Available online at www.sciencedirect.com
SCIENCE DIRECT®
C. R. Acad. Sci. Paris, Ser. I 336 (2003) 201–205

Combinatorics

New results on the Erdös–Szemerédi sum-product problems

Nouveaux résultats sur les problèmes sommes-produits d'Erdös et Szemerédi

Mei-Chu Chang

University of California at Riverside, Department of Mathematics, Riverside, CA 92521, USA

Received 12 July 2002; accepted 17 July 2002

Presented by Jean Bourgain

Abstract

In this Note, we present several contributions (or solutions) to problems related to the sizes of sum sets and product sets of integers (or complex numbers), considered in [8]. We also introduce some new methods in this area of research. ***To cite this article: M.-C. Chang, C. R. Acad. Sci. Paris, Ser. I 336 (2003).***

Résumé

Dans cette Note, nous présentons diverses contributions (ou solutions) à des questions concernant la taille d'ensembles somme et produit d'ensembles finis d'entiers (ou de nombres complexes), posées dans [8]. Nous introduisons également quelques méthodes nouvelles dans ce domaine de recherche. ***Pour citer cet article : M.-C. Chang, C. R. Acad. Sci. Paris, Ser. I 336 (2003).***

Version française abrégée

Soit A un ensemble fini d'entiers arbitraires de cardinal $|A| = N$. Pour tout entier $h \geqslant 1$, notons hA (resp. A^h) l'ensemble de toutes les sommes (resp. produits) de h éléments de A (en admettant les répétitions). On démontre que si

$$\left|A^2\right| < CN, \tag{1}$$

où C est une constante arbitraire, alors on a toujours

$$|hA| > c_h(C)N^h \quad \text{pour tout } h \geqslant 2. \tag{2}$$

E-mail address: mcc@math.ucr.edu (M.-C. Chang).

1631-073X/03/$ – see front matter
doi:10.1016/S1631-073X(03)00018-9

Réciproquement, si

$$|2A| < CN \tag{3}$$

alors

$$\left|A^h\right| > c_{h,\varepsilon}(C)N^{h-\varepsilon} \quad \text{pour tous } h \geqslant 2 \text{ et } \varepsilon > 0. \tag{4}$$

Rappelons une conjecture due à Erdös et Szemerédi [8]

$$\min_{|A|=N}\left(|hA| + \left|A^h\right|\right) > c_{h,\varepsilon}N^{h-\varepsilon} \quad \text{pour tout } \varepsilon > 0, \tag{5}$$

les énoncés précédents la confirme dans les cas particuliers (1) et (3). Soit $A[1]$ (resp. $A\{1\}$) l'ensemble de toutes les sommes (resp. produits) d'élements *distincts* de A et posons

$$g(N) = \min_{|A|=N}\left(\left|A[1]\right| + \left|A\{1\}\right|\right). \tag{6}$$

En élaborant la démonstration de (2), on démontre que

$$g(N) > N^{C(\ln N)/(\ln\ln N)}, \tag{7}$$

où $c > 0$ est une constante absolue. Ceci répond complètement à un problème également posé dans [8] (où une borne supérieure du type (7) est obtenue).

La preuve de (4) repose sur une estimation uniforme du nombre de factorisations $r_h(k; P)$ d'un entier k comme produit de h éléments de P, où P est une progression arithmétique généralisée de dimension d. On démontre en effet que, $N = |P|$,

$$r_h(k; P) < \mathrm{e}^{C_{d,h}(\ln N)/(\ln\ln N)}. \tag{8}$$

On se ramène au cas des progressions arithmétiques par l'intermédiaire du théorème de Freiman.

Nous indiquons également d'autres applications de ce résultat à divers problèmes considérés dans [8].

1. Introduction

Our main reference is the paper [8] in which a number of problems on sum and product sets of finite sets of integers (or real or complex numbers) are proposed. Although research over recent years has lead to certain progress, most of those problems are still very far from being solved. In this Note, some further contributions will be described, as are some new methods of attack. First, we introduce some terminology. Let A be a finite set of complex numbers. Define

$$2A = A + A = \{a + a' \mid a \in A,\ a' \in A\} \quad \text{(the sum set)}$$

and

$$A^2 = AA = \{a \cdot a' \mid a \in A,\ a' \in A\} \quad \text{(the product set)}.$$

More generally, for a fixed integer $h \geqslant 2$, let hA and A^h be the h-fold sum and set, respectively.

A first conjecture in [8] is that $2A$ and A^2 cannot both be small. More precisely

Conjecture 1. $\min_{|A|=N}(|2A| + |A^2|) > c_\varepsilon N^{2-\varepsilon}$ *for all* $\varepsilon > 0$.

More generally,

Conjecture 1′. $\min_{|A|=N}(|hA| + |A^h|) > c_{\varepsilon,h}N^{h-\varepsilon}$ *for all* $h \geqslant 2$ *and* $\varepsilon > 0$.

These problems are open (also for sets of integers). It was proven in [8] that, for $A \subset \mathbb{Z}$, $|A| = N$, one has that $|2A| + |A^2| > N^{1+\delta}$, for N sufficiently large and for some absolute constant $\delta > 0$. The best result to date is due to Elekes [5], with lower bound $cN^{5/4}$. Elekes' approach is geometric and based on the Szemerédi–Trotter theorem [12] on point-line incidences. Very recently, Elekes and Ruzsa established the following general inequality

$$|A + A|^4 |AA| \ln |A| > |A|^6 \tag{9}$$

(see [7]), again using the [12] theorem. As a consequence of (9), it follows that Conjecture 1 holds if we assume moreover $|2A| < C|A|$.

Besides the results stated in the next section, very little seems known related to Conjecture 1′ with $h > 2$. The argument from [7] does not give information on multiple products A^h for $h > 2$.

Returning to [8], an even more daring conjecture is proposed. Let $G \subset A \times A$ be an undirected graph and define *sum and product sets along G* as

$$A \overset{G}{+} A = \{a + a' \mid (a, a') \in G\} \quad \text{and} \quad A \overset{G}{\times} A = \{a \cdot a' \mid (a, a') \in G\}.$$

Conjecture 2. *For all* $\varepsilon > 0, 0 < \delta < 1$

$$\left|A \overset{G}{+} A\right| + \left|A \overset{G}{\times} A\right| > c_{\varepsilon,\delta} |G|^{1-\varepsilon} \tag{10}$$

if $|A| = N$, $|G| > N^{1+\delta}$.

(We assume here $A \subset \mathbb{Z}$ or $A \subset \mathbb{R}$.)

Virtually nothing was known here (Elekes' method does provide some information). We did establish (10) in the case $|G| > cN^2$, $|A \overset{G}{+} A| < CN$ (with $c > 0$, and $C < \infty$ arbitrary constants).

Next, define for $A \subset \mathbb{Z}$ the sets $A[1]$ and $A\{1\}$ of all sums and products, respectively, of distinct elements of A.

Conjecture 3 [8]. *Define* $g(N) = \min_{|A|=N}(|A[1]| + |A\{1\}|)$. *Then* $g(N)$ *grows faster than any power of* N, *and in fact*

$$g(N) > \mathrm{e}^{C(\ln N)^2/(\ln\ln N)} \quad \textit{for some constant } C > 0. \tag{11}$$

We recently did establish this fact in [3].

In [6], it is shown that if $A \subset \mathbb{R}$ is a finite set, $|A| = N$ and f a strictly convex (or concave) function defined on an interval containing A, then always

$$|A \pm A| \left|f(A) \pm f(A)\right| > cN^{5/2}. \tag{12}$$

Their approach uses an extension of the [12] theorem to 'pseudo-line systems' and, at this point only applies to the real case. As a consequence of (12), the authors obtain

$$|A + A| + \left|\frac{1}{A} + \frac{1}{A}\right| > cN^{5/4}. \tag{13}$$

One of the results obtained in [3] is that if $A \subset \mathbb{C}$, $|A| = N$ satisfies $|A + A| < CN$, then $|1/A + 1/A| > c_\varepsilon N^{2-\varepsilon}$ for all $\varepsilon > 0$.

2. New results

In what follows, we state precisely some of the results from [3,4] on the problems mentioned above. The letters c, C are used for various constants.

Proposition 1 [3]. *If $A \subset \mathbb{Z}$, $|A| = N$ and $|A^2| < CN$, then*

$$|hA| > c_h(C)N^h \quad \text{for all } h \geqslant 2.$$

Proposition 2 [4]. *If $A \subset \mathbb{C}$, $|A| = N$ and $|2A| < CN$, then*

$$\left|A^h\right| > c_{h,\varepsilon}(C)N^{h-\varepsilon} \quad \text{for all } h \geqslant 2 \text{ and } \varepsilon > 0.$$

Proposition 3 [4]. *Denote $r_h(x; A)$ the number of ways to write x as a product of h elements from the set A. Then, under the assumptions of Proposition* 2*, there is a uniform bound*

$$r_h(x; A) < \mathrm{e}^{C_h(\ln N)/(\ln\ln N)}, \tag{14}$$

where C_h is a constant depending on C and h.

Proposition 4 [3]. *Let $g(N)$ be defined as in* (6)*, restricting A to subsets of $\mathbb{Z}$. Then* (11) *holds.*

Proposition 5 [4]. *Let $A \subset \mathbb{C}$, $|A| = N$ and $G \subset A \times A$. Assume*

$$|G| > \delta N^2 \quad \text{and} \quad \left|A \overset{G}{+} A\right| < CN. \tag{15}$$

Then

$$\left|A \overset{G}{\times} A\right| > c_\varepsilon(\delta, C)N^{2-\varepsilon} \quad \text{for all } \varepsilon > 0. \tag{16}$$

Proposition 6 [4]. *If $A \subset \mathbb{C}$, $|A| = N$ and $|A + A| < CN$, then*

$$\left|\frac{1}{A} + \frac{1}{A}\right| > c_\varepsilon(C)N^{2-\varepsilon} \quad \text{for all } \varepsilon > 0. \tag{17}$$

Proposition 7 [4]. *Let $A \subset \mathbb{C}$, $|A| = N$ and $p(X) \in \mathbb{C}[X]$ of degree $r \geqslant 2$. If $|A + A| < CN$, then again*

$$\left|p(A) + p(A)\right| > c_\varepsilon(C, r)N^{2-\varepsilon}. \tag{18}$$

3. Comments on the proofs

First, the assumption $|A + A| < C|A|$ (and also $|A \times A| < C|A|$) is exploited through Freiman's theorem (see [10] for details and [2] for the strongest version in terms of bounds). This remarkable theorem states that if A is a finite subset of a torsion free Abelian group, $|A| = N$ and $|A + A| < CN$, then A is contained in a generalized d-dimensional arithmetic progression

$$A \subset P = \left\{ c_0 + \sum_{i=1}^{d} k_i c_i \;\middle|\; k_i \in \mathbb{Z},\ 0 \leqslant k_i \leqslant J_i \ (1 \leqslant i \leqslant d) \right\}, \tag{19}$$

where $d \leqslant d(C)$ and $\prod_{i=1}^{d} J_i \leqslant C'(C)N$. (The progression may moreover be assumed *proper*, meaning that all sums in (19) represent different elements.) Proposition 1 uses a weak form of Freiman's theorem together with

Harmonic Analysis methods. More precisely, we exploit moment inequalities for trigonometric polynomials whose frequencies have certain "lacunarity" properties (in the spirit of [11]).

Proposition 4 is based on quantitative refinements of the proof of Proposition 1, combined with Plünnecke's inequalities (see [10], Section 7).

Proposition 2 (which generalizes the [7] result to arbitrary h) obviously follows from Proposition 3. By Freiman's theorem, it suffices to establish an inequality

$$r_h(x;\, P) < \mathrm{e}^{C_{d,h}(\ln J)/(\ln\ln J)}, \tag{20}$$

where P is defined by (19), and $J = \max_i J_i$.

Our approach to establish (20) is totally different from [7] and we rely heavily on the theory of algebraic number fields K obtained as finite extensions of $\mathbb{Q}$ (see [1]). In particular, a key point is the number of factorizations of an algebraic integer $\alpha \in K$ as a product $\alpha = \alpha_1\alpha_2$ with $\alpha_i \in K$ $(i = 1, 2)$ and such that the minimal polynomial of each α_i has coefficients bounded by J^C.

Propositions 5–7 are further applications of (20). To establish Proposition 5, we rely moreover on a recent result due to Laczkovich and Ruzsa [9], stating that under assumption (15), there is a subset $A' \subset A$ satisfying

$$|A' + A'| < C'N \quad \text{and} \quad \bigl|G \cap (A' \times A')\bigr| > \delta' N^2 \tag{21}$$

with $\delta', C' > 0$ depending on δ and C. Their result is based on Gower's improvement of the Balog–Szemerédi theorem (see [10]).

References

[1] L.I. Borevich, I.R. Shafarevich, Number Theory, Academic Press, 1966.
[2] M. Chang, A polynomial bound in Freiman's theorem, Duke Math. J. 113 (3) (2002) 399–419.
[3] M. Chang, Erdös–Szemerédi problem on sum set and product set, Ann. of Math., submitted.
[4] M. Chang, Factorization in generalized arithmetic progressions and applications to the Erdös–Szemerédi sum-product problems, Preprint, 2002.
[5] G. Elekes, On the number of sums and products, Acta Arith. 81 (4) (1997) 365–367.
[6] G. Elekes, M. Nathanson, I. Ruzsa, Convexity and sumsets, J. Number Theory, to appear.
[7] G. Elekes, J. Ruzsa, Few sums, many products, Preprint.
[8] P. Erdös, E. Szemerédi, On sums and products of integers, in: P. Erdös, L. Alpàr, G. Haláz (Eds.), Stud. Pure Math., pp. 215–218.
[9] Laczkovich, I. Ruzsa, Preprint.
[10] M. Nathanson, Additive Number Theory, Springer, 1996.
[11] W. Rudin, Trigonometric series with gaps, J. Math. Mech. 9 (1960) 203–227.
[12] E. Szemerédi, W. Trotter, Extremal problems in discrete geometry, Combinatorics 3 (3–4) (1983) 387–392.