Reprinted from JOURNAL OF NUMBER THEORY
All Rights Reserved by Academic Press, New York and London

Vol. 6, No. 6, December 1974
Printed in Belgium

On Products of Integers

S. L. G. CHOI AND P. ERDÖS

Mathematics Department, University of British Columbia, Vancouver 8, B.C., Canada
and
Hungarian Academy of Sciences, Budapest, Hungary

Received January 6, 1974

DEDICATED TO PROFESSOR K. MAHLER ON THE OCCASION OF HIS 70TH BIRTHDAY

The main objective of this paper is to investigate the relation between the number of integers in a given subset $\mathscr{A}$ of the integers $1, 2,..., n$ and the number of integers that can be chosen from $1, 2,..., n$ so that their pairwise products all appear in $\mathscr{A}$. Other related problems are also considered.

1. INTRODUCTION

The problems under investigation in the present paper are of the following type: Given a set $\mathscr{A}$ in $[1, n]$, what is the relation between $|\mathscr{A}|$ and the number of integers that can be chosen from $[1, n]$ whose pairwise products all appear in $\mathscr{A}$? We prove the following theorems.

THEOREM 1. *There exists $\alpha > 0$ and a set $\mathscr{A}$ in $[1, n]$ where $|\mathscr{A}| > n - n(\log n)^{-\alpha}$ so that there cannot be three integers b_1, b_2, b_3 with products $b_i b_j$ $(1 \leqslant i < j \leqslant 3)$ all in $\mathscr{A}$.*

THEOREM 2. *For each $k \geqslant 3$ there exists a positive $\beta_k < 1$ so that if $\mathscr{A}$ is a set of integers in $[1, n]$, where $|\mathscr{A}| > n - n(\log n)^{-\beta_k}$, then there are integers $b_1,..., b_k$ whose products $b_i b_j$ $(1 \leqslant i < j \leqslant k)$ all appear in $\mathscr{A}$.*

THEOREM 3. *Corresponding to $\delta > 0$ there exists an integer $t = t(\delta)$, where $t \to \infty$ as $\delta \to 0$, so that if $\mathscr{A}$ is a set of integers in $[1, n]$, where*

$$|\mathscr{A}| > (1 - \delta)n, \qquad n \geqslant n_0(\delta),$$

then there are t integers $b_1,..., b_t$ and some number μ so that $b_i b_j \mu$ $(1 \leqslant i < j \leqslant t)$ all appear in $\mathscr{A}$.

THEOREM 4. *Corresponding to each* $\delta > 0$ *there exists* $C = C(\delta)$ *and a set* $\mathscr{A}$ *of integers in* $[1, n]$, *where*

$$|\mathscr{A}| \geqslant (1 - \delta)n,$$

so that for every $\alpha = k/m$, *where* $m \leqslant n$, *there are at most* $t \leqslant (\log n)^C$ *integers* $b_1, \ldots, b_t$ *integers with* $b_i b_j \alpha$ *all appearing in* $\mathscr{A}$.

THEOREM 5. *Let* p *be a prime. Suppose* $a_1, \ldots, a_t \bmod p$ *are* t *distinct congruence classes* $\bmod p$, *where* $t \geqslant (\frac{1}{2} + \epsilon)p$. *Then there are at least* $s \gg \log\log p$ *congruence classes* $\bmod p$ $b_1, \ldots, b_s$ *so that* $b_i b_j$ *are all in* a's $\bmod p$.

THEOREM 6. *Suppose* $a_1, \ldots, a_t \bmod p$ *are* t *distinct congruence classes where* $t \geqslant (\frac{2}{3} + \epsilon)p$. *Then there are* k *classes* $\bmod p$ $a_{i_1}, \ldots, a_{i_k}$ *so that* $a_{i_j} a_{i_l}$ *are all in* a's $\bmod p$.

THEOREM 7. *For every* r *there exists* $\delta_r > 0$ *so that if* $a_1, \ldots, a_t \bmod p$ *are* t *distinct congruence classes, where* $t \geqslant (1 - \delta_r)p$, *then, provided* $p \geqslant p_0(k, r)$, *there are* k *classes* $b_1, \ldots, b_k \bmod p$ *so that* $\prod_{i=1}^{k} b_i^{\epsilon_i}$ $(\sum \epsilon_i \leqslant r$, $\epsilon_i = 0, 1)$, *are all in* a's $\bmod p$.

2. PROOFS OF THEOREMS

Proof of Theorem 1. We let $\mathscr{A}$ consist of the integers in $(n/\log n, n)$ which have no divisors in $(n^{1/2}/\log n, n^{1/2})$. Then it follows from the method of Erdös [1, 2] that

$$|\mathscr{A}| > n - n(\log n)^{-\alpha}, \qquad \text{for some} \quad \alpha > 0.$$

It is clear that we cannot choose three integers b_1, b_2, b_3 with $b_i b_j$ in $\mathscr{A}$, since at most one b can be $\geqslant n^{1/2}$ and at most one can be less than $n^{1/2}(\log n)^{-1}$, and there can be none in $(n^{1/2}/\log n, n^{1/2})$.

An example giving a somewhat weaker result is as follows: Let $\mathscr{A}$ consist of those integers in $[1, n]$ not of the form xy, where $x \leqslant n^{1/2}$ and $y \leqslant n^{1/2}$.

Proof of Theorem 2. Let $\mathscr{T}$ denote the set of integers in $(\frac{1}{2}n^{1/2}, n^{1/2})$ having $[(\log\log n)/2]$ distinct prime factors. Then the number t of elements in $\mathscr{T}$ is given by

$$t = (1 + o(1)) \frac{n^{1/2}}{2\log n} \frac{(\log\log n)^{(\log\log n)/2}}{[\frac{1}{2}\log\log n]!}.$$

We shall call an integer in $\mathscr{T}$ good if it has at least $\epsilon \log\log n$ prime factors $p_1, ..., p_r$, $r \geqslant \epsilon \log\log n$, so that $d/d' > 4$ for any two distinct divisors d, d', $(d > d')$, of $p_1 \cdots\cdots p_r$. Let $\mathscr{T}_1 = \{b_1, ..., b_k\}$ denote the subset of good integers in $\mathscr{T}$. By a simple computation[1] we have

$$k = (1 + o(1))t.$$

It is also clear that the equation $m = b_1 b_j$ has at most $2^{(1-\epsilon)\log\log n}$ solutions in b_i, b_j, since if $b_i b_j = b_i' b_j'$, then b_i/b_i' cannot be equal to d/d' where d and d' are distinct divisors of $p_1 \cdots\cdots p_r$. Thus the total number of distinct (pairwise) products determined by the integers of $\mathscr{T}_1$ is at least

$$\frac{k^2}{2^{(1-\epsilon)\log\log n}} \geqslant \frac{\frac{1}{4}(1 + o(1))n}{2^{(1-\epsilon)\log\log n}(\log n)^2} \frac{(\log\log n)^{\log\log n}(2e)^{\log\log n}}{(2\pi)(\log\log n)^{\log\log n}}$$
$$\geqslant \frac{n}{(\log n)^{1-\epsilon_1}},$$

where $\epsilon_1 = \epsilon/2$, say. Since $|\mathscr{A}| > n - n(\log n)^{-\beta_k}$, by choosing $\beta_k < 1$ sufficiently close to 1, we may assert that there is an integer b, say b_{i_1} so that $b_{i_1} b_j$ belongs to $\mathscr{A}$ for at least $\frac{1}{2}k$ integers b_j in $\mathscr{T}_1$. We may now repeat the argument with these integers b_j instead of $\mathscr{T}_1$, and so on. This completes the proof of the theorem.

It would be of interest to determine β_k exactly.

Proof of Theorem 3. We may assume δ small. It involves only a straightforward computation to show that the number of integers $\leqslant n$ of the form $2^a d$, (d odd, $\delta_1 n \leqslant d \leqslant n$) is at most

$$n(1 + o(1))(1 - \delta_1 + (\delta_1 \log \delta_1)(2 \log 2)^{-1}).$$

We determine δ_1 by

$$\delta_1 - \delta_1 \log \delta_1/2 \log 2 = 2\delta$$

so that in particular

$$\delta_1 < c\delta/\log(1/\delta), \tag{1}$$

where c is an absolute constant. There are thus at least δn integers in $\mathscr{A}$ of the form $2^a d$, d odd and $d \leqslant \delta_1 n$. Since there are $n(1 + o(1))(2\delta)$ such integers altogether, we conclude that $\mathscr{A}$ contains at least $\frac{1}{2} + o(1)$ of such integers. Therefore there exists in $\mathscr{A}$ a set of the form

$$2^{a_1}d, 2^{a_2}d, ..., 2^{a_k}d, \qquad d \leqslant \delta_1 n, \tag{2}$$

[1] It is sufficient, for our present purposes, that k should be sufficiently numerous, say $k \geqslant ct$, where $c > 0$ is an absolute constant.

where
$$k \geqslant (\tfrac{1}{2} + o(1))\,(\log(n/a)/\log 2) \tag{3}$$
and
$$a_1 < \cdots < a_k \leqslant \log(n/a)/\log 2. \tag{4}$$

Now at least $k/2$ integers of one of the sequences
$$a_1 < \cdots < a_k \tag{5}$$
$$a_1 - 1 < \cdots < a_k - 1 \tag{6}$$

are even integers. Then, in view of (3) and (4), the method of [3, in particular, Theorem 5 corollary] gives us at least t integers $c_1 ,..., c_t$, where $t \gg \log\log(\log(n/a)/\log 2) \gg \log\log\log(1/\delta_1)$, so that $c_i + c_j$ are among (5) or (6) according as (5) or (6) contains $\geqslant k/2$ even integers. In the first case we choose $b_i = 2^{c_i}$ and $\mu = d$; and in the second $b_i = 2^{c_i}$, $\mu = 2d$. Clearly $b_1 ,..., b_t$ and μ are such that $b_i b_j \mu$ all appear in (2) and hence in $\mathscr{A}$. It is also clear from (1) that $\log\log\log(1/\delta_1)$ tends to ∞ as $\delta \to 0$.

Proof of Theorem 4. We shall choose our sequence $\mathscr{A}$ from the set $\mathscr{S}$ where $\mathscr{S}$ consists of all integers of the form x^2y in $[0, n]$, where y is square free and $x = 1, 2,..., l$. Clearly
$$|\mathscr{S}| \geqslant \left(\frac{6n}{\pi^2} + o(1)\right) \sum_{x=1}^{l} \frac{1}{x^2},$$

and by choosing $l = l(\delta)$ we have
$$|\mathscr{S}| = (1 - \delta_1)n, \tag{7}$$
where
$$\delta_1 \leqslant \delta/2 \tag{8}$$

For a given rational k/m, $(k, m) = 1$, and a given sequence $b_1 < \cdots < b_t$, where
$$t = 3(\log n)^l, \tag{9}$$

we shall estimate the number of sequences $\mathscr{A}$, $|\mathscr{A}| = (1 - \delta)n$, containing $b_i b_j(k/m)$ $(1 \leqslant i < j \leqslant t)$. Let $p_1 ,..., p_j$ be the distinct primes dividing m. Clearly
$$j < \log n.$$

Let $p_i^{\nu_i}$ be the largest power of p_i dividing m. For each $i = 1,..., j$, p_i must divide all the b's, with at most one exception, to the same power, $p_i^{\mu_i}$, say. Let
$$Q = p_i^{\mu_1} \cdots p_j^{\mu_j}.$$

Then, provided we exclude $\leqslant \log n$ of the b's, each b is divisible by Q and not divisible by $p_i^{u_i+1}$ for any $i = 1,..., j$. Thus the number of these b's with no prime factor $> l$ other than $p_1 ,..., p_j$ is at most $(\log n)^l$, since there are $\leqslant (\log n)^l$ integers in $[1, n]$ whose prime factors are all $\leqslant l$. Therefore in view of (9), there exist

$$t_1 \geqslant t/2 \tag{10}$$

integers among the b's, say

$$b_1 ,..., b_{t_1} \tag{11}$$

so that each is divisible by at least one prime $> l$ other than $p_1 ,..., p_j$. Since $b_i b_j(k/m)$ $(1 \leqslant i < j \leqslant t_1)$ belong to $\mathscr{A}$ and hence to $\mathscr{S}$, each $p > l$ other than $p_1 ,..., p_j$ can divide at most one of the integers (11). This enables us to conclude that $b_i b_j$ $(1 \leqslant i < j \leqslant t_1)$ and hence also $b_i b_j(k/m)$, are all distinct. Thus at least $\frac{1}{2}t_1(t_1 - 1)$ numbers of $\mathscr{A}$ are fixed by the sequence $b_1 ,..., b_t$ and the rational k/m. The number of sequences $\mathscr{A}$ containing all $b_i b_j(k/m)$ is then at most

$$E_1 = \binom{(1 - \delta_1)n - \frac{1}{2}t_1(t_1 - 1)}{(1 - \delta)n - \frac{1}{2}t_1(t_1 - 1)},$$

on recalling (7). The number of k/m is at most n^3 and the number of sequences $b_1 ,..., b_t$ is $\binom{n}{t}$. Without any restriction there are

$$E_2 = \binom{(1 - \delta_1)n}{(1 - \delta)n}$$

choices for $\mathscr{A}$. We need therefore only show

$$E_2 > n^2 \binom{n}{t} E_1 . \tag{12}$$

We have

$$E_2/E_1 \gg e^{\frac{1}{2}t_1^2 \log((1-\delta_1)/(1-\delta_2))} > e^{\frac{1}{8}t^2 \log((1-\delta_1)/(1-\delta))}$$

in view of (10), whereas

$$n^2 \binom{n}{t} \leqslant n^t n^3 \leqslant e^{t \log n + 3 \log n}.$$

Since $t \geqslant (\log n)^l$, $\frac{1}{8}t^2 \log((1 - \delta_1)/(1 - \delta))$ is much larger than $t \log n + 3 \log n$. This proves (12) and completes the proof of the theorem.

Proof of Theorem 5. Let g be a primitive root mod p so that for each $i = 1, \ldots, t$

$$a_i \equiv g^{\alpha_i} \pmod{p}, \qquad \alpha_i \leqslant p - 1.$$

We obtain a set of t exponents

$$\alpha_1, \ldots, \alpha_t. \tag{13}$$

Now the method of [3, Theorem 5 corollary] gives $s \gg \log\log p$ integers

$$\beta_1, \ldots, \beta_s$$

so that $\beta_i + \beta_j$ all appear in (13). Let b_i be defined by

$$b_i \equiv g^{\beta_i} \pmod{p}.$$

Then $b_i b_j$ are all in the a's mod p as asserted.

The proofs of Theorems 6 and 7 are effected by similar straightforward adaption of Theorems 7 and 9 of [3].

References

1. P. Erdös, Note on sequences of integers no one of which is divisible by any other, *J. London Math. Soc.* **10** (1935), 42–44.
2. P. Erdös, A generalization of a theorem of Besicovitch, *J. London Math. Soc.* **10** (1935), 126–128.
3. S. L. G. Choi, P. Erdös, and E. Szemeredi, Some additive and multiplicative problems in number theory, *Acta Arith.*, submitted for publication.

Printed by the St Catherine Press Ltd., Tempelhof 37, Bruges, Belgium.