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>
INVERSE THEOREMS AND THE NUMBER OF SUMS AND PRODUCTS

by

Melvyn B. Nathanson & Gérald Tenenbaum

Abstract. — Let $\varepsilon > 0$. Erdős and Szemerédi conjectured that if $A$ is a set of $k$ positive integers which large $k$, there must be at least $k^{2-\varepsilon}$ 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

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

and

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

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.

© Astérisque 258, SMF 1999
and so the number of sums and products of two elements of $A$ is
\[ |E_2(A)| \leq k^2 + k. \]

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
\[ |A| = k \geq k_0(\varepsilon), \]
then
\[ |E_2(A)| \gg e^{k^2 - \varepsilon}. \]

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
\[ |E_2(A)| \geq ck^{32/31}, \]
where $c = 0.00028\ldots$.

Erdős and Szemerédi [4] also remarked that, in the special case that $|2A| \leq ck$, “perhaps there are more than $k^2/(\log k)^e$ 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
\[ (1) \quad \frac{k^2}{(\log k)^e} e^{-c\sqrt{\log_2 k \log_3 k}} \ll |A^2| \ll \frac{k^2}{(\log k)^e \sqrt{\log_2 k}}, \]
where $\log_r$ denotes the $r$-fold iterated logarithm, and
\[ (2) \quad \varepsilon_0 = 1 - \left( \frac{1 + \log_2 2}{\log 2} \right) \geq 0.08607 \]
(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 $|2A| \leq 3k - 4$, 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 $|A_1 + A_2| \leq 3k - 4$, then we have $|A_1 A_2| \gg (k/\log k)^2$. 

ASTÉRISQUE 258
2. Product sets of arithmetic progressions

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

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

We shall always assume that

$$\ell \geq 2.$$  

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 $m$,

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

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

**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

1. $0 < s \leq q$ and $(s, q) = 1$,
2. $q < y^{1-\alpha}$,
3. and $x^{\beta} < y \leq x$.

Then

$$\sum_{\substack{w \equiv s (\operatorname{mod} q) \leq y \leq x}} \tau(w) \ll_{\alpha, \beta} \frac{\varphi(q) y \log x}{q^2}.$$  

**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 $\ell$ be integers such that $h \geq 0$, $\ell \geq 2$, $0 < s \leq q$, and $(s, q) = 1$. Let $Q$ be the arithmetic progression

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

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 $q \leq (h + 1)q < \ell^5$, 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 \( h < \ell \), then, since \( 2 < \ell q < \ell q \), we have

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

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

\[
x^\beta = ((h + \ell)q)^\beta < (\ell hq)^\beta < \ell^6 \beta = \ell \leq \ell q = y \leq x.
\]

This shows that (5) holds.

Applying Lemma 1, we obtain

\[
\sum_{w \in Q} \tau(w) = \sum_{w \equiv s \pmod{q} \atop hq < w \leq (h + \ell)q} \tau(w) \ll \frac{\varphi(\ell)(\ell q) \log((h + \ell)q)}{q^2} < \ell \log(\ell(h + 1)q) \ll \ell \log \ell \ll \ell \log \ell.
\]

This completes the proof.

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

\[
\varrho_{Q_1,Q_2}(m) \ll \varepsilon \ell^\varepsilon
\]

for every \( \varepsilon > 0 \), and

\[
\sum_{m \in Q_1 Q_2} \varrho_{Q_1,Q_2}(m)^2 \ll (\ell \log \ell)^2.
\]

**Proof.** Let \( Q_i = \{r_i + uq_i : 0 \leq u < \ell \} \) 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 \( 0 < s_i \leq q_i \) and \( h_i \geq 0 \). Then

\[
Q_i = \{s_i + v q_i : h_i \leq v < h_i + \ell \}.
\]

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

\[
(8) \quad h_1 q_1 < w_1 = s_1 + v_1 q_1 \leq (h_1 + \ell) q_1 \leq \ell (h_1 + 1) q_1
\]

and

\[
(9) \quad h_2 q_2 < w_2 = s_2 + v_2 q_2 \leq (h_2 + \ell) q_2 \leq \ell (h_2 + 1) q_2.
\]

We can assume that

\[
(h_2 + 1) q_2 \leq (h_1 + 1) q_1.
\]

There are two cases. In the first case,

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

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

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

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

\[
\varrho_{Q_1,Q_2}(m) \leq \tau(m) \ll \varepsilon m^{\varepsilon/12} \ll \varepsilon \ell^\varepsilon.
\]

This proves (6).
To prove (7), we use the submultiplicativity of the divisor function, that is, \( \tau(uv) \leq \tau(u)\tau(v) \) for all positive integers \( u, v \). Then

\[
\sum_{m \in Q_1 Q_2} \varrho_{Q_1, Q_2}(m)^2 = \sum_{w_1 \in Q_1} \sum_{w_2 \in Q_2} \varrho_{Q_1, Q_2}(w_1w_2) \\
\leq \sum_{w_1 \in Q_1} \sum_{w_2 \in Q_2} \tau(w_1w_2) \\
\leq \sum_{w_1 \in Q_1} \tau(w_1) \sum_{w_2 \in Q_2} \tau(w_2) \ll \ell^2(\log \ell)^2,
\]

where the last upper bound follows from Lemma 2.

Consider now the second case

\[(h_1 + 1)q_1 \geq \ell^5.\]

We shall prove that

\[(10) \quad \varrho_{Q_1, Q_2}(m) \leq 3\]

for all \( m \geq 1 \). Suppose that \( w_1 = r_1 + uq_1 \in Q_1 \) and \( w'_1 = r_1 + u'q_1 \in Q_1 \) are distinct divisors of \( m \), and that \( w_1 < w'_1 \). Then \( (r_1, q_1) = 1 \) implies that \( (w_1, q_1) = (w'_1, q_1) = 1 \), and so \( ((w_1, w'_1), q_1) = 1 \). Since \( (w_1, w'_1) \) divides \( w'_1 - w_1 = (u' - u)q_1 \), it follows that \( (w_1, w'_1) \) divides \( u' - u \), and so

\[1 \leq (w_1, w'_1) \leq u' - u < \ell.\]

Suppose that \( \varrho_{Q_1, Q_2}(m) \geq 4 \). Then \( m \) has at least four distinct representations in the form \( m = w_1w_2 \) with \( w_1 \in Q_1 \) and \( w_2 \in Q_2 \), and so \( m \) has at least four different divisors in \( Q_1 \), that is, at least four divisors of the form

\[r_1 + uq_1 = s_1 + (h_1 + u)q_1\]

with \( 0 \leq u < \ell \). At most one of these divisors is \( s_1 + h_1q_1 \), and so \( m \) has at least three different divisors, which we shall denote by \( w_1, w'_1 \), and \( w''_1 \), such that

\[\min\{w_1, w'_1, w''_1\} \geq s_1 + (h_1 + 1)q_1 > (h_1 + 1)q_1 \geq \ell^5.\]

Let \([w_1, w'_1, w''_1]\) denote the least common multiple of \( w_1, w'_1 \), and \( w''_1 \). Since each of these three numbers is a divisor of \( m \), we have

\[
m \geq [w_1, w'_1, w''_1] \geq \frac{w_1w'_1w''_1}{(w_1, w'_1)(w_1, w''_1)(w'_1, w''_1)} \geq \left(\frac{(h_1 + 1)q_1}{\ell}\right)^3 \geq \frac{(h_1 + 1)q_1}{\ell^3} (h_1 + 1)^2 q_1^2 \geq \ell^2 \left(\frac{(h_1 + 1)q_1}{\ell}\right)^2 \geq \ell(h_1 + 1)q_1 \cdot \ell(h_2 + 1)q_2 \geq w_1w_2 = m,
\]

which is impossible. This proves (10), and inequalities (6) and (7) follow immediately.
**Lemma 4.** Let $Q$ be an arithmetic progression of length $\ell \geq 2$, and let $m \in Q^2$. Then
\begin{equation}
\varrho_Q(m) \ll \varepsilon \ell^\varepsilon
\end{equation}
for every $\varepsilon > 0$, and
\begin{equation}
\sum_{m \in Q^2} \varrho_Q(m)^2 \ll (\ell \log \ell)^2.
\end{equation}

**Proof.** This follows immediately from Lemma 3 with $Q_1 = Q_2 = Q$.

**Lemma 5.** Let $Q_1$ and $Q_2$ be arithmetic progressions of length $\ell \geq 2$. Then
\begin{equation}
|Q_1 Q_2| \gg \left( \frac{\ell}{\log \ell} \right)^2.
\end{equation}

**Proof.** Let $\varrho_{Q_1, Q_2}(m)$ denote the number of representations of $m$ in the form $m = q_1 q_2$, where $q_1 \in Q_1$ and $q_2 \in Q_2$. By the Cauchy-Schwarz inequality and inequality (7) of Lemma 3,
\begin{align*}
\ell^2 &= \sum_{m \in Q_1 Q_2} \varrho_{Q_1, Q_2}(m) \\
&\leq |Q_1 Q_2|^{1/2} \left( \sum_{m \in Q_1 Q_2} \varrho_{Q_1, Q_2}(m)^2 \right)^{1/2} \\
&\ll |Q_1 Q_2|^{1/2} \ell \log \ell.
\end{align*}
Therefore,
\begin{equation}
|Q_1 Q_2| \gg \left( \frac{\ell}{\log \ell} \right)^2.
\end{equation}
This completes the proof.

**Lemma 6.** Let $Q$ be an arithmetic progression of length $\ell \geq 2$. Then
\begin{equation}
|Q^2| \gg \left( \frac{\ell}{\log \ell} \right)^2.
\end{equation}

**Proof.** This follows immediately from Lemma 5 with $Q_1 = Q_2 = Q$.

3. Application of some inverse theorems

We shall use the following two inverse theorems of Freiman.

**Lemma 7 (Freiman).** Let $A$ be a nonempty set of $k$ positive integers. If
\begin{equation}
|2A| \leq 3k - 4,
\end{equation}
then $A$ is a subset of an arithmetic progression of length $\ell < 2k$.

**Proof.** See [5, 7, 10, 12].
**Lemma 8 (Freiman).** — Let $A_1$ and $A_2$ be nonempty finite sets of positive integers, and let $|A_i| = k_i$ for $i = 1, 2$. If

$$|A_1 + A_2| \leq k_1 + k_2 + \min\{k_1, k_2\} - 4,$$

then $A_1$ and $A_2$ are subsets of arithmetic progressions $Q_1$ and $Q_2$, respectively, where $Q_1$ and $Q_2$ have the same difference and the same length $\ell < k_1 + k_2$.

**Proof.** See [6, 9, 12, 15].

**Theorem 1.** — Let $A$ be a finite set of positive integers, and let $|A| = k \geq 2$. If

$$|2A| \leq 3k - 4,$$

then

$$|A^2| \gg \left(\frac{k}{\log k}\right)^2.$$

**Proof.** By Lemma 7, if $|2A| \leq 3k - 4$, then there exists an arithmetic progression $Q$ of length $\ell < 2k$ such that $A \subseteq Q$. Since

$$\varrho_A(m) \leq \varrho_Q(m),$$

it follows from (12) that

$$k^2 = \sum_{m \in A^2} \varrho_A(m) \leq |A^2|^{1/2} \left( \sum_{m \in A^2} \varrho_A(m)^2 \right)^{1/2} \leq |A^2|^{1/2} \left( \sum_{m \in Q^2} \varrho_Q(m)^2 \right)^{1/2} \ll |A^2|^{1/2} \ell \log \ell \ll |A^2|^{1/2} k \log k.$$

Therefore,

$$|A^2| \gg \left(\frac{k}{\log k}\right)^2. \quad (13)$$

This completes the proof.

**Theorem 2.** — Let $\lambda \geq 1$. Let $A_1$ and $A_2$ be finite sets of positive integers such that $|A_i| = k_i \geq 2$ for $i = 1, 2$ and

$$\frac{1}{\lambda} \leq \frac{k_2}{k_1} \leq \lambda. \quad (14)$$

If

$$|A_1 + A_2| \leq k_1 + k_2 + \min\{k_1, k_2\} - 4,$$

then

$$|A_1 A_2| \gg \lambda \frac{k_1 k_2}{(\log(k_1 k_2))^2}. $$
Proof. It follows from (14) that
\[(k_1 + k_2)^2 \leq (1 + \lambda)^2 k_1^2 = (1 + \lambda)^2 \lambda k_1 / (k_1 / \lambda) \leq (1 + \lambda)^2 \lambda k_1 k_2,
\]
and so
\[k_1 + k_2 \ll \lambda (k_1 k_2)^{1/2}.
\]
By Lemma 8, if \(|A_1 + A_2| \leq k_1 + k_2 + \min\{k_1, k_2\} - 4\), there exist arithmetic progressions \(Q_1\) and \(Q_2\), each of length \(\ell < k_1 + k_2\), such that \(A_1 \subseteq Q_1\) and \(A_2 \subseteq Q_2\). Since
\[\varrho_{A_1, A_2}(m) \leq \varrho_{Q_1, Q_2}(m),
\]
it follows from (7) that
\[k_1 k_2 = \sum_{m \in A_1 A_2} \varrho_{A_1, A_2} (m)
\leq |A_1 A_2|^{1/2} \left( \sum_{m \in A_1 A_2} \varrho_{A_1, A_2} (m)^2 \right)^{1/2}
\leq |A_1 A_2|^{1/2} \left( \sum_{m \in Q_1 Q_2} \varrho_{Q_1, Q_2} (m)^2 \right)^{1/2}
\ll |A_1 A_2|^{1/2} \ell \log \ell \ll |A_1 A_2|^{1/2} (k_1 + k_2) \log (k_1 + k_2)
\ll \lambda |A_1 A_2|^{1/2} (k_1 k_2)^{1/2} \log (k_1 k_2).
\]
Therefore,
\[(15) \quad |A_1 A_2| \gg \lambda \frac{k_1 k_2}{(\log (k_1 k_2))^2}.
\]
This completes the proof.

Theorem 3. — Let \(A_1\) and \(A_2\) be finite sets of positive integers such that \(|A_1| = |A_2| = k \geq 2\). If
\[|A_1 + A_2| \leq 3k - 4,
\]
then
\[|A_1 A_2| \gg \left( \frac{k}{\log k} \right)^2.
\]
Proof. This follows immediately from Theorem 2 with \(k_1 = k_2 = k\) and \(\lambda = 1\).

4. Open problems

By Theorem 1, if \(|A| = k\) and \(|2A| \leq 3k - 4\), then \(|A^2| \gg k^{2-\varepsilon}\). This gives the first general case in which we know that the conjecture of Erdős and Szemerédi is true. It would be nice to prove that if \(c \geq 3\) and if \(A\) is a finite set of \(k\) positive integers such that
\[(16) \quad |2A| \leq ck,
\]
then
\[ |A^2| \gg_{\varepsilon, \kappa} \kappa^{2-\varepsilon} \]

By a general inverse theorem of Freiman [7, 12, 13], a finite set of integers whose sumset satisfies inequality (16) is a "large" subset of what is called an \( n \)-dimensional arithmetic progression. This is a set \( Q \) with the following structure: For \( n \geq 1 \), there exist positive integers \( r, q_1, \ldots, q_n, \ell_1, \ldots, \ell_n \) such that
\[ Q = \{ r + u_1 q_1 + \cdots + u_n q_n : 0 \leq u_i < \ell_i \text{ for } i = 1, \ldots, n \}. \]

The length of \( Q \) is defined as \( \ell(Q) = \ell_1 \cdots \ell_n \). Clearly,
\[ |Q| \leq \ell(Q) \]
for every \( n \)-dimensional arithmetic progression. Freiman's inverse theorem should be applicable to the Erdős-Szemerédi conjecture for sets satisfying the additive condition (16).

Let \( Q \) be an \( n \)-dimensional arithmetic progression of the form (17). If \( j \) is such that \( \ell_j = \max\{\ell_i : i = 1, \ldots, n\} \) in (17), then
\[ Q \supseteq Q_j = \{ r + u_j q_j : 0 \leq u_j < \ell_j \}. \]

It follows from Lemma 6 that
\[ |Q^2| \gg |Q_j^2| \gg \left( \frac{\ell_j}{\log \ell_j} \right)^2. \]

The following example shows that this inequality is almost best possible. Fix \( n \geq 2 \). For \( \ell \geq 2 \), consider the \( n \)-dimensional arithmetic progression \( Q \) with \( r = 1 \), \( q_i = i \) and \( \ell_i = \ell \) for \( i = 1, \ldots, n \). Then
\[ Q = \{ 1 + \sum_{i=1}^n i u_i : 0 \leq u_i < \ell \} \subseteq \left[ 1, 1 + \frac{1}{2} n(n + 1)(\ell - 1) \right] \subseteq [1, n^2 \ell]. \]

We apply the lower bound (18) with \( \ell = \max\{\ell_i : i = 1, \ldots, n\} \), and we apply the upper bound (1) with \( k = n^2 \ell \). For sufficiently large \( \ell \) we obtain
\[ \left( \frac{\ell}{\log \ell} \right)^2 \ll |Q^2| \ll \frac{k^2}{(\log k)^{\varepsilon_0}} \ll n \frac{\ell^2}{(\log \ell)^{\varepsilon_0}}, \]
where \( \varepsilon_0 \) is defined by (2). Since \( \ell(Q) = \ell^n \), it is clearly not true that
\[ |Q^2| \gg_{n, \varepsilon} \ell(Q)^{2-\varepsilon}. \]

It would be interesting to obtain sufficient conditions for an \( n \)-dimensional arithmetic progression \( Q \) to satisfy
\[ |Q^2| \gg_{n, \varepsilon} |Q|^{2-\varepsilon}. \]

Let \( A \) be a set of \( k \) positive integers. For \( h \geq 3 \), let \( E_h(A) \) denote the set of all numbers that can be written as the sum or product of \( h \) elements of \( A \). Erdős and Szemerédi [4] also conjectured that
\[ |E_h(A)| \gg_{\varepsilon} k^{h-\varepsilon} \]
for all \( \varepsilon > 0 \). Nothing is known about this.
References


