Astérisque

ANDRÁS SÁRKŐZY

On finite addition theorems

Astérisque, tome 258 (1999), p. 109-127
<http://www.numdam.org/item?id=AST_1999__258__109_0>

© Société mathématique de France, 1999, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM
Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Astérisque **258**, 1999, p. 109–127

ON FINITE ADDITION THEOREMS

by

András Sárkőzy

Abstract. — If a finite set A of integers included in $\{1,\dots,N\}$ has more than N/k elements, one may expect that the set ℓA of sums of ℓ elements of A, contains, when ℓ is comparable to k, a rather long arithmetic progression (which can be required to be homogeneous or not). After presenting the state of the art, we show that some of the results cannot be improved as far as it would be thought possible in view of the known results in the infinite case. The paper ends with lower and upper bounds for the order, as asymptotic bases, of the subsequences of the primes which have a positive relative density.

1. Throughout this paper we use the following notations: $c_1, c_2 \dots$ denote positive absolute constants. If $f(n) = O(g(n))$, then we write $f(n) \ll g(n)$. The cardinality of the finite set S is denoted by $|S|$. The set of the integers, non-negative integers, resp. positive integers is denoted by $\mathbb{Z}$, $\mathbb{N}_0$ and $\mathbb{N}$. $\mathcal{A}$, $\mathcal{B}$ ... denote (finite or infinite) subsets of $\mathbb{N}_0$, and the counting functions of their positive parts are denoted by $A(n)$, $B(n)$, ..., so that, *e.g.*, $A(n) = |\mathcal{A} \cap \{1, 2, \dots n\}|$. The Schnirelmann density of the set $\mathcal{A} \subset \mathbb{N}_0$ is denoted by $\sigma(\mathcal{A})$, while the asymptotic density, asymptotic lower density, resp. asymptotic upper density of it is denoted by $d(\mathcal{A})$, $\underline{d}(\mathcal{A})$ and $\overline{d}(\mathcal{A})$ (see [16] for the definition of these density concepts). $\mathcal{A}_1 + \mathcal{A}_2 + \dots + \mathcal{A}_k$ denotes the set of the integers that can be represented in the form $a_1 + a_2 + \dots + a_k$ with $a_1 \in \mathcal{A}_1$, $a_2 \in \mathcal{A}_2$, ..., $a_k \in \mathcal{A}_k$; in particular, we write

$$\mathcal{A} + \mathcal{A} = 2\mathcal{A} = S(\mathcal{A}),$$

$$k\mathcal{A} = \mathcal{A} + (k-1)\mathcal{A} \quad \text{for} \quad k = 3, 4, \dots,$$

and

$$0\mathcal{A} = \{0\}, \quad 1\mathcal{A} = \mathcal{A}.$$

1991 ***Mathematics Subject Classification.*** — 11B13, 11B25, 11B05.

Key words and phrases. — additive number theory, density, additive bases, structure theory of set addition.

Research partially supported by Hungarian National Foundation for Scientific Research, Grant No. 1811.

© Astérisque 258, SMF 1999

If $\mathcal{A} \subset \mathbb{N}$ then $\mathcal{P}(\mathcal{A})$ denotes the set of the distinct positive integers n that can be represented in the form $n = \sum_{a \in \mathcal{A}} \varepsilon_a a$ where $\varepsilon_a = 0$ or 1 for all a and, if $\mathcal{A}$ is infinite, then all but finitely many of the ε's are equal to 0. (This notation will be used only in Section 3, while later the letter $\mathcal{P}$ will be reserved for denoting sets of primes.) An arithmetic progression is said to be *homogeneous* if it consists of the consecutive multiples of a non-zero number, i.e., it is of the form $kd, (k+1)d, \ldots, \ell d$ (where $d \neq 0$).

2. The classical Schnirelmann-Mann-Kneser-Folkman theory of the set addition studies sums of *infinite* sets (the density and, in case of Kneser's theorem, the structure of the sum set). However, in many applications we are dealing with *finite* sets; in such a case, we cannot use this classical set addition theory or, in the best case, we have difficulties in applying it. Thus recently I have worked out a theory of addition of *finite* sets (partly jointly with Erdős, resp. Nathanson) which is more or less analogous to the case of infinite sets, and several conclusions and applications of this theory are close to the ones obtained by Freiman using a completely different approach. A considerable part of this work was inspired by a paper of Erdős and Freiman [5]. In this paper, first I will give a brief survey of my papers written on this subject. In the second half of the paper two further related problems will be studied.

3. Nathanson and I [20] proved that if we take "many" integers up to N, and we add the set obtained in this way sufficiently many times, then the sum set contains a long arithmetic progression:

Theorem 1. — *If $N \in \mathbb{N}$, $k \in \mathbb{N}$, $\mathcal{A} \subset \{1, 2, \ldots, N\}$ and*

$$|\mathcal{A}| \geq \frac{N}{k} + 1, \tag{3.1}$$

then there exists an integer d with

$$1 \leq d \leq k - 1 \tag{3.2}$$

such that if h and z are any positive integers satisfying the inequality

$$\frac{N}{h} + zd \leq |\mathcal{A}|,$$

then the sum set $(2h)\mathcal{A}$ contains an arithmetic progression with z terms and difference d.

Choosing here $h = 2k$ and $z = [N/2kd]$, we obtain

Corollary 1. — *If $N \in \mathbb{N}$, $k \in \mathbb{N}$, $\mathcal{A} \subset \{1, 2, \ldots, N\}$ and $\mathcal{A}$ satisfies (3.1), then there exists an integer d satisfying (3.2) such that $4k\mathcal{A}$ contains an arithmetic progression with difference d and length $[N/2kd] \geq [N/2(k-1)k]$.*

The proof of Theorem 1 was based on Dyson's theorem [3] (which slightly generalizes Mann's theorem [19]). We used Theorem 1 to study a problem of Erdős and Freud on the solvability of the equation

$$a_1 + a_2 + \cdots + a_x = 2^y, \quad a_1, a_2, \ldots, a_x \in \mathcal{A} \tag{3.3}$$

in "large" subsets $\mathcal{A}$ of $\{1, 2, \ldots, N\}$ (in sets $\mathcal{A}$ with $|\mathcal{A}| > [N/3]$). Indeed, we improved on a result of Erdős and Freiman [5]. Later Freiman [14] found another ingenious approach and he improved further on the result.

Corollary 1 was sufficient to study equation (3.3), however, it is not sharp in the sense that it guarantees an arithmetic progression of length only $\gg N/k^2$ in the sum set while one would expect a longer arithmetic progression and, indeed, later I needed a sharper result of this type. In fact, I proved [21] that having the same assumptions as in Corollary 1, one can guarantee a much longer *homogeneous* arithmetic progression in a sum set $\ell\mathcal{A}$ with $\ell \ll k$ (in many applications, we need the existence of a *homogeneous* arithmetic progression in the sum set, and this fact causes certain difficulties):

Theorem 2. — *If $N \in \mathbb{N}$, $k \in \mathbb{N}$, $\mathcal{A} \subset \{1, 2, \ldots, N\}$ and (3.1) holds, then there are integers d, ℓ, m such that (3.2) holds, moreover we have*

$$1 \leq \ell < 118k \tag{3.4}$$

and

$$\{(m+1)d, (m+2)d, \ldots, (m+N)d\} \subset \ell\mathcal{A}. \tag{3.5}$$

It is easy to see that this theorem is the best possible apart from the constant factor 118 in (3.4). This result can be considered as the finite analog of Kneser's theorem [18] (see Lemma 2 below). The proof of Theorem 2 is complicated, it uses both Dyson's theorem and Kneser's theorem.

One might like to sharpen this result by showing that all the elements of the arithmetic progression in (3.5) can be represented as the sum of possibly few *distinct* elements of $\mathcal{A}$; see [20] and Alon [1] for results of this type. The case when the number of distinct summands is unlimited will be studied later (Theorem 4 below).

Before the famous $\alpha + \beta$ conjecture was proved by Mann [19], Khintchin [17] had settled that most important special case of the conjecture when sum sets of the form $k\mathcal{A}$ are considered; indeed, he proved that

$$\sigma(k\mathcal{A}) \geq \min(1, k\sigma(\mathcal{A})). \tag{3.6}$$

In [23] I proved the following finite analog of this result:

Theorem 3. — *If $N \in \mathbb{N}$, $k \in \mathbb{N}$, $\mathcal{A} \subset \{1, 2, \ldots, N\}$ and $|\mathcal{A}| \geq 2$, then there are m, d such that $m \in \mathbb{Z}, d \in \mathbb{N}$,*

$$d < 2\frac{N}{|\mathcal{A}|} \tag{3.7}$$

and

$$|\{m+d, m+2d, \ldots, m+Nd\} \cap k\mathcal{A}| \geq \left(\min(1, \frac{1}{800}k\frac{|\mathcal{A}|}{N})\right) N. \tag{3.8}$$

The proof is similar to the proof of Theorem 2, although also further ideas are needed. Again, it is easy to see that this theorem is the best possible apart from the constants 2 in (3.7) and, mostly, $\frac{1}{800}$ in (3.8) (we will return to this question in

section 4). Note that an easy consideration shows that here we have to give up the requirement that the arithmetic progression in (3.8) should be homogeneous.

An infinite set $\mathcal{A} \subset \mathbb{N}$ is said to be *subcomplete* if it contains an infinite arithmetic progression. Improving on a result of Erdős [4], Folkman [11] proved the following remarkable theorem: if $\mathcal{A} \subset \mathbb{N}$ is an infinite set such that there are $\varepsilon > 0$ and N_0 with

$$A(N) > N^{1/2+\varepsilon} \text{ for } N > N_0,$$

then $\mathcal{P}(\mathcal{A})$ is subcomplete. Improving on a result of Alon and Freiman [2], I proved [22] the following finite analogue of Folkman's theorem:

Theorem 4. — *If $N \in \mathbb{N}$, $N > 2500$, $\mathcal{A} \subset \{1, 2, \ldots, N\}$ and*

$$|\mathcal{A}| > 200(N \log N)^{1/2}, \tag{3.9}$$

then there are integers d, y, z such that

$$\begin{aligned} 1 \le d &< 10^4 \frac{N}{|\mathcal{A}|}, \\ z &> 7^{-1} 10^{-4} |\mathcal{A}|^2, \\ y &< 7 \cdot 10^4 N z |\mathcal{A}|^{-2} \end{aligned} \tag{3.10}$$

and

$$\{yd, (y+1)d, \ldots, zd\} \subset \mathcal{P}(\mathcal{A}).$$

Previously Alon and Freiman had proved a similar result with $N^{2/3+\varepsilon}$ on the right hand side of (3.9) and a slightly weaker inequality in place of (3.10). Moreover, independently and nearly simultaneously Freiman [13] proved a result essentially equivalent to Theorem 4 above. I derived Theorem 4 from Theorem 2; this part of the proof is easier, than the proof of Theorem 2. Freiman's proof is also complicated; he combines methods from the geometry of numbers and exponential sums in the manner of his book [12].

Again, Theorem 4 is the best possible apart from the constant factors and, perhaps, the factor $(\log N)^{1/2}$ on the right hand side of (3.9). Probably this logarithmic factor (or, at least, some of it) is unnecessary, although it is quite interesting and unexpected that exactly the same factor appears also in Freiman's result (obtained by a completely different method).

Theorem 4 has many applications. Alon and Freiman [2] found the first applications of a result of this type. Several further applications are discussed in my paper [22]. Papers [6], [7], [8] and [10] contain further applications.

Erdős and I [9] studied the following problem: what happens, if we replace assumption (3.9) by a slightly weaker one so that $|\mathcal{A}|$ drops below $N^{1/2}$? It turns out that there is a sharp drop in the length of the maximal arithmetic progression that we can guarantee in $\mathcal{P}(\mathcal{A})$, however, still it must contain quite a long one. Indeed, let $u = F(N, t)$ denote the greatest integer u such that for every $\mathcal{A} \subset \{1, 2, \ldots, N\}$ with $|\mathcal{A}| = t$, the set $\mathcal{P}(\mathcal{A})$ contains u consecutive multiples of a positive integer d:

$$\{(x+1)d, (x+2)d, \ldots, (x+u)d\} \subset \mathcal{P}(\mathcal{A})$$

for some x and d, and let $v = G(n,t)$ denote the greatest integer v such that for every $\mathcal{A} \subset \{1,2,\dots,N\}$ with $|\mathcal{A}| = t$, the set $\mathcal{P}(\mathcal{A})$ contains an arithmetic progression of length v:

$$\{y + (z+1)d, y + (z+2)d, \dots, y + (z+v)d\} \subset \mathcal{P}(\mathcal{A})$$

for some y, z and $d(> 0)$. Clearly, $F(N,t) \le G(N,t)$ for all N and $t \le N$, and since

$$\mathcal{P}(\{1,2,\dots,t\}) = \{1,2,\dots,t(t+1)/2\} \subset \{1,2,\dots,t^2\},$$

thus we have

$$(F(N,t) \le) G(N,t) \le t^2$$

for all N and $t \le N$. On the other hand, by Theorem 4 for $t \gg (N \log N)^{1/2}$ we have

$$\begin{aligned} F(N,t) &> z - y > z - 7.10^4 N z |\mathcal{A}|^{-2} \\ &= z(1 - 7.10^4 N |\mathcal{A}|^{-2}) \gg z \gg |\mathcal{A}|^2 = t^2 \end{aligned}$$

if $t \gg (N \log N)^{1/2}$.

Theorem 5. — *If $N \ge N_0$ and $18(\log N)^2 < t \le N$, then we have*

$$(G(N,t) \ge) F(N,t) > \frac{1}{18} \frac{t}{(\log N)^2}.$$

Theorem 6

(i) If $N > N_0$ and $c \log N < t < \frac{1}{3} N^{1/3}$, then we have

$$F(N,t) < 16 \frac{t}{\log N} \log\left(\frac{t}{\log N}\right).$$

(ii) If $\varepsilon > O$ and $t_0(\varepsilon) < t < (1-\varepsilon)N^{1/2}$, then we have $F(N,t) < (1+\varepsilon)t$.

Theorem 7

(i) If $N > N_0$ and $\exp(2(\log N)^{1/2}) < t < N^{1/4}$, then we have

$$G(N,t) < t \exp\left(4 \max\left(\frac{\log N}{\log t}, \frac{(\log t)^2}{\log N}\right)\right).$$

(ii) $t_0 < t < \frac{1}{2} N^{1/2}$ we have $G(N,t) < 2t^{3/2}$.

Paper [9] contains several further related results.

4. As we mentioned above, Theorem 4 is nearly sharp in the sense that apart from the constant factors and the, perhaps, unnecessary factor $(\log N)^{1/2}$ on the right hand side of (3.9), the theorem is the best possible.

On the other hand, it is easy to see that the other two main theorems Theorem 2 and 3 are the best possible apart from the constants on the right hand side of (3.4) and (3.8) (and, less importantly, (3.7)). One might like to determine or, at least, to estimate these constants. This problem can be considered as the finite analog of the famous $\alpha + \beta$ problem (apart from the fact that here we restrict ourselves to sum sets $\mathcal{A}_1 + \mathcal{A}_2 + \dots + \mathcal{A}_k$ with $\mathcal{A}_1 = \mathcal{A}_2 = \dots = \mathcal{A}_k$). Since Theorems 2 and 3 are closely related, thus here I will study only the constant in Theorem 3.

If $N \in \mathbb{N}$, $k \in \mathbb{N}$, $\mathcal{A} \subset \{1, 2, \ldots, N\}$ and $|\mathcal{A}| \geq 2$, then let $E(N, k, \mathcal{A})$ denote the maximal number of elements of $k\mathcal{A}$ contained in an arithmetic progression of length N:

$$E(N, k, \mathcal{A}) = \max_{m \in \mathbb{Z}, d \in \mathbb{N}} |\{m + d, m + 2d, \ldots, m + Nd\} \cap k\mathcal{A}|.$$

For $k \in \mathbb{N}$, $k \geq 2$ let $C(k)$ denote the greatest number such that for all $N \in \mathbb{N}$, $\mathcal{A} \subset \{1, 2, \ldots, N\}$ and $|\mathcal{A}| \geq 2$ we have

$$E(N, k, \mathcal{A}) \geq \left(\min(1, C(k)k\frac{|\mathcal{A}|}{N})\right) N,$$

and define C by $C = \inf_{k=2,3,\ldots} C(k)$ so that C is the greatest number such that for all $N \in \mathbb{N}$, $k \in \mathbb{N}$, $k \geq 2$, $\mathcal{A} \subset \{1, 2, \ldots, N\}$ and $|\mathcal{A}| \geq 2$ we have

$$E(N, k, \mathcal{A}) \geq \left(\min(1, Ck\frac{|\mathcal{A}|}{N})\right) N.$$

Moreover, for $k \in \mathbb{N}$, $k \geq 2$ let $C_\infty(k)$ denote the greatest number such that for all $\varepsilon > 0$ there is an $L = L(\varepsilon)$ with the property that for all $N \in \mathbb{N}$, $\mathcal{A} \subset \{1, 2, \ldots, N\}$ and $|\mathcal{A}| > L$ we have

$$E(N, k, \mathcal{A}) \geq \left(\min(1, (C_\infty(k) - \varepsilon)k\frac{|\mathcal{A}|}{N})\right) N,$$

and define C_∞ by $C_\infty = \inf_{k=2,3,\ldots} C_\infty(k)$.

By Theorem 3 we have

$$C_\infty \geq C \geq \frac{1}{800}. \tag{4.1}$$

In the proof of Theorem 3, I did not force to give a possibly sharp lower bound for C and C_∞. Correspondingly, by a careful analysis of the proof, the lower bound in (4.1) (mostly the one for C_∞) could be improved considerably; however, to get above, say, $\frac{1}{10}$ with the lower bound, essential new ideas would be needed.

Khintchin's theorem (3.6) may suggest that, perhaps, we have $C = C_\infty = 1$. This is not so; indeed, for $|\mathcal{A}| = 2$, $k \in \mathbb{N}$ clearly we have $k|\mathcal{A}| = k + 1$ so that

$$E(N, k, \mathcal{A}) \leq k + 1.$$

Thus for $|\mathcal{A}| = 2$, $k \in \mathbb{N}$, $N \geq k + 1$ we have

$$E(N, k, \mathcal{A}) \leq k + 1 = \left(\min(1, \frac{k+1}{2k} \cdot k\frac{|\mathcal{A}|}{N})\right) N$$

which shows that $C(k) \leq \frac{k+1}{2k}$, $C \leq 1/2$. One might think that this example is the "worst" one so that $C = 1/2$ and, perhaps, $C_\infty = 1$. I will show that this guess is also wrong; the next two sections will be devoted to giving possibly sharp upper bounds for C and C_∞.

5. First it will be proved:

Theorem 8. — *If $N \in \mathbb{N}$,*

$$N \geq k+2 \tag{5.1}$$

and $k \in \mathbb{N}$, then for $\mathcal{A} = \{1, 2, N\}$ we have

$$E(N, k, \mathcal{A}) = k+2. \tag{5.2}$$

For $N \geq k+2$ this implies

$$E(N, k, \mathcal{A}) = \left(\min(1, \frac{k+2}{3k} \cdot k\frac{|\mathcal{A}|}{N})\right) N.$$

It follows that

Corollary 2. — *For all $k \in \mathbb{N}$, $k \geq 2$ we have*

$$C(k) \leq \frac{k+2}{3k}$$

so that

$$C \leq \frac{1}{3}.$$

Proof of Theorem 8. — Clearly we have

$$\begin{aligned} k\mathcal{A} = k\{1,2,N\} &= \bigcup_{i=0}^{k} (i\{N\} + (k-i)\{1,2\}) \\ &= \bigcup_{i=0}^{k} \{iN+k-i, iN+k-i+1, \ldots, iN+2(k-i)\} = \bigcup_{i=0}^{k} \mathcal{B}_i, \end{aligned}$$

where

$$\mathcal{B}_i = \{iN+k-i, iN+k-i+1, \ldots, iN+2(k-i)\}.$$

Consider now an arithmetic progression $\mathcal{Q}(m,d,N) = \{m+d, m+2d, \ldots, m+Nd\}$ with $m \in \mathbb{Z}$, $d \in \mathbb{N}$. Assume first that $d \geq k+1$. Then for $0 \leq i \leq k$, the difference between the greatest and smallest of $\mathcal{B}_i$ is

$$(iN+2(k-i)) - (iN+k-i) = k-i \leq k < d,$$

thus clearly, $\mathcal{Q}(m,d,N)$ may contain at most one element of each $\mathcal{B}_i$. It follows that

$$\begin{aligned} |\mathcal{Q}(m,d,N) \cap k\mathcal{A}| &= |\mathcal{Q}(m,d,N) \cap \bigcup_{i=0}^{k} \mathcal{B}_i| \\ &\leq \sum_{i=0}^{k} \left|\mathcal{Q}(m,d,N) \cap \mathcal{B}_i\right| \leq \sum_{i=0}^{k} 1 = k+1 \text{ (for } d \geq k+1). \end{aligned}$$

Assume now that

$$d \leq k. \tag{5.3}$$

Clearly, we have

$$
\begin{aligned}
&|\mathcal{Q}(m,d,N)\cap\mathcal{B}_i| \\
&\quad\le |\{n : n\equiv m \pmod d,\quad iN+k-i\le n\le iN+2(k-i)\}| \\
&\quad\le \left[\frac{k-i}{d}\right]+1 \qquad \text{for } i=0,1,\dots,k.
\end{aligned}
\tag{5.4}
$$

Assume that $0\le i<j\le k$ and both $\mathcal{B}_i$ and $\mathcal{B}_j$ meet $\mathcal{Q}(m,d,N)$. Then the difference between the smallest element of $\mathcal{B}_j$ and the greatest element of $\mathcal{B}_i$ cannot exceed the difference between the greatest and smallest elements of $\mathcal{Q}(m,d,N)$:

$$(jN+k-j)-(iN+2(k-i))\le (N-1)d$$

whence, by (5.1),

$$j-i\le d+\frac{k-i}{N-1}\le d+\frac{k}{N-1}<d+1.$$

Moreover, if $j-i=d$, then denote the greatest element of $\mathcal{Q}(m,d,N)\cap\mathcal{B}_{i+d}$ (where $i+d=j$) by u. Then $v<u-d(N-1)$ implies that $v\notin\mathcal{Q}(m,d,N)$ since $u\in\mathcal{Q}(m,d,N)$, $u-v>d(N-1)$, and the greatest difference between two elements of $\mathcal{Q}(m,d,N)$ is $d(N-1)$. Thus we have

$$
\begin{aligned}
&|\mathcal{Q}(m,d,N)\cap\mathcal{B}_i|+|\mathcal{Q}(m,d,N)\cap\mathcal{B}_{i+d}| \\
&\quad\le |\{n : n\equiv m \pmod d,\quad u-d(N-1)\le n\le iN+2(k-i)\}| \\
&\qquad\qquad + |\{n' : n'\equiv m \pmod d,\quad (i+d)N+k-(i+d)\le n'\le u\}|.
\end{aligned}
\tag{5.5}
$$

To each n' counted in the second term we may assign the integer $n=n'-d(N-1)$ which satisfies $n\equiv m \pmod d$ and $iN+k-i\le n\le u-d(N-1)$. Thus the sum estimated in (5.5) is

$$
\begin{aligned}
&\le |\{n : n\equiv m \pmod d,\quad u-d(N-1)\le n\le iN+2(k-i)\}| \\
&\qquad\qquad + |\{n : n\equiv m \pmod d,\quad iN+k-i\le n\le u-d(N-1)\}| \\
&= |\{n : n\equiv m \pmod d,\quad iN+k-i\le n\le iN+2(k-i)\}|+1
\end{aligned}
$$

(the last term 1 stands for $u-d(N-1)$ counted in both terms of the previous sum) and thus we have

$$
\begin{aligned}
&|\mathcal{Q}(m,d,N)\cap\mathcal{B}_i|+|\mathcal{Q}(m,d,N)\cap\mathcal{B}_{i+d}| \\
&\qquad\qquad \le \left(\left[\frac{k-i}{d}\right]+1\right)+1=\left[\frac{k-i}{d}\right]+2.
\end{aligned}
\tag{5.6}
$$

It follows from (5.4) and the discussion above that if $i_1<i_2<\cdots<i_t$ denote the integers i with $\mathcal{Q}(m,d,N)\cap\mathcal{B}_i\ne\varnothing$, then either we have $t\le d$ and then

$$
\begin{aligned}
\sum_{j=1}^{t}|\mathcal{Q}(m,d,N)\cap\mathcal{B}_{i_j}| &\le \sum_{j=1}^{t}\left(\left[\frac{k-i_j}{d}\right]+1\right) \\
&\le \sum_{j=0}^{t-1}\left(\left[\frac{k-j}{d}\right]+1\right)\le \sum_{j-0}^{d-1}\left[\frac{k-j}{d}\right]+d
\end{aligned}
$$

or we have $t = d+1$, $i_2 = i_1 + 1$, $i_3 = i_1 + 2$, $\dots$, $i_t = i_{d+1} = i_1 + d$ and then, using also (5.6),

$$\begin{aligned}\sum_{j=1}^{t} |\mathcal{Q}(m,d,N) \cap \mathcal{B}_{i_j}| &= (|\mathcal{Q}(m,d,N) \cap \mathcal{B}_{i_1}| + |\mathcal{Q}(m,d,N) \cap \mathcal{B}_{i_t}|) \\ &\quad + \sum_{j=2}^{t-1} |\mathcal{Q}(m,d,N) \cap \mathcal{B}_{i_j}| \\ &\le \left(\left[\frac{k-i_1}{d}\right] + 2\right) + \sum_{j=2}^{t-1} \left(\left[\frac{k-i_j}{d}\right] + 1\right) \\ &= \sum_{j=1}^{t-1} \left(\left[\frac{k-i_j}{d}\right] + 1\right) + 1 \le \sum_{j=0}^{t-2} \left(\left[\frac{k-j}{d}\right] + 1\right) + 1 \\ &= \sum_{j=0}^{d-1} \left[\frac{k-j}{d}\right] + (d+1).\end{aligned}$$

In both cases we have

$$\begin{aligned}|\mathcal{Q}(m,d,N) \cap k\mathcal{A}| &\le \sum_{j=1}^{t} |\mathcal{Q}(m,d,N) \cap \mathcal{B}_{i_j}| \\ &\le \sum_{j=0}^{d-1} \left[\frac{k-j}{d}\right] + (d+1).\end{aligned}$$

Define the integers q, r by $k = qd + r$, $0 \le r < d$. Then, using (5.3), we have

$$\begin{aligned}\sum_{j=0}^{d-1} \left[\frac{k-j}{d}\right] + (d+1) &= \sum_{j=0}^{r} \left[\frac{k-j}{d}\right] + \sum_{j=r+1}^{d-1} \left[\frac{k-j}{d}\right] + (d+1) \\ &= (r+1)q + (d-1-r)(q-1) + (d+1) = qd + r + 2 = k + 2\end{aligned}$$

which proves that

$$E(N,k,\mathcal{A}) \le k+2. \tag{5.7}$$

To see that also

$$E(N,k,\mathcal{A}) \ge k+2 \tag{5.8}$$

holds, observe that by (5.1) we have

$$\{k, k+1, \dots, 2k, N+k-1\} \subset \{(k-1)+1, (k-1)+2, \dots, (k-1)+N\} \cap k\mathcal{A}.$$

(5.2) follows from (5.7) and (5.8), and this completes the proof of the theorem. □

6. In this section it will be proved:

Theorem 9. — *If* $N \in \mathbb{N}$, $i \in \mathbb{N}$, $k \in \mathbb{N}$,

$$N > 4ki, \tag{6.1}$$

and we write $\mathcal{A} = \{1, 2, \ldots, i, N-i+1, N-i+2, \ldots, N\}$, *then we have*

$$E(N, k, \mathcal{A}) \leq ki + i.$$

For $N > 4ki$ this implies

$$E(N, k, \mathcal{A}) \leq ki + i = \left(\min(1, \frac{k+1}{2k} \cdot k\frac{|\mathcal{A}|}{N})\right) N$$

so that

Corollary 3. — *For all* $k \in \mathbb{N}$, $k \geq 2$ *we have*

$$C_\infty(k) \leq \frac{k+1}{2k}$$

whence

$$C_\infty \leq \frac{1}{2}.$$

Proof of Theorem 9. — Clearly we have

$$\begin{aligned} k\mathcal{A} &= k\{1, 2, \ldots, i, N-i+1, N-i+2, \ldots, N\} \\ &= k(\{0, N-i\} + \{1, 2, \ldots, i\}) = k\{0, N-i\} + k\{1, 2, \ldots, i\} \\ &= \{0, N-i, \ldots, k(N-i)\} + \{k, k+1, \ldots, ki\} \\ &= \bigcup_{j=0}^{k} \{j(N-i)+k, j(N-i)+k+1, \ldots, j(N-i)+ki\} = \bigcup_{j=0}^{k} \mathcal{B}_j, \end{aligned}$$

where

$$\mathcal{B}_j = \{j(N-i)+k, j(N-i)+k+1, \ldots, j(N-i)+ki\}.$$

Consider now an arithmetic progression $\mathcal{Q}(m, d, N) = \{m+d, m+2d, \ldots, m+Nd\}$ with $m \in \mathbb{Z}$, $d \in \mathbb{N}$. We have to distinguish two cases. Assume first that

$$d \geq k+1. \tag{6.2}$$

Then we have

$$\begin{aligned} |\mathcal{Q}(m, d, N) \cap k\mathcal{A}| &= |\mathcal{Q}(m, d, N) \cap \bigcup_{j=0}^{k} \mathcal{B}_j| \\ &\leq \sum_{j=0}^{k} |\mathcal{Q}(m, d, N) \cap \mathcal{B}_j|. \end{aligned} \tag{6.3}$$

Here clearly we have

$$
\begin{aligned}
&|\mathcal{Q}(m,d,N) \cap \mathcal{B}_j| \\
&\qquad \le |\{n : n \equiv m \pmod d, \quad j(N-i)k \le n \le j(N-i)+ki\}| \\
&\qquad \le \left[\frac{ki-k}{d}\right] + 1 \text{ for } j = 0, 1, \ldots, k.
\end{aligned} \tag{6.4}
$$

It follows from (6.2), (6.3) and (6.4) that

$$
\begin{aligned}
|\mathcal{Q}(m,d,N) \cap k\mathcal{A}| &\le \sum_{j=0}^{k} \left(\left[\frac{ki-k}{d}\right] + 1 \right) \\
&= (k+1)\left(\left[\frac{ki-k}{d}\right] + 1 \right) \le (k+1)\left(\frac{ki-k}{k+1} + 1 \right) \\
&= ki + 1 \ (\text{ for } d \ge k+1).
\end{aligned} \tag{6.5}
$$

Assume now that

$$
d \le k. \tag{6.6}
$$

Note that the assumption (6.2) was not used in the proof of (6.4) so that (6.4) holds also in this case.

Assume that $0 \le u < v \le k$ and both $\mathcal{B}_u$ and $\mathcal{B}_v$ meet $\mathcal{Q}(m,d,N)$. Then the difference between the smallest element of $\mathcal{B}_v$ and the greatest element of $\mathcal{B}_u$ cannot exceed the difference between the greatest and smallest elements of $\mathcal{Q}(m,d,N)$:

$$
(v(N-i)+k) - (u(N-i)+ki) \le (N-1)d
$$

whence, by (6.1) and (6.6),

$$
v - u \le d + \frac{(i-1)d + (ki-k)}{N-i} < d + \frac{2(ki-k)}{N/2} < d+1.
$$

Moreover, if $v - u = d$, then denote the greatest element of $\mathcal{Q}(m,d,N) \cap \mathcal{B}_{u+d}$ (where $u + d = v$) by x. Then $y < x - d(N-1)$ implies that $y \notin \mathcal{Q}(m,d,N)$ since $x \in \mathcal{Q}(m,d,N), x - y > d(N-1)$, and the greatest difference between two elements of

$\mathcal{Q}(m,d,N)$ is $d(N-1)$. Thus we have

$$\begin{aligned}
&|\mathcal{Q}(m,d,N)\cap\mathcal{B}_u| + |\mathcal{Q}(m,d,N)\cap\mathcal{B}_{u+d}| \\
&\le |\{n : n\equiv m \pmod d,\quad x-(N-1)d\le n\le u(N-i)+ki\}| \\
&\qquad + |\{n : n\equiv m \pmod d,\quad (u+d)(N-i)+k\le n\le x\}| \\
&\le \left(\left[\frac{(u(N-i)+ki)-(x-(N-1)d)}{d}\right]+1\right) \\
&\qquad + \left(\left[\frac{x-((u+d)(N-i)+k)}{d}\right]+1\right) \qquad (6.7)\\
&\le \frac{u(N-i)+ki-x+(N-1)d}{d} \\
&\qquad + \frac{x-u(N-i)-d(N-i)-k}{d}+2 \\
&= i+1+\frac{ki-k}{d}.
\end{aligned}$$

It follows from (6.4), (6.6) and the discussion above that if $j_1<j_2<\cdots<j_t$ denote the integers j with

$$\mathcal{Q}(m,d,N)\cap\mathcal{B}_j\ne\varnothing,$$

then either we have $t\le d$ and then

$$\begin{aligned}
\sum_{\ell=1}^{t}|\mathcal{Q}(m,d,N)\cap\mathcal{B}_{j_\ell}| &\le \sum_{\ell=1}^{t}\left(\left[\frac{ki-k}{d}\right]+1\right) \\
&\le d\left(\left[\frac{ki-k}{d}\right]+1\right)\le ki-k+d\le ki,
\end{aligned}$$

or we have $t=d+1$, $j_2=j_1+1$, $j_3=j_1+2$, $\dots$, $j_t=j_{d+1}=j_1+d$ and then, using also (6.7),

$$\begin{aligned}
\sum_{\ell=1}^{t}|\mathcal{Q}(m,d,N)\cap\mathcal{B}_{j_\ell}| &= (|\mathcal{Q}(m,d,N)\cap\mathcal{B}_{j_1}|+|\mathcal{Q}(m,d,N)\cap\mathcal{B}_{j_t}|) \\
&\qquad + \sum_{\ell=2}^{t-1}|\mathcal{Q}(m,d,N)\cap\mathcal{B}_{j_\ell}| \\
&\le i+1+\frac{ki-k}{d}+(t-2)\left(\left[\frac{ki-k}{d}\right]+1\right) \\
&\le i+t-1+(t-1)\frac{ki-k}{d} = i+d+ki-k\le ki+i.
\end{aligned}$$

In both cases we have

$$|\mathcal{Q}(m,d,N)\cap k\mathcal{A}|\le\sum_{\ell=1}^{t}|\mathcal{Q}(m,d,N)\cap\mathcal{B}_{j_\ell}|\le ki+i$$

which completes the proof of the theorem. □

7. One might like to make a guess on the values of the constants C and C_∞. Suggested by the results above, I would risk two conjectures:

(i) we have
$$C < C_\infty$$
(this is, perhaps, not quite hopeless);

(ii) we have
$$C_\infty = \frac{1}{2};$$
this seems to the closest finite analog of the $\alpha + \beta$ conjecture but probably it will not be easy to prove it.

On the other hand, I have no idea whether Corollary 2 gives the best possible upper bound for C, i.e., we have $C = 1/3$; it is quite possible that (perhaps, using computers) one can find a set $\mathcal{A}$ whose study leads to an upper bound smaller than $1/3$.

8. In the rest of this paper, I will study another extension of the classical Schnirelmann-Khintchin-Mann-Kneser theory of addition theorems. Namely, in this theory as well as in the finite case studied above, our basic problem is the following: we start out from a set $\mathcal{A}$ whose density in a certain sense is $\geq \delta (> 0)$ and then our goal is to give a lower bound for the density of $k\mathcal{A}$ in terms of k and δ. (This lower bound is usually $k\delta$ or, at least, $ck\delta$.) In particular, how large k is needed to be to ensure that the density of $k\mathcal{A}$ should be 1 ? (Khintchin's theorem (3.6) and my Theorem 3 above are typical results of this type). This problem can be generalized in the following way:

Suppose we start out from a set $\mathcal{B}$ known to be a basis, like the set of the primes or k-th powers. What happens if we take a subset $\mathcal{A}$ of $\mathcal{B}$ whose "density relative to $\mathcal{B}$" is $\geq 1/k$ (where $k \in \mathbb{N}$, $k \geq 2$), i.e., we take $\geq 100/k$ percent of the elements of $\mathcal{B}$ as $\mathcal{A}$? What additional condition is needed to ensure that $\mathcal{A}$ should form a basis, and if such a condition holds, then what upper bound can be given for the order of the basis $\mathcal{A}$ in terms of k and the order of the basis $\mathcal{B}$? The difficulty is that usually one needs a coprimality condition concerning the set $\mathcal{A}$. The most interesting problem of this type is when $\mathcal{B}$ consists of the primes, namely, then no coprimality condition is needed. Thus here we shall restrict ourselves to this special case. In other words, the problem is the following:

Assume that $k \in \mathbb{N}$, $k \geq 2$ and $\mathcal{P}$ is an infinite set of primes with the property that

$$\liminf_{n \to +\infty} \frac{P(n)}{\pi(n)} \geq \frac{1}{k}. \tag{8.1}$$

Then by Schnirelman's method, it can be shown that $\{0\} \cup \mathcal{P}$ is an asymptotic basis of finite order. Let $H = H(k)$ denote the smallest integer h such that for every set $\mathcal{P}$ of primes satisfying (8.1), $\{0\} \cup \mathcal{P}$ is an asymptotic basis of order $\leq h$ (i.e., H is the smallest integer such that for every $\mathcal{P}$ satisfying (8.1), every large integer can be represented as the sum of at most H elements of $\mathcal{P}$). The problem is to estimate H in terms of k. It will be proved that

Theorem 10. — *For all $k \in \mathbb{N}$ we have*

$$c_1 k \log\log(k+2) < H(k) < c_2 k^4. \tag{8.2}$$

Probably the lower bound gives the right order of magnitude of $H(k)$; unfortunately, I have not been able to prove this. Moreover, we remark that a finite analog of Theorem 10 (a theorem covering finite sets $\mathcal{P}$ of primes) could be proved as well but it would be much more complicated; thus we restrict ourselves to the much simpler infinite case.

Proof. — First we will prove the lower bound in (8.2). We will show that if c_3 is a small positive constant to be fixed later, then for every $k \in \mathbb{N}$ there is a positive integer m such that

$$m > c_3 k \log\log(k+2) \tag{8.3}$$

and

$$\varphi(m) \le k. \tag{8.4}$$

Indeed, denote the i-th prime by q_i, and define t by

$$q_1 q_2 \dots q_t \le c_3 k \log\log(k+2) < q_1 q_2 \dots q_{t+1}. \tag{8.5}$$

(If $c_3 k \log\log(k+2) < 2$, then (8.3) and (8.4) hold with $m = 2$.) By the prime number theorem, it follows from (8.5) that

$$q_t = (1+o(1)) \log k \qquad (\text{for } k \to +\infty). \tag{8.6}$$

Define u by

$$u = \left[\frac{c_3 k \log\log(k+2)}{q_1 q_2 \cdots q_{t-1}}\right]$$

and let

$$m = q_1 q_2 \dots q_{t-1}(u+1). \tag{8.7}$$

Then (8.3) holds trivially. Moreover, for $k \to +\infty$ clearly we have

$$m = (1+o(1)) c_3 k \log\log(k+2). \tag{8.8}$$

By Mertens' formula, it follows from (8.6), (8.7) and (8.8) that for $k > k_o$ (where k_o may depend also on c_3)

$$\begin{aligned}\varphi(m) = m \prod_{p|m}(1-\frac{1}{p}) &\le m \prod_{i=1}^{t-1}(1-\frac{1}{q_i}) \\ &< c_4 \frac{m}{\log q_{t-1}} < 2c_4 \frac{m}{\log\log(k+2)} \\ &< 3c_4 \frac{c_3 k \log\log(k+2)}{\log\log(k+2)} = 3c_3 c_4 k\end{aligned}$$

so that (8.4) holds if we choose $c_3 = 1/3c_4$ and $k > k_o$. Finally, if $k \le k_o$, then (8.3) and (8.4) hold with $m = 1$ at the expense of replacing the constant c_3 computed above by another smaller constant (small enough in terms of k_o) and this proves the existence of a number m satisfying (8.3) and (8.4).

Now define $\mathcal{P}$ by

$$\mathcal{P} = \{p : p \text{ prime}, p \equiv 1 \pmod{m}\}.$$

Then by the prime number theorem for the arithmetic progressions of small moduli, it follows from (8.4) that for $n \to +\infty$ we have

$$P(n) = (1 + o(1))\frac{\pi(n)}{\varphi(m)} > (1 + o(1))\frac{\pi(n)}{k}$$

which proves (8.1). Moreover, if $v < m$, then $v(\{0\} \cap \mathcal{P})$ does not contain the positive multiples of m, thus if the order of the asymptotic basis $\{0\} \cup \mathcal{P}$ is h, then, by (8.3), we have

$$h \geq m > c_3 k \log\log(k + 2)$$

which proves the lower bound in (8.2).

To prove the upper bound, we need two lemmas.

Lemma 1. — *There is an absolute constant c_5 such that if $\mathcal{P}$ is a set of primes satisfying (8.1) and N is large enough depending on $\mathcal{P}$, then we have*

$$S(\mathcal{P}, N) > c_5 N k^{-4} \tag{8.9}$$

where $S(\mathcal{P}, N)$ denotes the counting function of the set $S(\mathcal{P}) = \mathcal{P} + \mathcal{P}$.

Proof of Lemma 1. — Let $R(n)$ denote the number of pairs (p, q) of primes with

$$p + q = n$$

so that, by Brun's sieve (see, *e.g.*, [15, p. 80]), for $n \in \mathbb{N}$, $n > 1$ we have

$$R(n) < c_6 \prod_{p|n}(1 + \frac{1}{p})\frac{n}{(\log n)^2}. \tag{8.10}$$

Moreover, denote the number of solutions of

$$p + q = n, \quad p \in \mathcal{P},\ q \in \mathcal{P}$$

by $r(\mathcal{P}, n)$.

By (8.1) and the prime number theorem, for sufficiently large N we have

$$\begin{aligned}\sum_{n=1}^{N} r(\mathcal{P}, n) &= \sum_{n=1}^{N} |\{(p, q) : p + q \leq N,\ p, q \in \mathcal{P}\}| \\ &\geq \sum_{n=1}^{N} |\{(p, q) : p, q \leq N/2,\ p, q \in \mathcal{P}\}| = (P([N/2]))^2 \\ &\geq (1 + o(1))\frac{1}{k^2}(\pi([N/2]))^2 > \frac{1}{5k^2}\frac{N^2}{(\log N)^2}.\end{aligned}$$

Thus by Cauchy's inequality we have

$$\begin{aligned}\sum_{n=1}^{N} r^2(\mathcal{P},n) &\geq \left(\sum_{n=1}^{N} r(\mathcal{P},n)\right)^2 |\{n : n \in S(\mathcal{P}),\ n \leq N\}|^{-1} \\ &> \frac{1}{25k^4}\frac{N^4}{(\log N)^4}\frac{1}{S(\mathcal{P},N)}.\end{aligned} \tag{8.11}$$

On the other hand, by (8.10) we have

$$\begin{aligned}\sum_{n=1}^{N} r^2(\mathcal{P},n) &\leq \sum_{n=1}^{N} R^2(n) < c_7\frac{N^2}{(\log N)^4}\sum_{n=1}^{N}\prod_{p|n}(1+\frac{1}{p})^2 \\ &< c_8\frac{N^2}{(\log N)^4}\sum_{n=1}^{N}\prod_{p|n}(1+\frac{2}{p}) \\ &= c_8\frac{N^2}{(\log N)^4}\sum_{n=1}^{N}\sum_{d|n,|\mu(d)|=1}\frac{2^{\omega(d)}}{d} \\ &= c_8\frac{N^2}{(\log N)^4}\sum_{d\leq N,|\mu(d)|=1}\frac{2^{\omega(d)}}{d}[\frac{N}{d}] \\ &\leq c_8\frac{N^3}{(\log N)^4}\sum_{|\mu(d)|=1}\frac{2^{\omega(d)}}{d^2} \\ &= c_8\frac{N^3}{(\log N)^4}\prod_{p}(1+\frac{2}{p^2}) < c_9\frac{N^3}{(\log N)^4}.\end{aligned} \tag{8.12}$$

(8.9) follows from (8.11) and (8.12), and this completes the proof of Lemma 1. □

Lemma 2. — *If $\ell \in \mathbb{N}$, and $\mathcal{A}$ is an infinite set of non-negative integers such that $0 \in \mathcal{A}$ and*

$$\underline{d}(\ell\mathcal{A}) < \ell\underline{d}(\mathcal{A}),$$

then there is a set $\mathcal{E}$ and a number g such that

$$\mathcal{E} \subset \ell\mathcal{A}, \tag{8.14}$$

$$0 \in \mathcal{E}, \tag{8.15}$$

there is a number n_o such that

$$e \in \mathcal{E},\ e' \equiv e \pmod{g},\ e' \geq n_o \text{ imply } e' \in \mathcal{E} \tag{8.16}$$

(so that $[n_o,+\infty) \cap \mathcal{E}$ is the union of the intersection of certain modulo g residue classes, including the 0 residue class, with $[n_o,+\infty)$) and

$$d(\mathcal{E}) \geq \ell\underline{d}(\mathcal{A}) - \frac{\ell}{g}. \tag{8.17}$$

Proof of lemma 2. — This follows from Kneser's theorem [18] and, indeed, it is a special case of [16, p. 57, Theorem 19].

To complete the proof of the upper bound in (8.2), first we use Lemma 2 with $\ell = [\frac{2}{c_5}k^4]+1$ (where c_5 is the constant in Lemma 1) and with $S(\{0\}\cup\mathcal{P}) = 2(\{0\}\cup\mathcal{P})$ in place of $\mathcal{A}$. By Lemma 1 we have

$$\underline{d}(S(\{0\}\cup\mathcal{P})) \geq \liminf_{N\to+\infty} \frac{S(\mathcal{P},N)}{N} \geq c_5 k^{-4}.$$

Thus we have

$$\ell\underline{d}(\{0\}\cup S(\mathcal{P})) \geq \left(\left[\frac{2}{c_5}k^4\right]+1\right)c_5k^{-4} > 2 \tag{8.18}$$

so that (8.13) certainly holds thus, indeed, Lemma 2 can be applied. By (8.17) and (8.18), we have

$$1 \geq d(\mathcal{E}) \geq \ell\underline{d}(S(\{0\}\cup\mathcal{P})) - \frac{\ell}{g} > 2 - \frac{\ell}{g}$$

whence

$$g < \ell. \tag{8.19}$$

Now it will be proved that every large integer n can be represented in the form

$$p_1 + p_2 + \cdots + p_u = n \text{ with } p_1, p_2, \ldots p_u \in \mathcal{P},\ u \leq 3l-2. \tag{8.20}$$

Indeed, let p' denote the smallest prime with

$$p' > g, \quad p' \in \mathcal{P}, \tag{8.21}$$

and assume that

$$n \geq n_o + (g-1)p' \tag{8.22}$$

where n_o is defined by (8.16). By (8.21) we have $(p', g) = 1$, thus there is an integer i such that

$$n - ip' \equiv 0 \pmod{g} \tag{8.23}$$

and

$$0 \leq i \leq g-1. \tag{8.24}$$

By (8.22) and (8.24) we have

$$n - ip' \geq (n_o + (g-1)p') - (g-1)p' = n_o. \tag{8.25}$$

It follows from (8.14), (8.15), (8.16), (8.23) and (8.25) that

$$n - ip' \in \mathcal{E} \subset \ell\mathcal{A} = \ell S(\{0\}\cup\mathcal{P}) = (2\ell)(\{0\}\cup\mathcal{P})$$

so that there are primes $p_1, p_2, \ldots, p_v$ with

$$n - ip' = p_1 + p_2 + \cdots + p_v, \quad p_1, p_2, \ldots p_v \in \mathcal{P} \tag{8.26}$$

and

$$v \leq 2\ell. \tag{8.27}$$

(8.26) can be rewritten in the form

$$p_1 + p_2 + \cdots + p_v + ip' = n.$$

This is a representation of the form (8.20) where, by (8.19), (8.24) and (8.27), the number of the terms on the left hand side is

$$u = v + i \leq 2\ell + g - 1 \leq 3\ell - 2.$$

Thus every integer n satisfying (8.22) has a representation in form (8.20). It follows that $\{0\} \cup \mathcal{P}$ is an asymptotic basis of order

$$h \leq 3\ell - 2 = 3\left(\left[\frac{2}{c_5}k^4\right] + 1\right) - 2 < c_{10}k^4$$

which proves the upper bound in (8.2). □

References

[1] N. Alon, *Subset sums*, J. Number Theory, **27**, 1987, 196–205.

[2] N. Alon and G. Freiman, *On sums of subsets of a set of integers*, Combinatorica, **8**, 1988, 297–306.

[3] F. Dyson, *A theorem on the densities of sets of integers*, J. London Math. Soc., **20**, 1945, 8–14.

[4] P. Erdős, *On the representation of large integers as sums of distinct summands taken from a fixed set*, Acta. Arith., **7**, 1961/62, 345–354.

[5] P. Erdős and G. Freiman, *On two additive problems*, J. Number Theory, **34**, 1990, 1–12.

[6] P. Erdős, J.-L. Nicolas and A. Sárkőzy, *On the number of partitions of n without a given subsum*, II, Analytic Number Theory, Proceedings of a Conference in Honor of P. T. Bateman, B. C. Berndt et al. eds., Birkhäuser, Boston-Basel-Berlin, 1990, 205–234.

[7] P. Erdős, J.-L. Nicolas and A. Sárkőzy, *On the number of pairs of partitions of n without common subsums*, Colloquium Math., **63**, 1992, 61–83.

[8] P. Erdős and A. Sárkőzy, *On a problem of Straus*, Disorder in Physical Systems (a volume in Honour of John M. Hammersley), G. R. Grimmett and D. J. Welsh eds., Clarendon Press, Oxford, 1990, 55–66.

[9] P. Erdős and A. Sárkőzy, *Arithmetic progression in subset sums*, Discrete Mathematics, **102**, 1992, 249–264.

[10] P. Erdős, A. Sárkőzy and C. L. Stewart, *On prime factors of subset sums*, J. London Math. Soc., **49**, 1994, 209–218.

[11] J. Folkman, *On the representation of integers as sums of distinct terms from a fixed sequence*, Canadian J. Math, **18**, 1966, 643–655.

[12] G. A. Freiman, *Foundations of a Structural Theory of Set Additions*, Translations of Mathematical Monographs, **37**, Amer. Math. Soc., Providence, RI.

[13] G. A. Freiman, *New analytical results in subset-sum problem*, Discrete Mathematics, **114**, 1993, 205–218.

[14] G. A. Freiman, *Sumsets and powers of 2*, Coll. Math. Soc. J. Bolyai, **60**, 1992, 279–286.

[15] H. Halberstam and H.-E. Richert, *Sieve Methods*, Academic Press, 1974.

[16] H. Halberstam and K.F. Roth, *Sequences*, Springer Verlag, Berlin, 1983.

[17] A. Khintchin, *Zur additiven Zahlentheorie*, Math. Sb. N.S., **39**, 1932, 27–34.

[18] M. Kneser, *Abschätzungen der asymptotischen Dichte von Summenmengen*, Math. Z, **58**, 1953, 459–484.

[19] H. B. Mann, *A proof of the fundamental theorem on the density of sums of sets of positive integers*, Ann. Math., **43**, 1942, 523–527.

[20] M. B. Nathanson and A. Sárkőzy, *Sumsets containing long arithmetic progressions and powers of 2*, Acta Arith., **54**, 1989, 147–154.

[21] A. Sárkőzy, *Finite addition theorems, I*, J. Number Theory, **32**, 1989, 114–130.

[22] A. Sárkőzy, *Finite addition theorems, II*, J. Number Theory, **48**, 1994, 197–218.

[23] A. Sárkőzy, *Finite addition theorems, III*, Publ. Math. d'Orsay, **92–01**, 105–122

[24] L. G. Schnirelmann *Über additive Eigenschaften von Zahlen*, Annals Inst. Polyt. Novocherkassk, **14**, (1930), 3–28; Math. Annalen, **107**, 1933, 649–90.

A. Sárkőzy, Department of Algebra and Number Theory, Eőtvős Loránd University, Rákóczi út 5, H-1088 Budapest, Hungary • *E-mail :* sarkozy@cs.elte.hu