ON MULTIPLICATIVE DECOMPOSITIONS OF POLYNOMIAL SEQUENCES

L. HAJDU AND A. SÁRKÖZY

Dedicated to Robert Tijdeman on the occasion of his 75th birthday.

ABSTRACT. In this paper we consider the multiplicative decomposability of the set of values assumed by a quadratic polynomial. First we show that any large set of shifted squares is multiplicatively primitive. Then we sharpen and extend this result in various directions.

1. INTRODUCTION

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*

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

If

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

then this 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

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

hold then (1.2) is called a multiplicative decomposition or briefly m-decomposition of $\mathcal{A}$.

In 1948 H. H. Ostmann [6, 7] introduced some definitions and 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 reducible if it has an (additive) decomposition*

$$\mathcal{A} = \mathcal{B} + \mathcal{C} \quad \text{with} \quad |\mathcal{B}| \geq 2,\ |\mathcal{C}| \geq 2. \tag{1.3}$$

2010 *Mathematics Subject Classification.* 11N25, 11N32, 11D09.

Key words and phrases. Multiplicative decomposition, shifted squares, quadratic polynomials, Pell equations.

Research supported in part by the NKFIH grants K115479 and K119528.

If there are no sets $\mathcal{B},\mathcal{C}$ with these properties then $\mathcal{A}$ is said to be primitive or 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 primitive if every $\mathcal{A}'$ with $\mathcal{A}'\sim\mathcal{A}$ is primitive.*

Observe that Definition 1.2 can be extended from non-negative integers to any semigroup $\mathcal{G}$, and if $\mathcal{G}$ is an additive semigroup then we may speak of a-reducibility, a-primitivity and a-irreducibility, while if a multiplication is defined in $\mathcal{G}$ and (1.3) is replaced by

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

then we may speak of m-reducibility, m-primitivity and m-irreducibility. Correspondingly, 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, and an infinite set $\mathcal{B}$ of positive integers is said to be totally m-primitive if every $\mathcal{B}'$ with $\mathcal{B}'\sim\mathcal{B}$ is m-primitive.

Ostmann also formulated the following beautiful conjecture:

Conjecture 1.1. *The set $\mathcal{P}$ of primes is totally a-primitive.*

Hornfeck, Hofmann and Wolke, Elsholtz and Puchta proved partial results toward this conjecture (see [4] for references), however, the conjecture is still open. Elsholtz [2] also studied multiplicative decompositions of shifted sets $\mathcal{P}'+\{a\}$ with $\mathcal{P}'\sim\mathcal{P}$.

Another related conjecture was formulated by Erdős:

Conjecture 1.2. *If we change $o(n^{1/2})$ elements of the set*

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

of squares up to n, then the new set is always totally a-primitive.

The second author and Szemerédi [11] proved this conjecture in the following slightly weaker form:

Theorem A. *If $\varepsilon>0$ and we change $o(n^{1/2-\varepsilon})$ elements of the set of the squares up to n, then we get a totally a-primitive set.*

(More precisely, this was proved in [11] with $o(n^{1/2}2^{-(3+\varepsilon)\log n/\log\log n})$ in place of $o(n^{1/2-\varepsilon})$.)

In the papers mentioned above decompositions of certain sets of integers have been studied. The second author [9] proposed to study analogous problems in finite fields. He conjectured in [9] that

Conjecture 1.3. *For every prime p the set*

$$Q = \{n : n \in \mathbb{F}_p,\ \left(\frac{n}{p}\right) = +1\} \tag{1.5}$$

of the quadratic residues modulo p is a-primitive.

Later he also conjectured [10]:

Conjecture 1.4. *For every prime large enough and every $c \in \mathbb{F}_p$, $c \neq 0$ the set Q'_c defined by*

$$Q'_c = (Q + \{c\}) \setminus \{0\} = Q_c \setminus \{0\}$$

(where Q is defined by (1.5)) is m-primitive.

Towards both Conjectures 1.3 and 1.4 partial results have been proved by the second author [9, 10], Shkredov [13] and Shparlinski [15], however, both conjectures are still open.

Further related references are presented in [4].

In Conjecture 1.2 and Theorem A we consider additive decomposability of sets composed from the set $\mathcal{M}$ of squares appearing in (1.4). In this paper our main goal is to study multiplicative decomposablity of sets of this type. Clearly, the set $\mathcal{M}$ itself is m-reducible since we have $\mathcal{M} = \mathcal{M} \cdot \mathcal{M}$. Thus if we are looking for a non-trivial problem on the m-decomposability (or rather the lack of decomposability, i.e., m-primitivity) of sets related to $\mathcal{M}$, then we have to switch from the study of $\mathcal{M}$ to the study of the set

$$\mathcal{M}' = \mathcal{M} + \{1\} = \{1, 2, 5, 10, \ldots, x^2 + 1, \ldots\} \tag{1.6}$$

of shifted squares. (Note that similar shifting happens in many other problems, see e.g. [2, 10, 8].) So that in this paper we will start out from the following problem:

Problem 1. Is it true that the set $\mathcal{M}'$ of shifted squares defined in (1.6) is m-primitive?

(Observe that this is the integer analogue of of the problem formulated in Conjecture 1.4.) We will show that the answer to this question is affirmative, and we will sharpen and extend this result in various directions. However, in this paper we will stick to the case when the polynomials involved (like the polynomial $x^2 + 1$ in (1.6)) are of second degree, and both the case of higher order polynomials and the multiplicative analogues of Theorem A will be studied in the sequel(s) of this paper.

Throughout this paper we will use the following notations: $\mathcal{A}, \mathcal{B}, \mathcal{C}, \ldots$ will denote (usually infinite) sets of positive integers, and their counting

functions will be 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 will be denoted by $\mathbb{N}$.

2. Large subsets of the shifted squares are totally m-primitive

First we will show that if the counting function of a subset of $\mathcal{M}'$ increases faster than $\log x$, then the subset must be m-primitive:

Theorem 2.1. *If*

$$\mathcal{R} = \{r_1, r_2, \ldots\} \subset \mathcal{M}', \quad r_1 < r_2 < \ldots, \tag{2.1}$$

and $\mathcal{R}$ is such that

$$\limsup_{x \to +\infty} \frac{R(x)}{\log x} = +\infty, \tag{2.2}$$

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

Proof. We will prove by contradiction: assume that contrary to the statement of the theorem there are $\mathcal{R}' \subset \mathbb{N}$, n_0, $\mathcal{B} \subset \mathbb{N}$, $\mathcal{C} \subset \mathbb{N}$ such that

$$\mathcal{R}' \cap [n_0, +\infty) = \mathcal{R} \cap [n_0, +\infty), \tag{2.3}$$

$$|\mathcal{B}| \ge 2, \quad |\mathcal{C}| \ge 2 \tag{2.4}$$

and

$$\mathcal{R}' = \mathcal{B} \cdot \mathcal{C}. \tag{2.5}$$

We have to distinguish two cases:

Case 1. Assume that either

$$|\mathcal{B}| = 2 \tag{2.6}$$

or

$$|\mathcal{C}| = 2;$$

we may assume that (2.6) holds, and let $\mathcal{B} = \{b_1, b_2\}$ with $b_1 < b_2$.

By (2.2) and (2.3) there are arbitrarily large integers K and N such that

$$R'(N) > K \log N; \tag{2.7}$$

by taking such numbers K and N large enough in terms of n_0, b_1 and b_2 we can achieve that

$$\{b_1, b_2\} \cdot (\mathcal{C} \cap [0, N]) \supset \mathcal{R}' \cap [0, N]$$

holds, and then by (2.5) and (2.7) it follows that

$$2C(N) \ge R'(N) > K \log N. \tag{2.8}$$

Now assume that $N > n_0$ and write

$$\tilde{\mathcal{C}} = \mathcal{C} \cap (n_0, N]. \tag{2.9}$$

Then by (2.8) we have

$$|\tilde{\mathcal{C}}| = C(N) - C(n_0) > \frac{K}{2} \log N - n_0 > \frac{K}{3} \log N \tag{2.10}$$

(if $N \geq 2$ and K is large enough in terms of n_0).

Consider any $c \in \tilde{\mathcal{C}}$. Then

$$n_0 \leq b_1 n_0 < b_1 c < b_2 c \leq b_2 N, \tag{2.11}$$

and by (2.3), (2.5) and (2.11) we have

$$b_1 c \in \mathcal{R}' \cap (n_0, b_2 N] \quad \text{and} \quad b_2 c \in \mathcal{R}' \cap (n_0, b_2 N]. \tag{2.12}$$

It follows from (2.1), (2.3) and (2.12) that

$$b_1 c \in \mathcal{M}' \quad \text{and} \quad b_2 c \in \mathcal{M}',$$

thus there are $x \in \mathbb{N}$, $y \in \mathbb{N}$ with

$$b_2 c = x^2 + 1, \quad b_1 c = y^2 + 1 \tag{2.13}$$

whence

$$0 = b_1(b_2 c) - b_2(b_1 c) = b_1(x^2 + 1) - b_2(y^2 + 1) = b_1 x^2 - b_2 y^2 - (b_2 - b_1)$$

so that

$$b_1 x^2 - b_2 y^2 = b_2 - b_1. \tag{2.14}$$

Observe that by (2.11) and (2.13) we have

$$\max(|x|^2, |y|^2) < b_2 c \leq b_2 N$$

whence

$$\max(|x|, |y|) \leq (b_2 N)^{1/2} \leq N \tag{2.15}$$

if

$$N \geq b_2.$$

For every $c \in \tilde{\mathcal{C}}$ the positive integers x, y defined by (2.13) satisfy (2.14) and (2.15) so that by (2.10) we have

$$\left|\{(x, y) \in \mathbb{Z}^2 : b_1(x^2 + 1) = b_2(y^2 + 1) \text{ with } \max(|x|, |y|) \leq N\}\right| \geq$$
$$\geq |\tilde{\mathcal{C}}| > \frac{K}{3} \log N. \tag{2.16}$$

Now we will prove

Lemma 2.1. *Let $f(z) = uz^2+vz+w$ with $u, v, w \in \mathbb{Z}$, $u(v^2-4uw) \neq 0$, and let k, ℓ be distinct positive integers. Then there exists an effectively computable constant $C_0 = C_0(u, v, w, k, \ell)$ such that*

$$\left|\left\{(x, y) \in \mathbb{Z}^2 : kf(x) = \ell f(y) \text{ with } \max(|x|, |y|) < N\right\}\right| < C_0 \log N,$$

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

Proof. Throughout the proof, $C_1, C_2, \dots$ will denote effectively computable constants depending only on u, v, w, k, ℓ.

Write $k\ell = dt^2$ where d is square-free. Then by a simple calculation the equation $kf(x) = \ell f(y)$ can be rewritten as

$$X^2 - dY^2 = c \tag{2.17}$$

with

$$X = 2kux + kv, \quad Y = 2uty + vt, \quad c = k(k-\ell)(v^2 - 4uw).$$

Observe that in case of $d = 1$ both $X - Y$ and $X + Y$ are divisors of c, hence as $c \neq 0$, equation (2.17) allows only C_1 solutions in X, Y in this case. This clearly yields that there are at most C_2 pairs (x, y) with $kf(x) = \ell f(y)$ whenever $d = 1$. Thus we may assume that $d > 1$. Then (2.17) is a (general) Pell type equation. As it is well-known (see e.g. Theorem 1 on p. 118 of [1] or Corollary A.6 on p. 25 of [14]), if (X, Y) is a solution to equation (2.17) then we have

$$X + \sqrt{d}Y = \mu\varepsilon^s \quad \text{and} \quad X - \sqrt{d}Y = \nu\varepsilon^m.$$

Here $s, m \in \mathbb{Z}$ and ε is a generator of the subgroup of units of $\mathbb{Z}[\sqrt{d}]$ having norm $+1$. Further, μ, ν belong to some fixed finite subset Γ of $\mathbb{Z}[\sqrt{d}]$ such that $|\Gamma| < C_3$, and for all $\gamma \in \Gamma$ we have $N_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(\gamma) = c$ and $|\gamma| > C_4$. Note that the first assertion follows e.g. from Theorem 5 and its proof on p. 90 of [1], and for the last assertion we also need Theorem A.3 of [14] on p. 26 (which is in fact a theorem of Landau [5]), and also the equality $\min(|\gamma|, |\bar{\gamma}|) = |c|/\max(|\gamma|, |\bar{\gamma}|)$ for any $\gamma \in \Gamma$. Here $\bar{\gamma}$ is the conjugate of γ over $\mathbb{Q}(\sqrt{d})$. We may further assume that $|\varepsilon| > 1$. Then, as it is well-known (see e.g. results of Schinzel [12] being valid in much more general settings) we have $|\varepsilon| \geq (1 + \sqrt{5})/2$. Observe that by taking conjugates, this implies that

$$X + \sqrt{d}Y = \tau\varepsilon^n \quad \text{or} \quad X - \sqrt{d}Y = \tau\varepsilon^n$$

is valid with some $\tau \in \Gamma$ and non-negative integer n. For any fixed $\tau \in \Gamma$, write (X_n, Y_n) for the solution corresponding to n, and (x_n, y_n) for the values we get from the inverse of the substitutions after (2.17). Then we have

$$(1 + \sqrt{d}) \max(|X_n|, |Y_n|) > C_4((1 + \sqrt{5})/2)^n,$$

which easily yields that apart from at most C_5 pairs (x_n, y_n) also

$$\max(|x_n|, |y_n|) > C_6((1+\sqrt{5})/2)^n.$$

This shows that for these values of n, $N > \max(|x_n|, |y_n|)$ implies $n < C_7 \log N$. Since the number of possible values of τ is bounded by C_3, the lemma follows. □

We may apply this lemma with

$$f(z) = z^2 + 1,$$

$k = b_1$, $\ell = b_2$ since then the conditions in the lemma hold. We obtain that there exists an effectively computable constant $C_1 = C_1(b_1, b_2)$ such that

$$\left|\{(x,y) \in \mathbb{Z}^2 : b_1(x^2+1) = b_2(y^2+1) \text{ with } \max(|x|,|y|) < N\}\right| < \\ < C_1 \log N. \quad (2.18)$$

If we have

$$K > 3C_1$$

then (2.18) contradicts (2.16) which proves that Case 1 cannot occur.

Case 2. Assume that

$$|\mathcal{B}| \geq 3 \quad \text{and} \quad |\mathcal{C}| \geq 3. \quad (2.19)$$

By (2.2) and (2.19) there are infinitely many integers N such that

$$R(N) > 2 \log N \quad (2.20)$$

and

$$B(N) \geq 3, \quad C(N) \geq 3. \quad (2.21)$$

Consider an integer N large enough, in particular satisfying (2.20), and let

$$\sqrt{\log N} > 2n_0. \quad (2.22)$$

By (2.3) and (2.5), every

$$r \in \mathcal{R} \cap [n_0, N] \quad (2.23)$$

can be written in the form

$$r = bc$$

with

$$b \in \mathcal{B} \cap [1, N], \quad c \in \mathcal{C} \cap [1, N]. \quad (2.24)$$

Thus the number of r's satisfying (2.23) is at most as large as the number of pairs (b, c) satisfying (2.24) which is $B(N)C(N)$, and this is

$$B(N)C(N) \geq |\{r : r \in \mathcal{R} \cap (n_0, N]\}| = R(N) - R(n_0) \geq R(N) - n_0,$$

whence, by (2.20) and (2.22), for N large

$$B(N)C(N) > \log N. \tag{2.25}$$

We may assume that $B(N) \le C(N)$. Then it follows from (2.25) that

$$C(N) > \sqrt{\log N}. \tag{2.26}$$

Define $\tilde{\mathcal{C}}$ again by (2.9). Then by (2.22) and (2.26) we have

$$|\tilde{\mathcal{C}}| = C(N) - C(n_0) \ge C(N) - n_0 > \frac{1}{2}\sqrt{\log N}. \tag{2.27}$$

For every $c \in \tilde{\mathcal{C}}$, consider the integers

$$b_i c \quad \text{with } i = 1, 2, 3.$$

Each of these integers satisfies

$$b_i c \in \mathcal{B} \cdot \mathcal{C} = \mathcal{R}'$$

and

$$b_i c \ge c > n_0,$$

thus by (2.3) we have

$$b_i c \in \mathcal{R}' \cap [n_0, +\infty) = \mathcal{R} \cap [n_0, +\infty) \subset \mathcal{R} \subset \mathcal{M}',$$

thus there are positive integers x, y, z with

$$b_1 c = z^2 + 1, \tag{2.28}$$

$$b_2 c = x^2 + 1, \tag{2.29}$$

$$b_3 c = y^2 + 1. \tag{2.30}$$

It follows from these equations that

$$b_3(x^2 + 1) - b_2(y^2 + 1) = b_3 b_2 c - b_2 b_3 c = 0$$

and

$$b_1(x^2 + 1) - b_2(z^2 + 1) = b_1 b_2 c - b_2 b_1 c = 0$$

whence, writing

$$f(t) = t^2 + 1, \tag{2.31}$$

the positive integers x, y and z satisfy the system of equations

$$b_3 f(x) = b_2 f(y), \quad b_1 f(x) = b_2 f(z). \tag{2.32}$$

By (2.27), the number of these triples x, y, z defined by (2.28), (2.29) and (2.30) is

$$|\tilde{\mathcal{C}}| > \frac{1}{2}\sqrt{\log N},$$

so that

$$|\{(x, y, z) \in \mathbb{N}^3 : x, y, z \text{ satisfy (2.32)}\}| > \frac{1}{2}\sqrt{\log N}. \tag{2.33}$$

Now we will need

Lemma 2.2. *Let $f(t) = ut^2 + vt + w$ with $u, v, w \in \mathbb{Z}$, $u(v^2 - 4uw) \neq 0$, and let k, ℓ, m be distinct positive integers. Then there exists an effectively computable constant $C^* = C^*(u, v, w, k, \ell, m)$ such that all integer solutions x, y, z of the system of equations*

$$\ell f(x) = kf(y), \quad mf(x) = kf(z) \tag{2.34}$$

satisfy

$$\max(|x|, |y|, |z|) < C^*.$$

Proof. By a simple calculation, the system (2.34) can be rewritten as

$$\ell X^2 - kY^2 = (\ell - k)\Delta, \quad mX^2 - kZ^2 = (m - k)\Delta,$$

where

$$X = 2ux + v, \quad Y = 2uy + v, \quad Z = 2uz + v, \quad \Delta = v^2 - 4uw.$$

Corollary 6.1 on p. 114 of [14] implies that here either $\max(|X|, |Y|, |Z|)$ is effectively bounded in terms of u, v, w, k, ℓ, m, or $(\ell - k)(m - k)$ is a square and $\frac{\ell-k}{m-k} = \frac{\ell}{m}$. However, one can readily check that the last assertion cannot hold. Thus the lemma follows. □

Since the polynomial $f(t)$ in (2.31) satisfies the conditions in Lemma 2.2 and the coefficients b_1, b_2, b_3 in (2.32) are positive integers, we may apply Lemma 2.2 in order to estimate the size of the solutions (x, y, z) of the system (2.32). We obtain that these solutions satisfy (2.34), thus their number is bounded; but this fact contradicts (2.33) for N large enough, and this completes the proof of Theorem 2.1. □

3. Theorem 2.1 is nearly sharp

Now we will prove that Theorem 2.1 is nearly sharp, more precisely,

Theorem 3.1. *There is a subset $\mathcal{R} \subset \mathcal{M}'$ and a number x_0 such that for $x > x_0$ we have*

$$R(x) > \frac{1}{\log 51} \log x. \tag{3.1}$$

Proof. Denote the solutions of the Pell equation

$$y^2 - 2z^2 = 1 \tag{3.2}$$

(ordered increasingly) by $(y_1, z_1) = (3, 2)$, $(y_2, z_2) = (17, 12)$, …, (y_n, z_n), …; it is known from the theory of the Pell equations (see e.g. Section 5 of Chapter 2 of [1]) that the positive integers y_n, z_n are defined by

$$y_n + z_n\sqrt{2} = (y_1 + z_1\sqrt{2})^n = (3 + 2\sqrt{2})^n. \tag{3.3}$$

Then define the subset $\mathcal{R} \subset \mathcal{M}'$ by

$$\mathcal{R} = \{z_1^2 + 1, \dots, z_n^2 + 1, \dots\} \cup \{y_1^2 + 1, \dots, y_n^2 + 1, \dots\}. \tag{3.4}$$

Then it follows from (3.2) that

$$2(z_n^2 + 1) = y_n^2 + 1,$$

thus we have

$$\{1, 2\} \cdot \{z_1^2 + 1, z_2^2 + 1, \dots, z_n^2 + 1, \dots\} = \mathcal{R} \tag{3.5}$$

so that $\mathcal{R}$ is m-reducible.

Moreover, by (3.3) we have

$$y_{n+1} + z_{n+1}\sqrt{2} = (y_1 + z_1\sqrt{2})^{n+1} = (y_1 + z_1\sqrt{2})(y_1 + z_1\sqrt{2})^n =$$
$$= (y_1 + z_1\sqrt{2})(y_n + z_n\sqrt{2}) = (y_1 y_n + 2z_1 z_n) + (y_1 z_n + y_n z_1)\sqrt{2}$$

whence

$$y_{n+1} = y_1 y_n + 2z_1 z_n = 3y_n + 4z_n \tag{3.6}$$

and

$$z_{n+1} = y_1 z_n + z_1 y_n = 2y_n + 3z_n. \tag{3.7}$$

y_n and z_n are positive and their coefficients in the last sum in (3.6) are greater than in (3.7), thus we have

$$y_{n+1} > z_{n+1} \quad (\text{for } n = 0, 1, \dots). \tag{3.8}$$

Then it follows from (3.6) and (3.8) that

$$y_{n+1} < 7y_n,$$

thus we get by induction that

$$y_n < 7^n \quad \text{for } n = 1, 2, \dots,$$

whence

$$y_n^2 + 1 < 50^n \quad \text{for } n = 1, 2, \dots.$$

If for some n and x we have

$$50^n \le x, \tag{3.9}$$

then, by (3.4),

$$\{y_1^2 + 1, y_2^2 + 1, \dots, y_n^2 + 1\} \subset \mathcal{R} \cap (0, x],$$

thus

$$R(x) \ge n. \tag{3.10}$$

(3.9) holds with

$$n = \left[\frac{\log x}{\log 50}\right] \tag{3.11}$$

so that for large x (3.1) follows from (3.10) and (3.11). □

We remark that the construction presented in the proof of Theorem 3.1 can be generalized. There we started out from the Pell equation $y^2 - 2z^2 = 1$. If we consider a positive integer $k > 1$ for which the equation

$$y^2 - kz^2 = k - 1$$

has non-trivial solution (e.g. this holds for $k = 5$ when $y = 3$, $z = 1$ is a solution), and we denote its positive integer solutions (in increasing order) by $(y_1, z_1), (y_2, z_2), \ldots$, then we have

$$\{1, k\} \cdot \{z_1^2 + 1, z_2^2 + 1, \ldots, z_n^2 + 1, \ldots\} = \\ = \{z_1^2 + 1, \ldots, z_n^2 + 1, \ldots\} \cup \{y_1^2 + 1, \ldots, y_n^2 + 1, \ldots\} \subset \mathcal{M}'$$

so that the set

$$\{z_1^2 + 1, \ldots, z_n^2 + 1, \ldots\} \cup \{y_1^2 + 1, \ldots, y_n^2 + 1, \ldots\}$$

is m-reducible, and its counting function increases faster, than $c \log x$.

4. General polynomials of second degree

In this section we investigate the m-decomposability of of the set of the values assumed by general quadratic polynomials. Though we could also discuss this situation in the generality of the previous sections, we shall restrict ourselves to the investigation of the main property of totally m-primitivity. So we prove the following

Theorem 4.1. *Let f be a polynomial with integer coefficients of degree two having positive leading coefficient, and set*

$$\mathcal{M}_f = \{f(x) : \ x \in \mathbb{Z}\} \cap \mathbb{N}.$$

Then $\mathcal{M}_f$ is totally m-primitive if and only if f is **not** *of the form $f(z) = a(bz + c)^2$ with integers a, b, c, $a > 0, b > 0$.*

Proof. Assume first that f is of the form $f(z) = a(bz+c)^2$ with $a, b, c \in \mathbb{Z}$, $a > 0, b > 0$. Then one can readily check that e.g.

$$\mathcal{M}_f = \{1, (b + 1)^2\} \cdot \mathcal{M}_f.$$

Suppose next that $\mathcal{M}_f$ is not totally m-primitive. To describe those f for which this is the case, we can closely follow the proof of Theorem 2.1, even with some simplifications. Let $n_0 \in \mathbb{N}$ and $\mathcal{A}, \mathcal{B}, \mathcal{C} \subset \mathbb{N}$ such that $\mathcal{M}_f \cap [n_0, +\infty) = \mathcal{A} \cap [n_0, +\infty)$, $|\mathcal{B}| \geq 2$, $|\mathcal{C}| \geq 2$ and $\mathcal{A} = \mathcal{B} \cdot \mathcal{C}$. We may assume that $B(n) \leq C(n)$ for infinitely many $n \in \mathbb{N}$. Let $b_1, b_2 \in \mathcal{B}$ with $b_1 \neq b_2$, and let $N \in \mathbb{N}$ to be specified later. For all $c \in \mathcal{C}$ with $c \leq N$ we have

$$b_1 c = f(x) \quad \text{and} \quad b_2 c = f(y) \tag{4.1}$$

with some $x, y \in \mathbb{Z}$. Observe that we have $\max(|x|, |y|) < C_1\sqrt{N}$, where C_1 is a constant depending only on b_1, b_2 and f. If N is chosen such that $C(N) \geq B(N)$, and also N is large enough in terms of n_0, then we clearly have $C(N) \geq \sqrt{A(N)} \geq C_2\sqrt[4]{N}$ with some constant C_2 depending only on n_0 and f. Then equation (4.1) yields that

$$b_2 f(x) - b_1 f(y) = 0$$

has $C_2\sqrt[4]{N}$ solutions in $(x, y) \in \mathbb{Z}^2$ with $\max(|x|, |y|) < C_1\sqrt{N}$. Now if N is chosen to be large enough, by Lemma 2.1 this shows that the above Pell type equation must be degenerate. That is, writing $f(z) = uz^2 + vz + w$, as $u \neq 0$, we must have $v^2 - 4uw = 0$. This immediately gives that f has a double rational root, say p/q with $\gcd(p, q) = 1$, $q > 0$, and $f(z) = u(z - p/q)^2$. Then $q^2 \mid u$, and writing $u = aq^2$ we get $f(z) = a(qz - p)^2$. Hence the theorem follows. □

References

[1] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, 1966, pp. 435.

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

[3] M. Z. Garaev and S. V. Konyagin, *Multiplicative decomposition of arithmetic progressions in prime fields*, J. Number Theory **145** (2014), 540–553.

[4] K. Gyarmati and A. Sárközy, *On reducible and primitive subsets of $\mathbb{F}_p$, I*, Integers **15A** (2015), No. A6, 21 pp.

[5] E. Landau, *Verallgemeinerung eines Pólyaschen Satzes auf algebraische Zahlkörper*, Nachr. Ges. Wiss. Göttingen (1918), 478–488.

[6] H.-H. Ostmann, *Untersuchungen über den Summenbegriff in der additiven Zahlentheorie*, Math. Ann. **120** (1948), 165–196.

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

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

[9] A. Sárközy, *On additive decomposition of the set of quadratic residues modulo p*, Acta Arith. **155** (2012), 41–51.

[10] A. Sárközy, *On multiplicative decompositions of the shifted quadratic residues modulo p*, in: Number Theory, Analysis and Combinatorics, W. de Gruyter, 2014; pp. 295–307.

[11] A. Sárközy and E. Szemerédi, *On the sequence of squares*, Mat. Lapok **16** (1965), 76–85 (in Hungarian).

[12] A. Schinzel, *On the product of the conjugates outside the unit circle of an algebraic number*, Acta Arith. **24** (1973), 385–399.

[13] J. D. Shkredov, *Sumsets in quadratic residues*, Acta Arith. **164** (2014), 221–243.

[14] T. Shorey, R. Tijdeman, *Exponential Diophantine equations*, Cambridge University Press, 1986, pp. 240.

[15] I. E. Shparlinski, *Additive decompositions of subgroups of finite fields*, SIAM J. Discrete Math. **27** (2013), 1870–1879.

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