

# ThePolynomialMethod

Nick Adfor

January 19, 2026

## 0.1 Introduction

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

**Theorem 1** (Cauchy Davenport Theorem [3]). *If  $p$  is a prime, and  $A, B$  are two nonempty subsets of  $\mathbb{Z}_p$ , 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 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 2.** *Let  $p$  be a prime, and let  $A_0, A_1, \dots, A_k$  be nonempty subsets of the cyclic group  $\mathbb{Z}_p$ . 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*

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

Note that the very special case of this proposition in which  $k = 1$ ,  $A_0 = A$  and  $A_1 = A \setminus \{a\}$  for an arbitrary element  $a \in A$  implies that if  $A \subset \mathbb{Z}_p$  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 3** ([4]). *If  $p$  is a prime, and  $A$  is a nonempty subset of  $\mathbb{Z}_p$ , 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 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.

## 0.2 The General Theorem

Let  $p$  be a prime. For a polynomial  $h = h(x_0, x_1, \dots, x_k)$  over  $\mathbb{Z}_p$  and for subsets  $A_0, A_1, \dots, A_k$  of  $\mathbb{Z}_p$ , define

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

Our main tool is the following.

**Theorem 4.** Let  $p$  be a prime and let  $h = h(x_0, \dots, x_k)$  be a polynomial over  $\mathbb{Z}_p$ . Let  $A_0, A_1, \dots, A_k$  be nonempty subsets of  $\mathbb{Z}_p$ , 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

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

is nonzero (in  $\mathbb{Z}_p$ ) then

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

(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 5.** Let  $P = P(x_0, x_1, \dots, x_k)$  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  $P(x_0, x_1, \dots, x_k) = 0$  for all  $(k+1)$ -tuples  $(x_0, \dots, x_k) \in A_0 \times A_1 \times \dots \times A_k$ , 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  $P = P(x_0, \dots, x_k)$  and sets  $A_i$  satisfying the hypotheses of the lemma, let us write  $P$  as a polynomial in  $x_k$ , that is,

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

where each  $P_i$  is a polynomial with  $x_j$ -degree bounded by  $c_j$ . For each fixed  $k$ -tuple  $(x_0, \dots, x_{k-1}) \in A_0 \times A_1 \times \dots \times A_{k-1}$ , the polynomial in  $x_k$  obtained from  $P$  by substituting the values of  $x_0, \dots, x_{k-1}$  vanishes for all  $x_k \in A_k$ , and is thus identically 0. Thus  $P_i(x_0, \dots, x_{k-1}) = 0$  for all  $(x_0, \dots, x_{k-1}) \in A_0 \times \dots \times A_{k-1}$ . 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.  $\square$

*Proof of Theorem 4.* Suppose the assertion is false, and let  $E$  be a (multi-)set of  $m$  (not necessarily distinct) elements of  $\mathbb{Z}_p$  that contains the set  $\bigoplus_h \sum_{i=0}^k A_i$ . Let  $Q = Q(x_0, \dots, x_k)$  be the polynomial defined as follows:

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

Note that

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

This is because for each such  $(x_0, \dots, x_k)$  either  $h(x_0, \dots, x_k) = 0$  or  $x_0 + \dots + x_k \in \bigoplus_h \sum_{i=0}^k A_i \subset E$ . 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  $(x_0 + \dots + x_k)^m h(x_0, \dots, x_k)$ , 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  $\bar{Q} = \bar{Q}(x_0, \dots, x_k)$  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  $\bar{Q}$  as well. However, the  $x_i$ -degree of  $\bar{Q}$  is at most  $c_i$  and hence, by Lemma 5 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  $\bar{Q}$  is not 0 (in  $\mathbb{Z}_p$ ). 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  $\bar{Q}$  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  $\bar{Q}$  is not identically zero, supplying the desired contradiction and completing the proof.  $\square$

The simplest application of Theorem 4 is the following proof of the Cauchy-Davenport Theorem (Theorem 3).

*Proof of Theorem 3.* If  $|A| + |B| \leq p + 1$  apply Theorem 4 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  $|A + B| \geq |A + B'| = p$ .  $\square$

### 0.3 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 6.** *Let  $c_0, \dots, c_k$  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*

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

is

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

*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

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

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

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

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  $j = k, k-1, \dots, 1$ . Therefore, these two matrices have the same determinant. It thus follows that

$$\begin{aligned} \frac{m!}{c_0!c_1!\cdots c_k!} \prod_{k \geq i > j \geq 0} (c_i - c_j) &= \frac{m!}{c_0!c_1!\cdots c_k!} \det((c_i)_j)_{0 \leq i \leq k, 0 \leq j \leq k} \\ &= \frac{m!}{c_0!c_1!\cdots c_k!} \sum_{\sigma \in S_{k+1}} (-1)^{\text{sign}(\sigma)} (c_0)_{\sigma(0)} (c_1)_{\sigma(1)} \cdots (c_k)_{\sigma(k)} \\ &= \sum_{\sigma \in S_{k+1}} (-1)^{\text{sign}(\sigma)} \frac{m!}{(c_0 - \sigma(0))!(c_1 - \sigma(1))! \cdots (c_k - \sigma(k))!} = C, \end{aligned}$$

completing the proof.  $\square$

Let  $p$  be a prime, and let  $A_0, A_1, \dots, A_k$  be nonempty subsets of the cyclic group  $\mathbb{Z}_p$ . Define

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

In this notation, the assertion of Proposition 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

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

*Proof of Proposition 2.* Define

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

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

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

By assumption  $m < p$  and by Lemma 6 the coefficient of  $\prod_{i=0}^k x_i^{c_i}$  in  $h \cdot (x_0 + \cdots + x_k)^m$  is

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

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 4.  $\square$

**Theorem 7.** *Let  $p$  be a prime, and let  $A_0, \dots, A_k$  be nonempty subsets of  $\mathbb{Z}_p$ , where  $|A_i| = b_i$ , and suppose  $b_0 \geq b_1 \geq \cdots \geq b_k$ . Define  $b'_0, \dots, b'_k$  by*

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

If  $b'_k > 0$  then

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

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

*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  $\bigoplus_{i=0}^k A'_i \subset \bigoplus_{i=0}^k A_i$ . If  $\sum_{i=0}^k b'_i \leq p + \binom{k+2}{2} - 1$  then

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

by Proposition 2, as needed. Otherwise, we claim that there are  $1 \leq b''_k < b''_{k-1} < \dots < b''_0$ , 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  $(d_0, \dots, d_k)$  with  $d_0 > d_1 > \dots > d_k \geq 1$  to sequences of the same kind defined as follows. The sequence  $(k+1, \dots, 1)$  is mapped to itself. For any other sequence  $(d_0, \dots, d_k)$ , let  $j$  be the largest index for which  $d_j > k+1-j$  and define  $T(d_0, \dots, d_k) = (d_0, \dots, d_{j-1}, d_j - 1, d_{j+1}, \dots, d_k)$ . 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 from  $(k+1, \dots, 1)$ , and thus, by repeatedly applying  $T$  to our sequence  $(b'_0, \dots, b'_k)$  we get the desired sequence  $(b''_0, \dots, b''_k)$ , 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 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  $p \geq b_0 \geq \dots \geq b_k \geq 1$ . This is shown by defining  $A_i = \{1, 2, 3, \dots, b_i\}$  for all  $i$ . It is easy to check that for these sets  $A_i$ , the set  $\bigoplus_{i=0}^k A_i$  is empty if  $b'_k \leq 0$  and in any case it is contained in the set of consecutive residues

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

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

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

**Theorem 8 ([4]).** *Let  $p$  be a prime and let  $A$  be a nonempty subset of  $\mathbb{Z}_p$ . 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 7 with  $A_i = A$  for all  $i$ . Here  $b'_i = |A| - i$  for all  $0 \leq i \leq k$  and hence

$$\begin{aligned} |(k+1) \wedge A| &= |\bigoplus_{i=0}^k A_i| \geq \min \left\{ p, \sum_{i=0}^k (|A| - i) - \binom{k+2}{2} + 1 \right\} \\ &= \min \left\{ p, (k+1)|A| - \binom{k+1}{2} - \binom{k+2}{2} + 1 \right\} \\ &= \min \{p, (k+1)|A| - (k+1)^2 + 1\}. \end{aligned}$$

$\square$

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].

## 0.4 Further Examples

An easy application of Theorem 4 is the following result, proved in [1].

**Proposition 9.** *If  $p$  is a prime and  $A, B$  are two nonempty subsets of  $\mathbb{Z}_p$ , then*

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

*Proof.* The proof is by applying Theorem 4 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.  $\square$

Two easy extensions of the above proposition are the following.

**Proposition 10.** *If  $p$  is a prime and  $A_0, A_1, \dots, A_k$  are nonempty subsets of  $\mathbb{Z}_p$ , then for every  $g \in \mathbb{Z}_p$ ,*

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

*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 4 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  $h \cdot (x_0 + \dots + x_k)^m$  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.  $\square$

**Proposition 11.** *If  $p$  is a prime and  $A_0, A_1, \dots, A_k$  are subsets of  $\mathbb{Z}_p$ , where  $|A_i| \geq k + 1$  for all  $i$ , then*

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

*Proof.* If  $\sum_{i=0}^k |A_i| - (k+1)^2 < p$  apply Theorem 4 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  $A'_i$ .  $\square$

**Remark 1.** *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*

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

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

**Proposition 12.** *If  $p$  is a prime and  $A_0, \dots, A_k$  are subsets of  $\mathbb{Z}_p \setminus \{1, -1\}$ , 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  $A_i \subset \mathbb{Z}_p \setminus \{1, -1\}$  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  $\mathbb{Z}_p \setminus \{1, -1\}$  obtained by choosing, for each pair  $x, 1/x \in \mathbb{Z}_p \setminus \{1, -1, 0\}$ , 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  $x \in \mathbb{Z}_p \setminus \{1, -1, 0\}$  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  $x_1, \dots, x_s$  be  $s$  elements in  $\mathbb{Z}_p \setminus \{1, -1, 0\}$  so that the product of no two is 1. For each of the  $2^s$  vectors  $\delta = (\delta_1, \dots, \delta_s) \in \{-1, 1\}^s$  define a subset  $A_\delta$  by  $A_\delta = \{x_1^{\delta_1}, \dots, x_s^{\delta_s}\}$ . It is easy to see that every choice of a member from each  $A_\delta$  must contain some element  $x_i$  and its inverse. This completes the proof.  $\square$

We conclude the section with the following.

**Proposition 13.** *If  $p$  is a prime and  $A, B$  are two nonempty subsets of  $\mathbb{Z}_p$ , with  $|A| > |B|$  then for any  $e \in \mathbb{Z}_p$*

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

*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 4 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  $|A + B| \geq |A + B'| = p$ .  $\square$

**Remark 2.** *The last estimate is tight for all possible cardinalities  $|A| > |B| > 1$  as shown by the following example.*

$$A = \{a, a + d, a + 2d, \dots, a + c_0d\}, \quad B = \{a, a + d, a + 2d, \dots, a + c_1d\},$$

where  $a, d$  are chosen so that  $a(a + d) = (a + c_0d)(a + c_1d) = e$ . 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

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

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  $(c_0 c_1 e)(c_0 - 1)(c_1 - 1)$  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 13 to  $A$  and a subset of cardinality  $s - 1$  of  $B$  we conclude that in this case for every  $e \in \mathbb{Z}_p$

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

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.

## 0.5 Concluding Remarks and Open Problems

1. All the results proved above hold for subsets of an arbitrary field of characteristic  $p$  instead of  $\mathbb{Z}_p$  with the same proof.
2. Theorem 8 implies that if  $A$  is a subset of  $\mathbb{Z}_p$  and  $|A| \geq (p + s^2 - 1)/s$ , then  $s^\wedge A = \mathbb{Z}_p$ . 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  $w(\langle v \rangle^t)$  the minimum possible number of wits needed for this task. It is shown in [14] that  $w(\langle v \rangle^t) = \Theta(\max\{t, \frac{t \log v}{\log t}\})$  and it is conjectured that in fact as  $t$  and  $v$  tend to infinity

$$w(\langle v \rangle^t) = (1 + o(1)) \max \left\{ t, \frac{t \log v}{\log t} \right\}.$$

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

$$w(\langle v \rangle^{\epsilon v}) \geq 2\epsilon v.$$

3. Lemma 6 can be extended to compute the coefficient of  $\prod_{i=0}^k x_i^{c_i}$  in the polynomial

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

for an arbitrary positive integer  $\alpha$ . In particular, Dyson’s conjecture (first proved by Gunson [7] and Wilson [18]) determines the coefficient of  $\prod_{i=0}^k x_i^{|E|/2}$  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 analogous result for Proposition 2, Theorem 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.

## Acknowledgments

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

# Bibliography

- [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. 1993.
- [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.