The polynomial method and restricted sums of congruence classes *

Noga Alon † Melvyn B. Nathanson ‡ Imre Z. Ruzsa §

Abstract

We present a simple and general algebraic technique for obtaining results in Additive Number Theory, and apply it to derive various new extensions of the Cauchy-Davenport Theorem. In particular we obtain, for subsets $A_0, A_1, \ldots, A_k$ of the finite field Z_p, a tight lower bound on the minimum possible cardinality of

$$\{a_0 + a_1 + \ldots + a_k : a_i \in A_i, a_i \neq a_j \ for \ 0 \leq i < j \leq k\}$$

as a function of the cardinalities of the sets A_i.

1 Introduction

The Cauchy-Davenport Theorem, which has numerous applications in Additive Number Theory, is the following.

Theorem 1.1 ([3]) *If p is a prime, and A, B are two nonempty subsets of Z_p, then*

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

This theorem can be proved quickly by induction on $|B|$. A different proof has recently been found by the authors [1]. This proof is based on a simple algebraic technique, and its main advantage is that it

*J. of Number Theory 56 (1996), 404-417.

†Department of Mathematics, Raymond and Beverly Sackler Faculty of Exact Sciences, Tel Aviv University, Tel Aviv, Israel. Email: noga@math.tau.ac.il. Research supported in part by a United States Israeli BSF grant and by the Fund for Basic Research administered by the Israel Academy of Sciences.

‡Department of Mathematics, Lehman College (CUNY), Bronx, NY 10468, USA. Email: nathansn@dimacs.rutgers.edu. Research supported in part by grants from the PSC-CUNY Research Award Program.

§Mathematical Institute of the Hungarian Academy of Sciences, Budapest, P.O.B. 127, H-1364, Hungary. Email: h1140ruz@ella.hu. Research supported in part by DIMACS, Rutgers University, and by the Hungarian National Foundation for Scientific Research, Grant No. 1901.

extends easily and gives several related results. Some of the simplest results are described in [1]. In the present paper we describe the general technique and apply it to deduce various additional consequences. A representative example is the following.

Proposition 1.2 *Let p be a prime, and let $A_0, A_1, \ldots, A_k$ be nonempty subsets of the cyclic group Z_p. If $|A_i| \neq |A_j|$ for all $0 \leq i < j \leq k$ and $\sum_{i=0}^{k} |A_i| \leq p + \binom{k+2}{2} - 1$ then*

$$|\{a_0 + a_1 + \ldots + a_k : a_i \in A_i, a_i \neq a_j \quad for \quad all \quad i \neq j\}| \geq \sum_{i=0}^{k} |A_i| - \binom{k+2}{2} + 1.$$

Note that the very special case of this proposition in which $k = 1$, $A_0 = A$ and $A_1 = A - \{a\}$ for an arbitrary element $a \in A$ implies that if $A \subset Z_p$ and $2|A| - 1 \leq p + 2$ then the number of sums $a_1 + a_2$ with $a_1, a_2 \in A$ and $a_1 \neq a_2$ is at least $2|A| - 3$. This easily implies the following theorem, conjectured by Erdős and Heilbronn in 1964 (cf., e.g., [5]) and proved very recently by Dias Da Silva and Hamidoune [4], using some tools from linear algebra and the representation theory of the symmetric group.

Theorem 1.3 ([4]) *If p is a prime, and A is a nonempty subset of Z_p, then*

$$|\{a + a' : a, a' \in A, a \neq a'\}| \geq min\{p, 2|A| - 3\}.$$

The rest of the paper is organized as follows. In Section 2 we present and prove a general result and show how it implies the Cauchy Davenport theorem. In section 3 we consider the addition of distinct residues and prove Proposition 1.2 and some of its consequences. Section 4 contains some further applications of the general theorem and the final Section 5 concludes with various remarks and open problems.

2 The general theorem

Let p be a prime. For a polynomial $h = h(x_0, x_1, \ldots, x_k)$ over Z_p and for subsets $A_0, A_1, \ldots, A_k$ of Z_p, define

$$\oplus_h \sum_{i=0}^{k} A_i = \{a_0 + a_1 + \ldots + a_k : a_i \in A_i, \quad h(a_0, a_1, \ldots, a_k) \neq 0\}.$$

Our main tool is the following.

Theorem 2.1 *Let p be a prime and let $h = h(x_0, \ldots, x_k)$ be a polynomial over Z_p. Let $A_0, A_1, \ldots, A_k$ be nonempty subsets of Z_p, where $|A_i| = c_i + 1$ and define $m = \sum_{i=0}^{k} c_i - deg(h)$. If the coefficient of $\prod_{i=0}^{k} x_i^{c_i}$ in*

$$(x_0 + x_1 + \cdots + x_k)^m h(x_0, x_1, \ldots, x_k)$$

is nonzero (in Z_p) then

$$|\oplus_h \sum_{i=0}^{k} A_i| \geq m+1$$

(and hence $m < p$).

In order to prove this theorem we need the following simple and well known lemma, which is proved in various places (see, e.g., [2]). Since the argument is very short we reproduce it here.

Lemma 2.2 *Let $P = P(x_0, x_1, \ldots, x_k)$ be a polynomial in $k+1$ variables over an arbitrary field F. Suppose that the degree of P as a polynomial in x_i is at most c_i for $0 \leq i \leq k$, and let $A_i \subset F$ be a set of cardinality $c_i + 1$. If $P(x_0, x_1, \ldots, x_k) = 0$ for all $(k+1)$-tuples $(x_0, \ldots, x_k) \in A_0 \times A_1 \times \ldots \times A_k$, then $P \equiv 0$, that is: all the coefficients in P are zeros.*

Proof. We apply induction on k. For $k = 0$, the lemma is simply the assertion that a non-zero polynomial of degree c_0 in one variable can have at most c_0 distinct zeros. Assuming that the lemma holds for $k-1$, we prove it for k ($k \geq 1$). Given a polynomial $P = P(x_0, \ldots, x_k)$ and sets A_i satisfying the hypotheses of the lemma, let us write P as a polynomial in x_k, that is,

$$P = \sum_{i=0}^{c_k} P_i(x_0, \ldots, x_{k-1}) x_k^i,$$

where each P_i is a polynomial with x_j-degree bounded by c_j. For each fixed k-tuple $(x_0, \ldots, x_{k-1}) \in A_0 \times A_1 \times \ldots \times A_{k-1}$, the polynomial in x_k obtained from P by substituting the values of $x_0, \ldots, x_{k-1}$ vanishes for all $x_k \in A_k$, and is thus identically 0. Thus $P_i(x_0, \ldots, x_{k-1}) = 0$ for all $(x_0, \ldots, x_{k-1}) \in A_0 \times \ldots \times A_{k-1}$. Hence, by the induction hypothesis, $P_i \equiv 0$ for all i, implying that $P \equiv 0$. This completes the induction and the proof of the lemma. □

Proof of Theorem 2.1. Suppose the assertion is false, and let E be a (multi-) set of m (not necessarily distinct) elements of Z_p that contains the set $\oplus_h \sum_{i=0}^{k} A_i$. Let $Q = Q(x_0, \ldots, x_k)$ be the polynomial defined as follows:

$$Q(x_0, \ldots, x_k) = h(x_0, x_1, \ldots x_k) \cdot \prod_{e \in E} (x_0 + \ldots + x_k - e).$$

Note that

$$Q(x_0, \ldots, x_k) = 0 \quad for \quad all \quad (x_0, \ldots, x_k) \in (A_0, \ldots, A_k). \tag{1}$$

This is because for each such $(x_0, \ldots, x_k)$ either $h(x_0, \ldots, x_k) = 0$ or $x_0 + \ldots + x_k \in \oplus_h \sum_{i=0}^{k} A_i \subset E$. Note also that $deg(Q) = m + deg(h) = \sum_{i=0}^{k} c_i$ and hence the coefficient of the monomial $x_0^{c_0} \cdots x_k^{c_k}$ in Q

is the same as that of this monomial in the polynomial $(x_0 + \ldots + x_k)^m h(x_0, \ldots, x_k)$, which is nonzero, by assumption.

For each i, $0 \leq i \leq k$, define

$$g_i(x_i) = \prod_{a \in A_i} (x_i - a) = x_i^{c_i+1} - \sum_{j=0}^{c_i} b_{ij} x_i^j.$$

Let $\overline{Q} = \overline{Q}(x_0, \ldots x_k)$ be the polynomial obtained from the standard representation of Q as a linear combination of monomials by replacing, repeatedly, each occurrence of $x_i^{c_i+1}$ by $\sum_{j=0}^{c_i} b_{ij} x_i^j$. Note that since for every $x_i \in A_i$, $x_i^{c_i+1}$ is equal to this sum, equation (1) holds for $\overline{Q}$ as well. However, the x_i-degree of $\overline{Q}$ is at most c_i and hence, by Lemma 2.2 it is identically zero. To obtain a contradiction, we claim that the coefficient of the monomial $\prod_{i=0}^k x_i^{c_i}$ in $\overline{Q}$ is not 0 (in Z_p). To see this note that the coefficient of this monomial in Q is nonzero modulo p by assumption. The crucial observation is that the coefficient of this monomial in $\overline{Q}$ is equal to its coefficient in Q. This is because the process of replacing each of the expressions $x_i^{c_i+1}$ by $\sum_{j=0}^{c_i} b_{ij} x_i^j$ does not affect the above monomial itself. Moreover, since the total degree of Q is $\sum_{i=0}^k c_i$ and the process of replacing the expressions as above strictly reduces degrees, this process cannot create any additional scalar multiples of this monomial, proving the claim.

It thus follows that $\overline{Q}$ is not identically zero, supplying the desired contradiction and completing the proof. □

The simplest application of Theorem 2.1 is the following proof of the Cauchy Davenport Theorem (Theorem 1.1).

Proof of Theorem 1.1. If $|A| + |B| \leq p + 1$ apply Theorem 2.1 with $h \equiv 1$, $k = 1$, $A_0 = A$, $A_1 = B$ and $m = |A| + |B| - 2$. Here $c_0 = |A| - 1$, $c_1 = |B| - 1$ and the relevant coefficient is $\binom{m}{c_0}$ which is nonzero modulo p (as $m < p$). If $|A| + |B| > p + 1$ simply replace B by a subset B' of cardinality $p + 1 - |A|$ and apply the result above to A and B' to conclude that in this case $|A + B| \geq |A + B'| = p$. □

3 Adding distinct residues

The following Lemma can be easily deduced from the known results about the Ballot problem (see, e.g., [8]), as well as from the known connection between this problem and the hook formula for the number of Young tableaux of a given shape. Here we present a simple, self contained proof.

Lemma 3.1 *Let $c_0, \ldots, c_k$ be nonnegative integers and suppose that $\sum_{i=0}^k c_i = m + \binom{k+1}{2}$, where m is a*

nonnegative integer. Then the coefficient of $\prod_{i=0}^{k} x_i^{c_i}$ *in the polynomial*

$$(x_0 + x_1 + \ldots + x_k)^m \prod_{k \geq i > j \geq 0} (x_i - x_j)$$

is

$$\frac{m!}{c_0! c_1! \ldots c_k!} \prod_{k \geq i > j \geq 0} (c_i - c_j).$$

Proof. The product $\prod_{k \geq i > j \geq 0}(x_i - x_j)$ is precisely the Vandermonde determinant $det\ (x_i^j)_{0 \leq i \leq k, 0 \leq j \leq k}$ which is equal to the sum

$$\sum_{\sigma \in S_{k+1}} (-1)^{sign(\sigma)} \prod_{i=0}^{k} x_i^{\sigma(i)},$$

where S_{k+1} denotes the set of all permutations of the $k+1$ symbols $0, \ldots, k$. It thus follows that the required coefficient, which we denote by C, is given by

$$C = \sum_{\sigma \in S_{k+1}} (-1)^{sign(\sigma)} \frac{m!}{(c_0 - \sigma(0))!(c_1 - \sigma(1))! \ldots (c_k - \sigma(k))!}.$$

Similarly, the product $\prod_{k \geq i > j \geq 0}(c_i - c_j)$ is the Vandermonde determinant $det\ (c_i^j)_{0 \leq i \leq k, 0 \leq j \leq k}$. For two integers $r \geq 1$ and s let $(s)_r$ denote the product $s(s-1)\cdots(s-r+1)$ and define also $(s)_0 = 1$ for all s. Observe that the matrix $((c_i)_j)_{0 \leq i \leq k, 0 \leq j \leq k}$ can be obtained from the matrix $(c_i^j)_{0 \leq i \leq k, 0 \leq j \leq k}$ by subtracting appropriate linear combinations of the columns with indices less than j from the column indexed by j, for each $j = k, k-1, \ldots, 1$. Therefore, these two matrices have the same determinant. It thus follows that

$$\frac{m!}{c_0! c_1! \ldots c_k!} \prod_{k \geq i > j \geq 0} (c_i - c_j) = \frac{m!}{c_0! c_1! \ldots c_k!} det\ ((c_i)_j)_{0 \leq i \leq k, 0 \leq j \leq k}$$

$$= \frac{m!}{c_0! c_1! \ldots c_k!} \sum_{\sigma \in S_{k+1}} (-1)^{sign(\sigma)} (c_0)_{\sigma(0)} (c_1)_{\sigma(1)} \cdots (c_k)_{\sigma(k)}$$

$$= \sum_{\sigma \in S_{k+1}} (-1)^{sign(\sigma)} \frac{m!}{(c_0 - \sigma(0))!(c_1 - \sigma(1))! \ldots (c_k - \sigma(k))!} = C,$$

completing the proof. □

Let p be a prime, and let $A_0, A_1, \ldots, A_k$ be nonempty subsets of the cyclic group Z_p. Define

$$\oplus_{i=0}^{k} A_i = \{a_0 + a_1 + \ldots + a_k : a_i \in A_i, a_i \neq a_j \ \ for \ \ all \ \ i \neq j\}.$$

In this notation, the assertion of Proposition 1.2 is that if $|A_i| \neq |A_j|$ for all $0 \leq i < j \leq k$ and $\sum_{i=0}^{k} |A_i| \leq p + \binom{k+2}{2} - 1$ then

$$|\oplus_{i=0}^{k} A_i| \geq \sum_{i=0}^{k} |A_i| - \binom{k+2}{2} + 1.$$

Proof of Proposition 1.2. Define

$$h(x_0,\ldots,x_k)=\prod_{k\geq i>j\geq 0}(x_i-x_j),$$

and note that for this h, the sum $\oplus_{i=0}^{k}A_i$ is precisely the sum $\oplus_h \sum_{i=0}^{k}A_i$. Suppose $|A_i|=c_i+1$ and put

$$m=\sum_{i=0}^{k}c_i-\binom{k+1}{2}\ \ (=\sum_{i=0}^{k}|A_i|-\binom{k+2}{2}).$$

By assumption $m<p$ and by Lemma 3.1 the coefficient of $\prod_{i=0}^{k}x_i^{c_i}$ in

$$h\cdot(x_0+\ldots+x_k)^m$$

is

$$\frac{m!}{c_0!c_1!\ldots c_k!}\prod_{k\geq i>j\geq 0}(c_i-c_j),$$

which is nonzero modulo p, since $m<p$ and the numbers c_i are pairwise distinct. Since $m=\sum_{i=0}^{k}c_i+deg(h)$, the desired result follows from Theorem 2.1. □

Theorem 3.2 *Let p be a prime, and let $A_0,\ldots,A_k$ be nonempty subsets of Z_p, where $|A_i|=b_i$, and suppose $b_0\geq b_1\ldots\geq b_k$. Define $b'_0,\ldots,b'_k$ by*

$$b'_0=b_0\ \ and\ \ \ \ b'_i=min\{b'_{i-1}-1,b_i\},\ \ for\ \ 1\leq i\leq k. \tag{2}$$

If $b'_k>0$ then

$$|\oplus_{i=0}^{k}A_i|\geq min\{p,\sum_{i=0}^{k}b'_i-\binom{k+2}{2}+1\}.$$

Moreover, the above estimate is sharp for all possible values of $p\geq b_0\geq\ldots\geq b_k$.

Proof. If $b'_i\leq 0$ for some i then $b'_k\leq 0$ and thus $b'_i>0$ for all i. For each i, $1\leq i\leq k$, let A'_i be an arbitrary subset of cardinality b'_i of A_i. Note that the cardinalities of the sets A'_i are pairwise distinct and that $\oplus_{i=0}^{k}A'_i\subset\oplus_{i=0}^{k}A_i$. If $\sum_{i=0}^{k}b'_i\leq p+\binom{k+2}{2}-1$ then

$$|\oplus_{i=0}^{k}A_i|\geq|\oplus_{i=0}^{k}A'_i|\geq\sum_{i=0}^{k}b'_i-\binom{k+2}{2}+1,$$

by Proposition 1.2, as needed. Otherwise, we claim that there are $1\leq b"_k<b"_{k-1}<\ldots<b"_0$, where $b"_i\leq b'_i$ for all i and $\sum_{i=0}^{k}b"_i=p+\binom{k+2}{2}-1$. To prove this claim, consider the operator T that maps sequences of integers $(d_0,\ldots,d_k)$ with $d_0>d_1\ldots>d_k\geq 1$ to sequences of the same kind defined as

follows. The sequence $(k+1,\ldots,1)$ is mapped to itself. For any other sequence $(d_0,\ldots,d_k)$, let j be the largest index for which $d_j > k+1-j$ and define $T(d_0,\ldots,d_k) = (d_0,\ldots,d_{j-1},d_j-1,d_{j+1},\ldots,d_k)$. Clearly, the sum of the elements in $T(D)$ is one less than the sum of the elements of D for every D that differs than $(k+1,\ldots,1)$, and thus, by repeatedly applying T to our sequence $(b'_0,\ldots,b'_k)$ we get the desired sequence $(b"_0,\ldots,b"_k)$, proving the claim.

Returning to the proof of the theorem in case $\sum_{i=0}^{k} b'_i > p + \binom{k+2}{2} - 1$, let $b"_i$ be as in the claim, and apply Proposition 1.2 to arbitrary subsets $A"_i$ of cardinality $b"_i$ of A'_i.

It remains to show that the estimate is best possible for all $p \geq b_0 \geq \ldots, b_k \geq 1$. This is shown by defining $A_i = \{1,2,3,\ldots,b_i\}$ for all i. It is easy to check that for these sets A_i, the set $\oplus_{i=0}^{k} A_i$ is empty if $b'_k \leq 0$ and in any case it is contained in the set of consecutive residues

$$\binom{k+2}{2}, \binom{k+2}{2}+1, \ldots, \sum_{i=0}^{k} b'_i,$$

where the numbers b'_i are defined by (2). This completes the proof. □

The following result of Dias da Silva and Hamidoune [4] is a simple consequence of (a special case of) the above theorem.

Theorem 3.3 ([4]) *Let p be a prime and let A be a nonempty subset of Z_p. Let $s^\wedge A$ denote the set of all sums of s distinct elements of A. Then $|s^\wedge A| \geq min\{p, s|A| - s^2 + 1\}$.*

Proof. If $|A| < s$ there is nothing to prove. Otherwise put $s = k+1$ and apply Theorem 3.2 with $A_i = A$ for all i. Here $b'_i = |A| - i$ for all $0 \leq i \leq k$ and hence

$$|(k+1)^\wedge A| = |\oplus_{i=0}^{k} A_i| \geq min\{p, \sum_{i=0}^{k}(|A|-i) - \binom{k+2}{2} + 1\}$$

$$= min\{p, (k+1)|A| - \binom{k+1}{2} - \binom{k+2}{2} + 1\} = min\{p, (k+1)|A| - (k+1)^2 + 1\}.$$

□

The case $s = 2$ of the last theorem settles a problem of Erdős and Heilbronn. Partial results on this conjecture (before its proof in [4]) had been obtained in [12], [9], [13], [11], and [6].

4 Further examples

An easy application of Theorem 2.1 is the following result, proved in [1].

Proposition 4.1 *If p is a prime and A, B are two nonempty subsets of Z_p, then*

$$|\{a+b : a \in A, b \in B, ab \neq 1\}| \geq min\{p, |A|+|B|-3\}.$$

The proof is by applying Theorem 2.1 with $k=1$, $h = x_0x_1 - 1$, $A_0 = A$, $A_1 = B$, and $m = |A|+|B|-4$. It is also shown in [1] that the above estimate is tight in all nontrivial cases. Two easy extensions of the above proposition are the following.

Proposition 4.2 *If p is a prime and $A_0, A_1, \ldots, A_k$ are nonempty subsets of Z_p, then for every $g \in Z_p$,*

$$|\{a_0 + \ldots + a_k : a_i \in A_i, \prod_{i=0}^{k} a_i \neq g\}| \geq min\{p, \sum_{i=0}^{k} |A_i| - 2k - 1\}.$$

Proof. If $g = 0$ the result follows trivially from the Cauchy Davenport Theorem, and we thus assume that $g \neq 0$. Suppose, first, that $|A_i| > 1$ for all i. If $\sum_{i=0}^{k} |A_i| - 2k - 2 < p$ apply Theorem 2.1 with $h = \prod_{i=0}^{k} x_i - g$ and $m = \sum_{i=0}^{k} |A_i| - 2k - 2$. Here $c_i = |A_i| - 1$ and the coefficient of $\prod_{i=0}^{k} x_i^{c_i}$ in $h \cdot (x_0 + \ldots + x_k)^m$ is $m!/\prod(c_i - 1)!$, which is nonzero modulo p, implying the desired result. Otherwise, replace some of the sets A_i by nonempty subsets A_i' satisfying $|A_i'| > 1$ and $\sum_{i=0}^{k} |A_i'| = p + 2k + 1$ and apply the result to the sets A_i'.

When $|A_i| = 1$ for several sets A_i it is easy to deduce the result by applying the previous case to the sets A_j of cardinality greater than 1 with an appropriately modified value of g. We omit the details. □

Proposition 4.3 *If p is a prime and $A_0, A_1, \ldots, A_k$ are subsets of Z_p, where $|A_i| \geq k+1$ for all i, then*

$$|\{a_0 + \ldots + a_k : a_i \in A_i, a_i \cdot a_j \neq 1 \ for\ all\ 0 \leq i < j \leq k\}| \geq min\{p, \sum_{i=0}^{k} |A_i| - (k+1)^2 + 1\}.$$

Proof. If $\sum_{i=0}^{k} |A_i| - (k+1)^2 < p$ apply Theorem 2.1 with $h = \prod_{0 \leq i < j \leq k} (x_i \cdot x_j - 1)$ and $m = \sum_{i=0}^{k} |A_i| - (k+1)^2$. Otherwise, replace some of the sets A_i by nonempty subsets A_i' satisfying $\sum_{i=0}^{k} |A_i'| = p + (k+1)^2$ and apply the result to the sets A_i'. □

Remark. The estimate in the last proposition is *not* sharp. In particular, it is not too difficult to show that if every A_i is of cardinality greater than $2 + \log_2(k+1)$ then the set

$$S = \{a_0 + \ldots + a_k : a_i \in A_i, a_i \cdot a_j \neq 1 \ for\ all\ 0 \leq i < j \leq k\} \tag{3}$$

is nonempty. In fact, the following slightly stronger result is valid.

Proposition 4.4 *If p is a prime and $A_0, \ldots, A_k$ are subsets of $Z_p - \{1, -1\}$, each of cardinality $s > \log_2(k+1)$ then the set S defined in (3) is nonempty. This is tight for all $s \leq (p-3)/2$, as for each such s there is a collection of 2^s sets $A_i \subset Z_p - \{1, -1\}$ of cardinality s each for which the set S from (3) is empty.*

Proof. If $s > \log_2(k+1)$, let H be a random subset of $(p-1)/2$ of the elements of $Z_p - \{1,-1\}$ obtained by choosing, for each pair $x, 1/x \in Z_p - \{1,-1,0\}$, randomly and independently, exactly one of them to be a member of H. In addition, add 0 to H. If $A_i \cap H \neq \emptyset$ for every i, the desired result follows by choosing $a_i \in A_i \cap H$ and by observing that $g \cdot g' \neq 1$ for every (not necessarily distinct) $g, g' \in H$. However, for every fixed i, if A_i contains 0 or contains both x and $1/x$ for some $x \in Z_p - \{1,-1,0\}$ then certainly $A_i \cap H \neq \emptyset$. Otherwise, the probability that $A_i \cap H = \emptyset$ is precisely $2^{-s} < 1/(k+1)$ showing that with positive probability $A_i \cap H \neq \emptyset$ for all i, as needed.

If $s \leq (p-3)/2$ let $x_1, \ldots, x_s$ be s elements in $Z_p - \{1,-1,0\}$ so that the product of no two is 1. For each of the 2^s vectors $\delta = (\delta_1, \ldots, \delta_s) \in \{-1,1\}^s$ define a subset A_δ by $A_\delta = \{x_1^{\delta_1}, \ldots, x_s^{\delta_s}\}$. It is easy to see that every choice of a member from each A_δ must contain some element x_i and its inverse. This completes the proof. □

We conclude the section with the following.

Proposition 4.5 *If p is a prime and A, B are two nonempty subsets of Z_p, with $|A| > |B|$ then for any $e \in Z_p$*

$$|\{a+b : a \in A, b \in B, ab \neq e \text{ and } a \neq b\}| \geq min\{p, |A| + |B| - 4\}. \tag{4}$$

Proof. If $|B| \leq 2$ and $b' \in B$, then A contains a subset A' of $|A|-2$ elements which are neither b' nor eb'^{-1} and hence in this case

$$|\{a+b : a \in A, b \in B, ab \neq e \text{ and } a \neq b\}| \geq |b' + A'| = |A| - 2 \geq |A| + |B| - 4,$$

as needed. We thus assume that $|A| > |B| \geq 3$. If $|A| + |B| - 5 < p$, apply Theorem 2.1 with $k = 1$, $h = (x_0 - x_1)(x_0 \cdot x_1 - e)$, $A_0 = A$, $A_1 = B$ and $m = |A| + |B| - 5$. Here $c_0 = |A| - 1$, $c_1 = |B| - 1$, and the coefficient of $x_0^{c_0} \cdot x_1^{c_1}$ in $h \cdot (x_0 + x_1)^m$ is

$$\binom{m}{c_0 - 2} - \binom{m}{c_0 - 1} = \frac{m!}{(c_0-1)!\,(c_1-1)!}(c_0 - c_1),$$

which is nonzero modulo p. If $|A| + |B| - 5 \geq p$ replace B by a subset B' of cardinality $p + 4 - |A|$ $(< |A|)$ and apply the result to A and B' to conclude that in this case $|A + B| \geq |A + B'| = p$. □

Remark. The last estimate is tight for all possible cardinalities $|A| > |B| > 1$ as shown by the following example.

$$A = \{a, a+d, a+2d, \ldots, a+c_0 d\}, \quad B = \{a, a+d, a+2d, \ldots, a+c_1 d\},$$

where a, d are chosen so that $a(a+d) = (a+c_0 d)(a+c_1 d) = e$. The only solution of these equations in case $c_1 = 1$ (i.e., $|B| = 2$), is $e = 0$ and $d = -a$ supplying the two sets

$$A = \{a, 0, \ldots, -(c_0 - 1)a\} \quad B = \{a, 0\}.$$

If $c_1 \geq 2$ the possible solutions are given by

$$a = \sqrt{\frac{c_0 c_1 e}{(c_0-1)(c_1-1)}}, \quad d = -\frac{(c_0+c_1-1)a}{c_0 c_1}.$$

Such a solution exists for every e for which the quantity $(c_0c_1e)(c_0-1)(c_1-1)$ is a quadratic residue.
For $|B| = 1$ the right hand side of (4) can be improved to $|A| - 2 = |A| + |B| - 3$, as explained above, and this is trivially tight.
If $|A| = |B| = s > 2$ then, by applying Proposition 4.5 to A and a subset of cardinality $s-1$ of B we conclude that in this case for every $e \in Z_p$

$$|\{a+b : a \in A, b \in B, ab \neq e \text{ and } a \neq b\}| \geq min\{p, |A| + |B| - 5\}.$$

It is not difficult to check that if $s \leq 2$ then the set in the left hand side of the last inequality may be empty. For all $s \geq 3$ the above estimate is tight, as shown by an easy modification of the example described above.

5 Concluding remarks and open problems

1. All the results proved above hold for subsets of an arbitrary field of characteristic p instead of Z_p, with the same proof.

2. Theorem 3.3 implies that if A is a subset of Z_p and $|A| \geq (p+s^2-1)/s$, then $s\hat{}A = Z_p$. This can be used to construct certain explicit codes for write once memories, a notion introduced by Rivest and Shamir in [14]. Here is a brief description of this application. Motivated by the existence of memory devices as optical disks or paper tapes that have a number of "write once" bits (called *wits*), each of which contains initially a 0 that can be *irreversibly* changed to a 1, the authors of [14] considered the problem of finding efficient encoding schemes that enable one to use a small number of wits to represent and update one of v possible values t times. Following [14] let us denote by $w(< v >^t)$ the minimum possible number of wits needed for this task. It is shown in [14] that $w(< v >^t) = \Theta(max\{t, \frac{t \log v}{\log t}\})$ and it is conjectured that in fact as t and v tend to infinity

$$w(< v >^t) = (1+o(1))max\{t, \frac{t \log v}{\log t}\}.$$

This conjecture is false, since it is not difficult to show that, e.g., for every fixed positive $\epsilon < 0.5$,

$$w(< v >^{\epsilon v}) \geq 2\epsilon v.$$

To see this, notice that since there are at most w ways to update a written w-wit value by changing a single 0 to a 1, there is a choice of updating the required values that will force any scheme using less than $v-1$ wits to change at least 2 wits from 0 to 1 in every update, implying the last inequality.

Theorem 3.3 can be used to supply an explicit scheme that resembles and improves one of the schemes of [14] and shows that for every prime p

$$w(< p >^{0.35p}) \leq p-1.$$

Although one can obtain somewhat better schemes this one has the advantage that it may be useful for "dirty" memories, that is, memories in which some (small) number of arbitrarily chosen wits have been set to a 1- see [14] for more details on this issue. The scheme works as follows. Let the wits be $w_1, \ldots, w_{p-1}$. A given configuration always reperesents the value $(\sum_{i:\ w_i=1} i)\ (mod\ p)$. By Theorem 3.3, as long as there are at least $(p+s^2-1)/s$ wits with a 0, it is possible to make any required update by changing at most s wits to a 1. Therefore, one can use this scheme for at least t updates, where for large p, t satisfies

$$t \geq (1+o(1))p[(1-1/2)1/2+(1/2-1/3)1/3+(1/3-1/4)1/4+\ldots] = (1+o(1))p[2-\frac{\pi^2}{6}] > 0.35p.$$

We omit the details.

3. It should be clear from the results in the previous two sections that there are numerous additional possible applications of Theorem 2.1, although many of them would not be very natural. As shown in Section 3, the main problem in applying the theorem in various cases is the computation of the required coefficient modulo p. In some cases this can lead to interesting combinatorial questions. Thus, for example, suppose we wish to apply the theorem to bound the minimum possible cardinality of the set

$$\{a_0+\ldots+a_k : a_i \in A_i, a_i - a_j \notin E\},$$

where here A_i and $E=-E$ are subsets of Z_p. (The case $E=\{0\}$ is the one considered in Section 3). Here one should consider the polynomial

$$h = \prod_{e \in E} \prod_{0 \leq i < j \leq k} (x_i - x_j - e)$$

and compute the appropriate coefficient in $h \cdot (x_0+\ldots+x_k)^m$. This task seems complicated, although there is a considerable amount of known information on some of the coefficients of monomials of degree $deg(h)$ of h. Note that the coefficients of such monomials are independent of E and depend

only on its cardinality $|E|$. In particular, Dyson's conjecture (first proved by Gunson [7] and Wilson [18]) determines the coefficient of $\prod_{i=0}^{k} x_i^{k|E|/2}$ for even values of $|E|$. See also [15], [19] for some related results.

4. Vosper [16], [17] determined all cases of equality in the Cauchy Davenport Theorem. It would be interesting to prove an anlogous result for Proposition 1.2, Theorem 1.3 or the results in Section 4.

5. There are numerous variants of the Cauchy Davenport Theorem for the non-prime case, including results by Chowla, Scherk, Sheperdson, Kneser and others. See [10] for many of these results. It would be interesting to obtain non-prime analogs for the results obtained here.

Acknowledgment The first author would like to thank Doron Zeilberger for helpful discussions.

References

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

[2] N. Alon and M. Tarsi. Colorings and orientations of graphs. *Combinatorica*, 12:125–134, 1992.

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

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

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

[6] 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. In: *Structure Theory of Set Addition*, June 1993, CIRM Marseille, pp. 99-108, 1993.

[7] J. Gunson, Proof of a conjecture of Dyson in the statistical theory of energy levels. *J. Math. Phys.* 3: 752–753, 1962.

[8] M. P. A. Macmahon, *Combinatory Analysis.* Chelsea Publishing Company, 1915, Chapter V.

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

[10] M. B. Nathanson. *Additive Number Theory: 2. Inverse Theorems and the Geometry of Sumsets.* Springer-Verlag, New York, 1995.

[11] L. Pyber. On the Erdős-Heilbronn conjecture. Personal communication.

[12] U.-W. Rickert. *Über eine Vermutung in der additiven Zahlentheorie.* PhD thesis, Tech. Univ. Braunschweig, 1976.

[13] Ö. J. Rödseth. Sums of distinct residues mod p. *Acta Arith.* 65: 181–184, 1994.

[14] R. L. Rivest and A. Shamir. How to reuse a "write once" memory. *Information and Computation*, 55: 1–19, 1982.

[15] J. R. Stembridge, A short proof of Macdonald's Conjecture for the root systems of type A, *Proc. AMS* 102: 777–786, 1988.

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

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

[18] K. Wilson. Proof of a conjecture of Dyson. *J. Math. Phys.* 3: 1040–1043, 1962.

[19] D. Zeilberger. A combinatorial proof of Dyson's conjecture. *Discrete Math.* 41: 317–321, 1982.