Indecomposability of sequences defined by polynomials and by narrow sets of primes

L. Hajdu

University of Debrecen

Number Theory Seminar

22 April, 2022

Plan of the talk

Introduction

I. Indecomposability of value sets of polynomials

- Problems and earlier results
- New results

II. Indecomposability of sets defined by narrow sets of primes

- Problems and earlier results
- New results

The new results presented are joint with **K. Győry** and **A. Sárközy**.

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 $\mathcal{A}$.

Introduction

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.

Introduction

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 $\mathcal{P}' \sim \mathcal{P}$.

Polynomials - 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 $o(X^{1/2-\varepsilon})$.

Polynomials - 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.

Polynomials - the problem and its background

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

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

Theorem 2 (Sárközy and H)

Let $f \in \mathbb{Z}[x]$ *with* $deg(f) \geq 2$ *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 $a, b, c, k \in \mathbb{Z}$, $a > 0, b > 0, k \geq 2$. *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

In the proof of Theorem 2 the following tools are used:

• a bound for the number of solutions of Pell equations with $\max(|x|, |y|) < N$ (used in case $\deg(f) = 2$),

• a deep result of **Bilu and Tichy** concerning integer solutions of equations of the type $f(x) = g(y)$ (used in case $\deg(f) \geq 3$).

Quadratic polynomials - shifted squares

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

Theorem 3 (Sárközy, H)

If

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

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 3

In the proof of Theorem 3 the following tools are used:

• a bound for the number of solutions of Pell equations with $\max(|x|, |y|) < N$,

• a classical result of **Baker** concerning the finiteness of solutions of simultaneous Pell equations.

Theorem 3 is nearly sharp

Theorem 4 (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 4

Denote the solutions of the Pell equation

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

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

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

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

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

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

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 5 (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 5

Let $\mathcal{R}$ be a set obtained in the way described in the theorem. Assume that $\mathcal{R} = \mathcal{A} \cdot \mathcal{B}$.

Take distinct $b_1, b_2 \in \mathcal{B}$. Then for any $a \in \mathcal{A}$ we have $b_i a = r_a^{(i)}$ $(i = 1, 2)$.

Hence $b_2 r_a^{(1)} = b_1 r_a^{(2)}$, 'typically' yielding $b_1 x^k - b_2 y^k = b_2 - b_1$. However, not always!

The heart of the proof is to guarantee that we can find 'sufficiently many' solutions of an equation $b_1 x^k - b_2 y^k = b_2 - b_1$.

Sketch of the proof of Theorem 5 - continued

For this, 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.

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 ...

Sets generated by narrow sets of primes - background

Definition

Denote the greatest prime factor of the positive integer n by $p^+(n)$.

Then n is said to be smooth (or friable) if $p^+(n)$ is "small" in terms of n.

More precisely, if $y = y(n)$ is a monotone increasing function on $\mathbb{N}$ assuming positive values and $n \in \mathbb{N}$ is such that $p^+(n) \leq y(n)$, then we say that n is y-smooth, and we write $\mathcal{F}_y$ ($\mathcal{F}$ for "friable") for the set of all y-smooth positive integers.

Note that if $y(n)$ tends to infinity, then for any prime q there is an $N \in \mathcal{F}_y$ with $p^+(N) = q$.

Sets generated by narrow sets of primes - background

Conjecture (Sárközy)

If $0 < \varepsilon < 1$,

$$y(n) = n^{\varepsilon},$$

the set $\mathcal{F}_y \subset \mathbb{N}$ *is defined by*

$$\mathcal{F}_y = \{n : n \in \mathbb{N}, p^+(n) \le y(n) = n^{\varepsilon}\}$$

and $\mathcal{F}'_y \subset \mathbb{N}$ *is a set such that*

$$\mathcal{F}'_y \sim \mathcal{F}_y,$$

then there are no sets $\mathcal{A}, \mathcal{B} \subset \mathbb{N}$ *with* $|\mathcal{A}|, |\mathcal{B}| \ge 2$ *and*

$$\mathcal{A} + \mathcal{B} = \mathcal{F}'_y.$$

Sets generated by narrow sets of primes - background

Elsholtz and Harper (2015), with sieve methods:

Theorem B

There exists a large absolute constant $D > 0$*, and a small absolute constant* $\kappa > 0$*, such that the following is true. Suppose* $y(n)$ *is an increasing function such that*

$$(\log n)^D \le y(n) \le n^\kappa \quad \text{for large } n, \tag{1}$$

and such that

$$y(2n) \le y(n)(1 + (100 \log y(n))/\log n).$$

Then a ternary decomposition

$$\mathcal{A} + \mathcal{B} + \mathcal{C} \sim \mathcal{F}'_y,$$

where $\mathcal{A}, \mathcal{B}$ *and* $\mathcal{C}$ *contain at least two elements each, does not exist.*

Sets generated by narrow sets of primes - new results

Put $\mathcal{G}_y := \mathcal{F}_y + \{1\}$.

Theorem 6 (Győry, Sárközy, H)

If $y(n)$ is an increasing function with $y(n) \to \infty$ and

$$y(n) < 2^{-32} \log n \quad \textit{for large } n,$$

then $\mathcal{F}_y$ is totally a-primitive, *while $\mathcal{G}_y$ is totally* m-primitive.

If $y(n)$ is increasing then the set $\mathcal{F}_y$ is m-reducible since $\mathcal{F}_y = \mathcal{F}_y \cdot \mathcal{F}_y$, and we also have $\mathcal{F}_y \sim \mathcal{F}_y \cdot \{1, 2\}$.

Thus if we want to prove an *m-primitivity* theorem involving $\mathcal{F}_y$ then we have to switch from $\mathcal{F}_y$ to the shifted set $\mathcal{G}_y$.

Sketch of the proof of Theorem 6

Assume to the contrary that $\mathcal{F}'_y = \mathcal{A} + \mathcal{B}$, wlog $B(N) \geq A(N)$ for infinitely many N.

Let $a_1, a_2 \in \mathcal{A}$. Then for any $b \in \mathcal{B}$ large enough we have $X_b, Y_b \in \mathcal{F}_y$ with $X_b = a_2 + b$, $Y_b = a_1 + b$, yielding $X_b - Y_b = a_2 - a_1$.

If we consider everything up to some bound N, this is an S-unit equation.

Setting $\Psi(x, y) = |\{n : n \leq x,\ p^+(n) \leq y\}|$, we get $B(N) > \frac{1}{2}(\Psi(N, y(N)))^{1/2}$.

On the other hand, by using a bound of **Beukers and Schlickewei** on the number of solutions of S-unit equations, we get $\frac{1}{3}(\Psi(N, y(N)))^{1/2} < 2^{16(\pi(y(N))+1)}$.

Sketch of the proof of Theorem 6 - continued

Lemma 2 (de Bruijn)

Write

$$Z = \frac{\log x}{\log y} \log \left(1 + \frac{y}{\log x}\right) + \frac{y}{\log y} \log \left(1 + \frac{\log x}{y}\right).$$

Then we have, uniformly for $x \geq y \geq 2$,

$$\log \Psi(x, y) = Z \left(1 + O\left(\frac{1}{\log y} + \frac{1}{\log \log 2x}\right)\right).$$

This by some additional argument implies the statement.

The additive case - a converse statement

Theorem 7 (Győry, Sárközy, H)

Let $y(n)$ be any monotone increasing function on $\mathbb{N}$ with

$$\frac{n}{2} < y(n) < n \quad \textit{for all } n \in \mathbb{N}.$$

Then $\mathcal{F}_y$ is not *totally a-primitive. In particular, in this case the set*

$$\mathcal{F}_y \cap [9, +\infty)$$

is a-reducible, namely, we have $\mathcal{F}_y \cap [9, +\infty) = \mathcal{A} + \mathcal{B}$ with

$$\mathcal{A} = \{n \in \mathbb{N} : \textit{none of } n, n+1, n+3, n+5 \textit{ is prime}\}, \ \mathcal{B} = \{0, 1, 3, 5\}.$$

Note that if the prime k-tuple conjecture is true for $k = 2, 3$, then there is no decomposition with $2 \leq |\mathcal{B}| \leq 3$.

A problem in the multiplicative case

Let $y(n)$ be any monotone increasing function on $\mathbb{N}$ with

$$\frac{n}{2} < y(n) < n \quad \text{for all } n \in \mathbb{N}.$$

Problem (Győry, Sárközy, H)

Is the set $\mathcal{G}_y$ totally m-primitive?

Theorem 8 (Győry, Sárközy, H)

For any $\mathcal{C} \subset \mathbb{N}$ with $\mathcal{C} \sim \mathcal{G}_y$ there is no decomposition of the form $\mathcal{C} = \mathcal{A} \cdot \mathcal{B}$ with $|\mathcal{B}| < +\infty$.

An analogous problem involving thin sets of primes

Elsholtz and Harper proved:

Theorem C

Let $\mathcal{P} = \{p_1, p_2, \ldots, p_r\} \subset \mathbb{P}$ *be any* finite *set of primes, and let*

$$\mathcal{R}(\mathcal{P}) = \{n \in \mathbb{N} : p \mid n \implies p \in \mathcal{P}\}.$$

Then $\mathcal{R}(\mathcal{P})$ *is totally a-primitive.*

They also remarked that it follows from a result of **Tijdeman** that:

Theorem D

There exists an infinite *set* $\mathcal{P}$ *of primes, such that the set* $\mathcal{R}(\mathcal{P})$ *is totally a-primitive.*

An analogous problem involving thin sets of primes

Note that we have $\mathcal{R}(\mathcal{P}) = \{1, p_1\} \cdot \mathcal{R}(\mathcal{P})$. Put $\mathcal{T}(\mathcal{P}) = \mathcal{R}(\mathcal{P}) + \{1\}$.

Theorem 9 (Győry, Sárközy, H)

If $\mathcal{P} = \{p_1, p_2, \dots\} \subset \mathbb{P}$ (with $p_1 < p_2 < \dots$) is a non-empty (finite or infinite) set of primes such that there is a number x_0 with

$$P(x) < \frac{1}{51} \log \log x \quad \textit{for } x > x_0,$$

then the set $\mathcal{R}(\mathcal{P})$ is totally a-primitive, while $\mathcal{T}(\mathcal{P})$ is totally m-primitive.

Main tools used in the proof:

• bounds for various functions related to prime numbers,

• bounds for the number of solutions of S-unit equations.

A converse statement

Theorem 10 (Győry, Sárközy, H)

Let $\mathcal{P} = \mathbb{P} \setminus \mathcal{Q}$ with a finite set $\mathcal{Q} \subset \mathbb{P}$, and let either $t \geq 2$ or $t = \infty$. Then $\mathcal{R}(\mathcal{P})$ has a decomposition $\mathcal{R}(\mathcal{P}) = \mathcal{A} + \mathcal{B}$ with $|\mathcal{A}| = \infty$ and $|\mathcal{B}| = t$.

• It is also shown that the statement is sharp in the sense that one can find arbitrary 'thin' infinite sets $\mathcal{Q}$ such that $\mathcal{R}(\mathcal{P})$ does not allow such a decomposition with $|\mathcal{B}|$ finite.

• Similar statements are also proved for $\mathcal{T}(\mathcal{P})$.

Two problems

Problem (Győry, Sárközy, H)

Does a set $\mathcal{P} \subset \mathbb{P}$ exist such that its counting function $P(x)$ satisfies $P(x)/\log\log x \to \infty$ and $\mathcal{R}(\mathcal{P})$ is totally a-primitive?

Problem (Győry, Sárközy, H)

Is it true, that if $\mathcal{Q} \subset \mathbb{P}$, $\mathcal{Q}$ is $\mathrm{infinite}$, and $\mathcal{P}$ is defined by $\mathcal{P} = \mathbb{P} \setminus \mathcal{Q}$, then $\mathcal{R}(\mathcal{P})$ is totally a-primitive?

We conjecture that the answer is affirmative in both cases.

Thank you very much for your attention!