ON MULTIPLICATIVE DECOMPOSITIONS OF POLYNOMIAL SEQUENCES, III

L. HAJDU AND A. SÁRKÖZY

ABSTRACT. In two earlier papers we studied the multiplicative decomposability of polynomial sequences $\{f(x) : x \in \mathbb{Z}, f(x) > 0\}$. Here we extend this problem by considering also sequences which can be obtained from sequences of this type by changing "not too many" elements of them. In particular, we prove the multiplicative analogue of a theorem of Szemerédi and the second author (related to a problem of Erdős).

1. INTRODUCTION

In [4] and [5] we studied multiplicative decompositions of polynomial sequences of positive integers, and this paper is the third (and last) one in this series.

First we recall some notations, definitions and results from [4] and [5]. $\mathcal{A}, \mathcal{B}, \mathcal{C}, \ldots$ 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 $\mathbb{N}$.

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

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

If

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

2010 *Mathematics Subject Classification.* 11N25, 11N32, 11D41.

Key words and phrases. Multiplicative decompositions, shifted powers, binomial Thue equations, continued fractions, bipartite graphs.

Research supported in part by the NKFIH grants K115479, K119528 and K128088, 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* $\mathcal{A}$*.*

In [9] and [10] H. H. Ostmann introduced some definitions concerning additive properties of sequences of non-negative integers and studied some related problems. The most interesting definitions are:

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

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

If there are no sets $\mathcal{B}, \mathcal{C}$ *with these properties then* $\mathcal{A}$ *is said to be* a-primitive *or* a-irreducible*.*

(More precisely, Ostmann used the terminology "reducible", "primitive", "irreducible" without the prefix a-. However, since we will study both additive properties and their multiplicative analogues thus to distinguish between them we will use a prefix a- in the additive case and a prefix m- in the multiplicative case.)

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* $\mathcal{A}' \sim \mathcal{A}$ *is* a-primitive*.*

Example 1.1. *It is easy to see that if*

$$\mathcal{A} = \{a_1, a_2, \dots\} \quad (\textit{with } a_1 < a_2 < \dots)$$

is an infinite set of non-negative integers with

$$\lim_{n \to +\infty} (a_{n+1} - a_n) = +\infty,$$

then $\mathcal{A}$ *is totally a-primitive. Thus in particular, the sequence*

$$\mathcal{M}_2 = \{0, 1, 4, 9, \dots, n^2, \dots\} \tag{1.4}$$

of squares is totally a-primitive.

Erdős conjectured that much more is true:

Conjecture 1.1. *If we change* $o(X^{1/2})$ *elements of the set* (1.4) *up to* X*, then the new set is always* totally a-primitive*.*

The second author and Szemerédi [13] proved this conjecture in the following slightly weaker form:

Theorem A. *If $\varepsilon > 0$ and we change $o\left(X^{1/2}\ 2^{-(3+\varepsilon)\log X \log\log X}\right)$ elements of the set* (1.4) *up to X, then we get a totally a-primitive set.*

(We presented a short survey of other related papers in [4]. In particular, the a-primitivity of certain special sets is studied in [11], [14] and [16].)

Observe that Definition 1.2 can be extended from non-negative integers to any *additive* semigroup G (all we have to do is to replace "non-negative integers" by "elements of G"). One might like to also extend this definition to *multiplicative* semigroups by replacing "additive decomposition" by "multiplicative decomposition". However, some caution is needed here. Namely, if both addition and multiplication are defined in the given set and it contains both an additive null element 0 and a multiplicative unit element 1 (like in cases of the non-negative integers or $\mathbb{F}_p$), then every subset $\mathcal{A}$ with $|\mathcal{A}| \geq 2$ and containing 0 has a trivial multiplicative decomposition

$$\mathcal{A} = \{0, 1\} \cdot \mathcal{A}$$

which satisfies both (1.1) and (1.3). The simplest way to aviod trivial decompositions of this type is to restrict ourselves to sets not containing 0. Then in the two most important special cases the multiplicative analogues of Definitions 1.2 and 1.4 are:

Definition 1.5. *If $\mathcal{A}$ is a finite or infinite set of positive integers or $\mathcal{A} \subset \mathbb{F}_p^*(= \mathbb{F}_p \setminus \{0\})$ then it is said to be* m-reducible *if it has a* multiplicative decomposition

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

(where $\mathcal{B} \subset \mathbb{N}, \mathcal{C} \subset \mathbb{N}$ or $\mathcal{B} \subset \mathbb{F}_p^*, \mathcal{C} \subset \mathbb{F}_p^*$, respectively). If there are no such sets $\mathcal{B}, \mathcal{C}$ then $\mathcal{A}$ is said to be m-primitive *or* m-irreducible.

(In particular, the m-primitivity of certain special sets is studied in [3] and [12].)

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.*

In Part I we started out from the *multiplicative* analogue of our remark on the totally a-primitivity of the sequence (1.4). By Definition 1.5, the notions of m-reducibility and m-primitivity are restricted to *positive* integers, thus we have to delete 0 from the set $\mathcal{M}_2$ and to consider instead the set $\mathcal{M}_2^+ = \{1, 4, 9, \dots, x^2, \dots\}$. However, this set

is trivially m-reducible since we have $\mathcal{M}_2^+ = \mathcal{M}_2^+ \cdot \mathcal{M}_2^+$. Thus to get a non-trivial problem on squares, we have to shift them:

Problem 1. Is it true that the set

$$\mathcal{M}_2' = \{0, 1, 4, 9, \ldots, x^2, \ldots\} + \{1\} = \{1, 2, 5, 10, \ldots, x^2 + 1, \ldots\}$$

of shifted squares is m-primitive?

In [4] we proved that the answer to this question is affirmative in a much stronger form: if the counting function of a subset of $\mathcal{M}_2'$ increases faster than $\log X$, then the subset must be totally m-primitive:

Theorem B. *If*

$$\mathcal{R} = \{r_1, r_2, \ldots\} \subset \mathcal{M}_2', \quad r_1 < r_2 < \ldots,$$

and

$$\limsup_{X \to \infty} \frac{R(X)}{\log X} = \infty,$$

then $\mathcal{R}$ *is* totally m-primitive.

We also proved that Theorem B is nearly sharp:

Theorem C. *There is an m-reducible subset* $\mathcal{R} \subset \mathcal{M}_2'$ *and a number* X_0 *such that for* $X > X_0$ *we have*

$$R(X) > \frac{1}{\log 51} \log X.$$

In [5] we studied the analogous problems for shifted k-th powers with $k > 2$. Write $\mathcal{M}_k = \{0, 1, 2^k, 3^k, \ldots, x^k, \ldots\}$ and

$$\mathcal{M}_k' = \mathcal{M}_k + \{1\} = \{1, 2, 2^k + 1, 3^k + 1, \ldots, x^k + 1, \ldots\}. \tag{1.5}$$

We proved:

Theorem D. *If* $k > 2$,

$$\mathcal{R} = \{r_1, r_2, \ldots\} \subset \mathcal{M}_k', \ r_1 < r_2 < \ldots,$$

and $\mathcal{R}$ *is infinite, then* $\mathcal{R}$ *is* totally m-primitive.

(So for $k > 2$, Theorem C has no analogue: there are no exceptional subsets of $\mathcal{M}_k'$.)

In both [4] and [5] we also studied the totally m-primitivity of more general polynomial sets $\{f(x) : \ x \in \mathbb{Z}, f(x) > 0\}$ (where $f(x) \in \mathbb{Z}[x]$).

So far we have studied the sets of squares and shifted squares, and also their subsets obtained by deleting many (but not "too many") elements of them. But what happens if instead of dropping elements,

we add new elements to these sets? The most interesting set obtained in this way is certainly the set of all powers x^k with $k \geq 2$:

$$\mathcal{P} = \{1, 2^2, 2^3, 3^2, 2^4, 5^2, 3^3, 2^5, \dots, x^k, \dots\}. \tag{1.6}$$

(Note that this set contains $X^{1/2} + O(1)$ squares up to X, and $(1 + o(1))X^{1/3}$ further powers are added.)

Theorem 1.1. *The set $\mathcal{P}$ in* (1.6) *is* totally m-primitive.

Proof. Let $\mathcal{P}'$ be any set of positive integers with $\mathcal{P}' \sim \mathcal{P}$. Then there exists a positive integer X_0 such that

$$\mathcal{P} \cap [X_0, \infty) = \mathcal{P}' \cap [X_0, \infty).$$

Suppose to the contrary that

$$\mathcal{P}' = \mathcal{A} \cdot \mathcal{B} \quad \text{with } \mathcal{A}, \mathcal{B} \subset \mathbb{N} \text{ and } |\mathcal{A}|, |\mathcal{B}| \geq 2.$$

Let p be any prime with $p > X_0$. Then $p^2 \in \mathcal{P}'$, and we have one of the following:

i) $p \in \mathcal{A} \cap \mathcal{B}$,
ii) $1 \in \mathcal{A}$, $p^2 \in \mathcal{B}$,
iii) $p^2 \in \mathcal{A}$, $1 \in \mathcal{B}$.

In case i) take any prime q with $q > X_0$ and $p \neq q$. As $q^2 \in \mathcal{P}'$, we get that one of q, q^2 belongs to $\mathcal{A} \cup \mathcal{B}$. However, then one of pq, pq^2 is in $\mathcal{P}'$, a contradiction. Thus i) cannot hold, and by symmetry we may assume that $p \notin \mathcal{B}$.

If $p \notin \mathcal{A}$, then by symmetry again we may assume that we are in case ii). On the other hand, if $p \in \mathcal{A}$, then $1 \notin \mathcal{B}$, otherwise $p \in \mathcal{P}'$ would hold. So in any case, we may assume that we are in case ii). Observe that this implies that if $q > X_0$ is any prime with $p \neq q$, then $q \notin \mathcal{A}$, $q \notin B$. (Indeed, otherwise one of q, p^2q would belong to $\mathcal{P}'$.) Hence as $q^2 \in \mathcal{P}'$, we have $q^2 \in \mathcal{A} \cup \mathcal{B}$. We show that $q^2 \notin \mathcal{A}$, and then necessarily $q^2 \in \mathcal{B}$. Assume to the contrary that $q^2 \in \mathcal{A}$. Take a prime $r > X_0$ different from p, q. As $1 \in \mathcal{A}$ and $p^2 \in \mathcal{B}$, we know that $r \notin \mathcal{A} \cup \mathcal{B}$. However, as $r^3 \in \mathcal{P}'$, this implies that $r^3 \in \mathcal{A} \cup \mathcal{B}$. But then one of p^2r^3, q^2r^3 is in $\mathcal{P}'$ - a contradiction. So $q^2 \in \mathcal{B}$ must hold. Hence for any prime q with $q > X_0$ and $q \neq p$ we obtain $q^2 \in \mathcal{B} \setminus \mathcal{A}$. We show that $p^2 \in \mathcal{B} \setminus \mathcal{A}$ also holds. As $p^2 \in \mathcal{B}$, we only need to check that $p^2 \notin \mathcal{A}$. This can be done with a similar argument as above. Indeed, assuming $p^2 \in \mathcal{A}$, if r is a prime with $r > X_0$ and $r \neq p$ then $r^3 \in \mathcal{P}'$ (as $r \notin \mathcal{A} \cup \mathcal{B}$ by $p^2r \notin \mathcal{P}'$), whence $r^3 \in \mathcal{A} \cup \mathcal{B}$ implying $p^2r^3 \in \mathcal{P}'$ - a contradiction again. Thus we conclude that

$$\{p^2 : p \text{ prime}, \ p > X_0\} \subset \mathcal{B} \setminus \mathcal{A}.$$

Note that this together with $1 \in \mathcal{A}$ implies that neither $\mathcal{A}$ nor $\mathcal{B}$ contains any prime. Now we show that all the powers of primes above X_0 belong to $\mathcal{B} \setminus \mathcal{A}$. We proceed by induction. Assume that for some $i \geq 3$ we have

$$\{p^{i-1} : p \text{ prime}, \ p > X_0\} \subset \mathcal{B} \setminus \mathcal{A}.$$

(This holds with $i = 3$.) Suppose that for some prime q with $q > X_0$ we have $q^i \notin \mathcal{B} \setminus \mathcal{A}$. Hence if $q^i \in \mathcal{B}$ then also $q^i \in \mathcal{A}$. On the other hand, if $q^i \notin \mathcal{B}$, then since none of $q, \dots, q^{i-1}$ belongs to $\mathcal{A}$, by $q^i \in \mathcal{P}'$ we get $q^i \in \mathcal{A}$. That is, in any case, we have $q^i \in \mathcal{A}$. Take any prime $r > X_0$ with $r \neq q$, and observe that by the induction hypothesis $r^{i-1} \in \mathcal{B}$ holds. Thus we get $r^{i-1}q^i \in \mathcal{P}'$, which is a contradiction. Thus our claim follows, and we obtain

$$\bigcup_{i=2}^{\infty} \{p^i : p \text{ prime}, \ p > X_0\} \subset \mathcal{B} \setminus \mathcal{A}.$$

Let now $a \in \mathcal{A}$ with $a > 1$. (As $|\mathcal{A}| \geq 2$, such an a must exist.) Let

$$a = p_1^{\alpha_1} \dots p_\ell^{\alpha_\ell}$$

be the prime factorization of a, and put

$$\alpha = \max_{1 \leq i \leq \ell} \alpha_i.$$

Take any prime $p > X_0$ different from $p_1, \dots, p_\ell$. As $p^{\alpha+1} \in \mathcal{B}$, we get that $ap^{\alpha+1} \in \mathcal{P}'$ should hold. However, this is a contradiction, and the statement follows. □

It is also a natural question to ask: what happens if we start out from the set $\mathcal{M}_k'$ of the *shifted* k-th powers ($k \geq 2$) and we combine *deletion and addition* of many but "not too many" elements? Is it true that the sets obtained in this way are always totally m-primitive? (Observe that this is not so with $\mathcal{M}_k$ in place of $\mathcal{M}_k'$ since the set $\mathcal{M}_k$ itself is m-reducible: $\mathcal{M}_k = \mathcal{M}_k \cdot \mathcal{M}_k$.) We conjecture that the answer to this question is affirmative in the following strong form:

Conjecture 1.2. *If $k \geq 2$ and we change $o(X^{1/k})$ elements of the set $\mathcal{M}_k'$ in* (1.5) *up to X, then the new set is always* totally m-primitive.

(Note that this is the multiplicative analogue of Erdős's Conjecture 1.1.) This paper is devoted to the study of this problem. As in the case of Conjecture 1.1, this conjecture in its original form seems to be beyond reach but we will be able to prove a result (Theorem 2.1 below) which is just slightly weaker.

We mention that this main result of ours will imply that the set of shifted powers

$$\mathcal{P}' = \mathcal{P}+\{1\} = \{2, 2^2+1, 2^3+1, 3^2+1, 2^4+1, 5^2+1, 3^3+1, 2^5+1, \dots, x^k+1, \dots\}$$

is totally m-primitive. One might wonder whether this assertion could be obtained "directly" through the theory of diophantine equations. Following our approach (see Section 3), assuming that $\mathcal{P}'$ is not totally m-primitive, we could get equations of the form

$$Ax^n - By^m = C \tag{1.7}$$

with A, B, C fixed, however, with all x, y, n, m being variables. In general, *not any* finiteness result is known for the solutions of this equation. By a classical conjecture of Pillai, equation (1.7) has only finitely many solutions for any A, B, C with $ABC \neq 0$. However, the conjecture is confirmed only for the case $A = B = C = 1$, when (1.7) is the Catalan equation having the only solution

$$(x, y, n, m) = (3, 2, 2, 3).$$

This result is due to Mihăilescu [7]. (For more details about (1.7) and Pillai's conjecture, see e.g. [15].) So we do not see any other method to prove that $\mathcal{P}'$ is totally m-primitive, only the one through our Theorem 2.1 below.

2. The main result and the structure of the proof

We will prove the following theorem:

Theorem 2.1. *For $k \geq 2$ and any $\varepsilon > 0$ changing*

$$o\left(X^{1/k} \exp\left(-(\log 2 + \varepsilon)\frac{\log X}{\log\log X}\right)\right)$$

elements of $\mathcal{M}'_k$ up to X (deleting some of its elements and adding positive *integers) the new set $\mathcal{R}$ obtained in this way is* totally m-primitive.

We remark that this theorem is the multiplicative analogue of Theorem A (apart from the constant in the exponent). However, the only connection between the proofs of the two theorems is that Wigert's theorem (appearing as Lemma 6.1 later in this paper) is used in both proofs. Apart from this, the proof of Theorem 2.1 is more complicated than that of Theorem A.

Proof of Theorem 2.1. It suffices to prove that every set $\mathcal{R}$ obtained in the way described in the theorem is m-primitive (since then for every

such $\mathcal{R}$, every set $\mathcal{R}' \subset \mathbb{N}$ with $\mathcal{R}' \sim \mathcal{R}$ also satisfies the conditions in the theorem with $\mathcal{R}'$ in place of $\mathcal{R}$, thus $\mathcal{R}'$ is also m-primitive).

We will prove by contradiction: assume that for some $\varepsilon > 0$ there is an $\mathcal{R}$ of the type described in the theorem which is m-reducible, so that $\mathcal{R}$ is of the form

$$\mathcal{R} = \mathcal{Q} \cup \mathcal{S} \tag{2.1}$$

with

(2.2)

$$\mathcal{Q} \subset \mathcal{M}_k', \quad |(\mathcal{M}_k' \backslash \mathcal{Q}) \cap [1, X]| = o\left(X^{1/k} \exp\left(-(\log 2 + \varepsilon)\frac{\log X}{\log\log X}\right)\right),$$

$$\mathcal{S} \cap \mathcal{M}_k' = \emptyset, \quad S(X) = o\left(X^{1/k} \exp\left(-(\log 2 + \varepsilon)\frac{\log X}{\log\log X}\right)\right) \tag{2.3}$$

and there are

$$\mathcal{A} \subset \mathbb{N}, \quad \mathcal{B} \subset \mathbb{N} \tag{2.4}$$

with

$$|\mathcal{A}| \geq 2, \quad |\mathcal{B}| \geq 2, \tag{2.5}$$

$$\mathcal{R} = \mathcal{A} \cdot \mathcal{B}. \tag{2.6}$$

Then it follows trivially from the definition of $\mathcal{M}_k'$ and $\mathcal{R}$ that

(2.7)

$$R(X) = X^{1/k} + o\left(X^{1/k} \exp\left(-(\log 2 + \varepsilon)\frac{\log X}{\log\log X}\right)\right) (= (1+o(1))X^{1/k}).$$

In order to to deduce a contradiction from assumptions (2.1)-(2.6), we will have to distinguish two cases. First (in Section 3) we will consider the case when the counting function of one of the two sets $\mathcal{A}, \mathcal{B}$ is "very large" infinitely often (which implies that the other counting function is "very small", thus this case can be considered asymmetric). This case can be handled relatively easily by the methods used in [4] and [5], more precisely, by using the theory of Pell equations and a consequence of a classical theorem of Baker [1]. The second case is when both counting functions $A(X)$ and $B(X)$ increase "not too fast". This ("symmetric") case is much more difficult. Namely, the effective estimates obtained by Baker's method contain constants depending on the coefficients of the diophantine equations in question, and we need better control for this dependence than the ones that can be deduced by Baker's method. To get around this difficulty, we will need tools (definitions, notation, results and lemmas) from graph theory and the theory of continued fractions which will be presented in Sections 4 and 5, respectively. The

proof of Theorem 2.1 will be completed in Section 6 by using these lemmas in Sections 4 and 5. The last section (Section 7) will contain comments and unsolved problems.

3. Case 1: asymmetric decomposition

First we will study

CASE 1. Assume that for some $\varepsilon > 0$ the counting functions of the sets $\mathcal{A}, \mathcal{B}$ in (2.4) satisfy

$$\max\{A(X), B(X)\} > X^{1/k} \exp\left(-\left(\log 2 + \frac{\varepsilon}{2}\right)\frac{\log X}{\log\log X}\right) \quad \text{for infinitely many } X \in \mathbb{N}. \tag{3.1}$$

Consider a large integer X satisfying (3.1). We may assume without loss of generality that

$$B(X) \geq A(X) \tag{3.2}$$

so that by (3.1) we have

$$B(X) > X^{1/k} \exp\left(-\left(\log 2 + \frac{\varepsilon}{2}\right)\frac{\log X}{\log\log X}\right). \tag{3.3}$$

Let $\mathcal{A} = \{a_1, a_2, \dots\}$ with $(0 <) a_1 < a_2 < \dots$. Then by (2.1)-(2.6) for both $i = 1, 2$, and every

$$b \in \mathcal{B} \cap \{1, 2, \dots, X\}, \tag{3.4}$$

we have

$$0 < a_i b \leq a_2 b \leq a_2 X \tag{3.5}$$

and

$$a_i b \in \mathcal{A} \cdot \mathcal{B} = \mathcal{R} = \mathcal{Q} \cup \mathcal{S}$$

so that either

$$a_i b \in \mathcal{Q} \cap \{1, 2, \dots, a_2 X\} \tag{3.6}$$

or

$$a_i b \in \mathcal{S} \cap \{1, 2, \dots, a_2 X\} \tag{3.7}$$

holds (by (2.2) and (2.3), (3.6) and (3.7) cannot hold simultaneously). Let $\mathcal{B}'$ denote the set of the integers b satisfying (3.4) and also (3.6) for both $i = 1$ and $i = 2$. Now we will estimate $|\mathcal{B}'|$. By (2.3) and (3.3) we have

(3.8)

$$|\mathcal{B}'| = \left|\{b : b \in \mathcal{B} \cap \{1, 2, \dots, X\}\} \setminus \bigcup_{i=1}^{2} \{b : a_i b \in \mathcal{S} \cap \{1, 2, \dots, a_2 X\}\}\right| \geq$$

$$\geq |\{b : b \in \mathcal{B} \cap \{1,2,\dots,X\}\}| - \sum_{i=1}^{2} |\{b : a_i b \in \mathcal{S} \cap \{1,2,\dots,a_2X\}\}| \geq$$

$$\geq B(X) - 2S(a_2X) \geq$$

$$\geq X^{1/k} \exp\left(-\left(\log 2 + \frac{\varepsilon}{2}\right)\frac{\log X}{\log\log X}\right) - 2a_2^{1/k}X^{1/k} \exp\left(-(\log 2+\varepsilon)\frac{\log a_2X}{\log\log a_2X}\right) >$$

$$> X^{1/k} \exp\left(-\left(\log 2 + \frac{2\varepsilon}{3}\right)\frac{\log X}{\log\log X}\right)$$

if X is large enough.

On the other hand, by (2.2) and the definition of $\mathcal{B}'$, for every $b \in \mathcal{B}'$ we have $a_1b \in \mathcal{Q} \subset \mathcal{M}_k'$ and $a_2b \in \mathcal{Q} \subset \mathcal{M}_k'$ thus there are non-negative integers u, v with

$$a_1b = v^k + 1 \tag{3.9}$$

and

$$a_2b = u^k + 1 \tag{3.10}$$

so that

$$0 = a_1(a_2b) - a_2(a_1b) = a_1(u^k+1) - a_2(v^k+1) = a_1u^k - a_2v^k + (a_1 - a_2)$$

whence

$$a_1u^k - a_2v^k = a_2 - a_1, \tag{3.11}$$

and by (3.5), (3.9) and (3.10) here we have

$$\max\{|u|,|v|\}^k + 1 \leq a_2b + 1 \leq 2a_2b \leq 2a_2X$$

whence

$$\max\{|u|,|v|\} < (2a_2)^{1/k}X^{1/k}. \tag{3.12}$$

Thus by (3.8) we have obtained that the number of solutions of the diophantine equation (3.11) under condition (3.12) is at least $|\mathcal{B}'|$ so that by (3.8),

(3.13)

$$|\{(u,v) \in (\mathbb{N}\cup\{0\})^2 : a_1u^k - a_2v^k = a_2 - a_1,\ \max\{|u|,|v|\} < (2a_2)^{1/k}X^{1/k}\}| \geq$$

$$\geq |\mathcal{B}'| > X^{1/k} \exp\left(-\left(\log 2 + \frac{2\varepsilon}{3}\right)\frac{\log X}{\log\log X}\right).$$

Now we need two lemmas from [4] and [5] in order to give an upper bound for the cardinality of the set estimated in (3.13).

Lemma 3.1. *Let $f(z) = Kz^2 + Lz + M$ with $K, L, M \in \mathbb{Z}$, $K(L^2 - 4KM) \neq 0$, and let r, s be distinct positive integers. Then there exists an effectively computable constant $c_0 = c_0(K, L, M, r, s)$ such that*

$$\left|\left\{(u, v) \in \mathbb{Z}^2 : rf(u) = sf(v) \text{ with } \max\{|u|, |v|\} < N\right\}\right| < c_0 \log N$$

for any integer N with $N \geq 2$.

Proof. This is Lemma 2.1 in [4] (where it was proved by using the theory of general Pell type equations). □

Lemma 3.2. *Let A, B, C, k be integers with $ABC \neq 0$ and $k \geq 3$. Then for all integer solutions u, v of the equation*

$$Au^k + Bv^k = C$$

we have $\max\{|u|, |v|\} < c_1$ where $c_1 = c_1(A, B, C, k)$ is a constant depending only on A, B, C, k.

Proof. This is Lemma 2.1 in [5] (which follows from a classical theorem of Baker [1]). □

If $k = 2$, then we may apply Lemma 3.1 with $f(z) = z^2 + 1$, $r = a_1$, $s = a_2$ and $N = [(2a_2)^{1/2} X^{1/2}]$. We obtain for large X that

(3.14)

$$|\{(u, v) \in (\mathbb{N} \cup \{0\})^2 : a_1(u^2 + 1) = a_2(v^2 + 1),\ \max\{|u|, |v|\} < N\}| \leq$$

$$\leq |\{(u, v) \in \mathbb{Z}^2 : a_1 u^2 - a_2 v^2 = a_2 - a_1,\ \max\{|u|, |v|\} < N\}| <$$

$$< c_0 \log N \leq c_0 \log((2a_2)^{1/2} X^{1/2}) < c_2 \log X$$

with some $c_2 = c_2(a_1, a_2)$.

If $k \geq 3$ then applying Lemma 3.2 with $A = a_1$, $B = -a_2$ and $C = a_2 - a_1$ (so that $ABC \neq 0$ holds by $0 < a_1 < a_2$), we obtain that

$$|\{(u, v) \in (\mathbb{N} \cup \{0\})^2 : a_1 u^k - a_2 v^k = a_2 - a_1\}| < c_3 \quad (\text{for } k \geq 3) \tag{3.15}$$

with some absolute constant $c_3 = c_3(a_1, a_2, k)$.

Combining (3.14) and (3.15) we get that there is an absolute constant $c_4 = c_4(a_1, a_2, k)$ such that for $k \geq 2$ and large enough X we have

$$|\{(u, v) \in (\mathbb{N} \cup \{0\})^2 : a_1 u^k - a_2 v^k = a_2 - a_1,\ \max\{u, v\} < (2a_2)^{1/k} X^{1/k}\}| < c_4 \log X.$$

But for every X large enough (in terms of a_1, a_2, k and ε) this inequality contradicts the inequality in (3.13) so that, indeed, Case 1 cannot occur.

4. A lemma on bipartite graphs

We will use the basic graph theoretic definitions and terminology as they appear in [2] (but the notation will be modified slightly to fit better to the notation used in the first two parts of this paper).

Definition 4.1. *A graph G is said to be a* bipartite *graph with vertex classes U and V if its vertex set W is of form $U \cup V$ with $U \cap V = \emptyset$, and every edge of G joins a vertex in U to a vertex in V, and then we write $G = G(U, V)$. Moreover, a bipartite graph $G = G(U, V)$ is said to be* complete *if every vertex in U is joined to every vertex in V. $K(s, t)$ denotes the complete bipartite graph whose vertex classes contain s and t vertices, respectively.*

Definition 4.2. *The* Zarankiewicz function *$Z(m, n; s, t)$ denotes the largest possible number of edges in a bipartite graph $G(U, V)$ with $|U| = m$, $|V| = n$ which does not contain a subgraph $K(s, t)$.*

(K. Zarankiewicz proposed to study this function in certain special cases in 1951.)

Lemma 4.1. *For any positive integers m, n, s, t we have*

$$Z(m, n; s, t) \le (s-1)^{1/t}(n-t+1)m^{1-1/t} + (t-1)m.$$

Proof. This is Theorem 10 in [2], p.113. □

We will use the following consequence of Lemma 4.1:

Lemma 4.2. *Let $G = G(U, V)$ be a bipartite graph on the vertex classes $U = \{U_1, U_2, \dots, U_r\}$ and $V = \{V_1, V_2, \dots, V_s\}$, and denote the number of edges of G (the* size *of G) by t. Assume that $r = |U|$, $s = |V|$, and t are such that*

$$2 \le r \le s \le \frac{t}{3}, \tag{4.1}$$

and write

$$h = \left[\frac{4}{9}\frac{t^2}{r^2 s}\right]. \tag{4.2}$$

Then $G(U, V)$ contains a $K(2, h)$ subgraph, i.e. a complete bipartite subgraph $G'(U', V')$ so that

$$U' = \{U_1', U_2'\} \subset U \quad (\text{with } U_1' \ne U_2'),$$

$$V' = \{V_1', V_2', \dots, V_h'\} \subset V \quad (\text{with } V_i' \ne V_j' \text{ for } i \ne j)$$

and both U_1' and U_2' are joined to each of $V_1', V_2', \dots, V_h'$.

Proof. By the definition of the Zarankiewicz function (Definition 4.2), it suffices to prove that it follows from the assumptions in the lemma that

$$t > Z(r,s;2,h) = Z(s,r;h,2) \tag{4.3}$$

(the last equality is trivial since clearly the change of order of the vertex classes does not change the value of the function). By using Lemma 4.1 with s, r, h and 2 in place of m, n, s and t, respectively, we get

$$Z(s,r;h,2) < (h-1)^{1/2}(r-2+1)s^{1-1/2}+(2-1)s \le (h-1)^{1/2}rs^{1/2}+s.$$

Thus to prove (4.3), it suffices to show that

$$(h-1)^{1/2}rs^{1/2}+s < t,$$

or in equivalent form,

$$(h-1)^{1/2} < \frac{t-s}{rs^{1/2}},$$

$$h-1 < \frac{(t-s)^2}{r^2 s}.$$

So that by (4.1), it suffices to show that

$$h-1 < \frac{\left(\frac{2}{3}t\right)^2}{r^2 s},$$

$$h < \frac{4}{9}\frac{t^2}{r^2 s}+1$$

which holds by (4.2). □

5. Tools from the theory of continued fractions

First we recall some basic facts on continued fractions. We will follow the notation and presentation of [6], Chapter X.

A fraction of the form

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_N}}}} \tag{5.1}$$

is called *continued fraction*. The continued fraction in (5.1) is also denoted by

$$[a_0, a_1, \ldots, a_N]. \tag{5.2}$$

The numbers $a_0, a_1, a_2, \ldots, a_N$ are called *partial quotiens* or simply *quotients*. For $n \in \{0, 1, \ldots, N\}$ the number $[a_0, a_1, \ldots, a_n]$ is called

the n-th *convergent* to $[a_0, a_1, \dots, a_N]$. It can be calculated by the following recursion:

Lemma 5.1. *If p_n and q_n are defined by*

$$p_0 = a_0,\ p_1 = a_1a_0 + 1,\ p_n = a_np_{n-1} + p_{n-2}\ (\textit{for } n \in \{2, 3, \dots, N\}),$$

$$q_0 = 1,\ q_1 = a_1,\ q_n = a_nq_{n-1} + q_{n-2}\ (\textit{for } n \in \{2, 3, \dots, N\}),$$

then

$$[a_0, a_1, \dots, a_n] = \frac{p_n}{q_n}.$$

(This is Theorem 149 in [6].)

If the quotients $a_1, a_2, \dots, a_N$ are positive (a_0 can be zero or negative) and $a_0, a_1, \dots, a_N$ are all integers, then the continued fraction (5.2) is said to be *simple*. From now on we will restrict ourselves to simple continued fractions.

If $a_0, a_1, a_2, \dots$ are integers and $a_1, a_2, \dots$ are positive, then $x_n = [a_0, a_1, \dots, a_n]$ tends to a limit x when $n \to \infty$, and we say that

$$x = [a_0, a_1, \dots], \tag{5.3}$$

and $x_n = \frac{p_n}{q_n} = [a_0, a_1, \dots, a_n]$ are convergents to $[a_0, a_1, \dots]$ (see Theorem 166 in [6]). Note that if the sequence $a_0, a_1, a_2, \dots$ is infinite then x must be irrational, and if x is irrational, then it has a unique representation in form (5.3).

Lemma 5.2. *Of any two consecutive convergents $\frac{p}{q}$ to x in* (5.3)*, one at least satisfies*

$$\left|\frac{p}{q} - x\right| < \frac{1}{2q^2}.$$

(This is Theorem 183 in [6].)

Lemma 5.3. *If x is of form* (5.3) *(so that it is irrational) and*

$$\left|\frac{p}{q} - x\right| < \frac{1}{2q^2}$$

then $\frac{p}{q}$ is a convergent to x.

(This is Theorem 184 in [6].)

We will also need the following lemma:

Lemma 5.4. *If x is an irrational number of form* (5.3) *and $\frac{p_n}{q_n}$ is the n-th convergent to it, then for every $n \in \mathbb{N}$ we have*

$$q_{n+2} > 2q_n.$$

Proof. By Lemma 5.1 we have

$$q_{n+2} = a_{n+2}q_{n+1} + q_n \geq q_{n+1} + q_n > 2q_n.$$

□

(Indeed, Lemmas 5.3 and 5.4 will play an important role in the completion of the proof of our Theorem 2.1.)

6. Case 2: symmetric decomposition

In Section 3 we showed that if the set $\mathcal{R}$ satisfies the assumptions in Theorem 2.1 then it cannot have decomposition of form (2.6) which is *asymmetric*, i.e. it is such that inequality (3.1) of Case 1 holds. It remains to show that there is no *symmetric* decomposition either, i.e. the opposite of (3.1) cannot hold either:

CASE 2. Assume that for some $\varepsilon > 0$ there is a number $X_0 = X_0(\varepsilon)$ such that the sets $\mathcal{A}, \mathcal{B}$ in (2.4) satisfy the inequality

(6.1)
$$\max\{A(X), B(X)\} \leq X^{1/k} \exp\left(-\left(\log 2 + \frac{\varepsilon}{2}\right)\frac{\log X}{\log\log X}\right) \text{ for } X > X_0(\varepsilon).$$

To deduce a contradiction from (2.1)-(2.6) and (6.1), first we introduce some notations. For $X \geq 1$ let $H = H(X)$ denote the smallest positive integer with

$$\left(\frac{4}{3}\right)^H \geq X,$$

so that

$$H = \left\lceil \frac{\log X}{\log 4/3} \right\rceil. \tag{6.2}$$

Write $n_i = \left(\frac{4}{3}\right)^i$ for $i = -1, 0, 1, 2, \ldots$ and $\mathcal{N}_i = \mathbb{N} \cap (n_{i-1}, n_i]$ for $i = 0, 1, 2, \ldots$, and for any $\mathcal{D} \subset \mathbb{N}$ let $\mathcal{D}_i = \mathcal{D} \cap \mathcal{N}_i$. Then clearly we have

$$\{1, 2, \ldots, X\} \subset \bigcup_{i=0}^{H} \mathcal{N}_i. \tag{6.3}$$

Denote the elements of $\mathcal{Q}_H$ by $\bar{q}_1 < \bar{q}_2 < \cdots < \bar{q}_w$. Then by (2.2) and (6.2), for $X \to \infty$ we have

$$w = |\mathcal{Q}_H| = |\mathcal{Q} \cap (n_{H-1}, n_H]| = Q(n_H) - Q(n_{H-1}) =$$

$$= n_H^{1/k} - n_{H-1}^{1/k} + o\left(n_H^{1/k} \exp\left(-(\log 2 + \varepsilon)\frac{\log n_H}{\log\log n_H}\right)\right) =$$

$$= \left(\frac{4}{3}\right)^{H/k} - \left(\frac{4}{3}\right)^{(H-1)/k} + o\left(n_H^{1/k}\ \exp\left(-(\log 2+\varepsilon)\frac{\log n_H}{\log\log n_H}\right)\right) =$$

$$= \left(\frac{4}{3}\right)^{(H-1)/k}\left(\left(\frac{4}{3}\right)^{1/k} - 1\right) + o\left(X^{1/k}\ \exp\left(-(\log 2+\varepsilon)\frac{\log X}{\log\log X}\right)\right)$$

whence

$$w = |\mathcal{Q}_H| > c_5 X^{1/k} \quad \text{for } X > X_0 \tag{6.4}$$

with some positive constant c_5 depending only on k and ε.

By (2.6), for every

$$\bar{q}_\ell \in \mathcal{Q}_H \tag{6.5}$$

there are $a \in \mathcal{A}, b \in \mathcal{B}$ with

$$ab = \bar{q}_\ell. \tag{6.6}$$

Suppose that for some $\bar{q}_\ell$ we have

$$a \in \mathcal{A}_i,\ b \in \mathcal{B}_j, \tag{6.7}$$

i.e.,

$$\left(\frac{4}{3}\right)^{i-1} < a \le \left(\frac{4}{3}\right)^{i}, \quad \left(\frac{4}{3}\right)^{j-1} < b \le \left(\frac{4}{3}\right)^{j}. \tag{6.8}$$

By (6.5) and (6.6) we have

$$ab = \bar{q}_\ell \in \left(\left(\frac{4}{3}\right)^{H-1}, \left(\frac{4}{3}\right)^{H}\right], \tag{6.9}$$

and by (6.8),

$$\left(\frac{4}{3}\right)^{i+j-2} < ab \le \left(\frac{4}{3}\right)^{i+j}. \tag{6.10}$$

It follows from (6.9) and (6.10) that

$$H \le i + j \le H + 1 \tag{6.11}$$

whence

$$j = H - i \text{ or } H - i + 1. \tag{6.12}$$

The index ℓ can be chosen in $w(= |\mathcal{Q}_H|)$ ways in (6.5), and for every $\bar{q}_\ell$ in (6.5) there is at least one pair (a, b) satisfying (6.6) and (6.7) with some i, j. For fixed i, j the number of these pairs is $|\mathcal{A}_i||\mathcal{B}_j|$ thus we must have

$$\sum_i \sum_j |\mathcal{A}_i||\mathcal{B}_j| \ge w \tag{6.13}$$

where by (6.12) clearly

$$i \in \{0, 1, 2, \dots, H\} \tag{6.14}$$

and we have to take all the pairs i, j satisfying (6.12).

Now we will consider the maximal term $|\mathcal{A}_i||\mathcal{B}_j|$ of the double sum on the left hand side of (6.13). By (6.12) and (6.14) this double sum has at most $2(H+1) < 4H$ terms, thus this maximal term satisfies

$$|\mathcal{A}_i||\mathcal{B}_j| > \frac{w}{4H}$$

whence, by (6.2) and (6.4), it follows that if X is large enough, then

$$|\mathcal{A}_i||\mathcal{B}_j| > c_6 \frac{X^{1/k}}{\log X} \tag{6.15}$$

with a positive constant c_6 depending only on k and ε.

Write

$$\mathcal{A}_i = \{a_{e+1}, a_{e+2}, \dots, a_{e+r}\}, \quad \mathcal{B}_j = \{b_{f+1}, b_{f+2}, \dots, b_{f+s}\} \tag{6.16}$$

(with $a_{e+1} < a_{e+2} < \cdots < a_{e+r}$, $b_{f+1} < b_{f+2} < \cdots < b_{f+s}$). We may assume without loss of generality that

$$|\mathcal{A}_i| = r \le |\mathcal{B}_j| = s. \tag{6.17}$$

Then by (6.15) we have

$$rs > c_6 \frac{X^{1/k}}{\log X}, \tag{6.18}$$

and it follows from (6.2), (6.12) and the definition of $\mathcal{B}_j$ that

$$\mathcal{B}_j \subset \left[1, \left(\frac{4}{3}\right)^{H+1}\right] \cap \mathcal{B} \subset [1, 2X] \cap \mathcal{B}, \tag{6.19}$$

thus by (6.1),

$$s = |\mathcal{B}_j| \le B(2X) < X^{1/k} \exp\left(-\left(\log 2 + \frac{\varepsilon}{3}\right) \frac{\log X}{\log\log X}\right) \tag{6.20}$$

for X large enough. By (6.15) and (6.20) we have

$$r = |\mathcal{A}_i| > c_6 \frac{X^{1/k}}{\log X} \cdot \frac{1}{|\mathcal{B}_j|} > \exp\left(\left(\log 2 + \frac{\varepsilon}{4}\right) \frac{\log X}{\log\log X}\right) \tag{6.21}$$

for X large enough.

Now we define a bipartite graph $G(U, V)$ on the vertex classes $U = \{U_1, U_2, \dots, U_r\}$ and $V = \{V_1, V_2, \dots, V_s\}$ so that for $m \in \{1, 2, \dots, r\}$

and $n \in \{1, 2, \dots, s\}$ the vertices U_m and V_n are joined if and only if $a_{e+m}(\in \mathcal{A}_i)$ and $b_{f+n}(\in \mathcal{B}_j)$ are such that

$$a_{e+m}b_{f+n} \in \mathcal{Q}.$$

Moreover, define h as in (4.2):

$$h = \left[\frac{4}{9}\frac{t^2}{r^2 s}\right],$$

where t denotes the number of edges of G. We will show that (4.1) in Lemma 4.1 also holds. To prove this, we have to estimate t. Clearly we have

$$\begin{aligned} t &= |\{(m,n) : 1 \le m \le r,\ 1 \le n \le s,\ a_{e+m}b_{f+n} \in \mathcal{Q}\}| = \\ &= |\{(m,n) : 1 \le m \le r,\ 1 \le n \le s\}| - \\ &|\{(m,n) : 1 \le m \le r,\ 1 \le n \le s,\ a_{e+m}b_{f+n} \notin \mathcal{Q}\}| = \\ &= rs - |\{(m,n) : 1 \le m \le r,\ 1 \le n \le s,\ a_{e+m}b_{f+n} \in \mathcal{S}\}|. \end{aligned} \tag{6.22}$$

If $1 \le m \le r$ and $1 \le n \le s$, then as in (6.8)-(6.12), by (6.2) we have

$$a_{e+m}b_{f+n} \le \left(\frac{4}{3}\right)^{H+1} \le 2X. \tag{6.23}$$

It follows that writing $d(n) = \sum_{d|n} 1$ we have

$$\begin{aligned} &|\{(m,n) : 1 \le m \le r,\ 1 \le n \le s,\ a_{e+m}b_{f+n} \in \mathcal{S}\}| = \\ &= \sum_{\substack{1 \le z \le 2X \\ z \in \mathcal{S}}} |\{(m,n) : 1 \le m \le r,\ 1 \le n \le s,\ a_{e+m}b_{f+n} = z\}| \le \\ &\le \sum_{\substack{1 \le z \le 2X \\ z \in \mathcal{S}}} |\{m : 1 \le m \le r,\ a_{e+m} \mid z\}| \le \\ &\le \sum_{\substack{1 \le z \le 2X \\ z \in \mathcal{S}}} d(z) \le \sum_{\substack{1 \le z \le 2X \\ z \in \mathcal{S}}} \max_{z \le 2X} d(z) = S(2X) \max_{z \le 2X} d(z). \end{aligned} \tag{6.24}$$

Now we need the following lemma:

Lemma 6.1. *If $\varepsilon > 0$, $X > X_0(\varepsilon)$ then we have*

$$\max_{z \le X} d(z) < \exp\left((\log 2 + \varepsilon)\frac{\log X}{\log\log X}\right).$$

Proof. This is a classical theorem of Wigert [17]. (See [8], p.56 for a slightly sharper form of this estimate which, however, would not lead to a significant improvement on our main theorem.) □

It follows from (2.3), (6.24) and Lemma 6.1 that

$$(6.25)\quad |\{(m,n): 1\le m\le r,\ 1\le n\le s,\ a_{e+m}b_{f+n}\in\mathcal{S}\}| =$$
$$= o\left(X^{1/k}\ \exp\left(-(\log 2+\varepsilon)\frac{\log X}{\log\log X}\right)\right)\exp\left(\left(\log 2+\frac{\varepsilon}{2}\right)\frac{\log X}{\log\log X}\right) =$$
$$= o\left(X^{1/k}\ \exp\left(-\frac{\varepsilon}{2}\ \frac{\log X}{\log\log X}\right)\right).$$

By (6.18), (6.22) and (6.25) we have

$$(6.26)\qquad t = rs - o\left(X^{1/k}\ \exp\left(-\frac{\varepsilon}{2}\ \frac{\log X}{\log\log X}\right)\right) = (1+o(1))rs.$$

If X is large enough then (4.1) in Lemma 4.1 holds by (6.17), (6.20), (6.21) and (6.26). Note that by (4.2), (6.21) and (6.26) we also have

(6.27)
$$h = \left[\frac{4}{9}\frac{t^2}{r^2 s}\right] = \left(\frac{4}{9}+o(1)\right)\frac{t}{r} = \left(\frac{4}{9}+o(1)\right)s \ge \left(\frac{4}{9}+o(1)\right)r >$$
$$> \frac{1}{3}\exp\left(\left(\log 2+\frac{\varepsilon}{4}\right)\frac{\log X}{\log\log X}\right)$$

for large X.

So that the graph $G = G(U,V)$ defined above satisfies all the assumptions in Lemma 4.2, thus the lemma can be applied, and we get that there are vertices $U_{i_1}, U_{i_2}, V_{j_1}, V_{j_2}, \dots, V_{j_h}$ with

$$i_1 < i_2,\ j_1 < j_2 < \cdots < j_h$$

so that both U_i's are joined with each of the V_j's. Then by the definition of the graph this means that if we write $\bar a_1 = a_{e+i_1}$, $\bar a_2 = a_{e+i_2}$, $\bar b_1 = b_{f+j_1}, \bar b_2 = b_{f+j_2}, \dots, \bar b_h = b_{f+j_h}$ then we have

$$(6.28)\qquad \bar a_1 < \bar a_2,\ \bar b_1 < \bar b_2 < \cdots < \bar b_h,$$

for $\mu = 1,2$ and $\nu = 1,2,\dots,h$

$$(6.29)\qquad \bar a_\mu \bar b_\nu \in \mathcal{Q}(\subset \mathcal{M}'_k)\quad (\text{for } \mu = 1,2,\ \nu = 1,2,\dots,h),$$

and by $\bar a_\mu \in \mathcal{A}_i$ and $\bar b_\nu \in \mathcal{B}_j$ we also have

$$(6.30)\qquad \left(\frac{4}{3}\right)^{i-1} < \bar a_\mu \le \left(\frac{4}{3}\right)^{i} \text{ and } \left(\frac{4}{3}\right)^{j-1} < \bar b_\nu \le \left(\frac{4}{3}\right)^{j}$$

whence

$$(6.31)\quad \left(\frac{4}{3}\right)^{i+j-2} < \bar a_\mu \bar b_\nu \le \left(\frac{4}{3}\right)^{i+j}\ (\text{for } \mu = 1,2,\ \nu = 1,2,\dots,h).$$

By (6.28) and (6.29) there are pairwise different positive integers $x_1, x_2, \dots, x_h$ and $y_1, y_2, \dots, y_h$, respectively, such that

$$\bar{a}_1\bar{b}_\ell = y_\ell^k + 1,\ \bar{a}_2\bar{b}_\ell = x_\ell^k + 1 \text{ (for } \ell = 1, 2, \dots, h) \tag{6.32}$$

and

$$x_1 < x_2 < \cdots < x_h,\ y_1 < y_2 < \cdots < y_h. \tag{6.33}$$

It follows from (6.32) that

$$\bar{a}_1\bar{a}_2\bar{b}_\ell = \bar{a}_2(y_\ell^k + 1) = \bar{a}_1(x_\ell^k + 1)$$

whence

$$\bar{a}_1 x_\ell^k - \bar{a}_2 y_\ell^k = \bar{a}_2 - \bar{a}_1 \quad (\text{for } \ell = 1, 2, \dots, h). \tag{6.34}$$

By the definitions of $\bar{a}_1$ and $\bar{a}_2$, and by (6.28), $\bar{a}_1$, $\bar{a}_2$ and $\bar{a}_2 - \bar{a}_1$ are positive integers, so that

$$\bar{a}_1 x^k - \bar{a}_2 y^k = \bar{a}_2 - \bar{a}_1 \tag{6.35}$$

is a diophantine equation with positive coefficients, and by (6.33) and (6.34) the pairs $(x_1, y_1), (x_2, y_2), \dots, (x_h, y_h)$ are different solutions of this diophantine equation. Dividing both sides of this equation by the (positive) greatest common divisor of $\bar{a}_1$ and $\bar{a}_2$, we get the diophantine equation

$$Ex^k - Fy^k = G \tag{6.36}$$

with positive integer coefficients

$$E = \frac{\bar{a}_1}{(\bar{a}_1, \bar{a}_2)},\ F = \frac{\bar{a}_2}{(\bar{a}_1, \bar{a}_2)},\ G = \frac{\bar{a}_2 - \bar{a}_1}{(\bar{a}_1, \bar{a}_2)} \tag{6.37}$$

which is equivalent to equation (6.35), and where

$$E \in \mathbb{N},\ F \in \mathbb{N},\ G \in \mathbb{N} \tag{6.38}$$

and

$$(E, F) = 1. \tag{6.39}$$

Moreover, by (6.34) each of the pairs (x_ℓ, y_ℓ) (with $\ell = 1, 2, \dots, h$) considered above is such that it is a solution of equation (6.36), and it satisfies the equations in (6.32) with some $\bar{b}_\ell \in \mathcal{B}_j$, thus by (6.23) and (6.32) we have

$$y_\ell^k + 1 = \bar{a}_1\bar{b}_\ell < \bar{a}_2\bar{b}_\ell = x_\ell^k + 1 \le 2X \text{ for } \ell = 1, 2, \dots, h. \tag{6.40}$$

To deduce a contradiction from the facts above, we have to distinguish two cases.

CASE 2a. Assume first that $\left(\frac{F}{E}\right)^{1/k}$ is an irrational number. Then by the definition of h and since $h \geq 3$ follows from (6.27) for large X, the pairs $(x_1, y_1), (x_2, y_2), (x_3, y_3)$ are solutions of (6.36) so that

$$Ex_i^k - Fy_i^k = G \quad (\text{for } i = 1, 2, 3)$$

whence

$$\left(\frac{x_i}{y_i}\right)^k - \frac{F}{E} = \frac{G}{Ey_i^k}.$$

Thus

$$\left|\frac{x_i}{y_i} - \left(\frac{F}{E}\right)^{1/k}\right| = \frac{G}{Ey_i^k}\left(\sum_{j=0}^{k-1}\left(\frac{x_i}{y_i}\right)^j\left(\frac{F}{E}\right)^{(k-1-j)/k}\right)^{-1} \leq \tag{6.41}$$

$$\leq \frac{G}{Ey_i^k}\left(\frac{F}{E}\right)^{-(k-1)/k} = \frac{G}{E}\left(\frac{E}{F}\right)^{(k-1)/k}\frac{1}{y_i^k} \quad (\text{for } i = 1, 2, 3).$$

By (6.28), (6.30) and (6.37) we have

$$\frac{G}{E}\left(\frac{E}{F}\right)^{(k-1)/k} = \frac{\bar{a}_2 - \bar{a}_1}{\bar{a}_1}\left(\frac{\bar{a}_1}{\bar{a}_2}\right)^{(k-1)/k} < \frac{\bar{a}_2}{\bar{a}_1} - 1 < \frac{4}{3} - 1 = \frac{1}{3}. \tag{6.42}$$

It follows from (6.41) and (6.42) that

$$\left|\frac{x_i}{y_i} - \left(\frac{F}{E}\right)^{1/k}\right| < \frac{1}{2y_i^k} \quad (\text{for } i = 1, 2, 3).$$

We have assumed that $\left(\frac{F}{E}\right)^{1/k}$ is irrational and $k \geq 2$, thus by Lemma 5.3 this inequality implies that $\frac{x_1}{y_1}, \frac{x_2}{y_2}, \frac{x_3}{y_3}$ are convergents to $\left(\frac{F}{E}\right)^{1/k}$. By (6.33) we have $y_1 < y_2 < y_3$. Thus if $\frac{x_1}{y_1}$ is, say, the n-th convergent to $\left(\frac{F}{E}\right)^{1/k}$ so that $x_1 = p_n$, $y_1 = q_n$, then by Lemma 5.4 we must have

$$y_3 \geq q_{n+2} > 2q_n = 2y_1. \tag{6.43}$$

On the other hand, by (6.31), (6.32) and (6.33) we have

$$\left(\frac{4}{3}\right)^{i+j-2} < \bar{a}_1\bar{b}_1 = y_1^k + 1 < y_3^k + 1 = \bar{a}_1\bar{b}_3 < \left(\frac{4}{3}\right)^{i+j}$$

whence

$$\left(\frac{4}{3}\right)^2(y_1^k + 1) > y_3^k + 1. \tag{6.44}$$

It follows from (6.43) and $k \geq 2$ that

$$y_3^k + 1 > (2y_1)^k + 1 = 2^k y_1^k + 1 \geq 4y_1^k + 1 \geq 3y_1^k + 2 > \left(\frac{4}{3}\right)^2(y_1^k + 1)$$

which contradicts (6.44) and this proves that Case 2a cannot occur.

CASE 2b. Assume now that $\left(\frac{F}{E}\right)^{1/k}$ is a rational number, say

$$\left(\frac{F}{E}\right)^{1/k} = \frac{p}{q}$$

with

$$p \in \mathbb{N},\ q \in \mathbb{N} \text{ and } (p,q) = 1, \tag{6.45}$$

whence

$$\frac{F}{E} = \frac{p^k}{q^k}.$$

By (6.38), (6.39) and (6.45) it follows that

$$F = p^k,\ E = q^k.$$

Then equation (6.36) can be rewritten as

$$(qx)^k - (py)^k = G$$

whence

$$(qx - py)\left((qx)^{k-1} + (qx)^{k-2}(py) + \cdots + (py)^{k-1}\right) = G.$$

Here G is a positive integer and if x, y are positive integers then by (6.45) both G and the second factor on the left hand side are positive integers, thus the first factor

$$D = qx - py \tag{6.46}$$

is also a positive integer for which we have

$$D \mid G, \tag{6.47}$$

and

$$(qx)^{k-1} + (qx)^{k-2}(py) + \cdots + (py)^{k-1} = \frac{G}{D}. \tag{6.48}$$

A number D satisfying (6.47) can be chosen in $d(G)$ ways. If D is fixed, then from (6.46) we get $qx = D + py$. Thus we may replace qx in (6.48) by $D + py$, and then we get a polynomial of degree $k-1$ in y on the left hand side with positive coefficients. So the equation can have at most one positive integer solution y. If D and y are fixed, then there is 0 or 1 integer x satisfying (6.46). Thus denoting the number of solutions of equation (6.36) by N we have

$$N \le d(G). \tag{6.49}$$

As in (6.7)-(6.12) and (6.19), we have

$$G \le \bar{a}_2 \in \mathcal{A}_i \subset [1, 2X] \cap \mathcal{A}$$

thus we have

$$G \leq 2X. \tag{6.50}$$

By (6.50) and Lemma 6.1 we get from (6.49) that if X is large enough in terms of ε then we have

$$N < \exp\left(\left(\log 2 + \frac{\varepsilon}{5}\right)\frac{\log X}{\log\log X}\right) \quad (\text{for } X > X_1(\varepsilon)). \tag{6.51}$$

On the other hand, we have seen that each of the pairs (x_1, y_1), $(x_2, y_2), \ldots, (x_h, y_h)$ is a solution of (6.35) and thus also of (6.36) so that we have

$$N \geq h$$

where h is defined by (4.2) thus by (6.27) we have

$$N \geq h = \left[\frac{4}{9}\,\frac{t^2}{r^2 s}\right] > \frac{1}{3}\exp\left(\left(\log 2 + \frac{\varepsilon}{4}\right)\frac{\log X}{\log\log X}\right) \quad (\text{for } X > X_2(\varepsilon)).$$

This contradicts (6.51) for X large enough, so that Case 2b cannot occur either for large X.

Thus in both cases our indirect assumption leads to a contradiction (for large X) which completes the proof of our theorem. □

7. Problems and remarks

As we remarked earlier both Conjecture 1.1 and Conjecture 1.2 seem to be beyond reach in their original form, only slightly weaker theorems of type Theorem A and Theorem 2.1 can be proved. Indeed, in both cases we have to change the conjectured bound for the number of elements changed up to X from $o(X^{1/2})$ (in case of the squares) to

$$o\left(X^{1/2}\ \exp\left(-c\,\frac{\log X}{\log\log X}\right)\right)$$

(and in case of the k-th powers $X^{1/k}$ replaces $X^{1/2}$). The unwanted factor $\exp\left(-c\,\frac{\log X}{\log\log X}\right)$ originates mostly from the application of Wigert's estimate (Lemma 6.1)

$$\max_{z\leq X} d(z) < \exp\left((\log 2 + \varepsilon)\frac{\log X}{\log\log X}\right), \tag{7.1}$$

and this upper bound is nearly sharp. One might like to improve on Theorem A and Theorem 2.1 by showing that there are only "few" z values to consider for which $d(z)$ is nearly as large as the upper bound

in (7.1), and for almost all z the value of $d(z)$ is closer to the average value

$$\frac{1}{X}\sum_{z\le X} d(z) = (1+o(1))\log X.$$

However, even pushing this idea through would lead to the loss of a factor $\log X$ at least, and splitting the sets $\mathcal{A}, \mathcal{B}$ as in (6.7) and (6.8) also leads to the loss of $(\log X)^c$. So that it seems that for sure one must loose a factor $(\log X)^c$ at least. There is a large gap between the factors $(\log X)^c$ and $\exp\left(c\,\frac{\log X}{\log\log X}\right)$, thus we might like to tighten this gap. Already a significant achievement would be to settle the following problem:

Problem 1. Show that Theorem A and Theorem 2.1 can be sharpened so that one may change

$$o\left(X^{1/2}\ \exp\left(-c\,\frac{\log X}{\log\log X}\right)\right)\ \text{and}\ o\left(X^{1/k}\ \exp\left(-c\,\frac{\log X}{\log\log X}\right)\right)$$

elements, respectively, of the given set with an absolute constant c *smaller than* $\log 2$.

Next we propose some similar questions on multivariate polynomials. In [5] we formulated some questions and problems related to totally m-decomposability of sets of shifted products of powers of the form $x^k y^\ell + 1$, and more generally, of sets of values of bivariate polynomials $f(x,y) \in \mathbb{Z}[x,y]$. Now we present some remarks and pose some questions concerning general multivariate polynomials with integral coefficients.

Let $f(x_1, x_2, \dots, x_n) \in \mathbb{Z}[x_1, x_2, \dots, x_n]$ with $n \ge 1$. One may ask when is the set

$$\mathcal{A}_f = \{f(x_1, x_2, \dots, x_n) : x_1, x_2, \dots, x_n \in \mathbb{Z}\} \cap \mathbb{N}$$

totally m-primitive? We may assume that $\mathcal{A}_f$ is infinite, otherwise the question is trivial. One can make the following observation: if f is a homogeneous form, i.e. every term of f has (total) degree D, then for any $X_0 > 0$ the set

$$\mathcal{A}_f \cap (X_0, \infty) \tag{7.2}$$

is m-reducible. Indeed, writing

$$f(x_1, x_2, \dots, x_n) = \sum_{i=1}^{N} a_i x_1^{d_1^{(i)}} x_2^{d_2^{(i)}} \dots x_n^{d_n^{(i)}}$$

with some $N \in \mathbb{N}$, $a_1, a_2, \dots, a_N \in \mathbb{Z} \setminus \{0\}$ and $d_1^{(i)}, d_2^{(i)}, \dots, d_n^{(i)} \in \mathbb{N}$ with

$$d_1^{(i)} + d_2^{(i)} + \cdots + d_n^{(i)} = D$$

for some $D \in \mathbb{N}$, we clearly have

$$\mathcal{A}_f \cap (X_0, \infty) = (\mathcal{A}_f \cap (X_0, \infty)) \cdot \{1, z^D\}$$

for any $z \in \mathbb{N}$, $z > X_0$. Also, if f is the linear combination of powers of x_i, say

$$f(x_1, x_2, \dots, x_n) = \sum_{j=1}^{n} b_j x_j^{t_j}$$

with integers b_j and positive integers t_j $(j = 1, \dots, n)$ then letting $T = \operatorname*{lcm}_{1 \le j \le n} t_j$, for any $X_0 > 0$ and $z > X_0$ we have

$$\mathcal{A}_f \cap (X_0, \infty) = (\mathcal{A}_f \cap (X_0, \infty)) \cdot \{1, z^T\}.$$

That is, $\mathcal{A}_f \cap (X_0, \infty)$ is m-reducible again. Moreover, if f is linear in one of its variables, say in x_1, then the set (7.2) can be m-reducible again. Indeed, write

$$f(x_1, x_2, \dots, x_n) = g(x_2, \dots, x_n)x_1 + h(x_2, \dots, x_n),$$

and take arbitrary $u_2, \dots, u_n \in \mathbb{Z}$ such that $g(u_2, \dots, u_n) \neq 0$. Put

$$g_0 = g(u_2, \dots, u_n), \quad h_0 = h(u_2, \dots, u_n).$$

If $g_0 \mid h_0$, then letting $X_1 = \left|\frac{h_0}{g_0}\right|$, for any $z \in \mathbb{N}$ with $z > X_1$ we clearly have $z|g_0| \in \mathcal{A}_f$. Thus for any $z \in \mathbb{N}$ with $z > \max\{X_0, X_1\}$ we have

$$\mathcal{A}_f \cap (X_0, \infty) = (\mathcal{A}_f \cap (X_0, \infty)) \cdot \{1, z|g_0|\}.$$

Perhaps, it is possible to give a complete characterization of the polynomials f that are linear in one of their variables, and for which $\mathcal{A}_f \cap \mathbb{N}$ is not totally m-primitive. More precisely, we propose the following problem.

Problem 2. Characterize the polynomials $g(x_2, \dots, x_n), h(x_2, \dots, x_n) \in \mathbb{Z}[x_2, \dots, x_n]$ for which the set

$$\{x_1 g(x_2, \dots, x_n) + h(x_2, \dots, x_n) : x_1, x_2, \dots, x_n \in \mathbb{Z}\} \cap \mathbb{N}$$

is totally m-primitive.

Already the case $n = 2$ is of interest, so we formulate the following special case of Problem 2 separately:

Problem 3. Characterize the polynomials $g(y), h(y) \in \mathbb{Z}[y]$ for which the set

$$\{xg(y) + h(y) : x, y \in \mathbb{Z}\} \cap \mathbb{N}$$

is totally m-primitive.

In particular,

Problem 4. Is the set

$$\{x(y^2+2)+1 : x, y \in \mathbb{Z}\} \cap \mathbb{N}$$

totally m-primitive?

Note that if we write y^2+1 in place of y^2+2 above then we get a trivial problem, since then (taking $x \geq 0$ and $y = 0$) the above set is just $\mathbb{N}$.

It would be very interesting to see a characterization of totally m-primitivity in the general case. We do not formulate this problem more precisely, since already finding the exact conditions may be challenging. (Though, on the other hand, it might happen that the three cases indicated above, in some sense cover all the possible m-reducible cases.) For example, the range of the polynomial $f(x, y) = x^2 + 2xy^2 + y^4$ is *not* totally m-primitive: indeed, for any large z we have

$$(\{x^2+2xy^2+y^4 : x, y \in \mathbb{Z}\} \cap \mathbb{N}) \cap (X_0, \infty) =$$
$$= ((\{x^2+2xy^2+y^4 : x, y \in \mathbb{Z}\} \cap \mathbb{N}) \cap (X_0, \infty)) \cdot \{1, z^4\}.$$

Observe that f does not belong to any of the three families above, however, $f(x, y)$ is obtained from a form by a simple substitution. (Namely, we have $f(x, y) = (x+y^2)^2$.) We still formulate a simple case as a concrete problem (whose solution may be the first step towards a general theorem).

Problem 5. Let k, ℓ be positive integers greater than one. Is it true that the set

$$\{x^k + y^\ell + 1 : x, y \in \mathbb{Z},\ (x, y) \neq 0\}$$

is totally m-primitive?

Note that this problem is the additive analogue of Conjecture 1 from [5], where polynomials of the shape $x^k y^\ell + 1$ are considered.

In case of Problems 2, 3 and 5 it could be interesting already giving possibly general sufficient conditions for totally primitivity of large families of sets in question.

References

[1] A. Baker, *Contributions to the theory of Diophantine equations. I. On the representation of integers by binary forms*, Phil. Trans. R. Soc. London Ser. A **263** (1968), 173–191.

[2] B. Bollobás, *Modern Graph Theory*, Springer, 1998.

[3] K. Fried and K. Gyarmati, *On multiplicative bases of finite sets*, Integers (to appear).
[4] L. Hajdu and A. Sárközy, *On multiplicative decompositions of polynomial sequences, I*, Acta Arith. **184** (2018), 139–150.
[5] L. Hajdu and A. Sárközy, *On multiplicative decompositions of polynomial sequences, II*, Acta Arith. **186** (2018), 191–200.
[6] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers, 6th ed.*, Oxford University Press, 2008.
[7] P. Mihăilescu, *Primary Cyclotomic Units and a Proof of Catalan's Conjecture*, J. Reine angew. Math. **572** (2004), 167–195.
[8] H. L. Montgomery and R. C. Vaughan, *Multiplicative Number Theory, I. Classical Theory*, Cambridge Univ. Press, Cambridge, 2007.
[9] H.-H. Ostmann, *Untersuchungen über den Summenbegriff in der additiven Zahlentheorie*, Math. Ann. **120** (1948), 165–196.
[10] H.-H. Ostmann, *Additive Zahlentheorie*, Springer, Berlin, 1956.
[11] A. Sárközy, *On additive decomposition of the set of quadratic residues modulo p*, Acta Arith. **155** (2012), 41–51.
[12] A. Sárközy, *On multiplicative decompositions of the set of shifted quadratic residues modulo p*, in: Number Theory, Analysis and Combinatorics, W. de Gruyter, 2014; pp. 295–307.
[13] A. Sárközy and E. Szemerédi, *On the sequence of squares*, Mat. Lapok **16** (1965), 76–85 (in Hungarian).
[14] J. D. Shkredov, *Sumsets in quadratic residues*, Acta Arith. **164** (2014), 221–243.
[15] T. Shorey, R. Tijdeman, *Exponential Diophantine equations*, Cambridge University Press, 1986, pp. 240.
[16] I. E. Shparlinski, *Additive decompositions of subgroups of finite fields*, SIAM J. Discrete Math. **27** (2013), 1870–1879.
[17] S. Wigert, *Sur l'ordre de grandeur du nombre des diviseurs d'un entier*, Ark. Mat. **3** (1906/7), 1–9.

L. Hajdu
University of Debrecen, Institute of Mathematics
H-4010 Debrecen, P.O. Box 12.
Hungary
E-mail address: hajdul@science.unideb.hu

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