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 $3|A| - 4 = |2A| \leq$