G be a finite abelian group. For a subset A of G, we denote by $2A$ the sumset $A + A := \{x + y : x, y \in A\}$ and by $\overline{A}$ the complement of A, $G \setminus A$. A classical result due to Freiman is the $3k-4$ Theorem, which states that if a finite set $A \subseteq \mathbb{Z}$ has doubling $|2A|/|A|$ close to the minimum, then A is efficiently covered by an arithmetic progression:

Theorem 1.1 (Freiman's $3k-4$ Theorem)**.** *Let A be a finite subset of $\mathbb{Z}$ with $|2A| = 2|A| + r \leq 3|A| - 4$. Then there is an arithmetic progression $P \subseteq \mathbb{Z}$ such that $A \subseteq P$ and $|P \setminus A| \leq r + 1$.*

A central topic in additive number theory is the study of variants of this theorem in other groups. We focus on the case $\mathbb{Z}/p\mathbb{Z}$, where there is a well-known conjecture on what this theorem could look like (see [**12**, Conjecture 19.2]):

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

Received May 17, 2019.
2010 *Mathematics Subject Classification.* Primary 11P70; Secondary 11B75.

Progress towards this conjecture has been made by many authors: Rødseth [**15**]; Green and Ruzsa [**11**]; Serra and Zémor [**18**]; Candela, Serra and Spiegel [**5**]; etc. In [**12**] there are other results towards Conjecture 1.2 as well as many techniques that will be used in this article. Our main results regarding this conjecture are:

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

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

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

and

Theorem 1.4. *Let p be prime, let $\eta \in (0,1)$, let $A \subseteq \mathbb{Z}/p\mathbb{Z}$ be a set with density $|A|/p \geq \eta > 0$ and let $\alpha = -\frac{5}{4} + \frac{1}{4}\sqrt{9 + 8\,\eta\, p \sin(\pi/p)/\sin(\pi\eta/3)}$. Define $r := |2A| - 2|A|$ and suppose*

$$|2A| \neq \mathbb{Z}/p\mathbb{Z}, |2A| \leq (2+\alpha)|A| - 3 \text{ and } |A| \leq \frac{p-r}{3}.$$

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

In Theorem 1.3 the doubling constant 2.1386... is smaller than the 2.4 given by Freiman [**10**] and Rødseth [**15**]. However, these versions require the size of A to be bounded by $p/35$ and $p/10.7$ respectively whereas we only require $|2A| \leq (3/4)|A|$. Recall that these two quantities are related through $r = |2A| - 2|A|$ so they are not completely independent. Conjecture 1.2 says that r should be allowed to go up to $|A| - 4$ and in this case the bound on $|2A|$ is $(3/4)p - 1/16$ which is almost equal to ours. The reason why the value of α is the root of a polynomial of degree 4 comes from the proof. Roughly speaking, we end up with an identity like $(|A|/p)^2 = \sum \widehat{1_A}\widehat{1_A}\overline{\widehat{1_{2A}}}$ and we do a standard bound involving Cauchy-Schwarz, Plancherel's identity and an inequality of Freiman [**13**, Theorem 1] to relate $|A|$ and $|2A|$ (in the next section we explain better the use of Freiman's inequality).

Theorem 1.4 was motivated by the study of m-sum-free sets. For $m \geq 3$ an integer and p a prime greater than m, a set $A \subseteq \mathbb{Z}/p\mathbb{Z}$ is said to be m-sum-free if the equation $x + y = mz$ has no solution with $(x,y,z) \in A^3$. Let $d_m(\mathbb{Z}/p\mathbb{Z}) := \max\left\{\frac{|A|}{p} : A \subseteq \mathbb{Z}/p\mathbb{Z}\ m\text{-sum-free}\right\}$. If A is m-sum-free then $2A$ is disjoint from $m \cdot A = \{ma : a \in A\}$ thus $|2A| + |m \cdot A| \leq p$. If we define $r := |2A| - 2|A|$, then it is clear that the previous inequality gives $|A| \leq (p-r)/3$. Using the Cauchy-Davenport inequality we can deduce that $r \geq -1$ and thus, if we define

$$d_m := \lim_{p\to\infty} d_m(\mathbb{Z}/p\mathbb{Z})$$

(the limit exists by [**6**]), then $d_m \leq 1/3$. The first non-trivial bound for d_m was given by Candela and De Roton in [**4**, Theorem 3.1], where they used a result of Serra and Zémor [**18**] to obtain $d_m \leq 1/3.0001$. Using similar techniques and Theorem 1.4, we are able to push this bound to $d_m \leq 1/3.1955$. To conclude this section let us mention that there exists a construction by Tomasz Shoen showing that $d_m \geq \frac{1}{2m}\lfloor\frac{m}{4}\rfloor$ for all $m \geq 3$ (personal communication). More precisely:

Lemma 1.5 (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 $p = 2mn+1$. Hence, $\lim_{\substack{p\to\infty \\ p\ prime}} d_m(\mathbb{Z}/p\mathbb{Z}) \geq \frac{1}{2m}\lfloor\frac{m}{4}\rfloor$.*

The proof of the above lemma can be found in [**3**] but let us briefly mention that it consists on constructing a set with the above properties which at the end is roughly the sum of two arithmetic progressions.

2. Overview of the proofs

In this section we present the ideas underlying the proofs of the results mentioned above. For the complete proofs, see [**3**].

Let p be a prime, let $g \in \mathbb{Z}/p\mathbb{Z}$ be a non-zero element (which is then a generator of the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$) and for 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. 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, $b_0 \in \mathbb{Z}/p\mathbb{Z}$. Therefore, 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 $A+B$.

Sketch of proof of Theorem 1.3. We will use the asymmetric version of the $3k-4$ theorem as it appears in [**12**, Theorem 7.1] and two observations. The first one is that if $P \subseteq A \subseteq \mathbb{Z}/p\mathbb{Z}$, with P an arithmetic progression, then $\overline{A} \subseteq \overline{P}$, where $\overline{P}$ is another arithmetic progression with the same difference. The second one is that if $A, B \subseteq \mathbb{Z}/p\mathbb{Z}$, then $-A+\overline{A+B} \subseteq \overline{B}$. Let us now look at pairs of sets $A', B' \subseteq A$ such that $A'+B'$ rectifies. The ideal case would be if for $A' = B' = A$, the sum-set $A'+B'$ rectified, because then we could go via a Freiman isomorphism to $\mathbb{Z}$, apply there the known $3k-4$ theorem, and then go back to $\mathbb{Z}/p\mathbb{Z}$. This is why it is natural to split the problem into two parts:
Case 1 will be when among the pairs $A'+B'$ that rectify there are some that are *large* (precisely $|A'|+|B'|+\min\{|A'|,|B'|\}-4 \geq |2A|$).
Case 2 will be when for all pairs that rectify, the opposite inequality holds.

If we are in *Case 1* we prove that indeed the largest pair of rectifiable sum-sets $A'+B'$ occurs when $A' = B' = A$. By contradiction, assume without loss of generality that $|A'| \geq |B'|$ is the rectifiable pair with the largest sum $|A'|+|B'|$ and $B' \neq A$. Then we go through a Freiman isomorphism ψ to $\mathbb{Z}$ and apply the

$3k-4$ theorem to $\psi(A'+B')$, which will provide us progressions $\psi(A') \subseteq P_A$, $\psi(B') \subseteq P_B$ and $P_{A+B} \subseteq \psi(A'+B')$. These progressions will give us that the pair $(-A') + (\overline{A+A'})$ is also rectifiable (using observations like for instance that $\overline{A+A'} \subseteq \overline{B'+A'} \subseteq \overline{\psi^{-1}(P_{A+B})}$). With some more work we will conclude that $|-A' + \overline{A+A'}| \leq |A'| + |\overline{A+A'}| + \min\{|A'|, |\overline{A+A'}|\} - 4$, which allows us to use the asymmetric version of the $3k-4$ Theorem as in [**12**, Theorem 7.1] to obtain the progressions $\psi(-A') \subseteq P_{-A'}$, $\psi(\overline{A+A'}) \subseteq P_{\overline{A+A'}}$ and $P_{-A'+\overline{A+A'}} \subseteq \psi(-A'+\overline{A+A'})$. By the second observation we will be able to recover information about A using that $\psi^{-1}(P_{-A'+\overline{A+A'}}) \subseteq -A' + \overline{A+A'} \subseteq \overline{A}$ and this is how we will obtain that A is efficiently covered by an arithmetic progression. We end up showing that $A+A'$ must rectify or otherwise the assumption $|2A| \leq 3/4p$ would be violated. Thus we have a contradiction with the assumption that $|A'|+|B'|$ was chosen to be maximal.

To deal with *Case 2*, define the exponential sum $S_A(d) = \sum_{x\in A} \mathrm{e}^{\frac{2\pi \mathrm{i}}{p}\mathrm{d}x}$ for a non-zero $d \in \mathbb{Z}/p\mathbb{Z}$. It is intuitive that if the points $e^{\frac{2\pi \mathrm{i}}{p}\mathrm{d}x}$ are randomly distributed among the the circle, then $|S_A(d)|$ should be small, whereas if a lot of them are concentrated near (say) 1, then the sum should be large. But *Case 2* is precisely when we rule out this possibility because if we let $C_u := \{\mathrm{e}^{\mathrm{i}x} : x \in (u, u+\pi)\}$, d^{-1} be the multiplicative inverse of $d \in \mathbb{Z}/p\mathbb{Z}$ and $A' := \{x \in A : \mathrm{e}^{\frac{2\pi \mathrm{i}}{p}\mathrm{d}x} \in C_u\}$, then $\ell_{d^{-1}}(A') \leq \frac{p+1}{2}$ and $A'+A'$ rectifies. To conclude we use an estimate of Freiman [**13**, Theorem 1] that gives a bound for $|S_A(d)|$ in this situation. What remains is just a long but standard calculation involving the identity $|A|^2 p = \sum_{x\in\mathbb{Z}/p\mathbb{Z}} S_A(x) S_A(x) \overline{S_{2A}(x)}$, giving a contradiction with the fact that $|2A| \leq (2+\alpha)|A| - 3$. □

The second result, Theorem 1.4, is a refinement whose proof uses the same ideas but in *Case 2* needs a sharper bound on $|S_A(d)|$ given by [**13**, Theorem 2], and some minor changes to adapt the argument to the new bound $|A| \leq \frac{p-r}{3}$.

Finally, let us mention how this result can be used to estimate the quantity d_m. The ideas are simple. First, as we said before if $A \subseteq \mathbb{Z}/p\mathbb{Z}$ is m-sum-free we can assume that $|A| \leq (p-r)/3$. Thus, we have one of the conditions of Theorem 1.4 for free. Now there are two cases: either $|2A| > (2+\alpha)|A|-3$ or $|2A| \leq (2+\alpha)|A|-3$. In the former we deduce immediately that $(2+\alpha)|A|-3+|A| \leq |2A|+|m\cdot A| \leq p$. Then we must have $|A| \leq (p+3)/(3+\alpha)$. In the second case, we can apply Theorem 1.4 to conclude that we can approximate A by an arithmetic progression P_A, and $2A$ contains a large arithmetic progression P_{2A}. This allows us to work with intervals instead of arbitrary sets because the property $2A \cap m\cdot A = \emptyset$ implies that $|P_{2A} \cap (m\cdot P_A)|$ is *small.* But now $m\cdot P_A$ is approximately uniformly distributed among $\mathbb{Z}/p\mathbb{Z}$ (under some technical conditions), and as $|P_{2A}|$ is *large*, it is easy to deduce that $|P_A|$ cannot be *large.*

Acknowledgment. We are very grateful to Tomasz Schoen for providing the construction in Lemma 1.5 and for some useful remarks.

References

1. Baltz A., Hegarty P., Knape J., Larsson U. and Schoen T., *The structure of maximum subsets of* $\{1,\ldots,n\}$ *with no solutions to* $a+b=kc$, Electron. J. Combin. **12** (2005), #19.

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

3. Candela P., González-Sánchez D. and Grynkiewicz D. J. *On sets with small sumset and* m*-sum-free sets in* $\mathbb{Z}/p\mathbb{Z}$, preprint (2019).

4. Candela P. and de Roton A., *On sets with small sumset in the circle*, Q. J. Math. **70** (2019), 49–69.

5. Candela P., Serra O. and Spiegel C., *A step beyond Freiman's theorem for set addition modulo a prime*, `arXiv:1805.12374`.

6. Candela P. and Sisask O., *On the asymptotic maximal density of a set avoiding solutions to linear equations modulo a prime*, Acta Math. Hungar. **132** (2011), 223–243.

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

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

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

10. Freiman G., *Inverse problems in additive number theory. Addition of sets of residues modulo a prime*, Dokl. Akad. Nauk **141** (1961), 571–573.

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

12. Grynkiewicz D. J., *Structural Additive Theory*, Development in Mathematics 30, Springer-Verlag, 2013.

13. Lev V. F., *Distribution of points on arcs*, Integers **5** (2005), #11.

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

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

16. Roth K. F., *On certain sets of integers* J. Lond. Math. Soc. **28** (1953), 104–109.

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

18. Serra O. and Zémor G., *Large sets with small doubling modulo p are well covered by an arithmetic progression*, Ann. Inst. Fourier (Grenoble) **59** (2009), 2043–2060.

19. Vosper G., *The critical pairs of subsets of a group of prime order*, J. Lond. Math. Soc. **31** (1956), 200–205.

P. Candela, Universidad Autónoma de Madrid, and ICMAT Ciudad Universitaria de Cantoblanco Madrid, Spain,
e-mail: `pablo.candela@uam.es`

D. González-Sánchez, Universidad Autónoma de Madrid, and ICMAT Ciudad Universitaria de Cantoblanco, Madrid, Spain,
e-mail: `diego.gonzalezs@predoc.uam.es`

D. J. Grynkiewicz, Department of Mathematical Sciences, University of Memphis, Memphis, USA,
e-mail: `diambri@hotmail.com`