On the sets of simple sums and products of k integers

Bogdan Grechuk • 20 Feb 2026

This post continues my series on favorite theorems of the 21st century. For an overview of the categories and earlier selections, see this post.

My choice for 2001 in Number Theory is Chang's resolution of a conjecture of Erdős and Szemerédi predicting that a finite set of integers cannot simultaneously have "few" subset sums and "few" subset products. More precisely, they conjectured a *superpolynomial* lower bound on the combined size of the sets of simple sums and simple products of k distinct integers.

Let $A = \{a_1, a_2, \dots, a_k\}$ be a set of k distinct integers. Define the sets of *simple sums* and *simple products* by

$$S(A) = \left\{ \sum_{i=1}^{k} \epsilon_i a_i \,\middle|\, \epsilon_i \in \{0,1\} \right\}, \qquad \Pi(A) = \left\{ \prod_{i=1}^{k} a_i^{\epsilon_i} \,\middle|\, \epsilon_i \in \{0,1\} \right\}.$$

Thus $S(A)$ consists of all subset sums of A, and $\Pi(A)$ of all subset products. Set

$$g(k) = \min_{A:\,|A|=k} \big(|S(A)| + |\Pi(A)|\big),$$

where $|.|$ denotes the cardinality of a set.

Erdős and Szemerédi (Erdős and Szemerédi 1983) conjectured that $S(A)$ and $\Pi(A)$ cannot both be small. In quantitative terms, they predicted that $g(k)$ grows faster than any fixed power of k; that is, $g(k)$ is superpolynomial in k.

In November 2001, Chang (Chang 2003) confirmed this conjecture with a strikingly precise estimate.

Theorem 1 (Chang, 2001) *For every $\epsilon > 0$ there exists $k_0 = k_0(\epsilon)$ such that for all $k \geq k_0$,*

$$g(k) > k^{\left(\frac{1}{2}-\epsilon\right)\frac{\log k}{\log \log k}}.$$

The exponent

$$\left(\frac{1}{2} - \epsilon\right) \frac{\log k}{\log \log k}$$

grows without bound as $k \to \infty$, so the lower bound is genuinely superpolynomial.

A notable feature of the proof is its direction of attack. A common strategy in sum–product problems is to assume the sum set is small and deduce that the product set must then be large. Chang reverses this logic: assuming the product set is small, she shows that the sum set must necessarily be large. This shift in perspective turns out to be decisive.

Moreover, the result is essentially sharp. It is known that there exists a constant $c > 0$ such that

$$g(k) < k^{c \frac{\log k}{\log \log k}},$$

so Chang's theorem determines the correct order of growth up to a constant factor in the exponent.

The analogue of Theorem 1 for *general* (not necessarily simple) sums and products remains far more difficult and is still open.

For sets $A, B \subset \mathbb{Z}$, define

$$A + B = \{a + b : a \in A,\, b \in B\}, \qquad A \times B = \{ab : a \in A,\, b \in B\}.$$

For a positive integer k, define the k-fold sumset and product set by

$$kA = \underbrace{A + \cdots + A}_{k \text{ times}}, \qquad A^k = \underbrace{A \times \cdots \times A}_{k \text{ times}}.$$

Erdős and Szemerédi (Erdős and Szemerédi 1983) conjectured that for every $\epsilon > 0$ there exists $c_\epsilon > 0$ such that

$$\max\bigl(|kA|, |A^k|\bigr) \geq c_\epsilon |A|^{k-\epsilon}. \tag{1}$$

In other words, repeated addition or repeated multiplication must lead to near-maximal growth.

As partial progress toward (1), Bourgain and Chang (Bourgain and Chang 2004) proved in 2004 that for every integer $b > 0$ there exists $k = k(b)$ such that

$$\max\bigl(|kA|, |A^k|\bigr) \geq |A|^b$$

for every nonempty finite set $A \subset \mathbb{Z}$.

Even the case $k = 2$ of (1) remains open. In this case the conjecture predicts

$$\max\bigl(|A + A|, |A \times A|\bigr) \geq c_\epsilon |A|^{2-\epsilon}. \tag{2}$$

This is the celebrated Erdős–Szemerédi sum–product conjecture.

In 2009, Solymosi (Solymosi 2009) proved (2) with the exponent $\frac{4}{3}$ in place of 2. Subsequent work has improved this constant slightly. The current record, due to Bloom (Bloom 2025), establishes the exponent

$$\frac{4}{3} + \frac{2}{951}.$$

Chang's theorem thus stands as a landmark: it completely resolves the "simple" version of the conjecture and achieves the optimal growth rate up to constants in the exponent. At the same time, the general sum–product problem continues to challenge the field, illustrating once again how subtle the interplay between addition and multiplication can be in the integers.

References

Bloom, Thomas F. 2025. "Control and Its Applications in Additive Combinatorics." *arXiv Preprint arXiv:2501.09470*.

Bourgain, Jean, and Mei-Chu Chang. 2004. "On the Size of k-Fold Sum and Product Sets of Integers." *J. Amer. Math. Soc.* 17 (2): 473–97.

Chang, Mei-Chu. 2003. "The Erdős–Szemerédi Problem on Sum Set and Product Set." *Ann. Of Math.* 157 (3): 939–57.

Erdős, Paul, and Endre Szemerédi. 1983. "On Sums and Products of Integers." In *Studies in Pure Mathematics*, 213–18. Springer.

Solymosi, József. 2009. "Bounding Multiplicative Energy by the Sumset." *Adv. Math.* 222 (2): 402–8.