Some additive and multiplicative problems
in number theory

by

S. L. G. Choi (Vancouver, B. C.), P. Erdős and E. Szemerédi (Budapest)

Introduction. In this paper we consider various additive and multiplicative problems concerning sets of integers. The major aim of our investigation is in exhibiting the relationship between the number of elements in a given set of positive integers not exceeding \( n \) and the number of integers that can always be chosen (with or without the restriction that these should lie in the given set) so that their sums (or products), taken two at a time, should all lie in the given set. We shall only once consider the analogous question relating to sums formed with a variable number of summands.

Notation. The letters \( c_1, c_2, \ldots \) denote positive absolute constants, unless otherwise indicated. A sum or product in this paper will mean, unless otherwise indicated, one formed with distinct integers. A sequence will always mean a strictly increasing sequence of positive integers.

1. Let \( A \) denote a set of \( n + t \) integers not exceeding \( 2n \). It is clear that if \( t = 1 \) then in general one cannot choose three integers from \( 1, 2, \ldots, 2n \) whose sums, taken two at a time, all appear in \( A \); for instance we may let \( A \) consist of 2 and all the odd integers not exceeding \( 2n \). It turns out, however (as Theorems 1–4 below show), that corresponding to \( t = 2, c_2, c_2 \log n, c_2 n^{5/2} \) respectively, we can always choose three, four, five, or six integers respectively so that in each case all sums, taken two at a time, will appear in the given sequence \( A \); further, these results are essentially best possible. Theorems 5 and 6 below give us some idea of the rate of growth of the smallest integer \( t_k \) \( (k \geq 3) \) such that for any sequence of \( n + t_k \) integers not exceeding \( 2n \), we can always choose \( k \) integers all whose sums, taken two at a time, appear in the sequence.

Theorem 1. Suppose \( n \geq 4 \) and let \( A \) denote a sequence of \( n + 2 \) positive integers not exceeding \( 2n \). Then there are integers \( b_1, b_2, b_3 \) such that \( b_i + b_j \) \( (1 \leq i < j \leq 3) \) are all in \( A \).
But then by the induction hypothesis there exists a subset of form 
\[ \{x_0, \ldots, +0, x_0\} \]
in the set \( \{y_i^r; i = 1, \ldots, t_i\} \). Since for each \( y_i^r, y_i^r + m = y_i^r \) is also in \( B \), we conclude, by taking \( x_{k+1} = m \), that the set 
\[ \{x_k + \{0, x_0\} \} + \{0, x_0\} \]
is also a subset of \( B \).

As a consequence of Lemma \( A \), we prove the following

**Corollary.** Suppose \( n \geq n_0(k) \) and let \( B \) denote a sequence of \( t \) even integers not exceeding \( 2n \), where \( t \geq 2^{(k-1)(m-1)} \). Then there exist integers \( b_0, \ldots, b_t \) such that all \( b_i + b_j (0 \leq i < j \leq t) \) appear in \( A \).

**Proof.** By the lemma, \( A \) possesses a subset of type 
\[ \{x_0, \ldots, +0, x_0\} \]
We take \( b_0 = \frac{1}{2} x_0, b_1 = \frac{1}{2} x_0 + x_1, \ldots, b_t = \frac{1}{2} x_0 + x_t \). Since \( x_0 \) is an even integer, \( b_0, b_1, \ldots, b_t \) are integers whose sums \( b_i + b_j (0 \leq i < j \leq t) \) are all in \( A \).

**Theorem 2.** There exists a positive integer \( c_1 \) such that if \( n \geq n_0(n) \) and \( A \) denotes a sequence of \( n \) positive integers not exceeding \( 2n \), then there are \( b_1, b_2, b_3, b_4 \) such that all sums \( b_i + b_j (1 \leq i < j \leq 4) \) appear in \( A \).

**Proof.** Let \( c_1 \) be a sufficiently large integer. Let \( t \) denote the number of even integers in \( A \). Then
\[ c_1 \leq t \leq 10^{-2} n \]
the latter inequality holding in view of the corollary to Lemma \( A \), if \( n \) is chosen large enough. By the same corollary, provided \( c_1 \) is chosen large enough, we may assert that there exists an even integer \( 2m \) in \([20t, 2n - 20t]\). Let \( b_1, b_2 \) be even integers defined by
\[ b_1 + b_2 = 2m, \]
\[ b_1 - b_2 = \frac{1}{4} \] if \( m \) is even.

If \( a \) is any integer in \([m - 10t, m + 10t]\) then certainly
\[ 0 < a + b_1 \leq 2m, \]
\[ 0 < a + b_2 \leq 2m. \]

Now there are \( 5t \) pairs of odd integers \( x, y \) in \([m - 10t, m + 10t]\) such that \( x + y = 2m \). For each \( i = 1, 2 \), there are at most \( t \) odd integers \( a \) in \([m - 10t, m + 10t]\) such that \( b_1 + a \) is not an integer in \( A \). Thus there exist at least \( 3t \) pairs of odd integers \( x, y \in \{m - 10t, m + 10t\} \) with \( x + y = 2m \) and such that \( b_1 + x, b_2 + x, b_1 + y, b_2 + y \) are all in \( A \). Let \( b_1, b_2 \) be one such pair.
Then \(b_1, b_2, b_3, b_4\) are integers such that all the sums \(b_i + b_j\) \((1 \leq i < j \leq 4)\) are in \(A\).

**Theorem 3.** There exists an absolute constant \(c_2 > 0\) such that if \(n \geq n_0(c_2)\) and \(A\) is a sequence of \(n + m\) positive integers not exceeding \(2n\), where \(m \geq c_2 \log n\), then there are integers \(b_1, b_2, b_3, b_4\) such that \(b_i + b_j\) \((1 \leq i < j \leq 5)\) are all in \(A\). Further, the result no longer holds if \(c_2\) is replaced by \(c'_2\), where \(c'_2\) is sufficiently small.

**Proof.** Let \(t\) denote the number of even integers in \(A\). Then, provided \(n\) is sufficiently large, we may assume

\[
c_2 \log n \leq t \leq 10^{-2} n,
\]

the right-hand side inequality holding since otherwise an application of the corollary to Lemma A (with \(k = 4\)) gives the theorem. In view of the corollary again, provided \(c_2 > 0\) is sufficiently large, and \(n \geq n_0(c_2)\), there are at least \(2 \log_{32} n\) even integers from our sequence \(A\) falling into the interval \([40t, 2n - 40t]\). Therefore there exists a subinterval \([n_1, 2n_1]\) containing three even integers \(a^*_1 < a^*_2 < a^*_3\) from \(A\). Let the integers \(b_1 < b_2 < b_3\) be determined by

\[
\begin{align*}
    b_1 + b_2 &= a^*_1, \\
    b_2 + b_3 &= a^*_2, \\
    b_3 + b_4 &= a^*_3.
\end{align*}
\]

We thus obtain

\[
\begin{align*}
    b_1 &= \frac{1}{2}(a^*_1 + a^*_2 - a^*_3), \\
    b_2 &= \frac{1}{2}(a^*_2 - a^*_1 + a^*_3), \\
    b_3 &= \frac{1}{2}(a^*_3 - a^*_1 - a^*_2).
\end{align*}
\]

It is clear that \(b_1, b_2, b_3\) are either all odd or all even. Suppose they are all odd (the case when \(b_1, b_2, b_3\) are all even can be treated similarly). There are \(10t^2\) pairs of even integers \(b_i < b_j\) in \([[(a^*_1/2) - 20t, (a^*_2/2) + 20t]\) such that \(b_i + b_j = a^*_1\). We note that for any \(a\) in \([[(a^*_1/2) - 20t, (a^*_2/2) + 20t]\), \(a + b_i < 2n\) \((i = 1, 2, 3)\). We choose a pair \(b_i < b_j\) such that \(b_i + b_j = a^*_1\). Solving for \(b_i, b_j, b_1, b_2, b_3, b_4\), are all in \(A\). This is possible since for each \(i = 1, 2, 3\) there are at most \(t\) even integers \(a\) in \([[(a^*_1/2) - 20t, (a^*_2/2) + 20t]\) such that \(b_i + a = a^*_1\) is not in \(A\). This proves the main part of the theorem.

Finally, if \(A\) consists of all the odd integers and the integers \(2, 2^2, 2^3, \ldots, \) in \([1, 2n]\) then one cannot choose \(b_1, \ldots, b_4\) such that \(b_i + b_j\) \((1 \leq i < j \leq 5)\) are all in \(A\). This completes the proof of Theorem 3.

**Theorem 4.** There exists \(c_3 > 0\) such that if \(n \geq n_0(c_3)\) and \(A\) is a sequence of \(n + m\) positive integers not exceeding \(2n\), where \(m \geq c_3 n^{1/3}\), then one can find six integers \(b_1, \ldots, b_6\) whose sums \(b_i + b_j\) \((1 \leq i < j \leq 6)\) are all in \(A\). Further, the results becomes false if \(c_3\) is replaced by a sufficiently small constant \(c'_3\).

**Proof.** Let \(t\) denote the number of even integers in \(A\). Then we can assume, in view of the corollary to Lemma A, that

\[
c_3 n^{1/3} \leq t \leq 10^{-2} n,
\]

and that there are at least \(4t \geq 12n^{1/3}\) even integers of \(A\) falling into the interval \([40t, 2n - 40t]\). Thus, if \(c_3\) is sufficiently large, there exists a subinterval \([n_1, 2n_1]\) containing at least \(3n^{1/3}\) even integers of \(A\). Since the sum of any two integers in \([n_1, 2n_1]\) lies between \(2n_1\) and \(4n_1\), there exist even integers \(a_1, a_2, a_3, a_4, a_5, a_6\) of \(A\) such that

\[
a_1 + a_2 = a_3 + a_4 = a_5 + a_6
\]

and

\[
n_1 < a_2 < a_3 < a_4 < a_5 < a_6 < 2n_1.
\]

We determine integers \(b_1, b_2, b_3, b_4\) such that

\[
b_1 + b_2 = a_1, \quad b_3 + b_4 = a_3, \quad b_1 + b_3 = a_5, \quad b_2 + b_4 = a_6
\]

and thus also

\[
b_1 + b_3 = a_2, \quad b_2 + b_4 = a_4.
\]

It is clear that \(b_1 < b_3 < b_4 < b_5\) and that they are all odd or all even. Solving for \(b_1, b_2, b_3, b_4\) gives

\[
\begin{align*}
    b_1 &= \frac{1}{2}(a_2 - a_1), \\
    b_2 &= \frac{1}{2}(2a_1 - a_2 + a_3), \\
    b_3 &= \frac{1}{2}(a_5 - a_4 - a_2), \\
    b_4 &= \frac{1}{2}(a_5 - a_4 + a_2).
\end{align*}
\]

Since clearly \(b_1 > 0\) we have \(b_2 > 0, b_3 > 0, b_4 > 0\) as well.

If \(b_1, \ldots, b_6\) are all odd (even) then we determine even (odd) integers \(b_5, b_6\) in \([\frac{1}{2}a_5 - 20t, \frac{1}{2}a_6 + 20t]\) such that

\[
b_5 + b_6 = a_5
\]

and such that \(b_5 + b_i\) \((i = 1, 2, 3, 4)\) and \(b_5 + b_i\) \((i = 1, 2, 3, 4)\) are all in \(A\). This is possible since for each \(i = 1, 2, 3, 4\) there exist at most \(t\) even.
(odd) integers \(a\) in \([1^k, 2n, 3n, 4n, 5n]\) such that \(b + c\) does not belong to \(A\), but there are initially 10r possible choices for \(b, c\), each such that \(b + c = n\).

To prove the last part of the theorem we let \(A\) consist of all the odd integers \(\leq 2n\) and \(c\) \(n^{1/2}\) even integers \(= 2n\) so that the sums taken two at a time of these even integers are distinct. Suppose in fact there exist \(b_1, \ldots, b_6\) such that \(b + c\) \(= 1 \leq i < j \leq 6\) are all in \(A\). We shall deduce a contradiction. Clearly at most two of the integers \(b, c\) can be even otherwise we have a sum \(= 0\). Thus there are four odd \(b, c\), say \(b_1, b_2, b_3, b_4\). The sums \(b + b_2, b + b_3, b + b_4, b_2 + b_3, b_2 + b_4, b_3 + b_4\) are in \(A\). But then

\[(b_1 + b_2) + (b_3 + b_4) = (b_5 + b_6) + (b_2 + b_3),\]

violating our choice of the even numbers in \(A\).

We summarize the results contained in Theorems 1–4 as follows. We first recall the definition of \(t_b\) in the opening paragraph of this section. For large \(n\), Theorems 1–4 reveal that the order of magnitude of \(t_b (n = 3, 4, 5, 6)\) is known. More precisely

\[t_b = 2, \quad 2 < t_b \leq c_1, \quad c_1 n^{1/2} \leq t_b \leq c_2 n^{1/2},\]

where \(c_1, c_2, c_3, c_4, c_5, c_6\) are positive absolute constants. It might be of interest to determine these constants precisely. For \(b \geq 7\), the order of magnitude of \(t_b\) is not known, but Theorems 5 and 6 below give some indication of the possible rate of growth of \(t_b\). We mention that a slightly more precise form of Theorem 5 below is possible, but as there is no indication that Theorem 5 is anywhere near possible we shall not aim at precision here.

**Theorem 5.** Let \(k\) be a positive integer and \(n \geq n_0(k)\), and suppose \(A\) is a sequence of \(n + t\) positive integers not exceeding \(2n\), where \(t \geq 2k n^{1/2} - 20\). Then there exist integers \(b_1, \ldots, b_k\) all whose sums \(b_i + b_j \geq 0 \leq i < j \leq k\) are in \(A\).

**Proof.** Since there are at least \(t^2 n^{1/2} - 20\) even integers in \(A\), the theorem follows from the corollary of Lemma \(A\).

**Corollary.** If \(A\) is a sequence of \(n + t\) positive integers not exceeding \(2n\), where \(t \geq 8n\), and \(n \geq n_0(k)\), then we can find integers \(b_1, \ldots, b_k\) where \(k \leq \log\log n\), with the implied constant depending on \(k\), such that all sums \(b_i + b_j \geq 0 \leq i < j \leq k\) are in \(A\).

**Proof.** By Theorem 5 we can always choose \(b_1, \ldots, b_k\) if

\[n^{-k/2} k^k \leq \delta\]

which is valid if \(k \leq \log\log n\).

Before stating our next theorem, we prove a result concerning the frequency of occurrence of sequences with few distinct sums (taken two at a time).

**Lemma B.** Suppose \(a_1\) is given. Then there exist \(k_1, k_2\) depending only on \(a_1\) such that, if \(n \geq n_1(k_1, a_1)\), the number of choices of sequences \(A\)

\[a_1 < \ldots < a_k \leq n\]

each with \(\leq a_1 k\) distinct sums (taken two at a time), does not exceed \(n^{1/2}\).

We deduce the lemma from the following theorem of Freiman (see [2], p. 134) reworded to suit our present purposes.

**Theorem A.** Suppose the sequence \(A\)

\[a_1 < \ldots < a_k\]

is such that there are at most \(ck\) distinct sums \(a_i + a_j \leq i < j \leq k\), then there exist \(k^*\), \(c^*\) depending only on \(a_1\) and an integer \(m \leq \log\log n\), such that, if \(k \geq k^*\), there are arithmetic progressions \(b_0, b_1, \ldots, b_m\) each of length \(k^*\) \(a_1\) such that \(A\) is contained in the set \(S_m\), where the sets \(S_i = \{i, 0, 1, \ldots, m\}\) are defined inductively by

\[S_0 = B_0,\]

\[S_i = \bigcup_{b \in S_{i-1}} (S_{i-1} + b), \quad i \geq 1.\]

**Proof of Lemma B.** We apply Theorem A with \(c = a_1\). Then we have \(k_1 = k^*\) such that if \(k \geq k_1\), the sequence \(A\) is contained in \(S_m\), with \(S_m\) defined by (2). The number of choices for \(B_i (i = 0, 1, \ldots, m)\) is at most \(n^{1/2}\). Thus the total number of choices for \(S_m\) is \(\leq n^{1/2}\).

The number of choices of \(A\) corresponding to each choice of \(S_m\) is \(\leq (c^* k)^{1/2}\). Therefore, the total number of choices of \(A\) is

\[\leq n^{1/2} (c^* k)^{1/2} \leq n^{1/2}\]

where \(a_1\) depends only on \(a_1\) if we choose \(n \geq n_1(k, a_1)\).

**Theorem 6.** Suppose \(0 < \varepsilon < 1\) is given. Then there exist \(k_0(\varepsilon, c)\) and \(n_0(\varepsilon, c)\) such that if \(n \geq n_0(\varepsilon, c)\), there exists a sequence \(A\) of \(n + t\) positive integers consisting of all the odd integers \(\leq 2n\) and \(t\) positive even integers \(\leq 2n\), where \(t = [n^{1/2}]\), such that there are at most \(k_0(\varepsilon, c)\) \(1\) integers

\[b_1, \ldots, b_{k_0(\varepsilon, c)-1}\]

all whose sums \(b_i + b_j \leq i < j \leq k_0(\varepsilon, c)-1\) are in \(A\).

**Proof.** Let \(a = [2n] + 1\). We apply Lemma B with \(a_1 = a\). Let \(k_0 = 2a_0(k_0, \varepsilon), \\text{where}\ k_0\ \text{and} \ a_0\ \text{are the numbers in Lemma B corresponding to} \ a_1 = a^2\). Finally let \(n_0 = n_0(k_0, a_1)\) be the choice of \(n_1\) in Lemma B.
corresponding to \( k = k_0 \). We shall establish the theorem with these choices of \( k_0 \) and \( n_0 \). Accordingly let \( n \geq n_0 \), and we proceed to establish the existence of a sequence \( A \) with the desired property.

We determine first the number of choices of sequences \( B \)

\[
b_1 < \ldots < b_{k_0} < n
\]

so that the number of distinct even sums \( b_1 + b_j \) is \( \leq k_0 \). We let \( B^*, B^{**} \) denote the subsequences of \( B \) consisting of respectively the odd and even integers of \( B \). Further we denote by \( T(B^*), T(B^{**}) \) the number of distinct sums (taken two at a time) formed from the integers of \( B^* \) and \( B^{**} \) respectively. We have

\[
T(B^*) < ak_0,
T(B^{**}) < ak_0.
\]

We consider two cases according as both \( B^*, B^{**} \) have each \( \geq a^{-1}k_0 > k_1 \) integers or otherwise. Take the first case and let \( M_1 \) denote the number of choices of \( B \) in this case. Then

\[
T(B^*) < a^2|B^*| = a_1|B^*|
\]

and similarly

\[
T(B^{**}) < a_1|B^{**}|.
\]

Since \( |B^*| > k_1 \) and \( |B^{**}| > k_1 \) we may apply Lemma B to \( B^* \) and \( B^{**} \) to conclude that

\[
M_1 \leq n^{2k_0}.
\]

We next consider the second case. Let \( M_2 \) denote the number of choices of \( B \) in this case. One of the sets \( B^*, B^{**} \) has \( \leq a_1^{-1}k_0 \) integers and thus the number of choices for this set is \( \leq n^{2k_0} \). The number of choices for the other set is \( \leq n^{2k_0} \), by an application of Lemma B. Thus

\[
M_2 \leq 2n^{2k_0}k_0^{1/a}.
\]

Thus the number of choices of \( B \) each with \( \leq ak_0 \) distinct even sums is

\[
M_1 + M_2 \leq n^{2k_0} + 2n^{k_0}k_0^{1/a} \leq 2n^{k_0}k_0^{1/a}.
\]

since \( k_0 = 2a_1ak_1 \).

Each such sequence \( B \) determines at least \( k_0 - 3 \) even sums, so corresponding to a given \( B \), there exist \( \binom{n - k_0 - 3}{t - k_0 + 3} \) choices of \( A \) containing these sums. Let \( N_3 \) denote the number of choices of \( A \) corresponding to these \( B \). Then

\[
N_3 \leq \binom{n - k_0 - 3}{t - k_0 + 3} n^{k_0}.
\]

We now consider sequences \( B \) having each at least \( ak_0 \) distinct even sums. Each such sequence determines at least \( ak_0 \) distinct even sums and thus the number of choices of \( A \) containing these even sums is at most \( \binom{n}{t - ak_0} \). As there are \( \leq \frac{n}{k_0} \) choices for such \( B \), the number \( N_2 \) of choices of \( A \) corresponding to all such \( B \) satisfies

\[
N_2 \leq \binom{n}{t - ak_0} \frac{n}{k_0}.
\]

Since the total number of possible choices of \( A \) is \( \binom{n}{t} \) we have our theorem if we can prove

\[
\binom{n}{t} > N_1 + N_2.
\]

We shall establish this by showing that

\[
N_1 < \frac{1}{3} \binom{n}{t}, \quad N_2 < \frac{1}{3} \binom{n}{t}.
\]

We have

\[
\binom{n}{t} \left( \frac{n - k_0 + 3}{t - k_0 + 3} \right) \geq n^{k_0 + o(1)} \geq 2n^{\frac{k_0 - 1}{3}}
\]

on recalling \( a = [2/3] + 1 \) and \( t = [n - k_0] \). The above inequality implies \( N_1 < \frac{1}{3} \binom{n}{t} \) in view of (3).

Next

\[
\binom{n}{t} \left( \frac{n - ak_0}{t - [ak_0]} \right) \geq n^{ak_0 + o(1)} \geq 2 \binom{n}{k_0}
\]

on using \( a = [2/3] + 1 \) and \( t = [n - k_0] \). We have \( N_2 < \frac{1}{3} \binom{n}{t} \) in view of (4).

This completes the proof of Theorem 6.

2. In this section we consider the question of estimating the number of integers that can be chosen from a given sequence so that all sums, taken two at a time, should appear in the sequence. We shall prove three theorems (Theorem 7, 8, and 9) of which the last depends on the following theorem which has just been established by Szemerédi.

THEOREM B. For any given integer \( k \geq 2 \) let \( r_k(n) \) denote the largest number of integers that can be chosen from \( 1, 2, \ldots, n \) with no \( k \) terms in arithmetic progression. Then \( n^{-1}r_k(n) \to 0 \) as \( n \to \infty \).

We further remark that Theorem 7 would also follow from Szemerédi's result though we give a proof which uses only a theorem of Varnavides.
Theorem 7. For any given \( s > 0 \) and any integer \( k > 1 \), there exists \( n_0(s, k) \) so that if \( n \geq n_0(s, k) \) and \( A \) is a sequence of \( t \) integers not exceeding \( n \), where \( t \geq \left( \frac{3}{4} + s \right) n \), then we can find \( k \) integers

\[ a_1, a_2, \ldots, a_k \]

in \( A \), whose sums \( a_i + a_j \) (\( 1 \leq i < j \leq k \)) are all in \( A \).

Proof. Since \( t \geq \left( \frac{3}{4} + s \right) n \) there exist \( s \) integers, where \( s \geq n_0(s, n) \), in the sequence \( A \), say \( a_1, a_2, \ldots, a_k \), such that \( 2a_1, 2a_2, \ldots, 2a_k \) are also in \( A \). By a theorem of Van der Waerden (see [4]) there are \( c_k n^k \) triples \( a_i, a_j, a_k \) which form an arithmetic progression. Thus there is an integer, say \( a_1 \), for which there are \( \geq c_k n \) integers \( a_j \)'s so that

\[ \frac{3}{4}(a_1 + a_j) = a_1; \]

but then \( a_1 + a_j = 2a_1 \) is also in \( A \). Now repeat the same argument with these \( c_k n a_j \)'s, and so on. In this way one can find integers \( a_1, a_2, \ldots, a_k \) in \( A \) such that \( a_{i+1} + a_i \) (\( 1 \leq i \leq k-1 \) and \( k \) are all in \( A \).

The following theorem is a refinement of Theorem 7.

Theorem 8. Suppose \( k \) is given. Then there exists \( n_k > 0 \) such that if \( n \geq n_k(s, k) \) and \( A \) is a sequence of \( t \) integers not exceeding \( n \), where \( t \geq \left( \frac{3}{4} - \frac{1}{2} \right) n \), then one can find \( k \) integers in \( A \):

\[ a_1, a_2, \ldots, a_k \]

whose sums \( a_i + a_j \) (\( 1 \leq i < j \leq k \)) are all in \( A \).

Proof. Let \( s_k > 0 \) be a sufficiently small number. In view of Theorem 7, we may assume there are at most \( 2 n^2 \) integers \( a \) in \( A \) such that \( 2a \) is also in \( A \). Thus there exists a subset \( B \) of \( A \) with at least \( \left( \frac{3}{4} - 2 s_k \right) n \) integers and with the property that whenever a belongs to \( B \) then \( 2a \) does not belong to \( B \). This property is crucial in our proof and we refer to it as property P.

For \( j = 1, \ldots, k \), let

\[ I_j = (n 2^{-j}, n 2^{-j+2}) \]

\[ I_j^* = (n 2^{-j-1}, n 2^{-j}) \]

\[ B_j = B \cap I_j \]

\[ B_j^* = B \cap I_j^* \]

As property P implies that

\[ |B_j| + |B_j^*| \leq 2^{j-1} n \]

\( (j = 1, 2, \ldots, k) \)

and as

\[ |B| > \left( \frac{3}{4} - 2 s_k \right) n \]

we conclude that

\[ |B_j| + |B_j^*| \geq \left( 2^{j-1} - 2 s_k \right) n \]

\( (5) \)

Further, by repeated application of property P and using (5), we may assert that for each \( j = \frac{k}{2}, \frac{k}{2} - 1, \ldots, 1 \) and \( i = 0, 1, \ldots, k-j \), \( B_j \) contains all at most \( 2 \left( \frac{k}{2} + 1 \right) 2^{n-j} n \) integers of type \( a_i \) (where \( s \) is odd) in \( I_j \). By now choosing \( s_k \) small enough, we can find an integer \( b_j \) of type \( a_i \) in \( B_j \), an integer \( b_j \) of type \( a_i \) in \( B_j \), and an integer \( b_j \) of type \( 2^{-j} n \) in \( B_j \), where \( a_1, \ldots, a_k \) are all odd, such that \( b_i + b_j \) (\( 1 \leq i < j \leq k \)) are all in \( B \) and thus also in \( A \). This completes the proof.

Theorem 9. For any integer \( r > 0 \), and any integer \( k \), there exists \( n_0(\delta, r, k) \) such that if \( n \geq n_0(\delta, r, k) \) and \( A \) is a sequence of \( t \) positive integers not exceeding \( n \), where \( t \geq (1 - \delta) n \), then there exists a subsequence

\[ a_1 < \ldots < a_k \]

such that all sums of the form

\[ \sum_{j=1}^{k} e_j a_j \]

\( (e_j = 0, 1; 1 \leq \sum_{j=1}^{k} e_j \leq r) \)

are in \( A \).

Proof. We choose \( \delta = \frac{1}{(2r)^2} \) and suppose \( n \geq n_0(\delta, r, k) \). Then there exist \( n \geq n_0(\delta, r, k) \), a subsequence of \( A \):

\[ a_1 < \ldots < a_k \]

in \([r-1]^{-2} n, r^{-1} n]\) such that \( 2a_1, 3a_1, \ldots, ra_j \) for \( j = 1, 2, \ldots, s \) are all in \( A \). By Theorem B, we can find an arithmetic progression

\[ a, a+b, \ldots, a+2^{(k-1)b} \]

within \( a_1, \ldots, a_k \). Now we take

\[ b_1 = a, \quad b_2 = a+r! b, \quad \ldots, \quad b_s = a+r! (k-1) b \]

Clearly \( \sum_{j=1}^{s} b_j \), subject to \( 1 \leq \sum_{j=1}^{s} b_j \leq r \), are all in \( A \). This completes the proof of the theorem.

3. In this section we consider some aspects of the multiplicative analogue of the additive problems in § 1 and 2. Theorems 10–12 below represent the type of results that can be established by probabilistic arguments.

Theorem 10. Suppose \( n \) is any positive integer and \( n \geq n_0(\varepsilon) \). Then there exists a sequence \( A \) of \( \delta \) positive integers not exceeding \( n \), where \( k \geq n \left( 1 - \frac{\varepsilon}{\log n \log \log n} \right) \) such that for any \( s \), where \( s \) is an integer or the reciprocal of one, there exist at most \( t \leq s \varepsilon \log \log \log \log n \) integers

\[ b_1 < \ldots < b_t \]

where \( c_0 \) depends only on \( c_0 \), such that all products \( s^{-1} b_i b_j \) (\( 1 \leq i < j \leq t \)) are in \( A \).
The following lemma, whose proof is somewhat involved (see [4]) enables us to strengthen Theorem 10.

Lemma C. Suppose \( b \) is an integer, and \( t \geq (\log n)^k \), where \( \log n \) denotes the logarithmic function to the base 2. Then for any sequence

\[
a_1 < \cdots < a_t \leq n
\]

of \( t \) positive integers, there are at least \( ct^t \) distinct products \( a_i a_j \) \((1 \leq i < j \leq t)\) where \( c \) is a positive absolute constant.

Using the above lemma we obtain the following.

Theorem 11. Suppose \( 0 < a < 1 \), and \( n \geq \mathcal{N}_a(a) \). Then there exists a sequence of \( \delta \) positive integers not exceeding \( n \), where \( \delta \geq a \), such that for any \( s \), where \( s \) is an integer or the reciprocal of one, there exist at most \( \left[ \frac{\delta}{[\log n]} \frac{[\log n]}{[\log n]} \right] = \left[ \frac{\log n}{\log \log n} \right] \) integers

\[
b_1 < \cdots < b_t,
\]

where \( c_0 \) depends only on \( a \), such that all products \( s^{-1} b_i b_j \) \((1 \leq i < j \leq t)\) are in \( A \).

Proof. Arguing as in proof of Theorem 10 and using Lemma C instead of \( d(t) < 2^{(1+\epsilon)/\log \log t} \), we need only prove that

\[
\left( \frac{n}{\mathcal{N}_a} \right) \left( \frac{\mathcal{N}_a}{\mathcal{N}_a} \right) \geq \left( \frac{n}{\mathcal{N}_a} \right)^t.
\]

We note that the left hand side is \( \geq e^{\log n^{-\log \log n} t} \) which is greater than \( n^t \left( \frac{n}{\mathcal{N}_a} \right) \), if \( \mathcal{N}_a \) and hence also \( c_0 \) is large enough in terms of \( a \).

It seems quite plausible that the following conjecture is true:

Suppose \( a_1 < \cdots < a_t \leq n \), \( t \geq (\log n)^k \). Then there are \((1+\epsilon)^t\) distinct products \( a_i a_j \) \((1 \leq i < j \leq t)\), where \( \epsilon \) is some positive absolute constant.

The above conjecture, if true, would imply the following.

Theorem 12. Suppose \( 0 < a < 1 \) and \( n \geq \mathcal{N}_a(a) \). Then there exists a sequence \( A \) of \( \delta \) positive integers not exceeding \( n \), where \( \delta \geq a \), such that for any \( s \), where \( s \) is an integer or the reciprocal of one, there exist at most \( \frac{\delta}{[\log n]} \) integers

\[
b_1 < \cdots < b_t,
\]

where \( c_0 \) depends only on \( a \), such that \( b_i b_j s^{-1} \) \((1 \leq i < j \leq t)\) are all in \( A \).

The proof, which we omit, is an adaptation of the probabilistic argument used in the proof of Theorem 10. The theorems in this paragraph can undoubtedly be sharpened considerably. We hope to return to these questions at another occasion.
Brun's method and the Fundamental Lemma, II*

by

H. HALBERSTAM (Nottingham) and H.-E. RICHERT (Ulm)

To the memory of Yu. V. Linnik

1. Introduction. Let \( \mathfrak{A} \) be a finite sequence of (not necessarily distinct nor necessarily positive) integers, and let \( \mathfrak{P} \) be a set of primes. Let \( \mathfrak{B} \) denote the complement of \( \mathfrak{P} \) with respect to the set \( \mathfrak{B} \) of all primes, and let \((d, \mathfrak{B}) = 1\) signify that \(d\) has no prime factors in \(\mathfrak{B}\). For any real numbers \(w \) and \(z \) satisfying \(2 \leq w \leq z\) define

\[
P(w) := \prod_{\substack{p < z \\ p \not\in \mathfrak{B}}} p, \quad P_{w,z} = P(w)/P(w)
\]

and

\[
S(\mathfrak{A}; \mathfrak{B}, w) := \# \{a : a \in \mathfrak{A}, (a, P(w)) = 1\},
\]

where \(\# \{\ldots\}\) denotes the cardinality of the set \(\{\ldots\}\).

Let \(\omega(d)\) be a non-negative multiplicative arithmetic function on the sequence of square-free integers \(d\) which satisfies the following conditions:

\[
\omega(p) = 0 \quad \text{if} \quad p \not\in \mathfrak{B};
\]

there exists a constant \(A_1 \geq 1\) such that

\[
(\Omega_1) \quad \frac{\omega(p)}{p} \leq 1 - \frac{1}{A_1};
\]

there exist constants \(\kappa > 0\) and \(A_2 \geq 1\) such that

\[
(\Omega_2(\kappa)) \quad \sum_{\substack{\omega(p) \leq w \leq z \\ p \leq c}} \frac{\omega(p)}{p} \log p \leq \kappa \log \frac{z}{w} + A_2, \quad 2 \leq w \leq z.
\]

* This paper is a sequel to [1]. A brief announcement of its results was contained in [3].