Additive Latin Transversals

Noga Alon *

Abstract

We prove that for every odd prime p, every $k \leq p$ and every two subsets $A = \{a_1, \ldots, a_k\}$ and $B = \{b_1, \ldots, b_k\}$ of cardinality k each of Z_p, there is a permutation $\pi \in S_k$ such that the sums $a_i + b_{\pi(i)}$ (in Z_p) are pairwise distinct. This partially settles a question of Snevily. The proof is algebraic, and implies several related results as well.

1 Introduction

In this note we prove several results in Additive Number Theory, using the algebraic approach called *Combinatorial Nullstellensatz* in [1]. Other results in Additive Number Theory proved using this approach appear in [1] and in its many references, including, for example, [2], [3], [4].

Our first result here is the following theorem.

Theorem 1.1 *Let p be an odd prime, and let A and B be two subsets of cardinality k each of the finite field Z_p. Then there is a numbering $\{a_1, \ldots, a_k\}$ of the elements of A and a numbering $\{b_1, \ldots, b_k\}$ of those in B such that the sums $a_i + b_i$ (in Z_p) are pairwise distinct.*

This partially settles a question of Snevily, who conjectured that the above is in fact true even when the field Z_p is replaced by any Abelian group of odd order.

Since the above theorem is trivial for $k = p$ (as in this case we can simply take $a_i = b_i$), its assertion follows from the following more general result.

Theorem 1.2 *Let p be a prime, suppose $k < p$, let $(a_1, \ldots, a_k)$ be a sequence of not necessarily distinct members of the finite field Z_p and let B be a subset of cardinality k of Z_p. Then there is a numbering $\{b_1, \ldots, b_k\}$ of the elements of B such that the sums $a_i + b_i$ (in Z_p) are pairwise distinct.*

Note that this stronger theorem is not true if we replace Z_p by the ring of integers modulo a non-prime n. Indeed, if $n = ks$, $a_1 = a_2 = \ldots = a_{k-1} = 0$, $a_k = s$ and $B = \{0, s, 2s, \ldots, (k-1)s\}$

*Department of Mathematics, Raymond and Beverly Sackler Faculty of Exact Sciences, Tel Aviv University, Tel Aviv, Israel and Institute for Advanced Study, Princeton, NJ 08540, USA. Research supported in part by a State of New Jersey grant and by the Hermann Minkowski Minerva Center for Geometry at Tel Aviv University.

then it is easy to check that there is no numbering of the elements of B such that the sums $a_i + b_i$, $(1 \leq i \leq k)$ are pairwise distinct in Z_n. Similarly, the assertion of the theorem fails for $k = p$ as shown by taking $a_1 = a_2 = \ldots = a_{p-1} = 0$, $a_p = 1$ and $B = \{0, 1, \ldots, p-1\}$.

The rest of this note is organized as follows. In Section 2 we prove Theorem 1.2 (which implies Theorem 1.1). Section 3 contains some extensions, and Section 4 contains some related comments about Latin Transversals.

2 The proof

Our main tool is the following result proved in [1], where it is called *Combinatorial Nullstellensatz.*

Theorem 2.1 ([1]) *Let F be an arbitrary field, and let $f = f(z_1, \ldots, z_k)$ be a polynomial in $F[z_1, \ldots, z_k]$. Suppose the degree $deg(f)$ of f is $\sum_{i=1}^{k} t_i$, where each t_i is a nonnegative integer, and suppose the coefficient of $\prod_{i=1}^{k} z_i^{t_i}$ in f is nonzero. Then, if $S_1, \ldots, S_k$ are subsets of F with $|S_i| > t_i$, there are $s_1 \in S_1, s_2 \in S_2, \ldots, s_k \in S_k$ so that*

$$f(s_1, \ldots, s_k) \neq 0.$$

Proof of Theorem 1.2: Consider the following polynomial in k variables over Z_p:

$$f(x_1, \ldots, x_k) = \prod_{1 \leq i < j \leq k} (x_i - x_j) \prod_{1 \leq i < j \leq k} (a_i + x_i - a_j - x_j).$$

Consider the coefficient of the monomial $\prod_{i=1}^{k} x_i^{k-1}$ in f. Since the total degree of f is $k(k-1)$, which is equal to the degree of this monomial, it is obvious that this is precisely the coefficient of this monomial in the polynomial

$$\prod_{1 \leq i < j \leq k} (x_i - x_j) \prod_{1 \leq i < j \leq k} (x_i - x_j) = \prod_{1 \leq i < j \leq k} (x_i - x_j)^2.$$

However, this coefficient is $(-1)^{\binom{k}{2}} k!$, as can be easily seen directly from the Vandermonde identity,

$$\prod_{1 \leq i < j \leq k} (x_i - x_j) = \pm \det \begin{bmatrix} 1 & 1 & \ldots & 1 \\ x_1 & x_2 & \ldots & x_k \\ \ldots & \ldots & \ldots & \ldots \\ x_1^{k-1} & x_2^{k-1} & \ldots & x_k^{k-1} \end{bmatrix} = \sum_{\pi \in S_k} (-1)^{\sigma(\pi)} \prod_{i=1}^{k} x_{\pi(i)}^{k-i},$$

or by a (very) special case of the Dyson Conjecture (proved in [6], [7], see also [8]). Since $k < p$, this coefficient is nonzero modulo p, and therefore, by Theorem 2.1 with $t_1 = t_2 = \ldots = t_k = k - 1$, and $S_1 = S_2 = \cdots = S_k = B$, it follows that there are $b_i \in S_i = B$ such that

$$f(b_1, \ldots, b_k) = \prod_{1 \leq i < j \leq k} (b_i - b_j) \prod_{1 \leq i < j \leq k} (a_i + b_i - a_j - b_j) \neq 0.$$

Thus, the elements $b_i \in B$ are pairwise distinct, and the sums $a_i + b_i$ are pairwise distinct as well, completing the proof. $\square$

3 Extensions

The following result extends Theorem 1.2.

Theorem 3.1 *Let p be a prime and let R be an arbitrary subset of $2r$ nonzero elements of the finite field Z_p, where $R = -R$. Suppose $k(r+1) < p$, let $(a_1, \ldots, a_k)$ be a sequence of not necessarily distinct members of Z_p and let B be a subset of cardinality $|B| > (k-1)(r+1)$ of Z_p. Then there are k pairwise distinct elements $\{b_1, \ldots, b_k\}$ of B such that the sums $a_i + b_i$ are pairwise distinct and the difference between any two of these sums is not a member of R.*

Remark: The assumption that $|B| > (k-1)(r+1)$ is tight. Indeed, if $R = \{1, 2, \ldots, r\} \cup \{-1, -2, \ldots, -r\}$, $a_1 = a_2 = \ldots = a_k = 0$ and B is a set of only $(k-1)(r+1)$ consecutive elements of Z_p, then the assertion of the theorem does not hold. The same example shows that the assumption that $k(r+1) < p$ is tight as well.

The proof of the last theorem is almost identical to the previous one, but here we use a more sophisticated case of the Dyson Conjecture, proved in [6], [7].

Theorem 3.2 ([6], [7]) *The coefficient of the monomial $\prod_{i=1}^k x_i^{(k-1)c_i}$ in the polynomial*

$$\prod_{1 \le i < j \le k} (x_i - x_j)^{c_i + c_j}$$

is

$$(-1)^{c_2 + 2c_3 + \ldots + (k-1)c_k} \frac{(c_1 + c_2 + \ldots + c_k)!}{c_1! c_2! \ldots c_k!}.$$

Proof of Theorem 3.1: Consider the following polynomial in k variables over Z_p:

$$f(x_1, \ldots, x_k) = \prod_{1 \le i < j \le k} (x_i - x_j) \prod_{1 \le i < j \le k} (a_i + x_i - a_j - x_j) \prod_{s \in R} \prod_{1 \le i < j \le k} (a_i + x_i - a_j - x_j - s).$$

Consider the coefficient of the monomial $\prod_{i=1}^k x_i^{(k-1)(r+1)}$ in f. Since the total degree of f is $k(k-1)(r+1)$, which is equal to the degree of this monomial, it is obvious that this is precisely the coefficient of this monomial in the polynomial

$$\prod_{1 \le i < j \le k} (x_i - x_j)^{2r+2}.$$

However, this coefficient is

$$(-1)^{(r+1)\binom{k}{2}} \frac{((r+1)k)!}{((r+1)!)^k},$$

by Theorem 3.2 with $c_i = r+1$ for all i. Since $(r+1)k < p$, this coefficient is nonzero modulo p, and therefore, by Theorem 2.1 with $t_1 = t_2 = \ldots = t_k = (k-1)(r+1)$, and $S_1 = S_2 = \cdots = S_k = B$, it follows that there are $b_i \in S_i = B$ such that

$$f(b_1, \ldots, b_k) = \prod_{1 \le i < j \le k} (b_i - b_j) \prod_{1 \le i < j \le k} (a_i + b_i - a_j - b_j) \prod_{s \in R} \prod_{1 \le i < j \le k} (a_i + b_i - a_j - b_j - s) \neq 0.$$

Thus, the elements $b_i \in B$ are pairwise distinct, so are the sums $a_i + b_i$ and no two of them differ by an element of R. This completes the proof. $\Box$

The above result can be generalized further, by applying the assertion of Theorem 3.2 in its full generality. This gives the following (somewhat artificial) result.

Theorem 3.3 *Let p be a prime, and let $R_1, \ldots, R_k$ be k arbitrary subsets of nonzero elements of Z_p, where $|R_i| = r_i$. Suppose $\sum_{i=1}^{k}(r_i+1) < p$, let $(a_1, \ldots, a_k)$ be a sequence of not necessarily distinct members of Z_p and let $B_1, \ldots, B_k$ be k subsets of Z_p satisfying $|B_i| > (r_i+1)(k-1)$. Then there are k pairwise distinct elements $\{b_1, \ldots, b_k\}$, where $b_i \in B_i$, such that the sums $a_i + b_i$ are pairwise distinct and for every $i \neq j$, $a_i + b_i - a_j - b_j \notin R_i$.*

Proof: Define

$$f(x_1, \ldots, x_k) = \prod_{1 \le i < j \le k} (x_i - x_j) \prod_{1 \le i < j \le k} (a_i + x_i - a_j - x_j) \prod_{1 \le i \neq j \le k} \prod_{r \in R_i} (a_i + x_i - a_j - x_j - r).$$

Note that as before, Theorem 3.2 implies that the coefficient of $\prod_{i=1}^{k} x_i^{(k-1)(r_i+1)}$ in f is, up to a sign,

$$\frac{(\sum_{i=1}^{k}(r_i+1))!}{\prod_{i=1}^{k}(r_i+1)!},$$

which is non-zero in Z_p, as $\sum_{i=1}^{k}(r_i+1) < p$. Therefore, Theorem 2.1 with $t_i = (k-1)(r_i+1)$ and $S_i = B_i$ for $1 \le i \le k$ implies the desired result. $\Box$

4 Latin transversals

A *transversal* in an m by n matrix, with $m \le n$, is a set of m cells of the matrix, no two in the same row or in the same column. It is called a *Latin transversal* if no two cells contain the same symbol. There are lots of conjectures about the existence of Latin transversals in matrices, see, for example, [5] and its references. In particular, it is conjectured that every m by n matrix with $m < n$ in which each symbol appears at most n times contains a Latin transversal.

Some of our results can be formulated in terms of Latin transversals. Theorem 1.1 shows that for any odd prime p, every square submatrix of the addition table of Z_p contains a Latin transversal. Theorem 1.2 shows that for $k < p$, and every k by k submatrix M of the addition table of Z_p, every k by k matrix each row of which is a row of M (and repetitions are allowed) contains a Latin transversal. It seems, however, that the algebraic structure of the matrices considered is crucial here, and the study of the related questions for more general matrices requires other techniques.

References

[1] N. Alon, *Combinatorial Nullstellenstaz*, Combinatorics, Probability and Computing 8 (1999), 7-29.

[2] N. Alon, N. Linial, and R. Meshulam, *Additive bases of vector spaces over prime fields*, J. Combinatorial Theory Ser. A 57 (1991), 203–210.

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

[4] S. Eliahou, and M. Kervaire, *Sumsets in vector spaces over finite fields*, J. Number Theory 71 (1998), 12–39.

[5] P. Erdős, D. R. Hickerson, D. A. Norton, and S. K. Stein, *Has every Latin square of order n a partial Latin transversal of size $n-1$?*, Amer. Math. Monthly 95 (1988), 428–430.

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

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

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