Adding distinct congruence classes modulo a prime

Noga Alon [*] Melvyn B. Nathanson [†] Imre Ruzsa [‡]

1 The Erdős-Heilbronn conjecture

The Cauchy-Davenport theorem states that if A and B are nonempty sets of congruence classes modulo a prime p, and if $|A| = k$ and $|B| = l$, then the sumset $A + B$ contains at least $\min(p, k + l - 1)$ congruence classes. It follows that the sumset $2A$ contains at least $\min(p, 2k - 1)$ congruence classes. Erdős and Heilbronn conjectured 30 years ago that there are at least $\min(p, 2k - 3)$ congruence classes that can be written as the sum of two *distinct* elements of A. Erdős has frequently mentioned this problem in his lectures and papers (for example, Erdős-Graham [4, p. 95]). The conjecture was recently proven by Dias da Silva and Hamidoune [3], using linear algebra and the representation theory of the symmetric group. The purpose of this paper is to give a simple proof of the Erdős-Heilbronn conjecture that uses only the most elementary properties of polynomials. The method, in fact, yields generalizations of both the Erdős-Heilbronn conjecture and the Cauchy-Davenport theorem.

2 The polynomial method

Lemma 1 (Alon-Tarsi [2]) *Let A and B be nonempty subsets of a field F with $|A| = k$ and $|B| = l$. Let $f(x, y)$ be a polynomial with coefficients in F and*

*Institute for Advanced Study, Princeton, NJ 08540, and Department of Mathematics, Raymond and Beverly Sackler Faculty of Exact Sciences, Tel Aviv University, Tel Aviv, Israel. E-mail: noga@math.tau.ac.il. Research supported in part by the Sloan Foundation, Grant No. 93-6-6. Alon also wishes to thank Doron Zeilberger for helpful discussions.

†Department of Mathematics, Lehman College (CUNY), Bronx, New York 10468. E-mail: 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. E-mail: h1140ruz@ella.hu. Research supported in part by DIMACS, Rutgers University, and by the Hungarian National Foundation for Scientific Research, Grant No. 1901.

of degree at most $k-1$ in x and $l-1$ in y. If $f(a,b)=0$ for all $a \in A$ and $b \in B$, then $f(x,y)$ is identically zero.

Proof. This follows immediately from the fact that a nonzero polynomial $p(x) \in F[x]$ of degree at most $k-1$ cannot have k distinct roots in F. We can write

$$f(x,y) = \sum_{i=0}^{k-1} \sum_{j=0}^{l-1} f_{i,j} x^i y^j = \sum_{i=0}^{k-1} v_i(y) x^i,$$

where

$$v_i(y) = \sum_{j=0}^{l-1} f_{i,j} y^j$$

is a polynomial of degree at most $l-1$ in y. Fix $b \in B$. Then

$$u(x) = \sum_{i=0}^{k-1} v_i(b) x^i$$

is a polynomial of degree at most $k-1$ in x such that $u(a)=0$ for all $a \in A$. Since $u(x)$ has at least k distinct roots, it follows that $u(x)$ is the zero polynomial, and so $v_i(b)=0$ for all $b \in B$. Since $\deg(v_i(y)) \leq l-1$ and $|B|=l$, it follows that $v_i(y)$ is the zero polynomial, and so $f_{i,j}=0$ for all i and j. This completes the proof. □

Lemma 2 *Let A be a finite subset of a field F, and let $|A|=k$. For every $m \geq k$ there exists a polynomial $g_m(x) \in F[x]$ of degree at most $k-1$ such that*

$$g_m(a) = a^m$$

for all $a \in A$.

Proof. Let $A = \{a_0, a_1, \ldots, a_{k-1}\}$. We must show that there exists a polynomial $u(x) = u_0 + u_1 x + \cdots + u_{k-1} x^{k-1} \in F[x]$ such that

$$u(a_i) = u_0 + u_1 a_i + u_2 a_i^2 + \cdots + u_{k-1} a_i^{k-1} = a_i^m$$

for $i = 0, 1, \ldots, k-1$. This is a system of k linear equations in the k unknowns $u_0, u_1, \ldots, u_{k-1}$, and it has a solution if the determinant of the coefficients of the unknowns is nonzero. The Lemma follows immediately from the observation that this determinant is the Vandermonde determinant

$$\begin{vmatrix} 1 & a_0 & a_0^2 & \cdots & a_0^{k-1} \\ 1 & a_1 & a_1^2 & \cdots & a_1^{k-1} \\ \vdots & & & & \\ 1 & a_{k-1} & a_{k-1}^2 & \cdots & a_{k-1}^{k-1} \end{vmatrix} = \prod_{0 \leq i < j \leq k-1} (a_j - a_i) \neq 0.$$

□

Theorem 1 *Let p be a prime number, and let $F = \mathbf{Z}/p\mathbf{Z}$. Let A and B be nonempty subsets of the field F, and let*

$$A\hat{+}B = \{a + b \mid a \in A, b \in B, a \neq b\}.$$

Let $|A| = k$ and $|B| = l$. If $k \neq l$, then

$$|A\hat{+}B| \geq \min(p, k + l - 2\}.$$

Proof. Let $|A| = k$ and $|B| = l$. We can assume that

$$1 \leq l < k \leq p.$$

If $k + l - 2 > p$, let $l' = p - k + 2$. Then

$$2 \leq l' < l < k$$

and

$$k + l' - 2 = p.$$

Choose $B' \subseteq B$ such that $|B'| = l'$. If the Theorem holds for the sets A and B', then

$$|A\hat{+}B| \geq |A\hat{+}B'| \geq k + l' - 2 = p = \min(p, |A| + |B| - 2).$$

Therefore, we can assume that

$$k + l - 2 \leq p.$$

Let $C = A\hat{+}B$. We must prove that

$$|C| \geq k + l - 2.$$

Suppose that

$$|C| \leq k + l - 3.$$

Choose m so that

$$m + |C| = k + l - 3.$$

We shall construct three polynomials f_0, f_1, and f in $F[x, y]$ as follows: Let

$$f_0(x, y) = \prod_{c \in C} (x + y - c).$$

Then $\deg(f_0) = |C| \leq k + l - 3$ and

$$f_0(a, b) = 0 \text{ for all } a \in A, b \in B, a \neq b.$$

Let

$$f_1(x, y) = (x - y) f_0(x, y).$$

Then $\deg(f_1) = 1 + |C| \leq k + l - 2$ and

$$f_1(a, b) = 0 \text{ for all } a \in A, b \in B.$$

Multiplying f_1 by $(x+y)^m$, we obtain the polynomial

$$f(x, y) = (x - y)(x + y)^m \prod_{c \in C} (x + y - c)$$

of degree exactly $k + l - 2$ such that

$$f(a, b) = 0 \text{ for all } a \in A, b \in B.$$

Then

$$\begin{aligned} f(x, y) &= \sum_{\substack{i,j \geq 0 \\ i+j \leq k+l-2}} f_{i,j} x^i y^j \\ &= (x - y)(x + y)^{k+l-3} + \text{ lower order terms.} \end{aligned}$$

Since $1 \leq l < k \leq p$ and $1 \leq k + l - 3 < p$, it follows that the coefficient $f_{k-1,l-1}$ of the monomial $x^{k-1}y^{l-1}$ in $f(x, y)$ is

$$\binom{k+l-3}{k-2} - \binom{k+l-3}{k-1} = \frac{(k-l)(k+l-3)!}{(k-1)!(l-1)!} \not\equiv 0 \pmod{p}.$$

By Lemma 2, for every $m \geq k$ there exists a polynomial $g_m(x)$ of degree at most $k - 1$ such that $g_m(a) = a^m$ for all $a \in A$, and for every $n \geq l$ there exists a polynomial $h_n(y)$ of degree at most $l - 1$ such that $h_n(b) = b^n$ for all $b \in B$. We use the polynomials $g_m(x)$ and $h_n(y)$ to construct a new polynomial $f^*(x, y)$ from $f(x, y)$ as follows: If $x^m y^n$ is a monomial in $f(x, y)$ with $m \geq k$, then we replace $x^m y^n$ with $g_m(x)y^n$. Since $\deg(f(x, y)) = k + l - 2$, it follows that if $m \geq k$, then $n \leq l - 2$, and so $g_m(x)y^n$ is a sum of monomials $x^i y^j$ with $i \leq k - 1$ and $j \leq l - 2$. Similarly, if $x^m y^n$ is a monomial in $f(x, y)$ with $n \geq l$, then we replace $x^m y^n$ with $x^m h_n(y)$. If $n \geq l$, then $m \leq k - 2$, and so $x^m h_n(y)$ is a sum of monomials $x^i y^j$ with $i \leq k - 2$ and $j \leq l - 1$. This determines a new polynomial $f^*(x, y)$ of degree at most $k - 1$ in x and $l - 1$ in y. The process of constructing $f^*(x, y)$ from $f(x, y)$ does not alter the coefficient $f_{k-1,l-1}$ of the term $x^{k-1}y^{l-1}$, since this monomial does not occur in any of the polynomials $g_m(x)y^n$ or $x^m h_n(y)$. On the other hand,

$$f^*(a, b) = f(a, b) = 0$$

for all $a \in A$ and $b \in B$. It follows immediately from Lemma 1 that the polynomial $f^*(x, y)$ is identically zero. This contradicts the fact that the coefficient $f_{k-1,l-1}$ of $x^{k-1}y^{l-1}$ in $f^*(x, y)$ is nonzero, and completes the proof. □

Theorem 2 (Dias da Silva-Hamidoune [3]) *Let p be a prime number, and let $F = \mathbf{Z}/p\mathbf{Z}$. Let $A \subseteq F$, and let $|A| = k \geq 2$. Let $2^\wedge A$ denote the set of all sums of two distinct elements of A. Then*

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

Proof. Let $A \subseteq F$, $|A| \geq 2$. Choose $a \in A$, and let $B = A \setminus \{a\}$. Then $|B| = |A| - 1$ and, by Theorem 1,

$$|2^\wedge A| \geq |A \hat{+} B| \geq \min(p, |A| + |B| - 2) = \min(p, 2|A| - 3).$$

This completes the proof of the Erdős-Heilbronn conjecture.□

Let $k + l - 2 \leq p$, $1 \leq l < k \leq p$. Let $A = \{0, 1, 2, \ldots, k-1\}$ and $B = \{0, 1, 2, \ldots, l-1\}$. Then $A \hat{+} B = \{1, 2, \ldots, k+l-2\}$ and $2^\wedge A = \{1, 2, \ldots, 2k-3\}$. This example shows that the lower bounds in Theorem 1 and Theorem 2 are sharp.

3 Further applications of the method

The polynomial method is a powerful new technique to obtain results in additive number theory. For example, it gives the following simple proof of the Cauchy-Davenport theorem. Let A and B be subsets of $\mathbf{Z}/p\mathbf{Z}$, and let $C = A + B$. Let $|A| = k$ and $|B| = l$. We can assume that $k + l - 1 \leq p$. If $|C| \leq k + l - 2$, let $m = k + l - 2 - |C|$, and consider the polynomial

$$f(x, y) = (x + y)^m \prod_{c \in C} (x + y - c).$$

Then $f(a, b) = 0$ for all $a \in A$ and $b \in B$. The polynomial has degree $k + l - 2$, and the coefficient of the monomial $x^{k-1}y^{l-1}$ is exactly

$$\binom{k+l-2}{k-1} \not\equiv 0 \pmod{p}.$$

The proof proceeds exactly as the proof of Theorem 1.

As a final example of the method, we state and prove the following new result.

Theorem 3 *Let A and B be nonempty subsets of $F = \mathbf{Z}/p\mathbf{Z}$, and let*

$$C = \{a + b \mid a \in A, b \in B, ab \neq 1\}.$$

Let $|A| = k$ and $|B| = l$. Then

$$|C| \geq \min(p, k + l - 3\}.$$

Proof. If $k+l-3>p$, let $l'=p-k+3$. Then $3\leq l'<l$. Choose $B'\subseteq B$ such that $|B'|=l'$ and let

$$C'=\{a+b' \mid a\in A, b\in B', ab'\neq 1\}.$$

Since $C'\subseteq C$, it suffices to prove that $|C'|\geq k+l'-3$. Equivalently, we can assume that $k+l-3\leq p$, and we must prove that $|C|\geq k+l-3$.

Suppose that $|C|\leq k+l-4$. Choose m so that $|C|+m=k+l-4$, and consider the polynomial

$$f(x,y)=(xy-1)(x+y)^m\prod_{c\in C}(x+y-c).$$

Then $f(a,b)=0$ for all $a\in A$ and $b\in B$. The polynomial has degree $k+l-2$, and the coefficient of the monomial $x^{k-1}y^{l-1}$ is

$$\binom{k+l-4}{k-2}\not\equiv 0 \pmod{p}.$$

The proof continues exactly as the proof of Theorem 1. □

Let $k+l-3\leq p$, $k,l\geq 2$, and choose $d\in \mathbf{Z}/p\mathbf{Z}$, $d\neq 0$, such that

$$(1+(k-1)d)(1+(l-1)d)=1.$$

Let $A=\{1,1+d,1+2d,\ldots,1+(k-1)d\}$ and $B=\{1,1+d,1+2d,\ldots,1+(l-1)d\}$. Define C as in Theorem 3. Then $C=\{2+id \mid i=1,\ldots,k+l-3\}$. This example shows that the lower bound in Theorem 3 is sharp for all $k,l\geq 2$. If $k=1$, the correct lower bound is $|B|-1=k+l-2$.

4 Remarks

The results in this paper hold for addition in any field F, where p is equal to the characteristic of F if the characteristic is a prime, and $p=\infty$ if the characteristic is zero.

Dias da Silva and Hamidoune [3] proved the generalization of the Erdős-Heilbronn conjecture for h-fold sums: Let $h\geq 2$, and let $h^\wedge A$ denote the set of all sums of h distinct elements of A. If $A\subseteq \mathbf{Z}/p\mathbf{Z}$ and $|A|=k$, then

$$|h^\wedge A|\geq \min(p, hk-h^2+1).$$

This result can also be proved by the polynomial method, and we shall present this and other results in a subsequent paper [1].

Nathanson [7] contains proofs of the Cauchy-Davenport theorem and some of its generalizations, as well as a full exposition of the original Dias da Silva-Hamidoune proof of the Erdős-Heilbronn conjecture for h-fold sums. Partial results on the Erdős-Heilbronn conjecture had previously been obtained by Rickert [9], Mansfield [6], Rödseth [10], Pyber [8], and Freiman, Low, and Pitman [5].

References

[1] N. Alon, M. B. Nathanson, and I. Z. Ruzsa. The polynomial method and sums of congruence classes. in preparation.

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

[3] 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.

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

[5] 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. preprint, 1992.

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

[7] M. B. Nathanson. *Additive Number Theory: 1. Inverse Theorems and the Geometry of Sumsets.* Springer-Verlag, New York, 1994.

[8] L. Pyber. On the Erdős-Heilbronn conjecture. personal communication.

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

[10] Ö. J. Rödseth. Sums of distinct residues mod *p*. *Acta Arith.*, 1994. to appear.