ON MULTIPLICATIVE DECOMPOSITIONS OF POLYNOMIAL SEQUENCES, II

L. HAJDU AND A. SÁRKÖZY

ABSTRACT. In an earlier paper we studied the multiplicative decomposability of polynomial sequences $\{f(x) : x \in \mathbb{Z}, f(x) > 0\}$ for polynomials of second degree with integer coefficients. Here we study the decomposability of polynomial sequences of this form for polynomials $f(x)$ of degree greater than 2.

1. INTRODUCTION

This paper is the continuation of the paper [7]. In [7] we used the following notations and definitions and we proved the following results:

$\mathcal{A}, \mathcal{B}, \mathcal{C}, \ldots$ denote (usually infinite) sets of positive 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 will be denoted by $\mathbb{N}$.

In [7] we defined both additive and multiplicative decompositions of sequences of non-negative integers, and we presented a short survey of the papers [3, 4, 5, 8, 9, 10, 11, 12, 13, 14, 15] written on decomposition problems. Here we recall only the definitions related to multiplicative decompositions.

Definition 1.1. *A finite or infinite set $\mathcal{A}$ of positive integers is said to be* multiplicatively reducible *or briefly* m-reducible *if it has a multiplicative decomposition*

$$\mathcal{A} = \mathcal{B} \cdot \mathcal{C} \quad \textit{with} \quad |\mathcal{B}| \ge 2,\ |\mathcal{C}| \ge 2. \tag{1.1}$$

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

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

Key words and phrases. Multiplicative decomposition, shifted powers, polynomial values, binomial Thue equations, separable Diophantine equations.

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

Definition 1.2. *Two sets $\mathcal{A}, \mathcal{B}$ of positive integers are called* 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 1.3. *An infinite set $\mathcal{A}$ of positive integers is said to be* totally m-primitive *if every set $\mathcal{A}'$ of positive integers with $\mathcal{A}' \sim \mathcal{A}$ is m-primitive.*

In [7] we started out from the following problem:

Problem 1. Is it true that the set

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

of *shifted* squares is m-primitive?

(Note that the set $\mathcal{M}^+ = \{1, 4, 9, \ldots, x^2, \ldots\}$ has a trivial multiplicative decomposition $\mathcal{M}^+ = \mathcal{M}^+ \cdot \mathcal{M}^+$, thus in order to formulate a non-trivial problem on the m-decomposability of sets related to the squares, we have to consider the set $\mathcal{M}'$ of the shifted squares.)

In [7] we proved that the answer to the question in Problem 1 is affirmative in a much stronger form. Namely, we proved that if the counting function of a subset of $\mathcal{M}'$ increases faster than $\log x$, then the subset must be totally m-primitive:

Theorem A. *If*

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

and $\mathcal{R}$ is such that

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

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

Next we proved that Theorem A is nearly sharp:

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

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

Finally, we considered the case of general quadratic polynomials:

Theorem C. *Let f be a polynomial with integer coefficients of degree 2 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, $a > 0, b > 0$.*

In this paper our goal is to study the analogous problems for polynomials of degree greater than 2.

2. Infinite subsets of the shifted k-th powers are totally m-primitive

For $k \in \mathbb{N}$, $k > 2$ write

$$\mathcal{M}_k = \{0, 1, 2^k, 3^k, \ldots, x^k, \ldots\}$$

and

$$\mathcal{M}'_k = \mathcal{M}_k + \{1\} = \{1, 2, 2^k + 1, 3^k + 1, \ldots, x^k + 1, \ldots\} \tag{2.1}$$

First we will study

Problem 2. Is it true that for $k \in \mathbb{N}$, $k \geq 2$ the set $\mathcal{M}'_k$ of shifted k-th powers defined in (2.1) is totally m-primitive?

Note that in the special case $k = 2$ we proved in [7] that the answer to this question is affirmative in a much sharper form (see Theorem A in the Introduction). Here we will prove that for $k > 2$ an even stronger statement holds:

Theorem 2.1. *If $k \in \mathbb{N}$, $k > 2$,*

$$\mathcal{R} = \{r_1, r_2, \ldots\} \subset \mathcal{M}'_k, \ r_1 < r_2 < \ldots \tag{2.2}$$

and

$$\mathcal{R} \text{ is infinite}, \tag{2.3}$$

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

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

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

$$\mathcal{R}' \cap [n_0, +\infty) = \mathcal{R} \cap [n_0, +\infty), \tag{2.4}$$

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

and

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

By (2.3) and (2.4),

$$\mathcal{R}' \text{ is also infinite.} \tag{2.7}$$

It follows trivially from (2.6) and (2.7) that either $\mathcal{B}$ or $\mathcal{C}$ is infinite; we may assume that

$$\mathcal{C} \text{ is infinite.} \tag{2.8}$$

Let $\mathcal{B} = \{b_1, b_2, \ldots\}$ with $b_1 < b_2 < \ldots$ (by (2.5), $\mathcal{B}$ has at least two elements). Write

$$\mathcal{C}' = \mathcal{C} \cap [n_0, \infty);$$

by (2.8),

$$\mathcal{C}' \text{ is also infinite.} \tag{2.9}$$

Now consider any $c \in \mathcal{C}'$. Then

$$n_0 \le b_1 n_0 \le b_1 c < b_2 c, \tag{2.10}$$

and by (2.4), (2.6) and (2.10) we have

$$b_1 c \in \mathcal{R}' \cap [n_0, \infty) \quad \text{and} \quad b_2 c \in \mathcal{R}' \cap [n_0, \infty). \tag{2.11}$$

It follows from (2.2), (2.4) and (2.11) that

$$b_1 c \in \mathcal{M}'_k \quad \text{and} \quad b_2 c \in \mathcal{M}'_k, \tag{2.12}$$

thus there are $x = x(c) \in \mathbb{N}$, $y = y(c) \in \mathbb{N}$ with

$$b_2 c = x^k + 1, \quad b_1 c = y^k + 1$$

whence

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

so that

$$b_1 x^k - b_2 y^k = b_2 - b_1. \tag{2.13}$$

Clearly, if c and c' are different elements of $\mathcal{C}'$, then $x = x(c')$ and $y = y(c')$ are different solutions of the equation (2.13). Thus by (2.9),

$$\text{(2.13) has infinitely many solutions.} \tag{2.14}$$

Now we need the following lemma which is a simple consequence of a classical theorem of Baker [1], concerning Thue equations.

Lemma 2.1. *Let A, B, C, k be integers with $ABC \neq 0$ and $k \ge 3$. Then for all integer solutions x, y of the equation*

$$Ax^k + By^k = C \tag{2.15}$$

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

We may apply Lemma 2.1 with $A = b_1$, $B = -b_2$, $C = b_2 - b_1$ since then by $0 < b_1 < b_2$ and $k \ge 3$ the conditions in the lemma hold. Then we obtain that (2.13) may have only finitely many solutions, which contradicts (2.14) and this completes the proof of Theorem 2.1. □

3. General polynomials of degree greater than 2

In this section we will prove the analogue of Theorem C for polynomials of degree greater than 2:

Theorem 3.1. *Let $f \in \mathbb{Z}[x]$ with $\deg(f) \geq 3$ having positive leading coefficient, and set*

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

Then $\mathcal{A}$ is **not** *totally m-primitive if and only if $f(x)$ is of the form $f(x) = a(bx+c)^k$ with $a, b, c, k \in \mathbb{Z}$, $a > 0, b > 0, k \geq 3$. Further, if $f(x)$ is of this form, then $\mathcal{A}$ can be written as $\mathcal{A} = \mathcal{A}\mathcal{B}$ with $\mathcal{B} = \{1, (b+1)^k\}$.*

Proof. We will need a lemma, which is Lemma 2.1 in [7], and it concerns the number of solutions of general Pell-type equations up to N.

Lemma 3.1. *Let $f(z) = uz^2+vz+w$ with $u, v, w \in \mathbb{Z}$, $u(v^2-4uw) \neq 0$, and let n, ℓ be distinct positive integers. Then there exists an effectively computable constant $c_2 = c_2(u, v, w, n, \ell)$ such that*

$$\left|\left\{(x, y) \in \mathbb{Z}^2 : nf(x) = \ell f(y) \text{ with } \max(|x|, |y|) < N\right\}\right| < c_2 \log N,$$

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

We will also need a result about equations of type $f(x) = g(y)$. In fact, what we need is the special case when $g(y)$ is of the form $g(y) = tf(y)$. Our next statement, which is new and may be of independent interest, concerns this situation.

Proposition 3.1. *Let $f \in \mathbb{Z}[x]$ with $\deg(f) \geq 3$ and $t \in \mathbb{Q}$ with $t \neq \pm 1$. Suppose that the equation $f(x) = tf(y)$ has infinitely many solutions in integers x, y. Then $f(x)$ is of the form $f(x) = a(g(x))^m$ with some $a \in \mathbb{Z}$ and $g(x) \in \mathbb{Z}[x]$ with $\deg(g) = 1$ or 2.*

To prove the above proposition, we need a deep result of Bilu and Tichy [2]. To formulate this, first we need to introduce some notation.

Let α, β be nonzero rational numbers, $\mu, \nu, q > 0$ and $r \geq 0$ be integers, and let $v(x) \in \mathbb{Q}[x]$ be a nonzero polynomial (which can be constant). Write $D_\mu(x, \delta)$ for the μ-th Dickson polynomial, defined by

$$D_\mu(x, \delta) = \sum_{i=0}^{\lfloor \mu/2 \rfloor} d_{\mu,i} x^{\mu-2i} \qquad \text{with} \qquad d_{\mu,i} = \frac{\mu}{\mu-i}\binom{\mu-i}{i}(-\delta)^i.$$

We will say that two polynomials $F(x)$ and $G(x)$ form a standard pair over $\mathbb{Q}$ if one of the ordered pairs $(F(x), G(x))$ or $(G(x), F(x))$ appears in the table below.

kind	$(F(x), G(x))$ or $(G(x), F(x))$	parameter restriction(s)
first	$(x^q, \alpha x^r v(x)^q)$	$0 \leq r < q, (r, q) = 1,$ $r + \deg v(x) > 0$
second	$(x^2, (\alpha x^2 + \beta)v(x)^2)$	-
third	$(D_\mu(x, \alpha^\nu), D_\nu(x, \alpha^\mu))$	$(\mu, \nu) = 1$
fourth	$(\alpha^{\frac{-\mu}{2}} D_\mu(x, \alpha), -\beta^{\frac{-\nu}{2}} D_\nu(x, \beta))$	$(\mu, \nu) = 2$
fifth	$((\alpha x^2 - 1)^3, 3x^4 - 4x^3)$	-

Now we state a special case of the main result of [2].

Lemma 3.2. *Let $f(x), g(x) \in \mathbb{Q}[x]$ be nonconstant polynomials such that the equation $f(x) = g(y)$ has infinitely many solutions in rational integers x, y. Then $f = \varphi \circ F \circ \lambda$ and $g = \varphi \circ G \circ \kappa$, where $\lambda(x), \kappa(x) \in \mathbb{Q}[x]$ are linear polynomials, $\varphi(x) \in \mathbb{Q}[x]$, and $F(x), G(x)$ form a standard pair over $\mathbb{Q}$.*

Now we are ready to give the

Proof of Proposition 3.1. By Lemma 3.2, we see that in our case in any standard pair F, G corresponding to a case with infinitely many solutions we have $\deg(F) = \deg(G)$. This immediately implies that we have that either $f(x) = \varphi(x)$ and $tf(x) = \varphi(ax + b)$, or $f(x) = \varphi(x^2)$ and $tf(x) = \varphi(ax^2 + b)$ with some polynomial φ and $a, b \in \mathbb{Q}$. These imply $t\varphi(x) = \varphi(ax + b)$, or $t\varphi(x^2) = \varphi(ax^2 + b)$, respectively. Note that also in the latter case, comparing the coefficients, we have $t\varphi(X) = \varphi(aX + b)$. So in any case, the set of the roots of φ is closed under the transformation $z \to az + b$ and also under $z \to (z - b)/a$. As $t \neq \pm 1$, we have $|a| \neq 1$. We may assume that $|a| > 1$; the other case is similar. Suppose that φ has two distinct roots. Write z_1, z_2 for the roots of φ which are furthest (i.e. with $|z_1 - z_2|$ maximal). Then $|(az_1 + b) - (az_2 + b)| > |z_1 - z_2|$ yields a contradiction. That is, φ has only one (possibly multiple) root (given by $z_0 = b/(1 - a)$), and the statement follows. □

Now we can complete the proof of Theorem 3.1.

Since the second part of the statement can be readily checked, we only deal with the first part.

So suppose that $\mathcal{A}$ is **not** totally m-primitive. Then there is a set $\mathcal{A}' \subset \mathbb{N}$ with $\mathcal{A} \sim \mathcal{A}'$ such that $\mathcal{A}'$ can be written as $\mathcal{A}' = \mathcal{BC}$, where $\mathcal{B}, \mathcal{C} \subset \mathbb{N}$ with $|\mathcal{B}|, |\mathcal{C}| \geq 2$. We may assume that for infinitely many N, we have

$$|\{d \in \mathcal{C} : d \leq N\}| \geq |\{b \in \mathcal{B} : b \leq N\}|.$$

Let $b_1, b_2 \in \mathcal{B}$. Then, for all $d \in \mathcal{C}$ we have

$$b_1 d = f(x) \quad \text{and} \quad b_2 d = f(y) \tag{3.1}$$

for some $x, y \in \mathbb{Z}$, which depend on d. This yields that the equation $f(x) = tf(y)$ has infinitely many solutions in integers x, y, where $t = b_1/b_2$. Thus it follows by Proposition 3.1 that either $f(x) = a(bx + c)^k$ with $a, b, c \in \mathbb{Z}$, or $f(x) = a(g(x))^m$ where $g(x) \in \mathbb{Z}[x]$ with $\deg(g) = 2$ and $k = 2m$. Since in the first case we are done, we may assume that the second case holds. Further, we may suppose that the discriminant of $g(x)$ is not zero, otherwise the situation reduces to the case with $\deg(g) = 1$. Then by (3.1) we get $b_2(g(x))^m = b_1(g(y))^m$. This shows that b_2/b_1 is a full m-th power in $\mathbb{Q}$, and we obtain $b_2^* g(x) = b_1^* g(y)$ with some positive integers b_1^*, b_2^*. The last equation by Lemma 3.1 has only $O(\log N)$ solutions in (x, y) with $\max(|x|, |y|) < N$ for any N. (Here and later on in the proof, the implied constant in $O(.)$ depends on b_1, b_2, a, b, c, k.) Hence by

$$|x| = O(d^{1/k}) \quad \text{and} \quad |y| = O(d^{1/k})$$

we have

$$|\{d \in \mathcal{C} : d \le N\}| \le |\{d \in \mathcal{C} : d \le N^k\}| < O(\log N)$$

for any N, whence

$$|\{t \in \mathcal{BC} : t \le N\}| < O((\log N)^2)$$

for infinitely many N. However, on the other hand we have

$$|\{a \in \mathcal{A}' : a \le N\}| > O(N^{1/k})$$

for all N. This contradiction implies the statement. □

4. Problems and remarks

In this concluding section we propose some open problems and make some remarks.

First we point out that some of our results can be extended over rings of integers of algebraic number fields.

Remark 1. Theorem 2.1 can be extended over number fields. We do not work out the details here, only indicate the main points. Let K be an algebraic number field, and write O_K for its ring of integers. Then the sets

$$\mathcal{A}_\beta := \{\alpha^k + \beta : \alpha \in O_K\}$$

are totally m-decomposable for any $k \ge 3$ and $\beta \in O_K \setminus \{0\}$. (By this we mean that if $\mathcal{A}'_\beta \subset O_K$ such that the symmetric difference of $\mathcal{A}_\beta$ and $\mathcal{A}'_\beta$ is finite, then $\mathcal{A}'_\beta = \mathcal{BC}$ with $\mathcal{B}, \mathcal{C} \subset O_K$ implies that either one

of $\mathcal{B},\mathcal{C}$ has only one element, or one of these sets is $\{0,\varepsilon\}$, where ε is a unit in O_K.) Indeed, Lemma 2.1 essentially remains valid also in this generality, see results of Győry and Papp [6], and Chapter 5 of [16] for related results. (Of course, in this case one has to bound the *size* of the solutions x,y, and the bound will depend on certain parameters of K, as well. However, the essential fact from our viewpoint is that (2.15) has only finitely many solutions also in $x,y\in O_K$, for any $A,B,C\in O_K\setminus\{0\}$.) Thus the arguments of Theorem 2.1 can easily be extended to this more general situation. In fact, a special case remains, namely, where

$$\mathcal{A}'_\beta=\mathcal{BC}\quad\text{with}\quad\mathcal{B}=\{0,\gamma\},\ |\mathcal{C}|=\infty$$

where $\gamma\in O_K\setminus\{0\}$ is not a unit. However, in this case γ should divide all elements of $\mathcal{A}'_\beta$, in particular $(\alpha_1\gamma)^k+\beta$ and $(\alpha_2\gamma+1)^k+\beta$ for some $\alpha_1,\alpha_2\in O_K$, whence $\gamma\mid\beta$ and $\gamma\mid\beta+1$ in O_K. This yields that γ is a unit in O_K, which is excluded, and the argument is complete. Note that with any unit $\varepsilon\in O_K$ we can write

$$\mathcal{A}'_\beta:=\mathcal{A}_\beta\cup\{0\}=\{0,\varepsilon\}\cdot(\varepsilon^{-1}\mathcal{A}'_\beta),$$

so this decomposition is trivial and must be excluded.

Next we propose a problem concerning sets which can be simultaneously decomposed both additively and multiplicatively. To its formulation, we need to extend the notion of m-reducibility to sets of non-negative integers. Observe that for any set $\mathcal{A}$ of non-negative integers with $0\in\mathcal{A}$ we have the trivial identity $\mathcal{A}=\{0,1\}\cdot\mathcal{A}$. So we call a set $\mathcal{A}$ of non-negative integers m-reducible if it has a non-trivial multiplicative decomposition, that is if we can write $\mathcal{A}=\mathcal{BC}$ with $\mathcal{B},\mathcal{C}\subset\mathbb{N}\cup\{0\}$, $|\mathcal{B}|,|\mathcal{C}|\geq 2$ and $\mathcal{B}\neq\{0,1\}$, $\mathcal{C}\neq\{0,1\}$.

Problem 1. Describe those sets $\mathcal{A}$ of non-negative integers which are not totally a-primitive and not totally m-primitive at the same time. In particular, is it true that if $\mathcal{A}$ has both properties, then $\mathcal{A}$ can be written as

$$\mathcal{A}=\bigcup_{i=1}^{t}\{mx+r_i:x\in\mathbb{N}\cup\{0\}\}\setminus T$$

with some integers $m,r_1,\dots,r_t$ with $0\leq r_1<\ldots<r_t<m$ and finite set $T\subset\mathbb{N}\cup\{0\}$? Note that if $\mathcal{A}$ is of the above form, then we have $\mathcal{A}=\{0,sm\}+\mathcal{A}$ and $\mathcal{A}=\{1,sm+1\}\cdot\mathcal{A}$ with any $s>\max(T)$.

Remark 2. In view of our results in this paper and in [7], we know that in case of sets of polynomial values, the answer to the question in the above problem is affirmative.

While Problem 1 is, perhaps, not quite hopeless, the next problem seems to be more difficult.

Problem 2. Are there $k, \ell \in \mathbb{N}$ with $k > 1$ and $\ell > 1$ such that $\{x^k y^\ell + 1 : (x, y) \in \mathbb{N}^2\}$ is m-reducible? If yes, for what pairs $k, \ell \in \mathbb{N}$ is this set m-reducible? More generally, for $f(x, y) \in \mathbb{Z}[x, y]$ when is $\{f(x, y) > 0 : (x, y) \in \mathbb{Z}^2\}$ m-reducible?

Remark 3. If $k = 1$ or $\ell = 1$ then the set $\{x^k y^\ell + 1 : (x, y) \in \mathbb{N}^2\}$ is m-reducible:

$$\{xy^\ell + 1 : (x, y) \in \mathbb{N}^2\} = \{x^k y + 1 : (x, y) \in \mathbb{N}^2\} =$$
$$= \{2, 3, 4, \dots\} = \{1, 2, 3, 4, \dots\} \cdot \{2, 3, 4, \dots\}.$$

On the other hand, it follows from Theorem A and Theorem 2.1 that if $d = (k, \ell) > 1$ then $\{x^k y^\ell + 1 : (x, y) \in \mathbb{N}^2\}$ is totally m-primitive since it is a "large" subset of $\{z^d + 1 : z \in \mathbb{N}\}$. This fact seems to point to the direction that the answer to the first question is, perhaps, "no":

Conjecture 1. If $k, \ell \in \mathbb{N}$, $k > 1$ and $\ell > 1$ then the set $\{x^k y^\ell + 1 : (x, y) \in \mathbb{N}^2\}$ is totally m-primitive.

Here the difficulty is that in general the problem reduces to a diophantine equation in 4 variables, and we know much less on equations of this type than on equations in 2 variables. However, one might like to prove at least non-trivial partial results:

Problem 3. Is it true that if $\ell \in \mathbb{N}$, ℓ is odd, and $\ell > 1$ then the set $\{x^2 y^\ell + 1 : (x, y) \in \mathbb{N}^2\}$ is totally m-primitive? (Note that by Remark 3 this is true if ℓ is even.) Can one decide this at least for $\ell = 3$?

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] Yu. F. Bilu and R. F. Tichy, *The Diophantine equation $f(x) = g(y)$*, Acta Arith. **95** (2000), 261–288.

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

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

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

[6] K. Győry and Z. Z. Papp, *Effective estimates for the integer solutions of norm form and discriminant form equations*, Publ. Math. Debrecen **25** (1978), 311–325.

[7] L. Hajdu and A. Sárközy, *On multiplicative decompositions of polynomial sequences*, Acta Arith. (accepted).

[8] H.-H. Ostmann, *Untersuchungen über den Summenbegriff in der additiven Zahlentheorie*, Math. Ann. **120** (1948), 165–196.
[9] H.-H. Ostmann, *Additive Zahlentheorie*, Springer, Berlin, 1956.
[10] 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.
[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 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] I. E. Shparlinski, *Additive decompositions of subgroups of finite fields*, SIAM J. Discrete Math. **27** (2013), 1870–1879.
[16] T. Shorey, R. Tijdeman, *Exponential Diophantine equations*, Cambridge University Press, 1986, pp. 240.

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