Structure theorems for set addition: The power of the Combinatorial Nullstellensatz

Gyula Károlyi, Eötvös University, Budapest

During the last decade, the so-called 'polynomial method' has been leading to several new discoveries in combinatorial number theory, in particular in the additive theory. In this talk I intend to give a brief overview of this progress. Let me only mention here just one recent result that, in a certain sense, completes the solution of a long-standing conjecture of Erdős and Heilbronn:

Let A be a set of $k \geq 5$ elements of an Abelian group G in which the order of the smallest nonzero subgroup is larger than $2k-3$. Then the number of different elements of G that can be written in the form $a + a'$, where $a, a' \in A$, $a \neq a'$, is at least $2k-3$. (This has been shown by Dias da Silva and Hamidoune in 1994, in the case when G is a cyclic group of prime order.) *In addition, the bound is attained if and only if the elements of A form an arithmetic progression in G.*

The proof, for cyclic groups of prime order, depend on the so-called 'Combinatorial Nullstellensatz' of Alon. To transfer the results for arbitrary groups we use an appropriate generalization of the notion of direct sum. More general results may be obtained using the theory of Gröbner bases.