ISRAEL JOURNAL OF MATHEMATICS 92 (1995), 33-43

ON AN ADDITIVE PROBLEM OF ERDŐS AND STRAUS, 1

BY

J-M. DESHOUILLERS

Mathématiques Stochastiques, Université Bordeaux 2
33076 Bordeaux Cedex, France
e-mail: dezou@u-bordeaux2.fr

AND

G. A. FREIMAN

Raymond and Beverly Sackler Faculty of Exact Sciences
School of Mathematical Sciences, Tel Aviv Univesity
Ramat Aviv, Tel Aviv, Israel
e-mail: grisha@math.tau.ac.il

ABSTRACT

According to Erdős and Straus, we define an **admissible** subset $\mathcal{A}$ of $[1, \mathcal{N}]$ to be such that whenever an integer can be written as a sum of s distinct elements from $\mathcal{A}$, then s is well defined. Improving on previous results, we show that the cardinality of such an admissible subset $\mathcal{A}$ is at most $(2+o(1))\sqrt{N}$. As shown by Straus, the constant 2 cannot be improved upon.

P. Erdős [1] initiated in 1962 the study of finite sets $\mathcal{A}$ of integers, having the property that each time an integer can be written as a sum of a certain number of distinct elements from $\mathcal{A}$, it cannot be written as a sum of distinct elements from $\mathcal{A}$ with a different number of summands. Such sets have been called **admissible** by E. G. Straus in [5].

If we denote by $h^\wedge\mathcal{A}$ the set of integers which can be represented as a sum of h distinct elements from $\mathcal{A}$, the admissibility of $\mathcal{A}$ is equivalent to saying that $s^\wedge\mathcal{A} \cap t^\wedge\mathcal{A} = \emptyset$ for all $s \neq t$.

Received March 11, 1993 and in revised form March 22, 1994

Erdős proved that an admissible set included in $[1, N]$ has cardinality $O(N^{5/6})$ and suggested that in this case $|\mathcal{A}|$ is indeed maximal when $\mathcal{A}$ consists of consecutive integers at the upper end of the interval $[1, N]$.

Straus proved that for an admissible set $\mathcal{A}$ in $[1, N]$, one has $|\mathcal{A}| \le (4/\sqrt{3} + o(1))\sqrt{N}$, and that there exists $\mathcal{A}$ admissible in $[1, N]$ with $|\mathcal{A}| = \lfloor 2\sqrt{N} - 1 \rfloor$.

The constant $4/\sqrt{3} = 2.309...$ has been recently reduced by P. Erdős, J. L. Nicolas and A. Sarközy [2]. The primary aim of this paper is to reduce it to 2, which is best possible, as shown by Straus' example.

THEOREM 1: *There exists a constant C such that any admissible set $\mathcal{A}$ included in $[1, N]$ satisfies*

$$\operatorname{card} \mathcal{A} \le 2N^{1/2} + CN^{5/12}.$$

An interesting question is the determination of the structure of large admissible sets. The following result is a first step in this direction; its strength can be seen from the fact that Theorem 1 is an easy consequence of it. This result is however far from being stated in its strongest shape, and we shall come back later to that topic.

THEOREM 2: *Let $\mathcal{A}$ be an admissible set included in $[1, N]$, such that* $\operatorname{card} \mathcal{A} > 1.96\sqrt{N}$. *If N is large enough, there exists $\mathcal{C} \subset \mathcal{A}$ having the following properties:*

(i) $\operatorname{card} \mathcal{C} \le 10^5 N^{5/12}$,

(ii) *for some t, the set $t^\wedge \mathcal{C}$ contains an arithmetic progression with at least $3N^{5/6}$ terms, and difference d, say,*

(iii) *$\mathcal{A} \setminus \mathcal{C}$ is included in an arithmetic progression with difference d, and containing at most $N^{7/12}$ terms.*

It will be clear from the proof that a similar result may be obtained when 1.96 is replaced by any number larger than $4\sqrt{2/3} = 1.8856...$.

The key point in the proof of Theorem 2 is the following inverse additive result, which is a consequence of the structural result of the second author (cf. [3]).

THEOREM 3: *Let $\lambda < 6$ and $\mathcal{B}$ be a finite set of integers such that* $\operatorname{card}(4^\wedge \mathcal{B}) \le \lambda \operatorname{card} \mathcal{B}$. *There exist real numbers $C_1(\lambda)$ and $C_2(\lambda)$ such that $\lfloor (C_1 \operatorname{card} \mathcal{B})^\wedge \mathcal{B} \rfloor$ contains an arithmetic progression with at least $C_2(\lambda)(\operatorname{card} \mathcal{B})^2$ terms.*

In the remaining part of the paper, N denotes a sufficiently large integer, and $\mathcal{A}$ an admissible subset of $[1, N]$, for which $1.96\sqrt{N} \le \operatorname{card} \mathcal{A} \le 2.31\sqrt{N}$. Because of Straus' result, the upper bound is valid for any admissible set.

ACKNOWLEDGEMENT: Both authors are thankful to the Universities of Bordeaux 1 and 2, the University of Tel-Aviv, the Weizmann Institute of Sciences and its Bordeaux Delegation for facilitating their collaboration. They also wish to express their thanks to N. Alon and B. Sudakov for pointing out some inaccuracies on the first draft of the paper.

1. There exists some s for which $s^\wedge\mathcal{A}$ is small

PROPOSITION 1: *There exists an integer s belonging to $[|\mathcal{A}|/10,\ 3|\mathcal{A}|/4]$ such that $|s^\wedge\mathcal{A}| < 1.44s(|\mathcal{A}|-s)$.*

Proof: We assume that $|s^\wedge\mathcal{A}|$ is at least $1.44s(|\mathcal{A}|-s)$ for every s in the interval $\mathcal{I} := [|\mathcal{A}|/10, 3|\mathcal{A}|/4]$. Since $\mathcal{A}$ is admissible, the sets $s^\wedge\mathcal{A}$ are pairwise disjoint for s in $\mathcal{I}$, and all those sets are included in $[1, 0.75|\mathcal{A}|N]$. We thus have:

$$0.75|\mathcal{A}|N \geq \sum_{s\in\mathcal{I}} |s^\wedge\mathcal{A}| \geq 1.44\sum_{s\in\mathcal{I}}(s|\mathcal{A}|-s^2)$$

$$\geq 1.44\left(\frac{|\mathcal{A}|}{2}\left(\left(\frac{3|\mathcal{A}|}{4}\right)^2-\left(\frac{|\mathcal{A}|}{10}\right)^2\right)-\frac{1}{3}\left(\left(\frac{3|\mathcal{A}|}{4}\right)^3-\left(\frac{|\mathcal{A}|}{10}\right)^3\right)\right)+O(|\mathcal{A}|^2)$$

$$\geq 0.19578|\mathcal{A}|^3 + O\left(|\mathcal{A}|^2\right),$$

and this implies that $\mathcal{A}$ is at most $1.958N^{1/2}$ when N is large enough, a contradiction which proves Proposition 1. ∎

2. The set $\mathcal{A}$ contains a subset $\mathcal{B}$ such that $|4^\wedge\mathcal{B}|$ is small

PROPOSITION 2: *Let L be any integer between 1 and $|\mathcal{A}|/2000$. There exists $\mathcal{B}\subset\mathcal{A}$ with $|\mathcal{B}| = L$ such that $|4^\wedge\mathcal{B}|$ is less than $5.8|\mathcal{B}|$.*

Proof: We consider an integer s satisfying Proposition 1, and write $\mathcal{A} = \{a_1 < \cdots < a_{|\mathcal{A}|}\}$. For $0 \leq l \leq (|\mathcal{A}|-s-4)/4$, let

$$\mathcal{C}_l := \{a_{4l+1}, a_{4l+2}, \ldots, a_{4l+s+4}\}.$$

For $m < l$, the sets $s^\wedge\mathcal{C}_m$ and $s^\wedge\mathcal{C}_l$ are disjoint, except when $l = m+1$, in which case they have only one element in common, namely $a_{4l+1} + \cdots + a_{4l+s}$, so that we have

$$|s^\wedge\mathcal{A}| \geq \sum_l |s^\wedge\mathcal{C}_l| - (|\mathcal{A}| - s)/4.$$

By considering the map which associates to any subset of 4 distinct elements from $\mathcal{C}_l$ its complement in $\mathcal{C}_l$, we readily see that $|4^\wedge\mathcal{C}_l| = |s^\wedge\mathcal{C}_l|$, so that we have

$$|s^\wedge\mathcal{A}| \geq \sum_l |4^\wedge\mathcal{C}_l| - (|\mathcal{A}| - s)/4.$$

By Proposition 1, we have $|s^\wedge\mathcal{A}| < 1.44s(|\mathcal{A}| - s)$, and so for some l we have $|4^\wedge\mathcal{C}_l| < 5.77s$ if N is large enough.

We let $M := \lfloor\frac{s+4}{L}\rfloor$, so that $M \geq 200$, and break $\mathcal{C}_l$ into $M+1$ consecutive blocks of integers $\mathcal{B}_1, \ldots, \mathcal{B}_{M+1}$ where $|\mathcal{B}_m| = L$, for $1 \leq m \leq M$. We clearly have

$$4^\wedge\mathcal{B}_1 \cup \cdots \cup 4^\wedge\mathcal{B}_M \subset 4^\wedge\mathcal{C}_l,$$

where the terms in the union are pairwise disjoint, so that, for at least one index m in $[1, M]$, we have

$$|4^\wedge\mathcal{B}_m| \leq \frac{1}{M}|4^\wedge\mathcal{C}_l| \leq 5.77s/\lfloor(s+4)/L\rfloor < 5.8L.$$

Such a set $\mathcal{B}_m$ satisfies the conditions stated in Proposition 2. ∎

3. Three statements in additive number theory

In this section, we give some general results in additive number theory. The first one is the easiest case of the general inverse result which can be found in [4] (Thm. 1.9 p. 11); its original proof appeared in [3].

PROPOSITION 3.1: *Let $\mathcal{S}$ be a finite set of integers satisfying $|2\mathcal{S}| \leq 2|\mathcal{S}| - 1 + b$, where $b \leq |\mathcal{S}| - 3$. Then $\mathcal{S}$ is included in an arithmetic progression of length $|\mathcal{S}| + b$.*

The next two results are fairly elementary ones and are just stated and proved here for convenience. The reader will meet no difficulty in adjusting Proposition 3.2 to the case when the length for the arithmetic progression containing $\mathcal{S}$ is only known to be $\leq \kappa|\mathcal{S}|$ for some $\kappa < 2$.

PROPOSITION 3.2: *Let $\mathcal{S}$ be a set of integers such that $\mathcal{S}$ is included in an arithmetic progression of length $\leq 1.94|\mathcal{S}|$. For any $h \geq 2$, the set $h\mathcal{S}$ contains an arithmetic progression of length $0.01hS$ with the same difference as the first one.*

Proof: Let d be the difference of the arithmetic progression that contains $\mathcal{S}$, and write $\mathcal{S} = \{s_1 < \cdots < s_S\}$, and

$$\mathcal{T} := \left\{0, \frac{s_2 - s_1}{d}, \ldots, \frac{s_S - s_1}{d}\right\} = \{t_1 < \cdots < t_S\}.$$

The set $\mathcal{T}$ contains S integers and is included in the interval $[0, 1.94S]$. For any $z \in [1.94S, 2S-2]$, the sets $\mathcal{T}$ and $z - \mathcal{T}$ are in $[0, 2S-2]$, and since each of them has S elements, the pigeon-hole principle implies that they have a common point, so that $z \in 2\mathcal{T}$, and so $[1.94S, 2S-2]$ is contained in $2\mathcal{T}$.

Since $2\mathcal{T}$ contains an interval of length $0.06S - 1$, then for any $h \geq 2$, the set $h\mathcal{T}$ contains an interval of length $\lfloor \frac{h}{2} \rfloor (0.06S - 1) \geq 0.01hS$.

We easily transfer this result from $\mathcal{T}$ to $\mathcal{S}$, getting a proof of Proposition 3.2. ∎

PROPOSITION 3.3: *Let $\mathcal{B}$ be a set of integers; we have*

$$|2\mathcal{B}| \leq 3|\mathcal{B}| + |4^\wedge \mathcal{B}|.$$

Proof: We may assume that $|\mathcal{B}|$ is at least 2, and denote by b_1 and b_2 the two smallest elements in $\mathcal{B}$. Let us write $\mathcal{B}' := \mathcal{B} \setminus \{b_1, b_2\}$. We have

$$2\mathcal{B} \subset (\{b_1\} + \mathcal{B}) \cup (\{b_2\} + \mathcal{B}) \cup \{2b / b \in \mathcal{B}\} \cup 2^\wedge \mathcal{B}'.$$

The map which associates to each element x in $2^\wedge \mathcal{B}'$ the element $b_1 + b_2 + x$ is a one to one correspondance from $2^\wedge \mathcal{B}'$ to $4^\wedge \mathcal{B}$, so that $| 2^\wedge \mathcal{B}' | \leq | 4^\wedge \mathcal{B} |$. We thus have $| 2\mathcal{B} | \leq 3 | \mathcal{B} | + | 2^\wedge \mathcal{B}' | \leq 3 | \mathcal{B} | + | 4^\wedge \mathcal{B} |$. ∎

4. On the structure of $\mathcal{B}$ when $4^\wedge \mathcal{B}$ is small

This section is devoted to the proof of the structural result Theorem 3. We give a proof in the case $\lambda = 5.8$, which is enough for our purpose, and will permit us to specify almost all the involved constants. The reader will have no difficulty in deriving a proof of the general case along the same lines. More specifically, we show the following special case of Theorem 3.

PROPOSITION 4: *Let L be sufficiently large, and $\mathcal{B}$ be a set of L integers such that $|4^\wedge\mathcal{B}| \leq 5.8L$. Then the set $2\lfloor L10^{-6}\rfloor^\wedge\mathcal{B}$ contains at least $10^{-8}|\mathcal{B}|^2$ terms in an arithmetic progression.*

Proof: Let us consider a set $\mathcal{B}$ with L elements such that $|4^\wedge\mathcal{B}|$ is at most $5.8|\mathcal{B}|$; let us write

$$\mathcal{B} = \{b_1, \dots, b_L\},$$

and let us define

$$u := \lfloor L/1000 \rfloor \quad \text{and} \quad v := \lfloor L/1000000 \rfloor \times 2.$$

We let $\mathcal{S}$ consist of those elements in $2\mathcal{B}$ which are representable as the sum of two elements from $\mathcal{B}$ in at least $(v+1)$ ways. We have the following three facts:

(i) the number of pairs (b_i, b_j) with $1 \leq i < j \leq i+u$ is at least $(L-u)u$,

(ii) the number of pairs (b_i, b_j) which occur in the representation of some element in $2\mathcal{B}$ which is not in $\mathcal{S}$, is at most $\mid 2\mathcal{B} \mid v$,

(iii) every element in $2\mathcal{B}$ is representable as a sum $b_i + b_j$ with $1 \leq i < j \leq i+u$ in at most $u/2$ ways.

From those three facts, we readily deduce the lower bound

$$|\mathcal{S}| \geq \frac{(L-u).u - |2\mathcal{B}|v}{u/2}.$$

By Proposition 3.3 and the upper bound $|4^\wedge\mathcal{B}| \geq 5.8|\mathcal{B}|$, we know that $|2\mathcal{B}| \leq 8.8|\mathcal{B}|$; combined with the definition of u and v, this leads to

$$|\mathcal{S}| \geq 1.98L.$$

Let us now consider the set $2\mathcal{S}$. Since v is at least 1 (as soon as L is large enough), we have $2\mathcal{S} \subset 4^\wedge\mathcal{B}$, so that

$$|2\mathcal{S}| \leq 5.8L.$$

Combining the two previous inequalities, we get

$$|2\mathcal{S}| \leq 5.8L \leq 2 \times 1.98L - 1 + 1.85L \leq 2|\mathcal{S}| - 1 + 1.85L.$$

Since $1.85L \leq 1.98L - 3 \leq |\mathcal{S}| - 3$, we may apply Proposition 3.1, and so we know that $\mathcal{S}$ is included in an arithmetic progression of length $|\mathcal{S}| + 1.85L \leq |\mathcal{S}|(1 + 1.85/1.98) \leq 1.94|\mathcal{S}|$.

We now appeal to Proposition 3.2: for any $h \geq 2$, the set $h\mathcal{S}$ contains $0.01h|\mathcal{S}|$ terms in an arithmetic progression, and we apply this result for $h := v/2$, showing that the set $\frac{v}{2}\mathcal{S}$ contains an arithmetic progression with cardinality at least

$$\frac{v}{2}0.01.|\mathcal{S}| \geq \frac{L}{1980000} \times 0.01 \times 1.98L = 10^{-8}L^2.$$

To conclude the proof, it remains to show that an element in $\frac{v}{2}\mathcal{S}$ belongs to $v^\wedge\mathcal{B}$. Let indeed x be in $\frac{v}{2}\mathcal{S}$; we can write

$$x = s_1 + \cdots + s_{v/2};$$

we now may write s_1 as a sum of two distinct elements from $\mathcal{B}$, then s_2 as a sum of two distinct elements of $\mathcal{B}$, each of which is distinct from those used in $s_1, \ldots$ and so on, by the definition of $\mathcal{S}$. Our conclusion is that $2\lfloor L.10^{-6}\rfloor^\wedge\mathcal{B}$ contains an arithmetic progression with at least $L^2.10^{-8}$ terms, as stated in Proposition 4. ∎

5. The set $\mathcal{A}$ is essentially contained in a short arithmetic progression

This section is devoted to the proof of Theorem 2, which is stated in the introduction.

Let $L := 2\lfloor 10^4 N^{5/12}\rfloor$ and $t := 2\lfloor 10^{-6}L\rfloor$. By Proposition 2, we may find $\mathcal{B} \subset \mathcal{A}$ with $|\mathcal{B}| = L$ and $|4^\wedge\mathcal{B}| \leq 5.8|\mathcal{B}|$. By Proposition 4, the set $t^\wedge\mathcal{B}$ contains at least $10^{-8}L^2 \geq 3N^{5/6}$ terms in an arithmetic progression; let us call δ the difference of this arithmetic progression.

Our first step is to show that the elements of $\mathcal{D} := \mathcal{A} \setminus \mathcal{B}$ are located in less than $R := \lfloor N^{1/6}\rfloor$ distinct residue classes modulo δ. Let us assume that it is not true, and choose $d_1, \ldots, d_R$, elements in $\mathcal{D}$ which are pairwise incongruent mod δ. Let us now select $n := s - t - 1$ fixed elements $a_1, \ldots, a_n$ in $\mathcal{D} \setminus \{d_1, \ldots, d_R\}$.

All the sets $t^\wedge\mathcal{B} + \{a_1 + \cdots + a_n\} + \{d_i\}$ $(1 \leq i \leq R)$ are included in $s^\wedge\mathcal{A}$ and their union contains at least $R10^{-8}L^2$ distinct elements. This would lead to $|s^\wedge\mathcal{A}| \geq R10^{-8}\mathrm{L}^2 \geq 2\mathrm{N}$ in contradiction to $|s^\wedge\mathcal{A}| < 1.44s(|\mathcal{A}| - s) < 1.45|\mathcal{A}|^2/4 < 2N$.

Let $\{g_i\}_{1 \leq i \leq S}$ be the set of residues modulo δ such that $\mathcal{D}$ contains at least R distinct elements congruent to g_i modulo δ, and let us denote by $\mathcal{E}$ the set of all the elements in $\mathcal{D}$ which are congruent to some of the g_i modulo δ (i.e. $\mathcal{E}$ is the union of the "rich" classes of $\mathcal{D}$ modulo δ). The set $\mathcal{E} \setminus \mathcal{D}$ has cardinality at most R^2, and $\mathcal{E}$ has cardinality larger than $|\mathcal{A}| - |\mathcal{B}| - |\mathcal{E} \setminus \mathcal{D}| \geq N^{1/2}$. Since

$S \leq R$, this implies that $S \geq 1$ and that there exists at least one g_i, let us call it g_1, such that $\mathcal{E}$ contains at least R^2 elements congruent to g_1 modulo δ.

Our next step is to prove that for any i with $2 \leq i \leq S$, the element $g_1 - g_i$ (in $\mathbb{Z}/\delta\mathbb{Z}$) has order less than R. The proof is quite similar to that used in bounding the number of classes represented by $\mathcal{D}$ modulo δ. We assume that the order of $g_1 - g_i$ (modulo δ) is at least R and choose $e_1(1), \ldots, e_1(R)$ distinct in $\mathcal{E}$ and congruent to g_1 modulo δ, as well as $e_i(1), \ldots, e_i(R)$ distinct in $\mathcal{E}$ and congruent to g_i modulo δ. By our assumption on the order of $g_1 - g_i$, the elements

$$e_1(1) + \cdots + e_1(r) + e_i(r+1) + \cdots + e_i(R) \quad \text{for } 0 \leq r \leq R-1$$

are pairwise incongruent modulo δ, since

$$e_1(1) + \cdots + e_1(r) + e_i(r+1) + \cdots + e_i(R)$$

is congruent to $Rg_i + r(g_1 - g_i)$ modulo δ. Thus the cardinality of $t^\wedge\mathcal{B} + R^\wedge\{e_1(1), \ldots, e_1(R), e_i(1), \ldots, e_i(R)\}$ is at least $R.10^{-8}L^2 > 2N$; as previously, by choosing suitable elements in $\mathcal{A}$, we may deduce from this last inequality that $|s^\wedge\mathcal{A}|$ is larger than $2N$, a contradiction; the order of $g_1 - g_i$ is thus less than R.

Let us now select R^2 elements in $\mathcal{E}$, say $e_1(1), \ldots, e_1(R^2)$ which are congruent to g_1 modulo δ, and for each i with $2 \leq i \leq S$, let us select R elements in $\mathcal{E}$, say $e_i(1), \ldots, e_i(R)$, which are congruent to g_i modulo δ. This choice is possible by the definition of $\mathcal{E}$ and g_1. Let us call R the set of all those $(e_j(i))$.

Let $\mathcal{G}$ be the subgroup of $\mathbf{Z}/\delta\mathbf{Z}$, generated by $(g_1 - g_2, \ldots, g_1 - g_S)$; it is an abelian group generated by elements of order at most R, so that any element in $\mathcal{G}$ may be written as $n_1(g_1 - g_2) + \cdots + n_S(g_1 - g_s)$ with $n_i \leq R$. This implies that the integers $e_1(1) + \cdots + e_1(r_1) + e_2(1) + \cdots + e_2(r_2) + \cdots + e_S(1) + \cdots + e_S(r_S)$ represent all the elements of $\mathcal{G}$, when $(r_1, \ldots, r_S)$ run over the sets of integers satisfying:

$$r_1 + \cdots + r_S = R^2 \quad \text{and} \quad 0 \leq r_i \leq R \quad \text{for } 2 \leq i \leq S.$$

We summarize the situation, and let $\mathcal{F} := \mathcal{B} \cup (\mathcal{E} \setminus \mathcal{D}) \cup \mathcal{R}$ and $d := \delta/|G|$.

We have the following properties:

(α) $|\mathcal{F}| \leq 3 \times 10^4 N^{5/12}$,

(β) $t^\wedge\mathcal{F}$ contains an arithmetic progression with at least $3N^{5/6}$ terms and difference d,

(γ) $\mathcal{A} \setminus \mathcal{F}$ is included in an arithmetic progression modulo d.

Our last step in the proof of Theorem 2 is to show that a large part of $\mathcal{A} \setminus \mathcal{F}$ is in a short arithmetic progression. Let $T := \lfloor 3N^{5/12} \rfloor$, and let us consider the T smallest elements of $\mathcal{A} \setminus \mathcal{F}$ (let us call them $a_1 < \cdots < a_T$) and the T largest (which we call $a'_1 < \cdots < a'_T$). We consider the integers

$$b_1 = a_1 + \cdots + a_T,$$
$$b_2 = a_1 + \cdots + a_{T-1} + a'_T,$$
$$\cdots$$
$$b_{T+1} = a'_1 + \cdots + a'_{T-1} + a'_T.$$

If we denote by Δd the difference $a'_1 - a_T$, all the integers $b_1 < b_2 < \cdots < b_T$ are in the same class modulo d and the difference between any two of them is at least Δd. This implies that $t^\wedge \mathcal{F} + T^\wedge\{a_1, \ldots, a_T, a'_1, \ldots, a'_T\}$ contains at least $T \min(\Delta, 3N^{5/6})$ elements. By our now familiar argument, this implies that $T \min(\Delta, 3N^{5/6}) \leq |s^\wedge \mathcal{A}| \leq 2N$, so that $\Delta \leq N^{7/12}$. We finally define d as previously, $\mathcal{C}$ as $\mathcal{B} \cup \mathcal{E} \setminus \mathcal{D} \cup \mathcal{R} \cup \{a_1, \ldots, a_T, a'_1, \ldots, a'_T\}$; this set $\mathcal{C}$ satisfies the properties of Theorem 2. ∎

6. Proof of Theorem 1

Let $\mathcal{A}$ be an admissible subset included in $[1, N]$. If card $\mathcal{A}$ is less than $2N^{1/2} + 10^6 N^{5/12}$ or if N is small, then Theorem 1 trivially holds. We may thus assume that N is large enough and that card $\mathcal{A}$ is larger than $2N^{1/2} + 10^6 N^{5/12}$, so that Theorem 2 may be applied; we consider $\mathcal{C}$, d and t given by this result, and we denote by $u, u+d, \ldots, u+ld$ the arithmetic progression included in $t^\wedge \mathcal{C}$, with $l > 2N^{5/6}$. We choose an integer S larger than $2N^{1/2} + 1$, such that S is congruent to d mod 2 and card $(\mathcal{A} \setminus \mathcal{C}) > S$; we finally let $U = (S+d)/2$.

Our aim is to show that $t^\wedge \mathcal{C} + (U-d)^\wedge(\mathcal{A} \setminus \mathcal{C})$ and $t^\wedge \mathcal{C} + U^\wedge(\mathcal{A} \setminus \mathcal{C})$ have one element in common, which contradicts the fact that $\mathcal{A}$ is admissible; this contradiction will then imply that card $\mathcal{A} > 2N^{1/2} + 10^6 N^{5/12}$ cannot hold, and Theorem 1 will be proven.

Let us write $\mathcal{A} \setminus \mathcal{C} = \{a_1 < a_2 < \cdots\}$ and consider the elements:

$$a_1 + \cdots + a_{U-1} + a_U,$$
$$a_1 + \cdots + a_{U-1} + a_{U+1},$$

$$\dots$$
$$a_1 + \cdots + a_{U-1} + a_S,$$
$$a_1 + \cdots + a_U + a_S,$$
$$\dots$$
$$a_{S-U+1} + \cdots + a_S.$$

All those elements are distinct, congruent modulo d, and the difference between two consecutive elements is at most $dN^{7/12}$. By adding $t^\wedge\mathcal{C}$ we see that $t^\wedge\mathcal{C} + U^\wedge(\mathcal{A}\setminus\mathcal{C})$ contains all the elements which are congruent to $Ua_1 + u$ mod d, and lie in the interval $\mathcal{J} := [u + a_1 + \cdots + a_U, u + a_{S-U+1} + \cdots + a_S]$. The integer $u + a_{U+1} + \cdots + a_S$ belongs to $t^\wedge\mathcal{C} + (U-d)^\wedge(\mathcal{A}\setminus\mathcal{C})$; so it is congruent to $(U-d)a_1 + u$ modulo d, and so it is congruent to $Ua_1 + u$ modulo d. In order to get the desired contradiction, it is enough to prove that it belongs to $\mathcal{J}$, for which it is enough to prove that it is larger than $u + a_1 + \cdots + a_U$. We have thus reduced the problem to showing that

$$(*) \qquad a_1 + \cdots + a_U \le a_{U+1} + \cdots + a_S.$$

Let Md be a multiple of d which is at least a_U and less than a_{U+1}. We have

$$a_1 + \cdots + a_U \le (M - U + 1)d + \cdots + Md,$$

as well as

$$a_{U+1} + \cdots + a_S \ge Md + \cdots + (M + S - U - 1)d.$$

Thus, condition $(*)$ holds as soon as one has

$$M(M+1) - (M-U)(M-U+1) \le (M+S-U)(M+S-U-1) - M(M-1).$$

This last inequality is equivalent to

$$4dM + 1 \le d^2 + (S-1)^2,$$

which, in turns, holds because we have

$$S \ge 2\sqrt{N} + 1 \quad \text{and} \quad dM \le a_{U+1} \le N;$$

we have thus proven that inequality $(*)$ holds and, as we mentioned, this concludes the proof of Theorem 1. ∎

References

[1] P. Erdős, *Some remarks on number theory*, III, Math. Lapok **13** (1962), 28–38.

[2] P. Erdős, J-L. Nicolas and A. Sarközy, *Sommes de sous-ensembles*, Séminaire de Théorie des Nombres de Bordeaux **3** (1991), 55–72.

[3] G. A. Freiman, *The addition of finite sets*, Izvestiya Vysshikh Uchebnykh Zavedeniy Matematika **6(13)** (1959), 202–213 (Russian).

[4] G. A. Freiman, *Foundations of a Structural Theory of Set Addition*, Translations of Mathematical Monographs, Vol. 37, American Mathematical Society, Providence, RI, 1973, 108 pp.

[5] E. G. Straus, *On a problem in combinatorial number theory*, Journal of Mathematical Sciences **1** (1966), 77–80.