ON ADDITIVE AND MULTIPLICATIVE DECOMPOSITIONS OF SETS OF INTEGERS COMPOSED FROM A GIVEN SET OF PRIMES, II. (MULTIPLICATIVE DECOMPOSITIONS.)

K. GYŐRY, L. HAJDU AND A. SÁRKÖZY

Dedicated to the memory of Andrzej Schinzel.

Abstract. In part I of this paper we sharpened and extended some results of Elsholtz and Harper on the *additive* decomposability of sets of integers with restricted prime factors. In this paper we will study the *multiplicative* analogs of the results proved in part I.

1. Introduction

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

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

$$A(x) = |\{a : a \in \mathcal{A},\ a \le x\}|.$$

The set of the positive integers is denoted by $\mathbb{N}$, and we write $\mathbb{N} \cup \{0\} = \mathbb{N}_0$. The set of the rational and *positive* real numbers is denoted by $\mathbb{Q}$ and $\mathbb{R}$, respectively. The set of the (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 $\mathcal{A}, \mathcal{B}, \mathcal{C}$ subsets of $\mathcal{G}$ with*

$$|\mathcal{B}| \ge 2, \quad |\mathcal{C}| \ge 2. \tag{1.1}$$

Date: August 5, 2022.

2010 *Mathematics Subject Classification.* 11N99, 11P70, 11P99.

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

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.

If

$$\mathcal{A} = \mathcal{B} + \mathcal{C} \ (= \{b + c : b \in \mathcal{B},\ c \in \mathcal{C}\}), \tag{1.2}$$

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

$$\mathcal{A} = \mathcal{B} \cdot \mathcal{C} \ (= \{bc : b \in \mathcal{B},\ c \in \mathcal{C}\}) \tag{1.3}$$

hold, then (1.3) *is called a* multiplicative decomposition *or briefly* m-decomposition *of* $\mathcal{A}$*. Moreover, if* $\mathcal{A}$ *is* infinite*, and* $\mathcal{B}$ *or* $\mathcal{C}$ *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) *is an* a-F-decomposition *and* m-F-decomposition*, respectively.*

Definition 1.2. *A finite or infinite set* $\mathcal{A}$ *of non-negative integers is said to be* a-reducible *if it has an* additive decomposition

$$\mathcal{A} = \mathcal{B} + \mathcal{C} \quad \textit{with} \quad |\mathcal{B}| \geq 2,\ |\mathcal{C}| \geq 2 \tag{1.4}$$

(where $\mathcal{B} \subset \mathbb{N}_0$*,* $\mathcal{C} \subset \mathbb{N}_0$*). If there are no sets* $\mathcal{B}, \mathcal{C}$ *with these properties, then* $\mathcal{A}$ *is said to be* a-primitive *or* a-irreducible*. Moreover, an* infinte *set* $\mathcal{A} \subset \mathbb{N}_0$ *is said to be* a-F-reducible *if it has a* finite *a-decomposition of form* (1.4)*, while if it has no* finite *decomposition of this type, then it is said to be* a-F-primitive *or* a-F-irreducible*.*

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

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

The multiplicative analogs of Definitions 1.2 and 1.4 are:

Definition 1.5. *If* $\mathcal{A}$ *is an infinite set of* positive *integers, then it is said to be* m-reducible *if it has a* multiplicative decomposition

$$\mathcal{A} = \mathcal{B} \cdot \mathcal{C} \quad \textit{with} \quad |\mathcal{B}| \geq 2,\ |\mathcal{C}| \geq 2 \tag{1.5}$$

(where $\mathcal{B} \subset \mathbb{N}$*,* $\mathcal{C} \subset \mathbb{N}$*). If there are no such sets* $\mathcal{B}, \mathcal{C}$ *then* $\mathcal{A}$ *is said to be* m-primitive *or* m-irreducible*. Moreover, an infinite set* $\mathcal{A} \subset \mathbb{N}$ *is said to be* m-F-reducible *if it has a* finite *decomposition of form* (1.5)*, while if it has no* finite *m-decomposition of this type, then it is said to be* m-F-primitive *or* m-F-irreducible*.*

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

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

2. The problem, and the theorems to prove

In part I we proved the following theorems:

Theorem A. *If $\mathcal{P} = \{p_1, p_2, \dots\} \subset \mathbb{P}$ (with $p_1 < p_2 < \dots$) is a non-empty (finite or infinite) set of primes such that there exists a number x_0 with*

$$P(x) < \frac{1}{51} \log\log x \quad \text{for } x > x_0 \tag{2.1}$$

(where $P(x) = |\mathcal{P} \cap [1,x]|$), then the set

$$\mathcal{R}(\mathcal{P}) = \{n \in \mathbb{N} : p \mid n \implies p \in \mathcal{P}\} \tag{2.2}$$

is totally a-primitive.

Theorem B. *Let $\mathcal{P} \subset \mathbb{P}$ be of the form*

$$\mathcal{P} = \mathbb{P} \setminus \mathcal{Q} \text{ where } \mathcal{Q} \subset \mathbb{P} \tag{2.3}$$

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*

$$\mathcal{R}(\mathcal{P}) = \mathcal{A} + \mathcal{B}$$

such that $|\mathcal{A}| = \infty$ and $|\mathcal{B}| = t$.

Theorem C. *For any monotone non-decreasing function $f : \mathbb{N} \to \mathbb{R}$ with $\lim_{n\to\infty} f(n) = \infty$ there is an* infinite *set $\mathcal{Q} \subset \mathbb{P}$ satisfying $Q(n) < f(n)$ for all $n \in \mathbb{N}$, such that defining $\mathcal{P}$ by* (2.3)*, $\mathcal{P}$ is an infinite set of primes 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 defining $\mathcal{P}$ by $\mathcal{P} = \{p_1, p_2, \dots\} \subset \mathbb{P}$ and $\mathcal{R} = \mathcal{R}(\mathcal{P})$ by (2.2) clearly we have

$$\mathcal{R} = \mathcal{R}(\mathcal{P}) = \{1, p_1\} \cdot \mathcal{R}(\mathcal{P}),$$

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 usual in such a case (see [4, 10, 14] and the reference list of [14]), we have to consider the shifted set

$$\mathcal{T} = \mathcal{T}(\mathcal{P}) = \mathcal{R}(\mathcal{P}) + \{1\}. \tag{2.4}$$

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 a number 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 the set $\mathcal{T} = \mathcal{T}(\mathcal{P})$ is totally m-primitive.*

Here the situation is exactly the same as in the additive case in [9] where after presenting Theorem A (called Theorem 2.1 in [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 $p_1, p_2, \dots$ 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.

It follows easily from Theorem 2.1 (we leave the details to the reader):

Corollary 2.1. *If $\mathcal{P} = \{p_1, p_2, \dots\} \subset \mathbb{P}$ with $p_1 < p_2 < \dots$ is an infinite set of primes such that there exists a number k_0 so that we have*

$$p_k > e^{e^{52k}} \quad \text{for } k > k_0,$$

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*

$$\mathcal{T} = \mathcal{T}(\mathcal{P}) = \mathcal{T}(\mathbb{P} \setminus \mathcal{Q}) = \mathcal{A} \cdot \mathcal{B} \tag{2.5}$$

such that $|\mathcal{A}| = \infty$ and $|\mathcal{B}| = t$.

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 form (2.5):

Theorem 2.3. *For any monotone 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, we have* $Q(n) < f(n)$ *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 very 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 like to study the multiplicative analog of this problem (to consider the totally 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, however, 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 $\mathcal{T}' \subset \mathbb{N}$, $\mathcal{A} = \{a_1, a_2, \dots\} \subset \mathbb{N}$, $\mathcal{B} = \{b_1, b_2, \dots\} \subset \mathbb{N}$ (with $a_1 < a_2 < \dots$, $b_1 < b_2 < \dots$) such that

$$\mathcal{T}' \cap [n_0, \infty) = \mathcal{T} \cap [n_0, \infty), \tag{3.1}$$

$$\mathcal{T}' = \mathcal{A} \cdot \mathcal{B} \tag{3.2}$$

and

$$|\mathcal{A}| \geq 2, \quad |\mathcal{B}| \geq 2. \tag{3.3}$$

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

Lemma 3.1. *Let* $(0 <) q_1 < q_2 < \dots < q_s$ *be prime numbers, write* $\mathcal{S} = \{q_1, q_2, \dots, q_s\}$ *and*

(3.4)
$$\mathbb{Z}_{\mathcal{S}}^* = \left\{ \frac{a}{b} : a, b \in \mathbb{Z},\ ab \neq 0,\ (a,b) = 1,\ q \in \mathbb{P} \text{ and } q \mid ab \implies q \in \mathcal{S} \right\}.$$

If $A \in \mathbb{Q}$, $B \in \mathbb{Q}$ *and* $AB \neq 0$*, then the* S-unit equation

$$Ax + By = 1, \quad x, y \in \mathbb{Z}_{\mathcal{S}}^*$$

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 the set* $\mathcal{P} = \{p_1, p_2, \dots\}$ *is an* infinite *set of primes which satisfies* (2.1)*, then there are infinitely many* $k \in \mathbb{N}$ *such that*

$$\log p_{k+1} > 2^{51}(\log p_1 + \log p_2 + \cdots + \log p_k). \tag{3.5}$$

Proof. This is Lemma 3.2 in [9]. □

To deduce a contradiction from (3.1), (3.2) and (3.3), we have to distinguish two cases.

CASE 1. Assume first that $\mathcal{P}$ is *finite*; let $\mathcal{P} = \{p_1, p_2, \dots, p_s\}$ (with $p_1 < p_2 < \cdots < p_s$). 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) at least one of the sets $\mathcal{A}$ and $\mathcal{B}$ must be infinite; we may assume that $\mathcal{B}$ is infinite. Then there are infinitely many b with

$$b \in \mathcal{B}, \quad b > n_0. \tag{3.6}$$

For such an integer b write

$$a_2 b - 1 = x \tag{3.7}$$

and

$$a_1 b - 1 = y. \tag{3.8}$$

Then we have

$$a_1 x - a_2 y = a_1(a_2 b - 1) - a_2(a_1 b - 1) = a_2 - a_1.$$

Thus the integers x, y defined by (3.7) and (3.8) satisfy the equation

$$\frac{a_1}{a_2 - a_1} x - \frac{a_2}{a_2 - a_1} y = 1, \tag{3.9}$$

and taking different b values in (3.6), clearly we get different x, y solutions of this equation. Since there are infinitely many b values satisfying (3.6), thus it follows that (3.9) has infinitely many x, y solutions 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

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

whence

$$a_i b - 1 \in \mathcal{R} \quad (\text{for } i = 1, 2). \tag{3.10}$$

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

$$x, y \in \mathcal{R} = \mathcal{R}(\mathcal{P}) \subset \mathbb{Z}_{\mathcal{P}}^* \tag{3.11}$$

where $\mathbb{Z}_{\mathcal{P}}^*$ 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* x, y

solution which contradicts Lemma 3.1, and this completes the proof in CASE 1.

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

$$m = \max(a_2, b_2). \tag{3.12}$$

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 that

$$\log p_{K+1} > 2^{51}(\log p_1 + \log p_2 + \dots + \log p_K). \tag{3.13}$$

By (3.1) and (3.2) we have

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

It follows from this that

$$\left|\mathcal{T} \cap \left[n_0, \frac{p_{K+1}}{m}\right]\right| \le A\left(\frac{p_{K+1}}{m}\right) \cdot B\left(\frac{p_{K+1}}{m}\right). \tag{3.14}$$

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

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

Then it follows from (3.14) that

$$B\left(\frac{p_{K+1}}{m}\right) \ge \left|\mathcal{T} \cap \left[n_0, \frac{p_{K+1}}{m}\right]\right|^{1/2}. \tag{3.15}$$

Now we need a lower bound for the right hand side. By (2.4) we have

$$\left|\mathcal{T} \cap \left[n_0, \frac{p_{K+1}}{m}\right]\right| = \left|\mathcal{R} \cap \left[n_0 - 1, \frac{p_{K+1}}{m} - 1\right]\right| = \\ = R\left(\frac{p_{K+1}}{m} - 1\right) - R(n_0 - 2) > R\left(\frac{p_{K+1}}{m} - 1\right) - n_0. \tag{3.16}$$

Define the set $\mathcal{R}'$ so that $r \in \mathcal{R}'$ if and only if it is of the form

$$r = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_K^{\alpha_K} \text{ with } \alpha_i \in \{0, 1, \dots, 2^{50}\} \text{ for } i = 1, 2, \dots, K. \tag{3.17}$$

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

$$\log r = \log p_1^{\alpha_1} + \log p_2^{\alpha_2} + \cdots + \log p_K^{\alpha_K} \leq$$
$$\leq 2^{50}(\log p_1 + \log p_2 + \ldots + \log p_K) < \frac{1}{2}\log p_{K+1},$$

thus if K is large enough in terms of m, then

$$r < p_{K+1}^{1/2} = \frac{p_{K+1}}{p_{K+1}^{1/2}} < \frac{p_{K+1}}{m} \quad \text{(for all } r \in \mathcal{R}'\text{).} \tag{3.18}$$

It follows from (3.17) and (3.18) that

$$\mathcal{R}' \subset \mathcal{R} \cap \left[0, \frac{p_{K+1}}{m} - 1\right]$$

whence

$$R\left(\frac{p_{K+1}}{m} - 1\right) \geq |\mathcal{R}'|. \tag{3.19}$$

By (3.17) clearly we have

$$|\mathcal{R}'| = \left(2^{50} + 1\right)^K > 2^{50K}. \tag{3.20}$$

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

(3.21)

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

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

$$\mathcal{B}' = \mathcal{B} \cap \left(n_0, \frac{p_{K+1}}{m}\right]. \tag{3.22}$$

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

$$b \in \mathcal{B}' \tag{3.23}$$

and $i = 1, 2$ we have

$$n_0 < b \leq a_i b \leq mb < m \cdot \frac{p_{K+1}}{m} = p_{K+1} \quad \text{(for } b \in \mathcal{B}' \text{ and } i = 1, 2\text{)} \tag{3.24}$$

and

$$a_i b \in \mathcal{T} \cap (n_0, p_{K+1}] \quad \text{(for } b \in \mathcal{B}' \text{ and } i = 1, 2\text{).} \tag{3.25}$$

Define the integers x, y by

$$a_1 b = x + 1, \tag{3.26}$$

$$a_2 b = y + 1. \tag{3.27}$$

Then by (2.4) and (3.25) we have

$$x, y \in \mathcal{R} \cap [n_0, p_{K+1}]. \tag{3.28}$$

It follows from (3.26) and (3.27) that

$$a_1 a_2 b = a_2(a_1 b) = a_2(x+1) = a_2 x + a_2$$

and

$$a_1 a_2 b = a_1(a_2 b) = a_1(y+1) = a_1 y + a_1$$

so that

$$a_2 x + a_2 = a_1 y + a_1$$

whence

$$\frac{a_2}{a_1 - a_2} x - \frac{a_1}{a_1 - a_2} y = 1. \tag{3.29}$$

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 these (x, y) solutions of (3.29) is at least

$$N = |\mathcal{B}'| = \left| \mathcal{B} \cap \left(n_0, \frac{p_{K+1}}{m} \right] \right| = B\left(\frac{p_{K+1}}{m} \right) - B(n_0) > \tag{3.30}$$

$$> 2^{24K} - n_0 > 2^{23K}$$

for K large enough. On the other hand, observe that the coefficients $\frac{a_2}{a_1 - a_2}$ and $\frac{a_1}{a_1 - a_2}$ in the equation (3.29) are non-zero rational numbers, and writing $\mathcal{S} = \{p_1, p_2, \ldots, p_K\}$, by (3.28) and the definition of $\mathcal{R}$ (3.29) is an $\mathcal{S}$-unit equation with this $\mathcal{S}$ (with $|\mathcal{S}| = s = K$) in the sense described in Lemma 3.1. Thus by Lemma 3.1 the number N of its solutions satisfies

$$N < 2^{16(s+1)} = 2^{16K+16} < 2^{17K} \tag{3.31}$$

for K large enough. (3.30) contradicts (3.31) which completes the proof of Theorem 2.1. □

4. The proof of Theorem 2.2

We will need the following lemma:

Lemma 4.1. *Let $m \in \mathbb{N}$, $m \geq 2$ and for $r \in \mathbb{N}_0$, $0 \leq r < m$ put*

$$Z_r = \{z \in \mathbb{N}_0 : z \equiv r \pmod{m}\}.$$

Then for any $\mathcal{I} \subset \{0, 1, \ldots, m-1\}$ the set

$$Z_{\mathcal{I}} = \bigcup_{i \in \mathcal{I}} Z_i$$

is m-reducible. Further, for any t with $2 \le t \le \infty$ there exists a $\mathcal{C}_t \subset \mathbb{N}$ with $|\mathcal{C}_t| = t$ such that with $\mathcal{B} = Z_{\mathcal{I}}$ we have

$$Z_{\mathcal{I}} = \mathcal{B} \cdot \mathcal{C}_t.$$

Proof. Clearly, for any $\mathcal{C} \subset Z_1$ with $1 \in \mathcal{C}$ we have

$$Z_{\mathcal{I}} = Z_{\mathcal{I}} \cdot \mathcal{C}.$$

Indeed, $1 \in \mathcal{C}$ implies that

$$Z_{\mathcal{I}} \subset Z_{\mathcal{I}} \cdot \mathcal{C},$$

while since $zc \in Z_{\mathcal{I}}$ for any $z \in Z_{\mathcal{I}}$ and $c \in \mathcal{C}$, we also have

$$Z_{\mathcal{I}} \supset Z_{\mathcal{I}} \cdot \mathcal{C}.$$

The statement of the lemma follows from this. □

To derive the statement of the theorem from this lemma, observe first that if $\mathcal{P}$ contains all the primes then

$$\mathcal{T}(\mathcal{P}) = \{2, 3, 4, \dots\}$$

and the statement is trivial. Thus we may assume that there are some primes *not* belonging to $\mathcal{P}$; denote these primes by $q_1, q_2, \dots, q_n$. Then we have clearly

$$\mathcal{T}(\mathcal{P}) = \{a \in \mathbb{N} : a \not\equiv 1 \pmod{q_i} \text{ for } i = 1, 2, \dots, n\}.$$

In other words, a positive integer x is in $\mathcal{T}(\mathcal{P})$ if and only if

$$x \equiv 0, 2, 3, \dots, q_i - 2 \text{ or } q_i - 1 \pmod{q_i} \quad (\text{for } i = 1, 2, \dots, n).$$

Thus by the Chinese Remainder Theorem, $\mathcal{T}(\mathcal{P})$ is the union of some residue classes modulo $Q = q_1 q_2 \cdots q_n$. From this, the statement of the theorem follows by Lemma 4.1. □

5. The proof of Theorem 2.3

Let f be a function of the type described 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

$$\mathcal{H}_k = \{(u, v) : u, v \in \mathbb{N},\ 1 \le u, v \le k,\ u \ne v\},$$

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 $p_1, p_2, \dots, p_{e_\ell}$ with $e_\ell = h_1 + h_2 + \cdots + h_\ell$ are already defined. Then choose arbitrary primes $p_{e_\ell+1}, p_{e_\ell+2}, \dots, p_{e_\ell+h_{\ell+1}}$ satisfying

$$\max\left(\ell+1, t_{\ell+1}, \prod_{i=1}^{e_\ell} p_i\right) < p_{e_\ell+1} < p_{e_\ell+2} < \cdots < p_{e_\ell+h_{\ell+1}}, \tag{5.1}$$

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

$$\mathcal{Q} = \{p_1, p_2, p_3, \dots\} \quad \text{and} \quad \mathcal{P} = \mathbb{P} \setminus \mathcal{Q}.$$

It is clear from the definition 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_ℓ 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 totally m-F-primitive for this set $\mathcal{P}$, first we show the following property: for any positive integer $k > 1$, the set $\mathcal{T}(\mathcal{P})$ 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, let $k > 1$ be fixed, write (u_i, v_i) $(i = 1, \dots, h_k)$ for the elements of $\mathcal{H}_k$ in any order, and consider the following linear congruence system:

$$\begin{cases} x \equiv 0 \pmod{p_i} & (\text{for } i = 1, 2, \dots, e_{k-1}), \\ u_i x \equiv v_i \pmod{p_{e_{k-1}+i}} & (\text{for } i = 1, 2, \dots, h_k). \end{cases} \tag{5.2}$$

By (5.1) we have

$$u_i \leq k < p_{e_{k-1}+i} \quad (\text{for } i = 1, \dots, h_k),$$

thus 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 $p_j \in \mathcal{Q}$ 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 the system (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 of the system 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 by $z_k = s_k + 1$ we get $z_k \in \mathcal{T}(\mathcal{P})$. Assume that $uz_k/v \in \mathcal{T}(\mathcal{P})$ with some $(u,v) \in \mathcal{H}_k$. Then we have

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

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 $\mathcal{Q}$ such that $p \mid vs$. However, in view of $v \le k$ 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 $n_0 \in \mathbb{N}$ 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

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

with, say, $\mathcal{C}$ finite. Write $\mathcal{C} = \{c_1, c_2, \dots, c_m\}$ $(c_1 < c_2 < \cdots < c_m)$ with $m \ge 2$. Put $k = n_0 c_m$. By the property above, $\mathcal{T}(\mathcal{P})$ contains a multiplicatively k-isolated element z. It follows from the two equalities above that $z \in \mathcal{X}$, thus it cannot be written in the form

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

Take any $j \in \{1, 2, \dots, m\}$ with $j \ne i$, and put

$$z_0 = bc_j.$$

Then $z_0 \in \mathcal{X}$, $z_0 \ne z$. Observe that by $z_0 = zc_j/c_i$ and $z > k = n_0 c_m$ we have $z_0 > n_0$, whence $z_0 \in \mathcal{T}(\mathcal{P})$. However, this by $1 \le c_i, c_j \le k$ contradicts the fact that z is multiplicatively k-isolated. Hence the statement follows. □

6. Open problems

In this section we will present open problems related to the problems and results studied in this paper and our earlier papers [7, 8, 9, 10, 11, 12].

Ostmann was the first who proposed to study the decomposability of a set defined by a multiplicative property: in [13] he conjectured that the set $\mathbb{P}$ of the primes is totally a-primitive. This famous conjecture is still unsolved in its original form, however, there are some interesting partial results. In particular, Elsholtz [2, 3] proved that there are no sets $\mathcal{A}, \mathcal{B}, \mathcal{C}$ of non-negative integers such that

$$\mathbb{P} = \mathcal{A} + \mathcal{B} + \mathcal{C} \quad \text{with } |\mathcal{A}| \ge 2,\ |\mathcal{B}| \ge 2,\ |\mathcal{C}| \ge 2. \tag{6.1}$$

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. *Is it true that if $k \in \mathbb{N}$ then*

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

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

Problem 6.2. *Is it true that if $k \in \mathbb{N}$ then*

a) *the set*
$$\bar{\mathbb{P}}_k = \{n : n \in \mathbb{N},\ \omega(n) \le k\},$$
b) *the set*
$$\bar{\mathbb{P}}_k^+ = \{n : n \in \mathbb{N},\ \Omega(n) \le k\}$$
is 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 too difficult; then as a partial result one might like 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 a), 6.1 b), 6.2 a), 6.2 b) are

Problem 6.3. *Is it true that the set*

a) $\mathbb{P}_k + \{1\}$,
b) $\mathbb{P}_k^+ + \{1\}$,
c) $\bar{\mathbb{P}}_k + \{1\}$,
d) $\bar{\mathbb{P}}_k^+ + \{1\}$

is totally m-primitive?

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

Problem 6.4. *Is it true that the set $\mathcal{M}$ is totally a-primitive?*

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

Problem 6.5. *Is it true that the set $\mathcal{M} + \{1\}$ is totally m-primitive?*

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

$$\bar{\mathcal{M}} = \{n : n \in \mathbb{N},\ p \in \mathbb{P} \wedge p \mid n \implies p^2 \mid n\}.$$

Problem 6.6. *Is it true that the set $\bar{\mathcal{M}}$ is totally a-primitive?*

Problem 6.7. *Is it true that the set $\bar{\mathcal{M}} + \{1\}$ is totally m-primitive?*

It is an interesting feature of Problem 6.7 that it establishes a link between our papers [10, 11, 12] (in which we studied total m-primitivity of shifted polynomial sets) and [7, 8, 9] (in which we studied total m-primitivity of shifted sets defined by a multiplicative property). Indeed, the set $\bar{\mathcal{M}}$ defined above is defined by a multiplicative property, thus $\bar{\mathcal{M}} + \{1\}$ is of the second type. On the other hand, clearly $\bar{m} \in \bar{\mathcal{M}}$ if and only if there are $x \in \mathbb{N}$, $y \in \mathbb{N}$ such that $\bar{m} = x^3y^2$, thus $\bar{\mathcal{M}} + \{1\}$ can be also considered as a shifted polynomial set:

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

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 $\ell \in \mathbb{N}$, ℓ is odd, and $\ell > 1$ then the set $\{x^2y^\ell + 1 : (x,y) \in \mathbb{N}^2\}$ is totally m-primitive? ... 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 this set by

$$(\bar{\mathcal{M}} + \{1\} =)\ \mathcal{D} = \{d_1, d_2, \dots\} \quad (\text{with } d_1 < d_2 < \dots).$$

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 $\mathcal{A}, \mathcal{B}, \mathcal{C}$ are fixed positive integers and $z \to \infty$ then the number of solutions 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, even the number of solutions is $o(z^{\varepsilon})$ for any $\varepsilon > 0$.)

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 for proving the *existence* of totally a-primitive subsets possessing certain prescribed properties. Let Φ denote the set of the a-reducible subsets of $\mathbb{N}_0$, define the mapping ϱ from the subsets of $\mathbb{N}_0$ into the interval $[0,1]$ so that for $\mathcal{A} = \{a_1, a_2, \dots\} \subset \mathbb{N}_0$ (with $a_1 < a_2 < \dots$) let

$$\varrho(\mathcal{A}) = \sum_{a_i \in \mathcal{A}} \frac{1}{2^{a_i+1}}$$

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

$$\varrho(\Gamma) = \{\varrho(\mathcal{A}) : \mathcal{A} \in \Gamma\},$$

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

$$\lambda(\varrho(\Phi)) = 0.$$

The next problem is to prove the multiplicative analog of this result. Let Ψ denote the set of the m-reducible subsets of $\mathbb{N}$, define the mapping σ from the subsets of $\mathbb{N}$ into the interval $[0,1)$ so that for $\mathcal{A} = \{a_1, a_2, \dots\} \subset \mathbb{N}$ (with $a_1 < a_2 < \dots$) let

$$\sigma(\mathcal{A}) = \sum_{a_i \in \mathcal{A}} \frac{1}{2^{a_i}},$$

if Γ is a set of subsets of $\mathbb{N}$ then let

$$\sigma(\Gamma) = \{\sigma(\mathcal{A}) : \mathcal{A} \in \Gamma\}.$$

Problem 6.9. *Is it true that*

$$\lambda(\sigma(\Psi)) = 0 \ ?$$

In [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*

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

Problem 6.11. *Is it true that*

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

References

[1] F. Beukers and H.-P. Schlickewei, *The equation $x + y = 1$ in finitely generated groups*, Acta Arith. **78** (1996), 189–199.

[2] C. Elsholtz, *The inverse Goldbach problem*, Mathematika **48** (2001), 151–158.

[3] C. Elsholtz, *Some remarks on the additive structure of the set of primes*, Number theory for the millenium, I (Urbana IL., 2000), 419–427, (Proceedings of the Millenial Conference on Number Theory (Bennett et al.), AK Peters, 2002.

[4] C. Elsholtz, *Multiplicative decomposability of shifted sets*, Bull. London Math. Soc. **40** (2008), 97–107.

[5] C. Elsholtz and A. J. Harper, *Additive decomposability of sets with restricted prime factors*, Trans. Amer. Math. Soc. **367** (2015), 7403–7427.

[6] J.-H. Evertse and K. Győry, *Unit Equations in Diophantine Number Theory*, Cambridge University Press, 2015.

[7] K. Győry, L. Hajdu and A. Sárközy, *On additive and multiplicative decompositions of sets of integers with restricted prime factors, I. (Smooth numbers.)*, Indag. Math. **32** (2021), 365–374.

[8] K. Győry, L. Hajdu and A. Sárközy, *On additive and multiplicative decompositions of sets of integers with restricted prime factors, II. (Smooth numbers and generalizations.)*, Indag. Math. **32** (2021), 812–823.

[9] K. Győry, L. Hajdu and A. Sárközy, *On additive and multiplicative decompositions of sets of integers composed from a given set of primes, I. (Additive decompositions.)*, Acta Arith. **202** (2022), 29–42.

[10] L. Hajdu and A. Sárközy, *On multiplicative decompositions of polynomial sequences, I*, Acta Arith. **184** (2018), 139–150.

[11] L. Hajdu and A. Sárközy, *On multiplicative decompositions of polynomial sequences, II*, Acta Arith. **186** (2018), 191–200.

[12] L. Hajdu and A. Sárközy, *On multiplicative decompositions of polynomial sequences, III*, Acta Arith. **193** (2020), 193–216.

[13] H.-H. Ostmann, *Additive Zahlentheorie*, Springer, Berlin, 1956.

[14] J. Rivat and A. Sárközy, *On arithmetic properties of products and shifted products*, Analytic Number Theory, In Honor of Helmut Maier's 60th Birthday, eds. C. Pomerance et al., Springer, 2015, 345–355.

[15] E. Wirsing, *Ein metrischer Satz über Mengen ganzer Zahlen*, Arch. Math. **4** (1953), 392–398.

K. Győry
University of Debrecen, Institute of Mathematics
H-4002 Debrecen, P.O. Box 400.
Hungary
Email address: gyory@science.unideb.hu

L. Hajdu
University of Debrecen, Institute of Mathematics
H-4002 Debrecen, P.O. Box 400.
and ELKH-DE Equations, Functions, Curves and their Applications Research Group
Hungary
Email address: hajdul@science.unideb.hu

A. Sárközy
Eötvös Loránd University, Institute of Mathematics
H-1117 Budapest, Pázmány Péter sétány 1/C
Hungary
Email address: sarkozy@cs.elte.hu