ACTA ARITHMETICA
XCVI.2 (2000)

Some results in additive number theory I: The critical pair theory

by

Yahya Ould Hamidoune (Paris)

1. Introduction. Let G be an abelian group, and let A and B be finite subsets of G such that $2 \le |A|, |B|$. The Cauchy–Davenport Theorem [1, 3] states that $|A + B| \ge \min(|G|, |A| + |B| - 1)$ if $|G|$ is a prime. Vosper's Theorem [24] states that $|A + B| \ge \min(|G| - 1, |A| + |B|)$ if $|G|$ is a prime and if B is not an arithmetic progression. Mann's Theorem [19] states that $|A+B| < \min(|G|, |A|+|B|-1)$ only if there is a finite subgroup H such that $|H+B| < \min(|G|, |H|+|B|-1)$. Kneser's Theorem [15] states that $|A+B| \ge |A|+|B|-1$ if $A+B$ is non-periodic (i.e. for all $x \ne 0$, $A+B+x \ne A+B$). J. H. B. Kempermann [14] proposed a recursive procedure which transforms a pair (A, B) such that $A+B$ is non-periodic with $|A+B| = |A|+|B|-1$ into a pair (A', B') such that $|A'+B'| = |A'|+|B'|-1$, and $|A'|+|B'| < |A|+|B|$. Unfortunately $A' + B'$ could be periodic.

The classical applications of addition theorems include the representation of elements of a finite field as sums of kth powers. A. L. Cauchy proved that every element of $\mathbb{Z}/p\mathbb{Z}$ is the sum of k kth powers. A nice application of Vosper's Theorem due to S. Chowla, H. B. Mann and E. G. Straus [2] shows that for $k \ne (p-1)/2$, every element of $\mathbb{Z}/p\mathbb{Z}$ is the sum of $[k/2] + 1$ kth powers. This last result was generalized by A. Tietäväinen [23] to finite fields with odd characteristic as an application of Kempermann's theory.

Let $\Gamma = (V, E)$ be a reflexive relation. The *connectivity* of Γ is $\kappa(\Gamma) = \min\{|\Gamma(A) \setminus A| \mid |A| \ge 1 \text{ and } |\Gamma(A)| \le |V| - 1\}$. A set A attaining the above minimum is called a *fragment*. A fragment with minimal cardinality is called an *atom*. Some properties of the connectivity and atoms are proved in [6, 7, 8], for relations with a transitive group. In 1986, we observed that these results generalize known addition theorems including Mann's Theorem. In [9], we obtained a generalization of Vosper's Theorem to abelian groups. As an application, we generalized Chowla–Mann–Straus Theorem to arbitrary finite fields. In [11], we generalized several addition theorems to non-abelian

2000 *Mathematics Subject Classification*: 11B75, 11D04, 20K99.

groups and to a more general abstract setting (relations having a transitive group of automorphisms).

The notion of connectivity cannot be used to prove additive inequalities of the form $|A+B| \geq |A|+|B|+c$, for $c > 0$. For this reason we introduced in [10] the k-isoperimetric number, which may be defined by replacing 1 by k in the above definition of connectivity. Similarly we defined k-fragments and k-atoms.

In this paper, we investigate conditions of validity of the inequality $|A+B| \geq \min(|G|-1, |A|+|B|+1)$. The tools developed here allow us to recover easily some of our previous results. We shall formulate these results in order to make this paper self-contained. We shall illustrate our critical pair theory by only one application to the Diophantine Frobenius problem, in order to limit the size of the present paper. We plan to give more applications in the future.

Let $A \subset \mathbb{N}^*$ be a finite subset such that $\gcd(A) = 1$, $m = \max(A)$, and $n = |A|$. Recall that the *Frobenius number* of A, denoted by $G(A)$, is the maximal integer that cannot be expressed as a sum of elements of A. The determination of sets A with maximal Frobenius number was undertaken by several authors (cf. the references of [12]). The arithmetic progression $\{m, m-1, \ldots, m-n+1\}$ has a big Frobenius number. But one can do better if $m \equiv 0$ or $1 \bmod (n-1)$. Assume first $m \equiv 0 \bmod (n-1)$. One can see easily that

$$G\left(\frac{m}{n-1}, 2\frac{m}{n-1}, \ldots, m, m-1\right) > G(m, m-1, \ldots, m-n+1).$$

Assume now $m \equiv 1 \bmod (n-1)$. One can see easily that

$$G\left(\frac{m-1}{n-1}, 2\frac{m-1}{n-1}, \ldots, m-1, m\right) > G(m, m-1, \ldots, m-n+1).$$

It was conjectured by M. Lewin [18] that for sufficiently large m,

$$G(A) \leq \left[\frac{(m-2)(m-n+1)}{n-1}\right] - 1.$$

Put $m+i-1 = k_i(n+i-1) - r_i$, where $1 \leq r_i \leq n+i-1$. J. Dixmier [4] proved that $G(A) \leq (k_0-1)(m-r_0-1)-1$. As observed by J. Dixmier, this bound coincides with Lewin's conjectured bound if $m \equiv 0$ or 1 or 2. An alternative proof of Dixmier's Theorem is obtained by V. Lev [17].

As an application of our generalization of Vosper's Theorem, we proved in [12] that either A has a very special structure or $G(A) \leq (k_1-1)(m-r_1)-1$. Notice that this result for $m \leq 3n$ is proved by V. Lev in [16], using the $(3k-3)$-Theorem of Freiman [5]. The maximal possible values for $G(A)$ are obtained by J. Dixmier if $m \equiv 0$ or 1 or 2. Our bound is used in [12], to

prove the uniqueness of sets attaining the bound in this case. The proof given in [12] depends on a tedious density theorem.

In this paper we shall use a new method to prove bounds on the Frobenius number which avoids the density argument. We shall use this method to obtain a simple proof for Dixmier's Theorem, using Mann's Theorem. Notice that the existing proofs require the more difficult Kneser's Theorem. This method combined with Theorem 6.4 allows substantial simplifications of our previous proof.

Put $m = k(n-1)+r$, where $0 \le r \le n-2$. Let A have $\gcd(A) = 1$ and $\max(A) = m$. Recall that for $r \in \{0,1,2\}$, Dixmier's Theorem 10.1 implies that $G(A) \le [(m-2)(m-n+1)/(n-1)] - 1$. Assume now $r \ge 3$, $n \ne 5$ and $m \ge n^3 - 1$. Our Corollary 12.4 implies that

$$G(A) \le \left[\frac{m-2}{n-1}\right](m-n+1) - 1 < \left[\frac{(m-2)(m-n+1)}{n-1}\right] - 1.$$

Hence Lewin's conjecture holds. Moreover the inequality is strict for $r \ge 3$. Notice that our critical pair theory describes the structure of the sets having a maximal Frobenius number. These sets cannot be described using Kneser's Theorem.

The organization of the paper is the following. Section 3 contains some properties of the intersection of two k-atoms. In Section 4, we use the results of Section 3 to show that one of the 1-atoms of a finite abelian Cayley relation is a subgroup. We apply this result to prove some addition theorems in Section 4. In Section 5, we study the intersection of three 2-atoms. We show that it is empty under some conditions. In Section 6, we use the results of Section 5 to show that under some conditions, a 2-atom of a finite abelian Cayley relation is a subgroup. We apply this result in Section 7 to prove some addition theorems. In Section 8, we obtain conditions for the validity of $|A+B| \ge |A| + |B| + 1$. In Section 9, we introduce the Frobenius problem. Section 10 contains our new approach to the Frobenius number. Section 11 describes a special family with large Frobenius number in terms of congruences. In Section 12, we give a new proof for our bound on the Frobenius number [12] and some applications.

2. Terminology. We denote the set of integers by $\mathbb{Z}$. The set of non-negative integers is denoted by $\mathbb{N}$. We shall write $\mathbb{N}^* = \mathbb{N} \setminus 0$. The set of integers modulo m will be denoted by $\mathbb{Z}_m$. Let G be an abelian group. A subgroup H is called *proper* if $H \ne \{0\}$ and $H \ne G$. Let $A_1, \ldots, A_j \subset G$. As usual we write $A_1 + \ldots + A_j = \{x_1 + \ldots + x_j \mid x_i \in A_i\}$. If $A_1 = \ldots = A_j = A$, we write $jA = A_1 + \ldots + A_j$. Recall the convention $0A = \{0\}$.

The following easy lemma is the simplest addition theorem. It is due to L. Lagrange when A and B are the set of squares of a prime field.

LEMMA 2.1 (folklore). *Let G be a finite group, and let $A, B \subset G$. If $|A+B| > |G|$ then $A+B = G$.*

Let V be a set. By a *relation* we mean an ordered pair $\Gamma = (V, E)$, where $E \subset V \times V$. The relation Γ is said to be *reflexive* if $\{(x,x) \mid x \in V\} \subset E$. We write

$$\Gamma(A) = \{y \in V \mid \text{there is } x \in A \text{ such that } (x,y) \in E\}.$$

The *reverse* relation of Γ is by definition $\Gamma^- = \{(x,y) \mid (y,x) \in E\}$. We put $A^* = V \setminus \Gamma(A)$. We write

$$d(\Gamma) = \min\{|\Gamma(x)| \mid x \in V\}$$

if $V \neq \emptyset$. We set $d(\Gamma) = 0$ if $V = \emptyset$.

Let $\Gamma = (V, E)$ and $\Gamma' = (V', E')$ be two relations, and let $f : V \to V'$ be a bijection. The mapping f is called an *isomorphism* from Γ onto Γ' if for every $x \in V$, $f(\Gamma(x)) = \Gamma'(f(x))$. An isomorphism from Γ onto Γ is an *automorphism* of Γ. The relation Γ is called *point-transitive* if for all $x, y \in V$, there is an automorphism f of Γ such that $f(x) = y$. The relation Γ is *self-reverse* if Γ is isomorphic to Γ^-.

We shall use the following obvious and well known lemma without explicit mention.

LEMMA 2.2 (folklore). *Let $\Gamma = (V, E)$ be a point transitive relation. Then $d(\Gamma) = |\Gamma(x)|$ for any $x \in V$. If V is finite, then $d(\Gamma) = d(\Gamma^-)$.*

Our applications in this paper require only Cayley relations on abelian groups defined below.

EXAMPLE. Let G be an abelian group, and let B be a subset of G. Set $E = \{(x,y) \mid y - x \in B\}$. The *Cayley relation* defined by B on G is $\Lambda(G, B) = (G, E)$.

Notice that $\Lambda(G, B)$ is reflexive if and only if $0 \in B$. One may check easily that

$$(\Lambda(G,B))^- = \Lambda(G, -B). \tag{1}$$

Let $a \in G$. The *a-translation* is the map $\gamma_a : G \to G$ defined by $\gamma_a(x) = a + x$.

LEMMA 2.3. *Let G be an abelian group, and let $B \subset G$. Put $\Gamma = \Lambda(G, B)$. For every $A \subset G$, $\Gamma(A) = A + B$. For every a, γ_a is an automorphism of Γ. In particular Γ is a point-transitive relation. The map $x \mapsto -x$ is an isomorphism from $\Lambda(G, B)$ onto $\Lambda(G, -B)$. In particular $\Lambda(G, B)$ is self-reverse.*

The proof is easy.

A reflexive relation $\Gamma = (V, E)$ is called *k-separable* if there exists $X \subset V$ such that $|X| \geq k$ and $|V \setminus \Gamma(X)| \geq k$. Assume Γ reflexive and k-separable.

The *k-isoperimetric number* of Γ is by definition

$$\kappa_k(\Gamma) = \min\{|\Gamma(X)| - |X| \mid |X| \geq k \text{ and } |X^*| \geq k\}.$$

In the case where Γ is not k-separable, we write $\kappa_k(\Gamma) = |V|$. Note that $\kappa_1(\Gamma)$ is the connectivity of the relation Γ, considered in [6, 7, 8].

A subset $X \subset V$ is called a *k-fragment* if $|X| \geq k$, $|X^*| \geq k$, and $|\Gamma(X)| = |X| + \kappa_k(\Gamma)$. A k-fragment with minimal cardinality is a *k-atom*. The cardinality of a k-atom of Γ is denoted by $\alpha_k(\Gamma)$.

The following isoperimetric inequality follows easily from the definition. Let $X \subset V$ be such that $|X| \geq k$. Then

$$|\Gamma(X)| \geq \min(|V| - k + 1, |X| + \kappa_k(\Gamma)). \tag{2}$$

We shall use often the following obvious lemma:

LEMMA 2.4. *Let Γ and Γ' be reflexive relations, and let f be an isomorphism from Γ onto Γ'. Then $\kappa_k(\Gamma) = \kappa_k(\Gamma')$. Moreover f maps a k-fragment (resp. k-atom) onto a k-fragment (resp. k-atom).*

3. Topology of finite relations. We need an easy lemma proved in [6] for $k = 1$, and in [10] for arbitrary k.

LEMMA 3.1 (see [10]). *Let Γ be a k-separable finite reflexive relation, and let F be a k-fragment of Γ. Then Γ^- is k-separable, and F^* is a k-fragment of Γ^-. Moreover*

$$\kappa_k(\Gamma) = \kappa_k(\Gamma^-), \tag{3}$$

$$\Gamma^-(F^*) = V \setminus F. \tag{4}$$

Proof. The proof is given in [10]. ∎

LEMMA 3.2. *Let Γ be a 2-separable finite reflexive point-transitive relation such that $\kappa_2(\Gamma) \leq d(\Gamma) - 2$. Let F be a 1-fragment of Γ. Then $|F| \geq 2$. In particular $\kappa_2(\Gamma) = \kappa_1(\Gamma)$. Moreover a subset X is a 2-fragment of Γ if and only if X is 1-fragment of Γ.*

Proof. We have $|F| \geq 2$, since otherwise $\kappa_2(\Gamma) \geq \kappa_1(\Gamma) = |\Gamma(F)| - |F| = d(\Gamma) - 1$, a contradiction. By (3), $\kappa_2(\Gamma^-) = \kappa_2(\Gamma) \leq d(\Gamma) - 2 = d(\Gamma^-) - 2$. By Lemma 3.1, F^* is a 1-fragment. It follows that $|F^*| \geq 2$. Hence $\kappa_2(\Gamma) \leq |\Gamma(F)| - |F| = \kappa_1(\Gamma)$. Therefore $\kappa_2(\Gamma) = \kappa_1(\Gamma)$. It follows easily now that F is a 2-fragment of Γ if and only if F is a 1-fragment of Γ. ∎

Notice that Lemma 3.2 may be generalized to non-point-transitive relations. Let us formulate another easy lemma.

LEMMA 3.3. *Let Γ be a finite k-separable reflexive relation. Let F_1 and F_2 be two k-fragments such that $|F_1 \cap F_2| \geq k$. Put $\varepsilon = 1$ if F_1 is a k-atom*

not contained in F_2, *and* $\varepsilon = 0$ *otherwise. Then*

$$|F_1 \setminus F_2| \geq |\Gamma(F_1) \setminus \Gamma(F_2)| + \varepsilon. \tag{5}$$

Proof. We have the following table:

$V \setminus \Gamma(F_1)$	R_{31}	R_{32}	R_{33}
$\Gamma(F_1) \setminus F_1$	R_{21}	R_{22}	R_{23}
F_1	R_{11}	R_{12}	R_{13}
	F_2	$\Gamma(F_2) \setminus F_2$	$V \setminus \Gamma(F_2)$

By the definition of a k-fragment we have

$$|R_{21}| + |R_{22}| + |R_{23}| = \kappa_k(\Gamma).$$

The following inclusion follows by an easy verification:

$$\Gamma(F_1 \cap F_2) \setminus (F_1 \cap F_2) \subset R_{12} \cup R_{22} \cup R_{21}.$$

Since $|V \setminus \Gamma(F_1 \cap F_2)| \geq |V \setminus \Gamma(F_1)| \geq k$, we have $|\Gamma(F_1 \cap F_2) \setminus (F_1 \cap F_2)| \geq \kappa_k(\Gamma)$. Hence

$$|\Gamma(F_1 \cap F_2) \setminus (F_1 \cap F_2)| \geq \kappa_k(\Gamma) + \varepsilon,$$

since otherwise $F_1 \cap F_2$ would be a k-fragment strictly contained in a k-atom. It follows that

$$\begin{aligned} |R_{21}| + |R_{22}| + |R_{23}| &= \kappa_k(\Gamma) \\ &\leq |\Gamma(F_1 \cap F_2) \setminus (F_1 \cap F_2)| - \varepsilon \\ &\leq |R_{12}| + |R_{22}| + |R_{21}| - \varepsilon. \end{aligned}$$

Therefore $|R_{12}| \geq |R_{23}| + \varepsilon$. Now

$$\begin{aligned} |F_1 \setminus F_2| &= |R_{13}| + |R_{12}| \geq |R_{13}| + |R_{23}| + \varepsilon \\ &= |(V \setminus (\Gamma(F_2))) \setminus (V \setminus (\Gamma(F_1)))| + \varepsilon \\ &= |\Gamma(F_1) \setminus \Gamma(F_2)| + \varepsilon. \end{aligned}$$

This proves (5). ∎

The above lemma allows us to get a simple proof for the basic intersection property of the k-atoms.

Proposition 3.4 (see [10]). *Let* Γ *be finite* k*-separable reflexive relation such that* $\alpha_k(\Gamma) \leq \alpha_k(\Gamma^-)$. *Let* A *be a* k*-atom, and let* F *be a* k*-fragment of* Γ *such that* $|A \cap F| \geq k$. *Then* $A \subset F$. *In particular two distinct* k*-atoms intersect in at most* $k-1$ *elements.*

Proof. Put $\varepsilon = 1$ if $A \not\subset F$, and $\varepsilon = 0$ otherwise. By Lemma 3.1, F^* is a k-fragment of Γ^-. Therefore $|A| \leq \alpha_k(\Gamma^-) \leq |F^*|$. By (4), we have $\Gamma(A) \setminus \Gamma(F) = F^* \setminus A^*$.

By (5),

$$|A \setminus F| \geq |\Gamma(A) \setminus \Gamma(F)| + \varepsilon = |F^* \setminus A^*| + \varepsilon.$$

Therefore

$$|A^* \cap F^*| = |F^*| - |F^* \setminus A^*| \geq |A| - |A \setminus F| = |A \cap F| \geq k.$$

Now we apply (5) to the fragments A^* and F^* of Γ^-. It follows that $|F^* \setminus A^*| \geq |\Gamma^-(F^*) \setminus \Gamma^-(A^*)|$. By (4), we have $\Gamma^-(F^*) = V \setminus F$ and $\Gamma^-(A^*) = V \setminus A$. It follows that

$$|F^* \setminus A^*| \geq |\Gamma^-(F^*) \setminus \Gamma^-(A^*)| = |(V \setminus F) \setminus (V \setminus A)| = |A \setminus F|.$$

Therefore $\varepsilon = 0$. In particular $A \subset F$. ∎

4. Some applications. Let G be a finite abelian group, and let B be a subset of G such that $0 \in B$. We denote $\kappa_k(\Lambda(G, B))$ by $\kappa_k(G, B)$. When B generates G, we write $\kappa_k(B)$ instead $\kappa_k(G, B)$. We begin by the following easy lemma.

LEMMA 4.1. *Let G be a finite abelian group, and let B be a generating subset of G such that $0 \in B$. For all $k \geq 1$, $\kappa_k(B) \geq 1$.*

Proof. Suppose the contrary. There is $A \neq \emptyset$ such that $|G| > |A+B| = |A|$. Since $0 \in B$, we have $A = A + B$. It follows that

$$A + 2B = (A + B) + B = A + B = A.$$

Similarly for all $j \geq 1$, $A + jB = A$. It follows that $A + \bigcup_{j \geq 1} jB = A$. Since B generates the finite group G, we have $G = \bigcup_{j \geq 1} jB$. It follows that $A = G$, a contradiction. ∎

The next result describes the 1-atoms in finite abelian groups.

PROPOSITION 4.2 (see [8]). *Let G be a finite abelian group, and let B be a generating subset of G such that $0 \in B$. Let A be a 1-atom of $\Lambda(G, B)$ such that $0 \in A$. Then A is a subgroup.*

Proof. Since G is finite, it is enough to show that $x + A = A$ for every $x \in A$. Put $\Gamma = \Lambda(G, B)$. By Lemma 2.3, $x + A$ is 1-atom of Γ. By Lemma 2.3, $\alpha_1(\Gamma) = \alpha_1(\Gamma^-)$. Since $x \in A \cap (x + A)$, by Proposition 3.4 we have $x + A = A$. ∎

COROLLARY 4.3 (Mann Theorem [19]). *Let B be a generating subset of a finite abelian group G such that $0 \in B$. Let A be a subset of G such that $|A+B| \leq \min(|G|-1, |A|+|B|-2)$. Then there is a subgroup H of G such that $|H + B| \leq \min(|G| - 1, |H| + |B| - 2)$.*

Proof. Clearly B is 1-separable and $\kappa_1(B) \leq |B|-2$. Let H be a 1-atom of $\Lambda(G, B)$ containing 0. By Proposition 4.2, H is a subgroup. Now we have $|H + B| = |H| + \kappa_1(B) \leq |H| + |B| - 2$. By the definition of an atom, $|H + B| < |G|$. ∎

Corollary 4.4. *Let B be a generating subset of a finite abelian group G such that $0 \in B$. Then $\kappa_1(G,B) \geq |B|/2$. In particular for every non-empty subset A,*

$$|A+B| \geq \min(|G|, |A| + |B|/2). \tag{6}$$

Proof. Set $\Gamma = \Lambda(G,B)$. The result holds trivially if $G = B$. Assume $G \neq B$. Since $\{0\} + B \neq G$, Γ is 1-separable. Let H be a 1-atom of Γ containing 0. By Proposition 4.2, H is a subgroup. Since $H \neq G$, and B generates G, we have $|H+B| \geq 2|H|$. Hence $|H| \leq |H+B| - |H| = \kappa_1(\Gamma)$. It follows that

$$|B|/2 \leq |H+B|/2 = |H+B| - |H+B|/2 \leq |H+B| - |H| = \kappa_1(B).$$

Using (2), we obtain (6). ∎

A generalization of (6) to non-abelian groups and point-transitive relations is proved in [7]. The validity of (6) for not necessarily abelian groups was obtained independently by Olson [20].

5. Abstract critical pair theory. We need the following lemma partially contained in [10].

Lemma 5.1. *Let $\Gamma = (V,E)$ be a 2-separable reflexive relation on a finite set V such that $\alpha_2(\Gamma) \leq \alpha_2(\Gamma^-)$. Let M be a 2-atom of Γ. Let F be a 2-fragment of Γ such that $M \not\subset F$ and $M \cap F \neq \emptyset$. Then*

$$|M \cap F| = 1, \tag{7}$$

$$|M| - 1 \leq |F^* \setminus M^*|, \tag{8}$$

$$|\Gamma(M) \cap \Gamma(F)| \leq 1 + \kappa_2(\Gamma). \tag{9}$$

If $|F| < |M^*|$ and $\kappa_2(\Gamma) \leq d(\Gamma) - 1$ then $F \cup M$ is a 2-fragment of Γ.

Proof. (7) follows by Proposition 3.4. By Lemma 3.1, F^* and M^* are 2-fragments of Γ^-. Hence

$$|F^*| \geq \alpha_2(\Gamma^-) \geq \alpha_2(\Gamma) = |M|.$$

Let us prove (8). Assume first $|F^* \cap M^*| \leq 1$. We have clearly

$$|F^* \setminus M^*| \geq |F^*| - 1 \geq \alpha_2(\Gamma^-) - 1 \geq \alpha_2(\Gamma) - 1 = |M| - 1.$$

So we may assume $|F^* \cap M^*| \geq 2$. By (5) applied to Γ^-,

$$|F^* \setminus M^*| \geq |\Gamma^-(F^*) \setminus \Gamma^-(M^*)|.$$

By (4), $\Gamma^-(F^*) \setminus \Gamma^-(M^*) = (V \setminus F) \setminus (V \setminus M) = M \setminus F$. By (7), $|F^* \setminus M^*| \geq |M \setminus F| = |M| - 1$. This proves (8).

Now we have $\Gamma(F) \cap \Gamma(M) = \Gamma(M) \setminus (F^* \setminus M^*)$. Notice that $F^* \setminus M^* \subset \Gamma(M)$. Therefore

$$|\Gamma(F) \cap \Gamma(M)| = |\Gamma(M)| - |F^* \setminus M^*| \leq |\Gamma(M)| - |M| + 1 = \kappa_2(\Gamma) + 1.$$

Assume now $|F| < |M^*|$ and $\kappa_2(\Gamma) \le d(\Gamma)-1$. We have clearly $|F| < |M^*| = |V| - \kappa_2(\Gamma) - |M|$. Hence $|M| < |V| - \kappa_2(\Gamma) - |F| = |F^*|$. It follows from (8) that $|(F \cup M)^*| \ge |F^* \cap M^*| = |F^*| - |F^* \setminus M^*| \ge |M| + 1 - (|M| - 1) = 2$. Therefore

$$|(F \cup M)^*| \ge 2. \tag{10}$$

Choose $v \in F \cap M$. We have $\Gamma(v) \subset \Gamma(M) \cap \Gamma(F)$. Now we have clearly

$$\begin{aligned} |\Gamma(F \cup M)| &= |\Gamma(F)| + |\Gamma(M)| - |\Gamma(F) \cap \Gamma(M)| \\ &\le |F| + |M| + 2\kappa_2(\Gamma) - d(\Gamma). \end{aligned}$$

It follows that $|\Gamma(F \cup M)| \le |F \cup M| + \kappa_2(\Gamma)$. The definition of κ_2, (7) and (10) show that $F \cup M$ is 2-fragment. ∎

LEMMA 5.2. *Let $\Gamma = (V, E)$ be a reflexive relation on a finite set V. Suppose Γ is point-transitive and self-reverse. For all $v, w \in V$, there is an isomorphism ν from Γ onto Γ^- such that $\nu(v) = w$.*

Proof. Let ϕ be an isomorphism from Γ onto Γ^-. Put $\phi(v) = v'$ and choose an automorphism g of Γ such that $g(v') = w$. We may take $\nu = g \circ \phi$. ∎

PROPOSITION 5.3. *Let $\Gamma = (V, E)$ be a 2-separable reflexive relation on a finite set V. Suppose Γ is point-transitive and self-reverse. Let X_1, X_2, X_3 be three distinct 2-atoms of Γ, and let $v \in X_1 \cap X_2 \cap X_3$. Assume $|X_1| \ge 3$. Then there are $1 \le i < j \le 3$ such that*

$$|\Gamma(X_i) \cap \Gamma(X_j)| \ge \alpha_2(\Gamma) - 2 + d(\Gamma). \tag{11}$$

In particular

$$d(\Gamma) + \alpha_2(\Gamma) - 3 \le \kappa_2(\Gamma). \tag{12}$$

Proof. We first prove (11). We have $X_1^* \ne X_2^*$, since otherwise we would have $X_1 = X_2$, by (4). Since $|X_1^*| = |X_2^*|$, we may choose $w \in X_1^* \setminus X_2^*$. By Lemma 5.2, there is an isomorphism ν from Γ onto Γ^- such that $\nu(v) = w$. Put $K_i = \nu(X_i)$, $1 \le i \le 3$. Clearly K_1, K_2, K_3 are distinct 2-atoms of Γ^- containing w. By Proposition 3.4 applied to Γ^-, for all $1 \le s < t \le 3$,

$$K_s \cap K_t = \{w\}. \tag{13}$$

Suppose that for some $1 \le s < t \le 3$, $K_s \cup K_t \subset X_1^*$. By Lemma 3.1, X_2^* is a 2-fragment of Γ^-. Recall that $w \in (K_i \cap K_j) \setminus X_2^*$. By Proposition 3.4 applied to Γ^-, $|K_s \cap X_2^*| \le 1$ and $|K_t \cap X_2^*| \le 1$. It follows that $|(K_s \cup K_t) \cap (X_1^* \setminus X_2^*)| \ge |K_s \cup K_t| - 2 = 2|K_1| - 3 \ge |X_1|$, contradicting (8).

Hence at most one of the 2-atoms K_1, K_2, K_3 is contained in X_1^*. Then we may choose $1 \le i < j \le 3$ such that $K_i \not\subset X_1^*$, and $K_j \not\subset X_1^*$. Let us show that $X_1 \not\subset V \setminus \Gamma^-(K_i)$. Assume the contrary. By (4) applied to Γ^- we have $\Gamma(X_1) \subset \Gamma(V \setminus \Gamma^-(K_i)) = V \setminus K_i$. Now (4) yields $X_1^* = V \setminus (\Gamma(X_1)) \supset K_i$, a contradiction. Similarly $X_1 \not\subset V \setminus \Gamma^-(K_j)$. By Lemma 3.1, $V \setminus \Gamma^-(K_r)$

is a 2-fragment of Γ for all $1 \leq r \leq 3$. By Proposition 3.4 applied twice, $|X_1 \cap (V \setminus (\Gamma^-(K_i))) \cup (V \setminus (\Gamma^-(K_j)))| \leq 2$.

Set $W_0 = X_1 \cap \Gamma^-(K_i) \cap \Gamma^-(K_j)$. We have seen that $|W_0| \geq |X_1| - 2$. Since $\Gamma^-(w) \subset \Gamma^-(X_1^*)$, by (4) we have $W_0 \cap (\Gamma^-(w)) = \emptyset$. Clearly $W_0 \cup \Gamma^-(w) \subset \Gamma^-(K_i) \cap \Gamma^-(K_j)$. Therefore $|X_1| - 2 + d(\Gamma^-) \leq |\Gamma^-(K_i) \cap \Gamma^-(K_j)|$. Since Γ is self-reverse, we have $d(\Gamma^-) = d(\Gamma)$. It follows that

$$|X_1| - 2 + d(\Gamma) \leq |\nu^-(\Gamma^-(K_i) \cap \Gamma^-(K_j))| = |\Gamma(X_i) \cap \Gamma(X_j)|.$$

This proves (11). It follows by (9) that $d(\Gamma) + |X_1| - 2 \leq 1 + \kappa_2(\Gamma)$. This shows (12). ∎

6. The structure of 2-atoms. Let G be an abelian group, and let P_0 be a subset of G with cardinality ≤ 1. For any $d \in G$, we shall consider P_0 as an arithmetic progression with difference d. Let B be a subset of G. A subgroup H is called a *period* of B if $B + H = B$. A subset with a non-zero period is called *periodic*. A subgroup H is an *almost-period* of B if there is $b \in B$ such that H is a period of $B \setminus b$. A subset with a non-zero almost-period is called *almost-periodic*. Recall the following easy lemma.

LEMMA 6.1. *Let $B \subset G$ be such that $|\{0, d\} + B| = |B| + j$, and let K be the subgroup generated by d. There is a set T (possibly empty) and non-empty arithmetic progressions $P_1, \ldots, P_j$ with difference d such that B is a disjoint union of the sets $T + K, P_1, \ldots, P_j$.*

We are now ready to prove a structure theorem for the 2-atoms in a Cayley relation on a finite abelian group.

THEOREM 6.2. *Let B be a subset of a finite abelian group such that $0 \in B$. Put $\Gamma = \Lambda(G, B)$. Let A be a 2-atom of Γ such that $0 \in A$. If $|A| \geq \kappa_2(\Gamma) - |B| + 4$, then A is a subgroup.*

Proof. Assume first $|A| = 2$. It follows that $\kappa_2(B) \leq |B| - 2$. By Lemma 3.2, A is a 1-atom. By Proposition 4.2, A is a subgroup. So we may assume $|A| \geq 3$. Set $Q = \{x \mid x + A = A\}$. We show that $A = Q$. Assume the contrary. Choose $a \in A \setminus Q$. Since $A + Q = A$, we have $a + Q \subset A \cap (a + A)$. Since $a \notin Q$, we have $A + a \neq A$. By Proposition 3.4, $|Q| = 1$. Choose now two distinct elements $b, c \in A \setminus 0$. Since $|Q| = 1$, the 2-atoms $A, A - b, A - c$ are distinct. Since $0 \in A \cap (A - b) \cap (A - c)$, we have $|A| \leq \kappa_2(\Gamma) - |B| + 3$ by (12), contradicting the hypothesis. Therefore $A = Q$. But Q is clearly a subgroup. ∎

COROLLARY 6.3. *Let B be a subset of a finite abelian group such that $0 \in B$. Put $\Gamma = \Lambda(G, B)$. Let A be a 2-atom of Γ such that $0 \in A$. If $\kappa_2(\Gamma) = |B| - 1$, then either A is a subgroup or $|A| = 2$. If $\kappa_2(\Gamma) \leq |B| - 2$, then A is a subgroup.*

P r o o f. The first part is an immediate consequence of Theorem 6.2. The second one follows from Lemma 3.2 and Proposition 4.2. ∎

The following result will be applied to the Frobenius number.

THEOREM 6.4. *Let B be a generating subset of $\mathbb{Z}_m$ such that $0 \in B$, and $\kappa_2(B) = |B| - 1$. Also assume that B is not almost-periodic. Let H be a 2-atom of $\Lambda(G, B)$ such that $0 \in H$ and $|H| \geq 3$. If F is a 2-fragment then $F + H = F$. In particular for all $X \subset \mathbb{Z}_m$ such that $|X| \geq 2$ and $X + H \neq X$, $|X + B| \geq \min(m - 1, |X| + |B|)$.*

P r o o f. By Corollary 6.3, H is a subgroup. Let us prove that for all $x \in B$,

$$|(x + H) \cap B| \geq 2. \tag{14}$$

Assume the contrary and put $C = B \setminus x$. We have $|C| = |B| - 1 = \kappa_2(B) = |B + H| - |H| = |C + H|$. It follows that C is H-periodic, and hence B is almost-periodic, contradicting the assumption that B is not almost-periodic. Suppose $F + H \neq F$ and take a counterexample for which $|F|$ is maximal. There is $a \in F$ such that $a + H \not\subset F$. By replacing F by $F - a$, we may reduce to the case $a = 0$. So assume $a = 0$. By Proposition 3.4, $H \cap F = \{0\}$.

Assume first $|F^*| = |H|$. Choose $b \in F^*$. By Lemma 2.3, $F^* - b$ is a 2-atom of $\Lambda(G, -B)$. By Corollary 6.3, $F^* - b$ is a subgroup. Since $\mathbb{Z}_m$ has no distinct subgroups with the same order, we have $H = F^* - b$. By (4), $F = \mathbb{Z}_m \setminus (H + b - B)$. It follows that $F + H = F$, a contradiction.

Assume now $|F^*| > |H|$. By Lemma 5.1, $H \cup F$ is a 2-fragment. By the maximality of $|F|$, $(F \cup H) + H = F \cup H$. Hence $F' + H = F'$, where $F' = F \setminus 0$. We have $H \cap (F' + B) \neq \emptyset$, since otherwise $|H \cap B| \geq 2$ by (14). Hence

$$|F + B| = |F' + B| + |H \cap B| \geq |F' + B| + 2 \geq |F| + \kappa_2(B) + 1,$$

a contradiction. Since $(F' + B) + H = F' + B$, we have $H \subset F' + B$.

CASE 1: $B \subset F' + B$. It follows that $F + B = (F' + B) \cup B = F' + B$. Therefore $|F' + B| = |F + B| = |F'| + \kappa_2(B) + 1$. By a well known fact from elementary group theory, $|Y + H|$ is a multiple of $|H|$ for every Y. In particular $\kappa_2(B) = |H + B| - |H|$, $|F'|$ and $|F' + B|$ are multiples of $|H|$. It follows that 1 is a multiple of $|H|$, a contradiction.

CASE 2: $B \not\subset F' + B$. There is $x \in B$ such that $x \notin F' + B$. Since $(F' + B) + H = F' + B$, we have $(x + H) \cap (F' + B) = \emptyset$. By (14), we have $|F + B| \geq |F' + B| + |(x + H) \cap B| \geq |F' + B| + 2$. It follows from (2) that $|F + B| \geq |F'| + \kappa_2(B) + 2 = |F| + \kappa_2(B) + 1$, a contradiction. Hence $F + H = F$.

Assume now $X + H \neq X$ and $|X| \geq 2$. It follows that X is not a 2-fragment. By the definition of a 2-fragment, we have $|X + B| \geq \min(m - 1, |X| + |B|)$. ∎

We conclude this section by a description of 2-atoms which will be our main tool in the study of the Frobenius number. This description is implicit in [9].

Proposition 6.5. *Let B be a generating subset of a finite abelian group G such that $0 \in B$. Assume $\kappa_2(B) = |B| - 1$ and let H be a 2-atom containing 0. Then one of the following conditions holds*:

(i) $|H| > 2$, *and H is a subgroup.*
(ii) *B is an arithmetic progression.*
(iii) *B is almost-periodic.*
(iv) $|B| > |G|/2$, *and there is a proper subgroup K such that $|B| \geq |G| - |K| + 1$.*

Proof. Assume first $|H| > 2$. By Theorem 6.2, H is a subgroup. Hence (i) holds. Assume now $|H| = 2$ and put $H = \{0, d\}$. Let K be the subgroup generated by d. Now we have $|\{0, d\} + B| = 1 + |B|$. By Lemma 6.1, there is $T \subset G$ and an arithmetic progression $P \neq \emptyset$ with difference d such that $B = (T + K) \cup P$. If $T = \emptyset$, then (ii) holds. Assume $T \neq \emptyset$. If $B + K = G$, then (iv) holds. Assume now $B + K \neq G$. Since $d \neq 0$, we have $|K| \geq 2$. Also $G \setminus (B + K)$ is a union of K-cosets. Therefore

$$|T + K| + |P| - 1 = \kappa_2(B) \leq |B + K| - |K| \leq |T + K|.$$

It follows that $|P| = 1$. Hence (iii) holds. ∎

Theorem 6.6. *Let B be a generating subset of a finite abelian group G such that $0 \in B$ and $|B| \leq |G|/2$. Then one of the following conditions holds*:

(i) *For all $|A| \geq 2$, $|A + B| \geq \min(|G| - 1, |A| + |B|)$.*
(ii) *B is an arithmetic progression.*
(iii) *There is a subgroup H such that $|H + B| < \min(|G| - 1, |H| + |B| - 1)$.*

Proof. Suppose (i) not satisfied. It follows that B is 2-separable, and that $\kappa_2(B) \leq |B| - 1$. Let H be a 2-atom of $\Lambda(G, B)$ such that $0 \in H$.

Case 1: $\kappa_2(B) \leq |B| - 2$ *or* $|H| \geq 3$. By Corollary 6.3, H is a subgroup. By the definition we have

$$|H + B| < |G| \quad \text{and} \quad |B| - 1 \geq \kappa_2(B) = |H + B| - |H|.$$

This proves (iii).

Case 2: $\kappa_2(B) = |B| - 1$ *and* $|H| = 2$. By Proposition 6.5, either (ii) is satisfied or B is almost-periodic. Let K be an almost-period of B. We have

$|K+B| = |K|+|B|-1$. We have $K+B \neq G$, since $|B| \leq |G|/2$. This proves (iii), where K replaces H. ∎

7. Higher critical pair theory

THEOREM 7.1. *Let B be a subset of a finite abelian group such that $0 \in B$, and $|B| \leq |G|-7$. Put $\Gamma = \Lambda(G,B)$. Let H be a 2-atom of Γ such that $0 \in H$. If $\kappa_2(B) = |B|$, then either H is a subgroup or $|H| = 2$.*

Proof. Assume the contrary. By Theorem 6.2, $|H| = 3$. Let us show that $|H+H| \geq 6$. First observe that $H + x \neq H$ for all $x \neq 0$. Assume the contrary and let K be the subgroup generated by x. Since H is not a subgroup it follows that H is the union of at least two distinct K-cosets. Therefore $|H| \geq 2|K| \geq 4$, a contradiction. Put $H = \{a_0, a_1, a_2\}$, where $a_0 = 0$. By Proposition 3.4, $|(H+a_i) \cap (H+a_j)| \leq 1$ for all $i \neq j$. It follows that $|H+H| = |(H+a_0) \cup (H+a_1) \cup (H+a_2)| \geq 3|H| - 3 = 6$.

We now show that there is a 2-atom A containing 0 and $u \in A \setminus 0$ such that

$$|A+A| \geq 6 \quad \text{and} \quad |(A+u+B) \cap (A+B)| \geq |B|+1. \tag{15}$$

Put $X_i = H - a_i$, $0 \leq i \leq 2$. Since H is not a subgroup, X_0, X_1, X_2 are distinct 2-atoms containing 0. By (11), there is $i < j$ such that $|(X_i + B) \cap (X_j + B)| \geq |B|+1$. Clearly (15) holds if $i = 0$. So we may assume without loss of generality $i = 1$ and $j = 2$. In this case we put $A = H - a_1 + a_2$ and $u = a_2 - a_1$. Put $A = \{0, u, v\}$. Let us first show that $A+B = \{0,u\}+B$. Since $\{0,u\}$ is not a 2-fragment, we have $|A+B| \geq |\{0,u\}+B| \geq 3+|B| = |A+B|$. It follows that $A + B = \{0,u\} + B$. By (15), we have

$$\begin{aligned} |A+B+\{0,u\}| &= |A+B| + |A+B+u| - |(A+B) \cap (A+B+u)| \\ &\leq 2|A| + 2|B| - (|B|+1) = |B|+5. \end{aligned}$$

Hence

$$|A+A+B| = |A+B+\{0,u\}| \leq |B|+5 < |A+A| + \kappa_2(B).$$

By the definition of κ_2, we have $|A+A+B| \geq |G|-1$. It follows that $|B| \geq |G|-6$, a contradiction. ∎

8. The Frobenius problem. Let $A \subset \mathbb{N}^*$ be such that $\max(A) = m$. We write

$$\Phi(A) = \bigcup_{0 \leq j} jA, \qquad \Phi_k(A) = \Phi(A) \cap [(k-1)m+1, km].$$

Assume $\gcd(A) = 1$. The *Frobenius number* of A is by definition

$$G(A) = \max(\mathbb{Z} \setminus \Phi(A)).$$

We write $G(a_1,\dots,a_n)$ instead of $G(\{a_1,\dots,a_n\})$, and Φ (resp. Φ_k) for $\Phi(A)$ (resp. $\Phi_k(A)$) when the context is clear.

Let $m,d\in\mathbb{N}^*$ be such that $\gcd(m,d)=1$. Sylvester [22] proved that

$$G(m,m-d)=(m-1)(m-d-1)-1. \tag{16}$$

Roberts [21] showed that

$$G(m,m-d,\dots,m-(n-1)d)=(m-(n-1)d)\left[\frac{m-2}{n-1}\right]-d. \tag{17}$$

We have clearly

$$\Phi_k(A)+A\subset\Phi_{k+1}(A)\cup(\Phi_{k+1}(A)-m).$$

Reducing modulo m, we get

$$\overline{\Phi_k(A)}+\overline{A}\subset\overline{\Phi_{k+1}(A)}. \tag{18}$$

By iterating we obtain

$$k\overline{A}\subset\overline{\Phi_k(A)}. \tag{19}$$

Notice that (18) and (19) are used by J. Dixmier in [4]. We need the following well known lemma used by J. Dixmier [4].

Lemma 8.1 (folklore). *Let $A\subset\mathbb{N}^*$ be such that $|A|>\max(A)/2$. Then*

$$G(A)\le 2\max(A)-2|A|-1. \tag{20}$$

9. H-decompositions. A subset A of $\mathbb{N}$ will be called *saturated* if for all $x,y\in A$, either $x+y\in A$ or $x+y>\max(A)$. Let $\mathcal{F}$ be the set of all the saturated subsets A of $\mathbb{N}^*$ such that $A\cup\{0\}$ is the union of two arithmetic progressions with the same difference.

Let $A\subset\mathbb{N}^*$. Put $\max(A)=m$ and $n=|A|$. Let ν be the canonical morphism from $\mathbb{Z}$ onto $\mathbb{Z}_m$. We write $\overline{x}=\nu(x)$. Let H be a proper subgroup of $\mathbb{Z}_m$. Put $m=q|H|$. Then $H=\overline{\{q,2q,\dots,m\}}$. We may partition A into its traces on the cosets of $q\mathbb{Z}$. A partition $A=A_0\cup A_1\cup\ldots\cup A_u$ will be called an *H-decomposition* of A if the following conditions hold:

(i) $m\in A_0$.
(ii) For every i, $A_i-A_i\subset q\mathbb{Z}$.
(iii) For every $i\ne j$, $A_i-A_j\not\subset q\mathbb{Z}$.

Lemma 9.1. *Let $A\subset\mathbb{N}^*$ be such that $\gcd(A)=1$ and $\max(A)=m$. Let H be a proper subgroup of $\mathbb{Z}_m$ such that $|\overline{A}+H|\le|H|+|\overline{A}|-1$. Put $(u+1)|H|=|\overline{A}+H|$. Also assume that $2|A|\le m$. Then*

$$m\ge(2u+1)|H|. \tag{21}$$

In particular $|H|\le m/3$.

Proof. We have $2((u+1)|H|-|H|+1)\le 2|A|\le m$. Now (21) follows since $|H|\ge 2$ and $|H|$ divides m. Since $\gcd(A)=1$, the set $\overline{A}$ generates $\mathbb{Z}_m$.

Therefore $\overline{A} \not\subset H$, since H is a proper subgroup. It follows that $u \geq 1$. In particular $|H| \leq m/3$. ∎

LEMMA 9.2 (see [12]). *Let $A \subset \mathbb{N}^*$ be a saturated subset such that $\max(A) = m$. Let H be a proper subgroup of $\mathbb{Z}_m$. Let $A = A_0 \cup A_1 \cup \ldots \cup A_u$ denote an H-decomposition of A. Let $0 \leq s, t \leq u$. Assume $(A_s + A_t) \cap A = \emptyset$. Then*

$$|A_s| + |A_t| \leq |H| + 1. \tag{22}$$

Proof. For $i \geq 1$, set $m_i = \min(A_i)$. We have $|A_i| \leq (m - m_i)/q + 1$. It follows that

$$|A_s| + |A_t| \leq 2 + (2m - (m_s + m_t))/q.$$

Since $m_s + m_t \notin A$, we have $m_s + m_t > m$. Therefore

$$|A_s| + |A_t| < 2 + m/q = 2 + |H|.$$

Hence $|A_s| + |A_t| \leq |H| + 1$. ∎

LEMMA 9.3. *Let $A \subset \mathbb{N}^*$ be a saturated subset such that $\gcd(A) = 1$, $|A| = n$, and $\max(A) = m$. Also assume that $|A| \leq m/2$. Let H be a proper subgroup of $\mathbb{Z}_m$ such that $|\overline{A} + H| \leq |H| + |\overline{A}| - 2$. For $i \in \{0, 1\}$, put $m - 1 + i = k_i(n + i - 1) - r_i$, where $1 \leq r_i \leq n + i - 1$. Then*

$$G(A) \leq (k_0 - 1)(m - r_0 - 1) - 1. \tag{23}$$

Moreover,

$$\text{if} \quad A \notin \mathcal{F} \quad \text{then} \quad G(A) \leq (k_1 - 1)(m - r_1) - 1. \tag{24}$$

Proof. Let $A = A_0 \cup A_1 \cup \ldots \cup A_u$ denote an H-decomposition of A. Put $n_0 = |A_0|$ and $m = q|H|$. Let us first prove that $u = 1$. We may assume without loss of generality that $|A_1| \geq \ldots \geq |A_u|$. We shall prove that

$$(\overline{A \setminus A_u} + H) + \overline{A} + H \subset \overline{A} + H. \tag{25}$$

Assume the contrary. There are $0 \leq s \leq u - 1$ and $0 \leq t \leq u$ such that

$$(\overline{A}_s + \overline{A}_t + H) \cap (\overline{A} + H) = \emptyset.$$

We have necessarily $s \geq 1$, since $\overline{A}_0 + \overline{A} \subset \overline{A} + H$. Clearly

$$|H| - 2 \geq |\overline{A} + H| - |\overline{A}| \geq 2|H| - (|\overline{A}_s| + |\overline{A}_u|).$$

Therefore

$$|H| + 2 \leq |\overline{A}_s| + |\overline{A}_u| \leq |\overline{A}_s| + |\overline{A}_t|.$$

It follows using (22) that

$$|H| + 2 \leq |\overline{A}_s| + |\overline{A}_t| = |A_s| + |A_t| \leq |H| + 1,$$

a contradiction. This proves (25).

By (6) and (21),

$$|(\overline{A \setminus A_u} + H) + \overline{A} + H| \geq \min(m, u|H| + (u + 1)|H|/2) = (3u + 1)|H|/2.$$

It follows that $(u+1)|H| \geq (3u+1)|H|/2$. Therefore $u = 1$. Let us prove that

$$G(A) \leq (q-1)(m-2-(n-n_0-1)q)-1. \tag{26}$$

Put $a_1 = \min(A_1)$. Clearly $H = \overline{\{q, 2q, \ldots, m\}}$. Take $x > (q-1)a_1 - q$. We claim that there are $j \in \{0, \ldots, q-1\}$ and $s \in \mathbb{Z}$ such that

$$x = ja_1 + sq.$$

Clearly $A_0 \subset \{q, 2q, \ldots, m\}$ and $A_1 \subset a_1 + \{q, 2q, \ldots, m-q\}$. Since $u = 1$ and $\gcd(A) = 1$, $\overline{a}_1$ generates $\mathbb{Z}_m/H$. Therefore there is $0 \leq j \leq q-1$ such that $x - ja_0 \in q\mathbb{Z}$. This proves the claim.

We now show that $s \geq 0$. We have

$$(q-1)a_1 + sq \geq ja_1 + sq = x > (q-1)a_1 - q.$$

Therefore $sq > -q$, and hence $s \geq 0$. Clearly $a_1 \leq m - 1 - (n-n_0-1)q$. It follows that

$$\begin{aligned} G(A) &\leq (q-1)a_1 - q \leq (q-1)(m-1-(n-n_0-1)q) - q \\ &= (q-1)(m-2-(n-n_0-1)q) - 1. \end{aligned}$$

This proves (26).

Clearly $2|H| = |\overline{A} + H| \leq |H| + n - 2$. Therefore

$$(k_i - 1)(n+i-1) - i + 1 \leq m = q|H| < q(n-1).$$

It follows that for $0 \leq i \leq 1$,

$$k_i \leq q. \tag{27}$$

Put $E_i = (k_i - 1)(m - r_i + i - 1) - 1 - G(A)$. The maximal possible value of n_0 is m/q. It follows from (26) that

$$G(A) \leq (q-1)(2m-2-(n-1)q) - 1.$$

We have $E_0 \geq F_0(q)$, where

$$F_0(q) = (k_0 - 1)(m - r_0 - 1) - (q-1)(2m-2-(n-1)q).$$

By (27), we have $k_0 \leq q$. Assume first $q = k_0$. Then $E_0 \geq F_0(k_0) = 0$. Thus (23) holds in this case. Assume now $q \geq k_0 + 1$. It follows that $F_0(q)$ is increasing. Therefore $E_0 \geq F_0(q) \geq F_0(k_0+1)$. It follows that $E_0 \geq (k_0-1)(m-r_0-1) - k_0(2m-2-(n-1)(k_0+1)) = 2r_0 > 0$. This proves (23).

Let us prove (24). Assume that $A \notin \mathcal{F}$. Let us show that $n_0 \leq m/q - 1$. Assume the contrary. Then $q \in A$. Since A is saturated, it follows that $\{q, 2q, \ldots, m\} \subset A$. Therefore we have $A_0 = \{q, 2q, \ldots, m\}$. Similarly $A_1 = (a_1 + [0, q, \ldots, m-q]) \cap [1, m]$. Therefore $A \in \mathcal{F}$, a contradiction. Thus $n_0 \leq m/q - 1$. By (26),

$$G(A) \leq (q-1)(m-2-(n-n_0-1)q) - 1 \leq (q-1)(2m-2-nq) - 1.$$

It follows that $E_1 \geq F_1(q)$, where

$$F_1(q) = (k_1 - 1)(m - r_1) - (q - 1)(2m - 2 - nq).$$

By (27), we have $k_1 \leq q$. Assume first $q = k_1$. Then $E_1 \geq F_1(k_1) \geq 2(k_1 - 1) \geq 0$. Thus (24) holds in this case. Assume now $q \geq k_1 + 1$. It follows that $F_1(q)$ is increasing. Therefore $E_1 \geq F_1(q) \geq F_1(k_1 + 1)$. Hence

$$\begin{aligned} E_1 &\geq (k_1 - 1)(m - r_1) - k_1(2m - 2 - n(k_1 + 1)) \\ &= k_1(n + 2) - m + r_1 = 2r_1 + 2k_1 > 0. \end{aligned}$$

This proves (24). ∎

10. A theorem of J. Dixmier

THEOREM 10.1 (J. Dixmier [4]). *Let $A \subset \mathbb{N}^*$ be a finite subset such that* $\gcd(A) = 1$. *Set $m = \max(A)$ and $n = |A|$. Put $m - 1 = k(n-1) - r$, where $1 \leq r \leq n - 1$. Then $G(A) \leq (k - 1)(m - r - 1) - 1$.*

Proof. As observed by J. Dixmier [4], we may assume A to be saturated, without loss of generality. This follows since A is contained in some saturated set X such that $G(X) = G(A)$.

CASE 1: *For all $j \leq k-1$, $|j\overline{A}| \geq \min(m, 1 + j(n-1))$.* By the definition of k, one has $1 + j(n-1) = \min(m, 1 + j(n-1))$. Hence

$$\begin{aligned} |\Phi \cap [1, (k-1)m]| &= \sum_{1 \leq j \leq k-1} |\Phi_j| \geq \sum_{1 \leq j \leq k-1} (1 + j(n-1)) \\ &= (k-1)(2 + k(n-1))/2 = (k-1)(m + r + 1)/2. \end{aligned}$$

Recall that $A \subset \Phi \cap [1, (k-1)m] \subset \Phi(A)$. It follows that $G(A) = G(\Phi \cap [1, (k-1)m])$. By (20), $G(A) = G(\Phi \cap [1, (k-1)m]) \leq (k-1)(m-r-1) - 1$, and the result holds in this case.

CASE 2: *There exists $j \leq k - 1$ such that $|j\overline{A}| < \min(m, 1 + j(n-1))$.* We have $j \geq 2$. By Lemma 2.1, $2n \leq m$. Take a maximal $i \leq j - 1$ such that $|i\overline{A}| \geq 1 + i(n-1)$. Put $B = i\overline{A}$. We have $|B + \overline{A}| < \min(m, |B| + |\overline{A}| - 1)$. By Mann's Theorem (Corollary 4.3), there is a proper subgroup H such that $|H + \overline{A}| \leq |H| + |\overline{A}| - 2$. By (23), $G(A) \leq (k-1)(m-r-1) - 1$. ∎

11. Exceptional families

LEMMA 11.1. *Assume* $\gcd(m, d) = 1$. *Let $x, y \in \mathbb{Z}_m$. There is at most one arithmetic progression P with difference $\overline{d}$ and extremities x, y such that $|P| \leq m/2$.*

Proof. Let P be such an arithmetic progression. The other arithmetic progression with difference $\overline{d}$ and extremities x and y is $Q = (\mathbb{Z}_m \setminus P) \cup \{x, y\}$. It follows that $|Q| \geq m - |P| + 2 > m/2$. ∎

Let $q \in \mathbb{N}^*$ and let $x \in \mathbb{Z}$. We denote by $\eta_q(x)$ the unique integer y such that $y \equiv x \bmod q$ and $1 \leq y \leq q$.

LEMMA 11.2. *Put $m = m'd - r$, where $1 \leq r \leq d-1$ and $3 \leq d \leq m/2$. Let $1 \leq u \leq d$. Let $X \subset [1,m]$ be such that $|X| \leq m/2$ and $\overline{X}$ is an arithmetic progression with difference $\overline{d}$.*

(i) *If $u, u+r \in X$, then $\eta_d(u+r) \in X$.*
(ii) *If $u, u+d-r \in X$, then $\eta_d(u+d-r) \in X$.*

Proof. Let us prove (i). Assume $u, u+r \in X$. It follows that $2 \leq |X| \leq m/2$. Therefore $m \geq 4$. Set

$$P = \{u, u+d, \ldots, \eta_m(u+m'd-d), \eta_m(u+m'd)\}.$$

Since $u + m'd \equiv u + m + r \equiv u + r \bmod m$, we have $\eta_m(u+m'd) = u+r$. Clearly $\overline{P}$ is an arithmetic progression with difference $\overline{d}$ containing u and $u+r$. Obviously $|P| \leq 1 + m' \leq 1 + (m+d-1)/d \leq (m+5)/3 \leq m/2$. Since $\overline{X}$ is an arithmetic progression with difference $\overline{d}$ and since $|X| \leq m/2$, Lemma 11.1 shows that $P \subset X$. If $u + r \leq d$, then $u + r = \eta_d(u+r) \in P$. Suppose $u + r > d$. Since $u, r \leq d$, we have $1 \leq u + r - d \leq d$. But $u + (m'-1)d \equiv u + r - d \bmod m$. Then $u + r - d = \eta_d(u+r) \in P$. In particular $\eta_d(u+r) \in X$. This proves (i). The proof of (ii) is similar. ∎

LEMMA 11.3. *Let $A \subset \mathbb{N}^*$ be a saturated subset such that $\gcd(A) = 1$, and $|A| \leq \max(A)/2$. If $\overline{A}$ is an arithmetic progression, then $A \in \mathcal{F}$.*

Proof. Notice that for every saturated subset X containing 1, we have $X = [1, \max(X)]$. Therefore $1 \notin A$. Put $m = \max(A)$. Choose $d \in \mathbb{N}^*$ such that $d \leq m/2$, and $\overline{d}$ is the difference of the progression. Observe that such a d exists, since we may reverse the progression. On the other hand $\gcd(m,d) = 1$, since $\overline{d}$ generates $\mathbb{Z}_m$. Hence there is $1 \leq r \leq d-1$ such that $m = m'd - r$. It follows that r generates the integers mod d. Put

$$\overline{A} = \{-v\overline{d}, \ldots, -\overline{d}, 0, \overline{d}, \ldots, w\overline{d}\}.$$

Let us prove that

$$w \leq m' - 1.$$

Suppose the contrary. Then $\eta_m(m'd) = \eta_m(m+r) = r$. Hence $r \in A$. It follows that $2 \leq r \leq d-1$ and hence $d \geq 3$. We prove by induction that $\eta_d(jr) \in A$ for $1 \leq j \leq d-1$. The result holds for $j = 1$. Assume it holds for j. Clearly $\eta_d(jr) + r \leq d + r \leq 2d \leq m$. Since A is saturated, we have $\eta_d(jr) + r \in A$. It follows from Lemma 11.2 that $\eta_d((j+1)r) \in A$. Since r generates the integers modulo d, there is $j \leq d-1$ such that $\eta_d(jr) = 1$. Hence $1 \in A$, a contradiction.

Let us prove that

$$v \leq m' - 2.$$

Assume the contrary. Then $d-r = m-(m'-1)d \in A$. It follows that $2 \le d-r \le d-1$ and hence $d \ge 3$. We prove by induction that $\eta_d(j(d-r)) \in A$ for all $1 \le j \le d-1$. The result holds for $j=1$. Assume it holds for j. Clearly $\eta_d(j(d-r))+d-r \le 2d-r < 2d \le m$. Since A is saturated, we have $\eta_d(j(d-r))+d-r \in A$. It follows from Lemma 11.2 that $\eta_d((j+1)(d-r)) \in A$. Since $d-r$ generates the integers modulo d, there is $j \le d-1$ such that $\eta_d(j(d-r)) = 1$. Hence $1 \in A$, a contradiction.

Now $A = \{m, m-d, \dots, m-vd\} \cup \{d, \dots, wd\}$. Hence $A \in \mathcal{F}$. ∎

Let $\mathcal{K}$ be the set of all subsets A of $\mathbb{N}$ such that $A = \{m/2, m, x, x+m/2, 2x\}$, where m is even and $x < m/2$.

LEMMA 11.4. *Let A be a saturated subset such that* $\gcd(A) = 1$ *and* $|A| \le \max(A)/2$. *Assume that $\overline{A}$ is almost-periodic. Then $A \in \mathcal{K} \cup \mathcal{F}$.*

Proof. Let H be an almost-period of $\overline{A}$. Put $m = \max(A)$ and $m = q|H|$. Let $A_0, \dots, A_u$ be an H-decomposition of A. Without loss of generality, we may assume $|A_1| \ge \dots \ge |A_u|$.

Let us show that $|A_u| = 1$. Assuming the contrary, we have $|A_0| = 1$. By (21) we have $|\overline{A}+H| < m$. Since $\overline{A}$ generates $\mathbb{Z}_m$, $\overline{A}+H$ is not a subgroup. Hence

$$\overline{A}_i + \overline{A}_j + H \not\subset \overline{A} + H$$

for some $i, j \in \{0, 1, \dots, u\}$. Necessarily $1 \le i, j$, since $\overline{A_0 + A} \subset \overline{A} + H$. By (22), $2|H| = |A_i| + |A_j| \le |H| + 1$, a contradiction. Hence $|A_u| = 1$. We have

$$\overline{A}_i + \overline{A}_j + H \subset \overline{A} + H$$

for all $0 \le i, j \le u-1$, since otherwise by (22), $2|H| = |A_i| + |A_j| \le |H| + 1$, a contradiction. Put $T = A \setminus A_u$. Therefore

$$\overline{T+T} \subset \overline{A} + H.$$

Assume first that $\overline{T}$ is a subgroup. Since $|T| = n-1$, we have $T = \{m/(n-1), 2m/(n-1), \dots, m\}$. Since $|A_u| = 1$, we have $A \in \mathcal{F}$.

Assume now that $\overline{T}$ is not a subgroup. It follows that

$$\overline{T+T} = \overline{A} + H.$$

In particular $\overline{T}$ generates $\mathbb{Z}_m$. By (6) and (21),

$$|\overline{T} + \overline{T}| \ge \min(m, 3u|H|/2) = 3u|H|/2.$$

Therefore, $3u|H|/2 \le |\overline{T} + \overline{T}| = (u+1)|H|$. Hence $u \le 2$. Clearly $A \in \mathcal{F}$, if $u = 1$. We may assume $u = 2$. Since $\overline{T+T} = \overline{A} + H$, we have $\overline{A}_2 + H = \overline{A}_i + \overline{A}_j + H$ for some $0 \le i, j \le 1$. Necessarily $i = j = 1$. There is clearly $r < m/|H|$ such that $A_1 = \{r, r+q, \dots, r+m-q\}$. Clearly $A_0 = \{q, 2q, \dots, m\}$. Since A is saturated, necessarily $A_2 = \{2r\}$. Since A is saturated and $3r \notin A$, we have $3m/q > 3r > m$. Therefore $|H| = m/q < 3$. It follows that $|H| = 2$

and m is even. Clearly $A = \{m, m/2\} \cup \{r, m/2+r\} \cup \{2r\}$ for some $r < m/2$. Therefore $A \in \mathcal{K}$. ∎

LEMMA 11.5. *Let A be a saturated subset of $\mathbb{N}^*$ such that $\gcd(A) = 1$. Put $m = \max(A)$. Let H be a proper subgroup of $\mathbb{Z}_m$. Suppose that $\overline{A}$ is not almost-periodic and $|\overline{A} + H| \leq |H| + |\overline{A}| - 1$. Assume that $\overline{\Phi}_k \neq \mathbb{Z}_m$. Then $\overline{\Phi}_k + H \neq \overline{\Phi}_k$.*

Proof. Let $A_0, A_1, \ldots, A_u$ be an H-decomposition of A. Suppose on the contrary that $\overline{\Phi}_k$ is H-periodic. Since $\overline{A}$ generates $\mathbb{Z}_m$, $\overline{\Phi}_k + \overline{A} \neq \overline{\Phi}_k$. There are $x \in A$ and $z \in \Phi_k$ such that $\overline{x+z} \notin \overline{\Phi}_k$. Choose $0 \leq i \leq u$ such that $x \in A_i$. We have necessarily, $1 \leq i \leq u$, since $\overline{A}_0 \subset H$. Since $\overline{A}$ is not almost-periodic, we have $|A_i| \geq 2$. Therefore there is y such that $y \leq m-1-q$, and $y \in A_i$. Since $\overline{\Phi}_k$ is H-periodic, there is $w \in \Phi_k$ such that $w \leq (k-1)m + q$ and $\overline{z-w} \in H$. Clearly $w + y \leq (k-1)m + q + m - q - 1 = km - 1$. It follows that $w + y \in \Phi_k$. Therefore $\overline{w+y} \in \overline{\Phi}_k$. Thus $\overline{w+y} + H \subset \overline{\Phi}_k$. We obtain a contradiction, since $\overline{w+x} + H = \overline{y+z} + H$. ∎

As an exercise, the reader could prove in few lines that under the hypothesis of Lemma 11.5, $\overline{A}$ cannot be H-periodic.

12. An upper bound for the Frobenius number

THEOREM 12.1 (see [12]). *Let $A \subset \mathbb{N}^*$ be a finite subset such that $\gcd(A) = 1$. Suppose $A \notin \mathcal{F} \cup \mathcal{K}$. Put $n = |A|$ and $m = \max(A)$. Set $m = kn - r$, where $1 \leq r \leq n$. Then*

$$G(A) \leq (k-1)(m-r) - 1. \tag{28}$$

Proof. (28) reduces to (20) if $m < 2n$. Suppose $m \geq 2n$. Assume first that A is not saturated. Then there are $a, b \in A$ such that $a + b < m$ and $a + b \notin A$. Put $A' = A \cup \{a+b\}$. Clearly $G(A') = G(A)$. By Dixmier's Theorem 10.1, $G(A) = G(A') \leq (k-1)(m-r-1) - 1$, if $r \leq n-1$. So we may assume $r = n$. By Theorem 10.1,

$$G(A) = G(A') \leq (k-2)(m-2) - 1 = (k-1)(m-r) - 1 - 2k + 4.$$

But $2n \leq m = kn - n$. Therefore $k \geq 3$. Hence $G(A) \leq (k-1)(m-r) - 1 - 2k + 4$. So assume A is saturated. Let ν be the canonical morphism from $\mathbb{Z}$ onto $\mathbb{Z}_m$. We write $\overline{Y} = \nu(Y)$ for every $Y \subset \mathbb{Z}$.

CASE 1: $\kappa_2(\overline{A}) \geq n - 1$. We now prove that for all $j \leq k-1$,

$$|\Phi_j| \geq jn. \tag{29}$$

Assume first $\kappa_2(A) \geq n$. By (2), $|j\overline{A}| \geq \min(m-1, |(j-1)\overline{A}| + n)$. By iterating, we get $|j\overline{A}| \geq \min(m-1, jn) = jn$. By (19), we have (29). So we may assume $\kappa_2(\overline{A}) = n - 1$. Let H be a 2-atom containing 0. By Lemma 11.4, $\overline{A}$ is not almost-periodic. By Lemma 11.3, $\overline{A}$ is not an arithmetic

progression. By Proposition 6.5, H is a proper subgroup. By Lemma 11.5, $\overline{\Phi}_{j-1}+H \neq \overline{\Phi}_{j-1}$. By Theorem 6.4, $|\overline{\Phi}_{j-1}+\overline{A}| \geq \min(m-1, |\overline{\Phi}_{j-1}|+n)$. By (18), $|\overline{\Phi}_j| \geq \min(m-1, |\overline{\Phi}_{j-1}|+n)$. By induction, we obtain (29). Therefore

$$|\Phi \cap [1,(k-1)m]| \geq \sum_{1\leq j\leq k-1} jn = k(k-1)n/2 = (k-1)(m+r)/2.$$

By (20),

$$G(A) = G(\Phi\cap[1,(k-1)m]) \leq 2(k-1)m-(k-1)(m+r)-1 = (k-1)(m-r)-1.$$

Case 2: $\kappa_2(\overline{A}) \leq n-2$. Let H be a 2-atom containing 0. By Theorem 6.2, H is a proper subgroup. We have $n-2 \geq \kappa_2(\overline{A}) = |H+\overline{A}| - |H|$. The result now follows from (24). ∎

Theorem 12.1 is used in [12] to get some best possible bounds for $G(A)$ and even the uniqueness of the examples where the bound is attained.

Corollary 12.2. *Let* $A \subset \mathbb{N}^*$ *have* $\max(A) = m$ *and* $|A| = n$. *Suppose* $m \geq n(n-1)$. *If* $A \notin (\mathcal{F} \cup \mathcal{K})$, *then* $G(A) < G(m, m-1, \ldots, m-n+1)$.

Proof. Put $m-2 = s(n-1)+r$, where $0 \leq r \leq n-2$. We have $s \geq r+2$, since otherwise $m \leq (r+1)(n-1)+r \leq n(n-1)-1$, a contradiction. Put $s-r-2 = jn-t$, where $1 \leq t \leq n$. Notice that $j \geq 1$. We also have $s \geq 2+n(j-1) \geq j+1$. We have $m = (s-j)n-t$.

Set $D = G(m, m-1, \ldots, m-n+1) - G(A)$. By (28) and (17), we have

$$\begin{aligned} D &\geq s(m-n+1) - (s-j-1)(m-t) \\ &\geq jm + t(s-j-1) + m - s(n-1) > 0. \end{aligned}$$ ∎

The Frobenius number for sets that are unions of two arithmetic progressions with the same difference was investigated by A. Janz [13]. She showed that for $m \geq (9n^3-30n^2+4n-22)/4$ non-congruent to 0 or 1 mod $(n-1)$, $G(A) \leq G(m, m-1, \ldots, m-n+1)$ for all $A \in \mathcal{F}$. As shown in [12], $G(A)$ may be evaluated using (16). One may use this idea to get an easy proof of a sharper result.

Lemma 12.3. *Let* $A \in \mathcal{F}$ *be such that* $\gcd(A) = 1$. *Assume* $\max(A) = m$ *and* $|A| = n \geq 2$. *Put* $m = k(n-1)+r$, *where* $0 \leq r \leq n-2$. *Suppose* $m \geq n^3-1$. *Then for* $2 \leq r \leq n-2$, *and* $A \neq \{m, m-1, \ldots, m-n+1\}$, $G(A) < k(m-n+1)-1$.

Proof. Set $E = k(m-n+1)-1-G(A)$. Suppose on the contrary that $E \leq 0$. Set $A \cup \{0\} = \{0, d, 2d, \ldots, (n-j)d\} \cup \{m-u, m-u-d, \ldots, m-u-(j-1)d\}$. We have $n-j \neq 0$, since otherwise A would be an arithmetic progression with difference $d > 1$, and hence $E > 0$, by (17). By (16),

$$G(A) \leq (d-1)(m-u-(j-1)d-1)-1 \leq (d-1)(m-1-(j-1)d)-1.$$

Set $k(j-1)+r = s(n-j)+t$, $0 \leq t \leq n-j-1$. Clearly $m = (k+s)(n-j)+t$.

Since A is saturated, we must have $(n-j+1)d > m$. It follows that $d = [m/(n-j)] = k+s$. We have

$$\begin{aligned} G(A) &\le (k+s-1)(m-1-(j-1)(k+s))-1 \\ &= (k+s-1)(m-1-s(n-j)-t+r-(j-1)s)-1 \\ &= (k+s-1)(m-1-(n-1)s+r-t)-1 \\ &\le (k+s-1)(m-1-(n-1)s+r)-1. \end{aligned}$$

Notice that $s \ge 0$ by the definition. Also we have $k \ge 2$, since otherwise $n^3-1 \le m \le 2n-3$, a contradiction. It follows that

$$\begin{aligned} E &\ge k(k(n-1)-n+1+r)-(k+s-1)(k(n-1)+r-1-(n-1)s+r) \\ &\ge k(k(n-1)-1)-(k+s-1)(k(n-1)+2n-5-(n-1)s) \\ &= (n-1)s^2-(3n-6)s+2k-k(n-1)+2n-5 \\ &> (n-1)(s-3/2)^2-k(n-1). \end{aligned}$$

Therefore $s < 3/2+\sqrt{k}$. On the other hand, we have

$$k(j-1) < s(n-j)+t \le (s+1)(n-j)-1.$$

Therefore $s+1 > k(j-1)/(n-j) \ge k/(n-2)$. It follows that $k/(n-2) < 5/2+\sqrt{k}$. Thus $\sqrt{k} < n+1/2$ and so $k \le n^2+n$. Hence

$$m = k(n-1)+r \le (k+1)(n-1)-1 \le (n-1)(n^2+n+1)-1 = n^3-2,$$

a contradiction. ∎

Corollary 12.4. *Put $m = k(n-1)+r$, where $0 \le r \le n-2$. Suppose $n \ne 5$ and $m \ge n^3-1$. Also assume $2 \le r$. Let W_0 have the maximal Frobenius number among n-element sets W with $\gcd(W) = 1$ and $\max(W) = m$. Then $W_0 = \{m, m-1, \dots, m-n+1\}$.*

Proof. By (17), $G(m, m-1, \dots, m-n+1) = k(m-n+1)-1$. By Corollary 12.2, we may assume $W_0 \in \mathcal{F}$. The result follows easily from Lemma 12.3. ∎

Let A have $\gcd(A) = 1$ and $\max(A) = m$. Recall that for $r \in \{0,1,2\}$, Theorem 10.1 implies that $G(A) \le [(m-2)(m-n+1)/(n-1)]-1$. Assume now $3 \le r$. Corollary 12.4 implies that

$$G(A) \le \left[\frac{m-2}{n-1}\right](m-n+1)-1 < \left[\frac{(m-2)(m-n+1)}{n-1}\right]-1.$$

Hence Lewin's conjecture holds. Moreover the inequality is strict for $r \ge 3$.

References

[1] A. L. Cauchy, *Recherches sur les nombres*, J. Ecole Polytechnique 9 (1813), 99–116.
[2] S. Chowla, H. B. Mann and E. G. Straus, *Some applications of the Cauchy–Davenport theorem*, Norske Vid. Selsk. Forh. (Trondheim) 32 (1959), 74–80.

[3] H. Davenport, *On the addition of residue classes*, J. London Math. Soc. 10 (1935), 30–32.
[4] J. Dixmier, *Proof of a conjecture by Erdős and Graham concerning the problem of Frobenius*, J. Number Theory 34 (1990), 198–209.
[5] G. A. Freiman, *Foundations of a Structural Theory of Set Addition*, Transl. Math. Monographs 37, Amer. Math. Soc., Providence, RI, 1973.
[6] Y. O. Hamidoune, *Sur les atomes d'un graphe orienté*, C. R. Acad. Sci. Paris A 284 (1977), 1253–1256.
[7] —, *Quelques problèmes de connexité dans les graphes orientés*, J. Combin. Theory Ser. B 30 (1981), 1–10.
[8] —, *On the connectivity of Cayley digraphs*, Europ. J. Combin. 5 (1984), 309–312.
[9] —, *On subsets with a small sum in abelian groups*, ibid. 18 (1997), 541–556.
[10] —, *An isoperimetric method in Additive Theory*, J. Algebra 179 (1996), 622–630.
[11] —, *Subsets with a small product in groups. Structure Theory of set-addition*, Astérisque 258 (1999), xiv-xv, 281–308.
[12] —, *On the Diophantine Frobenius problem*, Portugal. Math. 55 (1998), 425–449.
[13] A. Janz, *Bestimmung der maximalen Frobeniuszahl*, Master Thesis, Johannes Gutenberg Universität, Mainz, April 1997.
[14] J. H. B. Kempermann, *On small sumsets in abelian groups*, Acta Math. 103 (1960), 66–88.
[15] M. Kneser, *Summenmengen in lokalkompakten abelschen Gruppen*, Math. Z. 66 (1956), 88–110.
[16] V. F. Lev, *On extremal aspects of the Frobenius problem*, J. Combin. Theory Ser. A 1 (1996), 111–119.
[17] —, *Structure theorem for multiple addition and the Frobenius problem*, J. Number Theory 58 (1996), 79–88.
[18] M. Lewin, *A bound for a solution of a linear diophantine problem*, J. London Math. Soc. 6 (1972), 61–69.
[19] H. B. Mann, *An addition theorem for sets of elements of an abelian group*, Proc. Amer. Math. Soc. 4 (1953), 423.
[20] J. E. Olson, *On the sum of two sets in a group*, J. Number Theory 18 (1984), 110–120.
[21] J. B. Roberts, *Note on linear forms*, Proc. Amer. Math. Soc. 7 (1956), 465–469.
[22] J. J. Sylvester, *Mathematical questions with their solutions*, Educational Times 41 (1884), 21.
[23] A. Tietäväinen, *On diagonal forms over finite fields*, Ann. Univ. Turku Ser. A I 118 (1968), 10pp.
[24] G. Vosper, *The critical pairs of subsets of a group of prime order*, J. London Math. Soc. 31 (1956), 200–205.

E. Combinatoire
Université P. et M. Curie
4 Place Jussieu
75005 Paris, France
E-mail: yha@ccr.jussieu.fr

Received on 23.1.1997
and in revised form on 10.3.2000 (3119)