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

K. GYŐRY, L. HAJDU AND A. SÁRKÖZY

ABSTRACT. In earlier papers Elsholtz and Harper, and the authors of this paper studied additive and multiplicative decomposability of sets of integers with restricted prime factors. Here we sharpen some results of Elsholtz and Harper on the additive decomposability of such sets by extending them to sets composed from a given "thin" (finite or infinite) set of primes, and we also study the additive decomposability of sets composed from a "very dense" set of primes.

1. INTRODUCTION

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

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

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 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

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: May 24, 2021.

2010 *Mathematics Subject Classification.* 11P32, 11P70.

Key words and phrases. Additive decompositions, multiplicative decompositions, sets of integers with restricted prime factors, unit equations.

Research supported in part by the NKFIH grants K115479, K119528, K128088, and K130909, and by the projects EFOP-3.6.1-16-2016-00022 and EFOP-3.6.2-16-2017-00015 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* (1.1) *or* (1.2) *is* finite*, then the decomposition is called a* finite decomposition *or briefly* F-decomposition*, and we say that* (1.1) *and* (1.2) *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*.*

Definitions 1.2 and 1.4 have multiplicative analogs, as well; we shall need them in part II of this paper.

Definition 1.5. *Denote the greatest prime factor of the positive integer* n *by* $p^+(n)$*. Then* n *is said to be* smooth *(or* friable*) if* $p^+(n)$ *is "small" in terms of* n*. More precisely, if* $y = y(n)$ *is a monotone increasing function on* $\mathbb{N}$ *assuming positive values and* $n \in \mathbb{N}$ *is such that* $p^+(n) \leq y(n)$*, then we say that* n *is* y-smooth*.*

2. The problem and the theorems to be proved

Many papers have been written on the non-existence of a-decompositions and m-decompositions of certain special sequences; surveys of results of this type are presented in [3, 4, 8, 9]. In particular, in [4]

Elsholtz and Harper studied the a-decomposability of sets of smooth numbers (by using sieve methods), while in [6] and [7] the authors of this paper studied both a-decomposability of sets of smooth numbers and the multiplicative analog of this problem. Among others, in [4] Elsholtz and Harper proved:

Theorem A. *Let $\mathcal{P} = \{p_1, p_2, \dots, p_r\} \subset \mathbb{P}$ be any* finite *set of primes, and let*

$$\mathcal{R}(\mathcal{P}) = \{n \in \mathbb{N} : p \mid n \implies p \in \mathcal{P}\}. \tag{2.1}$$

Then $\mathcal{R}(\mathcal{P})$ is totally a-primitive.

(We use a terminology slightly different from the one used by them.) They also remarked that it follows from Theorem 7 of Tijdeman [11] that

Theorem B. *There exists an* infinite *set $\mathcal{P}$ of primes, such that defining $\mathcal{R}(\mathcal{P})$ again by* (2.1)*, the set $\mathcal{R}(\mathcal{P})$ is totally a-primitive.*

In this paper our main goal is to sharpen and extend these results by showing that if $\mathcal{P}$ is any "thin" set of primes, then the same conclusion holds:

Theorem 2.1. *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 is a number x_0 with*

$$P(x) < \frac{1}{51} \log\log x \quad \text{for } x > x_0 \tag{2.2}$$

(where $P(x) = |\mathcal{P} \cap [1, x]|$), then the set $\mathcal{R}(\mathcal{P})$ (defined by (2.1)*) is totally a-primitive.*

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), 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 primes. 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.

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 we have*

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

then $\mathcal{R}(\mathcal{P})$ is totally a-primitive.

By Theorem 2.1, $\mathcal{R}(\mathcal{P})$ is totally a-primitive if $\mathcal{P}$ is a "very thin" set of primes. A natural question to ask is that what happens if $\mathcal{P}$ is "very dense"? If $\mathcal{P}$ contains all the primes, i.e. $\mathcal{P} = \mathbb{P}$, then defining $\mathcal{R}(\mathcal{P})$ again by (2.1) we have

$$\mathcal{R}(\mathcal{P}) = \mathcal{R}(\mathbb{P}) = \mathbb{N}$$

which is clearly an a-reducible set. Thus one may guess that if $\mathcal{P}$ is a "very dense" set of primes, in other words, if $\mathcal{P} \subset \mathbb{P}$ is of the form

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

and $\mathcal{Q}$ is a "very thin" set of primes, then $\mathcal{R}(\mathcal{P})$ is always a-reducible. Indeed, we will prove this in the special case when $\mathcal{Q}$ is finite in the stronger form that then $\mathcal{R}(\mathcal{P})$ has an additive decomposition

$$\mathcal{R}(\mathcal{P}) = \mathcal{A} + \mathcal{B} \tag{2.4}$$

such that the cardinality of one of $\mathcal{A}$ and $\mathcal{B}$ can be anything:

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 $t \in \mathbb{N}_0$, $t \geq 2$, or $t = \infty$. Then $\mathcal{R}(\mathcal{P})$ has an a-F-decomposition*

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

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

We will also prove 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, $\mathcal{R}(\mathcal{P})$ need not have an a-F-decomposition of form (2.4):

Theorem 2.3. *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.*

There is a large gap between the cases of thin and dense sets of primes, occurring in Theorem 2.1 and Theorems 2.2 and 2.3, respectively. For sets of primes of positive density Elsholtz [2] gave upper bounds of possible decompositions, together with certain examples.

(In the second part of this paper we will study the *multiplicative* analogs of the problems considered here.)

3. Two lemmas needed in the proof of Theorem 2.1

The crucial tool in the proof of Theorem 2.1 will be a result on unit equations (as in [6, 7]):

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

(3.1)
$$\mathbb{Z}_{\mathcal{S}} = \left\{ \frac{a}{b} : a, b \in \mathbb{Z},\ ab \neq 0,\ (a,b) = 1,\ q \in \mathbb{P} \text{ and } q \mid ab \implies q \in \mathcal{S} \right\}.$$

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 [5], 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* (2.2), *then there are infinitely many* $k \in \mathbb{N}$ *such that*

$$\log p_{k+1} > 2^{51}(\log p_1 + \log p_2 + \cdots + \log p_k). \tag{3.2}$$

Proof. Assume that contrary to the statement of the lemma there is a positive integer k_0 such that for $k \in \mathbb{N}$, $k \geq k_0$ we have

(3.3)
$$\log p_{k+1} \leq 2^{51}(\log p_1 + \log p_2 + \cdots + \log p_k) \quad (\text{for } k = k_0, k_0 + 1, \dots).$$

Our goal is to deduce a contradiction from (3.3).

Let k_0 denote the smallest positive integer with

$$p_{k_0} > x_0$$

(where x_0 is the number defined in the theorem), and let K be a large positive integer, in particular, let $K > x_0$. (Note that here, indeed, K can be taken large since $\mathcal{P}$ is assumed to be infinite.) Now we will derive from (3.3) by induction on i that for

$$i = 0, 1, 2, \dots, K - k_0 \tag{3.4}$$

we have

$$\log p_{K+1} \leq 2^{51}(1 + 2^{51})^i(\log p_1 + \log p_2 + \cdots + \log p_{K-i}). \tag{3.5}$$

This holds trivially for $i = 0$ by (3.3) and since $K > k_0$ is assumed. Assume now that (3.5) holds for some

$$i \in \{0, 1, \dots, K - k_0 - 1\}. \tag{3.6}$$

Then by (3.3) (with $K-i-1$ in place of k), it follows from (3.5) that

$$\begin{aligned}\log p_{K+1} &\le 2^{51}(1+2^{51})^i((\log p_1+\log p_2+\cdots+\log p_{K-i-1})+\log p_{K-i}) = \\ &= 2^{51}(1+2^{51})^i((\log p_1+\log p_2+\cdots+\log p_{K-i-1})+ \\ &\quad +2^{51}(\log p_1+\log p_2+\cdots+\log p_{K-i-1})) = \\ &= 2^{51}(1+2^{51})^{i+1}(\log p_1+\log p_2+\cdots+\log p_{K-(i+1)})\end{aligned}$$

so that (3.5) also holds with $i+1$ in place of i, which proves that, indeed, (3.5) holds for every i satisfying (3.4). Thus, in particular, (3.5) holds with $K-k_0$ in place of i:

$$\log p_{K+1} \le 2^{51}(1+2^{51})^{K-k_0}(\log p_1+\log p_2+\cdots+\log p_{k_0}).$$

Taking the logarithm of both sides we get for $K\to\infty$ that

$$\log\log p_{K+1} \le K\log(1+2^{51})+O(1). \tag{3.7}$$

Now define X by

$$X = X(K) = p_{K+1}$$

so that by $K\to\infty$ we also have $X = X(K)\to\infty$. Then clearly

$$P(X) = K+1.$$

Thus it follows from (3.7) that for $K\to\infty$ (so that also $X\to\infty$) we have

$$\log\log X \le (P(X)-1)\log(1+2^{51})+O(1) < 50P(X)$$

which contradicts (2.2) if K and thus also $X = X(K)$ is large enough, and this completes the proof of Lemma 3.2. □

4. Completion of 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 $\mathcal{R} = \mathcal{R}(\mathcal{P})$ (defined by (2.1)) is *not* totally a-primitive, so that there are a number $n_0\in\mathbb{N}$ and sets $\mathcal{R}'\subset\mathbb{N}$,

$$\mathcal{A} = \{a_1, a_2, \dots\}\subset\mathbb{N}_0, \quad \mathcal{B} = \{b_1, b_2, \dots\}\subset\mathbb{N}_0$$

(with $a_1 < a_2 < \dots$, $b_1 < b_2 < \dots$) such that

$$\mathcal{R}'\cap[n_0,\infty) = \mathcal{R}\cap[n_0,\infty), \tag{4.1}$$

$$\mathcal{R}' = \mathcal{A}+\mathcal{B} \tag{4.2}$$

and

$$|\mathcal{A}|\ge 2, \quad |\mathcal{B}|\ge 2. \tag{4.3}$$

If $\mathcal{P}$ is finite, then by Theorem A there are no n_0, $\mathcal{R}'$, $\mathcal{A}$, $\mathcal{B}$ with these properties, thus it suffices to study the case when

$$\mathcal{P} \text{ is infinite.} \tag{4.4}$$

By the definition of $\mathcal{P}$ and (4.4), we may apply Lemma 3.2. Then we obtain that there are infinitely many $k \in \mathbb{N}$ which satisfy (3.2). Let K be such an integer large enough so that

$$\log p_{K+1} > 2^{51}(\log p_1 + \log p_2 + \cdots + \log p_K) \tag{4.5}$$

and, in particular, let

$$p_K > n_0. \tag{4.6}$$

Write $m = \max(a_2, b_2)$. Then by (4.1), (4.2) and (4.6) we have

$$\mathcal{R} \cap [n_0, p_{K+1} - m] = \mathcal{R}' \cap [n_0, p_{K+1} - m] \subset$$
$$\subset (\mathcal{A} \cap [0, p_{K+1} - m]) + (\mathcal{B} \cap [0, p_{K+1} - m])$$

whence

$$|\mathcal{R} \cap [n_0, p_{K+1} - m]| \le A(p_{K+1} - m) \cdot B(p_{K+1} - m). \tag{4.7}$$

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

$$A(p_{K+1} - m) \le B(p_{K+1} - m).$$

Then it follows from (4.7) that for K large enough we have

$$B(p_{K+1} - m) \ge |\mathcal{R} \cap [n_0, p_K - m]|^{1/2} \ge \tag{4.8}$$
$$\ge (|\mathcal{R} \cap [0, p_{K+1}]| - m - n_0)^{1/2} > \frac{1}{2}(R(p_{K+1}))^{1/2}$$

since $\mathcal{R}$ is infinite. Now we define the set $\tilde{\mathcal{R}}$ so that $r \in \tilde{\mathcal{R}}$ if and only if r is of the form

$$r = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_K^{\alpha_K} \quad (\text{for all } r \in \tilde{\mathcal{R}}) \tag{4.9}$$

with

$$\alpha_i \in \{0, 1, \ldots, 2^{50}\} \quad \text{for } i = 1, 2, \ldots, K. \tag{4.10}$$

Then by (4.5), (4.9) and (4.10), clearly for all $r \in \tilde{\mathcal{R}}$ and K large enough we have

(4.11)
$$r = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_K^{\alpha_K} \le (p_1 p_2 \cdots p_K)^{2^{50}} = e^{2^{50}(\log p_1 + \log p_2 + \ldots + \log p_K)} <$$
$$< e^{\frac{1}{2}\log p_{K+1}} = p_{K+1}^{1/2} < p_{K+1} - m \quad (\text{for all } r \in \tilde{\mathcal{R}}).$$

It follows from (4.9) and (4.11) that

$$\tilde{\mathcal{R}} \subset \mathcal{R} \cap [0, p_{K+1} - m - 1]$$

whence

$$|\tilde{\mathcal{R}}| \leq R(p_{K+1} - m - 1). \tag{4.12}$$

By (4.9) and (4.10) clearly we have

$$|\tilde{\mathcal{R}}| = \left(2^{50} + 1\right)^K. \tag{4.13}$$

It follows from (4.8), (4.12) and (4.13) that for K large enough we have

$$\begin{aligned} B(p_{K+1} - m) > \frac{1}{2}(R(p_{K+1}))^{1/2} \geq \frac{1}{2}(R(p_{K+1} - m - 1))^{1/2} \geq \\ \geq \frac{1}{2}(|\tilde{\mathcal{R}}|)^{1/2} = \frac{1}{2}\left(2^{50} + 1\right)^{K/2} > 2^{24K}. \end{aligned} \tag{4.14}$$

Now we will complete the proof of Theorem 2.1 by showing that this lower bound for $B(p_{K+1} - m)$ contradicts the statement of Lemma 3.1. Write

$$\mathcal{B}' = \mathcal{B} \cap (n_0, p_{K+1} - m). \tag{4.15}$$

By (4.1), (4.2), (4.3) and (4.15), for all

$$b \in \mathcal{B}' \tag{4.16}$$

and $i = 1, 2$ we have

(4.17)

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

and

$$a_i + b \in \mathcal{R} \cap (n_0, p_{K+1}) \quad (\text{for } i = 1, 2). \tag{4.18}$$

Define $x \in \mathbb{N}$ and $y \in \mathbb{N}$ by

$$a_1 + b = x \tag{4.19}$$

and

$$a_2 + b = y \tag{4.20}$$

so that we have

$$y - x = a_2 - a_1. \tag{4.21}$$

Now write $\mathcal{S} = \{p_1, p_2, \ldots, p_K\}$. Then by the definition of $\mathcal{R}$ and (4.18), both x in (4.19) and y in (4.20) are composed from the primes in $\mathcal{S}$ so that by (3.1) we have

$$x, y \in \mathbb{Z}_{\mathcal{S}}. \tag{4.22}$$

(4.21) and (4.22) form an S-unit equation (as defined in Lemma 3.1), and x, y in (4.19) and (4.20) is a solution of this equation for every b satisfying (4.16), so that this equation must have at least $|\mathcal{B}'|$ solutions. By (4.14) and (4.15), for K large enough we have

$$|\mathcal{B}'| = |\mathcal{B} \cap (n_0, p_{K+1} - m)| \geq B(p_{K+1} - m - 1) - B(n_0) \geq \tag{4.23}$$
$$\geq B(p_K - m) - 1 - (n_0 + 1) > 2^{24K} - n_0 - 2 > 2^{23K},$$

so that the S-unit equation formed by (4.21) and (4.22) has more than 2^{23K} solutions.

On the other hand, by Lemma 3.1, for K large enough this equation may have only at most

$$2^{16(s+1)} = 2^{16(K+1)} < 2^{17K}$$

solutions, which is smaller, than the lower bound 2^{23K} for the number of solutions obtained in (4.23), and this contradiction completes the proof of Theorem 2.1. □

5. Proof of Theorem 2.2

We will need the following lemma:

Lemma 5.1. *For $m \in \mathbb{N}$, $m \geq 2$ and for $0 \leq h < m$ write*

$$\mathcal{N}_h = \{n \in \mathbb{N}_0 : n \equiv h \pmod{m}\}.$$

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

$$\mathcal{N}_{\mathcal{H}} := \bigcup_{h \in \mathcal{H}} \mathcal{N}_h$$

is a-reducible. Moreover, for any $t \in \mathbb{N}$ with $2 \leq t \leq \infty$ there exists a set $\mathcal{B}_t \subset \mathbb{N}_0$ such that $|\mathcal{B}_t| = t$ and we have

$$\mathcal{N}_{\mathcal{H}} = \mathcal{N}_{\mathcal{H}} + \mathcal{B}_t. \tag{5.1}$$

Proof. Observe that for any $\mathcal{B} \subset \mathcal{N}_0$ with $0 \in \mathcal{B}$ we have

$$\mathcal{N}_{\mathcal{H}} = \mathcal{N}_{\mathcal{H}} + \mathcal{B}.$$

Thus (5.1) holds if $\mathcal{B}_t$ is any set with $0 \in \mathcal{B}_t$, $|\mathcal{B}_t| = t$. The statement of the lemma follows from this. □

To complete the proof of Theorem 2.2, observe first that if $\mathcal{Q} = \emptyset$, then $\mathcal{P} = \mathbb{P}$ in (2.3) so that $\mathcal{R}(\mathcal{P}) = \mathbb{N}$ thus the claim is trivial. Thus we may assume that $\mathcal{Q} \neq \emptyset$; let $\mathcal{Q} = \{p_1, p_2, \ldots, p_k\}$. Then we have

$$\mathcal{R}(\mathcal{P}) = \{n : n \not\equiv 0 \pmod{p_i} \text{ for } i = 1, \ldots, k\}.$$

Thus $\mathcal{R}(\mathcal{P})$ is the union of those residue classes modulo $m = p_1 p_2 \cdots p_k$ whose elements are coprime with m, so that Lemma 5.1 can be applied

with $\mathcal{R}(\mathcal{P})$ in place of $\mathcal{N}_{\mathcal{H}}$, and then applying the lemma the result follows. □

6. Proof of Theorem 2.3

Let $f(n)$ be a function satisfying the assumptions in the theorem. We will define the set $\mathcal{Q}$ in (2.3) by recursion. Let $t_2 \in \mathbb{N}$ be any number with $f(t_2) > 2$, and let the first two elements of $\mathcal{Q}$ be any primes p_1, p_2 with $t_2 < p_1 < p_2$. Now assume that $k \in \mathbb{N}$, $k \geq 1$, and the primes $p_1, p_2, \dots, p_{2k}$ have been defined. Then let $t_{2k+2} \in \mathbb{N}$ be any number with $f(t_{2k+2}) > 2k+2$, and let p_{2k+1}, p_{2k+2} be any primes satisfying

$$\max\left(t_{2k+2}, \prod_{i=1}^{2k} p_i\right) < p_{2k+1} < p_{2k+2}. \tag{6.1}$$

Let $\mathcal{Q} = \{p_1, p_2, \dots\}$ and define $\mathcal{P}$ by (2.3). Then clearly $\mathcal{Q}$ is infinite and $Q(n) < f(n)$ for all $n \in \mathbb{N}$.

Now we will show that $\mathcal{R}(\mathcal{P})$ is totally a-F-primitive. First we prove the following property: for any $k \in \mathbb{N}$ the set $\mathcal{R}(\mathcal{P})$ contains a "k-*isolated*" element, i.e. an

$$r \in \mathcal{R}(\mathcal{P}) \text{ with } r > k \text{ and } r \pm i \notin \mathcal{R}(\mathcal{P}) \text{ for } i = 1, 2, \dots, k. \tag{6.2}$$

To prove this, fix k, and consider the following linear congruence system:

$$\begin{cases} x \equiv i \pmod{p_i} & (\text{for } i = 1, 2, \dots, k), \\ x \equiv -i \pmod{p_{k+i}} & (\text{for } i = 1, 2, \dots, k). \end{cases} \tag{6.3}$$

By the Chinese remainder theorem this system is solvable, and writing $M_k := \prod_{i=1}^{2k} p_i$, there is a unique solution r_k with $1 \leq r_k \leq M_k$. Let

$$p_j \in \mathcal{Q} \tag{6.4}$$

with some $j \in \mathbb{N}$.

If $j > 2k$, then by (6.1) we have

$$p_j \geq p_{2k+1} > \prod_{i=1}^{2k} p_i = M_k \geq r_k$$

thus $p_j \nmid r_k$. On the other hand, if $1 \leq j \leq 2k$, then we have

$$p_j > j \tag{6.5}$$

(since p_j is at least as large as the j-th prime, which is at least as large as $j+1$). By the definition of r_k, (6.3) and $j \leq 2k$, we also have either $p_j \mid r_k - j$ or $p_j \mid r_k + j$; by (6.5), in both cases it follows again that

$p_j \nmid r_k$. Thus r_k has no prime divisor satisfying (6.4), so that by (2.3), all the prime factors of r_k belong to $\mathcal{P}$, thus $r_k \in \mathcal{R}(\mathcal{P})$. Moreover, r_k is a solution of (6.3) thus $r_k - i \neq 1$ for $i = 1, 2, \ldots, k$ whence $r_k > k$, and it also follows from (6.3) (with r_k in place of x) that $r_k \pm i \notin \mathcal{R}(\mathcal{P})$ for $i = 1, 2, \ldots, k$. So that all the requirements in (6.2) hold with r_k in place of r thus, indeed, r_k is a k-isolated element in $\mathcal{R}(\mathcal{P})$.

Now assume that contrary to the statement of Theorem 2.3, $\mathcal{R}(\mathcal{P})$ is *not* totally a-F-primitive, i.e. there exist $\mathcal{R}' \subset \mathbb{N}_0$, $\mathcal{A} \subset \mathbb{N}_0$, $\mathcal{B} \subset \mathbb{N}_0$ and $n_0 \in \mathbb{N}$ such that

$$\mathcal{R}' \cap [n_0, \infty) = \mathcal{R}(\mathcal{P}) \cap [n_0, \infty), \tag{6.6}$$

$$\mathcal{R}' = \mathcal{A} + \mathcal{B}, \quad 2 \leq |\mathcal{A}|, \quad 2 \leq |\mathcal{B}| < \infty. \tag{6.7}$$

We will derive a contradiction from these assumptions. Write $\mathcal{B} = \{b_1 < b_2 < \cdots < b_m\}$ (with $m \geq 2$). Let

$$k = n_0 + b_m, \tag{6.8}$$

and let r be a k-isolated element of $\mathcal{R}(\mathcal{P})$ satisfying (6.2). Then by (6.2), (6.6), (6.7) and (6.8) we have $r \in \mathcal{R}'$, and there are $a \in \mathcal{A}$, $b_i \in \mathcal{B}$ such that

$$r = a + b_i.$$

Consider any $b_j \in \mathcal{B}$ with $j \neq i$, and write

$$r' = a + b_j.$$

Then $r' \neq r$, and it follows from (6.7) that we have

$$r' \in \mathcal{R}'. \tag{6.9}$$

Observe that then by (6.2) and (6.8) we have

$$\begin{aligned} r' = r + b_j - b_i > k + b_j - b_i = (n_0 + b_m) + b_j - b_i = \\ = n_0 + b_j + (b_m - b_i) \geq n_0 + b_j \geq n_0, \end{aligned}$$

so that by (6.6) and (6.9), $r' \in \mathcal{R}(\mathcal{P})$. However, $r \neq r'$ by $b_j \neq b_i$, moreover, by (6.8),

$$(0 <)|r' - r| = |b_j - b_i| \leq \max(b_j, b_i) \leq b_m \leq k$$

which contradicts the fact that r is k-isolated in $\mathcal{R}(\mathcal{P})$. $\square$

7. Further remarks, problems and conjectures

In Theorems 2.1, 2.2 and 2.3 we have studied only the extreme cases when the set $\mathcal{P}$ of primes generating $\mathcal{R}(\mathcal{P})$ is very thin (its counting function $P(x)$ is such that $P(x) \ll \log\log x$ and then $\mathcal{R}(\mathcal{P})$ is totally a-primtive) or it is very dense (it is of the form (2.3) where $\mathcal{Q}$ is either finite when $\mathcal{R}(\mathcal{P})$ is always a-F-reducible or it is "almost finite"). It is a natural question to ask: what happens if $\mathcal{P}$ is between these two extreme cases? As the density of $\mathcal{P}$ increases from very small to very large so that $\mathcal{R}(\mathcal{P})$ changes from totally a-primitive to a-reducible, then how and when does this change happen, and what can one say on the a-decomposability of $\mathcal{R}(\mathcal{P})$ for a "typical" (randomly chosen) set $\mathcal{P}$ midway? It seems hopeless to give a more or less complete answer to these questions but, at least, we may formulate some guesses what to expect and we may propose some problems to study for making initial steps toward the direction guessed.

Theorems 2.2 and 2.3 inspire the following problem:

Problem 7.1. *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*

a) *$\mathcal{R}(\mathcal{P})$ (defined by (2.1)) is totally a-F-primitive?*
b) *$\mathcal{R}(\mathcal{P})$ is totally a-primitive?*

We conjecture that the answer is affirmative in both cases, however, to prove this seems to be difficult in case a), and even more difficult in case b). The first step in this direction could be to settle the following (slightly easier) problems:

Problem 7.2. *Does a set $\mathcal{P} \subset \mathbb{P}$ exist such that its counting function $P(x)$ satisfies $P(x)/\log\log x \to \infty$ and $\mathcal{R}(\mathcal{P})$ is*

a) *totally a-F-primitive?*
b) *totally a-primitive?*

For sure the answer is affirmative in both cases (even we think that the counting function of such a set $\mathcal{P}$ may increase much faster than $\log\log x$ in both cases), and of course if this is shown in case b), then this implies that it is so in case a) as well; however, it seems much easier to handle case a).

A much more difficult version of this problem is the following:

Problem 7.3. *Is it true that there are functions $f(x)$, $g(x)$ with $f(x)/\log\log x \to \infty$ and $g(x)/\log\log x \to \infty$ such that for every $\mathcal{P} \subset \mathbb{P}$*

a) *with $P(x) \ll f(x)$ the set $\mathcal{R}(\mathcal{P})$ is a-F-primitive?*
b) *with $P(x) \ll g(x)$ the set $\mathcal{R}(\mathcal{P})$ is a-primitive?*

Again, we think that the answer is affirmative in both cases, but to show this, probably one needs different approach (we remark that Lemma 3.1 is sharp apart from constant factors).

Moreover, we remark that the natural approach to prove the affirmative answer to the questions in Problem 7.2 would be to give *constructive* proofs. However, there is another different approach using *measure theory* which may function more efficiently in some cases: instead of *constructing* sets $\mathcal{P}$ with the desired properties, we may give *existence proofs* by showing that there are *many sets* possessing these properties. To use such approach we may start out from results of Volkmann [12, 13], Wirsing [14] and the third author [10].

Let Σ denote the set of the subsets of $\mathbb{N}_0$, Σ_2 the set of the subsets in Σ that have at least two elements, and Σ_∞ the set of the infinite subsets in Σ. Let Φ denote the set of the a-reducible sets in Σ, so that $\Phi = \Sigma_2 + \Sigma_2$. To study subsets (defined by additive properties) in Σ by using measure theory, Wirsing proposed to consider the usual mapping of Σ into the interval $[0, 1]$: for $\mathcal{A} = \{a_1, a_2, \dots\} \in \Sigma$ (with $a_1 < a_2 < \dots$) let

$$\varrho(\mathcal{A}) = \sum_{a_i \in \mathcal{A}} \frac{1}{2^{a_i+1}}. \tag{7.1}$$

(Clearly, (7.1) defines a one-to-one mapping between the *infinite* sets $\mathcal{A} \in \Sigma$ and the points in the interval $(0, 1]$.) For $\Gamma \subset \Sigma$ we will write

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

For $S \subset [0, 1]$ let $\lambda(S)$ denote the Lebesgue measure of S, while the Hausdorff dimension of S will be denoted by $\dim S$. (The definition and some basic properties of the Hausdorff dimension are presented in [10]. In particular, for all $S \subseteq T \subseteq [0, 1]$ we have

$$0 \le \dim S \le \dim T \le \dim[0, 1] = 1,$$

and if $S \subset [0, 1]$ and $\dim S < 1$, then $\lambda(S) = 0$.)

In [14] Wirsing proved:

Theorem C. *We have*

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

So that, in terms of the Lebesgue measure, almost all $x \in [0, 1]$ are such that if $\varrho(\mathcal{A}) = x$ (with an infinite $\mathcal{A}$), then $\mathcal{A}$ is a-primitive (and it would be easy to see that here "a-primitive" can be replaced by "totally a-primitive"); thus we may briefly say that $\mathcal{A}$ *is (totally) a-primitive for almost all* $\mathcal{A} \in \Sigma$.

In [13] Volkmann gave a different proof for Theorem C and he also gave upper bounds for the Hausdorff dimension of $\varrho(S)$ for certain special subsets S of Φ. The third author [10] sharpened these results of Wirsing and Volkmann by proving

Theorem D. *We have*

$$\dim \varrho(\Phi) < 1 - 10^{-3}.$$

In [12] Volkmann gave a lower bound for $\dim \varrho(\Phi)$:

Theorem E. *We have*

$$\dim \varrho(\Phi) \geq \dim \varrho(\{0,1\} + \Sigma_2) = \frac{\log \gamma}{\log 2} \left(> \frac{4}{5} \right)$$

where γ is the (single) positive solution of the equation

$$z^3 - 2z^2 + z - 1 = 0.$$

In [10] it was also shown that

Theorem F. *We have*

$$\dim \varrho(\Sigma_\infty + \Sigma_\infty) \geq \frac{1}{3}.$$

The remark after Theorem C inspires the following question: is it true that $\mathcal{R}(\mathcal{P})$ is (totally) a-primitive for almost all $\mathcal{P} \subset \mathbb{P}$? We conjecture that the answer is affirmative. To formulate this conjecture more precisely, we have to introduce some more notation. Let Ψ denote the set of those sets $\mathcal{P} \subset \mathbb{P}$ for which $\mathcal{R}(\mathcal{P})$ is a-reducible:

$$\Psi = \{\mathcal{P} \subset \mathbb{P} : \mathcal{R}(\mathcal{P}) \in \Sigma_2 + \Sigma_2\}.$$

Moreover, we have to replace the mapping $\varrho : \Sigma \to [0,1]$ in (7.1) by the mapping $\eta : \mathbb{P} \to [0,1]$ defined so that if $\mathcal{P} \subset \mathbb{P}$ and q_i denotes the i-th prime: $q_1 = 2, q_2 = 3, q_3 = 5, \ldots$, then let

$$\eta(\mathcal{P}) = \sum_{i : q_i \in \mathcal{P}} \frac{1}{2^{i+1}},$$

and for $\Gamma \subset \mathbb{P}$ let $\eta(\Gamma)$ be the set consisting of the points $\eta(\mathcal{P})$ with $\mathcal{P} \in \Gamma$:

$$\eta(\Gamma) = \{\eta(\mathcal{P}) : \mathcal{P} \in \Gamma\}.$$

In Theorems C,D,E,F (and in other results in [10, 12, 13, 14] and in some related papers) subsets of Σ defined by additive properties are studied by using the mapping ϱ and measure theory; one might like to study the "$\mathbb{P}$, η analogs" of these "Σ, ϱ problems". However, it seems to be more difficult to handle the $\mathbb{P}$, η problems, than their Σ, ϱ

analogs, thus we will ease the Σ, ϱ problems slightly when formulating their $\mathbb{P}$, η analogs.

The first $\mathbb{P}$, η problem of this type to attack is certainly the following one:

Problem 7.4. *Is it true that*

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

We conjecture that this is true, perhaps even $\dim \eta(\Psi) < 1$ holds but this seems to be much more difficult to prove.

Theorems E and F inspire the following two problems:

Problem 7.5. *Is it true that*

$$\dim \eta(\{\mathcal{P} \subset \mathbb{P} : \mathcal{R}(\mathcal{P}) \in \{0,1\} + \Sigma_2\}) > 0 \ ?$$

Problem 7.6. *Is it true that*

$$\dim \eta(\{\mathcal{P} \subset \mathbb{P} : \mathcal{R}(\mathcal{P}) \in \Sigma_\infty + \Sigma_\infty\}) > 0 \ ?$$

Probably the answer to the questions in both Problem 7.5 and Problem 7.6 is affirmative; one might like to give lower bounds for the dimensions in both cases but it seems to be hopelessly difficult to determine their exact values.

8. Acknowledgement

The authors are grateful to the Referee for the insightful and helpful remarks.

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, *Additive decomposability of multiplicatively defined sets*, Func. et Approx. **35** (2006), 61–77.

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

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

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

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

[7] K. Győry, L. Hajdu, A. Sárközy, *On additive and multiplicative decompositions of sets of integers with restricted prime factors, II. (Smooth numbers and generalizations.)* (submitted).

[8] L. Hajdu and A. Sárközy, *On multiplicative decompositions of polynomial sequences, I*, Acta Arith. **184** (2018), 139–150.
[9] L. Hajdu and A. Sárközy, *On multiplicative decompositions of polynomial sequences, III*, Acta Arith. **193** (2020), 193–216.
[10] A. Sárközy, *Some metric problems in the additive number theory, I.*, Annales Univ. Sci. Budapest Eötvös, Sectio Math. **19** (1976), 107–127.
[11] R. Tijdeman, *On integers with many small prime factors*, Compositio Math. **26** (1973), 319–330.
[12] B. Volkmann, *Über Klassen von Mengen natürlicher Zahlen*, Crelle J. **190** (1952), 199–230.
[13] B. Volkmann, *Über die Klasse der Summenmengen*, Arch. Math. **6** (1955), 200–207.
[14] E. Wirsing, *Ein metrischer Satz über Mengen ganzer Zahlen*, Arch. Math. **4** (1953), 392–398.

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