# ON ADDITIVE AND MULTIPLICATIVE DECOMPOSITIONS OF SETS OF INTEGERS WITH RESTRICTED PRIME FACTORS, II. (SMOOTH NUMBERS AND GENERALIZATIONS.)

K. GYŐRY, L. HAJDU AND A. SÁRKÖZY

Abstract. In part I of this paper we studied additive decomposability of the set $\mathcal{F}_y$ of th $y$-smooth numbers and the multiplicative decomposability of the shifted set $\mathcal{G}_y = \mathcal{F}_y + \{1\}$. In this paper, focusing on the case of 'large' functions $y$, we continue the study of these problems. Further, we also investigate a problem related to the m-decomposability of $k$-term sumsets, for arbitrary $k$.

## 1. Introduction

First we recall some notation, definitions and results from part I of this paper [6] which we all also need here.

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

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

The set of the positive integers is denoted by $\mathbb{N}$, and we write $\mathbb{N}\cup\{0\} = \mathbb{N}_0$. The set of rational numbers is denoted by $\mathbb{Q}$.

We will need

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

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

*If*

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

*Date*: November 30, 2020.

2010 *Mathematics Subject Classification.* 11P45, 11P70.

*Key words and phrases.* Additive decompositions, multiplicative decompositions, smooth (friable) numbers, $S$-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.

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

**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

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

*(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*.*

**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*.*

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

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

*(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*.*

**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*.*

**Definition 1.7.** *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, and we write* $\mathcal{F}_y$ *(*$\mathcal{F}$ *for "friable") for the set of all* $y$*-smooth positive integers.*

Starting out from a conjecture of the third author [11] and a related partial result of Elsholtz and Harper [2], in [6] we proved the following two theorems:

**Theorem A.** *If* $y(n)$ *is an increasing function with* $y(n) \to \infty$ *and*

$$y(n) < 2^{-32} \log n \quad \text{for large } n, \tag{1.4}$$

*then the set* $\mathcal{F}_y$ *is totally* a-primitive*.*

(If $y(n)$ is increasing then the set $\mathcal{F}_y$ is m-reducible since $\mathcal{F}_y = \mathcal{F}_y \cdot \mathcal{F}_y$, and we also have $\mathcal{F}_y \sim \mathcal{F}_y \cdot \{1, 2\}$, thus if we want to prove an *m-primitivity* theorem involving $\mathcal{F}_y$ then we have to switch from $\mathcal{F}_y$ to the shifted set

$$\mathcal{G}_y := \mathcal{F}_y + \{1\}. \tag{1.5}$$

See also [1].)

**Theorem B.** *If $y(n)$ is defined as in Theorem 1.1, then the set $\mathcal{G}_y$ is totally m-primitive.*

Here our goal is to prove further related results. First we will prove a theorem in the direction opposite to the one in Theorem A. Indeed, we will show that if $y(n)$ grows faster than $n/2$, then $\mathcal{F}_y$ is *not* totally a-primitive.

**Theorem 1.1.** *Let $y(n)$ be any monotone increasing function on $\mathbb{N}$ with*

$$\frac{n}{2} < y(n) < n \quad \textit{for all } n \in \mathbb{N}.$$

*Then $\mathcal{F}_y$ is* not *totally a-primitive. In particular, in this case the set*

$$\mathcal{F}_y \cap [9, +\infty)$$

*is a-reducible, namely, we have*

$$\mathcal{F}_y \cap [9, +\infty) = \mathcal{A} + \mathcal{B}$$

*with*

$$\mathcal{A} = \{n \in \mathbb{N} : \textit{none of } n, n+1, n+3, n+5 \textit{ is prime}\}, \ \mathcal{B} = \{0, 1, 3, 5\}.$$

Next we will show that under a standard conjecture, the decomposition in Theorem 1.1 is best possible in the sense that no such decomposition is possible with $2 \le |\mathcal{B}| \le 3$. For this, we need to formulate the so-called prime $k$-tuple conjecture. A finite set $A$ of integers is called admissible, if for any prime $p$, no subset of $A$ forms a complete residue system modulo $p$.

**Conjecture 1.1** (The prime $k$-tuple conjecture)**.** *Let $\{a_1, \dots, a_k\}$ be an admissible set of integers. Then there exist infinitely many positive integers $n$ such that $n + a_1, \dots, n + a_k$ are all primes.*

**Remark.** By a recent, deep result of Maynard [8] we know that for each $k$, the above conjecture holds for a positive proportion of admissible $k$-tuples. We also mention that if the prime $k$-tuple conjecture is true, then there exist infinitely many $n$ such that $n + a_1, \dots, n + a_k$ are *consecutive* primes (see e.g. the proof of Theorem 2.4 of [7]).

**Theorem 1.2.** *Define $y(n)$ as in Theorem 1.1 and suppose that the prime $k$-tuple conjecture is true for $k = 2, 3$. Then for any $\mathcal{C} \subset \mathbb{N}$ with $\mathcal{C} \sim \mathcal{F}_y$ there is no decomposition of the form*

$$\mathcal{C} = \mathcal{A} + \mathcal{B}$$

*with*

$$2 \leq |\mathcal{B}| \leq 3.$$

We propose the following problem, which is a shifted, multiplicative analogue of the question studied in Theorems 1.1 and 1.2.

**Problem.** With the same $y = y(n)$ as in Theorem 1.1, write

$$\mathcal{G}_y = \mathcal{F}_y + \{1\} = \{m + 1 : m \in \mathcal{F}_y\}.$$

Is the set $\mathcal{G}_y$ totally m-primitive?

Towards the above problem, we prove that no appropriate decomposition is possible with $|\mathcal{B}| < +\infty$.

**Theorem 1.3.** *Let $y(n)$ be as in Theorem 1.1. Then for any $\mathcal{C} \subset \mathbb{N}$ with $\mathcal{C} \sim \mathcal{G}_y$ there is no decomposition of the form*

$$\mathcal{C} = \mathcal{A} \cdot \mathcal{B}$$

*with*

$$|\mathcal{B}| < +\infty.$$

Let

$$\Gamma := \{n_1, \ldots, n_s\}$$

be a set of pairwise coprime positive integers $> 1$, and let $\{\Gamma\}$ be the multiplicative semigroup generated by $\Gamma$, with $1 \in \{\Gamma\}$. If in particular, $n_1, \ldots, n_s$ are distinct primes, then we use the notation $\Gamma = S$, and $\{\Gamma\} = \{S\}$ is just the set of positive integers composed of the primes from $S$.

The next theorem shows that if $\Gamma$ is finite, then the sets of $k$-term and at most $k$-term sums of pairwise coprime elements of $\{\Gamma\}$ are totally m-primitive. For the precise formulation of the statement, write $H_1 := \{\Gamma\}$, and for $k \geq 2$ set

$$H_k := \{u_1 + \cdots + u_k : \ u_i \in \{\Gamma\}, \ \gcd(u_i, u_j) = 1 \text{ for } 1 \leq i < j \leq k\}$$

and

$$H_{\leq k} := \bigcup_{\ell=1}^{k} H_\ell.$$

**Theorem 1.4.** *Let $k \geq 2$. Then both $H_k$ and $H_{\leq k}$ are totally m-primitive, apart from the only exception exception of the case $\Gamma = \{2\}$ and $k = 3$, when we have*

$$H_{\leq 3} = \{1, 2\} \cdot \{2^\beta, 2^\beta + 1 : \beta \geq 0\}.$$

**Remark.** As we have

$$\{\Gamma\} = \{\Gamma\} \cdot \{\Gamma\},$$

the assumption $k \geq 2$ is clearly necessary. Further, the coprimality assumption in the definition of $H_k$ cannot be dropped. Indeed, letting

$$H_k^* := \{u_1 + \cdots + u_k : \ u_i \in \{\Gamma\} \text{ for } 1 \leq i \leq k\}$$

and

$$H_{\leq k}^* := \bigcup_{\ell=1}^{k} H_\ell^*$$

we clearly have

$$H_k^* = \{\Gamma\} \cdot H_k^* \quad \text{and} \quad H_{\leq k}^* = \{\Gamma\} \cdot H_{\leq k}^*.$$

## 2. Proof of Theorem 1.1

By the choice of $y(n)$ we see that $\mathcal{F}_y$ is the set of all composite integers. Put

$$\mathcal{C} = \mathcal{F}_y \cap [9, +\infty).$$

We show that by the definition of $\mathcal{A}$ and $\mathcal{B}$ as in the theorem, we have

$$\mathcal{C} = \mathcal{A} + \mathcal{B}.$$

To see this, first observe that by the assumptions on $\mathcal{A}$ and $\mathcal{B}$, all the elements of $\mathcal{A} + \mathcal{B}$ are composite. So we only need to check that all composite numbers $n$ with $n \geq 9$ belong to $\mathcal{A} + \mathcal{B}$. If $n$ is an odd composite number, then by $n \in \mathcal{A}$ we have

$$n \in (\mathcal{A} + \mathcal{B}). \tag{2.1}$$

So assume that $n$ is an even composite number with $n \geq 10$. Then one of $n-1, n-3, n-5$ is *not* a prime. As this number is clearly in $\mathcal{A}$, we have (2.1) again and our claim follows. □

## 3. Proof of Theorem 1.2

Let $\mathcal{C} \subset \mathbb{N}$ with $\mathcal{C} \sim \mathcal{F}_y$. Then, as we noted in the proof of Theorem 1.1, with some positive integer $n_0$ we have

$$\mathcal{C} \cap [n_0, +\infty) = \{n \in \mathbb{N} : n \geq n_0 \text{ and } n \text{ is composite}\}.$$

We handle the cases $k = 2$ and 3 separately.

Let first $k = 2$, that is assume that contrary to the assertion of the theorem the set $\mathcal{C}$ can be represented as

$$\mathcal{C} = \mathcal{A} + \mathcal{B} \tag{3.1}$$

with $|\mathcal{B}| = 2$. Set $B = \{b_1, b_2\}$. Clearly, without loss of generality we may assume that $b_1 < b_2$ and also that $b_1 = 0$. Indeed, the first assumption is trivial, and the second one can be made since (3.1) implies that

$$\mathcal{C} = \mathcal{A}^* + \{0, b_2 - b_1\}$$

with

$$\mathcal{A}^* = \mathcal{A} + \{b_1\} = \{a + b_1 : a \in \mathcal{A}\}.$$

As the set $\{-b_2, b_2\}$ is admissible, by our assumption on the validity of Conjecture 1.1 we get that there exist infinitely many integers $n$ such that $n - b_2$ and $n + b_2$ are both primes. In view of the Remark after Conjecture 1.1, we may assume that these primes are consecutive, that is, in particular, $n$ is composite. Observe that then, assuming that $n \geq n_0 + b_2$, we have $n - b_2 \notin \mathcal{A}$ and $n \notin \mathcal{A}$. Indeed, otherwise by the primality of $n - b_2$ and $n + b_2$, respectively, we get a contradiction: in case of $n - b_2 \in \mathcal{A}$ we have $n - b_2 \in \mathcal{C}$, while $n + b_2 \in \mathcal{A}$ implies that $n + b_2 \in \mathcal{C}$. But then we get $n \notin \mathcal{C}$, which is a contradiction.

Let now $k = 3$, that is assume that we have (3.1) with some $\mathcal{B}$ with $|\mathcal{B}| = 3$. Write $\mathcal{B} = \{b_1, b_2, b_3\}$. As in the case $k = 2$, we may assume that $0 = b_1 < b_2 < b_3$. Now we construct an admissible triple related to $\mathcal{B}$. If $b_2$ and $b_3$ are of the same parity, then either

$$t_1 = \{-b_3, -b_2, b_3\}$$

or

$$t_2 = \{-b_3, -b_2, b_2\}$$

is admissible, according as $3 \mid b_3$ or $3 \nmid b_3$. Further, if $b_2$ is odd and $b_3$ is even, then either

$$t_3 = \{-b_3 + b_2, b_3 - b_2, b_2\}$$

or

$$t_4 = \{-b_3 + b_2, -b_2, b_2\}$$

is admissible, according as $b_2 \equiv b_3 \pmod 3$ or $b_2 \not\equiv b_3 \pmod 3$. Finally, if $b_2$ is even and $b_3$ is odd, then either

$$t_5 = \{-b_3 + b_2, b_3 - b_2, b_3\}$$

or

$$t_6 = \{-b_3, b_3 - b_2, b_3\}$$

is admissible, according as $b_2 \equiv b_3 \pmod 3$ or $b_2 \not\equiv b_3 \pmod 3$. Let $1 \leq i \leq 6$ such that $t_i$ is admissible, and write $t_i = \{u_1, u_2, u_3\}$. According to Conjecture 1.1 (see also the Remark after it) we get that there exists an $n$ with $n \geq n_0 + b_3$ such that $n$ is composite, but

$$n + u_1, \quad n + u_2, \quad n + u_3$$

are all primes $\geq n_0$. However, then a simple check shows that for any value of $i$, we have that none of $n - b_3, n - b_2, n$ is in $\mathcal{A}$, since otherwise $\mathcal{C}$ would contain a prime $\geq n_0$. However, then we get $n \notin \mathcal{C}$. This is a contradiction, and our claim follows. $\square$

## 4. Proof of Theorem 1.3

Let $\mathcal{C} \subset \mathbb{N}$ with $\mathcal{C} \sim \mathcal{G}_y$. Then with some positive integer $n_0$ we have

$$\mathcal{C} \cap [n_0, +\infty) = \{n + 1 : n \geq n_0 - 1 \text{ and } n \text{ is composite}\}.$$

Assume to the contrary that we can write

$$\mathcal{C} = \mathcal{A} \cdot \mathcal{B} \tag{4.1}$$

with $|\mathcal{B}| < +\infty$. Put $B = \{b_1, \dots, b_\ell\}$ with $\ell \geq 2$ and $1 \leq b_1 < b_2 < \dots < b_\ell$.

Assume first that $1 \notin \mathcal{B}$ (that is, $b_1 > 1$). Let $n$ be an arbitrary (composite) multiple of the product $b_1 \dots b_\ell$ such that $n \geq n_0$. Then we immediately see that $n + 1$ is not divisible by any $b_i$ ($i = 1, \dots, \ell$), which shows that $n + 1 \notin \mathcal{C}$. However, this is a contradiction, and our claim follows in this case.

Suppose now that $1 \in \mathcal{B}$ (that is, $b_1 = 1$). For each of $i = 2, \dots, \ell$ choose a prime divisor $p_i$ of $b_i$, with the convention that $p_i = 4$ if $b_i$ is a power of 2, and let $P$ be the set of these primes. Observe that $P$ is non-empty. Take two distinct primes $q_1, q_2$ not belonging to $P$, and consider the following system of linear congruences:

$$\begin{aligned} x &\equiv 0 \pmod{q_i} \quad \text{for } i = 1, 2, \\ x &\equiv 1 \pmod{p} \quad \text{if } p \in P,\ p \mid b_2 - 1, \\ x &\equiv 0 \pmod{p} \quad \text{if } p \in P,\ p \nmid b_2 - 1. \end{aligned}$$

Let $x_0$ be an arbitrary positive solution to the above system. Put

$$N := q_1 q_2 \prod_{p \in P} p$$

and consider the arithmetic progression

$$(b_2 N)t + (b_2(x_0 + 1) - 1) \tag{4.2}$$

in $t \geq 0$. Observe that here we have $\gcd(b_2 N, b_2(x_0 + 1) - 1) = 1$. Indeed, $\gcd(b_2, b_2(x_0+1)-1) = 1$ trivially holds, and as $b_2(x_0+1)-1 = b_2 x_0 + b_2 - 1$, the relation $\gcd(N, b_2(x_0 + 1) - 1) = 1$ follows from the definition of $x_0$. Thus by Dirichlet's theorem there exist infinitely many integers $t$ such that (4.2) is a prime. Let $t$ be such an integer with $t > n_0$, and put

$$n := tN + x_0.$$

We claim that $n$ is composite with $n > n_0$, but $n + 1 \notin \mathcal{C}$. This will clearly imply the statement. It is obvious that $n > n_0$, and as $q_1 q_2 \mid N$ and $q_1 q_2 \mid x_0$, we also have that $n$ is composite. Further, we have that $n + 1 \notin \mathcal{A}$. Indeed, otherwise we would also have $b_2(n + 1) \in \mathcal{C}$, that is, $b_2(n + 1) - 1$ should be composite - however,

$$b_2(n + 1) - 1 = (b_2 N)t + (b_2(x_0 + 1) - 1)$$

is a prime. (The importance of this fact is that we cannot have $n+1 \in \mathcal{C}$ by the relation $n + 1 = (n + 1) \cdot 1$ with $n + 1 \in \mathcal{A}$ and $1 \in \mathcal{B}$.) Further, since $n + 1 \equiv 1, 2 \pmod{p}$ for $p \in P$ as $p_i \geq 3$ and $p_i \mid b_i$ we have $b_i \nmid n + 1$ for $i = 3, \ldots, \ell$. We need to check the case $i = 2$ separately. If $b_2 > 2$, then we have $p_2 \geq 3$ and $p_2 \mid b_2$, and we have $b_2 \nmid n+1$ again. On the other hand, if $b_2 = 2$ then as $b_2 - 1 = 1$ and $p_2 = 4$, we have $4 \mid n$, so $b_2 \nmid n + 1$ once again. So in any case, $b_i \nmid n + 1$ $(i = 2, \ldots, \ell)$. Hence $n + 1$ cannot be of the form $ab_i$ with $a \in \mathcal{A}$ and $i = 1, \ldots, \ell$. Thus our claim follows also in this case. □

## 5. Proof of Theorem 1.4

The proof of Theorem 1.4 is based on the following deep theorem. Recall that $\{\Gamma\}$ denotes the multiplicative semigroup generated by $\Gamma$. Consider the equation

$$a_1 x_1 + \cdots + a_m x_m = 0 \quad \text{in } x_1, \ldots, x_m \in \{\Gamma\}, \tag{5.1}$$

where $a_1, \ldots, a_m$ are non-zero elements of $\mathbb{Q}$. If $m \geq 3$, a solution of (5.1) is called *non-degenerate* if the left hand side of (5.1) has no vanishing subsums. Two solutions $x_1, \ldots, x_m$ and $x'_1, \ldots, x'_m$ are *proportional* if

$$(x'_1, \ldots, x'_m) = \lambda(x_1, \ldots, x_m)$$

with some $\lambda \in \{\Gamma\} \setminus \{1\}$.

**Theorem C.** *Equation* (5.1) *has only finitely many non-proportional, non-degenerate solutions.*

This theorem was proved independently by van der Poorten and Schlickewei [9] and Evertse [3] in a more general form. Later Evertse and Győry [4] showed that the number of non-proportional, non-degenerate solutions of (5.1) can be estimated from above by a constant which depends only on $\Gamma$. For related results, see the paper [10] and the book [5].

We shall use the following consequence of Theorem C.

**Corollary 5.1.** *There exists a finite set $\mathcal{L}$ such that if $x_1, \dots, x_\ell$ are pairwise coprime elements of $\{\Gamma\}$, $y_1, \dots, y_h$ are also pairwise coprime elements of $\{\Gamma\}$ such that $\ell, h \le k$, $\ell + h \ge 3$ and*

$$\varepsilon(x_1 + \dots + x_\ell) - \eta(y_1 + \dots + y_h) = 0 \tag{5.2}$$

*with some $\varepsilon, \eta \in \{\Gamma\}$ and without vanishing subsum on the left hand side, then*

$$x_1, \dots, x_\ell,\ y_1, \dots, y_h \in \mathcal{L}.$$

*Further, $\mathcal{L}$ is independent of $\varepsilon, \eta$.*

*Proof.* Without loss of generality we may assume that $\ell \ge 2$. Then Theorem C implies that

$$(\varepsilon x_1, \dots, \varepsilon x_\ell) = \nu(z_1, \dots, z_\ell),$$

where $\nu, z_1, \dots, z_\ell \in \{\Gamma\}$, and $z_1, \dots, z_\ell$ belong to a finite set. Hence, as

$$(x_1, \dots, x_\ell) = \nu^*(z_1, \dots, z_\ell)$$

with $\nu^* = \nu/\varepsilon$, in view of that $x_1, \dots, x_\ell \in \{\Gamma\}$ are pairwise coprime, we conclude that $x_1, \dots, x_\ell$ belong to a finite set (which is independent of $\varepsilon, \eta$). If we have $h = 1$, then expressing $y_1$ from (5.2), the statement immediately follows. On the other hand, if $h \ge 2$, then applying the above argument for $(\eta y_1, \dots, \eta y_h)$ in place of $(\varepsilon x_1, \dots, \varepsilon x_\ell)$, the statement also follows. □

Now we can prove our Theorem 1.4. Our argument will give the proof of our statement concerning both $H_k$ and $H_{\le k}$. First note that there is a constant $C_1$ such that if in $H_k$ (resp. in $H_{\le k}$) we have

$$u_1 + \dots + u_t > C_1$$

with $t = k$ (resp. with $2 \le t \le k$) and $\gcd(u_i, u_j) = 1$ for $1 \le i < j \le t$, then this sum is not contained in $\{\Gamma\}$. This is an immediate consequence of Theorem C.

Assume that contrary that contrary to the statement of the theorem for some $\mathcal{R}$ which is asymptotically equal to one of $H_k$ and $H_{\le k}$ we have

$$\mathcal{R} = \mathcal{A} \cdot \mathcal{B}$$

with

$$\mathcal{A}, \mathcal{B} \subset \mathbb{N}, \quad |\mathcal{A}|, |\mathcal{B}| \ge 2.$$

Since both $H_k$ and $H_{\le k}$ are infinite, so is $\mathcal{R}$, whence at least one of $\mathcal{A}$ and $\mathcal{B}$, say $\mathcal{B}$ is infinite.

We prove that

$$\mathcal{A} = \{a_0 t : t \in T\} \tag{5.3}$$

with some positive integer $a_0$ and $T \subset \{\Gamma\}$, such that $|T| \ge 2$. Indeed, take distinct elements $a_1, a_2 \in \mathcal{A}$. Then for all sufficiently large $b \in \mathcal{B}$ we have

$$r_1 := a_1 b = u_1 + \cdots + u_\ell \tag{5.4}$$

and

$$r_2 := a_2 b = v_1 + \cdots + v_h \tag{5.5}$$

with some $r_1, r_2 \in \mathcal{R}$, $\ell, h \le k$, and with $u_1, \dots, u_\ell, v_1, \dots, v_h \in \{\Gamma\}$ such that

$$\gcd(u_{i_1}, u_{i_2}) = \gcd(v_{j_1}, v_{j_2}) = 1 \ (1 \le i_1 < i_2 \le \ell, 1 \le j_1 < j_2 \le h). \tag{5.6}$$

We infer from (5.4) and (5.5) that

$$a_2(u_1 + \cdots + u_\ell) - a_1(v_1 + \cdots + v_h) = 0. \tag{5.7}$$

Since there are infinitely many $b \in \mathcal{B}$, and we arrive at (5.7) whenever $b$ is large enough, this equation has infinitely many solutions $u_1, \dots, u_\ell, v_1, \dots, v_h \in \{\Gamma\}$ with the property (5.6). However, by Theorem C this can hold only if, after changing the indices if necessary,

$$a_2 u_1 = a_1 v_1. \tag{5.8}$$

Let $d_1, d_2$ be the maximal positive divisors of $a_1, a_2$ from $\{\Gamma\}$, respectively. Write

$$a_1 = a_1' d_1 \quad \text{and} \quad a_2 = a_2' d_2, \tag{5.9}$$

and observe that by the pairwise coprimality of the elements of $\Gamma$ both $d_1, d_2$ and $a_1', a_2'$ are uniquely determined. In particular, none of $a_1', a_2'$ is divisible by any element of $\Gamma$. Equations (5.9) together with (5.8) imply

$$a_2' d_2 u_1 = a_1' d_1 v_1,$$

where $d_2u_1, d_1v_1 \in \{\Gamma\}$. We know infer that

$$a_0 := a'_1 = a'_2$$

and

$$a_1 = a_0t_1, \quad a_2 = a_0t_2 \quad \text{with } t_1, t_2 \in \{\Gamma\}.$$

It is important to note that $a_0$ is the greatest positive divisor of $a_1$ (and of $a_2$) which is not divisible by any element of $\Gamma$. Considering now $a_1, a_i$ instead of $a_1, a_2$ for any other $a_i \in \mathcal{A}$, we get in the same way that

$$a_i = a_0t_i \quad \text{with } t_i \in \{\Gamma\}.$$

This proves (5.3).

Write $\Gamma = \{n_1, \dots, n_s\}$ and put $m := \min(s, k)$. Denote by $\mathcal{R}^\circ$ the subset of $\mathcal{R}$ consisting of sums $u_1 + \dots + u_k$ with $u_1, \dots, u_m \in \{\Gamma\} \setminus \mathcal{L}$ such that

$$u_i = \begin{cases} n_i^{\alpha_i} & \text{with } \alpha_i > 1 \text{ for } i \le m, \\ 1 & \text{for } s < i \le k \text{ (if } s < k). \end{cases} \tag{5.10}$$

Clearly, $\mathcal{R}^\circ$ is an infinite set. Take $r_1 \in \mathcal{R}^\circ$ of the form

$$r_1 = u_1 + \dots + u_k$$

with $u_1, \dots, u_k$ satisfying (5.10). By what we have already proved, we can write

$$r_1 = a_0t_1b$$

with some $t_1 \in T$ and $b \in \mathcal{B}$. Put $r_2 = a_0t_2b$ with some $t_2 \in T$, $t_2 \neq t_1$ such that $r_2 \in \mathcal{R}$. Writing

$$r_2 = v_1 + \dots + v_h$$

with pairwise coprime $v_1, \dots, v_h \in \{\Gamma\}$, we get

$$t_2(u_1 + \dots + u_k) - t_1(v_1 + \dots + v_h) = 0. \tag{5.11}$$

Recall that by assumption, $u_i \in \{\Gamma\} \setminus \mathcal{L}$ for $i = 1, \dots, m$. Hence we must have $h \ge m$, and repeatedly applying Corollary 5.1 (after changing the indices if necessary) we get

$$t_2u_i - t_1v_i = 0 \quad (i = 1, \dots, m)$$

whence

$$\frac{u_1}{v_1} = \dots = \frac{u_m}{v_m},$$

that is

$$u_1v_i = v_1u_i \quad (2 \le i \le m).$$

If $m > 1$, then this by the coprimality of $u_1, \dots, u_k$ and $v_1, \dots, v_k$ gives $u_i = v_i$ $(i = 1, \dots, m)$. This is a contradiction, which proves the theorem whenever $m > 1$.

So we are left with the only possibility $m = 1$, that is, $s = 1$. Then, letting $\Gamma = \{n\}$, equation (5.11) reduces to

$$t_2 n^{\alpha_1} - t_1 n^{\alpha_2} = c, \tag{5.12}$$

where $c = t_1 w - t_2(k-1)$ with some $0 \leq w \leq k-1$. For any fixed $c \neq 0$ the above equation has only finitely many solutions in non-negative integers $\alpha_1, \alpha_2$. Indeed, we may easily bound $\min(\alpha_1, \alpha_2)$ first, and then also $\max(\alpha_1, \alpha_2)$. Hence we may assume that $c = 0$ in (5.12). Observe, that in the case of the set $H_k$ we have $w = k-1$, whence we get $t_1 = t_2$, a contradiction.

So in what follows, we may assume that we deal with the set $H_{\leq k}$. Observe that for any large $\beta$, both $n^\beta$ and $n^\beta + 1$ belong to $\mathcal{R}$. Hence, in view of (5.3) we get $a_0 = 1$, and all elements of $\mathcal{A}$ are powers of $n$. This implies that $1 \in \mathcal{A}$: indeed, since all elements of $\mathcal{A}$ are powers of $n$, we can have $n^\beta + 1 \in \mathcal{R}$ only if $1 \in \mathcal{A}$ (and $n^\beta + 1 \in \mathcal{B}$). Recall that $|\mathcal{A}| \geq 2$; let $n^\alpha \in \mathcal{A}$ with some $\alpha > 0$, and assume that $\alpha$ is minimal with this property. Obviously, for all large $\beta$ we must have $n^\beta + i \in \mathcal{B}$, for all $0 \leq i < k$. One of $k-2, k-1$ is not divisible by $n$; write $j$ for this number. (Note that for $k = 2$ we have $j = 1$.) Then, for all large $\beta$, we must have $n^\beta + j \in \mathcal{B}$. Consequently, we have

$$n^{\alpha+\beta} + n^\alpha j \in \mathcal{R}.$$

However, this implies that

$$n^\alpha j \leq k - 1.$$

Hence, in view of $j \in \{k-2, k-1\}$ (with $j = 1$ for $k = 2$) we easily get that the only possibility is given by

$$n = 2, \qquad \alpha = 1, \qquad k = 3.$$

Thus the theorem follows. □

## References


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

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

[3] J.-H. Evertse, *On sums of S-units and linear recurrences*, Compos. Math. **53** (1984), 225–244.

[4] J.-H. Evertse, K. Győry, *On the number of solutions of weighted unit equations*, Compos. Math. **66** (1988), 329–354.

[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.)* (submitted).
[7] L. Hajdu, N. Saradha, *On generalizations of problems of Recaman and Pomerance*, J. Number Theory **162** (2016), 552–563.
[8] J. Maynard, *Small gaps between primes*, Annals Math. **181** (2015), 383–413.
[9] A. J. van der Poorten, H. P. Schlickewei, *The growth condition for recurrence sequences*, Macquarie University Math. Rep., 1982, 82–0041.
[10] A. J. van der Poorten, H. P. Schlickewei, *Additive relations in fields*, J. Austral. Math. Soc. **51** (1991), 154–170.
[11] A. Sárközy, *Unsolved problems in number theory*, Periodica Math. Hungar. **42(1-2)** (2001), 17–35.

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