On additive and multiplicative decompositions of sets of integers composed from a given set of primes, II
(Multiplicative decompositions)

by

K. GYŐRY (Debrecen), L. HAJDU (Debrecen and Budapest) and
A. SÁRKÖZY (Budapest)

Dedicated to the memory of Andrzej Schinzel

1. Introduction. First we recall the notation and definitions from part I [9] that we will also use here.

\( A, B, C, \ldots \) denote (finite or infinite) sets of non-negative integers, and their counting functions are denoted by \( A(X), B(X), C(X), \ldots \), so that e.g.

\[ A(x) = |\{a : a \in A, a \leq x\}|. \]

The set of positive integers is denoted by \( \mathbb{N} \), and we write \( \mathbb{N} \cup \{0\} = \mathbb{N}_0 \).

The sets of rational numbers and of positive real numbers are denoted by \( \mathbb{Q} \) and \( \mathbb{R} \), respectively. The set of (positive) primes is denoted by \( \mathbb{P} \), and throughout this paper the word “prime” means positive prime.

We will need the following definitions:

**Definition 1.1.** Let \( \mathcal{G} \) be an additive semigroup and \( A, B, C \) subsets of \( \mathcal{G} \) with

\[ |B|, |C| \geq 2. \]  

(1.1)

If

\[ A = B + C \quad (= \{b + c : b \in B, c \in C\}), \]

then (1.2) is called an additive decomposition or briefly a-decomposition of \( A \), while if a multiplication is defined in \( \mathcal{G} \) and (1.1) and

\[ A = B \cdot C \quad (= \{bc : b \in B, c \in C\}) \]

(1.3)

2020 Mathematics Subject Classification: Primary 11N99; Secondary 11P70, 11P99.

Key words and phrases: multiplicative decompositions, shifted product of sets of integers, restricted prime factors, unit equations.

Received 5 August 2022; revised 16 April 2023.

Published online 19 July 2023.

DOI: 10.4064/aa220805-13-6
hold, then (1.3) is called a multiplicative decomposition or briefly m-decomposition of \( A \). Moreover, if \( A \) is infinite, and \( B \) or \( C \) in (1.2) or (1.3) is finite, then the decomposition is called a finite decomposition or briefly \( F \)-decomposition, and we say that (1.2) and (1.3) are an \( a \)-F-decomposition and \( m \)-F-decomposition, respectively.

**Definition 1.2.** A finite or infinite set \( A \) of non-negative integers is said to be \( a \)-reducible if it has an additive decomposition
\[
A = B + C \quad \text{with} \quad |B|, |C| \geq 2
\]
(where \( B, C \subset \mathbb{N}_0 \)). If there are no sets \( B, C \), then \( A \) is said to be \( a \)-primitive. Moreover, an infinite set \( A \subset \mathbb{N}_0 \) is said to be \( a \)-F-reducible if it has a finite additive decomposition of the form (1.4), while if it has no such finite decomposition, it is said to be \( a \)-F-primitive.

**Definition 1.3.** Two sets \( A, B \) of non-negative integers are said to be asymptotically equal if there is a number \( K \) such that \( A \cap [K, +\infty) = B \cap [K, +\infty) \), and then we write \( A \sim B \).

**Definition 1.4.** An infinite set \( A \) of non-negative integers is said to be totally \( a \)-primitive if every \( A' \) with \( A' \subset \mathbb{N}_0, A' \sim A \) is \( a \)-primitive, and it is called totally \( a \)-F-primitive if every \( A' \) with \( A' \subset \mathbb{N}_0, A' \sim A \) is \( a \)-F-primitive.

The multiplicative analogs of Definitions 1.2 and 1.4 are:

**Definition 1.5.** If \( A \) is an infinite set of positive integers, then it is said to be \( m \)-reducible if it has a multiplicative decomposition
\[
A = B \cdot C \quad \text{with} \quad |B|, |C| \geq 2
\]
(where \( B, C \subset \mathbb{N} \)). If there are no such \( B, C \), then \( A \) is said to be \( m \)-primitive. Moreover, an infinite set \( A \subset \mathbb{N} \) is said to be \( m \)-F-reducible if it has a finite decomposition of the form (1.5), while if it has no such finite \( m \)-decomposition, then it is said to be \( m \)-F-primitive.

(We remark that if \( A \subset \mathbb{N}_0 \) and \( 0 \in A \), then \( A \) has a trivial \( m \)-decomposition of the form (1.5) with \( B = A \) and \( C = \{0, 1\} \). To avoid such trivial decompositions, in the last definition it is better to restrict ourselves to sets \( A \) of positive integers.)

**Definition 1.6.** An infinite set \( A \subset \mathbb{N} \) is said to be totally \( m \)-primitive if every \( A' \subset \mathbb{N} \) with \( A' \sim A \) is \( m \)-primitive, and it is called totally \( m \)-F-primitive if every \( A' \subset \mathbb{N} \) with \( A' \sim A \) is \( m \)-F-primitive.

**2. The problem, and the theorems to prove.** In part I we proved the following theorems:
Theorem A. If $\mathcal{P} = \{p_1, p_2, \ldots\} \subset \mathbb{P}$ (with $p_1 < p_2 < \cdots$) is a non-empty (finite or infinite) set of primes such that there exists a number $x_0$ with
\begin{equation}
P(x) < \frac{1}{51} \log \log x \quad \text{for } x > x_0
\end{equation}
(where $P(x) = |\mathcal{P} \cap [1, x]|$), then the set
\begin{equation}
\mathcal{R}(\mathcal{P}) = \{n \in \mathbb{N} : p \mid n \Rightarrow p \in \mathcal{P}\}
\end{equation}
is totally $a$-primitive.

Theorem B. Let $\mathcal{P} \subset \mathbb{P}$ be of the form
\begin{equation}
\mathcal{P} = \mathbb{P} \setminus \mathcal{Q} \quad \text{where } \mathcal{Q} \subset \mathbb{P}
\end{equation}
with a finite set $\mathcal{Q}$, and let $t \in \mathbb{N}_0$, $t \geq 2$, or $t = \infty$. Then the set $\mathcal{R}(\mathcal{P})$ defined by (2.2) has an $a$-$F$-decomposition
\begin{equation}
\mathcal{R}(\mathcal{P}) = A + B
\end{equation}
such that $|A| = \infty$ and $|B| = t$.

Theorem C. For every non-decreasing function $f : \mathbb{N} \rightarrow \mathbb{R}$ with $\lim_{n \rightarrow \infty} f(n) = \infty$ there is an infinite set $\mathcal{Q} \subset \mathbb{P}$ satisfying $Q(n) < f(n)$ for all $n \in \mathbb{N}$, such that the set $\mathcal{P}$ defined by (2.3) is infinite and $\mathcal{R}(\mathcal{P})$ is totally $a$-$F$-primitive.

In this paper our goal is to prove the multiplicative analogs of these three theorems. Before formulating the multiplicative analog of Theorem A, observe that if $\mathcal{P} = \{p_1, p_2, \ldots\} \subset \mathbb{P}$ and $\mathcal{R} = \mathcal{R}(\mathcal{P})$ then clearly
\begin{equation}
\mathcal{R} = \mathcal{R}(\mathcal{P}) = \{1, p_1\} \cdot \mathcal{R}(\mathcal{P}),
\end{equation}
so that $\mathcal{R} = \mathcal{R}(\mathcal{P})$ has a non-trivial multiplicative decomposition. Thus instead of studying the multiplicative decomposability of $\mathcal{R}(\mathcal{P})$, as is usual in such cases (see \cite{4, 10, 14} and the reference list of \cite{14}), we consider the shifted set
\begin{equation}
\mathcal{T} = \mathcal{T}(\mathcal{P}) = \mathcal{R}(\mathcal{P}) + \{1\}.
\end{equation}

First we shall prove the multiplicative analog of Theorem A:

Theorem 2.1. If $\mathcal{P}$ is defined as in Theorem A (i.e. there exists an $x_0$ for which (2.1) holds), and $\mathcal{R}(\mathcal{P})$ and $\mathcal{T}(\mathcal{P})$ are defined by (2.2) and (2.4), respectively, then $\mathcal{T} = \mathcal{T}(\mathcal{P})$ is totally $m$-primitive.

Here the situation is exactly the same as in the additive case in \cite{9} where after presenting Theorem 2.1 in \cite{9} we wrote:

"We remark that in the proof of Theorem 2.1 all we use is only that the counting function of the set $\mathcal{P}$ satisfies (2.2) [called (2.1) here], and the elements $p_1, p_2, \ldots$ of $\mathcal{P}$ are pairwise coprime but apart from this we do not use that they are prime. Thus clearly this theorem can be extended to the
case when we assume only that the counting function of \( \mathcal{P} \subset \mathbb{N} \) satisfies (2.2) and its elements are pairwise coprime.”

Similarly, we can extend Theorem 2.1 here to the case when we assume only that the counting function of \( \mathcal{P} \subset \mathbb{N} \) satisfies (2.1) and its elements are pairwise coprime.

Theorem 2.1 easily implies (we leave the details to the reader):

**Corollary 2.1.** If \( \mathcal{P} = \{p_1, p_2, \ldots \} \subset \mathbb{P} \) with \( p_1 < p_2 < \cdots \) is an infinite set of primes with the property that there exists a number \( k_0 \) such that

\[
p_k > e^{52k}
\]

for \( k > k_0 \), then \( \mathcal{T}(\mathcal{P}) = \mathcal{R}(\mathcal{P}) + \{1\} \) is totally \( m \)-primitive.

We will also prove the multiplicative analogs of Theorems B and C:

**Theorem 2.2.** Let \( \mathcal{P} \subset \mathbb{P} \) be of the form (2.3) with a finite set \( \mathcal{Q} \subset \mathbb{P} \), and let either \( t \in \mathbb{N} \) and \( t \geq 2 \), or \( t = \infty \). Then the set \( \mathcal{T} = \mathcal{T}(\mathcal{P}) \) defined by (2.4) has a multiplicative decomposition

\[
\mathcal{T} = \mathcal{T}(\mathcal{P}) = \mathcal{T}(\mathbb{P} \setminus \mathcal{Q}) = A \cdot B
\]

such that \( |A| = \infty \) and \( |B| = t \).

We will also show that Theorem 2.2 is sharp in the sense that if \( \mathcal{Q} \) in (2.3) is infinite, then no matter how thin \( \mathcal{Q} \) is, \( \mathcal{T}(\mathcal{P}) \) need not have a finite \( m \)-decomposition of the form (2.5):

**Theorem 2.3.** For every non-decreasing function \( f: \mathbb{N} \to \mathbb{R} \) with \( \lim_{n \to \infty} f(n) = \infty \) there exists a set \( \mathcal{Q} \subset \mathbb{P} \) with the following properties: the set \( \mathcal{P} = \mathbb{P} \setminus \mathcal{Q} \) is infinite, \( Q(n) < f(n) \) for all \( n \in \mathbb{N} \), and the set \( \mathcal{T}(\mathcal{P}) \) defined by (2.4) is totally \( m \)-\( F \)-primitive.

**Remark.** In the additive case in [9], at the beginning of Section 7 we proposed some unsolved problems. Among others, we asked: “Is it true that if \( \mathcal{Q} \subset \mathbb{P} \), \( \mathcal{Q} \) is infinite, and \( \mathcal{P} \) is defined by \( \mathcal{P} = \mathbb{P} \setminus \mathcal{Q} \), then \( \mathcal{R}(\mathcal{P}) \) [defined by (2.2) here] is totally \( a \)-primitive?” Recently Ruzsa answered this question in the negative by showing in an elementary but ingenious way that there exists an infinite set \( \mathcal{Q} \subset \mathbb{P} \) such that for \( \mathcal{P} = \mathbb{P} \setminus \mathcal{Q} \) the set \( \mathcal{R}(\mathcal{P}) \) is not totally \( a \)-primitive. One might try to study the multiplicative analog of this problem (to consider the total \( m \)-primitivity of \( \mathcal{T}(\mathcal{P}) \) for \( \mathcal{P} = \mathbb{P} \setminus \mathcal{Q} \), \( \mathcal{Q} \subset \mathbb{P} \) infinite) and some other related problems proposed in [9].

**3. The proof of Theorem 2.1** Assume that \( \mathcal{P} \) satisfies the conditions in Theorem 2.1 but, contrary to the statement of the theorem, the set \( \mathcal{T} = \mathcal{T}(\mathcal{P}) \) (defined by (2.4)) is not totally \( m \)-primitive, so that there are \( n_0 \in \mathbb{N} \)
and sets $\mathcal{T}' \subset \mathbb{N}$, $\mathcal{A} = \{a_1, a_2, \ldots\} \subset \mathbb{N}$, $\mathcal{B} = \{b_1, b_2, \ldots\} \subset \mathbb{N}$ (with $a_1 < a_2 < \cdots$, $b_1 < b_2 < \cdots$) such that
\begin{align}
\mathcal{T}' \cap [n_0, \infty) &= \mathcal{T} \cap [n_0, \infty), \\
\mathcal{T}' &= \mathcal{A} \cdot \mathcal{B}, \\
|\mathcal{A}|, |\mathcal{B}| &\geq 2.
\end{align}

We will show that these assumptions lead to a contradiction. As in the additive case in [9], the crucial tool in the proof will be a result on unit equations:

**Lemma 3.1.** Let $(0 <) q_1 < \cdots < q_s$ be prime numbers, and write $S = \{q_1, \ldots, q_s\}$ and
\begin{equation}
\mathbb{Z}_S^* = \{a/b : a, b \in \mathbb{Z}, ab \neq 0, (a, b) = 1, q \in \mathbb{P} \text{ and } q \mid ab \Rightarrow q \in S\}.
\end{equation}
If $A, B \in \mathbb{Q}$ and $AB \neq 0$, then the $S$-unit equation
\begin{equation}
Ax + By = 1, \quad x, y \in \mathbb{Z}_S^*,
\end{equation}
has at most $2^{16(s+1)}$ solutions.

**Proof.** See Beukers and Schlickewei [1] or [6, p. 133].

We will also need the following lemma:

**Lemma 3.2.** If $\mathcal{P} = \{p_1, p_2, \ldots\}$ is an infinite set of primes which satisfies (2.1), then there are infinitely many $k \in \mathbb{N}$ such that
\begin{equation}
\log p_{k+1} > 2^{51}(\log p_1 + \cdots + \log p_k).
\end{equation}

**Proof.** This is Lemma 3.2 in [9].

To deduce a contradiction from (3.1)–(3.3), we distinguish two cases.

**Case 1.** Assume first that $\mathcal{P}$ is finite; let $\mathcal{P} = \{p_1, \ldots, p_s\}$ with $p_1 < \cdots < p_s$. The set $\mathcal{T}(\mathcal{P})$ (defined by (2.4)) is infinite since it contains $p_1^k + 1$ for every $k \in \mathbb{N}$. Thus it follows from (3.1) that $\mathcal{T}'$ is also infinite, so that by (3.2), $\mathcal{A}$ or $\mathcal{B}$ must be infinite; assume that $\mathcal{B}$ is infinite. Then there are infinitely many $b$ with
\begin{equation}
b \in \mathcal{B}, \quad b > n_0.
\end{equation}

For such an integer $b$ write
\begin{align}
a_2 b - 1 &= x, \\
a_1 b - 1 &= y.
\end{align}

Then we have
\begin{equation}
a_1 x - a_2 y = a_1 (a_2 b - 1) - a_2 (a_1 b - 1) = a_2 - a_1.
\end{equation}

Thus the integers $x, y$ defined by (3.7) and (3.8) satisfy the equation
\begin{equation}
\frac{a_1}{a_2 - a_1} x - \frac{a_2}{a_2 - a_1} y = 1,
\end{equation}

which contradicts Lemma 3.1.
and taking different $b$ values in (3.6), clearly we get different solutions $(x, y)$ of this equation. Since there are infinitely many $b$ values satisfying (3.6), it follows that (3.9) has infinitely many solutions $(x, y)$ of this type. However, it follows from (2.4) and (3.1)–(3.3), (3.6)–(3.8) that for $i = 1, 2$ and $b$ satisfying (3.6) we have

$$a_i b \in (A \cdot B) \cap [n_0, \infty) \subset T' \cap [n_0, \infty) = T \cap [n_0, \infty) \subset T = \mathcal{R} + \{1\},$$

whence

$$a_i b - 1 \in \mathcal{R} \quad (\text{for } i = 1, 2).$$

By (3.7), (3.8) and (3.10) we have

$$x, y \in \mathcal{R} = \mathcal{R}(\mathcal{P}) \subset \mathbb{Z}_p^*,$$

where $\mathbb{Z}_p^*$ is defined by (3.4) in Lemma 3.1 with $\mathcal{P}$ in place of $\mathcal{S}$. Thus the $\mathcal{P}$-unit equation formed by (3.9) and (3.11) has infinitely many solutions $(x, y)$, which contradicts Lemma 3.1 and this completes the proof in Case 1.

Case 2. Assume now that $\mathcal{P}$ is infinite; let $\mathcal{P} = \{p_1, p_2, \ldots\}$ with $p_1 < p_2 < \cdots$. By the assumptions in the theorem, $\mathcal{P}$ also satisfies (2.1), so that all the assumptions in Lemma 3.2 hold. Using this lemma, we find that there are infinitely many $k \in \mathbb{N}$ satisfying (3.5). Write

$$m = \max(a_2, b_2).$$

Let $K$ be an integer large enough (in particular, large in terms of $n_0$ in (3.1) and $m$ in (3.12)) which satisfies (3.5) with $K$ in place of $k$, so

$$\log p_{K+1} > 2^{51}(\log p_1 + \cdots + \log p_K).$$

By (3.1) and (3.2) we have

$$\mathcal{T} \cap \left[ n_0, \frac{p_{K+1}}{m} \right] = \mathcal{T}' \cap \left[ n_0, \frac{p_{K+1}}{m} \right] \subset \left( A \cap \left[ 1, \frac{p_{K+1}}{m} \right] \right) \cdot \left( B \cap \left[ 1, \frac{p_{K+1}}{m} \right] \right).$$

It follows that

$$\left| \mathcal{T} \cap \left[ n_0, \frac{p_{K+1}}{m} \right] \right| \leq A \left( \frac{p_{K+1}}{m} \right) \cdot B \left( \frac{p_{K+1}}{m} \right).$$

So far the sets $A$ and $B$ have played symmetric roles, thus we may assume that

$$A \left( \frac{p_{K+1}}{m} \right) \leq B \left( \frac{p_{K+1}}{m} \right).$$

Then it follows from (3.14) that

$$B \left( \frac{p_{K+1}}{m} \right) \geq \left| \mathcal{T} \cap \left[ n_0, \frac{p_{K+1}}{m} \right] \right|^{1/2}.$$
Now we need a lower bound for the right hand side. By (2.4) we have

\[
T \cap \left[ n_0, \frac{pK+1}{m} \right] = R \cap \left[ n_0 - 1, \frac{pK+1}{m} - 1 \right]
= R \left( \frac{pK+1}{m} - 1 \right) - R(n_0 - 2) > R \left( \frac{pK+1}{m} - 1 \right) - n_0.
\]

Define the set \( R' \) so that \( r \in R' \) if and only if \( r \) is of the form

\[
r = p_0^{\alpha_1} \cdots p_K^{\alpha_K} \text{ with } \alpha_i \in \{0, 1, \ldots, 2^{50}\} \text{ for } i = 1, \ldots, K.
\]

By (3.13), for \( K \) large enough and all \( r \in R' \) we have

\[
\log r = \log p_0^{\alpha_1} + \cdots + \log p_K^{\alpha_K} \\
\leq 2^{50}(\log p_1 + \cdots + \log p_K) < \frac{1}{2} \log p_{K+1},
\]

and thus if \( K \) is large enough in terms of \( m \), then

\[
r < p_{K+1}^{1/2} = \frac{pK+1}{p_{K+1}^{1/2}} < \frac{pK+1}{m} \text{ for all } r \in R'.
\]

It follows from (3.17) and (3.18) that

\[
R' \subset R \cap \left[ 0, \frac{pK+1}{m} - 1 \right],
\]

whence

\[
R \left( \frac{pK+1}{m} - 1 \right) \geq |R'|.
\]

By (3.17) we clearly have

\[
|R'| = (2^{50} + 1)^K > 2^{50K}.
\]

It follows from (3.15), (3.16), (3.19) and (3.20) for \( K \) large enough that

\[
B \left( \frac{pK+1}{m} \right) \geq \left| T \cap \left[ n_0, \frac{pK+1}{m} \right] \right|^{1/2} > \left( R \left( \frac{pK+1}{m} - 1 \right) - n_0 \right)^{1/2}
\geq (|R'| - n_0)^{1/2} > (2^{50K} - n_0)^{1/2} > 2^{24K}.
\]

Now we will complete the proof of Theorem 2.1 by showing that this lower bound contradicts Lemma 3.1. Write

\[
B' = B \cap \left[ n_0, \frac{pK+1}{m} \right].
\]

By (3.1), (3.2), (3.12) and (3.22), for all

\[
b \in B'
\]

and \( i = 1, 2 \) we have

\[
n_0 < b \leq a_ib \leq mb < m \cdot \frac{pK+1}{m} = p_{K+1},
\]

\[
a_ib \in T \cap (n_0, pK+1).
\]
Define the integers $x, y$ by
\begin{align}
(3.26) & \quad a_1 b = x + 1, \\
(3.27) & \quad a_2 b = y + 1.
\end{align}

Then by (2.4) and (3.25) we have
\begin{align}
(3.28) & \quad x, y \in \mathcal{R} \cap \left[n_0, pK+1\right].
\end{align}

It follows from (3.26) and (3.27) that
\begin{align}
(3.29) & \quad a_1 a_2 b = a_2(a_1 b) = a_2(x + 1) = a_2 x + a_2, \\
(3.30) & \quad a_1 a_2 b = a_1(a_2 b) = a_1(y + 1) = a_1 y + a_1,
\end{align}

so that
\begin{align}
(3.31) & \quad a_2 x + a_2 = a_1 y + a_1,
\end{align}

whence
\begin{align}
(3.32) & \quad \frac{a_2}{a_1 - a_2} x - \frac{a_1}{a_1 - a_2} y = 1.
\end{align}

Clearly, different $b$ values satisfying (3.23) define different pairs $(x, y)$ of integers in (3.26) and (3.27), thus by (3.21) and (3.22) the number $N$ of solutions $(x, y)$ of (3.31) is at least
\begin{align}
(3.32) & \quad N = |\mathcal{B}'| = |\mathcal{B} \cap \left(n_0, \frac{pK+1}{m}\right)| = B\left(\frac{pK+1}{m}\right) - B(n_0) \\
& \quad > 2^{24K} - n_0 > 2^{23K}
\end{align}

for $K$ large enough. On the other hand, the coefficients $\frac{a_2}{a_1 - a_2}$ and $\frac{a_1}{a_1 - a_2}$ in (3.31) are non-zero rational numbers, and writing $\mathcal{S} = \{p_1, \ldots, p_K\}$, by (3.28) and the definition of $\mathcal{R}$ we see that (3.31) is an $\mathcal{S}$-unit equation (with $|\mathcal{S}| = s = K$) as in Lemma 3.1. Thus by Lemma 3.1 the number $N$ of its solutions satisfies
\begin{align}
N & < 2^{16(s+1)} = 2^{16K+16} < 2^{17K}
\end{align}

for $K$ large enough. This contradicts (3.32) and completes the proof of Theorem 2.1. \hfill \blacksquare

4. The proof of Theorem 2.2. Observe first that if $\mathcal{P}$ contains all the primes then
\begin{align}
\mathcal{T}(\mathcal{P}) = \{2, 3, 4, \ldots\}
\end{align}

and the statement is trivial. Thus we may assume that there are some primes not belonging to $\mathcal{P}$; denote them by $q_1, \ldots, q_n$. Then by the Chinese Remainder Theorem we easily see that $\mathcal{T}(\mathcal{P})$ is a subset of $\mathbb{N}$ which is periodic modulo $Q := q_1 \cdots q_n$. From this the statement easily follows, as we can take $\mathcal{A} = \mathcal{T}(\mathcal{P})$ and $\mathcal{B}$ can be any subset of $\{b \in \mathbb{N} : b \equiv 1 \pmod{Q}\}$ with $1 \in \mathcal{B}$ and $|\mathcal{B}| = t$. \hfill \blacksquare
5. The proof of Theorem 2.3. Let \( f \) be a function as in the theorem. We construct \( \mathcal{P} \) with the prescribed properties explicitly. First we define \( \mathcal{Q} \), and then we take \( \mathcal{P} = \mathbb{P} \setminus \mathcal{Q} \).

We define the elements of \( \mathcal{Q} \) recursively, in the following way. For a positive integer \( k \), put

\[
\mathcal{H}_k = \{(u, v) : u, v \in \mathbb{N}, 1 \leq u, v \leq k, u \neq v\},
\]

and write

\[
h_k = |\mathcal{H}_k| = k(k - 1).
\]

Note that \( \mathcal{H}_1 = \emptyset \) and \( h_1 = 0 \). As the first two elements of \( \mathcal{Q} \), take two primes \( p_1, p_2 \) such that

\[
\max(2, t_2) < p_1 < p_2
\]

where \( t_2 \) is arbitrary with \( f(t_2) > 2 \). Note that \( h_2 = 2 \), and assume that for some \( \ell \geq 2 \), the primes \( p_1, \ldots, p_{\ell} \) with \( e_\ell = h_1 + \cdots + h_\ell \) are already defined. Then choose arbitrary primes \( p_{e_\ell + 1}, \ldots, p_{e_\ell + h_\ell + 1} \) satisfying

\[
\max \left( \ell + 1, t_{\ell+1}, \prod_{i=1}^{e_\ell} p_i \right) < p_{e_\ell + 1} < \cdots < p_{e_\ell + h_\ell + 1},
\]

where \( t_{\ell+1} \) is arbitrary with \( f(t_{\ell+1}) > e_\ell + h_\ell + 1 \). Then set

\[
\mathcal{Q} = \{p_1, p_2, \ldots\} \quad \text{and} \quad \mathcal{P} = \mathbb{P} \setminus \mathcal{Q}.
\]

It is clear that \( \mathcal{Q} \) is infinite and \( Q(n) < f(n) \) for all \( n \in \mathbb{N} \). The latter statement follows from the definition of \( t_\ell \) and

\[
t_{\ell+1} < p_{e_\ell + 1} < \cdots < p_{e_\ell + h_\ell + 1} \quad (\ell \geq 1).
\]

To prove that \( \mathcal{T}(\mathcal{P}) \) (defined by (2.4)) is then totally m-F-primitive, first we show the following property: for any positive integer \( k > 1 \), \( \mathcal{T}(\mathcal{P}) \) contains a multiplicatively \( k \)-isolated element \( z \), that is, there is a \( z \in \mathcal{T}(\mathcal{P}) \) with \( z > k \) and \( uz/v \notin \mathcal{T}(\mathcal{P}) \) for all \( (u, v) \in \mathcal{H}_k \). To prove this, fix \( k > 1 \), write \( (u_i, v_i) \) \( (i = 1, \ldots, h_k) \) for the elements of \( \mathcal{H}_k \) in any order, and consider the following linear congruence system:

\[
\begin{align*}
x & \equiv 0 \pmod{p_i} \quad \text{(for } i = 1, \ldots, e_k - 1), \\
u_i x & \equiv v_i \pmod{p_{e_k - 1 + i}} \quad \text{(for } i = 1, \ldots, h_k).
\end{align*}
\]

By (5.1) we have

\[
u_i \leq k < p_{e_k - 1 + i} \quad \text{for } i = 1, \ldots, h_k,
\]

so the congruence system (5.2) is solvable. Let \( z_k \) be a solution with \( 1 \leq z_k \leq U_k \), where

\[
U_k = \prod_{i=1}^{e_k} p_i.
\]
since $e_k = e_{k-1} + h_k$, by the Chinese Remainder Theorem such a $z_k$ exists (and in fact is unique). Put $s_k = z_k - 1$, and observe that as $z_k \neq 1$, we have $s_k > 0$. Let $p_j \in \mathbb{Q}$ with some $j \in \mathbb{N}$. If $j > e_k$, then in view of \([5.1]\) we have $p_j > U_k > s_k$, thus $p_j \nmid s_k$. Let now $1 \leq j \leq e_k$. If $1 \leq j \leq e_{k-1}$, then by the first congruence of \([5.2]\) we see that $p_j \nmid s_k$. On the other hand, if $e_{k-1} + 1 \leq j \leq e_k$ then by the second congruence we have

$$u(s_k + 1) \equiv v \pmod{p_j}$$

with some $(u, v) \in \mathcal{H}_k$. Hence, in view of $p_j > k$ again we get $p_j \nmid s_k$. Thus $s_k \in \mathcal{R}(\mathcal{P})$, whence $z_k = s_k + 1 \in \mathcal{T}(\mathcal{P})$. Assume that $uz_k/v \in \mathcal{T}(\mathcal{P})$ with some $(u, v) \in \mathcal{H}_k$. Then

$$uz_k = v(s + 1)$$

with some $s \in \mathcal{R}(\mathcal{P})$. Then by the second set of congruences in \([5.2]\), we can find a prime $p > k$ in $\mathbb{Q}$ such that $p \mid vs$. However, in view of $v \leq k$ and $s \in \mathcal{R}(\mathcal{P})$, this is impossible. That is, $z_k$ is a multiplicatively $k$-isolated element of $\mathcal{T}(\mathcal{P})$.

Let now $\mathcal{X}$ be any subset of $\mathbb{N}$ with $\mathcal{X} \sim \mathcal{T}(\mathcal{P})$. Let $n_0 \in \mathbb{N}$ be such that

$$\mathcal{X} \cap [n_0, \infty) = \mathcal{T}(\mathcal{P}) \cap [n_0, \infty).$$

Further, assume that contrary to the statement of the theorem we have

$$\mathcal{X} = \mathcal{B} \cdot \mathcal{C} \quad (|\mathcal{B}|, |\mathcal{C}| \geq 2)$$

with, say, $\mathcal{C}$ finite. Write $\mathcal{C} = \{c_1, \ldots, c_m\} \ (c_1 < \cdots < c_m)$ with $m \geq 2$. Put $k = n_0c_m$. By the property above, $\mathcal{T}(\mathcal{P})$ contains a multiplicatively $k$-isolated element $z$. It follows from the two equalities above that $z \in \mathcal{X}$, and thus $z$ cannot be written in the form

$$z = bc_i \quad \text{with some } b \in \mathcal{B}, \ i \in \{1, \ldots, m\}.$$ 

Take any $j \in \{1, \ldots, m\}$ with $j \neq i$, and put

$$z_0 = bc_j.$$ 

Then $z_0 \in \mathcal{X}$, $z_0 \neq z$. Observe that since $z_0 = zc_j/c_i$ and $z > k = n_0c_m$, we have $z_0 > n_0$, whence $z_0 \in \mathcal{T}(\mathcal{P})$. However, as $1 \leq c_i, c_j \leq k$, this contradicts $z$ being multiplicatively $k$-isolated. Hence the statement follows.  

6. Open problems. In this section we will present some open problems related to the problems and results studied in this paper, in [5] and in our earlier papers [7–12].

Ostmann was the first to propose the study of the decomposability of a set defined by a multiplicative property: in [12] he conjectured that the set $\mathbb{P}$ of all primes is totally a-primitive. This famous conjecture is still unsolved in its original form, but there are some interesting partial results. In particular,
Elsholtz [2, 3] proved that there are no sets $A, B, C$ of non-negative integers such that
\[(6.1) \quad \mathbb{P} = A + B + C \quad \text{with } |A|, |B|, |C| \geq 2.\]

Ostmann’s problem can be generalized in the following way:

Let $\omega(n)$ and $\Omega(n)$ denote the number of distinct prime factors and the total number of prime factors of the positive integer $n$, respectively.

**Problem 6.1.** Let $k \in \mathbb{N}$. Is the set
(a) $\mathbb{P}_k = \{n \in \mathbb{N} : \omega(n) = k\}$,
(b) $\mathbb{P}_k^+ = \{n \in \mathbb{N} : \Omega(n) = k\}$
totally a-primitive?

Note that the special case $k = 1$ of (a) is Ostmann’s problem.

**Problem 6.2.** Let $k \in \mathbb{N}$. Is the set
(a) $\bar{\mathbb{P}}_k = \{n : n \in \mathbb{N} : \omega(n) \leq k\}$,
(b) $\bar{\mathbb{P}}_k^+ = \{n : n \in \mathbb{N} : \Omega(n) \leq k\}$
totally a-primitive?

Probably the answer is affirmative in each of the four cases in Problems 6.1 and 6.2 but to prove this seems to be difficult; as a partial result one might try to prove that the sets defined in the four problems have no ternary decompositions (like the one in (6.1)).

The multiplicative analogs of Problems 6.1 and 6.2 are

**Problem 6.3.** Is the set
(a) $\mathbb{P}_k + \{1\}$,
(b) $\mathbb{P}_k^+ + \{1\}$,
(c) $\bar{\mathbb{P}}_k + \{1\}$,
(d) $\bar{\mathbb{P}}_k^+ + \{1\}$
totally m-primitive?

Another important special set defined by a multiplicative property is the set of squarefree integers:
\[M = \{n \in \mathbb{N} : |\mu(n)| = 1\}.\]

**Problem 6.4.** Is the set $M$ totally a-primitive?

(Again, one might first try to study the existence of ternary decompositions.)

**Problem 6.5.** Is the set $M + \{1\}$ totally m-primitive?

One may also consider the opposite of the property in the definition of $M$. A positive integer $n$ is said to be powerful if the exponent of every prime in
its prime factorization is at least 2. Denote the set of these numbers by \( \tilde{\mathcal{M}} \):

\[
\tilde{\mathcal{M}} = \{ n \in \mathbb{N} : p \in \mathbb{P} \land p \, | \, n \Rightarrow p^2 \, | \, n \}.
\]

**Problem 6.6.** Is the set \( \tilde{\mathcal{M}} \) totally a-primitive?

**Problem 6.7.** Is the set \( \tilde{\mathcal{M}} + \{1\} \) totally m-primitive?

It is an interesting feature of Problem 6.7 that it establishes a link between our papers [10–12] (in which we studied total m-primitivity of shifted polynomial sets) and [7–9] (in which we studied total m-primitivity of shifted sets defined by a multiplicative property). Indeed, \( \tilde{\mathcal{M}} \) is defined by a multiplicative property, thus \( \tilde{\mathcal{M}} + \{1\} \) is of the second type. On the other hand, clearly \( m \in \tilde{\mathcal{M}} \) if and only if there are \( x, y \in \mathbb{N} \) such that \( m = x^3 y^2 \), thus \( \tilde{\mathcal{M}} + \{1\} \) can also be considered as a shifted polynomial set:

\[
(6.2) \quad \tilde{\mathcal{M}} + \{1\} = \{ f(x, y) : x, y \in \mathbb{N} \} + \{1\} \quad \text{with} \quad f(x, y) = x^3 y^2.
\]

We wrote in [11]:

“**Conjecture 1.** If \( k, \ell \in \mathbb{N}, k > 1 \) and \( \ell > 1 \) then

\[
\{ x^k y^\ell + 1 : (x, y) \in \mathbb{N}^2 \}
\]

is totally m-primitive.

Here the difficulty is that in general the problem reduces to a diophantine equation in four variables, and we know much less on such equations than on equations in two variables. However, one might like to prove at least non-trivial partial results:

**Problem 2.** Is it true that if \( \ell \in \mathbb{N}, \ell \text{ is odd, and } \ell > 1 \) then the set \( \{ x^2 y^\ell + 1 : (x, y) \in \mathbb{N}^2 \} \) is totally m-primitive? \ldots Can one decide this at least for \( \ell = 3? \)”

Observe that the set in the special case described at the end of this problem is exactly the set defined in (6.2). Denote it by

\[
(\tilde{\mathcal{M}} + \{1\} =) \quad \mathcal{D} = \{ d_1, d_2, \ldots \} \quad \text{(with } d_1 < d_2 < \cdots \).
\]

Then it can be shown by our standard approach that the total m-primitivity of \( \mathcal{D} \) would follow from the affirmative answer to the following question:

**Problem 6.8.** *Is it true that if \( A, B, C \) are fixed positive integers and \( z \to \infty \) then the number of solutions \( (m, m') \) of the equation

\[
Am - Bm' = C, \quad m, m' \in \mathcal{M} \cap [0, z],
\]

is \( o(z^{1/4}) \) ?

(We conjecture that this is true, and even the number of solutions is \( o(z^\epsilon) \) for any \( \epsilon > 0 \).)

In [9] we remarked that it follows from a result of Wirsing [15] that in a well-defined sense almost all subsets of \( \mathbb{N}_0 \) are totally a-primitive; this
fact can be used to prove the existence of totally \(a\)-primitive subsets with certain prescribed properties. Let \(\Phi\) denote the set of \(a\)-reducible subsets of \(\mathbb{N}_0\), and define the mapping \(\varrho\) from the subsets of \(\mathbb{N}_0\) into \([0,1]\) so that for \(A = \{a_1, a_2, \ldots\} \subset \mathbb{N}_0\) (with \(a_1 < a_2 < \cdots\)),

\[
\varrho(A) = \sum_{a_i \in A} \frac{1}{2^{a_{i+1}}}
\]

(this defines a one-to-one correspondence between the infinite sets \(A \subset \mathbb{N}_0\) and the points of \((0,1]\)). If \(\Gamma\) is a set of subsets of \(\mathbb{N}_0\) then let

\[
\varrho(\Gamma) = \{\varrho(A) : A \in \Gamma\},
\]

and for \(S \subset [0,1]\) let \(\lambda(S)\) denote the Lebesgue measure of \(S\). Wirsing \cite{15} proved that

\[
\lambda(\varrho(\Phi)) = 0.
\]

The next problem is to prove the multiplicative analog of this result. Let \(\Psi\) denote the set of \(m\)-reducible subsets of \(\mathbb{N}\), and define the mapping \(\sigma\) from the subsets of \(\mathbb{N}\) into \([0,1)\) so that for \(A = \{a_1, a_2, \ldots\} \subset \mathbb{N}\) (with \(a_1 < a_2 < \cdots\)),

\[
\sigma(A) = \sum_{a_i \in A} \frac{1}{2^{a_i}}.
\]

If \(\Gamma\) is a set of subsets of \(\mathbb{N}\) then let

\[
\sigma(\Gamma) = \{\sigma(A) : A \in \Gamma\}.
\]

**Problem 6.9.** Is it true that

\[
\lambda(\sigma(\Psi)) = 0?
\]

In \cite{9} we also presented some results and problems on the Hausdorff dimension \(\dim \sigma(S)\) for certain additively defined sets \(S\) of subsets of \(\mathbb{N}_0\). The multiplicative analogs of some of these problems are:

**Problem 6.10.** Is it true that

\[
(\dim \sigma(\Psi) \geq) \dim \sigma(\{1, 2\} \cdot A : A \subset \mathbb{N}) > 0?
\]

**Problem 6.11.** Is it true that

\[
\dim \sigma(A \cdot B : A, B \text{ are infinite subsets of } \mathbb{N}) < 1?
\]

**Acknowledgements.** The authors are grateful to the referee for the insightful and helpful remarks.

Research supported in part by the Eötvös Loránd Research Network (ELKH), the NKFIH grants K115479, K119528, K128088, and K130909, and by the project EFOP-3.6.1-16-2016-00022 of the European Union, co-financed by the European Social Fund.
References


K. Győry
Institute of Mathematics
University of Debrecen
H-4002 Debrecen, Hungary
E-mail: gyory@science.unideb.hu

A. Sárközy
Institute of Mathematics
Eötvös Loránd University
H-1117 Budapest, Hungary
E-mail: sarkozy@cs.elte.hu

L. Hajdu
Institute of Mathematics
University of Debrecen
H-4002 Debrecen, Hungary
and
ELKH-DE Equations, Functions, Curves and their Applications Research Group
Budapest, Hungary
E-mail: hajdul@science.unideb.hu