https://nickadfor.github.io/ThePolynomialMethod/ https://github.com/NickAdfor/ThePolynomialMethoc

The Polynomial Method and Restricted Sums of Congruence Classes

Noga Alon, Melvyn B. Nathanson, Imre Z. Ruzsa

Journal of Number Theory 56 (1996), 404-417

Abstract

We present a general polynomial method for studying restricted sums of congruence classes modulo a prime. The method provides a unified approach to various problems in additive number theory, including the Cauchy-Davenport theorem and the Erdős-Heilbronn conjecture on sums of distinct residues.

Contents

Chapter 1

Introduction

Theorem 1 (Cauchy-Davenport Theorem). *Let p be a prime and A, B be nonempty subsets of the cyclic group $\mathbb{Z}_p$. Then*

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

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

The polynomial method provides a unified approach to various problems in additive number theory.

Proposition 2 (Proposition 1.2). *Let p be a prime, and let $A_0, A_1, \ldots, A_k$ 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*

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

Theorem 3 (Theorem 1.3, Erdős-Heilbronn Conjecture). *If p is a prime, and A is a nonempty subset of $\mathbb{Z}_p$, then*

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

Chapter 2

Preliminaries

Definition 4 (Restricted sum)**.** Let p be a prime. For a polynomial $h = h(x_0, x_1, \ldots, x_k)$ over $\mathbb{Z}_p$ and for subsets $A_0, A_1, \ldots, A_k$ of $\mathbb{Z}_p$, define

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

Definition 5 (Distinct residues sum)**.** Let p be a prime, and let $A_0, A_1, \ldots, A_k$ be nonempty subsets of $\mathbb{Z}_p$. Define

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

Lemma 6 (Combinatorial Nullstellensatz, 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 $P \equiv 0$.*

Chapter 3

General Polynomial Method Theorem

Theorem 7 (General Theorem 2.1)**.** *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*

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

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

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

(and hence $m < p$).

Proof. Suppose the assertion is false, and let E be a multiset of m elements of $\mathbb{Z}_p$ that contains $\oplus_h \sum_{i=0}^{k} A_i$. Let

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

Then $Q(x_0, \dots, x_k) = 0$ for all $(x_0, \dots, x_k) \in A_0 \times \cdots \times A_k$. The degree of Q is $\sum_{i=0}^{k} c_i$.

For each i, 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 $\overline{Q}$ be obtained from Q by replacing each $x_i^{c_i+1}$ with $\sum_{j=0}^{c_i} b_{ij} x_i^j$. Then $\overline{Q}$ vanishes on $A_0 \times \cdots \times A_k$ and has x_i-degree at most c_i. By Lemma 2.2, $\overline{Q} \equiv 0$.

However, the coefficient of $\prod_{i=0}^{k} x_i^{c_i}$ in $\overline{Q}$ equals its coefficient in Q, which is nonzero by assumption. This contradiction proves the theorem. $\square$

Chapter 4

Cauchy-Davenport Theorem Proof

Theorem 8 (Cauchy-Davenport Theorem Proof)**.** *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* $|A|+|B| > p+1$ *replace* B *by a subset* B' *of cardinality* $p + 1 - |A|$ *and apply the result above to conclude* $|A + B| \geq p$*.*

Chapter 5

Distinct Residues Sums

Lemma 9 (Lemma 3.1)**.** *Let* $c_0, \ldots, c_k$ *be nonnegative integers and suppose* $\sum_{i=0}^{k} c_i = m + \binom{k+1}{2}$, *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 the Vandermonde determinant $\det(x_i^j)_{0 \leq i \leq k, 0 \leq j \leq k}$. The result follows by combinatorial manipulation. □

Theorem 10 (Proposition 1.2 Proof)**.** *Define* $h(x_0, \ldots, x_k) = \prod_{k \geq i > j \geq 0} (x_i - x_j)$. *Suppose* $|A_i| = c_i + 1$ *and put* $m = \sum_{i=0}^{k} c_i - \binom{k+1}{2}$. *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* c_i *are pairwise distinct. Theorem 2.1 gives the result.*

Theorem 11 (Theorem 3.2)**.** *Let* p *be a prime, and let* $A_0, \ldots, A_k$ *be nonempty subsets of* $\mathbb{Z}_p$, *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* $1 \leq i \leq k$. *If* $b'_k > 0$ *then*

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

Chapter 6

Further Applications

Proposition 12 (Proposition 4.1)**.** *If p is a prime and A, B are two nonempty subsets of $\mathbb{Z}_p$, then*

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

Proposition 13 (Proposition 4.2)**.** *If p is a prime and $A_0, A_1, \ldots, A_k$ are nonempty subsets of $\mathbb{Z}_p$, then for every $g \in \mathbb{Z}_p$,*

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

Proposition 14 (Proposition 4.3)**.** *If p is a prime and $A_0, A_1, \ldots, A_k$ are subsets of $\mathbb{Z}_p$, where $|A_i| \geq k+1$ for all i, then*

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

Chapter 7

Concluding Remarks

Remark 15. All results hold for subsets of an arbitrary field of characteristic p instead of $\mathbb{Z}_p$, with the same proof.

Remark 16. Theorem 3.3 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 explicit codes for write-once memories.

Problem 17. Determine all cases of equality in Proposition 1.2, Theorem 1.3 or the results in Section 4.

Problem 18. Obtain non-prime analogs for the results obtained here.