PORTUGALIAE MATHEMATICA
Vol. 55 Fasc. 4 – 1998

ON THE DIOPHANTINE FROBENIUS PROBLEM

Y.O. Hamidoune

Abstract: Let $X \subset \mathbb{N}$ be a finite subset such that $\gcd(X) = 1$. The Frobenius number of X (denoted by $G(X)$) is the greatest integer without an expression as a sum of elements of X. We write $f(n, M) = \max\{G(X); \gcd(X) = 1, |X| = n \ \& \ \max(X) = M\}$.

We shall define a family $\mathcal{F}_{n,M}$, which is the natural extension of the known families having a large Frobenius number. Let A be a set with cardinality n and maximal element M. Our main results imply that for $A \notin \mathcal{F}_{n,M}$, $G(A) \le (M - n/2)^2/n - 1$. In particular we obtain the value of $f(n, M)$, for $M \ge n(n-1) + 2$. Moreover our methods lead to a precise description for the sets A with $G(A) = f(n, M)$.

The function $f(n, M)$ has been calculated by Dixmier for $M \equiv 0, 1, 2$ modulo $n-1$. We obtain in this case the structure of sets A with $G(A) = f(n, M)$. In particular, if $M \equiv 0 \bmod n-1$, a result of Dixmier, conjectured by Lewin, states that $G(A) \le G(N)$, where $N = \{M/(n-1), 2M/(n-1), ..., M, M-1\}$. We show that for $n \ge 6$ and $M \ge 3n-3$, $G(A) < G(N)$, for $A \ne N$.

1 – Introduction

Concerning the history of the Frobenius problem, we quote from [4]:

> "Given $0 < a_1 < \cdots < a_n$ with $\gcd(a_1, ..., a_n) = 1$. It is well known that the equation $N = \sum_{1 \le k \le n} a_k\, x_k$ has solutions in non negative integers provided N is large enough. Following [Johnson, (1960)], we let $G(a_1, ..., a_n)$ the greatest integer for which the above equation has no such solution.
>
> The problem of determining $G(a_1, ..., a_n)$, or at least obtaining non trivial estimates, was first raised by Frobenius and has been the subject of numerous papers."

Received: May 28, 1997.

For $A = \{a_1, ..., a_n\}$, we shall write $G(A) = G(a_1, ..., a_n)$. The case $|A| = 2$ was settled by Sylvester [20].

Erdös and Graham proved in [4] that $G(A) \leq 2(\max(A))^2/|A|$. They conjectured that for $|A| \geq 2$, $G(A) \leq (\max(A))^2/(|A|-1)$.

Later this conjecture was studied using addition theorems on cyclic groups. To get an idea about the work done and the methods of finite addition theorems, the reader may refer to the bibliography in particular: Vitek [21], Hofmeister [12], Rödseth [18] and Dixmier [2].

The conjecture of Erdös–Graham was proved by Dixmier [2], by combining Kneser's addition theorem for finite abelian groups and some new arguments carried over the integers.

Let us denote by $\Phi(A)$ the set of integers which have representations as sums of elements from A. Let $A \subseteq [1, M]$, Dixmier obtained the following density theorem [2]:

$$\left|\Phi(A) \cap \Big[(k-1)M+1,\ kM\Big]\right| \geq \min\Big(M,\ k|A|-k+1)\Big) \ .$$

As an application, Dixmier [2] obtained

$$G(A) \leq (M - n/2 + 1)\,(M - n/2)/(n-1) - 1 \ .$$

We shall use new addition theorems allowing to go beyond the conclusions of Kneser's Theorem to get a sharp upper bound for the Frobenius number.

Our method works almost entirely within congruences.

In the remaining of the introduction, A denotes a subset of $\mathbb{N}$ such that $\gcd(A) = 1$ and $|A| \geq 3$. We put $n = |A|$ and $M = \max(A)$.

We shall define in the appropriate section an exceptional family $\mathcal{F}_{n,M}$ very close to arithmetic progressions. Our basic density theorem states that for $A \notin \mathcal{F}_{n,M}$,

$$\left|\Phi(A) \cap \Big[(k-1)M+1,\ kM\Big]\right| \geq \min\Big(M-1,\ k|A|\Big) \ .$$

As a corollary we show that for $A \notin \mathcal{F}_{n,M}$, $G(A) \leq (M-n/2)^2/n - 1$.

In particular we calculate the maximal value of $G(A)$, denoted by $f(n, M)$, for $M \geq n(n-1) + 2$.

In the last part we study the uniqueness of the examples reaching the bounds. There are three kind of examples of sets with large Frobenius number, cardinality n and maximal element M: $P = \{M, M-1, ..., M-n+1\}$; $N = \{M/(n-1), 2M/(n-1), ..., M, M-1\}$, where $M \equiv 0$ modulo $n-1$ and $D = \{(M-1)/(n-1), 2(M-1)/(n-1), ..., (M-1), M\}$, where $M \equiv 1$ modulo $n-1$.

Let A be a set with cardinality n and maximal element M. It was conjectured by Lewin [14] and proved by Dixmier [2] that $G(A) \leq G(N)$ if $M \equiv 0$ modulo $n-1$. We show that for $n \geq 6$ and $M \geq 3n-3$, $G(A) < G(N)$, for $A \neq N$.

Another conjecture of Lewin [14] proved by Dixmier [2] states that $G(A) \leq G(D)$ if $M \equiv 1$ modulo $n-1$. We show that for $n \geq 6$ and $M \geq 3n-3$, $G(A) < G(D)$, for $A \neq N$ except if $M \equiv 0$ or 1 modulo $(M-1)/(n-1)+1$, where one other example attaining the bound is present.

The last case where an attainable bound was known is the case $M \equiv 2$ mod $n-1$. We show in this case that P is the unique example reaching the bound, except for $M \equiv 0$ or 1 modulo $(M-2)/(n-1)+1$, where one other example attaining the bound is present.

2 – Isoperimetric numbers

The isoperimetric method was first used to study some combinatorial problems on Cayley diagrams in [7, 6]. We observed later that the results obtained imply good estimations of the size of the sum of two sets, which is the object of Addition theorems mentioned above. This interaction motivates more elaborate techniques [8, 9, 10].

Let k be a positive integer and let G be a finite abelian group. Let B be a subset of G such that $0 \in B$ and $|B| \geq 2$.

Following the terminology of [10], we shall say that B is k-separable if there is $|X| \geq k$ such that $|X+B| \leq |G|-k$. Suppose B k-separable. The *k-isoperimetric number* is defined in [10] as

$$\kappa_k(B) = \min\Big\{|X+B|-|X| \;\Big|\; |X| \geq k \text{ and } |X+B| \leq |G|-k\Big\} . \tag{1}$$

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

$$|X+B| \geq \min\Big(|G|-k+1,\, |X|+\kappa_k(B)\Big) . \tag{2}$$

It may happen that B generates a proper subgroup H. In that case one may decompose $X = X_1 \cup \cdots \cup X_s$, where X_i is a nonempty intersection of some H-coset with X. Now we may apply (2) to $X_i - x$, for some $x \in X_i$. We shall use this decomposition only for $k=1$. We obtain in this case the following special case of a relation obtained in [9]:

$$\forall X,\;\; |X+B| \geq \min\Big(|X+H|,\, |X|+\kappa_1(H,B)\Big) . \tag{3}$$

A subset X will be called a (k,B)-*critical set* if $\kappa_k(B) = |X+B| - |X|$, $|X| \geq k$ and $|X+B| \leq |G| - k$.

A (k,B)-critical set with minimal cardinality will be called a (k,B)-*atom*. The reference to B will be omitted when the context is clear.

Let us formulate a special case of a result proved in [7] in the case of non necessarily abelian groups.

Proposition 2.1 ([7]). *Let B be a subset of G such that $0 \in B$ and $|B| \leq |G| - 1$. Let H be a $(1,B)$-atom such that $0 \in H$. Then H is a subgroup.*

We need the following special case of a result obtained in [6]. Notice that this result generalises a theorem proved independently by Olson [16].

Corollary 2.2 ([6]). *Let B be a generating proper subset of a finite abelian group G such that $0 \in B$. Then*

$$\kappa_1(G,B) \geq |B|/2 \ . \tag{4}$$

We need the following immediate consequence of a result in [8].

Proposition 2.3 ([8]). *Let B be a 2-separable subset of a finite abelian group G such that $\kappa_2(B) \leq |B| - 1 \leq |G|/2 - 1$. Then either B is an arithmetic progression or there is a subgroup H such that $|G| > |H+B| = |H| + \kappa_2(B)$.*

The above three results will be proved entirely with 5 pages in [11] and applied to Inverse Additive Theory.

3 – The Frobenius problem and congruences

Recall the following well known and easy lemma, stated usually with $H = G$:

Lemma 3.1 ([15]). *Let H be a subgroup of a finite abelian group G. Let X and Y be subsets of G such that $|X+H| = |Y+H| = |H|$ and $|X| + |Y| > |H|$. Then $|X+Y| = |H|$.*

Let $A \subseteq \mathbb{N}$ and set $M = \max(A)$. Following Dixmier [2], we put $\Phi(A) = \bigcup_{i\geq 1} iA$ and $\Phi_k(A) = \Phi(A) \cap [(k-1)M+1,\, kM]$.

The reference to A will be omitted when the context is clear. In particular we shall write $\Phi = \Phi(A)$.

In this section, we fix the following notations. Let M be a natural number and let ν be the canonical morphism from $\mathbb{Z}$ onto $\mathbb{Z}_M$.

For an integer m we shall write $\overline{m} = \nu(m)$. Mainly we shall be interested in the set $\overline{\Phi}_k = \nu(\Phi_k)$.

We have clearly, $\Phi_k + \Phi_1 \subseteq \Phi_{k+1} \cup \Phi_{k+1} - M$. Reducing modulo M, we get:

$$\overline{\Phi_k} + \overline{\Phi_1} \subseteq \overline{\Phi_{k+1}} \ . \tag{5}$$

By iterating we obtain

$$k\,\overline{\Phi_1} \subseteq \overline{\Phi_k} \ . \tag{6}$$

We shall need the following well known lemma used by Dixmier [2]. We shall supply a short proof of this lemma based on Lemma 3.1.

Lemma 3.2 ([2])**.** *Let M be a nonnegative integer and let $A \subseteq [1, M]$. Suppose $|A \cap [1, M]| > M/2$. Then $[M-1, \infty[\subseteq \Phi(A)$.*

Proof: We have clearly $2|\overline{A}| = 2|A| > M$. By Lemma 3.1, $\overline{A+A} = \overline{A}+\overline{A} = \mathbb{Z}_M$. For all $k \geq 2$, we have by (6), $|\overline{\Phi_k}| \geq |k\,\overline{\Phi_1}| \geq |2\,\overline{\Phi_1}| \geq |2\overline{A}| = M$. In particular $[M, \infty[\subseteq \Phi(A)$. It remains to show that $M-1 \in A \cup (A + A)$. Suppose $M-1 \notin A + A$. The above relations show that $2M-1 \in A + A$, which forces $M-1 \in A$. ∎

Let H be a subgroup of $\mathbb{Z}_M$. By a *H-string*, we shall mean a set R contained in some H-coset satisfying one of the following conditions:

- (**G1**) There is a generator q of H such that $R = \{z + q, ..., z + (|R|-1)q\}$, for some z.
- (**G2**) $R - y$ generates H for some $y \in R$ and $\exists\, R_0 \subseteq \mathbb{N}$ and $t \in \mathbb{N}$ such that $\overline{R_0} = R$ and $R_0 \subseteq [t,\, t + (M-1)/2]$.

Lemma 3.3. *Let H be a subgroup of $\mathbb{Z}_M$ and let R be a H-string. Then*

$$\forall\, X, \quad |X + R| \geq \min\Big(|X + H|,\, |X| + |R| - 1\Big) \ . \tag{7}$$

Proof: We may assume $|R| \geq 2$, since otherwise (7) holds trivially.

Let $y \in R$. Let us first prove that $\kappa_1(H, R-y) = |R|-1$. Suppose the contrary and let Q be a 1-atom of $(H, R-y)$ such that $0 \in Q$. By Proposition 2.1, Q is a subgroup. By the definition of a 1-atom:

$$|Q + R| < \min\Big(|H|,\, |Q| + |R| - 1\Big) \ .$$

Let $t = |R+Q|/|Q|$. We have $t \geq 2$, since $R - y$ generates H.

Consider first the case where (G1) is satisfied. Take $s \in R$. We have $|(Q+s) \cap R| \leq (|Q|+1)/2$, since otherwise $\exists\, s_1, s_2 \in R \cap (Q+s)$, such that $s_1 - s_2 = q$ and hence $Q = H$, contradicting $Q \neq H$. Hence $|R+Q| - |R| \geq (|Q|-1)t/2 \geq |Q|-1$, a contradiction.

Assume now (G2) satisfied. Since R has a representative R_0 contained in an interval with length $(M-1)/2$, we have also in this case $|R+Q| - |R| \geq (|Q|-1)t/2 \geq |Q|-1$.

Therefore $|Q|-1 \leq |Q+R| - |R| < |Q|-1$, a contradiction. Now we may apply (3) to obtain (7). ∎

Let Q be a subgroup of $\mathbb{Z}_M$ and let $v \in A$. Set $\overline{\Phi}_k \cap (j\,\overline{v} + Q) = Q(\overline{v}; k, j)$. The reference to v will be omitted and we shall write $Q(k,j) = Q(\overline{v}; k, j)$.

By (5), we have $Q(k,i) + Q(1,s) \subseteq \overline{\Phi_{k+1}}$. It comes

$$Q(k,i) + Q(1,s) \subseteq Q(k+1, i+s)\ . \tag{8}$$

We shall estimate $\overline{\Phi}_k \backslash (\overline{\Phi}_{k-1} + \overline{\Phi}_1)$, using the next lemma.

Lemma 3.4. *Let $A \subseteq [1,M]$ such that* $\gcd(A) = 1$ *and let Q be a subgroup of $\mathbb{Z}_M$. Let $v \in A$ such that $\overline{v} \notin Q$. Set $V_1 = \overline{\Phi_1} \cap (Q + \overline{v})$. Assume $V_1 \neq \emptyset$ and let $r_0 = M/|Q|$. Let $i \leq r_0 - 1$.*

If $|Q(k,i)| = |Q|$, then $Q(k,i+1)$ contains a Q-string with size $\geq |V_1| - 1$.

Moreover we have the following relation:

$$\textit{If}\quad |Q(k,i)| \geq |Q| - |V_1| + 2, \qquad \textit{then}\ \ Q(k,i+1) \neq \emptyset\ . \tag{9}$$

Proof: Set $M = q|Q|$. Clearly Q is generated by $\overline{q}$. Choose $0 \leq w_j \leq q-1$, such that $\overline{w_j} \in Q + j\,\overline{v}$, $\ 0 \leq j \leq r_0 - 1$.

There is clearly a representative x_1 of V_1 such that $1 \leq x_1 \leq w_1 + (|Q| - |V_1|)q$.

Set $Y = (k-1)M + w_i + \{0, q, \ldots, (|V_1|-2)q\}$. Assume $|Q(k,i)| \geq |Q|$. It follows that $Y \subseteq \Phi_k$. For every $y \in Y$, $(k-1)M + 1 \leq x_1 + y \leq (|Q| - |V_1|)q + w_1 + (k-1)M + w_i + (|V_1|-2)q < (k-1)M + |Q|q = kM$.

It follows that the string $\overline{x_1 + Y} \subseteq \overline{\Phi_k} \cap (Q + (i+1)\,\overline{v}) = Q(k, i+1)$. This proves the first part.

Assume now $|Q(k,i)| \geq |Q| - |V_1| + 2$. There is clearly a representative z of $Q(k,i)$ such that $(k-1)M + 1 \leq z \leq w_i + (|V_1|-2)q$.

Clearly $(k-1)M + 1 \leq x_1 + z \leq (|Q| - |V_1|)q + w_1 + (k-1)M + w_i + (|V_1|-2)q < (k-1)M + |Q|q = kM$. ∎

Let H be a subgroup of $\mathbb{Z}_M$. For $x \in \mathbb{Z}_M$, we shall denote by $\xi_H(x)$ the unique $r \in [0,\ M/|H|-1]$, verifying the condition $\overline{r} \in x+H$. Let $x_1, x_2 \in \mathbb{Z}_M$ be such that $x_1-x_2 \notin H$. Assume moreover $x_1+x_2 \in H$ or $2(x_1-x_2) \in H$, one may check easily that there exists $1 \le i \le 2$ such that

$$\xi(x_i) < M/(2|H|) \ . \tag{10}$$

Lemma 3.5. *Let H be a subgroup of $\mathbb{Z}_M$ and let $y_1, y_2 \in \overline{\Phi_1}$ such that $y_1+y_2+H \subseteq (2\overline{\Phi_1}+H)\backslash(\overline{\Phi_1}+H)$. Then*

$$|\overline{\Phi_1} \cap (y_1+H)| + |\overline{\Phi_1} \cap (y_2+H)| \le |H| + (\xi(y_1)+\xi(y_2))|H|/M \ . \tag{11}$$

Proof: Put $M = q|H|$.

For $1 \le i \le 2$, set $M_i = (y_i+H) \cap \overline{\Phi_1}$ and $m_i = \min\{m\colon\ m \in \Phi_1 \ \&\ \overline{m} \in M_i\}$ and put $r_i = \xi(y_i)$.

We have clearly, for $1 \le i \le 2$,

$$|M_i| \le 1 + (M-q+r_i-m_i)/q \ .$$

Since $m_1+m_2 \notin \Phi_1$, $M < m_1+m_2 \le M+r_1-q|M_1|+M+r_2-q|M_2| \le 2M+r_1+r_2-q(|M_1|+|M_2|)$. Therefore $|M_1|+|M_2| < |H|+(\xi(y_1)+\xi(y_2))|H|/M$. This shows (11). ∎

4 – The density of the Frobenius semigroup

We shall use the following lemma:

Lemma 4.1. *Let G be a finite abelian group. Let X be a generating subset of G such that $0 \in X$, $|X| = 3$ and $|2X| = 6$. Then*

$$\forall\, j \ge 1, \quad |jX| \ge \min\Big(|G|,\ 3j-1\Big) \ . \tag{12}$$

Proof: Consider first the case $|G| \le 7$. By our hypothesis $|2X| = 6$. By Lemma 3.1, $3X = G$. Hence (12) holds. Assume now $|G| \ge 8$. Since $|2X| = 6$, X is 2-separable. Clearly X is not an arithmetic progression since otherwise $|2X| = 5$.

We have for every proper subgroup $Q \subseteq G$, $|Q+X|-|Q| > \min(|G|-|Q|-1, 2)$. Since otherwise, we have necessarily, $|Q| = 2$ and $|Q+X| = 2|Q|$. It follows that $X = Q \cup \{x\}$. Hence $|2X| = 2|Q|+1 = 5$, a contradiction.

By Proposition 2.3, $\kappa_2(G, X) \geq 3$.

It follows by iterating (3) that

$$\forall j \geq 1, \quad |jX| \geq \min\Big(|G| - 1,\ 3j\Big) \ . \tag{13}$$

Suppose $|jX| \leq |G| - 1$. By Lemma 3.1, $|(j-1)X| + |X| \leq |G|$. By (13) $|(j-1)X| \geq 3(j-1)$. By (4), $\kappa_1(X) \geq 2$. By (2), $|jX| \geq 3(j-1) + 2 = 3j - 2$.

This proves (12). ∎

The following result implies a very restrictive structure when the Frobenius semigroup has a small density.

Theorem 4.2. *Let $A \subseteq \mathbb{N}$ such that* $\gcd(A) = 1$ *and set* $M = \max(A)$. *Then one of the following conditions holds:*

(i) $|\overline{\Phi_k}| \geq \min\Big(M-1,\ k|\Phi(A) \cap [1, M]|\Big)$.

(ii) *$\overline{\Phi_1}$ is an arithmetic progression.*

(iii) *$\overline{\Phi_1} = H \cup T$, where H is a subgroup and T is contained in some H-coset.*

(iv) *There is $r < M/2$ such that $\Phi_1 = \{r,\ 2r,\ M/2,\ r + M/2,\ M\}$.*

Proof: Condition (i) of Theorem 4.2 holds by Lemma 3.1 if $|\Phi_1| > M/2$. Therefore we may assume:

$$|\Phi_1| \leq M/2 \ . \tag{14}$$

Assume that $\overline{\Phi_1}$ is not an arithmetic progression. In particular $|\overline{\Phi_1}| \geq 2$. Condition (i) of Theorem 4.2 holds by (6), if $|k\,\overline{\Phi_1}| \geq \min(M-1,\ k|\overline{\Phi_1}|)$. Suppose the contrary, it follows that $k \geq 2$. Now we must have for some $1 \leq j \leq k-1$, $|j\,\overline{\Phi_1} + \overline{\Phi_1}| < \min(M-1,\ |j\overline{\Phi_1}| + |\overline{\Phi_1}|)$.

It follows that $(\mathbb{Z}_M, \overline{\Phi_1})$ is 2-separable and that

$$\kappa_2(\mathbb{Z}_M, \overline{\Phi_1}) \leq |\Phi_1| - 1 \ .$$

Since $\overline{\Phi_1}$ is not an arithmetic progression and by Proposition 2.3 there is a proper subgroup H of $\mathbb{Z}_M$ with the following property:

$$\min\Big(M - |H| - 2,\ |\Phi_1| - 1\Big) \geq \kappa_2(\overline{\Phi_1}) \geq |\overline{\Phi_1} + H| - |H| \ . \tag{15}$$

We shall now choose H to be with maximal cardinality satisfying (15). Put $r_0 = M/|H|$.

Set $H + \overline{\Phi_1} = \{z_0 + H, ..., z_\beta + H\}$, where $|(z_1 + H) \cap \overline{\Phi_1}| \geq \cdots \geq |(z_\beta + H) \cap \overline{\Phi_1}|$ and $z_0 = 0$. Clearly $|H + \overline{\Phi_1}| = (\beta + 1)\,|H|$. Set $T = \bigcup_{i \neq \beta} z_i + H$.

For $i \le \beta$, put $A_i = \overline{\Phi_1} \cap (z_i + H)$.

(15) implies immediately

$$\min\Big(M - |H| - 2,\, |A_0| + \cdots + |A_\beta| - 1\Big) \ge \kappa_2(\overline{\Phi_1}) \ge \beta|H| \ . \tag{16}$$

By (14) and (16), $M/2 \ge \sum_{0 \le i \le \beta} |A_i| \ge \beta|H| + 1$. Since $|H|$ divides M, we have

$$M \ge (2\beta + 1)\,|H| \ . \tag{17}$$

Assume first

$$|A_\beta| = 1 \ .$$

By (16), $|A_i| = |H|$, for all $i \ne \beta$. We have $z_i + z_j + H \subseteq \overline{\Phi}_1 + H$, for all $i, j \ne 1$, since otherwise by (11), $2|H| \le |H| + (2M/|H| - 2)|H|/M = |H| + 2 - 2|H|/M$. In particular

$$T + T \subseteq T \cup z_\beta + H \ . \tag{18}$$

Consider first the case where T generates a proper subgroup. Since $T \cup z_\beta + H$ generates $\mathbb{Z}_M$, we have $T + T \subseteq T$. Therefore T is a subgroup. In this case (iii) holds. We may then assume that T generates $\mathbb{Z}_M$.

By (4) and (17), $|2T| \ge \min(M, 3\beta|H|/2) = 3\beta|H|/2$. By (18), $3\beta|H|/2 \le |2T| \le (\beta + 1)\,|H|$.

Hence $\beta \le 2$. Clearly (iii) holds if $\beta = 1$. Assume $\beta = 2$. Since T is not a subgroup, we have necessarily by (18), $2z_1 + H = z_2 + H$. There is clearly $r' < M/|H|$ such that $\overline{r'} \in A_1$. Since $(3z_1 + H) \cap (A_0 \cup A_1 \cup A_2) = \emptyset$, (observe that $M \ge 5|H|$), we have necessarily $3r' > M$. It follows that $M < 3r' < 3M/|H|$ and hence $|H| = 2$. In this case we have clearly $\Phi_1 = \{M,\, M/2\} \cup \{r,\, M/2 + r\} \cup \{2r\}$, for some $r < M/2$ and Condition (iv) holds in this case.

We may therefore assume

$$|A_\beta| \ge 2 \ . \tag{19}$$

The case $\beta \ge 3$.

Let us show that T generates $\mathbb{Z}_M$. Suppose the contrary. It follows easily that $z_i + H + z_\beta + H \subseteq (2\overline{\Phi_1} + H) \setminus (\overline{\Phi_1} + H)$, for $1 \le i \le 2$. By (11), $|A_\beta| + |A_i| \le |H| + 1$. It follows by (16) that $|A_\beta| + |A_i| = |H| + 1$, for all $1 \le i \le 2$. By (16), $|H| - 1 \ge (\beta + 1)\,|H| - |A_0| - \cdots - |A_\beta| \ge 3|H| - |A_1| - |A_2| - |A_\beta| = |H| + |A_\beta| - 2$. Hence $|A_\beta| \le 1$, contradicting (19).

By (3), (4) and (17), $|\overline{\Phi_1} + H + T| \ge \min(M, |\overline{\Phi_1} + H + \kappa_1(T)) \ge |\overline{\Phi_1} + H| + \beta|H|/2 \ge |\overline{\Phi_1} + H| + 3|H|/2$. In particular there are $i, j \notin \{\beta\}$, such that $z_i + z_j + H \subseteq (2\Phi_1 + H) \setminus (\overline{\Phi_1} + H)$.

By (11), $|A_i| + |A_j| \leq |H| + 1$. It follows that $2|A_{\beta-1}| \leq |H| + 1$ and hence $2|A_\beta| \leq |H| + 1$. By (16),

$$|A_\beta| = |A_{\beta-1}| = (|H| + 1)/2 \ .$$

It follows that $|H| \geq 3$.

By (16), $|H| = |A_i|$, for all $1 \leq i \leq \beta - 2$.

Now we must have $\beta = 3$, since otherwise by (16), $|2\overline{\Phi_1} + H| - |\overline{\Phi_1} + H| \geq \min(M, 4|H|) = 4|H|$.

It follows that there are $s, t \in \{1, \beta\}$, such that $z_s + z_t \in (2\overline{\Phi_1} + H) \setminus (\overline{\Phi_1} + H)$ and $(s,t) \notin \{(\beta,\beta), (\beta,\beta–1), (\beta–1,\beta–1)\}$. Hence $|A_s| + |A_t| \geq |H| + (|H|+1)/2 \geq |H| + 2$, contradicting (11).

Observe that $z_i + z_1 + H \subseteq \overline{\Phi_1} + H$, for all i, since otherwise by (11) and (19), $2 + |H| \leq |A_i| + |A_1| \leq |H| + 1$, a contradiction. It follows that $z_1 + H + \overline{\Phi_1} + H = \overline{\Phi_1} + H$. Let Q be the subgroup generated by $H \cup z_1 + H$. Clearly $Q + \overline{\Phi_1} + H = \overline{\Phi_1} + H$. Hence $|Q|$ divides $4|H|$. Since $\overline{\Phi_1}$ generates $\mathbb{Z}_M$ and by (17), we have $Q \neq \mathbb{Z}_M$. We have necessarily $|Q| = 2|H|$. In particular $Q = H \cup z_1 + H$ and $2z_1 + H = H$. It follows also that $z_3 + H = z_2 + H$ and hence $z_3 + Q = z_2 + Q$. Therefore $|Q + \overline{\Phi_1}| = 2|Q| = 4|H|$. By the definition of κ_2 and (17), $|Q + \overline{\Phi_1}| \geq \min(M-1,\, |Q| + 3|H|) = 5|H|$, a contradiction.

Therefore we may assume $\beta \leq 2$.

The case $\beta = 2$.

Assume first

$$2z_1 + H \neq z_2 + H \quad \text{and} \quad 2z_2 + H \neq z_1 + H \ .$$

Let us show that

$$\forall\, i \geq 1, \quad 2z_i + H \neq H \ . \tag{20}$$

Suppose the contrary. It follows that $Q = H \cup z_i + H$ is a subgroup. Now we have by the maximality of H, $|Q + \overline{\Phi_1}| > \min(M - 1, |Q| + 2|H|) = 2|Q|$. But $|Q + \overline{\Phi_1}| \leq 2|Q|$, since $H \subseteq Q$, a contradiction.

Let us show that $2z_1 + H \neq 2z_2 + H$ and $z_1 + z_2 + H \neq H$. Suppose the contrary. By (10), $\exists\, 1 \leq i \leq 2$ such that $\xi(z_i) < M/(2|H|)$. By (20) and our hypothesis, $2z_i + H \subseteq (2\overline{\Phi_1} + H) \setminus (\overline{\Phi_1} + H)$. By (11), $2|A_i| \leq |H| + 2\xi(z_i)|H|/M < |H| + 1$.

Therefore $2|A_2| \leq 2|A_i| \leq |H|$.

By (19), our hypothesis and (11), $2|A_1| \leq |H| + 2\xi(z_1)|H|/M < |H| + 2$. By adding we get $|A_1| + |A_2| \leq |H| + 1/2$, contradicting (16).

Therefore the cosets H, z_1+H, z_2+H, $2z_1+H$, $2z_2+H$, z_1+z_2+H are all distinct. In particular

$$|2(H+\overline{\Phi_1})| = 6|H| \ .$$

We have clearly $(2\overline{\Phi_1}+H) \setminus (\overline{\Phi_1}+H) = \{2z_1+H, 2z_2+H, z_1+z_2+H\}$. By (11) and by (16), we have necessarily $|A_1| = |A_2| = (|H|+1)/2$ and by (16), $A_0 = H$. By Lemma 3.1, $2\overline{\Phi_1} = 2\overline{\Phi_1}+H$. It follows that

$$\forall j \geq 2, \quad j\overline{\Phi_1}+H = j\overline{\Phi_1} \ .$$

By (12)

$$\forall j \geq 2, \quad |j\overline{\Phi_1}| = j|H| \Big(|\overline{\Phi_1}+H|/|H|\Big) \geq \min\Big(M,\, 3j|H|-|H|\Big) \ .$$

It follows that

$$\forall j \geq 2, \quad |j\overline{\Phi_1}| \geq \min\Big(M,\, j(2|H|+1)\Big) = \min\Big(M, j|\overline{\Phi_1}|\Big) \ .$$

In particular (i) holds.

We may assume now

$$2z_1+H = 2z_2+H \quad \text{ or } \quad 2z_2+H = z_1+H \ .$$

There is $x \in \mathbb{Z}_M$ such that

$$\overline{\Phi_1}+H = H \cup x+H \cup 2x+H \ .$$

Put $\overline{\Phi_1} \cap (ix+H) = V_i$, $1 \leq i \leq 2$.

By (16), $|A_0|+|V_1|+V_2| \geq 2|H|+1$. By (17), $V_i+H+V_2+H \subseteq (2\overline{\Phi_1}+H) \setminus (\overline{\Phi_1}+H)$, $1 \leq i \leq 2$. By (11), $|V_i|+|V_2| \leq |H|+1$, $1 \leq i \leq 2$.

The above relations force

$$|V_1| \geq |V_2| \ \ \& \ \ A_0 = H \ \ \& \ \ |V_1|+|V_2| = |H|+1 \ .$$

Since the unique requirement was $|A_1| \geq |A_2|$, we may assume $V_1 = A_1$ and $V_2 = A_2$. The above relation takes the following form:

$$|A_0| = |A_1|+|A_2|-1 = |H| \ . \tag{21}$$

Let us show that A_1 and A_2 are H-strings. Set $M = |H|q$. We have $\overline{q} \in A_0$. Choose the smallest represantive w_i of A_i. Necessarily A_i must have $\{w_i, w_i+q, ..., w_i+M\} \cap [1, M]$ as a representative set. This follows since $q\,\mathbb{N}+w_i \subseteq \Phi$.

By (19) and the relation $|A_1| + |A_2| = |H| + 1$ obtained above, we have $|H| \geq 3$. We must have $|H| \geq 4$, since otherwise necessarily there is r such that $\Phi_1 = \{M, M/3, 2M/3, r + M/3, r + 2M/3, 2r + M/3, 2r + 2M/3\}$. Since $2r + 2M/3 < M$, $r < M/6$. Now $3r \in \Phi_1$. It follows that $3\overline{r} \in H$ and hence (observing that $\overline{r} + H$ generates $\mathbb{Z}_M/H$) $3|H| \geq M$, contradicting (17). We may now assume $|H| \geq 4$.

Choose v to be representative A_1. In the remaining of this proof, by $H(i,j)$ will mean $H(\overline{v}; i, j)$.

Since $H \cup \overline{v} + H \cup 2\overline{v} + H$ generates $\mathbb{Z}_M$, $\overline{v} + H$ generates $\mathbb{Z}_M/H$. In particular $t\overline{v} \notin H$, for all $1 \leq t \leq r_0 - 1$.

By (8), for all j,

$$H(k-1, j) + A_s \subseteq H(k, j + s) \ . \tag{22}$$

Let α be the smallest integer t such that $|\Phi_t| \geq M - 1$. We shall denote by $\theta(k)$ the greatest integer $j \leq r_0 - 1$, such that $|H(k,i)| = |H|$ for all $i \leq j - 1$ and $|H(k,j)| \geq 1$.

We shall prove by induction the following:

For every $2 \leq k \leq \alpha - 1$,

$$\sum_{0 \leq i \leq \theta(k)} |H(k,i)| \geq k|\Phi_1| \ . \tag{23}$$

For $k = 2$, by (22), (21) and Lemma 3.1 we have $|H(2,0)| = |H(2,1)| = |H(2,2)| = |H(2,3)| = |H|$ and $|H(2,4)| \geq 2|A_2| - 1 \geq 3$. It follows that $\theta(2) \geq 4$ and that $\sum_{0 \leq i \leq \theta(2)} |H(k,i)| \geq 4|H| + 3 > 2|\Phi_1|$. Hence (23) holds for $k = 2$. Suppose (23) proved for $k - 1$. Assume $k \leq \alpha - 1$.

Set $J = \theta(k-1)$. We have by (22) and (21), $H(k,i) \supseteq H(k-1, i-2) + A_2 = A_2 + H$, for $i = J, J+1$. Hence

$$\forall\, i \leq J + 1, \quad |H(k,i)| = |H| \ . \tag{24}$$

We have by (7) and (22),

$$|H(k, J+2)| \geq |H(k,J) + A_2| \geq \min\Big(|H|,\ |H(k-1,J)| + |A_2| - 1\Big) \ .$$

It follows that $\theta(k) \leq J + 2 \leq r_0 - 1$. Now $\sum_{0 \leq i \leq J+2} |H(k,i)| \geq (k-1)\,|\Phi_1| + |H| - |H(k-1,J)| + |H| + \min(|H|, |H(k-1,J)| + |A_2| - 1)$. Now (23) holds for k unless $|H(k-1,J)| = |H|$. In this case we have necessarily $J + 2 < r_0 - 1$. By Lemma 3.4, $|H(k, J+3)| \geq |A_1| - 1 \geq (|H|-1)/2 > 0$. It follows that $\theta(k) \geq J+3$. Now we have $\sum_{0 \leq i \leq J+3} |H(k,i)| \geq (k-1)\,|\Phi_1| + |H| + |H| + 1 = k|\Phi_1|$.

The case $\beta \leq 1$.

Since $\overline{\Phi_1}$ generates $\mathbb{Z}_M$, $\overline{\Phi_1}\backslash H \neq \emptyset$ and hence $\beta = 1$. Choose v to be a minimal representative of elements of A_1.

Since $H \cup \overline{v} + H$ generates $\mathbb{Z}_M$, $\overline{v} + H$ generates $\mathbb{Z}_M/H$. In particular $t\overline{v} \notin H$, for all $1 \leq t \leq r_0 - 1$.

We have also

$$2v > M \ . \tag{25}$$

Otherwise $2v \in \Phi_1$ which would lead to $2\overline{v} + H = H$. In particular $M = 2|H|$, contradicting (17).

Let H_0 be the subgroup generated by $A_1 - \overline{v}$. By (25), A_1 is a H_0-string.

In the remaining of this proof, by $Q(i,j)$ will mean $Q(\overline{v}; i, j)$, for any subgroup Q.

We have clearly $A_0 = H(\overline{v}; 1, 0)$ and $A_1 = H_0(\overline{v}; 1, 1)$.

Let α be the smallest integer t such that $|\Phi_t| \geq M - 1$. Assuming that (iii) is not satisfied, we have

$$|A_0| \leq |H| - 1 \ . \tag{26}$$

Let $k \leq \alpha - 1$. We shall denote by $\gamma(k)$ the greatest integer $j \leq r_0 - 1$ such that $\forall\, i \leq j - 1$, $|H_0(k,i)| \geq \min(|A_0|, |H_0|)$ and $H_0(k,j)$ contains a H_0-string with size $\geq |A_1| - 1$.

Clearly for all $k \geq 1$, $\gamma(k) \geq 2$.

Using (8) we have for $0 \leq s \leq 1$,

$$H(k-1, i) + A_s \subseteq H(k, i+s) \ . \tag{27}$$

Similarly we have easily,

$$H_0(k-1, i) + A_1 \subseteq H_0(k, i+1) \ . \tag{28}$$

Set $j = \gamma(k-1)$.

$$\forall\, i \leq j-1, \quad |H(k,i)| = |H| \ . \tag{29}$$

We shall use in the sequel the relations

$$|A_0| + |A_1| \geq |H| + 1 \quad \text{ and } \quad |H_0 + A_0| = |H| \ . \tag{30}$$

The first relation is a direct consequence of (16). The second follows by Lemma 3.1, since we have using (19) and (25), $|H_0| \geq 2|A_1| - 1 \geq |A_1| + 1$.

Now (29) follows by (27) and by Lemma 3.1.

Set $\delta(k) = 1$, if $|H(k-1, j-1)| = |H|$ and $\delta(k) = 0$ otherwise. We will use the obvious inequality: $|H| - |H(k-1, j-1)| \geq 1 - \delta(k)$, without reference. We shall prove the following relation:

$$|H(k,j)| \geq |H| - 1 + \delta(k) \ . \tag{31}$$

By (7) and since $H(k-1,j)$ contains a H_0-string with size $\geq |A_1| - 1$, we have by (27), (3) and (30) $|H(k,j)| \geq |A_0 + H(k-1,j)| \geq \min(|H|, |A_0| + |A_1| - 2) = |H| - 1$.

Hence (31) follows for $\delta(k) = 0$. Assume $\delta(k) = 1$. It follows that $|H(k-1, j-1)| = |H|$. By (28), $|H(k,j)| = |H|$. It follows that $\gamma(k) \geq j+1$.

Assuming one of the following conditions:

(**W1**) $\gamma(k-1) \leq r_0 - 2$ and $|H_0| \geq |H_0(k-1,j)| + |A_1| - 1$.

(**W2**) $\gamma(k-1) \leq r_0 - 3$.

We shall prove by induction the following relation:

$$\sum_{0 \leq i \leq \gamma(k)-1} |H(k,i)| + |H_0(k, \gamma(k))| \geq k|\Phi_1| \ . \tag{32}$$

Notice that the validity of (W1) (resp. (W2)) implies its validity for $k-1$ replacing k.

Condition (32) holds clearly if $k = 1$. Consider first the case where (W1) is satisfied.

By (28) and by (7), $|H_0(k, j+1)| \geq |H_0(k-1, j) + A_1| \geq \min(|H_0|, |H_0(k-1,j)| + |A_1| - 1)$. Therefore by (W1)

$$|H_0(k, j+1)| \geq |H_0(k-1, j)| + |A_1| - 1 \ .$$

We have clearly using (26) and (31), $|H_0(k, j+1)| + |H(k,j) \setminus H_0(k-1,j)| + |H(k, j-1) \setminus H(k-1, j-1)| \geq |H_0(k-1,j)| + |A_1| - 1 + |H| + \delta(k) - 1 - |H_0(k-1,j)| + 1 - \delta(k) = |H| + |A_1| - 1 \geq |\Phi_1|$. By adding this relation to (32), applied with $k-1$ replacing k, we get the validity of (32) for k.

Consider now the case where (W2) is satisfied and (W1) is not satisfied.

By (28) and by (7),

$$|H_0(k, j+1)| = |H_0| \ .$$

Notice that $|H_0(k-1, j)| = |H_0|$ implies $|H(k,j)| = |H|$. This follows by (30) and (27). In particular $\gamma(k) \geq J + 2$. By Lemma 3.4, $H_0(k, j+2)$ contains a H_0-string with size $\geq |A_1| - 1$. We have now using (31), (26) and the above observations

$$\begin{aligned}|H_0(k,j{+}2)| + |H_0(k,j{+}1)| + |H(k,j) \setminus H_0(k,j)| \geq \\ &\geq |A_1| - 1 + |H_0| + |H| - |H_0(k,j)| \\ &\geq |A_1| - 1 + |H| \\ &\geq |\Phi_1| \ .\end{aligned}$$

By adding this relation to (32) applied with $k-1$ replacing k, we get (32).

We shall now prove the following formula:

$$\sum_{0 \leq i \leq r_0 - 1} |H(k,i)| \geq k|\Phi_1| \ . \tag{33}$$

(33) follows immediately by (32) if one of the conditions (W1) or (W2) is satisfied. Assume the contrary. As before we put $j = \gamma(k-1)$.

We have by (31), $|H(k,j)| \geq |H| - 1$. Therefore $j \leq r_0 - 2$, since otherwise, we have $|\overline{\Phi_k}| \geq \sum_{0 \leq i \leq r_0 - 1} |H(k,i)| \geq (r_0 - 2)\,|H| + |H| - 1 = M - 1$, contradicting $k \leq \alpha - 1$.

Since (W1) and (W2) are not satisfied we have necessarily $j = r_0 - 2$ and

$$|H_0(k-1,j)| + |A_1| - 2 \geq |H_0| \ . \tag{34}$$

It follows that $|H_0(k,j+1)| \geq \min(|H_0|, |H_0(k-1,j)| + |A_1| - 1) = |H_0|$. We must have

$$H \neq H_0 \ .$$

Since otherwise, we have by (29),

$$|\overline{\Phi_k}| \geq \sum_{0 \leq i \leq r_0 - 1} |H(k,i)| \geq (r_0 - 2)\,|H| + |H| - 1 = M - 1,$$

contradicting $k \leq \alpha - 1$.

We have using (34), $|H_0| \leq |H_0(k{-}1,j)| + |A_1| - 2$. By (9), $H_0(k{-}1,j{+}1) \neq \emptyset$. It follows using (8) that $|H(k,j+1)| \geq |A_0 + H(k-1,j+1)| \geq |A_0|$.

By (25), $|A_1| \leq (|H_0|+1)/2$. It follows by (16) and (34), $(|H_0|+1)/2 + |A_0| \geq |A_1| + |A_0| = |\Phi_1| \geq |H| + 1 \geq 2|H_0| + 1$ and hence $|A_0| \geq (3|H_0| - 1)/2$.

Now we have using (29),

$$|H(k,j+1)| + |H(k,j) \setminus H_0(k,j)| \geq |A_0| + |H| - |H_0| \ .$$

Therefore we have by (25),

$$\begin{aligned}|H(k,j+1)| + |H(k,j) \setminus H_0(k,j)| &\ge |H| + (|H_0|-1)/2\\ &\ge |H| + |A_1| - 1\\ &\ge |\Phi_1| \ .\end{aligned}$$

By adding this relation to (33) applied with $k-1$ replacing k, we get (33).

Condition (i) of Theorem 4.2 follows from (33), since $\{H(k,i);\ i \le r_0-1\}$, form a partition of some subset of Φ_k. ∎

We shall use the result of Dixmier mentioned in the introduction. We shall deduce it from Theorem 4.2. A direct relatively simple proof can be obtained in 2 or 3 pages using the ideas of the last case of the proof of Theorem 4.2. Notice that for this bound we do not require the delicate Proposition 2.3, but only the easy Proposition 2.1.

Corollary 4.3 ([2]). *Let* $A \subseteq [1,M]$ *such that* $\gcd(A)=1$. *Then*

$$\Big|\Phi(A) \cap \Big[(k-1)M+1,\ kM\Big]\Big| \ge \min\Big(M,\ 1+k(|A|-1)\Big) \ . \tag{35}$$

Proof: The result holds obviously by Theorem 4.2 except possibly if Condition (iii) is satisfied. Set $M = q|H|$. Since $H \subseteq \overline{\Phi_1}$, one may see easily that $\Phi(A) \cap [1,M] = \{q, 2q, ..., M\} \cup \{M-q+r, M-2q+r, ..., (M-(|A|-|H|)q)+r\}$. The reader may check easily the validity of of (35) in this case. ∎

5 – The main density theorem

Recall the following result due to Sylvester [20]. Let $a_1, a_2 \in \mathbb{N}$ be such that $\gcd(a_1,a_2)=1$. Then

$$G(a_1,a_2) = (a_1-1)\,(a_2-1) - 1 \ . \tag{36}$$

Let us introduce few notations in order to state the main result in a concise way.

Let M be a nonnegative integer and let $3 \le n \le M$. By r, d, q will denote nonnegative integers.

We are going to define the exceptional sets with cardinality n and greatest element M having a small density.

The first member of this family is the arithmetic progression.

Set $P_{n,M,d} = \{M,\ M-d,\ ...,\ M-(n-1)d\}$. By a result of Roberts [17], $G(P_{n,M,d}) = [(M-2)/(n-1)]\,(M-(n-1)\,d)-d$. In this case we have clearly

$$G(P_{n,M,d}) \leq [(M-2)/(n-1)]\,(M-n+1)-1\ . \tag{37}$$

Moreover equality holds only if $d=1$.

We set $\mathcal{E}_{n,M,0} = \{P_{n,M,d} \mid 1 \leq d < M/2 \text{ and } \gcd(d,M)=1\}$.

Let $2 \leq q < M$ be a divisor M and $r \leq q-1$ be such that $\gcd(q,r)=1$.

We put $N_{n,M,q,r} = \{q, 2q, ..., M\} \cup \{M-q+r,\ M-2q+r,\ ...,\ 2M-qn+r\}$.

Since $\gcd(q,r)=1$ and $G(N_{n,M,q,r}) = G(q, 2M-qn+r)$, we have by (36)

$$\begin{aligned} G(N_{n,M,q,r}) &= (q-1)\,(2M-1-n\,q+r)-1 \leq \\ &\leq (q-1)\,(2M-2-(n-1)\,q)-1\ . \end{aligned} \tag{38}$$

We set $\mathcal{E}_{n,M,1} = \{N_{n,M,q,r} \mid 1 \leq r \leq q-1 \text{ and } \gcd(q,r)=1\}$.

We shall denote by $\eta(d,M)$ the unique integer in the interval $[0, d-1]$ such that $\eta(d,M) \equiv M$ modulo d.

Let $d < M/2$ be such that $\gcd(M,d)=1$. We put

$$D_{n,M,d} = \Big\{M,\ M-d,\ ...,\ M-(n-[M/d]-1)\,d\Big\} \cup \Big\{d,\ ...,\ [M/d]\,d\Big\}\ ,$$

for some $d < M/2$ which is coprime to M.

By (36) and since $G(D_{n,M,d}) = G(d,\ M-(n-1-[M/d])\,d)$,

$$G(D_{n,M,d}) = \Big(2M-\eta(d,M)-(n-1)\,d-1\Big)\,(d-1)-1\ . \tag{39}$$

We set $\mathcal{E}_{n,M,2} = \{D_{n,M,d} \mid 1 \leq d < M/2 \text{ and } \gcd(d,M)=1\}$.

It remains one exceptional family with cardinality 5.

Let $r < M/2$ and assume M even. Put $E_{5,M}(r) = \{r,\ 2r,\ M/2,\ r+M/2,\ M\}$. Clearly $G(E_{5,M}(r)) \leq (M-2)\,(M-4)/4-1$. We put

$$\mathcal{E}_{M,5,3} = \Big\{E_5(r) \mid\ 1 \leq r \leq M/2-1 \text{ and } \gcd(M,r)=1\Big\}\ .$$

We set:

$$\mathcal{F}_{n,M} = \mathcal{E}_{n,M,0} \cup \mathcal{E}_{n,M,1} \cup \mathcal{E}_{n,M,2}\ , \qquad n \neq 5\ ;$$

$$\mathcal{F}_{5,M} = \mathcal{E}_{5,M,0} \cup \mathcal{E}_{5,M,1} \cup \mathcal{E}_{5,M,2} \cup \mathcal{E}_{5,M,3}\ .$$

We use the convention $\max(\emptyset)=0$. For $0 \leq i \leq 3$, put

$$f_i(n,M) = \max\Big\{G(A);\ A \in \mathcal{E}_{n,M,i}\Big\}\ .$$

By (37),

$$f_0(n,M) = [(M-2)/(n-1)]\,(M-n+1) - 1\ . \tag{40}$$

By (38),

$$f_1(n,M) = \max\Big\{(q-1)\,(2M-2-q(n-1))-1\,;\ q \text{ divides }\ \text{properly} M\Big\}\ . \tag{41}$$

By (39),

$$f_2(n,M) = \max\Big\{\Big(M+d[M/d]-(n-1)\,d-1\Big)\,(d-1)-1\,;\ (M,d)=1\Big\}\ . \tag{42}$$

Observe that f_0, f_1, f_2, f_3 can be easily evaluted.

Our basic density result is the following one:

Theorem 5.1. *Let $A \subset [1,M]$ be such that $\gcd(A) = 1$, $|A| = n \geq 3$ and $M = \max(A)$. If $A \notin \mathcal{F}_{n,M}$, then*

$$\Big|\Phi(A) \cap \Big[(k-1)M+1,\ kM\Big]\Big| \geq \min\Big(M-1,\ k|A|\Big)\ . \tag{43}$$

Proof: Assume first $\Phi(A) \cap [1,M] \neq A$. By (35), $|\Phi(A)\cap[(k-1)M+1,\ kM]| \geq \min(M,\ k|A|+1)$. In this case (43) holds. We may then assume

$$\Phi(A) \cap [1,M] = A\ .$$

(43) holds clearly if Condition (i) of Theorem 4.2 is satisfied. Suppose the contrary. In particular $1 \notin A$. By Theorem 4.2, we have one of the following possibilities:

(**P1**). $\overline{A}$ is an arithmetic progression of $\mathbb{Z}_M$. Let $d \in \mathbb{N}$ be such that $d < M/2$ and $\overline{d}$ is a difference of the progression. Observe that such a d exists, since we may reverse the progression. On the other side $\gcd(M,d) = 1$, since $\overline{d}$ generates $\mathbb{Z}_M$ and hence $d \neq M/2$. Let $m \in A$ be such that $\overline{m}$ is the first element of the progression.

Put $M = M'd + r_1$, where $[M/d] = M'$. Since $\overline{d}$ generates $\mathbb{Z}_M$, we have $\gcd(M,d) = 1$. Let $T_0 = A \cap [1, d-1]$ and $T = \{d\} \cup T_0$. We shall denote the canonical morphism from $\mathbb{Z}$ onto $\mathbb{Z}_d$ by ϕ. Let us show that

$$\phi(T) + \phi(T) \subseteq \phi(T) \cup \{\phi(m)\}\ . \tag{44}$$

Since $\phi(d) = 0$, it would be enough to prove $\phi(T_0) + \phi(T_0) \subseteq \phi(T) \cup \{\phi(m)\}$.

Let $x_1, x_2 \in T_0$. We have $x_1 + x_2 \in \Phi_1$, since $d < M/2$. It follows that either $x_1 + x_2 \in T \cup \{m\}$ or $x_1 + x_2 - d \in T$. It follows that $\phi(x_1+x_2) \in \phi(T \cup \{m\})$.

Let us prove that $|T_0| \neq 1$. Suppose on the contrary $T_0 = \{r_2\}$. The ordering induced by the arithmetic progression modulo M, on $[1, M]$ is the following:

$$..., r_1, r_1 + d, ..., M - d, M, d, ..., M'd, d - r_1, ...$$

It follows that $r_2 \in \{r_1, d - r_1\}$. In both cases $\gcd(r_2, d) = 1$, since $\gcd(A) = 1$.

Now we must have $2r_2 > d$, since otherwise $2r_2 \in T_0$, contradicting the hypothesis $|T_0| = 1$. It follows since $2r_2 - d \neq r_2$, that $2\,\overline{r}_2$ is the first element in the progression. We can not have $2r_2 + d > M$ since otherwise $2r_2 + d - M = r_2$, contradicting $d < M/2$. It follows that $M \geq 2r_2 + d > 3r_2$. Now $2r_2 \notin \{3r_2 - d,$ $3r_2 - 2d\}$. It follows that $r_2 \in \{3r_2 - d, 3r_2 - 2d\}$, contradicting $\gcd(d, r_2) = 1$ and $r_2 \neq 1$.

Assume first $T_0 \neq \emptyset$. We have $|T| \geq 3$. If M is not the end of the progression, its next $d - r_1 \in T$. But this element generates $\mathbb{Z}_d$. If M is the end of the progression and since $|T| > 1$, we must have $M - M'd = r_1 \in T$. In both cases $\phi(T)$ contains a generator of $\mathbb{Z}_d$. By (44), the subgroup generated by $\phi(T)$ is contained in $\phi(T) \cup \{\phi(m)\}$.

Therefore $\mathbb{Z}_d \subseteq \phi(T) \cup \{\phi(m)\}$.

It follows that $1 \in T \cup \{m - d\}$, and since $1 \notin A$, $m = d + 1$. On the other side $2, 3, ..., d-1 \in T$. Unless $d = 3$, we have $G(A) = 1$ and (43) holds clearly. Therefore we may assume $d = 3$, $m = 4$ and $T_0 = \{2\}$. For $a \leq 5$, the result is obvious. In the other case we have $6 \in A$ and hence $3 \in A$. Now $\{2, 3\} \subseteq A$. Hence $G(A) = 1$. Clearly (43) holds in this case.

We may now assume $T_0 = \emptyset$. Clearly $A \supseteq \{M, M - d, ..., M - jd\}$, for some $0 \leq j$.

If $d \in A$, we must have since $\Phi_1 = A$, $A = \{M - jd,\ M - (j-1)d,\ ...,\ M - d,\ M,$ $d,\ 2d,\ ...,\ M'd\}$. It follows that $A = D_{n,M,d}$.

If $d \notin A$, we must have

$$A = \Big\{M,\ M - d,\ ...,\ M - (n-1)\,d\Big\} = P_{n,M,d}\ .$$

(**P2**). Condition (iii) of Theorem 4.2 holds. Clearly there exists a proper divisor q of M and $r \leq q - 1$ such that

$$\{q,\ 2q,\ ...,\ M\} \subseteq A \subseteq \{q,\ 2q,\ ...,\ M\} \cup \{M - q + r,\ M - 2q + r,\ ...,\ r\}\ .$$

Since $A = \Phi_1$ and $q \in A$, we must have $q + x \in A$, for all $x \in A \cap [1, M - q]$. This condition forces the following equality:

$$A = \{q,\ 2q,\ ...,\ M\} \cup \{M - q + r,\ M - 2q + r,\ ...,\ 2M - qn + r\} = N_{n,M,q,r}\ .$$

(**P3**) Condition (iv) of Theorem 4.2 holds. In particular $A = \{r,\, M/2,\, 2r,\, M/2+r,\, M\} = E_{5,M,3}$. ■

6 – The Frobenius number

Let us introduce the following notations.

$$\mathcal{S}_{n,M} = \Big\{A\colon\ |A| = n \ \ \&\ \ \max(A) \le M \ \ \&\ \ \gcd(A) = 1\Big\}\ .$$

$$\mathcal{T}_{n,M} = \Big\{A\colon\ |A| = n \ \ \&\ \ \max(A) = M \ \ \&\ \ \gcd(A) = 1\Big\}\ .$$

The best possible bound for $G(A)$, assuming $A \in \mathcal{S}_{n,M}$ is measured by the extremal function $g(n,M)$, defined by Erdös and Graham as:

$$g(n,M) = \max\Big\{G(A)\colon\ A \in \mathcal{S}_{n,M}\Big\}\ .$$

We shall study the related function:

$$f(n,M) = \max\Big\{G(A)\colon\ A \in \mathcal{T}_{n,M}\Big\}\ .$$

Clearly $f(n,M)$ determines $g(n,M)$. We will consider only $f(n,M)$, in order to limit the size of the present paper. The reader may certainly deduce the corresponding results for $g(n,M)$.

We shall denote by $\zeta(n,M)$ the unique integer $t \in [1,n]$ such that $M+t \equiv 0$ modulo n.

Theorem 6.1. *Let $A \subset [1,M]$ be such that $\gcd(A) = 1$ and $6 \le 2|A| \le \max(A)$. Set $n = |A|$, $M = \max(A)$. If $A \notin \mathcal{F}_{n,M}$, then*

$$G(A) \le \Big((M+\zeta(n,M))/n - 1\Big)\,\Big(M - \zeta(n,M)\Big) - 1\ . \tag{45}$$

In particular

$$G(A) \le (M-n/2)^2/n - 1\ . \tag{46}$$

Proof: Put $\zeta(n,M) = t$ and set $M+t = sn$. Set $\Phi = \Phi(A)$ and $\Phi_i = \Phi_i(A)$. Suppose $A \notin \mathcal{F}_{n,M}$. By (43), for all $i \le s-1$, $|\Phi_i| \ge in$.

Therefore $|\Phi \cap [1, M(s-1)]| \ge \sum_{1\le i\le s-1} in = s(s-1)n/2 = (s-1)(M+t)/2$.

It follows that

$$\Big|\Phi \cap \Big[1,\, M(s-1) - t(s-1) + 1\Big]\Big| \ge (s-1)(M+t)/2 - (s-1)\,t + 1\ .$$

It follows by Lemma 3.2 that $G(A) \leq (s-1)\,(M-t) - 1 = ((M+t)/n - 1) \cdot (M-t) - 1$. ∎

Theorem 6.1 allows to get in the major case best possible bounds for $G(A)$ and even the uniqueness of the examples reaching the bound. We shall study quickly the question omitting some of the details.

Assuming that $M-2$ has a not big residue modulo $n-1$ compared to M/n, one obtain the following sharp estimate for $G(A)$.

Theorem 6.2. *Set $M-2 = s(n-1)+r$, where $0 \leq r \leq n-2$. Suppose $r \leq s-2$. Then $G(A) < f_0(n,M)$ for all $A \in \mathcal{T}_{n,M} \backslash \mathcal{F}_{n,M}$.*
In particular $f(n,M) = \max\{f_i(n,M);\ 0 \leq i \leq 3\}$.

Proof: Take $A \in \mathcal{T}_{n,M} \backslash \mathcal{F}_{n,M}$.
Assume first $s-r-2 = 0$. We have $M+n = (s+1)\,n$.
By (45), we have

$$f_0(n,M) - G(A) \geq s\,(M-n+1) - s\,(M-n) > 0\ .$$

Assume $1 \leq s-r-2$. Set $s-r-2 = jn+t'$, where $1 \leq t' \leq n$.
We have $\zeta = t'$. Clearly $M+t' = (s-j)\,n$.
By (45), we have

$$f_0(n,M) - G(A) \geq s\,(M-n+1) - (s-j-1)\,(M-t') > 0\ .$$ ∎

Corollary 6.3. *Suppose $M \geq n(n-1)+2$. Then $f(n,M) = \max\{f_i(n,M);\ 0 \leq i \leq 3\}$. Moreover $G(A) < f(n,M)$ for all $A \in \mathcal{T}_{n,M} \backslash \mathcal{F}_{n,M}$.*

Proof: Take $A \in \mathcal{T}_{n,M} \backslash \mathcal{F}_{n,M}$.
Set $M-2 = s(n-1)+r$, where $0 \leq r \leq n-2$. We have $r \leq s-2$, since otherwise $M-2 \leq (n-1)^2 + n - 2$, a contradiction. By Theorem 6.2, we have $f_0(n,M) < G(A)$. ∎

The above corollary could hold for all values of n and M. In order to prove such a result one needs to examine the fatorisation of M, in order to be able to use f_1 and f_2.

A conjecture of Lewin [14], proved by Dixmier in [2] states that for every $A \in \mathcal{T}_{n,t(n-1)}$, $G(A) \leq G(N_{n,t(n-1),t,t-1})$. We obtain the following result:

Theorem 6.4. *Let $n \geq 6$ and let $3 \leq t$. Put $M = t(n-1)$. Then for every $A \in \mathcal{T}_{n,M} \backslash N_{n,M,t,t-1}$, $G(A) < G(N_{n,M,t,t-1})$.*

Proof: By (38), $G(N_{n,M,t,t-1}) = (t-1)(M-2) - 1$. Consider the following cases:

Case 1. $A \in \mathcal{E}_{n,M,0}$. By (37), $G(A) \leq f_0(n,M) = [(M-2)/(n-1)] \cdot (M-n+1) - 1 \leq (t-1)(M-n+1) - 1 < G(N_{n,M,t,t-1})$.

Case 2. $A \notin \mathcal{F}_{n,M}$. Assume first $t \leq n$. We have $\zeta(n,M) = t$. Since $t \geq 3$ and by (45), $G(A) \leq (t-1)(M-t) - 1 < G(N_{n,M,t,t-1})$. We may now suppose $t \geq n+1$. In particular $M \geq (n-1)(n+1) \geq n(n-1) + 2$. By Corollary 6.3, $G(A) < f_0(n,M) < G(N_{n,M,t,t-1})$, using Case 1.

Case 3. $A \in \mathcal{E}_{n,M,1}$, say $A = N_{n,M,q,r}$, where $q \neq t$ is a proper divisor of M. By (41), $G(A) \leq (q-1)(2M - 2 - q(n-1)) - 1$. However the quadratic expression achieves its maximal value $G(N_{n,M,t,t-1})$ with q integer uniquely at $q = t$. Now $G(A) < G(N_{n,M,t,t-1})$, since $A \neq N_{n,M,t,t-1}$.

Case 4. $A \in \mathcal{E}_{n,M,2}$, say $A = D_{n,M,d}$, where $\gcd(d,M) = 1$. By (39), $G(A) \leq (d-1)(2M - 1 - \eta(d,M) - d(n-1)) - 1 \leq (d-1)(2M - 2 - d(n-1)) - 1$, for some $d \neq t$. However the quadratic expression can not achieve its maximal value $G(N_{n,M,t,t-1})$ with d integer for $d \neq t$. Since $\gcd(t,M) \neq 1$, we have $G(A) < G(N_{n,M,t,t-1})$. ∎

A similar argument shows that there is exactly one $A \neq N_{5,M,t,t-1}$ with $G(A) = G(N_{5,M,t,t-1})$, namely $A = \{2t-1, 2t, 4t-2, 4t-1, 4t\}$, where $n = 5$.

Let t be an integer with $2 \leq t$. A conjecture of Lewin [14], proved by Dixmier in [2] states that for every $A \in \mathcal{T}_{n,t(n-1)+1}$, $G(A) \leq G(D_{n,t(n-1)+1,t})$. We obtain the following result:

Theorem 6.5. *Let $n \geq 6$ and let $3 \leq t$. Put $M = 1 + t(n-1)$. Then for every $A \in \mathcal{T}_{n,M} \backslash D_{n,M,t}$, one of the following conditions holds:*

(i) $G(A) < G(D_{n,M,t})$.

(ii) $M \equiv 0 \bmod t+1$ *and* $A = N_{n,M,(t+1),t}$.

(iii) $M \equiv 1 \bmod t+1$ *and* $A = D_{n,M,(t+1),t}$.

Proof: By (39), $G(D_{n,M,t}) = (t-1)(M-1) - 1$. Consider the following cases:

Case 1. $A \in \mathcal{E}_{n,M,0}$. By (37), $G(A) \le f_0(n,M) = [(M-2)/(n-1)] \cdot (M-n+1) - 1 \le (t-1)\,(M-n+1) - 1 < G(D_{n,M,t})$.

Case 2. $A \notin \mathcal{F}_{n,M}$. Assume first $t \le n+1$. We have $\zeta(n,M) = t-1$. By (45), $G(A) \le (t-1)\,(M-t) - 1 \le (t-1)\,(M-t+1) - 1 < G(D_{n,M,t})$. We may now suppose $t \ge n+2$. In particular $M \ge (n-1)\,(n+2) + 1 \ge n(n-1) + 2$. By Corollary 6.3, $G(A) < f_0(n,M) < G(D_{n,M,t})$, using Case 1.

Case 3. $A \in \mathcal{E}_{n,M,1}$, say $A = N_{n,M,q,r}$, where q is a proper divisor of M. By (41), $G(A) \le (q-1)\,(2M-2-q(n-1))-1$. However the quadratic expression achieves its maximal value $G(D_{n,M,t})$ with q integer, for $q=t$ or $q=t+1$. But t is coprime with M. It follows that $G(A) < G(D_{n,M,t})$, except for $A = N_{n,M,t+1,t}$, when $t+1 \equiv 0$ modulo M.

Case 4. $A \in \mathcal{E}_{n,M,2}$, say $A = D_{n,M,d}$, where $\gcd(d,M) = 1$. By (39), $G(A) \le (d-1)\,(2M-1-\eta(d,M)-d(n-1)) - 1(d-1)\,(2M-2-d(n-1)) - 1$, for some $d \ne t$. However the expression achieves its maximal value $G(D_{n,M,t})$ with d integer, for $d=t$ or $d=t+1$. The first value corresponds to $A = D_{n,M,t}$. Consider the possibility $d = t+1$. It follows that that $d+1$ is coprime with M and $\eta(d+1,M) = 1$. It follows that $G(A) < G(D_{n,M,t})$, except for $A = D_{n,M,t+1}$, where $M \equiv 1$ modulo $t+1$. ∎

Dixmier proved in [2] that for every $A \in \mathcal{T}_{n,t(n-1)+2}$, $G(A) \le G(P_{n,M,1})$. We obtain the following result.

Theorem 6.6. *Let $n \ge 6$ and let $2 \le t$. Put $M = 2 + t(n-1)$. Then for every $A \in \mathcal{T}_{n,M} \backslash P_{n,M,1}$, one of the following conditions holds.*

(**i**) $G(A) < G(P_{n,M,1})$.

(**ii**) $M \equiv 0 \bmod 1+t$ *and* $A = N_{n,M,(t+1),t}$.

(**iii**) $M \equiv 1 \bmod 1+t$ *and* $A = D_{n,M,t+1}$.

Proof: By (37), $G(P_{n,M,1}) = (M-2)(M-n+1)/(n-1)-1 = t(M-n+1)-1$. Consider the following cases:

Case 1. $A \notin \mathcal{F}_{n,M}$. By Theorem 6.2, $G(A) < G(P_{n,M,1}) = t(M-n+1)-1$.

Case 2. $A \in \mathcal{E}_{n,M,0} \backslash P_{n,M,1}$. By (37), $G(A) < G(P_{n,M,1})$.

Case 3. $A \in \mathcal{E}_{n,M,1}$, say $A = N_{n,M,q,r}$, where q is a proper divisor of M. By (41), $G(A) \le (q-1)\,(2M-2-q(n-1)) - 1$. However the quadratic expression achieves its maximal value for an integer q at $q = t+1$. It follows that $G(A) < G(P_{n,M,1})$, unless $q = t+1$ and $r = t$, which leads to $A = N_{n,M,t+1,t}$.

Case 4. $A \in \mathcal{E}_{n,M,2}$, say $A = D_{n,M,d}$, where $\gcd(d,M) = 1$. By (39), $G(A) \le (d-1)\,(2M - \eta(d,M) - 1 - d(n-1)) - 1 \le (d-1)\,(2M - 2 - d(n-1)) - 1$. However the above expression achieves its maximal value for an integer d unless $d = t+1$. It follows that $G(A) < G(P_{n,M,1})$, unless $A = D_{n,M,t+1}$ and $M \equiv 1 \mod t+1$. ∎

REFERENCES

[1] Brauer, A. – *On a problem of partitions,* Amer J. of Math., 76 (1954), 343–346.

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

[3] Djawadi, M. and Hofmeister, G. – Linear diophantine problems, *Arch. Math.,* 66 (1996), 19–29.

[4] Erdös, P. and Graham, R.L. – On a linear diophantine problem of Frobenius, *Acta Arith.,* 21 (1972), 399–408.

[5] Halberstam, H. and Roth, K.F. – *Sequences*, Springer-Verlag, 1982.

[6] Hamidoune, Y.O. – Quelques problèmes de connexité dans les graphes orientés, *J. Comb. Theory B,* 30 (1981), 1–10.

[7] Hamidoune, Y.O. – On the connectivity of Cayley digraphs, *Europ. J. Combinatorics,* 5 (1984), 309–312.

[8] Hamidoune, Y.O. – On subsets with a small sum in abelian groups' I: The Vosper property, *Europ. J. of Combinatorics,* 18 (1997), 541–556.

[9] Hamidoune, Y.O. – Subsets with a small product in groups, *Astérique*, to appear.

[10] Hamidoune, Y.O. – An isoperimetric method in Additive Theory, *J. Algebra,* 179 (1996), 622–630.

[11] Hamidoune, Y.O. – *An isoperimetric method II: Inverse Additive Theory*, In preparation.

[12] Hofmeister, G. – Linear diophantine problems, *Bull. Iranian Math. Soc.,* 8 (1981), 121–155.

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

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

[15] Mann, H.B. – *Addition Theorems: The Addition Theorems of Group Theory and Number Theory*, Interscience, New York, 1965.

[16] Olson, J.E. – On the sum of two sets in a group, *J. Number Theory,* 18 (1984), 110–120.

[17] Roberts, J.B. – Note on linear forms, *Proc. Amer Math. Soc.,* 7 (1956), 465–469.

[18] Rödseth, Ö.J. – Two remarks on linear forms in non-negative integers, *Math. Scand.,* 51 (1982), 193–198.

[19] Selmer, E.S. – On the linear diophantine problem of Frobenius, *J. Reine Angew. Math.,* 293/294 (1977), 1–17.

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

[21] VITEK, Y. – Bounds for a linear diophantine problem of Frobenius, II, *Canad. J. of Math.*, 28 (1976), 1280–1288.

Y.O. Hamidoune
Université Pierre et Marie Curie, E. Combinatoire, CASE 189,
4 Place Jussieu, 75005 Paris – FRANCE