On Additive Representation Functions

A. Sárközy* and V. T. Sós*

Mathematical Institute, Hungarian Academy of Sciences, Budapest Pf. 127, 1364, Hungary

1. Introduction

In this paper we give a short survey of additive representation functions, in particular, on their regularity properties and value distribution. We prove a couple of new results and present many related unsolved problems.

The study of additive representation functions is closely related to many other topics in mathematics: the first basic questions arose from Sidon's work in harmonic analysis; analytical methods (exponential sums) and combinatorial methods are equally used; Erdős and Rényi introduced probabilistic methods, etc.

Paul Erdős played a dominant role in the advance of this field. As Halberstam and Roth write in their excellent monograph [23] written on sequences of integers:

> Acknowledgements
> Anyone who turns the pages of this book, will immediately notice the predominance of results due to Paul Erdős. In so far as the substance of this book may be said to define a distinct branch of number theory – and its wide range of topics in classical number theory appears to justify this claim – Erdős is certainly its founder. He was the first to recognize its true potential and has been the central figure in many of its developments.
> The authors were indeed fortunate to have the benefit of many discussions with Dr. Erdős. His unique insight and encyclopedic knowledge were, of course, invaluable, but the authors are no less indebted to him for his constant interest and encouragement.

In the last 15 years the authors of this paper and Paul Erdős have written several joint papers on this field (a survey of our joint work is given in [21]). On this very special occasion we have the opportunity to emphasize and appreciate the importance of his contribution to this field, and to thank him for the many invaluable and fruitful discussions with him from which we have learned so much.

* Research partially supported by Hungarian National Foundation for Scientific Research, Grant No. 1901.

R. L. Graham et al. (eds.), *The Mathematics of Paul Erdös I*

2. Notations

The set of 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 their counting functions are denoted by $A(n)$, $B(n)$, ... so that, e.g.,

$$A(n) = |\{a: 0 < a \leq n, a \in \mathcal{A}\}|.$$

$\mathcal{A}_1 + \mathcal{A}_2 + \ldots + \mathcal{A}_k$ denotes the set of the integers that can be represented in the form $a_1 + a_2 + \ldots + a_k$ with $a_1 \in \mathcal{A}_1, \ldots, a_k \in \mathcal{A}_k$; in particular, we write $\mathcal{A} + \mathcal{A} = 2\mathcal{A} = \mathcal{S}(\mathcal{A})$. For $\mathcal{A} \subset \mathbb{N}$, $\mathcal{D}(\mathcal{A})$ denotes the difference set of the set $\mathcal{A}$, i.e., the set of the positive integers that can be represented in the form $a - a'$ with $a, a' \in \mathcal{A}$. For $\mathcal{A} = \{a_1, a_2, \ldots\} \subset \mathbb{N}_0$, $k \in \mathbb{N}$ we write $k \times \mathcal{A} = \{ka_1, ka_2, \ldots\}$.

Representation functions

For $\mathcal{A} \subset \mathbb{N}_0$, $n \in \mathbb{N}_0$ the number of solutions of the equations

$$\begin{aligned} a + a' &= n \qquad a, a' \in \mathcal{A}, \\ a + a' &= n, \qquad a, a' \in \mathcal{A}, \qquad a \leq a' \end{aligned}$$

and

$$a + a' = n, \qquad a, a' \in \mathcal{A}, \qquad a < a'$$

is denoted by $r_1(\mathcal{A}, n)$, $r_2(\mathcal{A}, n)$, resp. $r_3(\mathcal{A}, n)$ and are called the additive representation functions belonging to $\mathcal{A}$.

For $g \in \mathbb{N}$, $B_2[g]$ denotes the class of all (finite or infinite) sets $\mathcal{A} \subset \mathbb{N}_0$ such that for all $n \in \mathbb{N}_0$ we have $r_2(\mathcal{A}, n) \leq g$, i.e., the equation

$$a + a' = n, \qquad a, a' \in \mathcal{A}, \qquad a \leq a'$$

has at most g solutions. The sets $\mathcal{A} \in B_2[1]$ are called Sidon sets.

If $F(n) = O(G(n))$, then we write $F(n) \ll G(n)$.

3. The representation function of general sequences. The Erdős–Fuchs theorem and related results

Erdős and Turán [22] proved in 1941 that for an infinite set $\mathcal{A} \subset \mathbb{N}$, the representation function $r_1(\mathcal{A}, n)$ cannot be a constant from a certain point on. Dirac and Newman [6] proved that the same holds with $r_2(\mathcal{A}, n)$ in place of $r_1(\mathcal{A}, n)$. Since their proof is short and elegant, we present it here:

Let

$$f(x) = \sum_{a \in \mathcal{A}} x^a \qquad (\text{ for } x \text{ real }, \ |x| < 1) \ .$$

If $r_2(\mathcal{A}, n) = k$ for $n > m$, then

$$\frac{1}{2}(f^2(x) + f(x^2)) = \sum_{n=0}^{+\infty} r_2(\mathcal{A}, n)x^n = P_m(x) + k\frac{x^{m+1}}{1-x}$$

where $P_m(x)$ is a polynomial of degree $\leq m$. If $x \to -1$ from the right, then the right hand side has a finite limit while the left hand side tends to $+\infty$. This contradiction proves the theorem.

Moreover, in [22] Erdős and Turán conjectured that their result can be sharpened in the following way: if $\mathcal{A} \subset \mathbb{N}$ and $c > 0$, then

$$\sum_{n=1}^{N} r_1(\mathcal{A}, n) = cN + O(1)$$

cannot hold.

In [12], Erdős and Fuchs proved two theorems one of which sharpens the above mentioned result of Erdős and Turán:

Theorem 3.1 (Erdős and Fuchs [12]). *If $\mathcal{A} = \{a_1, a_2, \ldots\} \subset \mathbb{N}$, $c > 0$, or $c = 0$ and $a_k < Ak^2$ (for $k = 1, 2, \ldots$), and $i = 1, 2, 3$, then*

$$\limsup_{N \to +\infty} \frac{1}{N} \sum_{n=0}^{N} (r_i(\mathcal{A}, n) - c)^2 > 0 .$$

Their other, better known result (in fact, this is the result known as "the Erdős–Fuchs theorem") proves the conjecture of Erdős and Turán in the following sharper form:

Theorem 3.2 (Erdős and Fuchs [12]). *If $\mathcal{A} \subset \mathbb{N}$, $c > 0$, then*

$$\sum_{n=1}^{N} r_1(\mathcal{A}, n) = cN + o(N^{1/4}(\log N)^{-1/2}) \tag{3.1}$$

cannot hold.

One of the most important problems in number theory is the circle problem, i.e., the estimate of the number of lattice points in the circle $x^2+y^2 \leq N$. Writing

$$\triangle(N) = |\{(x, y): x, y \in \mathbb{Z},\ x^2 + y^2 \leq N\}| - \pi N ,$$

the problem is to estimate $\triangle(N)$. By a classical result of Hardy and Landau, one cannot have

$$\triangle(N) = o(N^{1/4}(\log N)^{1/4}) . \tag{3.2}$$

The importance of Theorem 3.2 is based on the fact that the special case $\mathcal{A} = \{1^2, 2^2, \ldots\}$ of it corresponds to the circle problem, and the Ω-estimate proved in the much more general Theorem 3.2 is only by a logarithm power worse than (3.2).

Theorem 3.2 has been extended in various directions. Bateman, Kohlbecker and Tull [3] studied the more general problem when the left hand side of (3.1) is approximated by an arbitrary "nice" function (instead of cN). Vaughan [40] extended the result to sums of $k(\geq 2)$ terms (see also Hayashi [24]). Richert [29] proved the multiplicative analogue of Theorem 3.2. Sárközy [34] extended Theorem 3.2 by giving an Ω-result on the number of solutions of

$$a+b\leq N, \qquad a\in\mathcal{A}, \qquad b\in B\ .$$

Jurkat showed (unpublished) that the factor $(\log N)^{-1/2}$ on the right hand side of (3.1) can be eliminated, and recently, Montgomery and Vaughan [28] published another proof of this result.

Erdős and Sárközy [14], [15] showed that if $f(n)\to+\infty$, $f(n+1)\geq f(n)$ for $n>n_0$ and $f(n)=o\left(\frac{n}{(\log n)^2}\right)$, then

$$\max_{n\leq N}|r_1(\mathcal{A},n)-f(n)|=o\left((f(N))^{1/2}\right) \tag{3.3}$$

cannot hold (see also Vaughan [40], Hayashi [24]). Erdős and the authors continued the study of the regularity properties of the functions $r_i(\mathcal{A},n)$ in [16], [17] and [18], first by studying the *monotonicity properties* of these functions (see also Balasubramanian [2]). In an interesting way, here the three representation functions $r_1(\mathcal{A},n)$, $r_2(\mathcal{A},n)$, $r_3(\mathcal{A},n)$ behave completely differently.

We proved

Theorem 3.3 (P. Erdős, A. Sárközy, V.T. Sós [17]). *(a) $r_1(\mathcal{A},n)$ can be monotone for $n>n_0$ only in the trivial case when $\mathcal{A}$ contains all the positive integers from a certain point on; $A(N)=N-c$ for $N>n_1$.*

(b) There is an infinite set $\mathcal{A}$ such that $N-A(N)\gg N^{1/3}$ and $r_3(\mathcal{A},n)$ is monotone increasing for $n>n_0$

(c) If

$$\lim_{N\to\infty}\frac{N-A(N)}{\log N}=+\infty$$

then $r_2(\mathcal{A},n)$ cannot be increasing from a certain point on. (See also Balasubramanian [2].)

But we still do not have the answer for

Problem 3.1. Does there exist an infinite set $\mathcal{A}$ such that $\mathbb{N}-\mathcal{A}$ is infinite and $r_2(\mathcal{A},n)$ is increasing from a certain point on?

As Theorem 4.3 below shows, it may change the nature of the problem completely if a "thin" set of sums can be neglected. Here we mention two problems of this type:

Problem 3.2. Does there exist a set $\mathcal{A} \subset \mathbb{N}$ such that $\mathbb{N} - \mathcal{A}$ is infinite and

$$r_1(\mathcal{A}; n+1) \geq r_1(\mathcal{A}, n)$$

holds on a sequence of integers n whose density is 1? If such a set exists, then how "dense" can $\mathbb{N} - \mathcal{A}$ be?

Problem 3.3. Does there exist an arithmetic function f satisfying $f(n) \to \infty$,
$f(n+1) \geq f(n)$ for $n > n_0$, and $f(n) = o\left(\frac{n}{(\log n)^2}\right)$ and a set $\mathcal{A}$ such that

$$|r_1(\mathcal{A}, n) - f(n)| = o\left((f(n))^{1/2}\right)$$

holds on a sequence of integers n whose density is 1?

Next we studied the following problem: for which sets $\mathcal{A} \subset \mathbb{N}$ is $|r_1(\mathcal{A}, n+1) - r_1(\mathcal{A}, n)|$ bounded? Since we have recently given a survey [21] of these results, thus we do not present further details here.

We complete this section by adding two problems that the first author of this paper could not settle in [34].

Problem 3.4. Is it true that if $a_1 < a_2 \dots$ and $b_1 < b_2 < \dots$ are infinite sets of positive integers with

$$\lim_{k \to +\infty} \frac{a_k}{b_k} = 1$$

and $c > 0$, then

$$|\{(i,j): a_i + b_j \leq N\}| = cN + O(1)$$

cannot hold?

Problem 3.5. Is it true that if $a_1 < a_2 < \dots$ is an infinite set of positive integers with

$$a_{k+1} - a_k \gg a_k^{1/2}$$

and $f(n)$ is a "nice" function (say, its second difference $f(n+2) - 2f(n+1) + f(n) \geq 0$) with

$$n \ll f(n) \ll n^{1+\varepsilon} ,$$

then

$$|\{(i,j): 0 < |a_i - a_j| \leq N\}| = f(N) + O(1)$$

cannot hold?

(This would cover Dirichlet's divisor problem in the same way as the Erdős–Fuchs theorem covers the circle problem.)

4. A conjecture of Erdős and Turán and related problems and results

In 1941 Erdős and Turán [22] formulated the following attractive conjecture:

Conjecture 4.1 (Erdős and Turán [22]). If $\mathcal{A} \subset \mathbb{N}$ and $r_1(\mathcal{A}, n) > 0$ for $n > n_0$ (i.e., $\mathcal{A}$ is an asymptotic basis of order 2), then $r_1(\mathcal{A}, n)$ cannot be bounded:

$$\limsup_{n \to +\infty} r_1(\mathcal{A}, n) = +\infty \ . \tag{4.1}$$

This harmlessly looking conjecture proved to be extremely difficult: since 1941 no serious advance has been made. Erdős and Turán formulated an even stronger conjecture:

Conjecture 4.2 (Erdős and Turán [22]). If $a_1 < a_2 < \dots$ is an infinite sequence of positive integers such that for some $c > 0$ and all $k \in \mathbb{N}$ we have $a_k < ck^2$, then (4.1) holds.

Erdős and Fuchs [12] remarked that having the same assumptions as in Conjecture 4.2, the mean square of $r_1(\mathcal{A}, n)$ can be bounded: there are a $c > 0$ and an infinite set $\mathcal{A} \subset \mathbb{N}$ such that $a_k < ck^2$ for all $k \in \mathbb{N}$ and

$$\limsup_{N \to +\infty} \frac{1}{N} \left(\sum_{n=1}^{N} r_1^2(\mathcal{A}, n) \right) < +\infty \ . \tag{4.2}$$

Answering a question of Erdős, Ruzsa has proved recently the analogous result in connection with Conjecture 1:

Theorem 4.1 (Ruzsa, [32]). *There is an infinite set $\mathcal{A} \subset \mathbb{N}$ such that $r_1(\mathcal{A}, n) > 0$ for all $n > n_0$ and (4.2) holds.*

If Conjecture 1 is true, then assuming that $\mathcal{A} \subset \mathbb{N}$, $\mathcal{A}$ is infinite and $r_2(\mathcal{A}, n)$ is bounded, the function $r_2(\mathcal{A}, n)$ must assume the value 0 infinitely often. Erdős and Freud [11] conjectured that having the same assumptions, $r_2(\mathcal{A}, n)$ must assume also the value 1 infinitely often, i.e., there are infinitely many integers $n \in \mathcal{S}(\mathcal{A})$ whose representation in the form

$$a + a' = n, \qquad a, a' \in \mathcal{A}, \qquad a \le a' \tag{4.3}$$

is unique. This attractive conjecture seems to be true although probably it is very difficult. Moreover, they write "Probably there are "more" integers n with a unique representation of the form (4.3) than integers n with more than one representation." We will show that this is not so; at least for $\mathcal{A} \in B_2(g)$, $g \ge 3$.

Theorem 4.2. *For every $g \in \mathbb{N}$, $g \geq 2$ there is an infinite set $\mathcal{A} \subset \mathbb{N}_0$ such that $\mathcal{A} \in B_2[g]$ and for $\varepsilon > 0$, $n > n_0$ we have*

$$|\{n: n \leq N,\ r_2(\mathcal{A}, n) = 1\}| < (1+\varepsilon)\frac{2}{2g-3}|\{n: n \leq N,\ r_2(\mathcal{A}, n) > 1\}| . \tag{4.4}$$

Proof. Let $\mathcal{E} = \{e_1, e_2, \ldots\}$ be an infinite Sidon set, and define $\mathcal{A}$ by

$$\mathcal{A} = 2g \times \mathcal{E} + \{0, 1, \ldots, g-1\} .$$

We will show that this set $\mathcal{A}$ has the desired properties:

(i) $\mathcal{A} \in B_2[g]$,
(ii) $\mathcal{A}$ satisfies (4.4).

If $r_2(\mathcal{A}, n) \geq 1$ for some $n \in \mathbb{N}$, i.e., $n \in \mathcal{S}(\mathcal{A})$, then, by the construction of the set $\mathcal{A}$, n can be represented in the form

$$(2ge + i) + (2ge' + j) = 2g(e + e') + (i + j) = n \tag{4.5}$$

where

$$e, e' \in \mathcal{E} , \tag{4.6}$$

$$0 \leq i, j \leq g - 1 , \tag{4.7}$$

$$2ge + i \leq 2ge' + j , \tag{4.8}$$

and $r_2(\mathcal{A}, n)$ is equal to the number of integers e, e', i, j satisfying (4.5), (4.6), (4.7) and (4.8). It follows from (4.7) and (4.8) that

$$e \leq e' \tag{4.9}$$

and

$$0 \leq i + j \leq 2g - 2 . \tag{4.10}$$

Define the integers u, v by

$$n = 2gu + v, \qquad 0 \leq v < 2g . \tag{4.11}$$

Then it follows from (4.5), (4.10) and (4.11) that

$$e + e' = u \tag{4.12}$$

and

$$i + j = v \tag{4.13}$$

(where $v \leq 2g - 2$). Since $\mathcal{E}$ is a Sidon set, (4.9) and (4.12) determine e and e' uniquely. Thus $r_2(\mathcal{A}, n)$ is equal to the number of pairs (i, j) satisfying (4.7), (4.8) and (4.13). If $e < e'$, then (4.8) holds automatically, and the number of solutions of (4.7) and (4.8) is $v + 1$ for $v \leq g - 1$ and $2g - v - 1$ for $g - 1 < v \leq 2g - 2$. Denote the set of the integers n that can be represented in the form

$$n = 2g(e+e') + i \qquad (\text{where } e < e',\ e, e' \in \mathcal{E}\ ) \tag{4.14}$$

with $i = 0$ or $2g-2$ by $\mathcal{K}$, and let $\mathcal{L}$ denote the set of the integers n of form (4.14) with $1 \le i \le 2g-3$. Then it follows from the discussion above that

$$r_2(\mathcal{A}, n) \begin{cases} = 1 & \text{for } n \in \mathcal{K} \\ > 1 & \text{for } n \in \mathcal{L} \end{cases} \tag{4.15}$$

and clearly we have

$$K(n) = \frac{2}{2g-3} L(n) + O(1)\ . \tag{4.16}$$

Finally, if $r_2(\mathcal{A}, n) \ge 1$ and $n \notin \mathcal{K} \cup \mathcal{L}$, then n can be represented in the form

$$n = 2ge + v \quad \text{with } e \in \mathcal{E}, \quad 0 \le v \le 2g-2;$$

let $\mathcal{M}$ denote the set of the integers n of this form. Clearly,

$$M(n) = o(K(n))\ . \tag{4.17}$$

It follows from (4.15), (4.16), (4.17) and

$$\{n : n \in \mathbb{N},\ r_2(\mathcal{A}, n) \ge 1\} = \mathcal{K} \cup \mathcal{L} \cup \mathcal{M}$$

that

$$|\{n : n \le N,\ r_2(\mathcal{A}, n) = 1\}| = (1 + o(1)) \frac{2}{2g-3} |\{n : n \le N,\ r_2(\mathcal{A}, n) > 1\}|$$

which completes the proof of the theorem.

By Theorem 4.2, it is not true that if $r_2(\mathcal{A}, n)$ is bounded, then

$$r_2(\mathcal{A}, n) = 1 \tag{4.18}$$

holds more often than

$$r_2(\mathcal{A}, n) > 1\ .$$

On the other hand, we think that (4.18) must hold for a positive percentage of the elements of $\mathcal{S}(\mathcal{A})$:

Problem 4.1. Show that if $\mathcal{A} \subset \mathbb{N}$ is an infinite set such that $r_2(\mathcal{A}, n)$ is bounded, then we have

$$\limsup_{n \to +\infty} \frac{|\{n : n \le N,\ r_2(\mathcal{A}, n) = 1\}|}{S(\mathcal{A}, N)} > 0 \tag{4.19}$$

Note that it could be shown that the lim sup in (4.19) cannot be replaced by lim inf.

Moreover, if (4.19) is true, then for sets $\mathcal{A} \in B_2[g]$ one might like to give a lower bound in terms of g for the lim sup in (4.19). Perhaps Theorem 4.2 is close to the truth so that this lim sup is $\gg \frac{1}{g}$. The special case $g = 2$ seems to be the most interesting and, perhaps, in this case there is a good chance for a reasonable lower bound:

Problem 4.2. Assuming, that $\mathcal{A} \subset \mathbb{N}$ is an infinite set with $\mathcal{A} \in B_2[2]$, i.e., $r_2(\mathcal{A}, n) \leq 2$ for all n, give a lower bound for

$$\limsup_{n \to +\infty} \frac{|\{n\colon n \leq N,\ r_2(\mathcal{A}, n) = 1\}|}{|\{n\colon n \leq N,\ r_2(\mathcal{A}, n) = 2\}|} .$$

By Theorem 4.2, this lim sup can be ≤ 2; is it true, that it is always ≥ 2?

By our conjecture formulated in Problem 4.1, the assumption

$$r_2(\mathcal{A}, n) = O(1) \tag{4.20}$$

implies that $r_2(\mathcal{A}, n) = 1$ must hold for a positive percentage of the elements of $\mathcal{S}(\mathcal{A})$. First we thought that (4.20) can be replaced by the weaker condition that $r_2(\mathcal{A}, n)$ is bounded apart from a "thin" set of integers n and still the same conclusion holds. Now we will show that this is not so and, indeed, for every finite set $U \subset \mathbb{N}$ there is a set $\mathcal{A}$ such that, apart from a "thin" set of integers n, $r_2(\mathcal{A}, n)$ assumes only the prescribed values $u \in U$ with about the same frequency.

For $\mathcal{A} \subset \mathbb{N}_0$, $u \in \mathbb{N}$ denote the set of the integers $n \in \mathbb{N}$ with

$$r_2(\mathcal{A}, n) = u$$

by $\mathcal{S}_u(\mathcal{A})$ so that $\mathcal{S}(\mathcal{A}) = \bigcup_{u=1}^{+\infty} \mathcal{S}_u(\mathcal{A})$.

Theorem 4.3. *Let $k \in \mathbb{N}$ and let $u_1 < u_2 < \ldots < u_k$ be positive integers. Then there is an infinite set $\mathcal{A} \subset \mathbb{N}_0$ such that writing*

$$\mathcal{B} = \mathbb{N} \setminus \left(\cup_{i=1}^{k} \mathcal{S}_{u_i}(\mathcal{A})\right)$$

we have

$$S_{u_i}(\mathcal{A}, N) = \frac{N}{k} + O(N^{\alpha})$$

and

$$B(N) = O(N^{\alpha})$$

where $\alpha = \frac{\log 3}{\log 4}$.

(Here $S_{u_i}(\mathcal{A}, N)$ denotes the counting function of $\mathcal{S}_{u_i}(\mathcal{A})$.)

Thus, e.g., there is a set $\mathcal{A}$ such that $r_2(\mathcal{A}, n) = 2$ for all but $O(N^{\alpha})$ values of n with $n \leq N$.

Proof. The proof will be based on the following lemma:

Lemma 4.1. *Let $\mathcal{F}$ and $\mathcal{G}$ denote the set of the non-negative integers that can be represented in the form $\sum_{i=0}^{m} \varepsilon_i 2^{2i}$, resp. $\sum_{i=0}^{m} \varepsilon_i 2^{2i+1}$ where $\varepsilon_i = 0$ or 1 for all i, and write $\mathcal{H} = \mathcal{F} \cup \mathcal{G}$. Then*

(i) every $n \in \mathbb{N}$ has a unique representation in the form

$$f + g = n, \quad f \in \mathcal{F}, \quad g \in \mathcal{G};$$

(ii) $S(\mathcal{F},N)=O(N^{\alpha})$;
(iii) $S(\mathcal{G},N)=O(N^{\alpha})$;
(iv) we have

$$|\{n: n\in\mathbb{N},\ r_2(\mathcal{H},n)>1\}|=O(N^{\alpha})\ .$$

Proof. (i) is trivial.

(ii) follows from the fact that if $n\in\mathcal{S}(\mathcal{F})$, then representing n in the form $n=\sum_{i=0}^{m}\varepsilon_i 4^i$ where $\varepsilon_i=0,1,2$ or 3, we have $0\le\varepsilon_i\le 2$ for all i, i.e., the digit 3 is missing.

(iii) follows from (ii) and $\mathcal{G}=2\times\mathcal{F}$.

Finally, (iv) follows from (i), (ii) and (iii), and this completes the proof of the lemma.

Now we will construct a set $\mathcal{A}$ of the desired properties. Denote the elements of the set $\mathcal{G}$ (defined in Lemma 4.1) by $(0=)g_1<g_2<\dots$, write $\mathcal{G}_i=\{g_1,g_2,\dots,g_{u_i}\}$ and $\mathcal{L}_i=k\times(\mathcal{F}+\mathcal{G}_i)+\{i\}$ for $i=1,2,\dots,k$, and finally, let $\mathcal{A}=\left(\bigcup_{i=1}^{k}\mathcal{L}_i\right)\bigcup(k\times\mathcal{G})$. Clearly, it suffices to show that

(i) if $i\in\{1,2,\dots,k\}$, $n\in\mathbb{N}$, $n\equiv i \pmod k$ and n is large enough (depending on u_i), then n has exactly u_i representations as the sum of an element of $\bigcup\limits_{j=k}^{k}\mathcal{L}_i$ and an element of $k\times\mathcal{G}$;

(ii) for $1\le i\le j\le k$ we have

$$|\{n: n\le N,\ n\in\mathcal{L}_i+\mathcal{L}_j\}|=O(N^{\alpha});$$

(iii) $S(k\times\mathcal{G},N)=O(N^{\alpha})$.

To prove (i), define m by $n=km+i$, and consider a representation of n in the desired form:

$$\ell+kg=n=km+i,\quad \ell\in\bigcup_{j=1}^{k}\mathcal{L}_j,\quad g\in\mathcal{G}\ , \tag{4.21}$$

By the definition of the sets $\mathcal{L}_j$, we have $\ell\in\mathcal{L}_j$ if and only if

$$\ell=k(f+g_t)+j \tag{4.22}$$

for some $f\in\mathcal{F}$, $1\le t\le u_j$. It follows from (4.21) and (4.22) that

$$k(f+g_t+g)+j=km+i\ . \tag{4.23}$$

By $1\le i,\ j\le k$, this implies that $i=j$. Thus (4.23) can be written in the equivalent form

$$f+g=m-g_t\ .$$

By (i) in Lemma 4.1, for $m>g_{u_i}$ and each of $t=1,2,\dots,u_i$, this equation has exactly one solution in f and g. Again by (i) in Lemma 1, these u_i pairs (f,g) determine distinct solutions (ℓ,g) of (4.21).

To complete the proof of (i), it remains to show that distinct pairs (ℓ, g), (ℓ', g') satisfying (4.21) (also with (ℓ', g') in place of (ℓ, g)) determine distinct representations of n if n is large enough, i.e., if

$$\ell + kg = n = \ell' + kg' \tag{4.24}$$

and n is large, then $\ell \neq kg'$, $\ell' \neq kg$. Indeed, assume that contrary to this statement we have

$$\ell = kg', \quad \ell' = kg . \tag{4.25}$$

Then by (4.24) and (4.25), $\ell + \ell' = n$. Hence

$$\ell \geq n/2 \tag{4.26}$$

or $\ell' \geq n/2$; we may assume that (4.26) holds. By (4.22) and (4.25) we have

$$\ell = k(f + g_t) + j = kg' . \tag{4.27}$$

By $1 \leq j \leq k$, it follows that $j = k$. Thus (4.27) implies

$$f + g_t + 1 = g' . \tag{4.28}$$

By (4.22) and (4.26), we have

$$f \longrightarrow +\infty \quad \text{as} \quad n \longrightarrow +\infty . \tag{4.29}$$

It is easy to see that

$$\lim_{x \longrightarrow +\infty} \min_{\substack{f \in \mathcal{F}, g \in \mathcal{G}, \\ f, g > x}} |f - g| = +\infty . \tag{4.30}$$

By (4.29) and (4.30), (4.28) cannot hold for $t \leq u_k$ and large n. This contradiction completes the proof of (i).

To prove (ii), observe that $n \in \mathcal{L}_i + \mathcal{L}_j$ implies that

$$n \in k \times (\mathcal{F} + \mathcal{G}_i) + \{i\} + k \times (\mathcal{F} + \mathcal{G}_j) + \{j\} = k \times \mathcal{S}(\mathcal{F}) + (\{i+j\} + k \times \mathcal{G}_i + k \times \mathcal{G}_j) .$$

Here $\{i+j\} + k \times \mathcal{G}_i + k \times \mathcal{G}_j$ is a finite set (in fact, it has at most u_k^2 elements). Thus (ii) follows from Lemma 4.1 (ii).

Finally, by $\mathcal{S}(k \times \mathcal{G}) = k \times \mathcal{S}(\mathcal{G})$, (iii) follows from Lemma 4.1 (ii).

Remark 4.1. Let $r_i \in Q^+$, $1 \leq i \leq k$ with $\sum_{i=1}^{k} r_i = 1$. Using the same idea as in the proof of Theorem 4 we can prove the existence of an infinite set $\mathcal{A} \subset \mathbb{N}_0$ for which

$$S_{u_i}(\mathcal{A}, N) = r_i N + O(N^\alpha) \qquad 1 \leq i \leq 1$$

with some $0 < \alpha < 1$. It seems likely that an analogous theorem holds with arbitrary given densities λ_i, $1 \leq i \leq k$, in place of r_i. If so, the proof will be more involved.

5. Sidon-sets: The Erdős - Turán theorem, related problems and results

In 1932 Sidon [36] in connection with his work in Fourier-analysis considered power series of type $\sum_{i=1}^{\infty} z^{a_i}$ when $\left(\sum_{i=1}^{\infty} z^{a_i}\right)^h$ is of bounded coefficients. This led tô the investigation of finite and infinite sequences (a_i) with the property that for g fixed the number of solutions

$$a_{i_1} + \ldots + a_{i_k} = n$$

is bounded by g for $n \in N$.

Sidon sequences correspond to the case $h = 2$ and $g = 1$, i.e. $r_2(\mathcal{A}, n) \leq 1$. Recall that for $g \in \mathbb{N}$, $B_2(g)$ denotes the class of all (finite or infinite) sets $\mathcal{A} \subset \mathbb{N}_0$ such that for all $n \in \mathbb{N}$ we have $r_2(\mathcal{A}, n) \leq g$.

Some specific lines of investigations are the following:

a) For $\mathcal{A} \in \mathcal{B}_2(g)$ and $\mathcal{A} \subset [1, \ldots, N]$ how large $|\mathcal{A}|$ can be? In the infinite case how fast the counting function $A(n)$ can grow?

b) what can we say about the structure of $\mathcal{A}$ resp. $\mathcal{A} + \mathcal{A}$ if $|\mathcal{A}|$ resp. $A(n)$ is large?

There is an excellent account on this subject in Halberstam - Roth [23] and also a recent survey Erdős - Freud [11].

While there are many results on Sidon sets, much less is known on sets $\mathcal{A} \in B_2[g]$. In particular, let $F(N, g)$ denote the cardinality of the largest set $\mathcal{A} \in B_2[g]$ selected from $\{1, 2, \ldots, N\}$. Chowla [4], Erdős and Turán [7], [22] gave quite sharp estimates for the cardinality of the largest Sidon set selected from $\{1, 2, \ldots, N\}$:

$$N^{1/2} - O(N^{5/16}) < F(N, 1) < N^{1/2} + O(N^{1/4}) \ . \qquad (5.1)$$

On the other hand, very little is known on $F(N, g)$ for $g > 1$. Clearly we have

$$F(N, g) \geq F(N, 1) \qquad \left(= (1 + o(1))N^{1/2}\right)$$

for all $g \in \mathbb{N}$. Erdős and Freud [11] showed that $F(N, 2) \geq 2^{1/2}N^{1/2}$. On the other hand, a trivial counting argument gives

$$F(N, g) \leq 2g^{1/2}N^{1/2} \ .$$

Problem 5.1. Show that for all $g \in \mathbb{N}$ the limit $\lim\limits_{N \to +\infty} F(N, g)N^{-1/2}$ exists, and determine the value of this limit. In particular, estimate $F(N, 2)$.

Further, very little is known on sets $\mathcal{A} \in B_2[g]$ and their Sidon subsets. Erdős, resp. Ruzsa (see [7]) studied the size of Sidon sets selected from given sets $\mathcal{A} \in B_2[g]$.

A related problem is the following:

Problem 5.2. Is it true that for $g \geq 2$, every Sidon set selected from $\{1, 2, \ldots, N\}$ can be embedded into a much greater set $\mathcal{A} \in B_2[g]$ selected from $\{1, 2, \ldots, N\}$?

In other words, if $\mathcal{A} \subset \{1, 2, \ldots, N\}$ is a Sidon set, then let $H(\mathcal{A}, N, g)$ denote the cardinality of the greatest set $\mathcal{E}$ such that $\mathcal{E} \in B_2[g]$, $\mathcal{E} \subset \{1, 2, \ldots, N\}$ and $\mathcal{A} \subset \mathcal{E}$. Is it true that writing $K(N, g) = \min(H(\mathcal{A}, N, g) - |\mathcal{A}|)$, where the minimum is taken over all Sidon sets $\mathcal{A}$ selected from $\{1, 2, \ldots, N\}$, we have

$$\lim_{N \to +\infty} K(N, 2) = +\infty \text{ ?}$$

How fast does the function $K(N, g)$ grow in terms of N? Is it true that

$$\lim_{N \to +\infty} (K(N, g+1) - K(N, g)) = +\infty \qquad \text{for all} \qquad g \in \mathbb{N} \text{ ?}$$

A Sidon set $\mathcal{A} \subset \{1, 2, \ldots, N\}$ is said to be *maximal* if there is no integer b such that $b \in \{1, 2, \ldots, N\}$, $b \notin \mathcal{A}$ and $\mathcal{A} \cup \{b\}$ is a Sidon set. (Note that very little is known on the cardinality of maximal Sidon sets; see Problem 15 in [15].) Another problem closely related to Problem 5.2:

Problem 5.3. Does there exist a *maximal* Sidon set such that it can be embedded into a much larger set $\mathcal{E} \in B_2[g]$?

In other words, let $L(N, g) = \max(H(\mathcal{A}, N, g) - |\mathcal{A}|)$ where $H(\mathcal{A}, N, g)$ is the function defined in Problem 5.2 and the maximum is taken over all *maximal* Sidon sets selected from $\{1, 2, \ldots, N\}$. Is it true that

$$\lim_{N \to +\infty} L(N, 2) = +\infty?$$

Is it true that

$$\lim_{N \to +\infty} (L(N, g+1) - L(N, g)) = +\infty$$

for all $g \in \mathbb{N}$?

As Section 4 also shows, it may change the nature of the problem completely if a "thin" set of sums can be neglected. Several problems of this type are:

Problem 5.4. How large set $\mathcal{A}$ can be selected from $\{1, 2, \ldots, N\}$ so that it is an "almost Sidon set" in the sense that

$$|\mathcal{S}(\mathcal{A})| = (1 + o(1)) \binom{|\mathcal{A}|}{2} \text{ ?} \tag{5.2}$$

It follows from a construction of Erdős and Freud [11] that there is a set $\mathcal{A}$ such that $\mathcal{A} \subset \{1, 2, \dots, N\}$, (5.2) holds and

$$|\mathcal{A}| > \left(\frac{2}{\sqrt{3}} + o(1)\right) N^{1/2}, \tag{5.3}$$

so that $|\mathcal{A}|$ can be much greater than $F(N, 1) = (1 + o(1))N^{1/2}$ (see (5.1)).

In the infinite case much less is known than in the finite case. Beyond what follows from (5.1), Erdős proved

Theorem 5.1 (Stöhr [38]). *There is an absolute constant $c > 0$, such that for every (infinite) Sidon-sequence $\mathcal{A}$*

$$A(n) < c(n/\log n)^{1/2}$$

holds infinitely often.

On the other hand, Krückeberg, improving a result of Erdős, proved in 1961

Theorem 5.2. *There is an (infinite) Sidon-sequence $\mathcal{A}$ such that*

$$A(n) > \frac{1}{\sqrt{2}} n^{1/2}$$

holds infinitely often.

It is not known whether or not the factor $1/\sqrt{2}$ is best possible. The greedy algorithm gives the existence of an (infinite) Sidon-sequence for which

$$A(n) > n^{1/3} \text{ for all } n \ .$$

Ajtai, Komlós and Szemerédi improved this [1]: There is a Sidon- sequence $\mathcal{A}$ such that

$$A(n) > c(n \log n)^{1/3} \text{ for all } n \geq n_0 \ .$$

Weak Sidon sets

We considered Sidon sets defined by

$$r_2(\mathcal{A}, n) \leq 1 \tag{5.4}$$

which means that we require

$$x + y \neq u + v \tag{5.5}$$

for any $x, y, u, v \in \mathcal{A}$ of which at least three are different.

In connection with some particular problems it is more appropriate to consider Sidon-sets where we require (5.5) only for $x, y, u, v \in \mathcal{A}$ where all four are distinct. (So we may have an arithmetic progression of length three, a solution of $x + y = 2u$.)

If

$$r_3(\mathcal{A}; n) \leq 1 \tag{5.6}$$

holds, $\mathcal{A}$ is called a weak Sidon set.

It is easy to see that the maximum size of Sidon set resp. of a weak Sidon set in [1,N] are asymptotically the same.

A problem of Erdős on the distribution of distances in the plane led us to formulate the following question:

Let $\mathcal{A}^*$ be a weak Sidon-set. How large Sidon-set $\mathcal{A}$ must be contained by $\mathcal{A}^*$?

Another formulation of the problem is:

Suppose that for $\mathcal{A}^* \subset [1, N]$ any four distinct $a_{i_1}, a_{i_2}, a_{i_3}, a_{i_4} \in \mathcal{A}^*$ determine at least five distinct differences:

$$|\{|a_{i_\nu} - a_{i_\mu}|, \quad 1 \leq \nu < \mu \leq 4\}| \geq 5 \,.$$

Let $h(\mathcal{A}^*)$ denote the cardinality of the largest Sidon set $\mathcal{A} \subseteq \mathcal{A}^*$.

Let

$$f(m) = \min_{|\mathcal{A}^*|=m} h(\mathcal{A}^*)$$

If $\mathcal{A}^*$ is a weak Sidon set, then for each $a \in \mathcal{A}^*$ there is at most one pair $b, c \in \mathcal{A}^*$ such that $b + c = 2a$. This implies that

$$f(m) \geq \frac{1}{2}m \,,$$

Gyárfás and Lehel [27] proved that with some absolute constant $\delta > \frac{1}{100}$

$$\left(\frac{1}{2} + \delta\right) m \leq f(m) \leq \frac{3}{5}m + 1 \,.$$

Problem 5.5. Prove that $\lim\limits_{m\to\infty} \frac{f(m)}{m}$ exists and determine the limit.

It is very probably that a dense weak Sidon set contains a Sidon set of almost the same size:

Problem 5.6. Suppose $\mathcal{A}^* \subset [1, N]$ and $m = |\mathcal{A}^*| > \varepsilon N^{1/2}$. Is it true that

$$h(\mathcal{A}^*) > \delta(\varepsilon) N^{1/2}$$

where $\delta \to 1$ if $\varepsilon \to 1$?

Remark 5.1. The problem of Sidon-sets resp. weak Sidon-sets is related to anti-Ramsey type problems.

Consider the complete graph K_N with vertex set $V(K_N) = \{1, \ldots, N\}$ and an edge-coloring φ: $[V]^2 \to V$ where $\varphi(a, b) = |a - b|$. A Sidon-set $\mathcal{A} \subseteq V$ is the vertex set of a so-called totally multicolored complete subgraph (where *all* the edges have different colors).

A weak Sidon set $\mathcal{A}^* \subseteq V$ corresponds to the vertex set of a complete subgraph where *independent* edges have different colors.

6. Difference-sets

Above we considered mostly sums $a + a'$. One might like to study the analogues of some of these problems with differences $a - a'$ in place of sums $a + a'$.

Problem 6.1. In [19] and [20] we studied the structure of the sum set $\mathcal{S}(\mathcal{A})$ of Sidon sets $\mathcal{A}$. What can be said about the structure of the difference set $\mathcal{D}(\mathcal{A})$ of Sidon sets $\mathcal{A}$; in particular,

a) what can be said about the number and length of blocks of consecutive integers in $\mathcal{D}(\mathcal{A})$,

b) about the size of the gaps between the consecutive elements of $\mathcal{D}(\mathcal{A})$, etc.?

Another closely related problem:

In [19] we studied the solvability of the equation

$$\mathcal{D}(\mathcal{A}) = \mathcal{B}$$

for fixed sets $\mathcal{B} \subset \mathbb{N}$ and, in particular, we gave a quite general sufficient condition for the solvability of this equation and in fact we showed that under quite general circumstances, not only the elements of the difference set $\mathcal{D}(\mathcal{A})$, but also the number of solutions of

$$a - a' = b, \qquad a, a' \in \mathcal{A}$$

(for all $b \in \mathcal{B}$) can be prescribed. The nature of the problem completely changes if we restrict ourselves to Sidon sets $\mathcal{A}$.

Problem 6.2. Find possibly general conditions such that for sets $\mathcal{B} \subset \mathbb{N}$ satisfying these conditions, there is a *Sidon set* $\mathcal{A}$ whose difference set is the given set $\mathcal{B}$.

One might like to see what is the connection between the behavior of sums and differences (see Ruzsa [33] for a related result):

Problem 6.3. Consider finite sets $\mathcal{A}$ such that

$$a - a' = d, \qquad a, a' \in \mathcal{A}$$

has at most two solutions for all $d \in \mathbb{N}$. What can be said about the size of the Sidon sets, respŝets $\mathcal{A} \in B_2[2]$ selected from such a set $\mathcal{A}$?

Problem 6.4. Do there exist numbers $\delta > 0, N_0$ such that for $N > N_0$ there is a set $\mathcal{A} \subset \{1, 2, \dots, N\}$ for which

$$|\mathcal{A}| > (1 + \delta)N^{1/2}$$

and both

$$\begin{aligned} a - a' &= d, \quad a, a' \in \mathcal{A} \\ a + a' &= n, \quad a, a' \in \mathcal{A}, \quad a \leq a' \end{aligned}$$

have at most two solutions for all $d \in \mathbb{N}$, $\rtimes \in \mathbb{N}$?

7. Generalizations

So far we have studied sums $a+a'$ and differences $a-a'$. Already in these two cases the difficulty of problems and the results can be completely different. It is even more so if we consider the linear form $ca+c'a'$, or more generally $f(a_1,\dots,a_k)=c_1a_1+\dots+c_ka_k$ where $c_i\in\mathbb{Z}$ for $1\le i\le k$ and the c_i's are fixed.

This is indicated already by the following simple but important example.

Example of Ruzsa. Let $\mathcal{A}=\{a\colon a=\sum\limits_{i=0}^{\infty}\varepsilon_i 2^{2i},\ \ \varepsilon_i=0 \text{ or } 1\}$. Then for $n\in\mathbb{N}$ the number of solutions

$$a+2a'=n, \qquad a,a'\in\mathcal{A},$$

is 1 for any $n\in\mathbb{N}$.

This shows that the behavior of the representation functions depends very much on the coefficients of the linear form. Here we formulate only a few questions by extending the problems we discussed above.

Problem 7.1. For which $(c_1,\dots,c_k)$ can the representation-function $R(\mathcal{A},c_1,\dots,c_k;n)$, counting the number of solutions of $c_1a_1+\dots+c_ka_k=n$ $(a_1,\dots,a_k\in\mathcal{A})$, be constant for $n>N_0$?

Problem 7.2. For which $(c_1,\dots,c_k)$ is there an Erdős-Fuchs type result, analogous to Theorem 3.1 and (3.2)?

Problem 7.3. For which linear forms is there an Erdős- Sárközy [15] type result, when $R_1(\mathcal{A},c_1,\dots,c_k;n)$ cannot be too close to a "nice" function?

Problem 7.4. When and how the results on the monotonicity of $r_i(\mathcal{A};n)$ (see Theorem 3.3) can be extended to the linear form $c_1a+\dots+c_ka_k$?

One may generalize these problems even further by studying *polynomials* $f(a_1,a_2,\dots,a_k)$. In particular, very little is known on *products* aa'. Erdős [7] estimated the cardinality of sets $\mathcal{A}$ such that $\mathcal{A}\subset\{1,2,\dots,N\}$ and all the products aa' with $a,a'\in\mathcal{A}$, $a\le a'$ are distinct. Moreover he [7] studied the multiplicative analogue of the Erdős-Turán conjecture mentioned in Section 2. Three further problems involving products are:

Problem 7.5. For $\mathcal{A}\in\mathbb{N}$, $n\in\mathbb{N}$, let $s(\mathcal{A},n)$ denote the number of solution of the equation

$$aa'=n, \quad a,a'\in\mathcal{A}, \quad a\le a'\ .$$

Characterize the regularity properties of this function $s(\mathcal{A},n)$ analogously as in the papers [14], [15], [16], [17], [18] where we discussed the additive analogue of this problem by studying $r_1(\mathcal{A},n)$, $r_2(\mathcal{A},n)$, $r_3(\mathcal{A},n)$. In particular, how well can one approximate $s(\mathcal{A},n)$ by a "nice" arithmetic function $f(n)$?

Problem 7.6. Find multiplicative analogue of the conjecture of Erdős and Freud mentioned in Section 2 and, perhaps, this can be attacked more easily. In other words, is it true that if $\mathcal{A} \subset \mathbb{N}$ is an infinite set such that the function $s(\mathcal{A}, n)$ defined in Problem 6.2 is bounded, then $s(\mathcal{A}, n) = 1$ for infinitely many values of n?

Problem 7.7. Roth [30], [31], Heath-Brown [26], Szemerédi [39] and others estimated the cardinality of sets $\mathcal{A} \subset \{1, 2, \dots, N\}$ not containing three-term arithmetic progressions. Find a multiplicative analogue of this problem: estimate the cardinality of the largest set $\mathcal{A} \subset \{1, 2, \dots, N\}$ not containing three term geometric progressions, i.e.,

$$a_1 a_2 = a_3^2, \qquad a_1, a_2, a_3 \in \mathcal{A}$$

implies that $a_1 = a_2 = a_3$. (Note that the square-free integers not exceeding N form a set $\mathcal{A}$ of this property.)

Ramsey-type problems

Many of the problems discussed above can be formulated in the following way: if $\mathcal{A}$ is a "dense" set of integers, then an equation of the form

$$f(a_1, a_2, \dots; a_k) = 0 \tag{7.1}$$

can be solved with $a_1, a_2, \dots, a_k \in \mathcal{A}$. There are several important results of the type where instead of considering solutions $a_1, a_2, \dots, a_k$ belonging to a "dense" set $\mathcal{A}$, we assume that a partition

$$\mathbb{N} = \bigcup_{i=1}^{\ell} \mathcal{A}^{(i)} \qquad (\mathcal{A}^{(i)} \cap \mathcal{A}^{(j)} = \emptyset \quad \text{for} \quad 1 \le i < j \le \ell) \tag{7.2}$$

of $\mathbb{N}$ is given, and then we are looking for "monochromatic" solutions of (10.1), i.e., for solutions $a_1, a_2, \dots, a_k$ such that all these a's belong to the same set $\mathcal{A}^{(i)}$; a result of this type can be called Ramsey type theorem. In particular, Schur [35] resp. van der Waerden [41] proved that the equation

$$a_1 + a_2 = a_3 \ ,$$

resp.

$$a_1 + a_2 = 2a_3, \qquad a_1 \ne a_2$$

has a monochromatic solution for every partition (7.2) of $\mathbb{N}$. (Indeed, van der Waerden proved the more general theorem that for every $k \in \mathbb{N}$ and every partition (7.2), there is a monochromatic arithmetic progression of k distinct terms.) It follows from these results that for every partition (7.2) both equations

$$a_1 a_2 = a_3$$

and

$$a_1 a_2 = a_3^2 \, , \qquad a_1 \neq a_2$$

have monochromatic solutions. (Indeed, in both cases there is a solution of the form $a_1 = 2^{b_1}$, $a_2 = 2^{b_2}$, $a_3 = 2^{b_3}$.)

Problem 7.8. Characterize the polynomials $f(a_1, a_2, \ldots, a_k)$ such that the equation (7.1) has a monochromatic solution for every partition of form (7.2) or, at least, find further polynomials $f(a_1, a_2, \ldots, a_k)$ with this property. In particular, does there exist an integer $m \geq 2$ such that the equation

$$a_1^2 + a_2^2 + \ldots + a_m^2 = a_{m+1}^2$$

has a monochromatic solution for every partition (7.2)?

8. Probabilistic methods. The theorems of Erdős and Rényi

In [36] Sidon asked the following question: Does there exist an $\mathcal{A} \subset \mathbb{N}$ s.t. $r_1(\mathcal{A}, n) \geq 1$ for all $n > n_0$, and $r_1(\mathcal{A}, n) = O(n^{\varepsilon})$? In 1956 Erdős gave an affirmative answer in the following sharper form:

Theorem 8.1 (Erdős [8]). *There is an infinite set $\mathcal{A} \subset \mathbb{N}$ such that*

$$c_1 \log n < r_1(\mathcal{A}, n) < c_2 \log n \qquad \text{for } n > n_0 \, .$$

Erdős proved this by a probabilistic argument. In fact, he proved that there are "many" sets $\mathcal{A} \subset \mathbb{N}$ with this property.

In 1960 Erdős and Rényi published an important paper in which, by using probabilistic methods, they proved several results on additive representation functions. The most interesting result is, perhaps, the following theorem:

Theorem 8.2 (Erdős and Rényi, [13]). *For all $\varepsilon > 0$, there is a $\lambda = \lambda(\varepsilon)$ such that there is an infinite $B_2[\lambda]$ set $\mathcal{A} \subset \mathbb{N}$ with*

$$A(n) > n^{1/2-\varepsilon} \qquad \text{for } n > n_0(\varepsilon) \, .$$

Note that for a $B_2[\lambda]$ set $\mathcal{A}$ we have $A(n) = O_\lambda(n^{1/2})$. Thus Theorem 8.2 provides a quite sharp answer to Sidon's first question, mentioned in Section 5.

Remarkably enough, this paper of Erdős and Rényi appeared in the same year as their paper written "On the evolution of random graphs" which had tremendous influence on graph theory and led to one of the most extensively investigated and comprehensive theories in graph theory. (See Bollobás [4].) On the other hand, the paper [13] was nearly unnoticed for about three decades.

The paper [13] of Erdős and Rényi was somewhat sketchy. In their monograph [15] Halberstam and Roth worked out the details. In [16], Erdős and Sárközy extended Theorem 8.1 by showing that if $f(n)$ is a "nice" function (e.g., combination of the functions n^α, $(\log n)^\beta$, $(\log\log n)^\gamma$) with $f(n) \gg \log n$, then there is an $\mathcal{A} \subset \mathbb{N}$ such that

$$|r_1(\mathcal{A}, n) - f(n)| \ll (f(n)\log n)^{1/2} .$$

(Compare this with their result [14] on equation (3.3).)

The really intensive work in this field started only about 2-3 years ago. Erdős, Nathanson, Ruzsa, Spencer and Tetali have proved several remarkable results. Since their papers have not appeared yet, some of them have not even been written up yet, it would be too early to survey their work here.

Remark 8.1. Many of the problems in additive number theory are or can be formulated for arbitrary groups, semigroups or for some specified structures, like for set systems. (An independent source for Sidon-type problems is for example coding theory.) We refer to a survey of V.T. Sós [36] on this subject.

References

1. M. Ajtai, J. Komlós, E. Szemerédi: A dense infinite Sidon-sequence, European J. Comb. 2 (1981), 1-11.
2. R. Balasubramanian, A note on a result of Erdős, Sárközy and Sós, Acta Arithmetica 49 (1987), 45-53.
3. P. T. Bateman, E. E. Kohlbecker and J. P. Tull, On a theorem of Erdős and Fuchs in additive number theory, Proc. Amer. Math. Soc. 14 (1963), 278-284.
4. B. Bollobás, Random graphs, Academic, New York, 1985.
5. S. Chowla, Solution of a problem of Erdős and Turán in additive number theory, Proc. Nat. Acad. Sci. India 14 (1944), 1-2.
6. G. A. Dirac, Note on a problem in additive number theory, J. London Math. Soc. 26 (1951), 312-313.
7. P. Erdős, Addendum, On a problem of Sidon in additive number theory and on some related problems, J. London Math. Soc. 19 (1944), 208.
8. P. Erdős, Problems and results in additive number theory, Colloque sur la Théorie des Nombres (CBRM) (Bruxelles, 1956), 127-137.
9. P. Erdős, On the multiplicative representation of integers, Israel J. Math. 2 (1964), 251-261.
10. P. Erdős, On some applications of graph theory to number theory, Publ. Ramanujan Inst. 1 (1969), 131-136.
11. P. Erdős and R. Freud, On Sidon-sequences and related problems, Mat. Lapok 1 (1991), 1-44 (in Hungarian).
12. P. Erdős and W. H. J. Fuchs, On a problem of additive number theory, J. London Math. Soc. 31 (1956), 67-73.

13. P. Erdős and A. Rényi, Additive properties of random sequences of positive integers, Acta Arithmetica 6 (1960), 83-110.
14. P. Erdős and A. Sárközy, Problems and results on additive properties of general sequences, I, Pacific J. 118 (1985), 347-357.
15. P. Erdős and A. Sárközy, Problems and results on additive properties of general sequences, II, Acta Math. Hung. 48 (1986), 201-211.
16. P. Erdős, A. Sárközy and V. T. Sós, Problems and results on additive properties of general sequences, III, Studia Sci. Math. Hung. 22 (1987), 53-63.
17. P. Erdős, A. Sárközy and V. T. Sós, Problems and results on additive properties of general sequences, IV, in: Number Theory, Proceedings, Ootacamund, India, 1984, Lecture Notes in Mathematics 1122, Springer-Verlag, 1985; 85-104.
18. P. Erdős, A. Sárközy and V. T. Sós, Problems and results on additive properties of general sequences, V, Monatshefte Math. 102 (1986), 183-197.
19. P. Erdős, A. Sárközy and V. T. Sós, On sum sets of Sidon sets, I, J. Number theory, to appear.
20. P. Erdős, A. Sárközy and V. T. Sós, On sum sets of Sidon sets, II, Israel J. Math., to appear.
21. P. Erdős, A. Sárközy and V. T. Sós, On additive properties of general sequences, Ann. Discrete Math., to appear.
22. P. Erdős and P. Turán, On a problem of Sidon in additive number theory and some related problems, J. London Math. Soc. 16 (1941), 212-215.
23. H. Halberstam and K. F. Roth, Sequences, Springer-Verlag, New York, 1983.
24. E. K. Hayashi, An elementary method for estimating error terms in additive number theory, Proc. Amer. Math. Soc. 52 (1975), 55-59.
25. E. K. Hayashi, Omega theorems for the iterated additive convolution of a nonnegative arithmetic function, J. Number Theory 13 (1981), 176-191.
26. R. Heath-Brown, Integer sets containing no arithmetic progressions, J. London Math. Soc. 35 (1987), 385-394.
27. A. Gyárfás, Z. Lehel, Linear sets with five distinct differences among any four elements (to appear).
28. H. L. Montgomery and R. C. Vaughan, On the Erdős-Fuchs theorems, in: A tribute to Paul Erdős, eds. A. Baker, B. Bollobás and A. Hajnal, Cambridge Univ. Press, 1990; 331-338.
29. H.-E. Richert, Zur multiplikativen Zahlentheorie, J. Reine Angew. Math. 206 (1961), 31-38.
30. K. F. Roth, On certain sets of integers, I, J. London Math. Soc. 28 (1953), 104-109.
31. K. F. Roth, On certain sets of integers, II, J. London Math. Soc. 29 (1954), 20-26.
32. I. Z. Ruzsa, A just basis, Monatsh. Math. 109 (1990), 145-151.
33. I. Z. Ruzsa, On the number of sums and differences, Acta Math. Hung. 59 (1992), 439-447.
34. A. Sárközy, On a theorem of Erdős and Fuchs, Acta Arithmetica 37 (1980), 333-338.
35. J. Schur, Über die Kongruenz $x^m + y^m \equiv z^m$ (mod p), Jahresbericht der Deutschen Math. Verein. 25 (1916), 114-117.
36. S. Sidon, Ein Satz über trigonomische Polynome und seine Anwendung in der Theorie der Fourier-Reihen, Math. Annalen 106 (1932), 536-539.
37. V.T. Sós, An additive problem on different structures, 3rd Internat. Comb. Conf., San Francisco 1989. Graph Theory, Comb. Alg. and Appl. SIAM, ed. Y. Alavi, F.R.K. Chung, R.L. Graham, D.F. Hsu (1991), 486-508.
38. A. Stöhr: Gelöste und ungelöste Fragen über Basen der natürlichen Zahlen, J. Reine Angew. Math. 194 (1955), 40-65, 111-140.

39. E. Szemerédi: On a set containing no k elements in an arithmetic progression, Acta Arithmetica 27 (1975), 199-245.
40. R. C. Vaughan, On the addition of sequences of integers, J. Number Theory 4 (1972), 1-16.
41. B. L. van der Waerden, Beweis einer Baudetschen Vermutung, Nieuw Arch. Wisk. 15 (1927), 212-216.