PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 125, Number 1, January 1997, Pages 9–16
S 0002-9939(97)03510-7

ON SUMS AND PRODUCTS OF INTEGERS

MELVYN B. NATHANSON

(Communicated by William W. Adams)

Abstract. Erdős and Szemerédi conjectured that if A is a set of k positive integers, then there must be at least $k^{2-\varepsilon}$ integers that can be written as the sum or product of two elements of A. Erdős and Szemerédi proved that this number must be at least $ck^{1+\delta}$ for some $\delta > 0$ and $k \geq k_0$. In this paper it is proved that the result holds for $\delta = 1/31$.

1. A conjecture of Erdős and Szemerédi

Let $h \geq 2$, and let $A_1, \ldots, A_h$ be finite sets of positive integers. We consider the *sumset*

$$A_1 + \cdots + A_h = \{a_1 + \cdots + a_h \mid a_i \in A_i \text{ for } i = 1, \ldots, h\}$$

and the *product set*

$$A_1 \cdots A_h = \{a_1 \cdots a_h \mid a_i \in A_i \text{ for } i = 1, \ldots, h\}.$$

If $A_i = A$ for all i, we let

$$hA = \{a_1 + \cdots + a_h \mid a_i \in A \text{ for } i = 1, \ldots, h\}$$

denote the h-fold sumset of A, and we let

$$A^h = \{a_1 \cdots a_h \mid a_i \in A \text{ for } i = 1, \ldots, h\}$$

denote the h-fold product set of A. We let

$$E_h(A) = hA \cup A^h$$

denote the set of all integers that can be written as the sum or product of h elements of A.

Clearly, if $|A| = k$, then

$$|hA| \leq \binom{k+h-1}{h}$$

and

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

Received by the editors June 25, 1994 and, in revised form, May 23, 1995.
1991 *Mathematics Subject Classification.* Primary 11B05, 11B13, 11B75, 11P99, 05A17.
Key words and phrases. Additive number theory, sumsets, sums and products of integers.
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 h elements of A is

$$|E_h(A)| \leq 2\binom{k+h-1}{h} = \frac{2k^h}{h!} + O(k^{h-1}).$$

Erdős and Szemerédi [1, 3] have 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

$$|E_h(A)| \gg k^{h-\varepsilon}.$$

Nothing is known about this conjecture for $h \geq 3$.

For $h = 2$, Nathanson and Tenenbaum [4] have proved that if $|A| = k$ and $|2A| \leq 3k-4$, then

$$|A^2| \gg k^{2-\varepsilon}.$$

This is the only case in which the full conjecture has been proven.

For an arbitrary set of k positive integers, Erdős and Szemerédi [3] have shown that there exists a real number $\delta > 0$ such that

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

Erdős [2] recently observed that "our paper with Szemerédi has nearly been forgotten." The purpose of this paper is to give a careful version of the Erdős-Szemerédi proof that allows the explicit calculation of an exponent δ.

Notation. For any set A of integers, let $|A|$ denote the cardinality of the set A, let $\max(A)$ denote the largest element of A, and let $\min(A)$ denote the smallest element of A. For $x \in \mathbf{R}$, let $[x]$ denote the largest integer not exceeding x. Note that $[x] > x/2$ if $x \geq 2$. Let $[x_1, x_2) = \{n \in \mathbf{Z} \mid x_1 \leq n < x_2\}$.

2. Sets of small diameter

In this section we obtain a result in the special case of sets of small diameter, and in the next section we show that the main theorem reduces to this special case.

Lemma 1. *Let B be a nonempty, finite set of positive integers such that*

$$\max(B) \leq 2\min(B).$$

Then

$$|E_2(B)| \geq \left(\frac{|B|}{384}\right)^{16/15}.$$

Proof. Let $|B| = k$. If $k < 384$, the inequality is trivial, so we can assume that

$$k \geq 384 = 2^5 12.$$

Then

$$(k/12)^{1/5} \geq 2.$$

Let

$$l = \left[\left(\frac{k}{12}\right)^{1/5}\right].$$

Then

$$l \geq \frac{1}{2}\left(\frac{k}{12}\right)^{1/5} = \left(\frac{k}{384}\right)^{1/5}.$$

Since

$$k \geq 12l^5,$$

it follows that

$$\left[\frac{k}{l}\right] \geq 12l^4. \tag{1}$$

Let $B = \{b_1, \ldots, b_k\}$, where

$$1 \leq b_1 < b_2 < \cdots < b_k \leq 2b_1.$$

For $i = 1, 2, \ldots, [k/l]$, let

$$B_i = \{b_{(i-1)l+1}, b_{(i-1)l+2}, \ldots, b_{il}\} \subseteq B$$

and

$$d_i = b_{il} - b_{(i-1)l+1}.$$

Choose i_0 so that

$$d_{i_0} = \min\{d_i \mid i = 1, \ldots, [k/l]\},$$

and let

$$B^* = B_{i_0}$$

and

$$d^* = d_{i_0}.$$

Suppose that

$$1 \leq i < j \leq \left[\frac{k}{l}\right] \text{ and } j - i \geq 3.$$

If

$$b_1^*, b_2^* \in B^* \text{ and } b_i' \in B_i, b_j' \in B_j,$$

then

$$x^* = b_2^* - b_1^* \leq d^*$$

and

$$x = b_j' - b_i' > d_{i+1} + d_{i+2} \cdots + d_{j-1} \geq 2d^* > 0.$$

It follows that

$$b_1^* + b_j' \neq b_2^* + b_i'.$$

Suppose that

$$b_1^* b_j' = b_2^* b_i'.$$

Since $b_i' < b_j'$, it follows that $b_2^* > b_1^*$ and so $x^* > 0$. Since

$$b_j' \leq b_k \leq 2b_1 \leq 2b_1^*,$$

it follows that

$$b_1^* b_j' = b_2^* b_i' = (b_1^* + x^*)(b_j' - x) = b_1^* b_j' + x^* b_j' - x b_1^* - x^* x,$$

and so

$$0 < x^* x = x^* b_j' - x b_1^* \leq b_1^*(2x^* - x) \leq b_1^*(2d^* - x) < 0,$$

which is absurd. Therefore,

$$b_1^* b_j' \neq b_2^* b_i'.$$

It follows that

$$(B^* + B_j) \cap (B^* + B_i) = \emptyset \tag{2}$$

and

$$(B^* \cdot B_j) \cap (B^* \cdot B_i) = \emptyset \tag{3}$$

for every pair i, j of integers such that $j - i \geq 3$.

We shall consider only the sets $B_1, B_4, B_7, \ldots$, that is, the sets B_i such that $i \equiv 1 \pmod 3$. There are at least

$$\frac{1}{3}\left[\frac{k}{l}\right]$$

such sets. Let

$$0 < \theta < 1$$

and

$$\beta = \theta/3 < 1/3.$$

Let

$$E(B^*, B_i) = (B^* + B_i) \cup (B^* \cdot B_i),$$

and let

$$I_1 = \{i \equiv 1 \pmod 3 \bigm| |E(B^*, B_i)| < l^{1+\beta}\}$$

and

$$I_2 = \{i \equiv 1 \pmod 3 \bigm| |E(B^*, B_i)| \geq l^{1+\beta}\}.$$

Then

$$|I_1| + |I_2| \geq \frac{1}{3}\left[\frac{k}{l}\right]. \tag{4}$$

Suppose that

$$|I_1| \geq \frac{1}{6}\left[\frac{k}{l}\right].$$

Let $i \in I_1$. For $m \in B^* \cdot B_i$, let $\rho(m)$ denote the number of representations of m in the form $b^* b'_i$, where $b^* \in B^*$ and $b'_i \in B_i$. Choose m' such that

$$\rho(m') = \max\{\rho(m) \bigm| m \in B^* \cdot B_i\}.$$

Since $|B^*| = |B_i| = l$, it follows that

$$l^2 = \sum_{m \in B^* \cdot B_i} \rho(m) \leq \rho(m')|B^* \cdot B_i| < \rho(m') l^{1+\beta},$$

and so

$$\rho(m') > l^{1-\beta}.$$

For $j = 1, \ldots, \rho(m')$, choose $b^*_j \in B^*$ and $b'_j \in B_i$ such that

$$b^*_j b'_j = m' \tag{5}$$

and $b^*_{j_1} \neq b^*_{j_2}$ for $j_1 \neq j_2$. There are $\rho(m')^2$ expressions of the form

$$b^*_j + b'_{j'} \in B^* + B_i,$$

where $j, j' = 1, \ldots, \rho(m')$. Since $i \in I_1$ and $\beta < 1/3$, it follows that

$$\rho(m')^2 > l^{2-2\beta} > l^{1+\beta} > |B^* + B'_i|,$$

and so there exist $b^*_{j_1}, b^*_{j_2} \in B^*$ and $b'_{j_3}, b'_{j_4} \in B_i$ such that $b^*_{j_1} \neq b^*_{j_2}$ and

$$b^*_{j_1} + b'_{j_3} = b^*_{j_2} + b'_{j_4}. \tag{6}$$

It follows from (5) that also

$$b^*_{j_3}b'_{j_3} = b^*_{j_4}b'_{j_4}. \tag{7}$$

What we have just shown is that for every $i \in I_1$ there exist four positive integers $b^*_{j_1}, b^*_{j_2}, b^*_{j_3}, b^*_{j_4} \in B^*$ and two positive integers $b'_{j_3}, b'_{j_4} \in B_i$ that satisfy equations (6) and (7). However, given any positive integers $b^*_{j_1}, b^*_{j_2}, b^*_{j_3}, b^*_{j_4}$, equations (6) and (7) have at most one solution in integers b'_{j_3}, b'_{j_4}. Since the number of quadruples of elements of B^* is exactly l^4, it follows from (1) that if $|I_1| \geq (1/6)[k/l]$, then

$$l^4 \geq |I_1| \geq \frac{1}{6}\left[\frac{k}{l}\right] \geq 2l^4,$$

which is absurd. Therefore,

$$|I_1| < \frac{1}{6}\left[\frac{k}{l}\right],$$

and so, by (4), we have

$$|I_2| \geq \frac{1}{6}\left[\frac{k}{l}\right].$$

Let

$$n \in \bigcup_{i\in I_2} E(B^*, B_i).$$

It follows from (2) and (3) that n belongs to at most two of the sets $E(B^*, B_i)$. Therefore,

$$\begin{aligned}
|E_2(B)| &\geq \left|\bigcup_{i\in I_2} E(B^*, B_i)\right| \geq (1/2)\sum_{i\in I_2}|E(B^*, B_i)| \\
&\geq (1/2)|I_2|l^{1+\beta} \geq (1/12)\left[\frac{k}{l}\right]l^{1+\beta} \geq (1/12)(12l^4)l^{1+\beta} \\
&= l^{5+\beta} \geq \left(\frac{k}{384}\right)^{1+\beta/5} = \left(\frac{k}{384}\right)^{1+\theta/15}.
\end{aligned}$$

Since this holds for all $\theta < 1$, we obtain

$$|E_2(B)| \geq \left(\frac{k}{384}\right)^{16/15}.$$

This completes the proof of the lemma.

3. The main result

Theorem 1. *Let A be a nonempty, finite set of positive integers. Then*

$$|E_2(A)| \geq c|A|^{32/31},$$

where $c = 0.00028\ldots$.

Proof. For $j = 1, 2, \ldots$, let

$$U_j = [2^{j-1}, 2^j)$$

and

$$V_j = [4^{j-1}, 4^j) = U_{2j-1} \cup U_{2j}.$$

Let

$$A_j = A \cap U_j = \{a \in A \mid 2^{j-1} \leq a < 2^j\}$$

for $j = 1, 2, \ldots$. Then $A = \bigcup_{j=1}^{\infty} A_j$, the sets A_j are pairwise disjoint, and

$$\sum_{j=1}^{\infty} |A_j| = k.$$

Let $\alpha > 0$, and let

$$c_1 = (384)^{-16/15}$$

and

$$c_2(\alpha) = \frac{c_1}{3 \cdot 2^{1+\alpha/15}} < \frac{c_1}{3} < \frac{1}{32}.$$

There are two cases. In the first case, we assume that if $A_j \neq \emptyset$, then

$$|A_j| \geq k^{\alpha}.$$

Since $\max(A_j) \leq 2\min(A_j)$, the set A_j satisfies the conditions of the lemma, and so

$$|E_2(A_j)| \geq c_1 |A_j|^{16/15}.$$

Let

$$n \in \bigcup_{j=1}^{\infty} E_2(A_j).$$

There exists a unique integer t such that

$$n \in V_t = U_{2t-1} \cup U_{2t}.$$

Observe that if $a, a' \in A_j$, then $a + a' \in U_{j+1}$ and $aa' \in V_j$. Suppose that $n \in E_2(A_j)$. If n is a product of two elements of A_j, then $n \in V_j$ and so $j = t$. If n is a sum of two elements of A_j, then $n \in U_{j+1}$, and so $j = 2t - 2$ or $2t - 1$. Therefore, n belongs to at most three of the sets $E_2(A_j)$. It follows that

$$\begin{aligned}
|E_2(A)| &\geq \left| \bigcup_{j=1}^{\infty} E_2(A_j) \right| \\
&\geq (1/3) \sum_{j=1}^{\infty} |E_2(A_j)| \\
&\geq (1/3) \sum_{j=1}^{\infty} c_1 |A_j|^{16/15} \\
&= (c_1/3) \sum_{j=1}^{\infty} |A_j| \cdot |A_j|^{1/15} \\
&\geq (c_1/3) k^{\alpha/15} \sum_{j=1}^{\infty} |A_j| \\
&= (c_1/3) k^{\alpha/15} k \\
&> c_2(\alpha) k^{1+\alpha/15}.
\end{aligned}$$

In the second case, there exist sets A_j such that

$$0 < |A_j| < k^{\alpha}.$$

Let

$$J = \{ j \mid 0 < |A_j| < k^{\alpha} \}.$$

If

$$\left|\bigcup_{j\in J} A_j\right| < k/2,$$

let

$$A' = A \setminus \left(\bigcup_{j\in J} A_j\right),$$

and let

$$A'_j = A' \cap U_j = \{a \in A' \mid 2^{j-1} \leq a < 2^j\}.$$

Then

$$k/2 < |A'| = k' \leq k.$$

If $A'_j \neq \emptyset$, then $A'_j = A_j$ and

$$|A'_j| = |A_j| \geq k^\alpha \geq (k')^\alpha.$$

Therefore, we can apply the previous case to the set A', and obtain

$$|E_2(A)| \geq |E_2(A')| \geq (c_1/3)(k')^{1+\alpha/15} > c_2(\alpha)k^{1+\alpha/15}.$$

On the other hand, if

$$k/2 \leq \left|\bigcup_{j\in J} A_j\right| < |J|k^\alpha,$$

then

$$|J| > k^{1-\alpha}/2.$$

Let $j_1 < j_2 < j_3 < \cdots$ be the elements of J arranged in increasing order, and choose

$$a_1^* \in A_{j_1}, a_3^* \in A_{j_3}, a_5^* \in A_{j_5}, \dots .$$

Let

$$A^* = \{a_{j_i}^* \mid i = 1, 3, 5, \dots\} \subseteq A.$$

Then

$$|A^*| \geq |J|/2 > k^{1-\alpha}/4.$$

Since $a_i^* \in A_{j_i}$, it follows that

$$2a_i^* < 2^{j_i+1} \leq 2^{j_{i+1}} \leq 2^{j_{i+2}-1} \leq a_{i+2}^*,$$

and so the sums of distinct pairs of elements of A^* are distinct. Therefore,

$$|E_2(A)| \geq |E_2(A^*)| \geq |2A^*| > |A^*|^2/2 > k^{2-2\alpha}/32 > c_2(\alpha)k^{2-2\alpha}.$$

Choose

$$\alpha = 15/31.$$

Then

$$2 - 2\alpha = 1 + \frac{\alpha}{15},$$

and we obtain

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

where

$$c = c_2(15/31) = \frac{1}{6 \cdot (384)^{16/15} \cdot 2^{1/31}} = 0.00028\dots .$$

This completes the proof of the theorem.

References

1. P. Erdős, Problems and results on combinatorial number theory III, in: M. B. Nathanson, editor, *Number Theory Day, New York 1976*, *Lecture Notes in Mathematics*, vol. 626, 1977, Springer-Verlag, Berlin, pp. 43–72. MR **57:**12442
2. P. Erdős, Problems and results in combinatorial analysis and combinatorial number theory, in: Y. Alavi, G. Chartrand, O. R. Ollerman, and A. J. Schwenk, editors, *Graph Theory, Combinatorics, and Applications*, 1991, John Wiley, New York, pp. 397–406. MR **93g:**05136
3. P. Erdős and E. Szemerédi, On sums and products of integers, in: P. Erdős, L. Alpár, G. Halász, and A. Sárközy, editors, *Studies in Pure Mathematics, To the Memory of Paul Turán*, 1983, Birkhäuser Verlag, Basel, pp. 213–218. MR **86m:**11011
4. M. B. Nathanson and G. Tenenbaum, Inverse theorems and the number of sums and products (to appear).

Department of Mathematics, Lehman College (CUNY), Bronx, New York 10468
E-mail address: `nathansn@alpha.lehman.cuny.edu`