Vu, Van H.; Wood, Philip Matchett
The inverse Erdős-Heilbronn problem. (English) Zbl 1248.11075

Authors’ summary: The famous Erdős-Heilbronn conjecture (first proved by J. Dias da Silva and Y. O. Hamidoune [Bull. Lond. Math. Soc. 26, 140–146 (1994; Zbl 0819.11007)]) asserts that if $A$ is a subset of $\mathbb{Z}/p\mathbb{Z}$, the cyclic group of the integers modulo a prime $p$, then

$$|A+ A| \geq \min\{2|A| - 3, p\}.$$ 

The bound is sharp, as is shown by choosing $A$ to be an arithmetic progression. A natural inverse result was proven by G. Károlyi [J. Algebra 290, No. 2, 557–593 (2005; Zbl 1095.11046)]: if $A \subset \mathbb{Z}/p\mathbb{Z}$ contains at least 5 elements and $|A+ A| \leq 2|A| - 3 < p$, then $A$ must be an arithmetic progression.

The authors consider a large prime $p$ and investigate the following more general question: what is the structure of sets $A \subset \mathbb{Z}/p\mathbb{Z}$ such that $|A+ A| \leq (2 + \varepsilon)|A|$?

Their main result is an asymptotically complete answer to this question: there exists a function $\delta(p) = o(1)$ such that if $200 < |A| \leq (1 - \varepsilon')p/2$ and if $|A+ A| \leq (2 + \varepsilon)|A|$, where $\varepsilon' - \varepsilon > \delta > 0$, then $A$ is contained in an arithmetic progression of length $|A+ A| - |A| + 3$.

With the extra assumption that $|A| \leq (\frac{1}{2} - \frac{1}{\log p})p$, the main result has Dias da Silva and Hamidoune’s theorem and Károlyi’s theorem as corollaries, and thus, the main result provides purely combinatorial proofs for the Erdős-Heilbronn conjecture and an inverse Erdős-Heilbronn theorem.

Reviewer: Olaf Ninnemann (Berlin)

MSC:
11P70 Inverse problems of additive number theory, including sumsets
11B13 Additive bases, including sumsets

Keywords:
restricted sumsets; Erdős-Heilbronn conjecture; inverse Erdős-Heilbronn theorem

Full Text: EMIS