Rev. Mat. Iberoamericana **21** (2005), no. 1, 133–161

A multiple set version of the $3k-3$ Theorem

Yahya ould Hamidoune and Alain Plagne

Abstract

In 1959, Freiman demonstrated his famous $3k-4$ Theorem which was to be a cornerstone in inverse additive number theory. This result was soon followed by a $3k-3$ Theorem, proved again by Freiman. This result describes the sets of integers $\mathcal{A}$ such that $|\mathcal{A}+\mathcal{A}| \leq 3|\mathcal{A}|-3$. In the present paper, we prove a $3k-3$ -like Theorem in the context of multiple set addition and describe, for any positive integer j, the sets of integers $\mathcal{A}$ such that the inequality $|j\mathcal{A}| \leq j(j+1)(|\mathcal{A}|-1)/2$ holds. Freiman's $3k-3$ Theorem is the special case $j=2$ of our result. This result implies, for example, the best known results on a function related to the Diophantine Frobenius number. Actually, our main theorem follows from a more general result on the border of $j\mathcal{A}$.

1. Introduction

The (Minkowski) *sumset* $\mathcal{C}+\mathcal{D}$ of any two subsets $\mathcal{C}$ and $\mathcal{D}$ of some (additively written) (semi-) group is classically defined as

$$\mathcal{C}+\mathcal{D}=\{c+d, \text{ where } c\in\mathcal{C}, d\in\mathcal{D}\}.$$

We denote $\mathcal{C}+\mathcal{C}$ by $2\mathcal{C}$ and, more generally, $h\mathcal{C}$ is recursively defined as $(h-1)\mathcal{C}+\mathcal{C}$.

In additive number theory, the following formula, valid for any two non-empty sets of integers $\mathcal{C},\mathcal{D}\subset\mathbb{Z}$,

$$|\mathcal{C}+\mathcal{D}| \geq |\mathcal{C}|+|\mathcal{D}|-1, \tag{1.1}$$

2000 Mathematics Subject Classification: 11P70, 11B75.
Keywords: $3k-3$ theorem, multiple set addition, $3k-4$ theorem, structure theory of set addition, Frobenius problem.

is the simplest one. This result is optimal. Indeed, it is easily seen that, if $|\mathcal{C}| = 1$ (and $\mathcal{D}$ is arbitrary), or if $|\mathcal{D}| = 1$ (and $\mathcal{C}$ is arbitrary), or if $\mathcal{C}$ and $\mathcal{D}$ are *arithmetic progressions* with the same difference, inequality (1.1) is an equality. Recall that, for the present purpose, arithmetic progressions will be always finite so that the third possible case is that one in which $\mathcal{C}$ and $\mathcal{D}$ are of the form

$$\mathcal{C} = \{c+(i-1)r, \text{ where } 1 \le i \le l\} \text{ and } \mathcal{D} = \{d+(i-1)r, \text{ where } 1 \le i \le l'\},$$

for an integer r (the common *difference*) and some positive integers l and l' (called the *lengths* of the arithmetic progressions). Conversely, it is a well-known fact that, in any other case than those above-mentioned, we can improve inequality (1.1) in

$$|\mathcal{C} + \mathcal{D}| \ge |\mathcal{C}| + |\mathcal{D}|. \tag{1.2}$$

For any non-zero real h (usually, we shall have $h \in \mathbb{N}$) and a given set $\mathcal{C}$ of integers, we also define $h.\mathcal{C}$ to be

$$h.\mathcal{C} = \{hc, \text{ where } c \in \mathcal{C}\}, \tag{1.3}$$

a set which, in the case when h is an integer, has in general nothing to do with $h\mathcal{C}$. However, since there is no risk of confusion, we will keep, here and thereafter, the classical notation $\mathbb{Z}/M\mathbb{Z}$ for what we should write $\mathbb{Z}/M.\mathbb{Z}$, according to this notation.

Freiman [5] (see also [8]) went a step beyond (1.1) by showing that if $\mathcal{A}$ is a set of integers such that $|\mathcal{A} + \mathcal{A}| \le 3|\mathcal{A}| - 4$, then $\mathcal{A}$ is a subset of a short arithmetic progression; more precisely there are integers a and r such that

$$\mathcal{A} \subset \{a + (i-1)r, \text{ where } 1 \le i \le l\},$$

where the length l of the arithmetic progression is less than or equal to $|\mathcal{A} + \mathcal{A}| - |\mathcal{A}| + 1$. This result is now called the $3k - 4$ Theorem after the early notation of Freiman which was to put $k = |\mathcal{A}|$. Freiman's $3k - 4$ Theorem was further generalized and reproved among others by Steinig, Lev and Smeliansky (see [6, 13, 17]). About the $3k - 4$ Theorem, the reader is also referred to the fundamental book by Freiman himself [7] and to the general account given by Nathanson [16].

Freiman pursued a bit further by showing a $3k-3$ Theorem [5]. Namely, he characterized all the sets of integers $\mathcal{A}$ satisfying the equality $|\mathcal{A} + \mathcal{A}| = 3|\mathcal{A}| - 3$. Together with the $3k - 4$ Theorem, this gives the following.

Theorem 1 (Freiman's $3k-3$ Theorem [5]) *Let $\mathcal{A}$ be a set of non-negative integers containing 0 and satisfying $\gcd(\mathcal{A}) = 1$. Define $M = \max(\mathcal{A})$. If the upper bound*

$$|2\mathcal{A}| \leq 3|\mathcal{A}| - 3$$

holds, then one of the following happens:

- $|\mathcal{A}| \geq 1 + M/2$,
- *$\mathcal{A}$ is the union of two arithmetic progressions with the same common difference,*
- *M is even and $\mathcal{A}$ is of the form $\mathcal{A} = \{0, M/2, M, x, x + M/2, 2x\}$ for some positive integer $x < M/2$.*

Note that the sets of the form $\mathcal{A} = \{0, M/2, M, x, x+M/2, 2x\}$ (for some positive integer $x < M/2$) which appear in the third possible conclusion of the $3k-3$ Theorem are called K_6 by Freiman.

In [11], the authors could both obtain a new proof and generalize Freiman's $3k-3$ Theorem to the case of $\mathcal{A} + \mathcal{A}'$ with $\mathcal{A}' = j.\mathcal{A}$ (for j, an integer).

Let us state a simple remark. It is clear that, for any two sets $\mathcal{C}$ and $\mathcal{D}$ of integers, neither $|\mathcal{C}|$ nor $|\mathcal{C} + \mathcal{D}|$ is changed by a translation or an integral dilatation. This remark allows us to consider instead of $\mathcal{A}$ itself, the set $\frac{1}{\gcd(\mathcal{A})}.(\mathcal{A} - \min(\mathcal{A})) \subset \mathbb{N}$, where we have used the notation (1.3) and where $\gcd(\mathcal{A})$ denotes the greatest common divisor of the elements of $\mathcal{A}$. In particular, this remark shows that the assumptions on the set $\mathcal{A}$ ($0 \in \mathcal{A}$ and $\gcd(\mathcal{A}) = 1$) appearing in Theorem 1 are not at all constraining and can be added without loss of generality. In the same way, this remark allows us to consider only in the sequel sets of the form $\mathcal{A} = \{a_1, \ldots, a_n\}$ having the following properties: $0 = a_1 < a_2 < \cdots < a_n$ and $\gcd(\mathcal{A}) = \gcd(a_1, a_2, \ldots, a_n) = 1$. Such sets will be called *normal*.

Motivated by the application to the Diophantine Frobenius problem, Lev [14] generalized the $3k-4$ Theorem to multiple set addition. In this respect, his result is essentially the following.

Theorem 2 (Corollary 1 of Lev's [14]) *Let $\mathcal{A}$ be a set of non-negative integers containing 0 and satisfying $\gcd(\mathcal{A}) = 1$. Define $M = \max(\mathcal{A})$. Let j be any integer greater than or equal to 2. If the upper bound*

$$|j\mathcal{A}| \leq \frac{j(j+1)}{2}\,(|\mathcal{A}| - 1) - \frac{j(j-1)}{2}$$

holds, then $|\mathcal{A}| \geq 2 + M/j$.

In this paper, we generalize in a similar way Freiman's $3k-3$ Theorem to multiple set addition. Our result is the following.

Theorem 3 *Let $\mathcal{A}$ be a set of non-negative integers containing 0 and satisfying $\gcd(\mathcal{A}) = 1$. Define $M = \max(\mathcal{A})$. Let j be any integer greater than or equal to 2. If the upper bound*

$$|j\mathcal{A}| \leq \frac{j(j+1)}{2}\,(|\mathcal{A}| - 1)$$

holds, then one of the following happens:

- $|\mathcal{A}| \geq 1 + M/j$,
- *$\mathcal{A}$ is the union of two arithmetic progressions with the same common difference,*
- *$\mathcal{A}$ is an arithmetic progression modulo M,*
- *M is even and $\mathcal{A}$ is of the form $\mathcal{A} = \{0, M/2, M, x, x + M/2, 2x\}$ for some positive integer $x < M/2$.*

Compared to Freiman's $3k-3$ Theorem, a new kind of exceptional sets arises: arithmetic progressions modulo M. Since an arithmetic progression modulo M is a special case of union of arithmetic progressions with the same difference, it can be seen as a generalization of the second type of exceptions (unions of two arithmetic progressions with the same common difference) which appeared already in the $3k-3$ Theorem. However, notice that there exist sets which are a union of two arithmetic progressions with the same difference which are *not* an arithmetic progression modulo M.

In the same fashion as Lev in [14], Theorem 3 is obtained through a more powerful result on the border of $j\mathcal{A}$ defined by

$$\mathcal{B} = (j\mathcal{A}) \setminus \big((j-1)\mathcal{A}\big).$$

To state the result in a clear way, we need to define first a class of sets for which our result does not apply. We therefore let $\mathcal{F}$ denote the set of all subsets of integers $\mathcal{A}$ such that one of the following structural conditions holds :

- $\mathcal{A}$ is the union of two arithmetic progressions with the same common difference,
- $\mathcal{A}$ is an arithmetic progression modulo M,
- $\mathcal{A}$ is of the form

  $$\{0, e, 2e, \ldots, M-2e, M-e, M\} \cup \{b, b+se, \ldots, b+use\},$$

  for some integer $M = \max(\mathcal{A})$ and where e, b, s and u are positive integers subject to $e|M$, $1 < e < M$ and $s \geq 2$,

- there exist four non-negative integers e, b, u and k such that e divides $M = \max(\mathcal{A})$, b belongs to $\{1, 2, \ldots, e-1\}$ and is coprime to M, $u \geq 2$ and $k \in \{0, 1, \ldots, M/e - 1\}$, such that $\mathcal{A}$ is of the form

$$\begin{aligned}\mathcal{A} &= \{0, e, 2e, \ldots, M-e, M\} \cup \{b, b+e, b+2e, \ldots, b+M-e\} \\ &\cup \{b_2, b_2+e, \ldots, b_2+M-e\} \cup \cdots \cup \{b_{u-2}, b_{u-2}+e, \ldots, b_{u-2}+M-e\} \\ &\cup \{b_{u-1}, b_{u-1}+e, b_{u-1}+2e, \ldots, b_{u-1}+M-e\} \cup \{b_u + ke\},\end{aligned}$$

  where b_i denotes the unique integer $\equiv ib$ modulo e in $\{0, 1, \ldots, e-1\}$.

In what follows, we shall refer to these four types of exceptions as exceptions of Type I, II, III or IV, respectively.

Notice that Type II exceptions are not obligatorily of Type IV. Also it is possible to be a union of two arithmetic progressions (Type I) with the same common difference without being an arithmetic progression modulo M (Type II), as mentioned before.

We notice that the sets appearing in Type IV exceptions are a natural generalization of the K_6 sets. In the case of Type IV exceptions, we may equivalently reformulate the description of the sets appearing as follows: there is a subgroup H of $\mathbb{Z}/\max(\mathcal{A})\mathbb{Z}$ such that the projection of $\mathcal{A}$ modulo H, $\psi(\mathcal{A})$, is an arithmetic progression (say, $0, b, 2b, \ldots, ub$) modulo H, starting from 0 and having at least 3 elements ($u \geq 2$). Moreover, $\mathcal{A}$ is composed of the following union of preimages:

$$\bigcup_{i=0}^{u-1} \left(\psi^{-1}(id) \cap \{0, 1, \ldots, \max(\mathcal{A})\}\right)$$

together with one element belonging to $\psi^{-1}(ud)$. That is, except the u-th one which has one element, all the H-cosets are full: they all possess $|H|$ elements except the first one, that of 0, which has $|H| + 1$ elements.

Theorem 4 *Let $\mathcal{A}$ be a set of non-negative integers containing 0 and satisfying $\gcd(\mathcal{A}) = 1$. Define $M = \max(\mathcal{A})$. Let j be any integer larger than or equal to 2. Assume that $\mathcal{A}$ is not in $\mathcal{F}$, then it verifies*

$$|(j\mathcal{A}) \setminus \big((j-1)\mathcal{A}\big)| \geq \min(M-1, j(|\mathcal{A}|-1)).$$

The outline of this paper is the following: in Section 2, we introduce the needed prerequisites. In Section 3, we proceed with the core of the paper, namely the proof of Theorem 4. In Section 4, we show how to recover Theorem 3 from Theorem 4. Finally, in Section 5, we illustrate the potential applications of this result by reproving in an efficient way a result on the Frobenius problem obtained in [10].

2. Preliminary

Several easy lemmata will be needed in what follows. We start by stating them and recalling some standard definitions.

Our first lemma is sometimes referred to as the Prehistorical lemma and is nothing else than an application of the pigeon-hole principle.

Lemma 5 (Prehistorical lemma) *Let H be a subgroup of some given finite Abelian group G. Let $\mathcal{C}$ and $\mathcal{D}$ be two subsets of G, each being included in a coset modulo H. If $|\mathcal{C}| + |\mathcal{D}| > |H|$ then $\mathcal{C} + \mathcal{D}$ is equal to a coset modulo H.*

We shall say that the coset $\mathcal{C}+\mathcal{D}$ is *complete* (or *full*). Indeed, any coset is *by definition* full but when a set $\mathcal{C}$ is only known to be included in a coset $a + H$, that will mean that $\mathcal{C} = a + H$.

In what follows, we use the following definition: for H a subgroup of G, we shall say that a subset $\mathcal{C}$ of G is *H-periodic* if it verifies $\mathcal{C} + H = \mathcal{C}$ or, equivalently, if it is a union of cosets modulo H. *The period* of a set $\mathcal{C}$ is the largest subgroup H such that $\mathcal{C}$ is H-periodic.

Now, we come to a lemma generalizing formula (1.1).

Lemma 6 *Let $m \in \mathbb{Z}$, $m \neq 0$. Let $\mathcal{C} \subset m.\mathbb{Z}$ and $\mathcal{D} \subset \mathbb{Z}$ be two non-empty sets. Then*

$$|\mathcal{C} + \mathcal{D}| \geq |\phi(\mathcal{D})|\ (|\mathcal{C}| - 1) + |\mathcal{D}|,$$

where ϕ denotes the canonical projection from $\mathbb{Z}$ onto $\mathbb{Z}/m\mathbb{Z}$.

Moreover, if $\mathcal{C}$ is not an arithmetic progression, this inequality can be improved to

$$|\mathcal{C} + \mathcal{D}| \geq |\phi(\mathcal{D})|\ (|\mathcal{C}| - 1) + |\mathcal{D}| + |\{j \in \mathbb{Z}/m\mathbb{Z} : |\phi^{-1}(j) \cap \mathcal{D}| > 1\}|.$$

Proof. We define a partition (into non-empty subsets) of $\mathcal{D}$ according to the cosets modulo $m.\mathbb{Z}$:

$$\mathcal{D} = \mathcal{D}_1 \cup \cdots \cup \mathcal{D}_k,$$

with $k = |\phi(\mathcal{D})|$. Since for any integers $i_1 \neq i_2$, the intersection $(\mathcal{C} + \mathcal{D}_{i_1}) \cap (\mathcal{C} + \mathcal{D}_{i_2})$ is empty, we have

$$|\mathcal{C} + \mathcal{D}| = |(\mathcal{C} + \mathcal{D}_1) \cup \cdots \cup (\mathcal{C} + \mathcal{D}_k)| = |\mathcal{C} + \mathcal{D}_1| + \cdots + |\mathcal{C} + \mathcal{D}_k|.$$

Let $i \in \{1, 2, \ldots, k\}$. By (1.1), we always have

$$|\mathcal{C} + \mathcal{D}_i| \geq |\mathcal{C}| + |\mathcal{D}_i| - 1. \tag{2.1}$$

Summing these contributions gives

$$\begin{aligned} |\mathcal{C}+\mathcal{D}| &\geq (|\mathcal{C}|+|\mathcal{D}_1|-1)+\cdots+(|\mathcal{C}|+|\mathcal{D}_k|-1) \\ &= k(|\mathcal{C}|-1)+|\mathcal{D}| = |\phi(\mathcal{D})|\ (|\mathcal{C}|-1)+|\mathcal{D}|. \end{aligned}$$

Suppose now that $\mathcal{C}$ is not an arithmetic progression (in particular $|\mathcal{C}|>1$), we may improve (2.1) when $|\mathcal{D}_i| \neq 1$ by using (1.2) instead of (1.1),

$$|\mathcal{C}+\mathcal{D}_i| \geq |\mathcal{C}|+|\mathcal{D}_i|.$$

Summing these contributions implies

$$|\mathcal{C}+\mathcal{D}| \geq (|\mathcal{C}|+|\mathcal{D}_1|-1)+\cdots+(|\mathcal{C}|+|\mathcal{D}_k|-1)+\sum_{1\leq i\leq k,\ |\mathcal{D}_i|\neq 1} 1$$

which gives the result. ■

From this we are able to deduce the following corollary.

Corollary 7 *Let $\mathcal{C}$ be a finite set of integers containing 0 and M be the largest element of $\mathcal{C}$. Denote again with a bar the reduction modulo M. Then, for any positive integer h, we have*

$$|h\mathcal{C}| \geq |(h-1)\mathcal{C}|+|h\overline{\mathcal{C}}|.$$

Proof. Let $\mathcal{D}=(h-1)\mathcal{C}$. Applying Lemma 6 with $m=M$ yields

$$|\{0,M\}+\mathcal{D}| \geq |\mathcal{D}|+|\overline{\mathcal{D}}|.$$

Now, in $h\mathcal{C}=\mathcal{C}+\mathcal{D}$, there are elements which do not belong to $\overline{\mathcal{D}}$ (observe that $\overline{\{0,M\}+\mathcal{D}}=\overline{\mathcal{D}}$) when projected onto $\mathbb{Z}/M\mathbb{Z}$. The number of these elements is at least $|(\overline{\mathcal{C}}+\overline{\mathcal{D}})\setminus\overline{\mathcal{D}}|$. Adding everything together yields the result announced. ■

We go on in these prerequisites by stating a generalization of Vosper's theorem that we obtained recently in [12]. Recall that inequality (1.1) is true in cyclic groups of prime order, at the price of a trivially necessary modification of the formula: what we can prove is that, if $\mathcal{C}$ and $\mathcal{D}$ are two non-empty subsets of $\mathbb{Z}/p\mathbb{Z}$, then

$$|\mathcal{C}+\mathcal{D}| \geq \min(p, |\mathcal{C}|+|\mathcal{D}|-1).$$

This result is called the Cauchy-Davenport theorem [1, 2]. Vosper's theorem [19] corresponds to inequality (1.2) and is therefore concerned with the cases in which the Cauchy-Davenport inequality is in fact an equality.

For stating the result obtained in [12], we shall need some natural notations. First, we shall say that a subset $\mathcal{C}$ of a finite Abelian group G is a *Vosper subset* of G if for any $\mathcal{D} \subset G$, with $|\mathcal{D}| \geq 2$, the inequality

$$|\mathcal{C} + \mathcal{D}| \geq \min(|G| - 1, |\mathcal{C}| + |\mathcal{D}|)$$

holds. Notice that a Vosper subset with cardinality one cannot exist in a group with cardinality four or more.

In a similar way, we shall say that a subset $\mathcal{C}$ of G is a *Cauchy subset* if for any non-empty $\mathcal{D} \subset G$, the inequality

$$|\mathcal{C} + \mathcal{D}| \geq \min(|G|, |\mathcal{C}| + |\mathcal{D}| - 1)$$

holds. The following lemma on Vosper and Cauchy subsets will be needed.

Lemma 8 *Any Vosper subset is a Cauchy subset.*

Proof. Suppose that the result is false and let $\mathcal{C}$ be a Vosper subset of some finite Abelian group G such that there is a $\mathcal{D} \subset G$ satisfying (notice that necessarily $|\mathcal{D}| > 1$)

$$|\mathcal{C} + \mathcal{D}| < \min(|G|, |\mathcal{C}| + |\mathcal{D}| - 1). \tag{2.2}$$

In particular,

$$|\mathcal{C} + \mathcal{D}| \leq |\mathcal{C}| + |\mathcal{D}| - 2 \tag{2.3}$$

which implies, by the Vosper property (applied with the set $\mathcal{D}$, of cardinality at least two), $|\mathcal{C}+\mathcal{D}| \geq |G|-1$. Again by (2.2), this implies $|\mathcal{C}+\mathcal{D}| = |G|-1$. But, then, inequality (2.3) yields $|\mathcal{C}|+|\mathcal{D}| \geq |G|+1$, and, by the Prehistorical lemma, $\mathcal{C} + \mathcal{D} = G$, a contradiction. ■

As our last result on Vosper sets, let us now mention a trivial necessary condition for being a Vosper subset, which will be needed in the sequel. The proof follows directly from the definition by a trivial induction argument.

Corollary 9 *Let G be any finite Abelian group and $\mathcal{C}$ be a Vosper subset with cardinality at least two of G. Let h be any positive integer, then*

$$|h\mathcal{C}| \geq \min(|G| - 1, h|\mathcal{C}|)\,.$$

Finally, for a subset $\mathcal{C}$ of any Abelian group G and any subgroup H of G, we shall denote by $\mathcal{C}/H$ the subset $\psi(\mathcal{C})$ of G/H, where ψ denotes the canonical projection from G onto G/H. Evidently, one has $(\mathcal{C} + H)/H = \mathcal{C}/H$.

We are now ready to enunciate the Theorem we obtained in [12]. The result we could obtain expresses, roughly speaking, the fact that, in any finite Abelian group, there is a strict subgroup (by which we mean a subgroup different from the ambient group itself) such that, modulo this subgroup, Vosper's theorem applies.

Theorem 10 (proved in [12]) *Let G be any finite Abelian group and $\mathcal{C}$ be a generating subset of G containing 0 such that $|\mathcal{C}| \leq |G|/2$. Then, there exists a subgroup H of G with*

$$|\mathcal{C}+H| < \min(|G|, |H|+|\mathcal{C}|) \tag{2.4}$$

such that $(\mathcal{C}+H)/H$ is either an arithmetic progression or a Vosper subset (in G/H).

As mentioned above, inequality (2.4) forces H to be different from G.

3. The proof of Theorem 4

3.1. Starting the proof

We consider a normal set $\mathcal{A}$ not in $\mathcal{F}$ and let $M = \max(\mathcal{A})$. Our aim is to prove that the lower bound

$$|(j\mathcal{A}) \setminus \big((j-1)\mathcal{A}\big)| \geq \min(M-1, j(|\mathcal{A}|-1)) \tag{3.1}$$

holds for any integer $j \geq 2$.

The case $j = 2$ is implied by the $3k-3$ Theorem, so we shall assume, all along the proof, that $j > 2$ or

$$j \geq 3.$$

Notice that the method proposed here could also work when $j = 2$ (but at the price of technicalities).

We shall denote by $\mathcal{B}$ the border of $j\mathcal{A}$,

$$\mathcal{B} = (j\mathcal{A}) \setminus \big((j-1)\mathcal{A}\big).$$

Notice that, since 0 belongs to $\mathcal{A}$, $(j-1)\mathcal{A} \subset j\mathcal{A}$ which implies

$$|\mathcal{B}| = |j\mathcal{A}| - |(j-1)\mathcal{A}|.$$

We denote $G = \mathbb{Z}/M\mathbb{Z}$ the cyclic group with M elements (notice that it is easy to check that the assumption $\mathcal{A} \notin \mathcal{F}$ implies $M \geq 6$, while $\{0,1,3,5,6\}$ does not belong to $\mathcal{F}$). We let ψ denote the canonical projection from $\mathbb{Z}$ onto G. In what follows, we shall also denote with a bar the projection ψ.

The method of proof relies on first reducing the problem modulo M and obtaining a modular set $\overline{\mathcal{A}}$. Observe immediately that

$$|\overline{\mathcal{A}}| = |\mathcal{A}| - 1.$$

At several places in the following, we will consider a partition of the border of $j\mathcal{A}$ into two parts (referred to as the interior $\mathcal{I}$ and the exterior $\mathcal{J}$),

$$\mathcal{B} = \mathcal{I} \cup \mathcal{J}, \tag{3.2}$$

in the following manner. Let x be in $\mathcal{B}$; if $\psi(x) \in (j-1)\overline{\mathcal{A}}$ then $x \in \mathcal{I}$, otherwise $x \in \mathcal{J}$. Let us rephrase this by saying that $\mathcal{J}$ is composed of the elements from $j\mathcal{A}$ belonging to a class modulo M not yet present in $(j-1)\overline{\mathcal{A}}$.

Notice that we may assume that

$$|j\overline{\mathcal{A}}| \leq j|\overline{\mathcal{A}}| - 1 \tag{3.3}$$

and

$$|j\overline{\mathcal{A}}| \leq M - 2. \tag{3.4}$$

Otherwise, using Corollary 7, we get

$$|j\mathcal{A}| \geq |(j-1)\mathcal{A}| + |j\overline{\mathcal{A}}| \geq |(j-1)\mathcal{A}| + \min(M-1, j|\overline{\mathcal{A}}|),$$

which implies (3.1) and the Theorem. In particular, we have

$$j\overline{\mathcal{A}} \neq G. \tag{3.5}$$

Notice that since $j \geq 2$, by the Prehistorical lemma, this implies

$$|\overline{\mathcal{A}}| \leq M/2. \tag{3.6}$$

3.2. Factorizing

We now apply Theorem 10 to $\overline{\mathcal{A}} \subset G = \mathbb{Z}/M\mathbb{Z}$. The conditions of application of this result are easily seen to be fulfilled in view of $|\overline{\mathcal{A}}| \leq M/2$ (equation (3.6)) and the fact that $\mathcal{A}$ is normal (which implies $\overline{\mathcal{A}}$ to be a generating set). Therefore, there exists a strict subgroup H of G with

$$|\overline{\mathcal{A}} + H| < \min(|G|, |H| + |\overline{\mathcal{A}}|) \tag{3.7}$$

such that $\overline{\overline{\mathcal{A}}}$, which is by definition the set of classes modulo H which are present in $\overline{\mathcal{A}}$, or in other terms

$$\overline{\overline{\mathcal{A}}} = (\overline{\mathcal{A}} + H)/H$$

verifies

Lemma 11 *The set $\overline{\overline{\mathcal{A}}}$ is either an arithmetic progression or a Vosper subset (in G/H).*

Notice that H, as a subgroup of $G = \mathbb{Z}/M\mathbb{Z}$ is of the shape $e\mathbb{Z}/M\mathbb{Z} \simeq \mathbb{Z}/(M/e)\mathbb{Z}$ for some integer e dividing M. This implies that G/H is simply $\mathbb{Z}/e\mathbb{Z}$. Since H is a strict subgroup of G, we have

$$e > 1.$$

To proceed further in our proof, we shall need to decompose our set $\overline{\mathcal{A}}$ according to a so-called H-tiling, or more prosaically, to residues modulo e. We start by defining

$$u = |\overline{\overline{\mathcal{A}}}| - 1$$

and by partitioning $\overline{\mathcal{A}}$ (and $\mathcal{A}$) into subsets of cosets modulo H (the H-tiling): in other words, we write

$$\mathcal{A} = \mathcal{A}^0 \cup \mathcal{A}^1 \cup \cdots \cup \mathcal{A}^u$$

with $u \geq 1$ (since $0 \in \mathcal{A}$ and $\gcd(\mathcal{A}) = 1$) and where each $\mathcal{A}^i$ is exactly the intersection of $\mathcal{A}$ with an arithmetic progression with difference e. This implies (with evident notations) trivially

$$\overline{\mathcal{A}} = \overline{\mathcal{A}}^0 \cup \overline{\mathcal{A}}^1 \cup \cdots \cup \overline{\mathcal{A}}^u \quad \text{and} \quad \overline{\overline{\mathcal{A}}} = \{\overline{\overline{\mathcal{A}}}^0, \overline{\overline{\mathcal{A}}}^1, \ldots, \overline{\overline{\mathcal{A}}}^u\}.$$

Notice that we have

$$|\overline{\mathcal{A}} + H| = (u+1)|H|.$$

We may now suppose, without loss of generality, that

$$|\overline{\mathcal{A}}^0| \geq |\overline{\mathcal{A}}^1| \geq \cdots \geq |\overline{\mathcal{A}}^{u-1}| \geq |\overline{\mathcal{A}}^u|. \tag{3.8}$$

With the convention (3.8), we readily see that for any pair of integers (i_1, i_2), except possibly if $(i_1, i_2) = (u, u)$, we have

$$|\overline{\mathcal{A}}^{i_1}| + |\overline{\mathcal{A}}^{i_2}| \geq |\overline{\mathcal{A}}^{u-1}| + |\overline{\mathcal{A}}^u| \geq |H| + 1, \tag{3.9}$$

since (3.7) implies

$$u|H| + 1 \leq \sum_{i=0}^{u} |\overline{\mathcal{A}}^i|. \tag{3.10}$$

An application of the Prehistorical lemma (Lemma 5) proves then that for any pair of integers (i_1, i_2), except possibly the pair (u, u), we have

$$|\overline{\mathcal{A}}^{i_1} + \overline{\mathcal{A}}^{i_2}| = |H|, \tag{3.11}$$

or, equivalently, that $\overline{\mathcal{A}}^{i_1} + \overline{\mathcal{A}}^{i_2}$ is a (full) coset modulo H. More generally, we may enunciate the following lemma which will be very useful in several places.

Lemma 12 *In the above-mentioned conditions, if we let h be any integer larger than or equal to 2, then the h-fold sumset $h\overline{\mathcal{A}}$ is composed as a union of (full) cosets modulo H and $h\overline{\mathcal{A}}^u$.*

In the same spirit, another useful lemma is this:

Lemma 13 *In the above-mentioned conditions, one has*

$$|(j-1)\overline{\overline{\mathcal{A}}}| + |\overline{\overline{\mathcal{A}}}| \leq |G/H| + 1.$$

Proof. Suppose this is false. It follows

$$|(j-1)\overline{\overline{\mathcal{A}}}| + \left|\overline{\overline{\mathcal{A}}} \setminus \{\overline{\overline{\mathcal{A}}}^u\}\right| \geq |G/H| + 2 - 1 > |G/H|$$

and the Prehistorical lemma gives

$$(j-1)\overline{\overline{\mathcal{A}}} + \left(\overline{\overline{\mathcal{A}}} \setminus \{\overline{\overline{\mathcal{A}}}^u\}\right) = G/H.$$

Now, since the set $(j-1)\overline{\mathcal{A}} + \left(\overline{\mathcal{A}} \setminus \{\overline{\mathcal{A}}^u\}\right)$ is a union of complete cosets modulo H (once again, by Lemma 12: we removed $\overline{\overline{\mathcal{A}}}^u$ from $\overline{\overline{\mathcal{A}}}$ in the second summand for this very reason), we deduce $j\overline{\mathcal{A}} = G$, in contradiction with (3.5). ■

More generally, this decomposition (H-tiling) will be the key tool in the following and the notation defined here will be retained from now on in the whole paper.

In the following subsections, we continue our proof of Theorem 4. We will use several times inequalities (3.3) and (3.4). As noted above, if one of these two inequalities is false, then (3.1) follows immediately.

3.3. Discarding the case where $\overline{\overline{\mathcal{A}}}$ is *not* an arithmetic progression

Let us accomplish the program given by the title of this section and prove the Theorem in the case where the set $\overline{\overline{\mathcal{A}}}$ is not an arithmetic progression, which we assume in this section. In particular, we have $u = |\overline{\overline{\mathcal{A}}}| - 1 \geq 2$ (any set with one or two elements is an arithmetic progression). In view of Lemma 11, this means that $\overline{\overline{\mathcal{A}}}$ has to be a Vosper subset.

The case $H = \{0\}$ cannot occur. Indeed, in that case, the set $\overline{\overline{\mathcal{A}}}$ coincides with $\overline{\mathcal{A}}$, $G/H = G$ and the set $\overline{\mathcal{A}}$ cannot be a Vosper subset of G because Corollary 9 implies (since $|\overline{\mathcal{A}}| = |\overline{\overline{\mathcal{A}}}| \geq 2$)

$$|j\overline{\mathcal{A}}| \geq \min(|G| - 1, j|\overline{\mathcal{A}}|)$$

contrarily to (3.3) and (3.4). Therefore we have $H \neq \{0\}$.

We shall need the H-tiling defined above. As announced, we retain the then-defined notation. Since $\overline{\overline{\mathcal{A}}}$ is a Vosper subset, it is also a Cauchy subset by Lemma 8, therefore

$$|j\overline{\overline{\mathcal{A}}}| \geq \min(|G/H|, |(j-1)\overline{\overline{\mathcal{A}}}| + |\overline{\overline{\mathcal{A}}}| - 1). \tag{3.12}$$

In fact, we even have the more precise inequality

$$|j\overline{\overline{\mathcal{A}}}| \geq |(j-1)\overline{\overline{\mathcal{A}}}| + |\overline{\overline{\mathcal{A}}}| - 1.$$

Indeed, assume the contrary, then on the one hand we have, by inequality (3.12),

$$|j\overline{\overline{\mathcal{A}}}| = |G/H| \leq |(j-1)\overline{\overline{\mathcal{A}}}| + |\overline{\overline{\mathcal{A}}}| - 2.$$

Again, since $\overline{\overline{\mathcal{A}}}$ is also a Cauchy set, we have

$$|\big((j-1)\overline{\overline{\mathcal{A}}} \setminus \{(j-1)\overline{\overline{\mathcal{A}}}^u\}\big) + \overline{\overline{\mathcal{A}}}| \geq \min\big(|G/H|, (|(j-1)\overline{\overline{\mathcal{A}}}|-1) + |\overline{\overline{\mathcal{A}}}|-1\big) = |G/H|.$$

Therefore

$$j\overline{\overline{\mathcal{A}}} \supset \big((j-1)\overline{\overline{\mathcal{A}}} \setminus \{(j-1)\overline{\overline{\mathcal{A}}}^u\}\big) + \overline{\overline{\mathcal{A}}} \supset G/H.$$

Since all the cosets corresponding to the elements of

$$\big((j-1)\overline{\overline{\mathcal{A}}} \setminus \{(j-1)\overline{\overline{\mathcal{A}}}^u\}\big) + \overline{\overline{\mathcal{A}}}$$

are full (in the same fashion as in the proof of Lemma 13), we get $j\overline{\mathcal{A}} = G$, a contradiction with (3.5).

Thus, we obtain

$$|j\overline{\overline{\mathcal{A}}}| \geq |(j-1)\overline{\overline{\mathcal{A}}}| + |\overline{\overline{\mathcal{A}}}| - 1 = |(j-1)\overline{\overline{\mathcal{A}}}| + u. \tag{3.13}$$

It follows, using Lemma 12 (recall that $j \geq 2$ holds),

$$\begin{aligned} |j\overline{\mathcal{A}}| &\geq (|(j-1)\overline{\overline{\mathcal{A}}}| + u - 1)|H| + |j\overline{\mathcal{A}}^u| \\ &\geq (|(j-1)\overline{\overline{\mathcal{A}}}| - 1)|H| + |(j-1)\overline{\mathcal{A}}^u| + u|H| \\ &\geq |(j-1)\overline{\mathcal{A}}| + u|H|. \end{aligned} \tag{3.14}$$

We now appeal to Lemma 13, which yields

$$|(j-1)\overline{\overline{\mathcal{A}}}| \leq |G/H| + 1 - |\overline{\overline{\mathcal{A}}}| = |G/H| + 1 - (u+1) \leq |G/H| - 2, \tag{3.15}$$

since $u \geq 2$.

Coming back to the bare bone of our approach, we apply Corollary 9 to $(j-1)\overline{\overline{\mathcal{A}}}$ (let us recall that $\overline{\overline{\mathcal{A}}}$ is a Vosper set). By (3.15), we get

$$|(j-1)\overline{\overline{\mathcal{A}}}| \geq \min(|G/H|-1,(j-1)|\overline{\overline{\mathcal{A}}}|) = (j-1)|\overline{\overline{\mathcal{A}}}| = (j-1)(u+1)$$

from which we obtain

$$|(j-1)\overline{\mathcal{A}}| \geq \big((j-1)(u+1)-1\big)|H| + |(j-1)\overline{\mathcal{A}}^u|. \tag{3.16}$$

This, with (3.14), shows, in the case when

$$|\overline{\mathcal{A}}^u| \leq \frac{j-2}{j-1}|H|,$$

that

$$\begin{aligned} |j\overline{\mathcal{A}}| &\geq \big((j-1)(u+1)-1\big)|H| + |(j-1)\overline{\mathcal{A}}^u| + u|H| \\ &\geq (ju+j-2)|H| + |(j-1)\overline{\mathcal{A}}^u| \\ &\geq ju|H| + (j-2)|H| + |\overline{\mathcal{A}}^u| \\ &\geq ju|H| + j|\overline{\mathcal{A}}^u| \\ &= j(u|H| + |\overline{\mathcal{A}}^u|) \geq j|\overline{\mathcal{A}}| \end{aligned}$$

contradicting (3.3). Since $j \geq 3$ implies $(j-2)/(j-1) \geq 1/2$, until the end of this subsection, we may therefore assume

$$|\overline{\mathcal{A}}^u| > \frac{|H|}{2}. \tag{3.17}$$

This supplementary hypothesis implies in particular, by Lemma 12 and the Prehistorical lemma (for $h\overline{\mathcal{A}}^u$), that all the cosets met by $h\overline{\mathcal{A}}$ are full (for $h \geq 2$). In other words, $h\overline{\mathcal{A}}$ is H-periodic for $h \geq 2$.

We now use the partition of $\mathcal{B}$ into $\mathcal{I} \cup \mathcal{J}$ introduced in (3.2). Evidently, we have

$$\big((j-1)\mathcal{A} + \{0,M\}\big) \setminus \big((j-1)\mathcal{A}\big) \subset \mathcal{I}. \tag{3.18}$$

By equation (3.16) and H-periodicity, we have

$$|(j-1)\overline{\mathcal{A}}| \geq (j-1)(u+1)|H| \geq (j-1)|\overline{\mathcal{A}}| = (j-1)(|\mathcal{A}|-1).$$

Lemma 6 (with $m = M$, $\mathcal{C} = \{0,M\}$ and $\mathcal{D} = (j-1)\mathcal{A}$) then yields

$$|(j-1)\mathcal{A} + \{0,M\}| \geq |(j-1)\mathcal{A}| + |(j-1)\overline{\mathcal{A}}| \geq |(j-1)\mathcal{A}| + (j-1)(|\mathcal{A}|-1).$$

With (3.18), this gives

$$|\mathcal{I}| \geq (j-1)(|\mathcal{A}|-1). \tag{3.19}$$

Concerning $\mathcal{J}$, by (3.13), we may select u distinct sums s_i+a_i (with $s_i \in (j-1)\overline{\overline{\mathcal{A}}}, a_i \in \overline{\overline{\mathcal{A}}}, 1 \le i \le u$) in $\big(j\overline{\overline{\mathcal{A}}}\big)\setminus\big((j-1)\overline{\overline{\mathcal{A}}}\big)$. Since $(j-1)\overline{\mathcal{A}}$ is H-periodic, for any $1 \le i \le u$, there is a set $\mathcal{S}_i \subset (j-1)\mathcal{A}$ with cardinality $|\mathcal{S}_i| = |H|$ such that all its elements are in the coset of s_i modulo H (or, equivalently, in the same residue class modulo e). We denote by $\mathcal{A}^{t_i}$ the class in which a_i falls. Now the sets of integers $\mathcal{A}^{t_i} + \mathcal{S}_i$ are disjoint subsets of $\mathcal{J}$ (their projection in G/H are by definition different) therefore, using (1.1), (3.8) and (3.17), we obtain

$$\begin{aligned}
|\mathcal{J}| &\ge \sum_{i=1}^{u} |\mathcal{A}^{t_i} + \mathcal{S}_i| \\
&\ge \sum_{i=1}^{u} (|\mathcal{A}^{t_i}| + |\mathcal{S}_i| - 1) \\
&\ge u(|\mathcal{A}^u| + |H| - 1) \\
&\ge u((|H|+1)/2 + |H| - 1) \\
&= u(3|H|/2 - 1/2) \\
&\ge (u+1)|H| - 1 \ge |\mathcal{A}| - 1. \qquad (3.20)
\end{aligned}$$

Collecting the different contributions in (3.2) given by (3.19) and (3.20), we get

$$|\mathcal{B}| = |\mathcal{I}| + |\mathcal{J}| \ge j(|\mathcal{A}| - 1),$$

that is (3.1) and the Theorem is proved in the case where $\overline{\overline{\mathcal{A}}}$ is not an arithmetic progression.

From now on, we are reduced to and therefore assume that

$$\overline{\overline{\mathcal{A}}} \text{ is an arithmetic progression.}$$

The case where H is trivial ($H = \{0\}$) is excluded since in that case, $\overline{\mathcal{A}}$ would be an arithmetic progression modulo M, which is not allowed for $\mathcal{A} \in \mathcal{F}$ (exceptions of Type II).

From now on, we will therefore assume that

$$|H| \ge 2.$$

3.4. New additional conditions on $\mathcal{A}$

Recall that we are now reduced to the case where $|H| \ge 2$ and the set $\overline{\overline{\mathcal{A}}}$ is an arithmetic progression in $G/H = \mathbb{Z}/e\mathbb{Z}$. Let us recall also that $e > 1$. Let d be an integer (with $1 \le d < M$), the projection (on G/H) of which is a difference of the arithmetic progression $\overline{\overline{\mathcal{A}}}$. Since $\gcd(\mathcal{A}) = 1$ and $0 \in \mathcal{A}$, it follows that $\gcd(d, e) = 1$.

We will use an H-tiling as defined in Section 3.2. The partition used here is obtained by defining $\mathcal{A}_i$ as the subset of $\mathcal{A}$ composed with its elements equal to id modulo e

$$\mathcal{A}_i = \{a \in \mathcal{A} \text{ such that } a \equiv id \bmod e\}.$$

This is a special case of H-tiling as defined above. Notice however that the notation used here is slightly different from that used there: for instance, there is no reason why $\mathcal{A}^i = \mathcal{A}_i$ should hold. But this is just a matter of indexation.

By assumption, 0 belongs to $\mathcal{A}$ and therefore $\mathcal{A}_0$ is not empty. Since $\mathcal{A}$ is an arithmetic progression modulo e, what we get is that the non-empty $\mathcal{A}_i$'s correspond to values of i in an *interval* of integers containing 0. Consequently, there exist two non-negative integers v and w such that

$$\mathcal{A} = \bigcup_{-v \le i \le w} \mathcal{A}_i.$$

With the preceding notation, we have $\overline{\overline{\mathcal{A}}_i} = (id \bmod e) \in \mathbb{Z}/e\mathbb{Z} = G/H$ and we can rephrase the preceding assertion with the formula

$$\overline{\overline{\mathcal{A}}} = \{-vd, \dots, 0, d, \dots, wd\} \bmod e = d.\{-v, \dots, 0, 1, \dots, w\} \bmod e.$$

If $v = w = 0$, $1 \neq e|a$ for any element a of $\mathcal{A}$, a situation which cannot occur because $\gcd(\mathcal{A}) = 1$. Therefore, we may assume

$$u = v + w \ge 1.$$

Changing if needed d into $M - d$, we may assume

$$w \ge 1.$$

In the case where also $v \ge 1$, there will be no loss of generality in assuming additionally that

$$|\mathcal{A}_w| \le |\mathcal{A}_{-v}| \tag{3.21}$$

and defining

$$\chi = |\mathcal{A}_{-v}| - |\mathcal{A}_w| \ge 0.$$

Evidently, since in this case v and w are non-zero, the same inequality should hold with bars. In the case where $v = 0$, we define arbitrarily χ to be zero.

Let us set

$$\delta = |\mathcal{A}_0| + |\mathcal{A}_w| - 2 - |H|. \tag{3.22}$$

By (3.9), it follows that

$$\delta = |\overline{\mathcal{A}}_0| + |\overline{\mathcal{A}}_w| - (|H| + 1) \ge 0.$$

We define also

$$\epsilon = \begin{cases} 1 & \text{if } \mathcal{A}_0 \text{ is } \textit{not} \text{ an arithmetic progression,} \\ 0 & \text{otherwise.} \end{cases}$$

Once again, we use the partition $\mathcal{B} = \mathcal{I} \cup \mathcal{J}$ defined in (3.2). Let us prove that

$$|\mathcal{I}| \geq |(j-1)\overline{\overline{\mathcal{A}}}| \ (|\mathcal{A}_0| + \epsilon - 1). \tag{3.23}$$

We clearly have

$$|\mathcal{I}| \geq |(j-1)\mathcal{A} + \mathcal{A}_0| - |(j-1)\mathcal{A}|. \tag{3.24}$$

Let us apply the first part of Lemma 6 with $m = e$, $\mathcal{C} = \mathcal{A}_0 \subset \{0, e, 2e, \dots, M\}$ and $\mathcal{D} = (j-1)\mathcal{A}$, ϕ being the projection modulo e. Since $\phi((j-1)\mathcal{A}) = (j-1)\overline{\overline{\mathcal{A}}}$, we obtain

$$|(j-1)\mathcal{A} + \mathcal{A}_0| \geq |(j-1)\overline{\overline{\mathcal{A}}}|(|\mathcal{A}_0| - 1) + |(j-1)\mathcal{A}|. \tag{3.25}$$

If $\epsilon = 0$, formula (3.23) follows immediately from (3.24) and (3.25).

Suppose now $\epsilon = 1$, that is $\mathcal{A}_0$ is not an arithmetic progression. In this case, one has $|\overline{\mathcal{A}}_0| \leq |H| - 1$ which implies, by (3.10), $|\mathcal{A}_i| = |\overline{\mathcal{A}}_i| \geq 2$ for any $i \neq 0$. Since we also have $|\mathcal{A}_0| \geq 2$, we deduce that any set of the form $\mathcal{A}_{i_1} + \cdots + \mathcal{A}_{i_{j-1}}$ has at least two elements. Now, for any residue class x modulo e, if the set $\phi^{-1}(x) \cap (j-1)\mathcal{A}$ is non-empty, it must contain some such sum and therefore has at least two elements. Consequently,

$$|\{x \in \mathbb{Z}/e\mathbb{Z} : \phi^{-1}(x) \cap (j-1)\mathcal{A} \neq \emptyset\}| = |(j-1)\overline{\overline{\mathcal{A}}}|.$$

Using this formula when applying the second part of Lemma 6 gives

$$|(j-1)\mathcal{A} + \mathcal{A}_0| \geq |(j-1)\overline{\overline{\mathcal{A}}}|(|\mathcal{A}_0| - 1) + |(j-1)\mathcal{A}| + |(j-1)\overline{\overline{\mathcal{A}}}|,$$

which implies formula (3.23).

As a consequence of (3.23), and since $\overline{\overline{\mathcal{A}}}$ is an arithmetic progression, we obtain

$$\begin{aligned} |\mathcal{I}| &\geq \big((j-1)(|\overline{\overline{\mathcal{A}}}| - 1) + 1\big) \ (|\mathcal{A}_0| + \epsilon - 1) \\ &= \big((j-1)u + 1\big)(|\mathcal{A}_0| + \epsilon - 1). \end{aligned} \tag{3.26}$$

What about $\mathcal{J}$? For sure, it contains

$$(j-1)\mathcal{A}_w + \mathcal{A}_1, \dots, (j-1)\mathcal{A}_w + \mathcal{A}_{w-1}, j\mathcal{A}_w$$

and, additionally in the case $v < 0$,

$$(j-1)\mathcal{A}_{-v} + \mathcal{A}_{-1}, \dots, (j-1)\mathcal{A}_{-v} + \mathcal{A}_{-v+1}, j\mathcal{A}_{-v}.$$

And all the two-by-two intersections of these sets are empty because their projection modulo e belong to distinct H-cosets. This follows easily from

$$\begin{aligned}(j-1)\overline{\overline{\mathcal{A}}} &= d.\{-(j-1)v,\dots,0,1,\dots,(j-1)w\} \bmod e,\\ j\overline{\overline{\mathcal{A}}} &= d.\{-jv,\dots,0,1,\dots,jw\} \bmod e,\end{aligned}$$

and $1+j(v+w)\le e$ (by Lemma 13).

Thus, applying repetitively (1.1) yields (notice that if $v=0$, the second sum is zero)

$$\begin{aligned}|\mathcal{J}| &\ge \sum_{s=1}^{w}|(j-1)\mathcal{A}_w+\mathcal{A}_s| + \sum_{1\le t\le v}|(j-1)\mathcal{A}_{-v}+\mathcal{A}_{-t}|\\ &\ge \sum_{s=1}^{w}\Big((j-1)(|\mathcal{A}_w|-1)+|\mathcal{A}_s|\Big)\\ &\qquad + \sum_{1\le t\le v}\Big((j-1)(|\mathcal{A}_{-v}|-1)+|\mathcal{A}_{-t}|\Big)\\ &= (j-1)w(|\mathcal{A}_w|-1)+(j-1)v(|\mathcal{A}_{-v}|-1)+(|\mathcal{A}|-|\mathcal{A}_0|)\\ &= (j-1)w(|\mathcal{A}_w|-1)+(j-1)v(|\mathcal{A}_w|+\chi-1)+(|\mathcal{A}|-|\mathcal{A}_0|)\\ &= (j-1)u(|\mathcal{A}_w|-1)+(j-1)v\chi+|\mathcal{A}|-|\mathcal{A}_0|. \qquad (3.27)\end{aligned}$$

We notice that, using the definition (3.22) of δ, we can write

$$\begin{aligned}u(|\mathcal{A}_0|+|\mathcal{A}_w|-2) &= (u-1)(|H|+\delta)+(|\mathcal{A}_0|+|\mathcal{A}_w|-2)\\ &= (|\mathcal{A}_0|+(u-1)|H|+|\mathcal{A}_w|)+(u-1)\delta-2\\ &\ge |\mathcal{A}|+(u-1)\delta-2.\end{aligned}$$

Using this, (3.26) and (3.27), we obtain

$$\begin{aligned}|\mathcal{I}|+|\mathcal{J}| &\ge ((j-1)u+1)(|\mathcal{A}_0|+\epsilon-1)+(j-1)u(|\mathcal{A}_w|-1)\\ &\qquad +(j-1)v\chi+|\mathcal{A}|-|\mathcal{A}_0|\\ &= (|\mathcal{A}|-1)+(j-1)u(|\mathcal{A}_0|+\epsilon-1+|\mathcal{A}_w|-1)+\epsilon+(j-1)v\chi\\ &= (|\mathcal{A}|-1)+(j-1)\big(u(|\mathcal{A}_0|+|\mathcal{A}_w|-2)+u\epsilon+v\chi\big)+\epsilon\\ &\ge (|\mathcal{A}|-1)+(j-1)\big(|\mathcal{A}|+(u-1)\delta-2+u\epsilon+v\chi\big)+\epsilon\\ &= j(|\mathcal{A}|-1)+(j-1)\big((u-1)\delta+u\epsilon+v\chi-1\big)+\epsilon\\ &\ge j(|\mathcal{A}|-1)+(j-1)\big((u-1)\delta+v\chi+\epsilon-1\big)+\epsilon. \qquad (3.28)\end{aligned}$$

A look at (3.1) shows that we are done except if

$$(j-1)((u-1)\delta+v\chi+\epsilon-1)+\epsilon<0, \qquad (3.29)$$

which we assume thereafter. This implies (since $j\ge 3$) that

$$\epsilon=0.$$

Therefore, from now on, we assume that $\mathcal{A}_0$ is an arithmetic progression. Since 0 and M are in $\mathcal{A}_0$, the fact that $\mathcal{A}_0$ is an arithmetic progression of integers implies that $\overline{\mathcal{A}}_0$ is a *subgroup* of H.

Moreover, inequality (3.29) implies also

$$(u-1)\delta = v\chi = 0.$$

Therefore either $u = 1$ (in which case $v = 0$) or $u \geq 2$: in this latter case, $\delta = 0$ and either $v = 0$, or $v > 0$ and $|\mathcal{A}_{-v}| = |\mathcal{A}_w|$ (equivalently $\chi = 0$).

We shall now prove that

$$|\mathcal{A}_i| = |H|, \tag{3.30}$$

for any value of i different from 0 and w. Equality (3.30) is obviously true in the case $u = 1$ since the existence of a value of $i \neq 0, w$ implies that $u = v + w \geq 2$. Now, if $u \geq 2$, by $\delta = 0$, we get

$$|\overline{\mathcal{A}}_0| + |\overline{\mathcal{A}}_w| = |H| + 1. \tag{3.31}$$

Since $(u+1)|H| = |\overline{\mathcal{A}} + H| \leq |\overline{\mathcal{A}}| + |H| - 1$, equation (3.31) implies

$$|\overline{\mathcal{A}}_{-v}| + \cdots + |\overline{\mathcal{A}}_{-1}| + |\overline{\mathcal{A}}_1| + \cdots + |\overline{\mathcal{A}}_{w-1}| \geq (u-1)|H|$$

and equality (3.30) holds necessarily.

3.5. Discarding the case $|\mathcal{A}_0| < |H| + 1$

Here, the subgroup $\overline{\mathcal{A}}_0$ has to be strict in view of the hypothesis of the subsection. In particular, we get

$$|\overline{\mathcal{A}}_0| \leq |H|/2.$$

In other words $\overline{\mathcal{A}}_0$ is of the form

$$\overline{\mathcal{A}}_0 = \{0, \lambda e, 2\lambda e, \ldots, M\}$$

for some integer $\lambda \geq 2$ dividing M/e.

By (3.9), for any value of i different from 0, we have

$$|\overline{\mathcal{A}}_i| \geq |H| + 1 - |\overline{\mathcal{A}}_0| \geq |H|/2 + 1 > |\overline{\mathcal{A}}_0|.$$

Hence $\overline{\mathcal{A}}_i$ meets at least two distinct $\overline{\mathcal{A}}_0$-cosets. Equivalently, each $\overline{\mathcal{A}}_i$ contains at least two different values modulo λe.

So we may improve on (3.26) by using again (the first part of) Lemma 6 but with the following parameters : $m = \lambda e$, $\mathcal{C} = \mathcal{A}_0 \subset \{0, \lambda e, 2\lambda e, \ldots, M\}$

and $\mathcal{D} = (j-1)\mathcal{A}$, ϕ being now the projection modulo λe. In the same way as in (3.26), we obtain

$$|\mathcal{I}| \geq |(j-1)\mathcal{A} + \mathcal{A}_0| - |(j-1)\mathcal{A}| \geq |\phi((j-1)\mathcal{A})|(|\mathcal{A}_0| - 1).$$

Since each $\overline{\mathcal{A}_i}$ contains at least two values different modulo λe, any element of $\overline{\mathcal{A}_{i_1}} + \cdots + \overline{\mathcal{A}_{i_{j-1}}}$ (with $(i_1, \ldots, i_{j-1}) \neq (0, \ldots, 0)$) contains at least two different elements modulo λe. On the other hand, $(j-1)\overline{\mathcal{A}_0}$ contains exactly one element modulo λe. Thus

$$|\phi((j-1)\overline{\mathcal{A}})| \geq 2|(j-1)\overline{\overline{\mathcal{A}}}| - 1$$

and we get

$$|\mathcal{I}| \geq \Big(2\big((j-1)u+1\big) - 1\Big)(|\mathcal{A}_0| - 1) = (2(j-1)u+1)(|\mathcal{A}_0| - 1)$$

which leads, restarting from (3.28) and using $u \geq 1, |\mathcal{A}_0| \geq 2$, to

$$\begin{aligned} |\mathcal{I}| + |\mathcal{J}| &\geq j(|\mathcal{A}| - 1) - (j-1) + (j-1)u(|\mathcal{A}_0| - 1) \\ &= j(|\mathcal{A}| - 1) + (j-1)\big(u(|\mathcal{A}_0| - 1) - 1\big) \\ &\geq j(|\mathcal{A}| - 1), \end{aligned}$$

which implies (3.1).

From now on, we consequently assume that

$$|\mathcal{A}_0| = |H| + 1, \tag{3.32}$$

that is to say $\overline{\mathcal{A}_0} = H$. Notice that this implies

$$v = 0$$

and, as a consequence, $w = u$. Indeed, suppose that $v > 0$. Since $|\mathcal{A}_0| = |H| + 1$, then by $\delta = 0$ and $\chi v = 0$, we have $|\mathcal{A}_{-v}| = |\mathcal{A}_w| = 1$ contrary to (3.30) for $i = -v$.

3.6. Conclusion of the proof

Suppose first that $u \geq 2$. In that case, $\overline{\mathcal{A}}$ is an arithmetic progression modulo H of length at least 3 and, since we must have $\delta = 0$, we obtain by (3.32) and (3.31) that $|\mathcal{A}_u| = 1$. But, with (3.30), this is exactly the description of an exception of Type IV, leading to a contradiction in view of $\mathcal{A} \notin \mathcal{F}$.

Therefore, we shall assume that

$$u = 1.$$

In this case, we have $\mathcal{A} = \mathcal{A}_0 \cup \mathcal{A}_1$. Since $\mathcal{A} \notin \mathcal{F}$, the case where $|\mathcal{A}_1| = 1$ cannot happen. Otherwise, $\mathcal{A}_1$ could be seen as an arithmetic progression with the same difference as that of $\mathcal{A}_0$ (and lead to a Type I exception); so we assume $|\mathcal{A}_1| \geq 2$.

Assume now that the set $\mathcal{A}_1$ is *not* an arithmetic progression. Then, since the residue class of $j\overline{\mathcal{A}}_1$ is not in $(j-1)\overline{\mathcal{A}}$, we have, with the preceding notation and by (1.2),

$$|\mathcal{J}| \geq |j\mathcal{A}_1| \geq j|\mathcal{A}_1|.$$

Adding this and (3.26) yields

$$|\mathcal{B}| \geq j(|\mathcal{A}_0| - 1) + j|\mathcal{A}_1| = j(|\mathcal{A}| - 1),$$

that implies (3.1).

So, until the end of this section, we assume that $\mathcal{A}_1$ *is* an arithmetic progression. This means that we are in the following situation: the difference of the arithmetic progression $\mathcal{A}_1$ is a multiple (say, s) of that of $\mathcal{A}_0$ (that is e). In this situation, $\mathcal{A}$ is of the form

$$\mathcal{A} = \underbrace{\{0, e, 2e, \ldots, M-e, M\}}_{\mathcal{A}_0} \cup \underbrace{\{b, b+se, \ldots, b+use\}}_{\mathcal{A}_1},$$

where e divides M ($e \neq 1, M$), b is coprime to e and s and u are two positive integers subject to $b + use < M$.

If $s = 1$, $\mathcal{A}$ is the union of two arithmetic progressions with the same common difference, which leads again to a Type I exception. If $s \geq 2$, we are led to a Type III exception. The Theorem is proved.

4. Recovering Theorem 3

The case $j = 2$ of Theorem 3 is implied by the $3k-3$ Theorem. Let j be an integer greater than or equal to 3. We assume the result to be proved up to $j-1$ and want to prove its validity for j. We proceed by induction.

Let $\mathcal{A}$ be a normal set of non-negative integers and $M = \max(\mathcal{A})$. We assume that $\mathcal{A}$ verifies $|\mathcal{A}| < 1 + M/j$, that $\mathcal{A}$ is not the union of two arithmetic progressions with the same common difference, nor an arithmetic progression modulo M nor of the form $\mathcal{A} = \{0, M/2, M, x, x + M/2, 2x\}$ for some positive integer $x < M/2$ (and M even).

We distinguish two cases according to whether or not $\mathcal{A}$ belongs to $\mathcal{F}$. If $\mathcal{A}$ belongs to $\mathcal{F}$, since by assumption $\mathcal{A}$ cannot be composed of two arithmetic progressions with the same common difference nor be an arithmetic progression modulo its maximal element, only two cases remain to be investigated: Type III and Type IV exceptions. This will be done in Section 4.1 and 4.2 respectively. The case when $\mathcal{A}$ does not belong to $\mathcal{F}$ will be treated in Section 4.3. As it will turn out, the induction hypothesis will be used only in this last case.

4.1. Type III exceptions

This case leads us to some kind of addendum to Section 3.6. We have $\mathcal{A} = \mathcal{A}_0 \cup \mathcal{A}_1$ with $\mathcal{A}_0$ and $\mathcal{A}_1$ two arithmetic progressions, the difference of $\mathcal{A}_1$ being a strict multiple of that of $\mathcal{A}_0$. Recall also that we may assume $|\mathcal{A}_0| \geq 3$ and $|\mathcal{A}_1| \geq 2$.

Evidently, if we replace $\mathcal{A}_0$ by one of its multiples $s\mathcal{A}_0$ and $\mathcal{A}_1$ by one of its multiples $t\mathcal{A}_1$, both sets are still arithmetic progressions and their differences are unchanged.

We shall need the following lemma which expresses that in such a situation, the sumset is large.

Lemma 14 *Let $\mathcal{C}$ and $\mathcal{D}$ be two arithmetic progressions of integers of length at least two, such that the difference of $\mathcal{D}$ is equal to q times that of $\mathcal{C}$. Then,*

$$|\mathcal{C}+\mathcal{D}| = \begin{cases} |\mathcal{C}| \times |\mathcal{D}| & \text{if } |\mathcal{C}| \leq q, \\ |\mathcal{C}| + q(|\mathcal{D}|-1) & \text{otherwise.} \end{cases}$$

In particular, if $q \geq 2$,

$$|\mathcal{C}+\mathcal{D}| \geq |\mathcal{C}| + 2(|\mathcal{D}|-1).$$

Proof. By translation and integral dilatation, it is sufficient to observe that the result holds in the case where $\mathcal{C} = \{0, 1, \ldots, c-1\}$ and $\mathcal{D} = \{0, q, \ldots, (d-1)q\}$. But we can compute immediately that if $c \leq q$, then

$$\mathcal{C}+\mathcal{D} = \{0, 1, \ldots, c-1, q, q+1, \ldots, q+c-1, 2q, \ldots, (d-1)q+c-1\}$$

which has cardinality $cd = |\mathcal{C}| \times |\mathcal{D}|$. Otherwise, that is if $c > q$,

$$\mathcal{C}+\mathcal{D} = \{0, 1, \ldots, (d-1)q+c-1\}$$

and

$$|\mathcal{C}+\mathcal{D}| = (d-1)q + c = |\mathcal{C}| + q(|\mathcal{D}|-1).$$

There remains to check that the final lower bound holds. Indeed if $|\mathcal{C}| \leq q$, this follows from

$$|\mathcal{C}| \times |\mathcal{D}| \geq |\mathcal{C}| + 2(|\mathcal{D}|-1),$$

an inequality equivalent to

$$(|\mathcal{C}|-2)(|\mathcal{D}|-1) \geq 0.$$

Otherwise, this follows simply from $q \geq 2$. ∎

Applying this shows that, for any positive integers s and t, we have

$$|s\mathcal{A}_0 + t\mathcal{A}_1| \geq |s\mathcal{A}_0| + 2(|t\mathcal{A}_1| - 1).$$

This yields, using again the partition into disjoint subsets

$$\bigcup_{s=0}^{j} \big((j-s)\mathcal{A}_0 + s\mathcal{A}_1\big)$$

and inequality (1.1),

$$\begin{aligned}
|j\mathcal{A}| &\geq |j\mathcal{A}_0| + \sum_{s=1}^{j-1} \big(|(j-s)\mathcal{A}_0| + 2(|s\mathcal{A}_1| - 1)\big) + |j\mathcal{A}_1| \\
&\geq \big(j(|\mathcal{A}_0| - 1) + 1\big) + j\big(|\mathcal{A}_1| - 1\big) + 1 \\
&\quad + \sum_{s=1}^{j-1} \Big(\big((j-s)(|\mathcal{A}_0| - 1) + 1\big) + 2\big(s(|\mathcal{A}_1| - 1) + 1\big) - 2\Big) \\
&= j(|\mathcal{A}_0| + |\mathcal{A}_1| - 2) + \frac{j(j-1)}{2}\big(|\mathcal{A}_0| - 1 + 2(|\mathcal{A}_1| - 1)\big) + j + 1 \\
&= \frac{j(j+1)}{2}\big(|\mathcal{A}| - 2\big) + \frac{j(j-1)}{2}(|\mathcal{A}_1| - 1) + j + 1 \\
&\geq \frac{j(j+1)}{2}\big(|\mathcal{A}| - 2\big) + \frac{j(j-1)}{2} + j + 1 \\
&= \frac{j(j+1)}{2}\big(|\mathcal{A}| - 1\big) + 1
\end{aligned}$$

and the conclusion follows.

4.2. Type IV exceptions

This section, devoted to the study of Type IV exceptions, leads us to some kind of addendum to Section 3.4 in the special case

$$u \geq 2.$$

We may come back to the proof and the notation of this section. Recall (that was (3.30)) that we have

$$|\mathcal{A}_i| = |H|$$

for any i different from 0 and u. Recall also that

$$|\mathcal{A}_0| = |H| + 1 \qquad \text{and} \qquad |\mathcal{A}_u| = 1.$$

Also, we have

$$|H| \geq 2.$$

Now, observe (just consider the associated residue classes) that the sets in the following list are two-by-two disjoints:

$$\begin{array}{ccccc}
 & & & j\mathcal{A}_0, & \\
(j-1)\mathcal{A}_0+\mathcal{A}_1, & (j-1)\mathcal{A}_0+\mathcal{A}_2, & \dots, & (j-1)\mathcal{A}_0+\mathcal{A}_{u-1}, \\
(j-2)\mathcal{A}_0+\mathcal{A}_1+\mathcal{A}_{u-1}, & (j-2)\mathcal{A}_0+\mathcal{A}_2+\mathcal{A}_{u-1}, & \dots, & (j-2)\mathcal{A}_0+2\mathcal{A}_{u-1}, \\
(j-3)\mathcal{A}_0+\mathcal{A}_1+2\mathcal{A}_{u-1}, & (j-3)\mathcal{A}_0+\mathcal{A}_2+2\mathcal{A}_{u-1}, & \dots, & (j-3)\mathcal{A}_0+3\mathcal{A}_{u-1}, \\
 & & \vdots & & \\
\mathcal{A}_0+\mathcal{A}_1+(j-2)\mathcal{A}_{u-1}, & \mathcal{A}_0+\mathcal{A}_2+(j-2)\mathcal{A}_{u-1}, & \dots, & \mathcal{A}_0+(j-1)\mathcal{A}_{u-1}, \\
\mathcal{A}_1+(j-1)\mathcal{A}_{u-1}, & \mathcal{A}_2+(j-1)\mathcal{A}_{u-1}, & \dots, & j\mathcal{A}_{u-1}, \\
(j-1)\mathcal{A}_{u-1}+\mathcal{A}_u, & (j-2)\mathcal{A}_{u-1}+2\mathcal{A}_u, & \dots, & j\mathcal{A}_u.
\end{array}$$

We count the number of elements of each sum in this list using what we just mentioned. Since all the $\mathcal{A}_i$'s are arithmetic progressions with the same common difference, the cardinality of each element from this list is easily calculated.

We have

$$|j\mathcal{A}_0| = j|H|+1.$$

On the second line, each sum (there are $u-1$ such sums) has

$$(j-1)|H|+(|H|-1)+1 = j|H|$$

elements. On the third line (there are also $u-1$ terms) each term has $j|H|-1$ elements and so on. On the last but one line, every set has $j|H|-j+1$ elements. Concerning the last line, the s-th sumset ($1 \le s \le j$) has $(j-s)(|H|-1)+1$ elements.

So, the total number of elements in $j\mathcal{A}$ is at least

$$\begin{aligned}
|j\mathcal{A}| &\ge (j|H|+1)+(u-1)\sum_{i=0}^{j-1}\big(j|H|-i\big)+\sum_{s=1}^{j}\big((j-s)(|H|-1)+1\big) \\
&= j|H|+1+(u-1)\Big(j^2|H|-\frac{j(j-1)}{2}\Big)+\frac{j(j-1)}{2}(|H|-1)+j.
\end{aligned}$$

Therefore,

$$\begin{aligned}
|j\mathcal{A}| &- \Big(\frac{j(j+1)}{2}(|\mathcal{A}|-1)+1\Big) = \\
&= |j\mathcal{A}|-\Big(\frac{j(j+1)}{2}\big((|H|+1)+(u-1)|H|+1-1\big)+1\Big) \\
&\ge j|H|+1+(u-1)\Big(j^2|H|-\frac{j(j-1)}{2}\Big) \\
&\quad +\frac{j(j-1)}{2}(|H|-1)+j-\Big(\frac{j(j+1)}{2}(u|H|+1)+1\Big) \\
&= j(j-1)\Big(\frac{(u-1)(|H|-1)}{2}-1\Big)
\end{aligned}$$

and the result follows unless $u = |H| = 2$. In this case, we are led to sets $\mathcal{A} = \mathcal{A}_0 \cup \mathcal{A}_1 \cup \mathcal{A}_2$, with $|\mathcal{A}_1| = 2$ and $|\mathcal{A}_2| = 1$, that is to a set $\mathcal{A}$ of the form

$$\mathcal{A} = \{0, M/2, M, x, x + M/2, 2x\},$$

a case excluded by hypothesis.

4.3. The generic case

Assume that $\mathcal{A}$ is not in $\mathcal{F}$ and apply Theorem 4. The numerical bound must hold

$$|\mathcal{B}| = |(j\mathcal{A}) \setminus \big((j-1)\mathcal{A}\big)| \geq \min(M-1, j(|\mathcal{A}|-1)) = j(|\mathcal{A}|-1),$$

on recalling $|\mathcal{A}| < 1 + M/j$. On the other hand, the same bound on $|\mathcal{A}|$ implies that we have $|\mathcal{A}| \leq (M-1)/j + 1 \leq (M-1)/(j-1) + 1$ and we can apply the induction hypothesis which gives

$$|(j-1)\mathcal{A}| \geq \frac{j(j-1)}{2}\,(|\mathcal{A}|-1) + 1.$$

Adding these two bounds together gives

$$\begin{aligned} |j\mathcal{A}| &= |(j-1)\mathcal{A}| + |\mathcal{B}| \\ &\geq \Big(\frac{j(j-1)}{2}(|\mathcal{A}|-1) + 1\Big) + j(|\mathcal{A}|-1) \\ &= \frac{j(j+1)}{2}(|\mathcal{A}|-1) + 1 \end{aligned}$$

and Theorem 3 is proved.

5. A Frobenius corollary

In the light of Theorem 3, we may revisit the Frobenius problem. Indeed, as a corollary of Theorem 3, we obtain a new proof of a result on the Frobenius problem (the best known of this nature).

Let $\mathcal{A}$ be a set of positive integers. It is a well known fact that, if $\gcd(\mathcal{A}) = 1$, then every sufficiently large integer can be written as a sum of elements from $\mathcal{A}$ (with repetitions allowed). The Diophantine Frobenius problem consists in determining the largest integer, denoted by $G(\mathcal{A})$, *not* representable in such a form. Sylvester [18] already knew that

$$G(\{a_1, a_2\}) = (a_1 - 1)(a_2 - 1) - 1.$$

However, as soon as $|\mathcal{A}| \geq 3$, computing this number is, in general, a difficult problem.

Here, we are interested in the following problem: given two positive integers n and M, with $3 \leq n \leq M$, what is the maximal value of $G(\mathcal{A})$ for $\mathcal{A} \subset \{1, \ldots, M\}$, $\gcd(\mathcal{A}) = 1$ and $|\mathcal{A}| = n$. Notice that the problem is trivial if $n = M$.

Erdös and Graham [4] proved that this maximal value is less than or equal to $2M^2/n$ and conjectured that this upper bound could be replaced by $M^2/(n-1)$. This conjecture was finally proved by Dixmier [3].

Theorem 15 (Dixmier's Theorem 3 in [3]) *Let $\mathcal{A}$ be a set of positive integers such that $\gcd(\mathcal{A}) = 1$. Define $M = \max(\mathcal{A})$, $n = |\mathcal{A}|$ and assume $2 \leq n < M$. Then, letting*

$$r = (n-1)\left(\left[\frac{M-1}{n-1}\right] + 1\right) - (M-1),$$

the unique integer, $1 \leq r \leq n-1$, equal to $-(M-1)$ modulo $n-1$, one has

$$G(\mathcal{A}) \leq \left[\frac{M-1}{n-1}\right](M-r-1) - 1.$$

A new proof of Dixmier's theorem was obtained by Lev [14] as an application of his multiple set version of the $3k-4$ Theorem quoted in the Introduction (Theorem 2). The following improvement was first obtained in [9]. As shown in this paper, it implies Lewin's conjecture [15].

Corollary 16 (of our Theorem 3) *Let $\mathcal{A}$ be a set of positive integers satisfying $\gcd(\mathcal{A}) = 1$. Define $M = \max(\mathcal{A}), n = |\mathcal{A}|$ and assume that $3 \leq |\mathcal{A}| \leq M/2$. Assume also that $\mathcal{A} \cup \{0\}$ is neither the union of two arithmetic progressions with the same common difference, nor of the form $\mathcal{A} = \{0, M/2, M, x, x + M/2, 2x\}$ for some positive integer $x < M/2$. Define $r = n([M/n] + 1) - M$. If $r \neq n$, then one has*

$$G(\mathcal{A}) \leq \left[\frac{M}{n}\right](M-r) - 1.$$

Here, we present a new proof of it, as an immediate corollary of our Theorem 3. In this sense, our approach generalizes that of Lev. We will need two lemmata. First, a slight generalization of a lemma by Dixmier [3] (Dixmier proved it only in a special case but the reader may observe that the following statement boils down to the original Dixmier's lemma):

Lemma 17 (Dixmier's lemma) *Let N be a positive integer and let $\mathcal{C} \subset \{1, \ldots, N\}$. If $N/2 < |\mathcal{C}| < N$, then*

$$G(\mathcal{C}) \leq 2(N - |\mathcal{C}|) - 1.$$

For stating the second lemma, we need a definition. A set of positive integers $\mathcal{A}$ with maximum M is said to be *saturated* if for any x, y in $\mathcal{A}$, either $x+y \in \mathcal{A}$ or $x+y > M$. The requested lemma is the following.

Lemma 18 (Lemma 11.3 in [9]) *Let $\mathcal{B}$ be a saturated set of positive integers. Assume that $\gcd(\mathcal{B}) = 1$, that $|\mathcal{B}| \leq \max(\mathcal{B})/2$ and that $\mathcal{B}$ is an arithmetic progression modulo $\max(\mathcal{B})$. Then $\mathcal{B} \cup \{0\}$ is the union of two arithmetic progressions with the same common difference.*

We are now ready to come to the proof of our Frobenius Corollary.

Proof of Corollary 16. Let us set $s = [M/n]+1 \geq 3$, so that $sn = M+r$. We stress the fact that r satisfies a priori $1 \leq r \leq n$, but here we assume $r < n$. We define $\mathcal{A}' = \mathcal{A} \cup \{0\}$. Notice that $\mathcal{A}'$ and $\mathcal{A}$ coincide modulo M but

$$|\mathcal{A}'| = |\mathcal{A}| + 1 = n + 1.$$

We now distinguish two cases depending on the structure of $\mathcal{A}$ modulo M.

Assume first that $\mathcal{A}$ is *not* an arithmetic progression modulo M. We have $(s-1)(|\mathcal{A}'|-1) = sn - n < sn - r = M$. In view of the assumptions on $\mathcal{A}'$ in Corollary 16, Theorem 3 implies

$$|(s-1)\mathcal{A}'| \geq \frac{s(s-1)}{2}n + 1.$$

Putting

$$\mathcal{C} = \big((s-1)\mathcal{A}'\big) \setminus \{0\} = \bigcup_{j=1}^{s-1} j\mathcal{A} \subset \{1, 2, \ldots, (s-1)M\},$$

it follows that

$$|\mathcal{C}| \geq \frac{s(s-1)}{2}n = \frac{(M+r)(s-1)}{2} = \frac{M(s-1)}{2} + \frac{r(s-1)}{2}.$$

We may assume that $|\mathcal{C}| < (s-1)M$ (otherwise $\mathcal{A}$ must contain 1 and $G(\mathcal{A}) = 0$). Since $r(s-1) > 0$, using Dixmier's lemma, we infer that

$$G(\mathcal{A}) = G(\mathcal{C}) \leq (s-1)(M-r) - 1 = \left[\frac{M}{n}\right](M-r) - 1,$$

which proves the result.

We now assume that $\mathcal{A}$ *is* an arithmetic progression modulo M. The set $\mathcal{A}$ cannot be saturated. Otherwise, by Lemma 18, $\mathcal{A}'$ must be a union of two arithmetic progressions with the same common difference, a case which

is excluded by assumption. So, there are x, y in $\mathcal{A}$, with $x+y \notin \mathcal{A}$ and $x+y < M$. Let us define $\mathcal{A}'' = \mathcal{A} \cup \{x+y\} \subset \{1, 2, \ldots, M\}$, a set with $|\mathcal{A}''| = n+1$ elements. We clearly have $G(\mathcal{A} \cup \{x+y\}) = G(\mathcal{A})$. On the other hand, we have $r = n([M/n]+1) - M$ which yields

$$\begin{aligned} r+1 &= n\left(\left[\frac{M}{n}\right]+1\right) - (M-1) \\ &= (|\mathcal{A}''|-1)\left(\left[\frac{M}{|\mathcal{A}''|-1}\right]+1\right) - (M-1) \\ &= (|\mathcal{A}''|-1)\left(\left[\frac{M-1}{|\mathcal{A}''|-1}\right]+1\right) - (M-1), \end{aligned}$$

since $M/(|\mathcal{A}''|-1) = M/n$ cannot be an integer (otherwise $r = n$). We may thus apply Dixmier's theorem to $\mathcal{A}''$. Since $G(\mathcal{A}) = G(\mathcal{A}'')$, we obtain:

$$\begin{aligned} G(\mathcal{A}) &\leq \left[\frac{M-1}{|\mathcal{A}''|-1}\right](M-(r+1)-1)-1 \\ &= \left[\frac{M-1}{n}\right](M-r-2)-1 \leq \left[\frac{M}{n}\right](M-r)-1. \end{aligned}$$

Hence the result. ■

References

[1] CAUCHY, A.-L.: Recherches sur les nombres. *J. École Polytech.* **9** (1813), 99–123.

[2] DAVENPORT, H.: On the addition of residue classes. *J. London Math. Soc.* **10** (1935), 30–32.

[3] DIXMIER, J.: Proof of a conjecture by Erdös and Graham concerning the problem of Frobenius. *J. Number Theory* **34** (1990), 198–209.

[4] ERDÖS, P., GRAHAM, R. L.: On a linear Diophantine problem of Frobenius. *Acta Arith.* **21** (1972), 399–408.

[5] FREIMAN, G. A.: On the addition of finite sets. I. *Izv. Vyssš. Učebn. Zaved. Matematika* **6** (13) (1959), 202–213.

[6] FREIMAN, G. A.: Inverse problems of additive number theory. VI. On the addition of finite sets. III. The method of trigonometric sums. *Izv. Vyssš. Učebn. Zaved. Matematika* **3 (28)** (1962), 151–157.

[7] FREIMAN, G. A.: *Foundations of a structural theory of set addition.* Transations of Mathmatical Monographs **37**. American Mathematical Society, Providence, R. I., 1973.

[8] FREIMAN, G. A.: Structure theory of set addition. *Astérisque* **258** (1999), 1–33.

[9] ould Hamidoune, Y.: Some results in additive number theory I: The critical pair theory. *Acta Arith.* **96** (2000), no. 2, 97–119.

[10] ould Hamidoune, Y.: On the Diophantine Frobenius problem. *Portugal. Math.* **55** (1998), no. 4, 425–449.

[11] ould Hamidoune, Y., Plagne, A.: A generalization of Freiman's $3k-3$ theorem. *Acta Arith.* **103** (2002), no. 2, 147–156.

[12] ould Hamidoune, Y., Plagne, A.: A new critical pair theorem applied to sum-free sets in Abelian groups. *Comment. Math. Helv.* **79** (2004), no. 1, 183–207.

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

[14] Lev, V. F.: Structure theorem for multiple addition and the Frobenius problem. *J. Number Theory* **58** (1996), 79–88.

[15] Lewin, M.: A bound for a solution of a linear Diophantine problem. *J. London Math. Soc. (2)* **6** (1972), 61–69.

[16] Nathanson, M. B.: *Additive number theory. Inverse problems and the geometry of sumsets.* Graduate Texts in Mathematics **165**. Springer-Verlag, New York, 1996.

[17] Steinig, J.: On Freiman's theorems concerning the sum of two finite sets of integers. *Astérisque* **258** (1999), 129–140.

[18] Sylvester, J. J.: Mathematical questions with their solutions. *Educational Times* **41** (1884), 21.

[19] Vosper, A. G.: The critical pairs of subsets of a group of prime order. *J. London Math. Soc.* **31** (1956), 200–205. Addendum to "The critical pairs of subsets of a group of prime order", *J. London Math. Soc.* **31** (1956), 280–282.

Recibido: 18 de diciembre de 2002.
Revisado: 13 de marzo de 2003.

Yahya ould Hamidoune
CNRS et Équipe Combinatoire
Université Pierre et Marie Curie
Case 189, 4 place Jussieu
75005 Paris, France
yha@ccr.jussieu.fr

Alain Plagne
CMLS
École polytechnique
91128 Palaiseau Cedex, France
plagne@math.polytechnique.fr