Sums and progressions
(DRAFT)

Noga Alon *

Abstract

A set of integers is called l-admissible if it contains no two subsets B and C satisfying $1 \leq |B| < |C| \leq l$ and $\sum_{b \in B} b = \sum_{c \in C} c$. It is shown that for every fixed l the maximum possible cardinality of an l-admissible subset of $\{1, 2, \ldots, m\}$ is $\frac{m}{l} + o(m)$. The proof is based on Roth's Theorem on sets of integers with no three-term arithmetic progressions. Similar ideas are used in characterizing sets of residues A modulo a prime number p for which the set $A \oplus A = \{(a + a')(\ mod\ p)\ : a, a' \in A, a \neq a'\}$ is of relatively small cardinality. Specifically it is proved that if $|A| = k < p/35$, $|A \oplus A| \leq (2.4 - \epsilon)k$ and $k > k_0(\epsilon)$, then A is contained in an arithmetic progression (modulo p) of length $1.4k$.

1 Introduction

In this note we consider two combinatorial problems in Additive Number Theory. Although the problems are seemingly unrelated, both of them can be treated by applying the same general approach, which combines some of the ideas in [1] with Roth's Theorem [11] and several additional ingredients. We start with the description of the problems and results.

1.1 Sums of distinct residues

For two subsets A, B of an abelian group let $A + B$ denote, as usual, the set

$$\{a + b : a \in A, b \in B\},$$

and define

$$A \oplus B = \{a + b : a \in A, b \in B, a \neq b\}.$$

For a prime p, let Z_p denote the group of integers modulo p.

*Department of Mathematics, Raymond and Beverly Sackler Faculty of Exact Sciences, Tel Aviv University, Tel Aviv, Israel

The Cauchy-Davenport Theorem ([4]) implies that if p is a prime, and A is a nonempty subset of Z_p, then

$$|A + A| \geq min\{p, 2|A| - 1\}. \tag{1}$$

A conjecture of Erdős and Heilbronn (cf., e.g., [7]), proved very recently by Dias Da Silva and Hamidoune [6], (see also [2], [3] for some extensions), asserts that if p is a prime and A is a nonempty subset of Z_p, then

$$|A \oplus A| \geq min\{p, 2|A| - 3\}. \tag{2}$$

Both theorems are tight for all possible values of $|A|$, as shown by taking A to be any arithmetic progression modulo p. Vosper ([15], [16]) proved that for $|A| < p/2$ equality holds in (1) only if A is an arithmetic progression. The analogous problem of characterizing all cases of equality in (2), raised in [3], seems more difficult.

In Section 2 we prove the following.

Theorem 1.1 *There is a positive constant $c > 0$ and an integer k_0 so that for every $k > k_0$, every prime p and every subset A of Z_p that satisfies $|A| = k < p/35$ and $|A \oplus A| \leq 2k - 1 + b - k/\log^c k$, where $b < 0.4k - 2$, the set A is contained in an arithmetic progression (modulo p) of length $k + b$.*

This improves the main result of [9], where a related statement for $b < 0.06k$ is established. Our short proof of Theorem 1.1 given here combines a trick from [1] with results of Ruzsa [12], Roth [11], Heath-Brown [10] and Szemerédi [14]. A corollary is the following result, answering the chracterization problem mentioned above for sufficiently large values of $|A|$ which do not exceed $p/35$.

Corollary 1.2 *There exists a k_0 so that if $k > k_0$, $p > 35k$ is a prime and $A \subset Z_p$ satisfies $|A \oplus A| = 2k - 3$, then A is an arithmetic progression modulo p.*

1.2 l-admissible sets

For an integer $l > 1$, a set of integers is called *l-admissible* if it contains no two subsets B and C satisfying $1 \leq |B| < |C| \leq l$ and $\sum_{b \in B} b = \sum_{c \in C} c$. Let $f(m, l)$ denote the maximum possible cardinality of an l-admissible subset of $\{1, 2, \ldots, m\}$. Two-admissible sets are usually called *sum-free* sets, and it is easy and known that $f(m, 2) = \lfloor (m+2)/2 \rfloor$. Since the set $\{m-x, m-x+1, \ldots, m\}$ for $x = \lfloor \frac{m+l-2}{l} \rfloor$ is l-admissible,

$$f(m, l) \geq \lfloor \frac{m + 2l - 2}{l} \rfloor \ (\ > m/l).$$

In Section 3 we prove the following.

Theorem 1.3 *There is a positive constant $\epsilon > 0$ and an integer m_0 so that for every $m > m_0$ and every l,*

$$f(m,l) \leq \frac{m}{l} + \sqrt{l}\frac{m}{\log^{\epsilon} m}.$$

In particular, for every fixed l, as m tends to infinity $f(m,l) = m/l + o(m)$.

The proof combines the technique of [1] based on Roth's Theorem with some additional ideas.

2 Modular sums of distinct residues

Let $r_3(n)$ denote the maximum possible cardinality of a subset of $\{1,\ldots,n\}$ that contains no three-term arithmetic progression. Roth [11] was the first to prove that $r_3(n) = o(n)$, and the best known upper bound for $r_3(n)$ is due to Heath-Brown [10] and Szemerédi [14], who showed that there is a $\delta > 0$ so that for all sufficiently large n

$$r_3(n) \leq n/\log^{\delta} n. \tag{3}$$

We need the following result of Ruzsa.

Lemma 2.1 ([12]) *Let C be a set of n integers that contains no three-term arithmetic progression and let B be an arbitrary set of k integers. Then*

$$|C+B| \geq \frac{n^{1/4}}{2r_3^{1/4}(n)} n^{1/4} k^{3/4}.$$

We will also use the following result of Freiman.

Lemma 2.2 ([8]) *If p is a prime, A is a subset of cardinality $k < p/35$ of Z_p, and $|A+A| = 2k-1+b$, with $b < 0.4k-2$, then A is contained in an arithmetic progression modulo p of length $k+b$.*

We now prove the following proposition, which supplies, in view of (3), the assertion of Theorem 1.1. Note that the term $256\sqrt{k}\sqrt{r_3(k)}$ $(= o(k))$ in the statement of this proposition can be easily improved, and we make no attempt to optimize this error term here.

Proposition 2.3 *For every prime p and every subset A of Z_p that satisfies $|A| = k < p/35$ and $|A \oplus A| \leq 2k-1+b-256\sqrt{k}\sqrt{r_3(k)}$, where $b < 0.4k-2$, the set A is contained in an arithmetic progression modulo p of length $k+b$.*

Proof. Given a set A as above, let C denote the set of all members of A which are not the middle term of any three-term arithmetic progression consisting of members of A (where here A is considered as a set of integers). Let n be the cardinality of C, and observe that C itself contains no

three-term arithmetic progression. Therefore, by Lemma 2.1, and since for every residue modulo p there are at most two integers equal to that residue modulo p which can be obtained as a sum of two integers in the interval $[0, p-1]$,

$$|C + A| \geq \frac{n^{1/4}}{4r_3^{1/4}(n)} n^{1/4} k^{3/4},$$

where the addition is computed in Z_p. Since $C + A \subset A \oplus A \cup \{2c : c \in C\}$ we conclude that

$$2.4k > |A \oplus A| \geq |C + A| - |C| \geq \frac{n^{1/4}}{4r_3^{1/4}(n)} n^{1/4} k^{3/4} - n.$$

Clearly $n \leq k$ and hence $r_3(n) \leq r_3(k)$ implying that

$$4k \geq 2.4k + n \geq \frac{n^{1/4}}{4r_3^{1/4}(k)} n^{1/4} k^{3/4},$$

which gives

$$|C| = n \leq 256\sqrt{k}\sqrt{r_3(k)}.$$

Observe, now, that every element of the form $2a$ with $a \in A - C$ lies in $A \oplus A$, since a is the middle term of a three-term arithmetic progression consisting of elements of A. Thus

$$|A + A| \leq |A \oplus A| + |\{2c : c \in C\}| \leq 2k - 1 + b - 256\sqrt{k}\sqrt{r_3(k)} + 256\sqrt{k}\sqrt{r_3(k)} = 2k - 1 + b,$$

and the result now follows from Lemma 2.2. □

Corollary 1.2 can be derived from Theorem 1.1 by applying the following simple lemma.

Lemma 2.4 *Let $A = \{a_0, a_1, \ldots, a_{k-1}\}$ be a set of k integers, where $0 = a_0 < a_1 < a_2 < \ldots < a_{k-1} = k - 1 + b$ and $b < (k-1)/3$. Then $|A \oplus A| \geq 2k - 3 + b$. In particular, if $|A \oplus A| = 2k - 3$ then $b = 0$.*

Proof. Define $D = \{0, 1, \ldots, k - 1 + b\} - A$ and observe that $|D| = b$. If c is any integer satisfying $2b + 1 \leq c \leq 2k - 3$ then c can be written in at least $b + 1$ ways as a sum $a + a'$ with $0 \leq a < a' \leq k + b - 1$. For a fixed such c, all these pairs $\{a, a'\}$ are pairwise disjoint and hence D can intersect at most b of them, implying that at least one such pair is a subset of A and showing that $c \in A \oplus A$. Put $x = |D \cap \{1, 2, \ldots, 2b\}|$ and $y = |D \cap \{k - b - 1, k - b, \ldots, k + b - 2\}|$. By assumption, $2b < k - b - 1$ and hence $x + y \leq b$. The set $A \oplus A$ contains exactly $2b - x$ members of the form $0 + a$ with $a \in A$, $1 \leq a \leq 2b$. Similarly, it contains exactly $2b - y$ members of the form $(k - 1 + b) + a$ with $a \in A$, $k - b - 1 \leq a \leq k + b - 2$. Altogether, we conclude that the cardinality of $A \oplus A$ is at least

$$|(A \oplus A) \cap \{1, \ldots 2b\}| + |(A \oplus A) \cap \{2b + 1, \ldots 2k - 3\}| + |(A \oplus A) \cap \{2k - 2, \ldots 2k + 2b - 3\}|$$

$$\geq (2b-x)+(2k-2b-3)+(2b-y)=2k-3+2b-(x+y)\geq 2k-3+b,$$

as needed. □

Proof of Corollary 1.2. Let A, k and p be as in the Corollary. By Theorem 1.1, if k is sufficiently large then A is contained in an arithmetic progression modulo p of length, say, $s \leq 1.1k$. Shifting it and multiplying it by an appropriate element modulo p we may assume that this progression is $0, 1, \ldots s-1 \leq 1.1k-1$, and that $0 \in A$. Since $k < p/35$ the modular addition of members of this interval is identical to their addition as integers, and the result thus follows from the last lemma. □

3 l-admissible sets

In this section we prove the following proposition, which, together with (3), implies the assertion Theorem 1.3.

Proposition 3.1 *For every $m \geq l > 1$,*

$$f(m,l) < \frac{m}{l} + 1 + (1+\sqrt{3(l-2)})r_3(m).$$

We need the following known combinatorial lemma.

Lemma 3.2 (De Caen [5]) *Every 3-uniform hypergraph with m vertices and at most sm edges contains an independent set of size at least $m/(1+\sqrt{3s})$, i.e., a set of at least $m/(1+\sqrt{3s})$ vertices that contains no edge.*

We also need the following result, which appears in various papers. As shown in [1] it is an easy consequence of the result of Scherk proved in [13].

Lemma 3.3 *Let A be a subset of an abelian group G of order r and supoose $|A| \geq r/l$. Then there is an integer s, $1 \leq s \leq l$, and a sequence $a_1, \ldots, a_s$ of not necessarily distinct elements of A whose sum in G is zero.*

Proof of Proposition 3.1. Let A be a subset of cardinality at least

$$\frac{m}{l} + 1 + (1+\sqrt{3(l-2)})r_3(m)$$

of $\{1, \ldots, m\}$. We must show that A is not l-admissible. Call an element of A *good* if it is the middle term of at least $l-1$ distinct three-term aritmetic progressions consisting of elements of A. Otherwise, call it *bad*. Let D denote the set of all bad elements of A. We claim that $|D| \leq (1+\sqrt{3(l-2)})r_3(m)$. To prove this claim, suppose it is false. Let H be the 3-uniform hypergraph whose vertices are all the members of D, where a triple forms an edge iff its members form a three-term arithmetic progression. By the definition of D, no member of D is the middle term of more

than $l-2$ three-term progressions, and hence the number of edges of H does not exceed $(l-2)|D|$. By Lemma 3.2, H contains an independent set of size at least $|D|/(1+\sqrt{3(l-2)}) > r_3(m)$. This set is a set of more than $r_3(m)$ integers in $\{1,\ldots,m\}$ which contains no three-term arithmetic progression, contradicting the definition of $r_3(m)$ and proving the claim.

Let r denote the maximum member of the set $A-D$ of all good members of A, and define $A' = A-(D\cup\{r\})$. The members of of A' are all distinct modulo r, and hence A' may be considered as a subset of the cyclic group Z_r. Also, $|A'| \geq m/l \geq r/l$, and thus, by Lemma 3.3, there are $a_1,\ldots,a_t \in A'$ and integers $\alpha_1,\ldots,\alpha_t$, where

$$\sum_{i=1}^{t} \alpha_i a_i \equiv 0 \ (\ mod\ r), \quad \alpha_i \geq 1, \quad \sum_{i=1}^{t} \alpha_i = s \leq l.$$

Since $r > a_i$ for all $1 \leq i \leq t$ this implies that there is a $\beta < s$ so that

$$\sum_{i=1}^{t} \alpha_i a_i = \beta r.$$

Therefore, there exists a solution to the equation

$$\sum_{i\in I} \alpha_i a_i = \sum_{j\in J} \beta_j a_j, \tag{4}$$

where $\alpha_i, \beta_j \geq 1$, $\sum_{i\in I}\alpha_i = s\ (\ \leq l)$, $\sum_{j\in J}\beta_j = \beta\ (\ < s)$, $a_i, a_j \in A$, and if $\alpha_i > 1$ then a_i is good, and, similarly, if $\beta_j > 1$ then a_j is good.

Consider a solution to this equation subject to the constraints above where the value of $\sum_{i\in I}\alpha_i^2 + \sum_{j\in J}\beta_j^2$ is minimum. We claim that for this solution $\alpha_i = 1$ for all $i \in I$ and $\beta_j = 1$ for all $j \in J$. To prove this claim, suppose it is false, and assume, first, that one of the coefficients α_i, say α_1 is at least 2. Since a_1 is good, $2a_1$ can be written as a sum of two distinct members of A in at least $l-1$ different ways. All these $2(l-1)$ members of A are pairwise distinct, and since there are at most $s-2 \leq l-2$ elements of A in the set $\{a_i : i \in I, i \neq 1\}$ there are some two elements d_1, d_2 of $A - \{a_i : i \in I, i \neq 1\}$ satisfying $d_1 + d_2 = 2a_1$. Clearly

$$d_1 + d_2 + (\alpha_1 - 2)a_1 + \sum_{i\in I, i\neq 1} \alpha_i a_i = \sum_{j\in J} \beta_j a_j,$$

and this contradicts the minimality of the sum $\sum_{i\in I}\alpha_i^2 + \sum_{j\in J}\beta_j^2$. The case $\beta_j \geq 2$ for some $j \in J$ leads to a similar contradiction, proving the claim. Therefore, there is a solution of (4) in which all the coefficients α_i and β_j are 1, showing that A is not an l-admissible set and completing the proof. □

References

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

[2] N. Alon, M. B. Nathanson and I. Z. Ruzsa, Adding distinct congruence classes modulo a prime, *American Math. Monthly*, to appear.

[3] N. Alon, M. B. Nathanson and I. Z. Ruzsa, The polynomial method and restricted sums of congruence classes, submitted.

[4] H. Davenport, On the addition of residue classes, *J. London Math. Soc.* 10, 30–32, 1935.

[5] D. De Caen, Extension of a theorem of Moon and Moser on complete graphs, *Ars Combinatoria* 16 (1983), 5-10.

[6] J. A. Dias da Silva and Y. O. Hamidoune, Cyclic spaces for Grassmann derivatives and additive theory, *Bull. London Math. Soc.*, 26:to appear, 1994.

[7] P. Erdős and R. L. Graham, *Old and New Problems and Results in Combinatorial Number Theory*, L'Enseignement Mathématique, Geneva, 1980.

[8] G. A. Freiman, *Foundations of a Structural Theory of Set Addition* (in Russian), Kazan. Gos. Ped. Inst., Kazan, 1966.

[9] G. A. Freiman, L. Low, and J. Pitman, The proof of Paul Erdős' conjecture of the addition of different residue classes modulo a prime number, to appear.

[10] D. R. Heath-Brown, Integer sets containing no arithmetic progressions, *J. London Math. Soc.* 35 (1987), 385-394.

[11] K. Roth, On certain sets of integers, *J. London Math. Soc.* 28 (1953), 104-109.

[12] I. Z. Ruzsa, *Arithmetical progressions and the number of sums*, to appear.

[13] P. Scherk, Amer. Math. Monthly 62 (1955), 46-47.

[14] E. Szemerédi, Integer sets containing no arithmetic progressions, *Acta Math. Acad. Sci. Hungar.* 56 (1990), 155-158.

[15] A. G. Vosper, The critical pairs of subsets of a group of prime order, *J. London Math. Soc.* 31: 200–205, 1956.

[16] A. G. Vosper, Addendum to "The critical pairs of subsets of a group of prime order", *J. London Math. Soc.* 31: 280–282, 1956.