ANNALES

DE

L'INSTITUT FOURIER

Oriol SERRA & Gilles ZÉMOR

Large sets with small doubling modulo p are well covered by an arithmetic progression

Tome 59, nº 5 (2009), p. 2043-2060.

<http://aif.cedram.org/item?id=AIF_2009__59_5_2043_0>

Ann. Inst. Fourier, Grenoble
59, 5 (2009) 2043-2060

LARGE SETS WITH SMALL DOUBLING MODULO p ARE WELL COVERED BY AN ARITHMETIC PROGRESSION

by Oriol SERRA & Gilles ZÉMOR (*)

ABSTRACT. — We prove that there is a small but fixed positive integer ϵ such that for every prime p larger than a fixed integer, every subset S of the integers modulo p which satisfies $|2S| \leqslant (2+\epsilon)|S|$ and $2(|2S|) - 2|S| + 3 \leqslant p$ is contained in an arithmetic progression of length $|2S| - |S| + 1$. This is the first result of this nature which places no unnecessary restrictions on the size of S.

RÉSUMÉ. — Nous démontrons qu'il existe un entier strictement positif ϵ, petit mais fixé, tel que pour tout nombre premier p plus grand qu'un entier fixé, tout sous-ensemble S des entiers modulo p qui vérifie $|2S| \leqslant (2+\epsilon)|S|$ et $2(|2S|)-2|S|+3 \leqslant p$ est contenu dans une progression arithmétique de longueur $|2S| - |S| + 1$. Il s'agit du premier résultat de cette nature qui ne contraint pas inutilement le cardinal de S.

1. Introduction

In 1959 Freiman [2] proved that if S is a set of integers such that

$$|2S| \leqslant 3|S| - 4$$

then S is contained in an arithmetic progression of length $|2S| - |S| + 1$.

This result is often known as Freiman's $(3k-4)$–Theorem. It has been conjectured that the same result also holds in the finite groups $\mathbb{Z}/p\mathbb{Z}$ of prime order. Working towards this conjecture, Freiman [3] proved (see also [4] and Nathanson [14] for the following formulation of the result):

Keywords: Sumset, arithmetic progression, additive combinatorics.
Math. classification: 11P70.
(*) Supported by the Spanish Ministry of Science under project MTM2008-06620-C03-01.

Theorem 1.1 (Freiman [3]). — *Let $S \subset \mathbb{Z}/p\mathbb{Z}$ such that $3 \leqslant |S| \leqslant c_0 p$ and*

$$|2S| \leqslant c_1|S| - 3,$$

with $0 < c_0 \leqslant 1/12$, $c_1 > 2$ and $(2c_1 - 3)/3 < (1 - c_0c_1)/c_1^{1/2}$. Then S is contained in an arithmetic progression of length $|2S| - |S| + 1$.

The largest possible numerical value of c_1 given by this theorem is $c_1 \approx 2.45$, which falls somewhat short of the value predicted by the conjecture (namely 3). In addition, Theorem 1.1 only guarantees the result for sets S that are small enough. For example, to guarantee $c_1 = 2.4$, the theorem needs the assumption $|S| \leqslant p/35$. This last assumption was improved to $|S| \leqslant p/10.7$ by Rødseth [15] but without improving the value of the constant c_1.

It follows from a recent result of Green and Rusza [5] on rectification of sets with small doubling in $\mathbb{Z}/p\mathbb{Z}$ that the value of c_1 can actually be pushed all the way to 3 while preserving the conclusion that S is contained in a short arithmetic progression, but this comes at the expense of a stringent condition on the size of S: namely the extra assumption $|S| < 10^{-180}p$.

In the present paper, we shall work at the conjecture from a different direction. Rather than focusing on the best possible value for the constant c_1, we shall try to lift all restrictions on the size of S. First we need to formulate properly what should be the right version of Freiman's $(3k-4)$–Theorem in $\mathbb{Z}/p\mathbb{Z}$.

For $-1 \leqslant m \leqslant |S| - 4$, we want the condition $|2S| = 2|S| + m$ to imply that S is included in an arithmetic progression of length $|S| + m + 1$. One fact that has not been spelt out explicitly in the literature is that for such a result to hold, some lower bound on the size of the *complement* $\mathbb{Z}/p\mathbb{Z} \setminus 2S$ of $2S$ must be formulated. Indeed, if $p - |2S|$ is too small, the conclusion will not hold even if m is small compared to $|S| - 4$. Consider in particular the following example. Let $S = \{0\} \cup \{m+3, m+4, \ldots, (p+1)/2\}$. We have $|2S| = p - (m+1) = 2|S| + m$, but straightforward counting shows that for fixed m and sufficiently large p any arithmetic progression of difference $d \neq 1$ that contains S must contain approximately $p/2$ elements not in S, hence S is not included in an arithmetic progression of length $|S| + m + 1$. For the desired result to hold, we must therefore add the condition $p - |2S| > m + 1$. We conjecture that this extra condition is sufficient for a $\mathbb{Z}/p\mathbb{Z}$-version of Freiman's $(3k-4)$–Theorem to hold. More precisely:

CONJECTURE 1.2. — *Let $S \subset \mathbb{Z}/p\mathbb{Z}$ and let $m = |2S| - 2|S|$. Suppose that m satisfies:*

$$-1 \leqslant m \leqslant \min\{|S| - 4, p - |2S| - 3\}.$$

Then S is included in an arithmetic progression of length $|S| + m + 1$.

Note that $p - |2S| = p - 2|S| - m$ can not be equal to $m + 2$, otherwise p would be an even number. Therefore the condition $m \leqslant p - |2S| - 3$ of the conjecture is equivalent to $p - |2S| > m + 1$ which is a necessary lower bound on $p - |2S|$, as the example above shows.

We remark that the cases $m = -1, 0, 1$ of this conjecture are known. They are implied by Vosper's theorem [19] ($m = -1$), by a result of Hamidoune and Rødseth [10] ($m = 0$) and by a result of Hamidoune and the present authors [11] ($m = 1$). In the present paper we shall prove conjecture 1.2 for all values of m up to $\epsilon|S|$, where ϵ is a fixed absolute constant. More precisely, our main result is:

THEOREM 1.3. — *There exist positive numbers p_0 and ϵ such that, for all primes $p > p_0$, any subset S of $\mathbb{Z}/p\mathbb{Z}$ such that*

(i) $|2S| < (2 + \epsilon)|S|$,

(ii) $m = |2S| - 2|S|$ *satisfies* $m \leqslant \min\{|S| - 4, p - |2S| - 3\}$,

is included in an arithmetic progression of length $|S| + m + 1$.

We shall prove this result with the numerical values $\epsilon = 10^{-4}$ and $p_0 = 2^{94}$.

In the past, the dominant strategy, already present in Freiman's original proof of Theorem 1.1, has been to *rectify* the set S, *i.e.*, find an argument that enables one to claim that the sum $S+S$ must behave as in $\mathbb{Z}$, and then apply Freiman's $(3k-4)$–Theorem. Rectifying S directly however, becomes more and more difficult when the size of S grows, hence the different upper bounds on S that one regularly encounters in the literature. In our case, without any upper bound on S, rectifying S by studying its structure directly is a difficult challenge. Our method will be indirect. Our strategy is to use an auxiliary set A that minimizes the difference $|S + A| - |S|$ among all sets such that $|A| \geqslant m+3$ and $|S + A| \leqslant p-(m+3)$. The set A is called an $(m + 3)$-atom of S and using such sets to derive properties of S is an instance of the isoperimetric (or atomic) method in additive number theory which was introduced by Hamidoune and developed in [6, 7, 8, 9, 17, 11, 12]. The point of introducing the set A is that we shall manage to prove that it is both significantly smaller than S and also has a small sumset $2A$. This will enable us to show that first the sum $A + A$, and then the sum $S + A$, must behave as in $\mathbb{Z}$. Finally we will use Lev and Smelianski's distinct set version [13] of Freiman's $(3k-4)$–Theorem to conclude.

The paper is organised as follows. The next section will introduce k-atoms and their properties that are relevant to our purposes. In Section 3 we will show how our method works proving Theorem 1.3 in the relatively easy case when m is an arbitrary constant or a slowly growing function of p (*i.e.*, $\log p$). In Section 4 we will prove Theorem 1.3 in full when m is a linear function of $|S|$.

2. Atoms

Let S be a subset of $\mathbb{Z}/p\mathbb{Z}$ such that $0 \in S$. For a positive integer k, we shall say that S is *k-separable* if there exists $X \subset \mathbb{Z}/p\mathbb{Z}$ such that $|X| \geqslant k$ and $|X+S| \leqslant p-k$.

Suppose that S is k-separable. The k-th *isoperimetric number* of S is then defined by

(2.1)

$$\kappa_k(S) = \min\{|X+S| - |X|, \mid \; X \subset \mathbb{Z}/p\mathbb{Z},\ |X| \geqslant k \text{ and } |X+S| \leqslant p-k\}.$$

For a k-separable set S, a subset X achieving the above minimum is called a *k-fragment* of S. A k-fragment with minimal cardinality is called a *k-atom*.

What makes k-atoms interesting objects is the following lemma:

Lemma 2.1 (The intersection property [7]). — *Let S be a subset of $\mathbb{Z}/p\mathbb{Z}$ such that $0 \in S$, and suppose S is k-separable. Let A be a k-atom of S. Let F be a k-fragment of S such that $A \not\subset F$. Then $|A \cap F| \leqslant k-1$.*

The following Lemma follows from [9, Theorem 6.1], see also [12]:

Lemma 2.2. — *Let $S \subset \mathbb{Z}/p\mathbb{Z}$ with $|S| \geqslant 3$ and $0 \in S$. Suppose S is 2-separable and $\kappa_2(S) \leqslant |S|+m$. Let A be a 2–atom of S. Then $|A| \leqslant m+3$.*

Lemma 2.2 implies the following upper bound on the size of atoms.

Lemma 2.3. — *Let $k \geqslant 3$ and let A be a k–atom of a k–separable set $S \subset \mathbb{Z}/p\mathbb{Z}$ with $0 \in S$, $|S| \geqslant 2$ and $\kappa_k(S) \leqslant |S|+m$. Then $|A| \leqslant 2m+k+2$.*

Proof. — The set A is clearly 2–separable. Let B be a 2–atom of A with $0 \in B$, so that $|B+A| \leqslant |B|+|A|+m$. Let $b \in B$, $b \neq 0$. By Lemma 2.2 we have $|B| \leqslant m+3$. Therefore,

$$|A \cup (b+A)| = |\{0,b\}+A| \leqslant |B+A| \leqslant |A|+2m+3. \qquad (2.2)$$

But $b+A$ is also a k–atom of S. By the intersection property, it follows that $|A\cap(b+A)|\leqslant k-1$. Hence $2|A|-(k-1)\leqslant|A\cup(b+A)|$ which together with (2.2) gives the result. □

From now on S will refer to a subset of $\mathbb{Z}/p\mathbb{Z}$ satisfying conditions (i) and (ii) of Theorem 1.3 for a fixed $\epsilon>0$ to be determined later, and m always denotes the integer $m=|2S|-|S|$. Without loss of generality we will also assume $0\in S$.

Note that condition (ii) implies that S is $(m+3)$–separable so that $(m+3)$-atoms of S exist. Note that by the definition of an atom, if X is an atom of S then so is $x+X$ for any $x\in\mathbb{Z}/p\mathbb{Z}$. Therefore there are atoms containing the zero element.

In the sequel A will denote an $(m+3)$–atom of S with $0\in A$. We will regularly call upon the following two inequalities:

$$|S+A|\leqslant|S|+|A|+m \tag{2.3}$$

which follows from the definition of an atom, and

$$|A|\leqslant 3m+5. \tag{2.4}$$

which follows from Lemma 2.3 with $k=m+3$.

The reader should also bear in mind that for all practical purposes, inequality (2.4) means that we will only be dealing with cases when $|A|$ is significantly smaller than $|S|$. Indeed, we shall prove Theorem 1.3 for a small value of ϵ, namely $\epsilon=10^{-4}$, so that $3m$ is very much smaller than $|S|$. We can also freely assume that $|S|\geqslant p/35$, since otherwise Freiman's Theorem 1.1 gives the result with $\epsilon=0.4$. The prime p will also be assumed to be larger than some fixed value p_0 to be determined later.

3. The case $m\leqslant\log p$

In this section we will deal with the case when m is a very small quantity, *i.e.,* smaller than a logarithmic function of p. This will allow us to introduce, without technical difficulties to hinder us, the general idea of the method which is to first show that A must be contained in a short arithmetic progression and then to transfer the structure of A to the larger set S. It will also serve the additional purpose of allowing us to suppose $m\geqslant 6$ when we switch to the looser condition $m\leqslant\epsilon|S|$.

We start by stating some results that we shall call upon. The first is a generalization of Freiman's Theorem in $\mathbb{Z}$ to sums of different sets and is proved by Lev and Smelianski in [13], we give it here somewhat reworded (see also [14, Th. 4.8], or [18, Th. 5.12] for a slightly weaker version).

Theorem 3.1 (Lev and Smelianski [13]). — *Let X and Y be two non-empty finite sets of integers with*

$$|X+Y| = |X| + |Y| + \mu.$$

Assume that $\mu \leqslant \min\{|X|, |Y|\} - 3$ and that one of the two sets X, Y has size at least $\mu + 4$. Then X is contained in an arithmetic progression of length $|X| + \mu + 1$ and Y is contained in an arithmetic progression of length $|Y| + \mu + 1$.

The second result we shall use is due to Bilu, Lev and Ruzsa [1, Theorem 3.1][(1)] and gives a bound on the length of small sets in $\mathbb{Z}/p\mathbb{Z}$. By the *length* $\ell(X)$ of a set $X \subset \mathbb{Z}/p\mathbb{Z}$ we mean the length (cardinality) of the shortest arithmetic progression which contains X.

Theorem 3.2 (Bilu, Lev, Ruzsa [1]). — *Let $X \subset \mathbb{Z}/p\mathbb{Z}$ with $|X| \leqslant \log_4 p$. Then $\ell(X) < p/2$.*

Theorem 3.2 will be used to show that, when m is small enough, then the atom A is contained in a short arithmetic progression.

Lemma 3.3. — *Suppose that $6m + 11 \leqslant \log_4 p$. Then A is contained in an arithmetic progression of length $2(|A| - 1)$.*

Proof. — Since we assume $|S| \geqslant p/35$, it follows from (2.3) and (2.4) that A is an $(m+4)$–separable set. Let therefore B be an $(m+4)$–atom of A containing 0, so that $|B + A| \leqslant |B| + |A| + m$. By Lemma 2.3 we have $|B| \leqslant 3m + 6$ so that $|A \cup B| \leqslant 6m + 11$. By the present lemma's hypothesis, it follows from Theorem 3.2 that $A \cup B$ is contained in an arithmetic progression of length less than $p/2$. The sum $A+B$ can therefore be considered as a sum of integers, so that Theorem 3.1 applies and A is contained in an arithmetic progression of length $|A|+m+1 \leqslant 2|A|-2$. □

We now proceed to deduce from Lemma 3.3 the structure of S. It will be convenient to introduce the following notation.

Recall that we denote by $\ell(X)$ the length of the smallest arithmetic progression containing X. By $\ell_X(Y)$ we shall denote the length of a smallest arithmetic progression of difference x containing Y, where x is the difference of a shortest arithmetic progression containing X.

The point of the above definition is that if we have $\ell_A(S) + \ell(A) \leqslant p$ then the sum $S + A$ can be considered as a sum in $\mathbb{Z}$, so that (2.3) and Theorem 3.1 applied to S and A imply Theorem 1.3. We summarize this point in the next Lemma for future reference.

(1) In [1] their statement is slightly different from Theorem 3.2, but this is actually what they prove.

LEMMA 3.4. — *If $\ell_A(S) + \ell(A) \leqslant p$ then Theorem 1.3 holds.*

Whenever we will wish transfer the structure of A to S we will assume that $\ell_A(S) + \ell(A) > p$ and look for a contradiction. We can think of this hypothesis as S having no 'holes' of length $\ell(A)$. In the present case of very small m, the desired result on S follows with very little effort.

LEMMA 3.5. — *Suppose that $6m + 11 \leqslant \log_4 p$. Then S is contained in an arithmetic progression of length $|S| + m + 1$.*

Proof. — By Lemma 3.3, A is contained in an arithmetic progression of difference r, that we can assume to equal $r = 1$, and of length $2(|A| - 1)$. In particular A has two consecutive elements. Without loss of generality we may replace A by a translate of A and assume that $\{0, 1\} \subset A$. Let $S = S_1 \cup \cdots \cup S_k$ be the decomposition of S into maximal arithmetic progressions of difference 1, so that

$$|S + A| \geqslant |S| + k.$$

Because of (2.3) we have $k \leqslant |A| + m$. By Lemma 3.4 we can assume every maximal arithmetic progression in the complement of S to have length at most $\ell(A)$. Therefore,

$$\ell_A(S) + \ell(A) \leqslant |S| + k\ell(A) \leqslant |S| + (|A| + m)2(|A| - 1).$$

Now by (2.4) we get

$$\ell_A(S) + \ell(A) \leqslant |S| + (4m + 5)(6m + 8) < |S| + (\log_4 p)^2 < \frac{p}{2} + (\log_4 p)^2$$

since $|S| < p/2$. We have $\log_4^2 p < p/2$ for all p therefore we get $\ell_A(S) + \ell(A) < p$, a contradiction. □

4. The general case

4.1. Overview

When m grows we encounter two difficulties. First, Theorem 3.2 will not apply anymore to any set containing A, and we need an alternative method to argue that A is contained in a short arithmetic progression. Second, even if we do manage to prove that A is contained in a short arithmetic progression, we will not be able to deduce the structure of S from (2.3) by the simple technique of the preceding section.

We will now use an extra tool, namely the Plünecke-Ruzsa estimates for sumsets; see *e.g.* [16, 14].

Theorem 4.1 (Plünecke-Ruzsa [16]). — *Let S and T be finite subsets of an abelian group with $|S+T| \leqslant c|S|$. There is a nonempty subset $S' \subset S$ such that*

$$|S' + jT| \leqslant c^j|S'|.$$

The Plünecke-Ruzsa inequalities applied to S and A will give us that there exists a positive δ such that either A is contained in a progression of length $(2-\delta)(|A|-1)$ or $2A$ is contained in an arithmetic progression of length $(2-\delta)(|2A|-1)$ (Lemma 4.4). We will then proceed to transfer the structure of A or $2A$ to S.

Again we shall use Lemma 3.4 to assume that S does not contain a "gap" of length $\ell(A)$ or $\ell(2A)$. We define the density of a set $X \subset \mathbb{Z}/p\mathbb{Z}$ as $\rho(X) = (|X|-1)/\ell(X)$. If $\ell(A) \leqslant (2-\delta)(|A|-1)$ we will argue that the sum $S+A$ must have a *density* at least that of A and get a contradiction with the upper bound on $|S+A|$. The details will be given in Subsection 4.3.

We will not be quite done however, because we can not guarantee that $\ell(A) \leqslant (2-\delta)(|A|-1)$ holds. In that case we have to fall back on the condition $\ell(2A) \leqslant (2-\delta)(|2A|-1)$, meaning that it is the set $2A$, rather than A, that has large enough density. In this case we have to work a little harder. We proceed in two steps: we first apply the Plünecke-Ruzsa inequalities again to show that there exists a *large* subset T of S such that $|T+2A|$ is small. We then apply the density argument to show that T must be contained in an arithmetic progression with few missing elements. We then focus on the remaining elements of S, *i.e.*, the set $S \setminus T$. We will again argue that if this set has a gap of length $\ell(A)$ the desired result holds and otherwise the density argument will give us that $S+A$ is too large. This analysis is detailed in Subsection 4.4 and will conclude our proof of Theorem 1.3.

4.2. Structure of A

Lemma 4.2. — *Suppose $6 \leqslant m \leqslant \epsilon|S|$ with $\epsilon \leqslant 10^{-4}$. Then for any positive integer $k \leqslant 32$ we have*

$$|kA| \leqslant k(|A|+m)\left(1+\frac{5k\epsilon}{2}\right)+1.$$

Proof. — Rewrite (2.3) as

$$|S+A| \leqslant |S|+|A|+m = c|S|,$$

with $c = 1 + \frac{|A|+m}{|S|}$. By Theorem 4.1 (Plünecke–Ruzsa), for each k there is a subset $S' = S'(k)$ such that

$$|S' + kA| \leqslant c^k |S'|. \tag{4.1}$$

Apply (2.4) and $m \geqslant 6$ to get $|A| \leqslant 3m + 5 \leqslant 4m$. Since $m \leqslant \epsilon|S|$ we obtain for the constant c just defined $c \leqslant 1 + 5\epsilon$. We clearly have

$$c^k|S'| \leqslant c^k|S| \leqslant (1+5\epsilon)^k|S| < 2|S| < p$$

for $k \leqslant 32$. Now apply the Cauchy-Davenport Theorem to $S' + kA$ in (4.1) to obtain $|S'| + |kA| - 1 \leqslant c^k|S'|$, from which

$$|kA| \leqslant (c^k - 1)|S'| + 1 \leqslant (c^k - 1)|S| + 1. \tag{4.2}$$

Numerical computations give that

$$(1+x)^k \leqslant 1 + kx + \frac{k^2}{2}x^2$$

for any positive real number $x \leqslant 5.10^{-4}$ and for $k \leqslant 32$. Hence, since $c = 1 + (|A|+m)/|S| \leqslant 1 + 5\epsilon$, we can write, for $k \leqslant 32$,

$$c^k = \left(1 + \frac{|A|+m}{|S|}\right)^k \leqslant 1 + k\frac{|A|+m}{|S|} + \frac{k^2}{2}\left(\frac{|A|+m}{|S|}\right)^2.$$

Applied to (4.2) we get

$$\begin{aligned} |kA| &\leqslant k(|A|+m) + \frac{k^2}{2}\left(\frac{(|A|+m)^2}{|S|}\right) + 1 \\ &\leqslant k(|A|+m)\left(1 + \frac{k}{2}\frac{(|A|+m)}{|S|}\right) + 1 \\ &\leqslant k(|A|+m)\left(1 + \frac{5k\epsilon}{2}\right) + 1, \end{aligned}$$

as claimed. □

Lemma 4.3. — *If $6 \leqslant m \leqslant \epsilon|S|$ with $\epsilon \leqslant 10^{-4}$, then A and $2A$ are contained in an arithmetic progression of length less than $p/2$.*

Proof. — Put $k = 2^j$ and $c_1 = 2.44$. Suppose that $|2^jA| \geqslant c_1|2^{j-1}A| - 3$ for each $1 \leqslant j \leqslant 5$. Then,

$$|32A| \geqslant c_1^5|A| - 3(c_1^5 - 1)/(c_1 - 1) \geqslant 86|A| - 179 \geqslant 65|A| + 10,$$

where in the last inequality we have used $|A| \geqslant m + 3 \geqslant 9$. On the other hand, by Lemma 4.2, we have

$$|kA| \leqslant k(|A|+m)\left(1 + \frac{5k\epsilon}{2}\right) + 1 \leqslant 2k(1 + \frac{5k\epsilon}{2})|A|, \tag{4.3}$$

which, for $k = 32$, gives $|32A| \leqslant 64(1+80\epsilon)|A| \leqslant 65|A|$, a contradiction.

Hence $|2^j A| \leqslant c_1|2^{j-1}A| - 3$ for some $1 \leqslant j \leqslant 5$. Since

$$|2^{j-1}A| \leqslant |16A| \leqslant 32(1+40\epsilon)|A| \leqslant 64(1+40\epsilon)\epsilon p < 8 \cdot 10^{-3}p,$$

where again we have used inequality (4.3) for $k = 16$ and $|A| \leqslant 4m \leqslant 4\epsilon|S| \leqslant 2\epsilon p$. It follows from Freiman's Theorem 1.1 (with $c_0 = 8 \cdot 10^{-3}$ and $c_1 = 2.44$) that $A \subset 2^{j-1}A$ is contained in an arithmetic progression of length at most

$$|2^j A| - |2^{j-1}A| + 1 < 1.44|2^{j-1}A| \leqslant (1.44)8 \cdot 10^{-3}p.$$

In particular, A and $2A$ are included in arithmetic progressions of lengths less than $p/2$. □

Now that we know that A and $2A$ are contained in an arithmetic progression of length smaller than $p/2$, we can apply to them the Freiman's $(3k-4)$–Theorem to get the following result.

Lemma 4.4. — *Suppose $6 \leqslant m \leqslant \epsilon|S|$ with $\epsilon \leqslant 10^{-4}$, and let $0 < \delta \leqslant 10^{-1}$. If A is* not *contained in an arithmetic progression of length $(2-\delta)(|A|-1)$ then $2A$ is contained in an arithmetic progression of length $(2-\delta)(|2A|-1)$.*

Proof. — Suppose first that $|2A| \geqslant (3-\delta)(|A|-1)$ and $|4A| \geqslant (3-\delta)(|2A|-1)$. Then

$$|4A| \geqslant (3-\delta)^2|A| - (3-\delta)^2 - (3-\delta) \geqslant (3-\delta)^2|A| - 12. \tag{4.4}$$

On the other hand, Lemma 4.2 for $k = 4$ and $\epsilon = 10^{-4}$ gives $|4A| \leqslant 4(1+10\epsilon)(|A|+m)+1$. By using (4.4) and $m \leqslant |A|-3$ we get

$$(3-\delta)^2|A| - 12 \leqslant 8(1+10\epsilon)|A| - 12(1+10\epsilon) + 1.$$

Since $m \geqslant 6$, we have $|A| \geqslant m+3 \geqslant 9$. Therefore we obtain

$$(3-\delta)^2|A| < \left(8(1+10\epsilon) + \frac{1}{9}\right)|A|,$$

a contradiction for $\delta \leqslant 0.1$.

Hence,

(a) either $|2A| < (3-\delta)(|A|-1) < 3|A|-3$, but since $\ell(A) < p/2$ by Lemma 4.3, Freiman's $(3k-4)$–Theorem applies and A is contained in an arithmetic progression of length $|2A|-(|A|-1) \leqslant (2-\delta)(|A|-1)$.

(b) Or $|4A| < (3-\delta)(|2A|-1) < 3|2A|-3$, but using Lemma 4.3 again, Freiman's $(3k-4)$–Theorem implies that $2A$ is contained in an arithmetic progression of length $(2-\delta)(|2A|-1)$.

□

4.3. Structure of S when $\ell(A)$ is small.

For a subset $B \subset \mathbb{Z}/p\mathbb{Z}$ define the *density* of B by

$$\rho B = \frac{|B| - 1}{\ell(B)}.$$

The next lemma gives a lower bound for the cardinality of a sumset of two subsets $B, C \in \mathbb{Z}/p\mathbb{Z}$ when $\ell(B) + \ell(C) > p$ in terms of their densities. In the statement, by an interval $[a, b)$ in $\mathbb{Z}_p$ we mean the set $\{a, a+1, \ldots, b-1\}$.

LEMMA 4.5. — *Let $0 \in C \subset \mathbb{Z}/p\mathbb{Z}$ with $C \subset [0, \ell(C))$ and $\ell(C) < p/2$. Let $I_1, \ldots, I_i, \ldots, I_{2t}$ be the sequence of intervals defined by $I_i = [(i-1)c, ic)$, where $c = \ell(C)$ and $t < p/2c$. Let $B \subset \mathbb{Z}/p\mathbb{Z}$ such that for every $i = 1, \ldots, 2t$, we have $I_i \cap B \neq \emptyset$. Then,*

$$|B + C| \geqslant |B \cup [(B + C) \cap I]| \geqslant |B| + (t - \frac{1}{2})\ell(C)\left(\rho C - \frac{|B \cap I|}{(2t-1)c}\right),$$

where $I = I_1 \cup \ldots \cup I_{2t}$.

Proof. — Let $B' = B \cap I$. Let $B_0^i = B' \cap I_{2i-1}$ and $B_1^i = B' \cap I_{2i}$ and define $B_0' = \bigcup_{i=1}^t B_0^i$, $B_1' = \bigcup_{i=1}^t B_1^i$ so that $B' = B_0' \cup B_1'$. Note that, since $C \subset [0, c)$,

$$(B_0^i + C) \cap (B_0^j + C) = \emptyset$$

for $i \neq j$ and that $B_0^i + C \subset I_{2i-1} \cup I_{2i}$. Therefore $B_0' + C$ can be written as the following union of disjoint sets.

$$B_0' + C = \bigcup_{i=1}^{t} (B_0^i + C) \subset I_1 \cup \ldots \cup I_{2t}.$$

Hence, since every set B_0^i is nonempty, the Cauchy-Davenport Theorem implies

$$|B_0' + C| \geqslant |B_0'| + t(|C| - 1). \tag{4.5}$$

In a similar manner we have

$$\begin{aligned}(B_1' + C) \cap I &= \bigcup_{i=1}^{t-1} (B_1^i + C) \ \cup \ (B_1^{2t} + C) \cap I \\ &\supset \bigcup_{i=1}^{t-1} (B_1^i + C) \ \cup B_1^{2t}\end{aligned}$$

so that, applying the Cauchy-Davenport Theorem for $i = 1 \ldots t-1$, we get

$$|(B_1' + C) \cap I| \geqslant |B_1'| + (t-1)(|C| - 1). \tag{4.6}$$

Now we have $|B+C| \geqslant |B\setminus B'| + |(B'_0+C)\cap I|$ and likewise $|B+C| \geqslant |B\setminus B'| + |(B'_1+C)\cap I|$, hence, applying (4.5) and (4.6),

$$\begin{aligned}|B+C| &\geqslant |B\setminus B'| + \frac{1}{2}\left(|(B'_0+C)\cap I| + |(B'_1+C)\cap I|\right)\\ &\geqslant |B| - |B'|/2 + (t-\frac{1}{2})(|C|-1)\\ &\geqslant |B| + (t-\frac{1}{2})c\left(\rho C - \frac{|B'|}{(2t-1)c}\right)\end{aligned}$$

which proves the result. □

Lemma 4.5 allows us to conclude the proof when the $(m+3)$–atom A is contained in a short arithmetic progression.

Lemma 4.6. — *Suppose $6 \leqslant m \leqslant \epsilon|S|$ with $\epsilon \leqslant 10^{-4}$. Suppose furthermore that $\ell(A) \leqslant (2-\delta)(|A|-1)$. Then $\ell(S) \leqslant |S|+m+1$.*

Proof. — Set $a = \ell(A)$. Write $p = 2ta + r$, $0 < r < 2a$ and partition $[0, 2ta)$ into the union of intervals $I_1, \dots, I_i, \dots, I_{2t}$, where we denote $I_i = [(i-1)a, ia)$. Let $I = \cup_{i=1}^{2t} I_i = [0, 2ta)$ and $S' = S \cap I$.

Suppose that $\ell_A(S) + \ell(A) > p$. Then we have $I_i \cap S' \neq \emptyset$ for each $i = 1, \dots 2t$. By Lemma 4.5 with $B = S$ and $C = A$,

$$|S+A| \geqslant |S| + (t-\frac{1}{2})a\left(\rho A - \frac{|S'|}{(2t-1)a}\right). \tag{4.7}$$

Now we have $(2t-1)a > p - 3a$ by definition of t. Since $|A| \leqslant 3m+5$ we have $a = \ell(A) \leqslant 2(|A|-1) \leqslant 6m+8$, and since we have supposed $m \geqslant 6$, we get $a \leqslant 8m$. We therefore have

$$(2t-1)a > p - 3a \geqslant p - 24m > (1-12\epsilon)p. \tag{4.8}$$

By the hypothesis of the Lemma we have $\rho A \geqslant 1/(2-\delta)$. Together with (4.8) we get, writing $|S'| \leqslant |S| < p/2$,

$$\rho A - \frac{|S'|}{(2t-1)a} > \frac{1}{2-\delta} - \frac{1}{2-24\epsilon}.$$

Finally, applying again (4.8), inequality (4.7) becomes

$$|S+A| > |S| + \frac{p}{2}(1-12\epsilon)\left(\frac{1}{2-\delta} - \frac{1}{2-24\epsilon}\right). \tag{4.9}$$

Now recall that by definition of A we have $|A| \geqslant m+3$. We will therefore get that (4.9) contradicts (2.3) whenever the righthand side of (4.9) is greater than $|S|+2|A|$. Since $|A| \leqslant 3m+5 \leqslant 4m \leqslant 2\epsilon p$, a contradiction is obtained whenever

$$\frac{1}{2}(1-12\epsilon)\left(\frac{1}{2-\delta}-\frac{1}{2-24\epsilon}\right) \geqslant 4\epsilon. \tag{4.10}$$

For $\epsilon \leqslant 10^{-4}$ the inequality (4.10) is verified for every $\delta > 5\cdot 10^{-3}$. Since Lemma 4.4 allows us to choose δ up to the value 10^{-1}, the hypothesis $\ell_A(S)+\ell(A) > p$ can not hold, so that the result follows from Lemma 3.4. □

4.4. Structure of S when $\ell(2A)$ is small.

To conclude the proof of Theorem 1.3 it remains to consider the case where $\ell(A) > (2-\delta)(|A|-1)$. We break up the proof into several lemmas.

LEMMA 4.7. — *Suppose $6 \leqslant m \leqslant \epsilon|S|$ with $\epsilon \leqslant 10^{-4}$. Suppose furthermore that $\ell(A) > (2-\delta)(|A|-1)$. Then*

(i) $|2A| \geqslant (3-\delta)(|A|-1)$.
(ii) $\ell(A) \leqslant (1-\delta/2)|2A|$.

Proof. — By point (a) of the final argument in the proof of Lemma 4.4 we know that we can not have $|2A| < (3-\delta)(|A|-1)$. This proves (i).

Since A is contained in an arithmetic progression of length less than $p/2$ (Lemma 4.3) we have $\ell(A) \leqslant (\ell(2A)+1)/2$. Now Lemma 4.4 implies $\ell(2A) \leqslant (2-\delta)(|2A|-1)$, hence $(\ell(2A)+1)/2 \leqslant (1-\delta/2)|2A|$. This proves (ii). □

Next we apply the Plünecke-Ruzsa inequalities to exhibit a subset T of S that sums to a small sumset with $2A$. We then show that this set T must be contained in an arithmetic progression with few missing elements.

LEMMA 4.8. — *Suppose $6 \leqslant m \leqslant \epsilon|S|$ with $\epsilon \leqslant 10^{-4}$. Suppose furthermore that $\ell(A) > (2-\delta)(|A|-1)$. Then there exists $T \subset S$ such that, denoting $\lambda = |T|/|S|$,*

$$|2A| \leqslant \lambda(4+10\epsilon)(|A|-1), \tag{4.11}$$

$$\ell(T) \leqslant |T| + 2\ell(A). \tag{4.12}$$

Proof. — By Theorem 4.1 and (2.3), there is $T \subset S$ such that

$$|T+2A| \leqslant (1+\frac{|A|+m}{|S|})^2|T| \leqslant |T| + 2(|A|+m)\frac{|T|}{|S|} + \frac{(|A|+m)^2}{|S|}\frac{|T|}{|S|}.$$

Writing $|A|+m \leqslant 3m+5+m \leqslant 5m \leqslant 5\epsilon|S|$ and $\lambda = |T|/|S|$ we get

$$|T+2A| \leqslant |T| + \lambda(|A|+m)(2+5\epsilon) < p. \tag{4.13}$$

Now apply the Cauchy-Davenport Theorem $|T+2A| \geqslant |T|+|2A|-1$ in (4.13) to get, since $|A| \geqslant m+3$,

$$|2A|-1 \leqslant \lambda(2|A|-3)(2+5\epsilon), \text{ and}$$

$$|2A| \leqslant 2\lambda(2+5\epsilon)(|A|-1) - \lambda(2+5\epsilon)+1. \tag{4.14}$$

Notice that if $\lambda(2+5\epsilon)<1$ then (4.14) gives $|2A| < 2(|A|-1)+1$ which contradicts the Cauchy-Davenport Theorem. Therefore we have $1-\lambda(2+5\epsilon) \leqslant 0$ and (4.14) yields (4.11).

In the remaining part we prove (4.12). Recall that the hypothesis of the present lemma together with Lemma 4.4 imply

$$\ell(2A) \leqslant (2-\delta)(|2A|-1). \tag{4.15}$$

Suppose first that

$$\ell_{2A}(T) + \ell(2A) > p. \tag{4.16}$$

Set $a_2 = \ell(2A)$ and $p = 2ta_2 + r$ with $0 < r < 2a_2$. Let $I = I_1 \cup \cdots \cup I_{2t}$ with $I_i = [(i-1)a_2, ia_2)$. By (4.16) we have $T \cap I_i \neq \emptyset$ for each $i = 1, \ldots, 2t$. By Lemma 4.5 with $B = T$ and $C = 2A$,

$$|T+2A| \geqslant |T| + (t-\frac{1}{2})a_2\left(\rho(2A) - \frac{|T'|}{(2t-1)a_2}\right) \tag{4.17}$$

where $T' = T \cap I$. By (4.15) we have $a_2 \leqslant 2|2A|$, so that by using (4.11) and $\lambda \leqslant 1$ we obtain the following rough upper bound

$$a_2 \leqslant (8+20\epsilon)|A| \leqslant 9(3m+5) \leqslant 36m$$

where we have used $\epsilon \leqslant 1/20$.

As in the proof of Lemma 4.6, we have, by definition of t,

$$(2t-1)a_2 \geqslant p - 3a_2 \geqslant p - 108m \geqslant p(1-54\epsilon) \tag{4.18}$$

so that, writing $|T'| \leqslant |T| \leqslant |S| \leqslant p/2$, and applying (4.15) we have

$$\rho(2A) - \frac{|T'|}{(2t-1)a_2} \geqslant \frac{1}{2-\delta} - \frac{1}{2-108\epsilon}.$$

Applying again (4.18), inequality (4.17) becomes

$$|T+2A| \geqslant |T| + \frac{p}{2}(1-54\epsilon)\left(\frac{1}{2-\delta} - \frac{1}{2-108\epsilon}\right). \tag{4.19}$$

On the other hand, (4.13) implies

$$|T+2A| \leqslant |T| + 10m + 25\epsilon m \leqslant |T| + p(5\epsilon + 25\epsilon^2/2)$$

which together with (4.19) gives

$$5\epsilon + 25\epsilon^2/2 \geqslant \frac{1}{2}(1 - 54\epsilon)\left(\frac{1}{2-\delta} - \frac{1}{2-108\epsilon}\right). \tag{4.20}$$

For $\epsilon = 10^{-4}$ the inequality (4.20) fails to hold for each $\delta \geqslant 2 \cdot 10^{-2}$. Since (4.15) holds for every $\delta \leqslant 10^{-1}$, the hypothesis (4.16) can not hold, so that the sumset $T + 2A$ behaves like a sum of integers. Let us write

$$|T + 2A| = |T| + |2A| + \mu$$

and check that the conditions of Theorem 3.1 hold. By Lemma 4.7 (i) we have

$$\begin{aligned} |2A| &\geqslant (3-\delta)(|A|-1) \\ &\geqslant (2+5\epsilon)|A| + (1-\delta-5\epsilon)|A| - 3 \\ &\geqslant (2+5\epsilon)|A| + \frac{3}{2} \end{aligned}$$

since $m \geqslant 6$ and $|A| \geqslant m + 3 \geqslant 9$. Therefore

$$\begin{aligned} 2|2A| &\geqslant 2(2+5\epsilon)|A| + 3 \\ &\geqslant (2+5\epsilon)(|A|+m) + 3, \end{aligned}$$

which, since $\mu \leqslant (|A|+m)(2+5\epsilon) - |2A|$ by (4.13), leads to

$$|2A| \geqslant \mu + 3. \tag{4.21}$$

Now by definition of λ we have $|T| = \lambda|S|$ and we also have $|S| \geqslant 11\epsilon|S|$, so that

$$\begin{aligned} |T| &\geqslant \lambda 11\epsilon|S| \geqslant \lambda 11 m \\ &\geqslant \lambda(2+5\epsilon)5m \geqslant \lambda(2+5\epsilon)(|A|+m) \end{aligned}$$

and, since $\mu \leqslant \lambda(|A|+m)(2+5\epsilon) - |2A|$ by (4.13), we obtain

$$|T| \geqslant \mu + |2A| \geqslant \mu + 4. \tag{4.22}$$

Inequalities (4.21) and (4.22) mean that Theorem 3.1 holds and we have:

$$\ell(T) \leqslant |T| + \mu + 1 \leqslant |T| + |2A| \leqslant |T| + \ell(2A) \leqslant |T| + 2\ell(A).$$

This proves (4.12) and concludes the lemma. □

LEMMA 4.9. — *Suppose* $6 \leqslant m \leqslant \epsilon|S|$ *with* $\epsilon \leqslant 10^{-4}$. *Suppose furthermore that* $\ell(A) > (2-\delta)(|A|-1)$. *Then* $\ell(S) \leqslant |S| + m + 1$.

Proof. — Let T be the set guaranteed by Lemma 4.8. Let $\overline{T} = S \setminus T$, which belongs to an interval of length $p - \ell(T)$. Set $a = \ell(A)$. Let us apply again Lemma 4.5, this time with $B = S$, $C = A$, and t defined so as to have $p - \ell(T) = 2ta + r$, $0 \leqslant r < 2a$. As before, set $I = I_1 \cup \cdots \cup I_{2t}$ with $I_i = [(i-1)a, ia)$. Note that $T \cap I = \emptyset$, so that $\overline{T} \cap I = S \cap I$. Let us first suppose

$$\ell_A(S) + \ell(A) > p \tag{4.23}$$

which implies $\overline{T} \cap I_i \neq \emptyset$ for every $i = 1, \ldots, 2t$, so that by Lemma 4.5, and denoting $\overline{T}' = \overline{T} \cap I = S \cap I$,

$$\begin{aligned} |S + A| &\geqslant |S \cup [(S + A) \cap I]| \\ &\geqslant |S| + (t - \frac{1}{2})a\left(\rho A - \frac{|\overline{T}'|}{(2t-1)a}\right). \end{aligned} \tag{4.24}$$

By definition of t and by (4.12) we have

$$(2t - 1)a > p - \ell(T) - 3a \geqslant p - |T| - 5a. \tag{4.25}$$

Now Lemma 4.7 (ii) and (4.11) give the following upper bound on a

$$a \leqslant |2A| \leqslant \lambda(4 + 10\epsilon)|A| \leqslant \lambda(4 + 10\epsilon)4m \leqslant \lambda(4 + 10\epsilon)2\epsilon p$$

so that we can write $-5a \geqslant -\lambda f(\epsilon)p$ with $f(\epsilon) = 10(4 + 10\epsilon)\epsilon$. Writing $|T| = \lambda|S| < \lambda p/2$, (4.25) becomes

$$(2t - 1)a > p(1 - \lambda(\frac{1}{2} + f(\epsilon))). \tag{4.26}$$

Next we write $|\overline{T}'| \leqslant |\overline{T}| = |S| - |T| = (1 - \lambda)|S|$, so that $|S| \leqslant p/2$ gives

$$|\overline{T}'| \leqslant \frac{p}{2}(1 - \lambda). \tag{4.27}$$

Finally we bound ρA from below. Apply again Lemma 4.7 (ii) and (4.11) to get

$$\ell(A) \leqslant (1 - \delta/2)|2A| \leqslant (1 - \delta/2)\lambda(4 + 10\epsilon)(|A| - 1),$$

so that we have

$$\rho A \geqslant \frac{1}{\lambda(1 - \delta/2)(4 + 10\epsilon)}. \tag{4.28}$$

Applying (4.26), (4.27) and (4.28) to (4.24) now gives

$$|S + A| > |S| + \frac{p}{2}\left[\frac{1 - \lambda(\frac{1}{2} + f(\epsilon))}{\lambda(1 - \delta/2)(4 + 10\epsilon)} - \frac{1}{2}(1 - \lambda)\right].$$

Together with (2.3), writing $|A| \leqslant 4m$ and $m \leqslant \epsilon p/2$, we obtain

$$\frac{1-\lambda(\frac{1}{2}+f(\epsilon))}{\lambda(1-\delta/2)(4+10\epsilon)} - \frac{1}{2}(1-\lambda) - 5\epsilon < 0. \tag{4.29}$$

Now there exists $\epsilon_\delta > 5.8\ 10^{-3} > 0$ such that for every $\epsilon \leqslant \epsilon_\delta$, the left-handside of (4.29) is strictly positive for every value of $\lambda \in [0,1]$. In that case (4.29) can not hold and we obtain a contradiction with the hypothesis (4.23). Therefore Theorem 3.1 implies the result. □

Numerical values. As it has been shown in the proofs Theorem 1.3 holds with $\epsilon = 10^{-4}$. As for the value of p_0, we use $m \geqslant 6$ in Section 4, so in order to cover smaller values of m, the prime p should satisfy the condition in Lemma 3.5 that $\log_4 p \geqslant 6m + 11 \geqslant 47$ which is equivalent to $p \geqslant 2^{94}$. We have tried to strike a balance between readability and obtaining the best possible constants. These values of ϵ and p_0 are not the best possible, but they give a reasonable account of what can be achieved through the methods of this paper.

BIBLIOGRAPHY

[1] Y. F. Bilu, V. F. Lev & I. Z. Ruzsa, "Rectification principles in additive number theory", *Discrete Comput. Geom.* **19** (1998), no. 3, Special Issue, p. 343-353, Dedicated to the memory of Paul Erdős.

[2] G. A. Freĭman, "The addition of finite sets. I", *Izv. Vysš. Učebn. Zaved. Matematika* **1959** (1959), no. 6 (13), p. 202-213.

[3] ———, "Inverse problems in additive number theory. Addition of sets of residues modulo a prime", *Dokl. Akad. Nauk SSSR* **141** (1961), p. 571-573.

[4] ———, *Foundations of a structural theory of set addition*, American Mathematical Society, Providence, R. I., 1973, Translated from the Russian, Translations of Mathematical Monographs, Vol 37, vii+108 pages.

[5] B. Green & I. Z. Ruzsa, "Sets with small sumset and rectification", *Bull. London Math. Soc.* **38** (2006), no. 1, p. 43-52.

[6] Y. O. Hamidoune, "On the connectivity of Cayley digraphs", *European J. Combin.* **5** (1984), no. 4, p. 309-312.

[7] ———, "An isoperimetric method in additive theory", *J. Algebra* **179** (1996), no. 2, p. 622-630.

[8] ———, "Subsets with small sums in abelian groups. I. The Vosper property", *European J. Combin.* **18** (1997), no. 5, p. 541-556.

[9] ———, "Some results in additive number theory. I. The critical pair theory", *Acta Arith.* **96** (2000), no. 2, p. 97-119.

[10] Y. O. Hamidoune & Ø. J. Rødseth, "An inverse theorem mod p", *Acta Arith.* **92** (2000), no. 3, p. 251-262.

[11] Y. O. Hamidoune, O. Serra & G. Zémor, "On the critical pair theory in $\mathbb{Z}/p\mathbb{Z}$", *Acta Arith.* **121** (2006), no. 2, p. 99-115.

[12] ———, "On the critical pair theory in abelian groups: beyond Chowla's theorem", *Combinatorica* **28** (2008), no. 4, p. 441-467.

[13] V. F. Lev & P. Y. Smeliansky, "On addition of two distinct sets of integers", *Acta Arith.* **70** (1995), no. 1, p. 85-91.

[14] M. B. Nathanson, *Additive number theory*, Graduate Texts in Mathematics, vol. 165, Springer-Verlag, New York, 1996, Inverse problems and the geometry of sumsets, xiv+293 pages.

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

[16] I. Z. Ruzsa, "An application of graph theory to additive number theory", *Sci. Ser. A Math. Sci. (N.S.)* **3** (1989), p. 97-109.

[17] O. Serra & G. Zémor, "On a generalization of a theorem by Vosper", *Integers* (2000), p. A10, 10 pp. (electronic).

[18] T. Tao & V. Vu, *Additive combinatorics*, Cambridge Studies in Advanced Mathematics, vol. 105, Cambridge University Press, Cambridge, 2006, xviii+512 pages.

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

Manuscrit re**c**cu le 3 avril 2008,
accepté le 15 décembre 2008.

Oriol SERRA
Universitat Politècnica de Catalunya
Matemàtica Aplicada IV
Campus Nord - Edif. C3, C. Jordi Girona, 1-3
08034 Barcelona (Spain)
oserra@ma4.upc.edu

Gilles ZÉMOR
Université Bordeaux 1
Institut de Mathématiques de Bordeaux, UMR 5251
351, cours de la Libération
33405 Talence (France)
zemor@math.u-bordeaux1.fr