Astérisque

GREGORY A. FREIMAN
LEWIS LOW
JANE PITMAN

Sumsets with distinct summands and the Erdős-Heilbronn conjecture on sums of residues

Astérisque, tome 258 (1999), p. 163-172
<http://www.numdam.org/item?id=AST_1999__258__163_0>

Astérisque **258**, 1999, p. 163–172

SUMSETS WITH DISTINCT SUMMANDS AND THE ERDŐS-HEILBRONN CONJECTURE ON SUMS OF RESIDUES

by

Gregory A. Freiman, Lewis Low & Jane Pitman

Abstract. — Let S be a set of integers or of residue classes modulo a prime p, with cardinality $|S| = k$, and let T be the set of all sums of two distinct elements of S. For the integer case, it is shown that if $|T|$ is less than approximately $2.5k$ then S is contained in an arithmetic progression with relatively small cardinality. For the residue class case a result of this type is derived provided that $k > 60$ and $p > 50k$. As an application, it is shown that $|T| \geq 2k-3$ under these conditions. Earlier results of Freiman play an essential role in the proofs.

1. Introduction

1.1. Let Z be the set of all integers and let F_p be the finite field of residue classes modulo p, where p is a prime number. If A is a subset of Z or F_p (written $A \subset Z$ or $A \subset F_p$) we denote the cardinality of A by $|A|$. For a finite subset A of Z or F_p we shall consider $2A$, the set of all sums of two elements of A, and also $2^\wedge A$, the set of all sums of two *distinct* elements of A, that is,

$$\begin{aligned} 2A &= \{a+b : a,b \in A\}, \\ 2^\wedge A &= \{a+b : a,b \in A,\ a \neq b\}. \end{aligned}$$

1.2. Sums of elements from a set of integers. — First we consider the sumset $2A$ for $A \subset Z$. We write

$$A = \{a_0, a_1, \ldots, a_{k-1}\}, \quad k = |A|,$$

where

$$a_0 < a_1 < \cdots < a_{k-1}\ .$$

Since the $k-1$ sums $a_i + a_{i+1}$ and the k sums $a_i + a_i = 2a_i$ are all distinct we have

$$|2A| \geq 2k-1, \tag{1}$$

1991 ***Mathematics Subject Classification.*** — 11 B75, 11 B13.
Key words and phrases. — sumset, set addition, sums of residues.

and it is easily seen that equality holds if and only if A is an arithmetic progression (that is, the differences $a_{i+1} - a_i$ are all equal). Freiman [6, page 11] has proved the following more precise result (which will be used in Section 2 below).

***Theorem A* (Freiman).** — *Let $D \subset Z$. If $|2D| \leq 2|D| - 1 + C_1$, where $C_1 \leq |D| - 3$, then $D \subset L$, where L is an arithmetic progression such that*

$$|L| \leq |D| + C_1$$

(so that D is obtained by deleting at most C_1 terms from the arithmetic progression L).

1.3. Sums of elements from a subset of F_p. — Next we look at $2A$ for $A \subset F_p$ such that $|A| = k$. By analogy with (1) we have the following special case of the well-known Cauchy-Davenport theorem:

$$|2A| \geq \min(p, 2k - 1). \tag{2}$$

More detailed results have been obtained by various authors and Freiman [6, p.46] has used the above theorem on $2D$ for $D \subset Z$ to obtain the following result in the same vein for $A \subset F_p$.

***Theorem B* (Freiman).** — *Let $A \subset F_p$ such that*

$$|A| = k < p/35.$$

Suppose that $|2A| = 2k - 1 + b$, $b < 0.4k - 2$. Then $A \subset L$, where L is an arithmetic progression in F_p such that $|L| = k + b$.

1.4. Sums with distinct summands and the Erdős-Heilbronn conjecture

For $A \subset Z$ as in 1.2 above, the $k - 1$ sums $a_i + a_{i+1}$ and the $k - 2$ sums $a_i + a_{i+2}$ are all distinct and belong to $2^{\wedge}A$. Thus

$$|2^{\wedge}A| \geq 2k - 3, \tag{3}$$

and it can be checked that for $k \geq 5$ equality holds if and only if A is an arithmetic progression.

By analogy with the Cauchy-Davenport theorem (2), Erdős and Heilbronn conjectured in the 1960's (see Erdős and Graham [5]) that for $A \subset F_p$ such that $|A| = k$ we must have

$$|2^{\wedge}A| \geq \min(p, 2k - 3). \tag{4}$$

Although there is a short elementary proof of (2) (see, for example, Davenport [3]), the corresponding result for distinct summands seems to be more difficult. As discussed further below, the full conjecture (4) has been proved since 1993. The main published contribution prior to 1993 seems to be that of Mansfield [7], who proved the following theorem.

***Theorem* (Mansfield).** — *Let $A \subset F_p$ such that $|A| = k$. Then the Erdős-Heilbronn conjecture (4) is true if*

$$\text{either} \quad k \leq 11 \quad \text{or} \quad 2^{k-1} \leq p.$$

Our aim in this paper was to develop analogues for $2^{\wedge}A$ of Freiman's results on $2D$, both for $D \subset Z$ and for $A \subset F_p$, which would be strong enough for the purposes of proving (4) for a wider range, as well as being of independent interest.

1.5. Results obtained. — In Section 2 we use simple combinatorial arguments together with Freiman's theorem on $2D$ for $D \subset Z$ to prove the following theorem.

Theorem 1. — *Let D be a set of k integers for which*

$$|2^{\wedge}D| \leq 2k - 3 + C,$$

where

$$0 \leq C \leq \frac{1}{2}(k-5).$$

Then D is contained in an arithmetic progression L such that

$$|L| \leq k + 2C + 2.$$

In Section 3 we use Theorem 1 and arguments based on trigonometric sums to prove the main result of the paper, which is as follows.

Theorem 2. — *Let $A \subset F_p$ such that*

$$|A| = k < \frac{p}{50}, \quad k > 60.$$

Suppose that

$$|2^{\wedge}A| \leq 2k - 3 + C,$$

where $C < 0.06k$. Then $A \subset L$, where L is an arithmetic progression in F_p such that

$$|L| \leq k + 2C + 2.$$

As a corollary, we will show that for $A \subset F_p$ such that $|A| = k$ the Erdős-Heilbronn conjecture (4) is true if

$$k < \frac{p}{50}, \quad k > 60. \tag{5}$$

Pybus [10] told us that he had obtained a proof of a version of the Erdős-Heilbronn conjecture based on different ideas. More recent work by others, including proofs of the full conjecture, will be discussed in Section 4 at the end of the paper.

1.6. Isomorphisms. — We note that the sumsets $2A$ and $2^{\wedge}A$ can be considered for any set A with addition. If A and B are two sets, each with an addition, and $\phi : A \to B$ is a bijection, we call ϕ an isomorphism if and only if

$$\phi(a) + \phi(b) = \phi(c) + \phi(d) \Leftrightarrow a + b = c + d.$$

We call A and B as above *isomorphic* if such an isomorphism exists, in which case we have

$$|2A| = |2B| \quad \text{and} \quad |2^{\wedge}A| = |2^{\wedge}B|.$$

We shall use the fact that affine transformations of Z or F_p are isomorphisms.

2. Sums of distinct elements from a set of integers

2.1. In this section we consider a set of integers A such that $|A| = k$ and use notation as at the beginning of section 1.2, together with some further vocabulary as follows. We note that $2^\wedge A$ is isomorphic to the set

$$\{\tfrac{1}{2}(a_i + a_j) : 1 \leq i < j \leq n\}$$

and it is helpful to think geometrically in terms of the points a_i and the mid-points of pairs a_i, a_j $(i < j)$. We shall say that a_i is *representable* if and only if a_i coincides with one of the mid-points, that is

$$2a_i \in 2^\wedge A.$$

We shall call a sum $a_i + a_{i+s}$ with $s \geq 1$ an *s-step sum*, and we recall that the 1-step and 2-step sums are all distinct. For $s \geq 1$, an s-step sum will be called *new* if and only if it is not equal to any j-step sum with $1 \leq j < s$. All 1-step and 2-step sums are new, but for $s \geq 3$ an s-step sum is not necessarily new. We shall use the notations

$$\begin{aligned} k_1 = k_1(A) &= \text{total number of } \textit{new } s\text{-step sums with } s \geq 3, \\ k_2 = k_2(A) &= \text{number of } a_j\text{'s which are } \textit{representable.} \end{aligned}$$

If an s-step sum $a_i + a_{i+s}$ is not new, then for some j, k such that $i < j < j+k < i+s$ we must have

$$a_i + a_{i+s} = a_j + a_{j+k}$$

and hence

$$0 < a_j - a_i = a_{i+s} - a_{j+k}\ .$$

We therefore consider the associated *difference set*

$$\mathcal{D}(a_i, a_{i+s}) = (a_{i+1} - a_i, a_{i+2} - a_{i+1}, \ldots, a_{i+s} - a_{i+s-1}).$$

Our proof of Theorem 1 will be based on the following lemma.

Lemma. — *For $A \subset Z$ such that $|A| = k$, $k \geq 5$, let k_1, k_2 be the number of new s-step sums with $s \geq 3$ and the number of representable elements of A as defined above. Then*

$$k_1 + k_2 \geq k - 4. \tag{6}$$

Proof. — Consider a particular subscript i such that $0 \leq i \leq k - 5$. If $a_i + a_{i+3}$ is not new we must have

$$\mathcal{D}(a_i, a_{i+3}) = (x, y, x)$$

for some $x, y > 0$, and so

$$\mathcal{D}(a_i, a_{i+4}) = (x, y, x, z)$$

for some z. If $z = x$ or $z = x + y$ then a_{i+3} is a mid-point and so is representable, while if $z \neq x$ and $z \neq x + y$ then $a_i + a_{i+4}$ is new. Thus at least one of the following three statements holds:

(i) $a_i + a_{i+3}$ is new; (ii) $a_i + a_{i+4}$ is new; (iii) a_{i+3} is representable.

This is true for $i = 0, 1, \ldots, k-5$; the new sums arising from (i) and (ii) for different i's are distinct, and the representable elements arising from (iii) are also distinct. Hence at least one element counted in $k_1 + k_2$ arises in this way from each of the $k-4$ possible values of the subscript i and so (6) follows.

We note that the above argument involves only 3-step and 4-step sums. By more detailed arguments using s-step sums with $s \geq 5$ it can be shown that in fact

$$k_1 + k_2 \geq k - 2 \quad \text{for} \quad k \geq 8. \tag{7}$$

2.2. Proof of Theorem 1. — We now consider $D \subset Z$ such that $|D| = k$. Let $k_1 = k_1(D)$, $k_2 = k_2(D)$ and suppose that D satisfies the hypotheses of Theorem 1, so that

$$|2^\wedge D| \leq 2k - 3 + C \tag{8}$$

$$0 \leq C \leq \tfrac{1}{2}(k-5). \tag{9}$$

Since

$$(2D)\backslash(2^\wedge D) = \{2d \mid d \in D, \ \ d \text{ is not representable}\}, \tag{10}$$

we have

$$|2D| = |2^\wedge D| + k - k_2 \ . \tag{11}$$

Using (8) and the above lemma we obtain

$$|2D| \leq 2k - 3 + C + k - k_2 = 3k - 3 + C - k_2 = 3k - 3 + C + k_1 - (k_1 + k_2)$$

$$\leq 3k - 3 + C + k_1 - (k-4) = 2k + 1 + C + k_1 \ . \tag{12}$$

The number of 1-step sums is equal to $k-1$, the number of 2-step sums is equal to $k-2$, and the number of new sums (different from these) is equal to k_1. Thus, we have

$$|2^\wedge D| = 2k - 3 + k_1 \ ,$$

and hence by (8),

$$k_1 \leq C.$$

Applying this inequality in (12), we get

$$|2D| \leq 2|D| - 1 + 2C + 2. \tag{13}$$

It now follows from (9) and (13), by Theorem A in Section 1.2, that $D \subset L$, where L is an arithmetic progression such that $|L| \leq |D| + 2C + 2$, as required.

3. Sums of distinct summands from a subset of F_p

3.1. The proof of our main result, Theorem 2, will depend on the use of trigonometric sums. We view the elements of F_p as residue classes modulo p, and note that for $a \in Z$ and $x \in F_p$, $e^{2\pi i a x/p}$ is defined uniquely by

$$e^{2\pi i a x/p} = e^{2\pi i a x_0/p} \ ,$$

where x_0 is any representative residue belonging to the residue class x.

For finite sets $A \subset F_p$ we shall consider trigonometric sums of the form

$$T = \sum_{x \in A} e^{2\pi i a x/p} . \tag{14}$$

We note that for such sums it is easily checked that if $k = |A|$ then

$$\sum_{a=1}^{p-1} \Big| \sum_{x \in A} e^{2\pi i a x/p} \Big|^2 \leq pk - k^2 . \tag{15}$$

3.2. We shall need the following lemma of Freiman [6].

Lemma. — *Let A be a subset of F_p such that $|A| = k$, and let $a \in Z$ such that $a \not\equiv 0$ (mod p) and let T be the corresponding trigonometric sum defined by (14). Suppose that $|T| > C_0 k$, where $0 < C_0 < 1$. Then, for some u and v in F_p such that $v \neq 0$, at least*

$$\frac{1}{2}(C_0 + 1)k$$

distinct elements of A belong to the arithmetic progression

$$\{u + sv : 0 \leq s \leq \tfrac{p-1}{2}\}.$$

Proof. — See Freiman [6], Section 1 of Chapter II, Corollary to Lemma on pages 46-47 and discussion on page 50.

3.3. Proof of Theorem 2. — We now turn to the proof of Theorem 2. We therefore consider $A \subset F_p$ such that

$$|A| = k < p/50, \tag{16}$$

$$|2\hat{}A| \leq 2k - 3 + C, \quad C < 0.06k, \quad k > 60. \tag{17}$$

Consider the sum

$$S = \sum_{a=0}^{p-1} \sum_{x_1, x_2 \in A} \sum_{x_3 \in 2\hat{}A} e^{2\pi i (a/p)(x_1 + x_2 - x_3)} .$$

We divide the sum S into two parts,

$$S = \sum_{a=0}^{p-1} \sum_{x_1, x_2 \in A} \sum_{x_3 \in 2A} - \sum_{a=0}^{p-1} \sum_{x_1, x_2 \in A} \sum_{x_3 \in (2A) \setminus (2\hat{}A)} = S_1 - S_2 , \tag{18}$$

say. Since each pair x_1, x_2 of elements of A yields exactly one x_3 in $2A$ such that $x_1 + x_2 = x_3$, we have

$$S_1 = k^2 p \tag{19}$$

(as in Freiman [6], p.48 (2.3.2)).

Denote by B the set of all elements of A which are *not* representable. Then, in view of (10) we have

$$S_2 = \sum_{a=0}^{p-1} \sum_{x_1, x_2 \in A} \sum_{a_j \in B} e^{2\pi i (a/p)(x_1 + x_2 - 2a_j)} .$$

For a_j in B, the equation $x_1 + x_2 - 2a_j = 0$ holds only if $x_1 = x_2 = a_j$ and therefore

$$S_2 = p|B|. \tag{20}$$

It follows from (18), (19) and (20) that

$$S \geq p(k^2 - k). \tag{21}$$

Then from (21) and the definition of S, we obtain

$$p(k^2-k) \leq \sum_{a=0}^{p-1} \Big| \sum_{x_1,x_2 \in A} \sum_{x_3 \in 2^\wedge A} e^{2\pi i(a/p)(x_1+x_2-x_3)} \Big|$$

$$= \sum_{a=0}^{p-1} \Big| \sum_{x\in A} e^{2\pi i(a/p)x} \Big|^2 \cdot \Big| \sum_{x \in 2^\wedge A} e^{2\pi i(a/p)x} \Big|$$

$$= k^2|2^\wedge A| + \sum_{a=1}^{p-1} \Big| \sum_{x\in A} e^{2\pi i(a/p)x} \Big|^2 \cdot \Big| \sum_{x\in 2^\wedge A} e^{2\pi i(a/p)x} \Big|$$

$$\leq k^2|2^\wedge A| + \max_{a \not\equiv 0 \pmod p} \Big| \sum_{x\in A} e^{2\pi i(a/p)x} \Big| \cdot \sum_{a=1}^{p-1} \Big| \sum_{x\in A} e^{2\pi i(a/p)x} \Big| \cdot \Big| \sum_{x\in 2^\wedge A} e^{2\pi i(a/p)x} \Big|.$$

By using Cauchy's inequality and applying (15) to A and $2^\wedge A$, we see that this expression is

$$\leq k^2|2^\wedge A| + \max_{a \not\equiv 0 \pmod p} \Big| \sum_{x\in A} e^{2\pi i(a/p)x} \Big| \cdot \sqrt{pk-k^2} \cdot \sqrt{p|2^\wedge A| - |2^\wedge A|^2}\,.$$

Dividing by pk^2 and solving the inequality for

$$U = \max_{a \not\equiv 0 \pmod p} \Big| \sum_{x\in A} e^{2\pi i(a/p)x} \Big|$$

we obtain

$$\frac{U}{k} \geq \frac{1-\alpha\beta-\gamma}{\sqrt{(\alpha(1-\beta)(1-\alpha\beta))}} = f(\alpha,\beta,\gamma), \text{ say,}$$

where

$$\alpha = \frac{|2^\wedge A|}{k}\,, \quad \beta = \frac{k}{p}\,, \quad \gamma = \frac{1}{k}\,,$$

and so, by (16) and (17)

$$0 < \alpha < 2.06 - 3\gamma, \quad 0 < \beta < \frac{1}{50}\,, \quad 0 < \gamma < \frac{1}{60} < \frac{1}{50}\,.$$

By consideration of partial derivatives in the relevant range it can be checked that

$$f(\alpha,\beta,\gamma) \geq f(2.06-3\gamma,\beta,\gamma) \geq f\left(2.01\,,\ \frac{1}{50}\,,\ \frac{1}{60}\right),$$

and hence

$$U > 0.6859k\,. \tag{22}$$

By applying the lemma in Section 3.2 above to the sum

$$T = \sum_{x \in A} e^{2\pi i (a/p)x}$$

and using (22), we see that there exist u, v in F_p with $v \neq 0$ and a subset A_1 of A such that

$$A_1 \subset \{u + vs : 0 \leq s \leq \tfrac{1}{2}(p-1)\}$$

and $|A_1| = m_1$, say, satisfies

$$m_1 = |A_1| \geq 0.8429k. \tag{23}$$

We consider the set

$$B_1 \subset \{0, 1, \ldots, \tfrac{1}{2}(p-1)\} \subset Z$$

defined by

$$B_1 = \{s : 0 \leq s \leq \tfrac{1}{2}(p-1),\ u + vs \in A_1\}. \tag{24}$$

By changing u and v if necessary we can assume that the first element of B_1 is 0 and that the greatest common divisor of the differences between successive elements of B_1 is 1.

Since the mapping ϕ given by $\phi(u + vs) = s$ gives an isomorphism of A_1 onto B_1 under addition mod p on A_1 and addition in Z on B_1, it follows that A_1 is isomorphic to B_1 as a subset of Z, so that (using (3) on B_1)

$$|B_1| = |A_1| = m_1\,, \quad |2^\wedge A_1| = |2^\wedge B_1| \geq 2m_1 - 3. \tag{25}$$

Suppose now that

$$|2^\wedge A_1| \geq 2|A_1| + C_1 - 3, \quad C_1 = \frac{|A_1| - 5}{2}\,.$$

Then from (23) it follows that

$$|2^\wedge A| \geq |2^\wedge A_1| \geq 2.5|A_1| - 5.5 \geq 2.107k - 5.5$$

and further, remembering that $k > 60$, we get

$$|2^\wedge A| \geq 2.06k - 3.$$

contradicting (17). Thus we can assume that

$$|2^\wedge A_1| < 2|A_1| + C_1 - 3,$$

and hence

$$|2^\wedge B_1| < 2|B_1| + C_1 - 3.$$

Then from Theorem 1 we get that B_1 is contained in an arithmetic progression $L \subset Z$ such that

$$|L| \leq |B_1| + 2C_1 + 2 = 2|B_1| - 3 \leq 2k - 3.$$

By our assumptions on B_1 (following (24)) it follows that

$$B_1 \subset L \subset \{0, 1, 2, \ldots, 2k-4\}. \tag{26}$$

All elements of F_p, and in particular those of A can be written in the form

$$a = u + vs, \quad 0 \leq s \leq p - 1,$$

for u, v as above. If A contained an element a with

$$6k < s < p - 4k \tag{27}$$

then in view of (24) and (26) and the fact that $p > 10k$ the sets $2^{\wedge}A_1$ and $A_1 + a$ would be disjoint and so, by (25) we would have

$$|2^{\wedge}A| \geq |A_1 + a| + |2^{\wedge}A_1| = m_1 + |2^{\wedge}A_1| \geq 3m_1 - 3$$

and hence by (23)

$$|2^{\wedge}A| > 2.06k - 3,$$

a contradiction to (17). Hence (27) does not hold for elements of A and it is easily seen that all elements of A can be written in the form $a = u + vs$ with

$$-4k \leq s \leq 6k.$$

As $p > 20k$, addition mod p on s in the above range $[-4k, 6k]$ coincides with ordinary addition. Thus A is isomorphic to the set $B \subset Z$ (with addition in Z) given by

$$B = \{s : u + vs \in A, -\tfrac{1}{2}(p-1) \leq s \leq \tfrac{1}{2}(p-1)\} \subset [-4k, 6k],$$

so that by (17)

$$|2^{\wedge}B| = |2^{\wedge}A| \leq 2k - 3 + C, \quad C < 0.06k.$$

By Theorem 1 it follows that B is contained in an arithmetic progression L' with

$$|L'| \leq k + 2C + 2,$$

where $C < 0.06k$, and so A is contained in the arithmetic progression

$$L = \{u + vs : s \in L'\}$$

with $|L| = |L'|$. This completes the proof of Theorem 2.

3.4. Application to Erdős Conjecture. — We now obtain the following corollary on the Erdős conjecture.

Corollary to Theorem 2. — *Let $A \subset F_p$ such that*

$$|A| = k < \frac{p}{50}, \quad k > 60.$$

Then

$$|2^{\wedge}A| \geq 2k - 3.$$

Proof. — If $|2^{\wedge}A| \geq 2k-2$ there is nothing to prove, so suppose that $|2^{\wedge}A| \leq 2k-3$. Then by Theorem 2 (with $C = 0$) we have $A \subset L$, where L is an arithmetic progression in F_p with $|L| \leq k + 2$. Since $p > 2k + 5$ and $|A| = k$, it follows that A is isomorphic to a set B of integers (under addition in Z) such that

$$|B| = k, \quad B \subseteq \{1, 2, \ldots, k+2\}.$$

Hence, using (3), we have

$$|2^{\wedge}A| = |2^{\wedge}B| \geq 2k - 3.$$

4. Postscript on the Erdős-Heilbronn conjecture

Rődseth [11], also using results of Freiman, has proved (4) for $p > ck$, for some positive constant c. More detailed arguments along the lines of the present paper and based on (7) can be used to obtain (4) for $p \geq 8k$, but some such restriction is essential to this approach.

Recently, two independent proofs have been given of the full Erdős-Heilbronn conjecture (4), without any restriction at all. For the first, see Dias da Silver and Hamidoune [4] and Nathanson [8]. The second, which uses only simple properties of polynomials over finite fields, is due to Alon, Nathanson and Ruzsa, [1],[2]. We are grateful to these authors for information about this work and to Professor Nathanson for the opportunity to see a preliminary version of his expository account of this topic in Nathanson [9].

References

[1] Alon N., Nathanson M. B. and Ruzsa I. Z., *Adding distinct congruence classes modulo a prime*, Amer. Math. Monthly, **102**, 1995, 250–255.

[2] Alon N., Nathanson M. B., and Ruzsa I. Z., *The polynomial method and restricted sums of congruence classes*, J. Number Theory, **56**, 1996, 404–417.

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

[4] Dias da Silva J. A. and Hamidoune Y. O., *Cyclic spaces for Grassman derivatives and additive theory*, Bull. London Math. Soc., **26**, 1994, 140–146.

[5] Erdős P. and Graham R. L., *Old and new results in combinatorial number theory*, Monographie 28 de L'Enseignement Math. Gen., 1980.

[6] Freiman G. A., *Foundations of a Structural Theory of Set Addition*, Translations of Mathematical Monographs, vol.37, Amer. Math. Soc., Providence, R.I., 1973.

[7] Mansfield R., *How many slopes in a polygon*, Israel J. Math., **39**, 1981, 265–272.

[8] Nathanson M. B., *Ballot numbers, alternating products and the Erdős-Heilbronn conjecture*, in Graham, R.L., and Nestril, J., (editors), *The Mathematics of Paul Erdős*, Springer, Heidelberg, 1994.

[9] Nathanson M. B., *Additive Number Theory 2: Inverse theorems and the geometry of sumsets*, Graduate Texts in Mathematics, Springer, New York, 1996.

[10] Pyber L., *Personal communication*, 1991.

[11] Rődset O. J., *Sums of distinct residues mod p*, Acta Arith., **65**, 1993, 181–184.

G.A. FREIMAN, School of Mathematical Sciences, Department of Mathematics, Raymond and Beverly Sackler, Faculty of Exact Sciences, Tel Aviv University, 69978 Tel Aviv, Israel
E-mail : grisha@math.tau.ac.il

L. LOW, Department of Pure Mathematics, University of Adelaide, Adelaide,, SA 5005, Australia
E-mail : llow@maths.adelaide.edu.au

J. PITMAN, Department of Pure Mathematics, University of Adelaide, Adelaide,, S.A. 5001, Australia
E-mail : jpitman@maths.adelaide.edu.au