Multiplicative decompositions of polynomial sequences

L. Hajdu

University of Debrecen

Representation Theory XVI

Inter-University Centre

Dubrovnik

June 23 - 29, 2019

Plan of the talk

- The problem and its background

- Shifted k-th powers - the case $f(x) = x^k + 1$ with $k \geq 3$

- General results - the case $\deg(f) \geq 3$

- Quadratic polynomials - the case $\deg(f) \geq 2$

- Shifted squares - the case $f(x) = x^2 + 1$ (a sharp result)

- A multiplicative analogue of a theorem of Sárközy and Szemerédi (related to a conjecture of Erdős)

- Remarks and open problems

The new results presented are joint with **A. Sárközy.**

The problem and its background

Definition

Let $\mathcal{G}$ be an additive semigroup and $\mathcal{A}, \mathcal{B}, \mathcal{C}$ subsets of $\mathcal{G}$ with $|\mathcal{B}| \geq 2$, $|\mathcal{C}| \geq 2$. Then

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

is an a-decomposition of $\mathcal{A}$, while if a multiplication is defined in $\mathcal{G}$ then

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

is an m-decomposition of $\mathcal{A}$.

The problem and its background

Definition

A finite or infinite set $\mathcal{A}$ of non-negative integers is said to be a-reducible or m-reducible if it has a decomposition as above. If there is no such decomposition then $\mathcal{A}$ is a-primitive or m-primitive.

Definition

Two sets $\mathcal{A}, \mathcal{B}$ of non-negative integers are asymptotically equal if there is a K such that $\mathcal{A} \cap [K, +\infty) = \mathcal{B} \cap [K, +\infty)$. Notation: $\mathcal{A} \sim \mathcal{B}$.

Definition

An infinite set $\mathcal{A}$ of non-negative integers is totally a-primitive resp. totally m-primitive if any $\mathcal{A}'$ with $\mathcal{A}' \sim \mathcal{A}$ is a-primitive resp. m-primitive.

The problem and its background

If $\mathcal{A}$ is a set of non-negative integers with $0 \in \mathcal{A}$, then $\mathcal{A} = \{0, 1\} \cdot \mathcal{A}$. Thus in the multiplicative case we restrict to sets of positive integers.

The above notions were introduced by **H. H. Ostmann (1948)** in the additive case, who also formulated the following nice conjecture:

Conjecture

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

For related results see papers of **Hornfeck, Hofmann, Wolke, Elsholtz, Puchta** and others - however, the conjecture is still open.

Elsholtz also studied multiplicative decompositions of shifted sets $\mathcal{P}' + \{a\}$ with $\mathcal{P}' \sim \mathcal{P}$.

The problem and its background

Another related conjecture was formulated by Erdős:

Conjecture

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

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

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

Sárközy and Szemerédi proved this conjecture in the following slightly weaker form:

Theorem A

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

In fact they got $o(X^{1/2}2^{-(3+\varepsilon)\log X/\log\log X})$ in place of $o(X^{1/2-\varepsilon})$.

The problem and its background

Sárközy proposed to study analogous problems in finite fields. He suggested the following conjectures:

Conjecture

For every prime p the set of the quadratic residues modulo p, i.e. $Q = \{n : n \in \mathbb{F}_p, \left(\frac{n}{p}\right) = +1\}$ *is a-primitive.*

Conjecture

For every prime large enough and every $c \in \mathbb{F}_p$, $c \neq 0$ *the set* $Q_c' = (Q + \{c\}) \setminus \{0\}$ *is m-primitive.*

For related results see papers of **Sárközy, Shkredov, Shparlinski** and others - however, both conjectures are still open.

The problem and its background

For $k \in \mathbb{N}$, $k \geq 2$ write $\mathcal{M}_k = \{0, 1, 2^k, 3^k, \dots, x^k, \dots\}$ and $\mathcal{M}'_k = \mathcal{M}_k + \{1\} = \{1, 2, 2^k + 1, 3^k + 1, \dots, x^k + 1, \dots\}$.

Problem 1

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

More generally:

Problem 2

Describe those polynomials $f(x) \in \mathbb{Z}[x]$ with $\deg(f) \geq 2$, for which the set $\mathcal{A}_f = \{f(x) : x \in \mathbb{Z}\} \cap \mathbb{N}$ is **not** *totally m-primitive.*

Finally, the multiplicative analogue of Erdős's conjecture:

Problem 3

Is it true that if $k \geq 2$ and we change $o(X^{1/k})$ elements of the set $\mathcal{M}'_k$ up to X, then the new set is always totally m-primitive?

The case $k \geq 3$ - shifted powers

Theorem 1 (Sárközy and H)

If k is a positive integer with $k \geq 3$ then any infinite subset of the set of shifted k-th powers $\mathcal{M}'_k$ is totally m-primitive.

In the proof we need the following result. It is a consequence of a classical theorem of **Baker**, concerning Thue equations.

Lemma 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

$$Ax^k + By^k = C$$

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.

Sketch of the proof of Theorem 1

Assume to the contrary that for an infinite $\mathcal{R} \subset \mathcal{M}'_k$ with some $\mathcal{R}' \sim \mathcal{R}$:

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

Here $|\mathcal{B}|, |\mathcal{C}| \geq 2$ and $\mathcal{R}'$ is also infinite.

We may assume that $\mathcal{C}$ is infinite.

Let $b_1, b_2 \in \mathcal{B}$ be fixed. Then for any $c \in \mathcal{C}$ large enough:

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

Sketch of the proof of Theorem 1 - continued

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 by

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

we get

$$b_1 x^k - b_2 y^k = b_2 - b_1.$$

Clearly, if c and c' are different then $x = x(c')$ and $y = y(c')$ are different solutions of the above equation.

Thus this equation has infinitely many solutions.

However, this contradicts Lemma 1.

The case of general polynomials of degree ≥ 3

Theorem 2 (Sárközy and H)

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

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

with

$$\mathcal{B} = \{1, (b + 1)^k\}.$$

The tools used in the proof of Theorem 2

Lemma 2

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 $N \geq 2$.

The proof of Lemma 2 is simple, it uses the theory of Pell equations.

The tools used in the proof of Theorem 2 - continued

Proposition

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.

The Proposition is of some independent interest.

Its proof relies heavily on a deep result of **Bilu and Tichy** concerning integer sloutions of equations of the type $f(x) = g(y)$.

Sketch of the proof of Theorem 2

It is clear that for

$$\mathcal{A} = \{a(bx+c)^k \ : \ x \in \mathbb{Z}\} \cap \mathbb{N}, \quad \mathcal{B} = \{1, (b+1)^k\}$$

we have

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

Suppose that $\mathcal{A}$ is **not** totally m-primitive.

Then there is a set $\mathcal{A}' \subset \mathbb{N}$ with $\mathcal{A} \sim \mathcal{A}'$:
$\mathcal{A}' = \mathcal{B} \cdot \mathcal{C}$ 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 $d \in \mathcal{C}$ large enough we have

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

for some $x, y \in \mathbb{Z}$, which depend on d.

Sketch of the proof of Theorem 2 - continued

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 the Proposition 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 $k = 2m$.

In the first case we are done.

In the second case the theorem follows with some additional argument based upon Pell equations through Lemma 2.

Quadratic polynomials - the general case

Theorem 3 (Sárközy and H)

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

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

Then $\mathcal{A}$ 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, $a > 0, b > 0$.

Sketch of the proof of Theorem 3

If $f(x) = a(bx + c)^2$ with $a, b, c \in \mathbb{Z}$, $a > 0, b > 0$ then

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

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

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

with $|\mathcal{B}|, |\mathcal{C}| \geq 2$.

Assume that $\mathcal{C}$ is infinite.

Let $b_1, b_2 \in \mathcal{B}$ be the two smallest elements of $\mathcal{B}$.

Sketch of the proof of Theorem 3 - continued

For all $d \in \mathcal{C}$ large enough we have

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

with some $x, y \in \mathbb{Z}$.

Thus

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

A counting argument shows that this Pell equation has to have $O(N^{1/4})$ solutions up to N.

Thus by Lemma 2 it must be degenerate.

Hence the theorem follows by simple manipulations.

Quadratic polynomials - shifted squares

In this case we can give much more precise statements than in the general case.

Theorem 4

If

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

such that

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

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

The tools used in the proof of Theorem 4

We shall need Lemma 2, saying that the number of solutions of Pell equations up to N is roughly at most $\log N$.

We shall also need the following result, which follows from a classical theorem of **Baker**, concerning simultaneous Pell equations.

Lemma 3

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 $C^* = C^*(u, v, w, s, \ell, m)$ such that all integer solutions x, y, z of the system of equations

$$\ell f(x) = sf(y), \quad mf(x) = sf(z)$$

satisfy

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

Sketch of the proof of Theorem 4

Assume to the contrary that for an infinite $\mathcal{R} \subset \mathcal{M}'_k$ with some $\mathcal{R}' \sim \mathcal{R}$:

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

Here $|\mathcal{B}|, |\mathcal{C}| \geq 2$ and $\mathcal{R}'$ is also infinite.

Case 1. Assume that $|\mathcal{B}| = 2$. Let $\mathcal{B} = \{b_1, b_2\}$ with $b_1 < b_2$.

For any $c \in \mathcal{C}$ large enough, we have

$$b_1 c \in \mathcal{M}'_2 \quad \text{and} \quad b_2 c \in \mathcal{M}'_2.$$

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

$$b_2 c = x^2 + 1, \quad b_1 c = y^2 + 1.$$

Sketch of the proof of Theorem 4 - continued

Hence we get

$$b_1 x^2 - b_2 y^2 = b_2 - b_1 .$$

From our assumption

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

we deduce

$$\left| \{(x, y) \in \mathbb{Z}^2 : b_1(x^2 + 1) = b_2(y^2 + 1) \text{ with } \max(|x|, |y|) \le N\} \right| >$$
$$> K \log N$$

with K arbitrarily large.

However, this contradicts Lemma 2.

Sketch of the proof of Theorem 4 - continued

Case 2. Assume that $|\mathcal{B}| \geq 3$ and $|\mathcal{C}| \geq 3$.

Let $b_1 < b_2 < b_3$ be elements of $\mathcal{B}$. Then for every $c \in \mathcal{C}$ large enough we have

$$b_i c \in \mathcal{M}_2' \quad (i = 1, 2, 3).$$

Thus there are positive integers x, y, z with

$$b_1 c = z^2 + 1, \quad b_2 c = x^2 + 1, \quad b_3 c = y^2 + 1.$$

Sketch of the proof of Theorem 4 - continued

It follows that

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

and

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

By our assumption on $\mathcal{R}$, after some calculations we get

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

for large N.

However, this contradicts Lemma 3 (about the finiteness of solutions of simultaneous Pell equations).

Theorem 4 is nearly sharp

Theorem 5 (Sárközy and H)

There exists an m-reducible subset $\mathcal{R} \subset \mathcal{M}_2'$ and a number x_0 such that for $x > x_0$ we have

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

Sketch of the proof of Theorem 5

Denote the solutions of the Pell equation

$$y^2 - 2z^2 = 1$$

(ordered increasingly) by $(y_1, z_1) = (3, 2)$, $(y_2, z_2) = (17, 12)$, $\ldots$

It is well-known that $y_n + z_n\sqrt{2} = (y_1 + z_1\sqrt{2})^n = (3 + 2\sqrt{2})^n$ $(n \geq 1)$.

Define the subset $\mathcal{R} \subset \mathcal{M}'_2$ by

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

Then as $2(z_n^2 + 1) = y_n^2 + 1$, we have that $\mathcal{R}$ is m-reducible:

$$\{1, 2\} \cdot \{z_1^2 + 1, z_2^2 + 1, \ldots, z_n^2 + 1, \ldots\} = \mathcal{R}.$$

A simple calculation also gives that

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

Changing elements of $\mathcal{M}_k'$

Now we are interested in **changing** elements of $\mathcal{M}_k'$.

The following result is a multiplicative analogue of Theorem A of Sárközy and Szemerédi (related to a conjecture of Erdős).

Theorem 6 (Sárközy and H)

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.

Sketch of the proof of Theorem 6

It suffices to prove that every set $\mathcal{R}$ obtained in the way described in the theorem is m-primitive.

Assume to the contrary that for some $\varepsilon > 0$ there is such an $\mathcal{R}$ which is m-reducible, of the form

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

with

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

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

and there are $\mathcal{A}, \mathcal{B} \subset \mathbb{N}$ with $|\mathcal{A}|, |\mathcal{B}| \geq 2$ and

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

Sketch of the proof of Theorem 6 - asymmetric case

First assume that the counting function of one of $\mathcal{A}, \mathcal{B}$ is "very large" (thus the other counting function is "very small") infinitely often.

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

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

In this case we can apply the already used tools directly: theory of Pell equations and Thue equations of the form

$$b_1 x^k - b_2 y^k = b_2 - b_1,$$

and the theorem follows from Lemmas 1 and 2.

Sketch of the proof of Theorem 6 - symmetric case

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

$$\max\{A(X), B(X)\} \le X^{1/k} \exp\left(-\left(\log 2 + \frac{\varepsilon}{2}\right)\frac{\log X}{\log\log X}\right)$$

$$\text{for } X > X_0(\varepsilon).$$

In this case both counting functions $A(X)$ and $B(X)$ increase "not too fast". This ("symmetric") case is much more difficult.

The reason is that now we cannot directly use the effective estimates obtained by Baker's method (or by the theory of Pell equations for $k = 2$): we cannot guarantee sufficiently many solutions for equations of the form

$$b_1 x^k - b_2 y^k = b_2 - b_1,$$

for **fixed** b_1, b_2.

Sketch of the proof of Theorem 6 - symmetric case

To overcome this difficulty, we combine various arguments.

First guarantee the existence of many $a \in \mathcal{A}$, $b \in \mathcal{B}$ in 'short multiplicative' intervals with $ab \in \mathcal{R}$.

Then building a bipartite graph on these a, b as vertices, connecting two of them if $ab \in \mathcal{M}'_k$, we guarantee the existence of many edges.

A theorem of Bollobás on the so-called Zarankiewicz function gives a 'large' complete bipartite subgraph, yielding 'many' solutions to

$$Ex^k - Fy^k = G$$

which are 'multiplicatively close' to each other.

Sketch of the proof of Theorem 6 - symmetric case

If $(F/E)^{1/k}$ is irrational, then we can use the theory of continued fractions to get a contradiction.

Indeed, the denominators of the continued fractions grow faster than the powers of 2, which is 'too much' for the 'multiplicatively close' solutions.

If $(F/E)^{1/k}$ is rational, then we use a classical theorem of **Wigert** giving

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

if $\varepsilon > 0$, $X > X_0(\varepsilon)$, to get a contradiction.

Indeed, this result gives that there cannot be sufficiently many solutions to the above equation.

Remarks and open problems

Remark

The results concerning the totally m-primitivity of sets of shifted powers can be extended for number fields.

Problem

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

If $k = 1$ *or* $\ell = 1$ *then the set* $\{x^k y^\ell + 1 : (x, y) \in \mathbb{N}^2\}$ *is m-reducible. On the other hand, 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* $\{z^d + 1 : z \in \mathbb{N}\}$*. So the answer to the first question is, perhaps, 'no'.*

Remarks and open problems

Conjecture

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.

Finally, the additive analogue of the above Conjecture:

Problem

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?

In fact, there are many more ...

Thank you very much
for your attention!