Astérisque

MELVYN B. NATHANSON
GÉRALD TENENBAUM

Inverse theorems and the number of sums and products

Astérisque, tome 258 (1999), p. 195-204
<http://www.numdam.org/item?id=AST_1999__258__195_0>

Astérisque **258**, 1999, p. 195–204

INVERSE THEOREMS AND THE NUMBER OF SUMS AND PRODUCTS

by

Melvyn B. Nathanson & Gérald Tenenbaum

Abstract. — Let $\epsilon > 0$. Erdős and Szemerédi conjectured that if A is a set of k positive integers which large k, there must be at least $k^{2-\epsilon}$ integers that can be written as the sum or product of two elements of A. We shall prove this conjecture in the special case that the number of sums is very small.

1. A conjecture of Erdős and Szemerédi

Let A be a nonempty, finite set of positive integers, and let $|A|$ denote the cardinality of the set A. Let

$$2A = \{a + a' : a, a' \in A\}$$

denote the 2-fold *sumset* of A, and let

$$A^2 = \{aa' : a, a' \in A\}$$

denote the 2-fold *product set* of A. We let

$$E_2(A) = 2A \cup A^2$$

denote the set of all integers that can be written as the sum or product of two elements of A. If $|A| = k$, then

$$|2A| \leqslant \binom{k+1}{2}$$

and

$$|A^2| \leqslant \binom{k+1}{2},$$

1991 ***Mathematics Subject Classification.*** — Primary 11B05, 11B13, 11B75, 11P99, 05A17.

Key words and phrases. — Additive number theory, sumsets, product sets, inverse theorems, Freiman's theorem, sums and products of integers, divisors.

M.B. N.: This work was supported in part by grants from the PSC-CUNY Research Award Program and the National Security Agency Mathematical Sciences Program.

and so the number of sums and products of two elements of A is

$$|E_2(A)| \leqslant k^2 + k.$$

Erdős and Szemerédi [**3**, p. 60] made the beautiful conjecture that a finite set of positive integers cannot have simultaneously few sums and few products. More precisely, they conjectured that for every $\varepsilon > 0$ there exists an integer $k_0(\varepsilon)$ such that, if A is a finite set of positive integers and

$$|A| = k \geqslant k_0(\varepsilon),$$

then

$$|E_2(A)| \gg_\varepsilon k^{2-\varepsilon}.$$

Very little is known about this question. Erdős and Szemerédi [**4**] have shown that there exists a real number $\delta > 0$ such that

$$|E_2(A)| \gg k^{1+\delta},$$

and Nathanson [**11**] proved that

$$|E_2(A)| \geqslant ck^{32/31},$$

where $c = 0.00028\ldots$.

Erdős and Szemerédi [**4**] also remarked that, in the special case that $|2A| \leqslant ck$, "perhaps there are more than $k^2/(\log k)^\varepsilon$ elements in A^2 ". This cannot be true for arbitrary finite sets of positive integers and arbitrarily small $\varepsilon > 0$. For example, if A is the set of all integers from 1 to k, then Tenenbaum [**16, 17**], improving a result of Erdős [**2**], proved that

$$\frac{k^2}{(\log k)^{\varepsilon_0}} e^{-c\sqrt{\log_2 k \log_3 k}} \ll |A^2| \ll \frac{k^2}{(\log k)^{\varepsilon_0}\sqrt{\log_2 k}}, \tag{1}$$

where $\log_r$ denotes the r-fold iterated logarithm, and

$$\varepsilon_0 = 1 - \left(\frac{1 + \log_2 2}{\log 2}\right) \geqslant 0.08607 \tag{2}$$

(cf. Hall and Tenenbaum [**8**, Theorem 23]).

Using an inverse theorem of Freiman, we shall prove that if A is a set of k positive integers such that $|2A| \leqslant 3k - 4$, then

$$|A^2| \gg (k/\log k)^2.$$

We obtain a similar result for the sumset and product set of two possibly different sets of integers. Let A_1 and A_2 be nonempty, finite sets of positive integers, and let

$$A_1 + A_2 = \{a_1 + a_2 : a_1 \in A_1, a_2 \in A_2\}$$

and

$$A_1 A_2 = \{a_1 a_2 : a_1 \in A_1, a_2 \in A_2\}.$$

Let $|A_1| = |A_2| = k$. We prove that whenever $|A_1 + A_2| \leqslant 3k - 4$, then we have $|A_1 A_2| \gg (k/\log k)^2$.

2. Product sets of arithmetic progressions

A set Q of positive integers is an *arithmetic progression* of length ℓ and difference q if there exist positive integers r, q, and ℓ such that

$$Q = \{r + uq : 0 \leqslant u < \ell\}.$$

We shall always assume that

$$\ell \geqslant 2.$$

For any sets A and B of positive integers, let $\varrho_{A,B}(m)$ denote the number of representations of m in the form $m = ab$, where $a \in A$ and $b \in B$. Let $\varrho_A(m) = \varrho_{A,A}(m)$. Let $\tau(m)$ denote the number of positive divisors of m. Clearly, for every integer m,

$$\varrho_{A,B}(m) \leqslant \tau(m).$$

If $A_1 \subseteq Q_1$ and $A_2 \subseteq Q_2$, then $\varrho_{A_1,A_2}(m) \leqslant \varrho_{Q_1,Q_2}(m)$.

***Lemma 1* (Shiu).** — *Let $0 < \alpha < 1/2$ and let $0 < \beta < 1/2$. Let x and y be real numbers and let s and q be integers such that*

$$0 < s \leqslant q \text{ and } (s,q) = 1, \tag{3}$$

$$q < y^{1-\alpha}, \tag{4}$$

and

$$x^{\beta} < y \leqslant x. \tag{5}$$

Then

$$\sum_{\substack{w \equiv s \pmod q \\ x-y < w \leqslant x}} \tau(w) \ll_{\alpha,\beta} \frac{\varphi(q) y \log x}{q^2}.$$

Proof. This is a special case of Theorem 2 in Shiu [**14**] (see also Vinogradov and Linnik [**18**] and Barban and Vehov [**1**]).

Lemma 2. — *Let s, q, h, and ℓ be integers such that $h \geqslant 0$, $\ell \geqslant 2$, $0 < s \leqslant q$, and $(s,q) = 1$. Let Q be the arithmetic progression*

$$Q = \{s + vq : h \leqslant v < h + \ell\}.$$

If $(h+1)q < \ell^5$, then

$$\sum_{w \in Q} \tau(w) \ll \ell \log \ell.$$

Proof. We apply Lemma 1 with $\alpha = \beta = 1/6$, $x = (h+\ell)q$, and $y = \ell q$. The integers s and q satisfy (3). Since $q \leqslant (h+1)q < \ell^5$, we have $q^{1/6} < \ell^{5/6}$, and so

$$q = q^{1/6} q^{5/6} < (\ell q)^{5/6} = y^{1-\alpha}.$$

This shows that (4) is satisfied.

To obtain (5), we consider two cases. If $h \leqslant \ell$, then, since $2 \leqslant \ell \leqslant \ell q$, we have

$$x^\beta = ((h+\ell)q)^\beta \leqslant (2\ell q)^\beta \leqslant (\ell q)^{2\beta} = (\ell q)^{1/3} < \ell q = y \leqslant x.$$

If $h > \ell$, then, since $hq < \ell^5$, we have

$$x^\beta = \{(h+\ell)q\}^\beta < (\ell h q)^\beta < \ell^{6\beta} = \ell \leqslant \ell q = y \leqslant x.$$

This shows that (5) holds.

Applying Lemma 1, we obtain

$$\begin{aligned} \sum_{w \in Q} \tau(w) &= \sum_{\substack{w \equiv s \pmod q \\ hq < w \leqslant (h+\ell)q}} \tau(w) \ll \frac{\varphi(q)(\ell q)\log((h+\ell)q)}{q^2} \\ &\ll \ell \log(\ell(h+1)q) \ll \ell \log \ell^6 \ll \ell \log \ell. \end{aligned}$$

This completes the proof.

Lemma 3. — *Let Q_1 and Q_2 be two arithmetic progressions of length $\ell \geqslant 2$, and let $m \in Q_1 Q_2$. Then*

$$\varrho_{Q_1,Q_2}(m) \ll_\varepsilon \ell^\varepsilon \tag{6}$$

for every $\varepsilon > 0$, and

$$\sum_{m \in Q_1 Q_2} \varrho_{Q_1,Q_2}(m)^2 \ll (\ell \log \ell)^2. \tag{7}$$

Proof. Let $Q_i = \{r_i + uq_i : 0 \leqslant u < \ell\}$ for $i = 1, 2$. We may assume without loss of generality that $(r_i, q_i) = 1$. We write $r_i = s_i + h_i q_i$, where $0 < s_i \leqslant q_i$ and $h_i \geqslant 0$. Then

$$Q_i = \{s_i + vq_i : h_i \leqslant v < h_i + \ell\}.$$

If $w_1 \in Q_1$ and $w_2 \in Q_2$, then, for suitable $v_1 \in [h_1, h_1 + \ell[$, $v_2 \in [h_2, h_2 + \ell[$, we have

$$h_1 q_1 < w_1 = s_1 + v_1 q_1 \leqslant (h_1 + \ell)q_1 \leqslant \ell(h_1+1)q_1 \tag{8}$$

and

$$h_2 q_2 < w_2 = s_2 + v_2 q_2 \leqslant (h_2 + \ell)q_2 \leqslant \ell(h_2+1)q_2. \tag{9}$$

We can assume that

$$(h_2+1)q_2 \leqslant (h_1+1)q_1.$$

There are two cases. In the first case,

$$(h_1+1)q_1 < \ell^5.$$

By (8) and (9), we deduce that

$$w_1 \leqslant \ell(h_1+1)q_1 < \ell^6, \quad \text{and} \quad w_2 \leqslant \ell(h_2+1)q_2 \leqslant \ell(h_1+1)q_1 < \ell^6.$$

If $m \in Q_1 Q_2$, then m is of the form $m = w_1 w_2$, and so $m < \ell^{12}$. Since, by a classical estimate, $\tau(m) \ll_\varepsilon m^{\varepsilon/12}$, it follows that

$$\varrho_{Q_1,Q_2}(m) \leqslant \tau(m) \ll_\varepsilon m^{\varepsilon/12} \ll_\varepsilon \ell^\varepsilon.$$

This proves (6).