On sum-free sets modulo p

Jean-Marc DESHOUILLERS* and Gregory A. FREIMAN†

To Eduard Wirsing, with respect and friendship, for his 75th birthday

Abstract

Let p be a sufficiently large prime and $\mathcal{A}$ be a sum-free subset of $\mathbb{Z}/p\mathbb{Z}$; improving on a previous result of V. F. Lev, we show that if $|\mathcal{A}| = \text{card}(\mathcal{A}) > 0.324p$, then $\mathcal{A}$ is contained in a dilation of the interval $[|\mathcal{A}|, p - |\mathcal{A}|]$ (mod. p).

1 Introduction

A subset $\mathcal{A}$ of an additive monoid $\mathcal{M}$ is said to be *sum-free* if the equation $a + b = c$ has no solution with elements a, b and c in $\mathcal{A}$. We are considering the case when $\mathcal{M} = \mathbb{Z}/p\mathbb{Z}$ for a prime number p. It follows easily from the Cauchy-Davenport Theorem (Lemma 1) that the cardinality of a sum-free subset $\mathcal{A}$ of $\mathbb{Z}/p\mathbb{Z}$ is at most $(p + 1)/3$. Some time ago, Vsevolod F. Lev raised the question of studying the structure of a sum-free subset $\mathcal{A}$ of $\mathbb{Z}/p\mathbb{Z}$ with cardinality less than $p/3$. In [5], V. Lev gave the structure of such a sum-free set with cardinality larger than $0.33p$.

In this paper, we extend Lev's result, showing the following.

Theorem 1. *Let p be sufficiently large a prime and $\mathcal{A}$ a sum-free subset of $\mathbb{Z}/p\mathbb{Z}$; if $|\mathcal{A}| = \text{card}(\mathcal{A}) > 0.324p$, then $\mathcal{A}$ is contained in a dilation of the interval $[|\mathcal{A}|, p - |\mathcal{A}|]$ (mod. p).*

*Supported by Université Victor Segalen Bordeaux 2 (EA 2961), Université Bordeaux1 and CNRS (UMR 5465)

†Supported by Tel Aviv University and ADEMAS Association

Our main ingredient (Lemma 3) is a combinatorial study of the so-called *rectified* part of $\mathcal{A}$, showing that it is included in an interval with many of its elements close to its end-points, which in turn leads to showing that many elements from $\mathbb{Z}/p\mathbb{Z}$ cannot be in $\mathcal{A}$. Equipped with this lemma, we show that if $\mathcal{A}$ contains at least one element from the interval $[-p/4\,,\,p/4]$ (mod. p), then there are so many places which must stay free from elements from $\mathcal{A}$, that it is impossible to find room for the rectified part of $\mathcal{A}$. Thus, the set $\mathcal{A}$ is included in the interval $[p/4\,,\,3p/4]$ (mod. p); at the very end of the paper, we easily deduce Theorem 1 from this fact.

This argument, when based on the classical rectification argument introduced by the second named author some forty years ago, would lead to the value $0.326p$ in Theorem 1. Fortunately, our argument can be combined with the improved version of the rectification argument introduced by V. Lev in [4], improvement which plays a crucial rôle in [5].

We take this opportunity to thank V. Lev for having communicated to us the preprints of his two above-mentioned papers [4] and [5], and for his numerous and detailed comments on a first draft of this paper.

2 Notation

It will be convenient to speak about "intervals" in $\mathbb{Z}/p\mathbb{Z}$ and it will also be convenient to avoid the natural normalizing factor p when describing the size of subsets of $\mathbb{Z}/p\mathbb{Z}$ and more generally to simplify the presentation of numerical considerations concerning subsets of $\mathbb{Z}/p\mathbb{Z}$. For those reasons, we introduce the following definitions and conventions.

Let us denote by σ the canonical map from $\mathbb{R}$ onto $\mathbb{T} = \mathbb{R}/\mathbb{Z}$; we keep the usual convention not to mention σ and write for example 0.5, or -0.5 as well, for the non zero solution of $x + x = 0$ in $\mathbb{T}$.

An *interval* in $\mathbb{T}$ is the image by σ of an interval of $\mathbb{R}$. For given α and β in $\mathbb{T}$, there are exactly two closed intervals with border points α and β and their only common points are α and β; when we wish to describe a closed interval in $\mathbb{T}$ the border points of which are α and β, we shall write $\langle \alpha\,,\,(\gamma)\,,\,\beta \rangle$, where γ is a point from the interval under consideration, which is different from α and β. In practice, when there is no ambiguity about the interval we consider, we shall not mention a point γ. The *size* of an interval is its (normalized Haar) measure in $\mathbb{T}$.

If two rational integers a and b are congruent modulo p, we have $\sigma(a/p) = \sigma(b/p)$, which permits to define a map τ from $(\mathbb{Z}/p\mathbb{Z}, +)$ to $(\mathbb{T}, +)$, which is easily seen to be an injective group homomorphism. We say that a subset of $\mathbb{Z}/p\mathbb{Z}$ is an *interval* if it is the inverse image, by τ^{-1}, of an interval in $\mathbb{T}$. For a set $\mathcal{A}$ in $\mathbb{Z}/p\mathbb{Z}$, we shall define its *size* by $\text{size}(\mathcal{A}) = \text{card}(\mathcal{A})/p$.

The notions of *size* we have introduced on $\mathbb{Z}/p\mathbb{Z}$ and $\mathbb{T}$ are different since one is discrete and the other continuous; however, in the case of intervals they are closely connected: let I be an interval in $\mathbb{T}$ and $\mathcal{I} = \tau^{-1}(I)$; we have the inequalities $\text{size}(I) - 1/p \leq \text{size}(\mathcal{I}) \leq \text{size}(I) + 1/p$. In practice, since we are considering large p, we are not going to write explicitly the terms $O(1/p)$ but use strict inequalities between the sizes of the sets under consideration.

For a real number u, we use the traditional notation $e(u) = \exp(2\pi i u)$, $e_p(u) = \exp(\frac{2\pi i u}{p})$ and $\|u\| = \min_{z\in\mathbb{Z}} |u - z|$; when $b \in \mathbb{Z}/p\mathbb{Z}$, the expression $e_p(b)$ (resp. $\|b/p\|$) denotes the common value of all the $e_p(\tilde{b})$'s (resp. $\|\tilde{b}/p\|$), where $\tilde{b}$ is any integer representing the class b.

Finally, for subsets $\mathcal{E}$ and $\mathcal{F}$ of an abelian group $\mathcal{G}$ (in practice $\mathbb{Z}/p\mathbb{Z}$ or $\mathbb{T}$), we let $\mathcal{E} + \mathcal{F} = \{e + f : e \in \mathcal{E}, f \in \mathcal{F}\}$, we denote by $\mathcal{E}^{sym}$ the set $\mathcal{E} \cup (-\mathcal{E})$, and we say that $\mathcal{E}$ is symmetric if $\mathcal{E} = \mathcal{E}^{sym}$.

3 Preliminary lemmas

Our first lemma is fairly classical (cf. [1]).

Lemma 1 (Cauchy-Davenport Theorem). *Let p be a prime number and $\mathcal{E}$ and $\mathcal{F}$ two non empty subsets of $\mathbb{Z}/p\mathbb{Z}$; then, one has* $\text{Card}(\mathcal{E} + \mathcal{F}) \geq \min(p, \text{Card}(\mathcal{E}) + \text{Card}(\mathcal{F}) - 1)$.

The following observation, discussed by V. F. Lev and the second named author, was presented in [5] as Lemma 2.

Lemma 2. *Let B, m and L be natural integers with $1 < L \leq 2B$ and $\mathcal{B}$ be a set of B integers included in $[m\,,\, m + L - 1]$. Then, for any integer $k \geq 1$ one has*

$$((L - B)/k\,,\, B/k) \subset \mathcal{B} - \mathcal{B}.$$

The next lemma is a formulation of the key innovation of the present paper. It says that if an interval $\mathcal{L}$ of $\mathbb{Z}$ of length L contains more than $\mathsf{L}/2$ elements from a sum-free set $\mathcal{A}$, and if a is an element from $\mathcal{A}$ of size between $\mathsf{L}/4$ and $\mathsf{L}/2$, then many elements from $\mathcal{A}$ are concentrated around the end-points of $\mathcal{L}$, and this in turn implies that $\mathcal{A}$ cannot contain elements which are in absolute value close to L. In the present paper, we shall only use the case when $k = 1$. We state and prove this lemma for natural integers; one readily checks that it can be extended to the case of residues modulo p, when $L < p$, if one interprets the interval $[m\,,\, m+\mathsf{L}-1]$ as being $\langle m\,,\,(m+\lfloor \mathsf{L}/2\rfloor)\,,\, m+\mathsf{L}-1\rangle$.

Lemma 3. *Let B, m and L be natural integers with $1 < \mathsf{L} < 2\mathsf{B}$; let $\mathcal{A}$ be a sum-free set and $\mathcal{B}$ be a subset of $\mathcal{A} \cap [m\,,\, m+\mathsf{L}-1]$ with cardinality B. Then, for any integer $k \geq 1$ and any element $a \in \mathcal{A}$ with $\mathsf{L}/4 < ka < \mathsf{L}/2$, one has*
(i) the intervals $[m\,,\, m+\mathsf{L}-2ka-1]$ and $[m+2ka\,,\, m+\mathsf{L}-1]$ contain each at least $\mathsf{B}-ka$ elements from $\mathcal{B}$,
(ii) the set $[2ka-(2\mathsf{B}-\mathsf{L})+1, 2ka+(2\mathsf{B}-\mathsf{L})-1] \cap (\mathcal{A} \cup (-\mathcal{A}))$ is empty.

Proof of Lemma 3 Since $\mathcal{A}$ is sum-free, for any element a from $\mathcal{A}$, any interval $[n\,,\, n+2a-1]$ contains at most a elements from $\mathcal{A}$: otherwise, by the pigeon-hole principle, we could find an element c in $[n\,,\, n+a-1] \cap \mathcal{A}$ such that $c+a$ is also in $\mathcal{A}$, a contradiction. Since $0 < 2ka < \mathsf{L}$, each of the intervals $[m\,,\, m+2ka-1]$ and $[m+\mathsf{L}-2ka\,,\, m+\mathsf{L}-1]$, which is the union of k intervals of the shape $[n\,,\, n+2a-1]$, contains at most ka elements of $\mathcal{A}$ (and so from $\mathcal{B}$); since $2ka \leq \mathsf{L}$ and $ka < \mathsf{L}/2 < \mathsf{B}$, then there are at least $\mathsf{B}-ka$ elements from $\mathcal{B}$ in each of the intervals $[m\,,\, m+\mathsf{L}-2ka-1]$ and $[m+2ka\,,\, m+\mathsf{L}-1]$. This proves (i).

Let us assume that the interval $[2ka-(2\mathsf{B}-\mathsf{L})+1, 2ka+(2\mathsf{B}-\mathsf{L})-1]$ contains an element from $\mathcal{A} \cup (-\mathcal{A})$, say $|x|$, where $x \in \mathcal{A}$.

If $|x| \geq 2ka$, we consider all the pairs $(m+h, m+h+|x|)$, for $0 \leq h \leq \mathsf{L}-|x|-1$; they have the following properties:

- at least one of the element in each pair does not belong to $\mathcal{A}$,

- all the elements from those pairs belong to $[m\,,\, m+\mathsf{L}-2ka-1] \cup [m+2ka\,,\, m+\mathsf{L}-1]$,

- the number of those pairs is $\mathsf{L}-|x| > \mathsf{L}-(2ka+(2\mathsf{B}-\mathsf{L})) = 2(\mathsf{L}-\mathsf{B}-ka)$.

This implies that strictly more than $2(\mathsf{L}-\mathsf{B}-ka)$ elements from $[m\,,\, m+\mathsf{L}-2ka-1] \cup [m+2ka\,,\, m+\mathsf{L}-1]$ do not belong to $\mathcal{A}$, and so strictly less than $2(\mathsf{B}-ka)$ belong to $\mathcal{B}$, which contradicts (i).

Similarly, if $|x| < 2ka$, we get a contradiction by the same reasoning, considering the pairs $(m+h, m+h+|x|)$ for $2ka-|x| \leq h \leq \mathsf{L}-2ka-1$. This proves (ii).

The next lemma is due to V. Lev [4]. When the cardinal of $\mathcal{A}$ is large compared to p, which is our case, it improves on a result of the second named author (cf. [3] for this lemma and some uses of it for inverse additive questions).

Lemma 4. *Let $\mathcal{D}$ be a subset of $\mathbb{Z}/p\mathbb{Z}$. There exists an interval $\mathcal{I}$ of $\mathbb{Z}/p\mathbb{Z}$ with size at most $1/2$ such that*

$$\mathrm{size}(\mathcal{D}\cap\mathcal{I}) \geq \frac{\mathrm{size}(\mathcal{D})}{2} + \frac{\arcsin(|\sum_{d\in\mathcal{D}} e_p(d)|\sin(\frac{\pi}{p}))}{2\pi}.$$

For the sake of further reference, we state a last combinatorial lemma.

Lemma 5. *Let K, H and m be positive integers such that $2\mathsf{K} \leq \mathsf{H}+1$, and $\mathcal{K}$ be a set of K integers included in $[m\,,\,m+\mathsf{H}-1]$. There exists a pair of elements k_1 and k_2 in $\mathcal{K}$ such that*

$$\mathsf{K}-1 \leq k_2-k_1 \leq \mathsf{H}-\mathsf{K}+1. \tag{1}$$

Proof of Lemma 5 We first prove the lemma under the extra assumption that $m=0$ and m belongs to $\mathcal{K}$. If some element k from $\mathcal{K}$ lies in $[\mathsf{K}-1\,,\,\mathsf{H}-\mathsf{K}]$, the lemma is proved with $k_1=0$ and $k_2=k$. We may assume that the K elements of $\mathcal{K}$ belong to $[0\,,\,\mathsf{K}-2]\cup[\mathsf{H}-\mathsf{K}+1\,,\,\mathsf{H}-1]$. Since all the K elements from $\mathcal{K}$ belong to one term of the $\mathsf{K}-1$ pairs $(n\,,\,n+\mathsf{H}-\mathsf{K}+1)$ for $0\leq n\leq \mathsf{K}-2$, there exists an n_0 for which both terms from $(n_0\,,\,n_0+\mathsf{H}-\mathsf{K}+1)$ belong to $\mathcal{K}$; the lemma is also proved in this case by taking $k_1=n_0$ and $k_2=n_0+\mathsf{H}-\mathsf{K}+1$. The general case is deduced from the special one we have just proved, by considering $\mathcal{K}'=\{k-\min_{\ell\in\mathcal{K}}\ell :\ k\in\mathcal{K}\}$.

4 Partial rectification

We show the existence of a subset $\mathcal{B}$ of (some dilation of) $\mathcal{A}$ which is included in half a circle, with

$$B > 0.2431 \tag{2}$$

and which is included in an interval $\mathcal{L}$ with size

$$L < 0.6760 - B < 0.4329\,, \tag{3}$$

the end points of which belong to $\mathcal{B}$. Moreover, in the sequel, $\mathcal{B}$ is chosen as a maximal subset of (some dilation of) $\mathcal{A}$ included in half a circle, and among those, it is chosen so that L is minimal.

A first consequence of the extremal properties of $\mathcal{B}$ and $\mathcal{L}$ is that the end-points of $\mathcal{L}$ belong to $\mathcal{B}$ and thus to $\mathcal{A}$.

A second consequence of the maximal choice for $\mathcal{B}$ is the following

$$\text{If } \mathcal{I} \text{ is an interval of } \mathbb{Z}/p\mathbb{Z} \text{ of size } 0.5 \text{ then } 0.324-B \leq \text{size}(\mathcal{I}\cap\mathcal{A}) \leq B. \quad (4)$$

The upper bound comes from the maximal choice for $\mathcal{B}$. Let $\mathcal{J}$ be the complementary interval of $\mathcal{I}$ in $\mathbb{Z}/p\mathbb{Z}$. We have $\text{size}(\mathcal{J}) = 0.5$ and, again by the maximal choice for $\mathcal{B}$, we have $\text{size}(\mathcal{J} \cap \mathcal{A}) \leq B$, so that $\text{size}(\mathcal{I} \cap \mathcal{A}) \geq A - B \geq 0.324 - B$, which proves the lower bound in (4).

Due to Lemma 4, our first task is to show that for some non zero t, the sum $|\sum_{a\in\mathcal{A}} e_p(t.a)|$ is large. Let us assume on the contrary that for all non zero t we have

$$|S(t)| \leq 0.1552899p\,, \text{ where } S(t) = \sum_{a\in\mathcal{A}} e_p(t.a). \quad (5)$$

Since $\mathcal{A}$ is sum-free, the equation $a - b = c$ has no solution in $\mathcal{A}$ and thus we have $\sum_{t=0}^{p-1} |S(t)|^2 S(t) = 0$, whence

$$|\mathcal{A}|^3 \leq \sum_{t=1}^{p-1} |S(t)|^3 \leq 0.1552899p \sum_{t=1}^{p-1} |S(t)|^2 \leq 0.1552899p|\mathcal{A}|(p - |\mathcal{A}|),$$

leading to a contradiction since $\text{card}\,\mathcal{A} > 0.324p$. Thus, there exists a non zero t for which relation (5) is not satisfied; by Lemma 4, there exists a subset $\mathcal{C}$ of $t \cdot \mathcal{A} := \{ta/a \in \mathcal{A}\}$ with cardinality larger than $0.2431p$. Since $t \cdot \mathcal{A}$ is sum-free, we have $\text{card}(\mathcal{C} + \mathcal{C}) + \text{card}\, t \cdot \mathcal{A} \leq p$, whence

$$\text{card}(\mathcal{C} + \mathcal{C}) \leq 0.676p < 3\mathcal{C} - 3. \quad (6)$$

We can find a set $\mathcal{C}' = \{c'_1, \ldots, c'_k\}$ of integral representatives of $\mathcal{C}$ with $c'_k - c'_1 < p/2$. Since $\mathcal{C}$ is included in half a circle, we have $\text{card}(\mathcal{C} + \mathcal{C}) = \text{card}(\mathcal{C}'+\mathcal{C}')$. If the greatest common divisor of the mutual distances between the (c'_k)'s is 1, then the so-called "Freiman's 3k-3 theorem" (cf. [6], Theorem 1.15) tells us that $\text{card}(\mathcal{C}' + \mathcal{C}') \geq c'_k - c'_1 + \text{card}\,\mathcal{C}'$; by the inequalities we have on $\text{card}\,\mathcal{C}'$ and $\text{card}(\mathcal{C}' + \mathcal{C}')$, we get $c'_k - c'_1 \leq \text{card}(\mathcal{C}' + \mathcal{C}') - \text{card}\,\mathcal{C}' \leq 0.676p - \text{card}\,\mathcal{C} < 0.4329p$. If the common divisor of the mutual distances between the (c'_k)'s is not 1, it has to be 2 since $\text{card}\,\mathcal{C}' > p/6$. In this case, we consider the integer t' in $[1\,,\, p - 1]$ such that $2t' \equiv t(\text{mod p})$; it is then possible to choose a set of integers $\mathcal{C}'' = \{c''_1, \ldots, c''_k\}$ which represents the set $\{x \in \mathbb{Z}/p\mathbb{Z}\,/\, 2x \in \mathcal{C}\}$ and is such that $c''_k - c''_1 < p/2$ and the greatest common divisor of the mutual distances between the (c''_k)'s is 1. As above, we show that $c''_k - c''_1 < 0.676p - \operatorname{card} \mathcal{C} < 0.4329p$. In both cases, we have shown that there exists a non zero u (which is t in the first case and t' in the second one) such that the set $u \cdot \mathcal{A}$ has a subset with more than $0.2431p$ elements which is included in an interval of size less than $0.676 - \operatorname{size} \mathcal{C} < 0.4329$. Since the statement of Theorem 1 is invariant under a dilation of $\mathcal{A}$, we shall assume in the sequel, without loss of generality, that $u = 1$.

5 Zones of $\mathbb{Z}/p\mathbb{Z}$ free from elements from $\mathcal{A}$

It will be convenient to identify $\mathcal{A}$ and its image $\tau(\mathcal{A})$ in $\mathbb{T}$. **We assume, throughout this section, that $\mathcal{A}$ contains at least one element from the interval** $\mathcal{I}^+ := \langle -0.25\,, (0)\,, 0.25\rangle$. We first produce some bounds for B and L and show that $\mathcal{A}$ contains a certain amount of well located elements in $\mathcal{I}^+$; we then use Lemma 3 and give further zones which are forbidden to elements from $\mathcal{A}$.

5.1 Due to the bounds (3) and (2), we have $5L < 9B$ and thus the intervals $\langle (L-B)/\ell, B/\ell\rangle$ and $\langle (L-B)/(\ell+1), B/(\ell+1)\rangle$ have a non trivial overlap for $\ell \geq 4$. By Lemma 2, and the trivial remark that 0 does not belong to $\mathcal{A}$, the set

$$(\langle 0\,, B/4\rangle \cup \langle (L-B)/3\,, B/3\rangle \cup \langle (L-B)/2\,, B/2\rangle \cup \langle (L-B)\,, B\rangle)^{sym} \quad (7)$$

contains no element from $\mathcal{A}$.

5.2 Let us now show that we have

$$B \leq 0.2571. \quad (8)$$

Indeed, if we have $B > 0.2571$, then, by (3) we have $L < 0.4189$ and thus the union $\langle 0\,, B/4\rangle \cup \langle (L-B)/3\,, B/3\rangle \cup \langle (L-B)/2\,, B/2\rangle$ is the interval $\langle 0\,, B/2\rangle$; since $B > 0.25$, all the elements from $\mathcal{A} \cap I^+$ must be in $(\langle B/2\,, L-B\rangle)^{sym}$. But the size of this non empty set is $2((L-B)-B/2) = 2(L-B)-B < 0.3236 - B$; however, by (4), the size of the set $\mathcal{A} \cap \mathcal{I}^+$ must be at least $0.324 - B$, leading to a contradiction.

5.3 By a similar argument, we give a lower bound for L, namely

$$L > 0.3982. \quad (9)$$

Let us assume that $L \leq 0.3982$; this and (2) imply $(L-B)/2 \leq 0.08 < B/3$. Thus, all the elements in $\mathcal{A} \cap \mathcal{I}^+$ are in $(\langle B/2\,,\,(L-B)\rangle \cup \langle B\,,\,0.25\rangle)^{sym}$ when $B \leq 0.25$, or in $\langle B/2\,,\,(L-B)\rangle^{sym}$ otherwise; in either case the size of $\mathcal{A} \cap \mathcal{I}^+$ is at most $2(0.25 - 0.2431 + (L-B) - B/2) = 0.0138 + 2L - 3B$, a quantity which is strictly less than $0.324 - B$, the minimal size for $\mathcal{A} \cap \mathcal{I}^+$ (cf. (4)).

5.4 We now prove

$$\text{size}(\langle B/2\,,\,L-B\rangle^{sym} \cap \mathcal{A}) \geq 0.0343, \tag{10}$$

by considering two cases, according as B is smaller or larger than 0.25.
In the first case, the size of the elements of $\mathcal{A} \cap \mathcal{I}^+$ which are not in $\langle B/2\,,\,L-B\rangle^{sym}$ is at most $2((L-B)/3 - B/4 + (L-B)/2 - B/3 + 0.25 - B)$; by keeping one B as such and using the bounds (2) and (3) for L and the other B's, our last expression is at most $0.2897 - B < A - B - 0.0343$, which, thanks to (4) leads to (10).
In the second case, we have $B > 0.25$; the first inequality in (3) then leads to $L < 0.426$; moreover, we have $B/4 > (L-B)/3$; thus, in this case, the size of the elements of $\mathcal{A} \cap \mathcal{I}^+$ which are not in $\langle B/2\,,\,L-B\rangle^{sym}$ is at most $\max(0, 2((L-B)/2 - B/3)) = \max(0, L - 2B/3 - B < 0.324 - B - 0.0343)$, which leads again to the validity of (10).

5.5 From (10), we deduce that, up to symmetry, the size of $\mathcal{A} \cap \langle B/2\,,\,L-B\rangle$ is larger than 0.0171. If $(L-B) - B/2 < 0.0514$, we immediately obtain the existence of two elements a_1 and a_2 in $\mathcal{A} \cap \langle B/2\,,\,L-B\rangle$ such that

$$0.0171 < \text{size}(\langle a_1\,,\,a_2\rangle) < 0.0514. \tag{11}$$

Let us now assume that $(L-B) - B/2 \geq 0.0514$; we can select a subset $\mathcal{K}$ of $\mathcal{A} \cap \langle B/2\,,\,L-B\rangle$ with size between 0.0171 and 0.01711, and by Lemma 5 (which was stated for integers but can readily be extended to short intervals in $\mathbb{Z}/p\mathbb{Z}$), we can find two elements a_1 and a_2 in $\mathcal{A} \cap \langle B/2\,,\,L-B\rangle$ such that $0.0171 < \text{size}(\langle a_1\,,\,a_2\rangle) < (L-B) - B/2 - 0.0171$. But, by (2) and (3) we have $(L-B) - B/2 < 0.06825$; this implies that the elements a_1 and a_2 satisfy (11).

By Lemma 3, if an element a in $\mathcal{A}$ is in $\langle B/2\,,\,L-B\rangle$, then the set $\langle 2a - (2B-L)\,,\,2a + (2B-L)\rangle^{sym}$ is free from elements from $\mathcal{A}$. Since $2 \text{x} 0.0514 < 0.1066 \leq 2\,(2B-L)$, the two intervals $\langle 2a_1 - (2B-L)\,,\,2a_1 + (2B-L)\rangle$ and $\langle 2a_2 - (2B-L)\,,\,2a_2 + (2B-L)\rangle$ overlap; thus, the set $(\langle 2a_1 - (2B-L)\,,\,2a_2 + (2B-L)\rangle)^{sym}$ contains no element from $\mathcal{A}$. Moreover, Relation (11) implies that the size of $\langle 2a_1 - (2B-L)\,,\,2a_2 + (2B-L)\rangle$ is at least $2 \times 0.0171 + 2(2B - L) \geq 0.1408$. Since $a_1 \leq (L - B) - 0.0171$, we have $2a_1 - (2B - L) \leq 0.2921$, and since $a_2 \geq B/2 + 0.0171$, we have $2a_2 + (2B - L) - 0.1408 \geq 3B/2 - L - 0.1408 + 0.0342 \geq 0.1898$. Letting $u = \max(2a_1 - (2B - L)\,,\, 0.1898)$, we have the following

$$\begin{aligned} &\text{for some } u \text{ with } 0.1898 \leq u \leq 0.2921, \\ &\text{the set } \langle u\,,\, u + 0.1408\rangle^{sym} \text{ contains no element from } \mathcal{A}. \end{aligned} \tag{12}$$

6 End of the proof of Theorem 1

We begin by showing in the next three subsections, that our assumption that $\mathcal{A}$ contains at least one element from the interval $\mathcal{I}^+$, defined as $\langle -0.25\,,\,(0)\,,\,0.25\rangle$, leads to a contradiction. We show indeed that there is no room in $\mathbb{Z}/p\mathbb{Z}$ for our interval $\mathcal{L}$; crucial facts concerning $\mathcal{L}$ is that it is not too small (by (9)), that its end-points are in $\mathcal{A}$ (by construction) and that it contains many elements of $\mathcal{A}$ around its ends (by Lemma 3). Theorem 1 is finally proved in the last subsection.

6.1 By the Cauchy-Davenport theorem, we have $\mathrm{card}(\mathcal{A} + (-\mathcal{A})) \geq 2\,\mathrm{card}\,\mathcal{A} - 1$ and so we have $\mathrm{size}\{\mathbb{Z}/p\mathbb{Z}\backslash(\mathcal{A}+(-\mathcal{A}))\} < 0.3521$. Moreover, the set $\mathbb{Z}/p\mathbb{Z}\backslash(\mathcal{A}+(-\mathcal{A}))$ is symmetric and contains $\mathcal{A}$ and thus it contains $\mathcal{B}$ as well as $\mathcal{B}^{sym}$; since $\mathcal{B}^{sym}$ is the disjoint union of $\mathcal{B} \cap (-\mathcal{B})$ and $(\mathcal{B}\backslash(-\mathcal{B}))^{sym}$, we have $\mathrm{size}(\mathcal{B} \cap (-\mathcal{B})) > 0.1341$. The interval $\mathcal{L}$ in $\mathbb{Z}/p\mathbb{Z}$ has a size which is at most 0.4329 (< 0.5) and contains at least $0.1341p$ symmetric elements: thus, either it contains $\langle -0.067\,,\,(0)\,,\,0.067\rangle$ or $\langle 0.433\,,\,(0.5)\,,\,0.567\rangle$.

Let us exclude the first case. Since $L > 0.3982$ (cf.(9)), $\mathcal{L}$ contains $\langle -0.067\,,\,0.25\rangle$, $\langle -0.14\,,\,0.14\rangle$ or $\langle -0.25\,,\,0.067\rangle$. But, by (7), (2) and (3), we see that the set
$(\langle 0\,,\,0.0607\rangle \cup \langle 0.0633\,,\,0.0810\rangle \cup \langle 0.0949\,,\,0.1215\rangle \cup \langle 0.1898\,,\,0.2431\rangle)^{sym}$
contains no element from $\mathcal{A}$. This readily implies that $\mathrm{size}(\mathcal{L}\backslash\mathcal{B}) \geq \mathrm{size}(\mathcal{L}\backslash\mathcal{A}) > 0.2 > 0.4329 - 0.2431 = L - B$, a contradiction. We thus have

$$\langle 0.433\,,\,(0.5)\,,\,0.567\rangle \subset \mathcal{L}. \tag{13}$$

6.2 Let us write $\mathcal{L} = \langle \ell_1\,,\,(0.5)\,,\,\ell_2\rangle$ with $0 < \ell_1 < 0.5 < \ell_2 < 1$. Recalling (12), we see that for no u with $0.1898 \leq u \leq 0.2921$ the interval $\mathcal{L}$ can contain all the symmetric set $\langle u\,,\,u + 0.1408\rangle^{sym}$, since otherwise it would contain too many points which are not in $\mathcal{A}$; but on the other hand, for no u the set $\mathcal{L}$ can avoid it completely, since otherwise $\mathcal{L}$ should be included in $\langle 0.33\,,\,0.67\rangle$, which is too short in view of (9). But the interval $\mathcal{L}$ has, by its definition, its end points in $\mathcal{A}$; this implies that for some u with $0.1898 \le u \le 0.2921$, $\mathcal{L}$ contains one, and only one, of the intervals $\langle u\,,\,u+0.1408\rangle$ or $-\langle u\,,\,u+0.1408\rangle$. Considering $-\mathcal{L}$ instead of $\mathcal{L}$ if necessary, we may assume without loss of generality that $\ell_1 \le 1-\ell_2$ and that for some u with $0.1898 \le u \le 0.2921$, $\mathcal{L}$ contains an interval $\langle u\,,\,u+0.1408\rangle$ free of elements from $\mathcal{A}$.

6.3 We now know that ℓ_1 has to be less than u. Let us first exclude the case when $B \le \ell_1 \le u$, which implies $u \ge B$. Since the size of $\mathcal{A}\cap\langle B/2\,,\,L-B\rangle$ is larger than 0.0174 (cf. the beginning of 5.5), there exists an element a of $\mathcal{A}$ in $\langle B/2+0.0174\,,\,L-B\rangle$ and *a fortiori* in $\langle 0.1386\,,\,0.1898\rangle$. This implies that $L-2a < 0.4329-2\text{x}0.1386 \le 0.1557$. By the first part of Lemma 3, the size of $\mathcal{A}\cap\langle \ell_1\,,\,\ell_1+L-2a\rangle$ is at least $B-a > 0.2431-0.1898 = 0.0533$. If $\ell_1+L-2a < u+0.1408$, then $\mathcal{A}\cap\langle \ell_1\,,\,\ell_1+L-2a\rangle$ is included in $\langle B\,,\,u\rangle$ and its size is at most $0.2921-0.2431 = 0.0490$, a contradiction. If $\ell_1+L-2a \ge u+0.1408$, then the "forbidden" interval $\langle u\,,\,u+0.1408\rangle$ is included in $\langle \ell_1\,,\,\ell_1+L-2a\rangle$ and the size of $\mathcal{A}\cap\langle \ell_1\,,\,\ell_1+L-2a\rangle$ is at most $0.1557-0.1408 = 0.0149$, leading again to a contradiction.

We now know that ℓ_1 is less than B and thus less than $L-B$. By (13) and (3), we have $\ell_1 \ge 0.567-L > 0.134$, so that ℓ_1 is an element from $\mathcal{A}\cap\langle B/2\,,\,L-B\rangle$. We may use Lemma 3, taking ℓ_1 itself as an element a; the interval $\langle \ell_1\,,\,L-\ell_1\rangle$ must contain at least $B-\ell_1$ elements from $\mathcal{A}$. Since $L-\ell_1 \ge L-B$, the interval $\langle \ell_1\,,\,L-\ell_1\rangle$ contains the "forbidden" interval $\langle L-B\,,\,B\rangle$; because of the other "forbidden" interval $\langle u\,,\,u+0.1408\rangle$, the interval $\langle \ell_1\,,\,L-\ell_1\rangle$ contains at most $u-B+(L-B)-\ell_1$ elements from $\mathcal{A}$; but we have, using (2) and (3): $u-B+(L-B)-\ell_1 < 0.2921+L-3B+(B-\ell_1) < B-\ell_1$, a final contradiction.

6.4 We have proved that $\mathcal{A}$ contains no element from $\mathcal{I}^+$. Let us denote by $\mathcal{L}$ the smallest interval that contains $\mathcal{A}$, this notation being consistent with our previous use of $\mathcal{L}$. The size of $\mathcal{L}$ is obviously at most $1/2$ and thus $L-A$ is less than 0.25. Arguing as in the beginning of Section 5, one shows that no element from $(\langle L-A\,,\,A\rangle)^{sym}$ is in $\mathcal{A}$; since $\mathcal{A}$ contains no element from $\langle -0.25\,,\,(0)\,,\,0,25\rangle$, we have proved that $\mathcal{A}$ is included in $\langle A\,,\,(0,5)\,,\,1-A\rangle$, which is Theorem 1.

References

[1] Cauchy, Augustin Louis, Recherches sur les nombres, J. École Polytechnique 9 (1813), 99–116.

[2] Freiman, Gregory A., Inverse problems of additive number theory, VI. On the addition of finite sets, III. Izv. Vysš. Učebn. Zaved. Matematika 28 (1962), 151–157.

[3] Freiman, Gregory A., Foundations of a structural theory of set addition. Translations of mathematical monographs, v. 37, AMS, Providence (RI), 1973, vii+108 pp.

[4] Lev, Vsevolod F., Distribution of points on arcs, INTEGERS: The Electronic Journal of Combinatorial Number Theory 5 (2) (2005), ♯A11.

[5] Lev, Vsevolod F., Large sum-free sets in $\mathbb{Z}/p\mathbb{Z}$, Israel Journal of Mathematics (to appear).

[6] Nathanson, Melvyn B., Additive number theory: inverse problems and the geometry of sumsets, Graduate Texts in Mathematics 165, Springer, New York (NY), 1996, xiv+293 pp.

Jean-Marc Deshouillers
Équipe de Statistique Mathématique et Applications, EA 2961
Université Victor Segalen Bordeaux 2
33076 BORDEAUX Cedex (France)
et
A2X, UMR 5465
Université Bordeaux 1 et CNRS
33405 TALENCE Cedex (France)
jean-marc.deshouillers@math.u-bordeaux1.fr

Gregory A. Freiman
Tel Aviv University
Usha 11
Ramat Aviv
TEL AVIV (Israel)
grisha@post.tau.ac.il