ACTA ARITHMETICA
186.2 (2018)

On multiplicative decompositions of polynomial sequences, II

by

L. Hajdu (Debrecen) and A. Sárközy (Budapest)

1. Introduction. This paper is a continuation of [7]. In [7] we used the following notations and definitions:

$\mathcal{A}, \mathcal{B}, \mathcal{C}, \ldots$ 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 positive integers is denoted by $\mathbb{N}$.

In [7] we defined both additive and multiplicative decompositions of sequences of nonnegative integers, and we presented a short survey of the papers [3–5, 8–16] on decomposition problems. Here we only recall 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

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

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

Definition 1.2. Two sets $\mathcal{A}, \mathcal{B}$ of positive integers are called *asymptotically equal* if there is a number K such that $\mathcal{A} \cap [K, \infty) = \mathcal{B} \cap [K, \infty)$; we then 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.

2010 *Mathematics Subject Classification*: 11N25, 11N32, 11D41.
Key words and phrases: multiplicative decomposition, shifted powers, polynomial values, binomial Thue equations, separable Diophantine equations.
Received 16 November 2017; revised 29 January 2018.
Published online 12 October 2018.

DOI: 10.4064/aa171116-7-3

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

PROBLEM 1. Is it true that the set

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

of *shifted* squares is m-primitive?

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

In [7] we proved that the answer to Problem 1 is affirmative in a much stronger form: 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*

$$\mathcal{R} = \{r_1, r_2, \dots\} \subset \mathcal{M}', \qquad r_1 < r_2 < \cdots,$$

and

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

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 of degree 2 with integer coefficients and 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 $f(x) = a(bx + c)^2$ with integers a, b, c, where $a, b > 0$.*

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

2. Infinite sets of shifted kth powers are totally m-primitive. For integer $k > 2$ write

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

and

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

First we will study

PROBLEM 2. Is it true that for $k \geq 2$ the set $\mathcal{M}'_k$ of shifted kth 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* $k > 2$,

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

and

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

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

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

Proof. Assume that, contrary to the statement, there are $\mathcal{R}' \subset \mathbb{N}$, n_0, $\mathcal{B} \subset \mathbb{N}$ and $\mathcal{C} \subset \mathbb{N}$ such that

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

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

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

By (2.3) and (2.4),

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

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 $b_1 < b_2 < \cdots$ (by (2.5), $\mathcal{B}$ has at least two elements). Write $\mathcal{C}' = \mathcal{C} \cap [n_0, \infty)$; by (2.8),

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

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

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

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

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

whence

$$0 = b_1(b_2c) - b_2(b_1c) = b_1(x^k + 1) - b_2(y^k + 1),$$

so that

$$b_1x^k - b_2y^k = b_2 - b_1. \tag{2.13}$$

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

(2.13) has infinitely many solutions. (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 $k \geq 3$. 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 $k \geq 3$ the conditions in the lemma hold. Then we see that (2.13) may have only finitely many solutions, which contradicts (2.14) and 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 $\deg(f) \geq 3$ and 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 $a, b, c, k \in \mathbb{Z}$, where $a, b > 0$ and $k \geq 3$. Further, if $f(x)$ is of this form, then $\mathcal{A}$ can be written as $\mathcal{A} = \mathcal{AB}$ with $\mathcal{B} = \{1, (b + 1)^k\}$.*

Proof. We will need a result of [7, Lemma 2.1] on 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*

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

for any integer $N \geq 2$.

We will also need a result about equations of type $f(x) = g(y)$. In fact, we need the special case when $g(y) = tf(y)$. 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 $f(x) = a(g(x))^m$ with some $a \in \mathbb{Z}$ and $g(x) \in \mathbb{Z}[x]$ with $\deg(g) = 1$ or 2.*

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

Let α, β be nonzero rational numbers, let $\mu, \nu, q > 0$ 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 μth Dickson polynomial, defined by

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

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 Table 1.

Table 1. Standard pairs

Kind	$(F(x), G(x))$ or $(G(x), F(x))$	Parameter restrictions
(i)	$(x^q, \alpha x^r v(x)^q)$	$0 \leq r < q, (r, q) = 1,$ $r + \deg v(x) > 0$
(ii)	$(x^2, (\alpha x^2 + \beta) v(x)^2)$	-
(iii)	$(D_\mu(x, \alpha^\nu), D_\nu(x, \alpha^\mu))$	$(\mu, \nu) = 1$
(iv)	$(\alpha^{-\mu/2} D_\mu(x, \alpha), -\beta^{-\nu/2} D_\nu(x, \beta))$	$(\mu, \nu) = 2$
(v)	$((\alpha x^2 - 1)^3, 3x^4 - 4x^3)$	-

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 prove the proposition:

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 $\deg(F) = \deg(G)$. Hence in Table 1 we obtain the following possibilities:

(i) $r = 0$, $q = 1$ and $\deg v(x) = 1$, thus $\{F(x), G(x)\} = \{x, ux + w\}$ with some $u, w \in \mathbb{Q}$,
(ii) $\deg v(x) = 0$, thus $\{F(x), G(x)\} = \{x^2, ux^2 + w\}$ with some $u, w \in \mathbb{Q}$,
(iii) $\mu = \nu = 1$, thus $F(x) = G(x) = x$,
(iv) $\mu = \nu = 2$, thus $\{F(x), G(x)\} = \{x^2 + u, x^2 + w\}$ with some $u, w \in \mathbb{Q}$,
(v) impossible.

In cases (i) and (iii) by Lemma 3.2 we find that $f(x) = \phi(x)$ and $tf(x) = \phi(ax + b)$ with some rational polynomial ϕ and $a, b \in \mathbb{Q}$. This yields

$$t\phi(x) = \phi(ax + b). \tag{3.1}$$

In case (ii) Lemma 3.2 implies that $f(x) = \phi((k_1x + \ell_1)^2)$ and $tf(x) = \phi(u(k_2x + \ell_2)^2 + w)$, or vice versa, with some rational polynomial ϕ and $k_1, k_2, \ell_1, \ell_2 \in \mathbb{Q}$. Hence we see that $f(k_0x + \ell_0) = \phi(x^2)$ and $tf(k_0x + \ell_0) = \phi(ax^2 + dx + b)$, or vice versa, with some $a, d, b, k_0, \ell_0 \in \mathbb{Q}$, $ak_0 \neq 0$. This shows that

$$t^{\varepsilon}\phi(x^2) = \phi(ax^2 + dx + b) \tag{3.2}$$

with $\varepsilon = \pm 1$. Now the substitution $x \to -x$ yields

$$\phi(ax^2 + dx + b) = \phi(ax^2 - dx + b).$$

Write $\phi(x) = a_nx^n + \cdots + a_1x + a_0$ with $a_n \neq 0$. Comparing the coefficients of x^{2n-1} in the above equality, we obtain

$$na_na^{n-1}dx^{2n-1} = -na_na^{n-1}dx^{2n-1},$$

whence $d = 0$ (as $na_na \neq 0$). Now comparing the coefficients in (3.2), we see that $t^{\varepsilon}\phi(x) = \phi(ax + b)$ is also valid. After applying the substitution $x \to (1/a)x - b/a$ and redefining a as $1/a$ and b as $-b/a$ if $\varepsilon = -1$, we deduce that (3.1) also holds in this case.

In case (iv) Lemma 3.2 implies that $f(x) = \phi_0((k_1x + \ell_1)^2 + u)$ and $tf(x) = \phi_0((k_2x + \ell_2)^2 + w)$, or vice versa, with some rational polynomial ϕ_0 and $k_1, k_2, \ell_1, \ell_2 \in \mathbb{Q}$. If we set $\phi(x) = \phi_0(x + u)$, this implies $f(x) = \phi((k_1x + \ell_1)^2)$ and $tf(x) = \phi((k_2x + \ell_2)^2 + w - u)$, or vice versa. Hence just as in case (ii), $\phi(x)$ satisfies (3.1) again.

Now suppose that $\phi(x) \in \mathbb{Q}[x]$ satisfies (3.1). Then the set of 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 farthest apart (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 $z_0 = b/(1 - a)$). This means that $\phi(x)$ is of the form $\phi(x) = c(x - z_0)^n$. Hence in view of the above analysis, the statement immediately 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 $|\mathcal{B}|, |\mathcal{C}| \geq 2$.

Let $b_1, b_2 \in \mathcal{B}$ be the two smallest elements of $\mathcal{B}$. Then, for all $d \in \mathcal{C}$,

$$b_1 d = f(x) \quad \text{and} \quad b_2 d = f(y) \tag{3.3}$$

for some $x, y \in \mathbb{Z}$, which depend on d. This implies that the equation $f(x) = tf(y)$ has infinitely many solutions in integers x, y, where $t = b_1/b_2$. Proposition 3.1 shows 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, as otherwise the situation reduces to the case with $\deg(g) = 1$. Then by (3.3) we get $b_2(g(x))^m = b_1(g(y))^m$. This shows that b_2/b_1 is a full mth power in $\mathbb{Q}$, and we obtain

$$b_2^* g(x) = b_1^* g(y) \tag{3.4}$$

with some positive integers b_1^*, b_2^*. Write $g(x) = g_2x^2 + g_1x + g_0$; the minimality of b_1, b_2 implies that $\max\{b_1, b_2\}$ can be effectively bounded from above in terms of a, g_2, g_1, g_0, k. Furthermore, by Lemma 3.1, equation (3.4) has only $O(\log N)$ solutions in (x, y) with $\max(|x|, |y|) < N$ for any $N > 1$. (Here and later on in the proof, the implied constant in $O(\cdot)$ depends on a, g_2, g_1, g_0, k.) Hence from

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

we have

$$|\{d \in \mathcal{C} : d \leq N\}| \leq |\{d \in \mathcal{C} : d \leq N^k\}| < O(\log N) \quad \text{for any } N > 1.$$

By interchanging the roles of $\mathcal{B}$ and $\mathcal{C}$, we similarly have

$$|\{d \in \mathcal{B} : d \leq N\}| < O(\log N) \quad \text{for any } N > 1.$$

Hence

$$|\{t \in \mathcal{BC} : t \leq N\}| < O((\log N)^2) \quad \text{for any } N > 1.$$

However,

$$|\{a \in \mathcal{A}' : a \leq N\}| > O(N^{1/k}) \quad \text{for all } N.$$

This contradiction completes the proof. ∎

4. Problems and remarks. First we point out that some of our results can be extended to rings of integers of algebraic number fields.

REMARK 1. Theorem 2.1 can be extended to 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 $k \geq 3$ and $\beta \in O_K \setminus \{0\}$. (By this we mean that if $\mathcal{A}'_\beta \subset O_K$ and 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 Győry and Papp [6], and [15, Chapter 5] 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:

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

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 implies that γ is a unit in O_K, which is excluded, and the argument is complete. Note that for 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 which seems to be difficult.

PROBLEM 1′. Are there $k, \ell \in \mathbb{N}$ with $k, \ell > 1$ such that the set $\{x^k y^\ell + 1 : (x, y) \in \mathbb{N}^2\}$ 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 2. If $k = 1$ or $\ell = 1$ then the set $\{x^k y^\ell + 1 : (x, y) \in \mathbb{N}^2\}$ is m-reducible:

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

On the other hand, it follows from Theorems A and 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 seems to suggest that the answer to the first question is, perhaps, "no":

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

Here the difficulty is that in general the problem reduces to a diophantine equation in four variables, and we know much less on such equations than on equations in two variables. However, one might wish to prove at least nontrivial partial results:

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

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

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.

References

[1] A. Baker, *Contributions to the theory of Diophantine equations. I. On the representation of integers by binary forms*, Philos. Trans. Roy. 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. London 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), paper 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, I*, Acta Arith. 184 (2018), 139–150.

[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 (C. Pomerance et al., eds.), Springer, 2015, 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, de Gruyter, 2014, 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 and R. Tijdeman, *Exponential Diophantine Equations*, Cambridge Univ. Press, 1986.

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

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

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