Nóra Varga

Diophantine equations with restricted coefficients

Joint work with **Lajos Hajdu** and **Rob Tijdeman**

Number Theory and Algebra Seminar
Debrecen, 17 March 2023

- **Introduction**
- New theorems
- Auxiliary results from others
- New lemmas
- Sketch of proofs

Introduction

Polynomials with restricted coefficients:
If the coefficients belong to the set

- $\{-1, 1\}$: Littlewood polynomials
- $\{0, 1\}$: Newman polynomials (assuming that the constant term is not zero)

The zeroes (in particular, the number of real zeroes) of polynomials with coefficients belonging to $\{-1, 0, 1\}$ have been studied by

- Bloch and Pólya (1932)
- Schur (1933)
- Szegő (1934)
- Erdős and Turán (1950)
- Drungilas and Dubickas (2009)
- Borwein and Erdélyi (1995, 1997)

Introduction

Further,

- Borwein and Mossinghoff (2000)
- Peled, Sen and Zeitouni (2016)
- Dubickas and Jankauskas (2009)
- Mossinghoff (2003)
- Hare, Jankauskas (2021)

- Introduction
- **New theorems**
- Auxiliary results from others
- New lemmas
- Sketch of proofs

Notations

- Let $S = \{p_1 < p_2 < \ldots < p_k\}$ be a finite set of primes, and write $\mathbb{Z}_S$ for the set of integers having no prime divisors outside S.
- Note that we have $\pm 1 \in \mathbb{Z}_S$ but $0 \notin \mathbb{Z}_S$ for any S.
- In particular, we have $\mathbb{Z}_S = \{-1, 1\}$ for $S = \emptyset$.
- Write P_S for the set of polynomials in $\mathbb{Z}[x]$ with coefficients belonging to $\mathbb{Z}_S$.

Theorem 1

Theorem (Hajdu,V, 2022)

Let $f(x) \in P_S$ *of degree* d *and* b *be a non-zero rational number. Then there exist effectively computable constants* $C_1 = C_1(p_k)$ *and* $C_2 = C_2(b, d, p_k)$ *depending only on* p_k *and on* b, d, p_k*, respectively, such that if* $d > C_1$ *then the equality*

$$f(x) = by^n \tag{1}$$

with $x, y, n \in \mathbb{Z}$ *and* $|y| > 1$ *implies* $n < C_2$*.*

Theorem 2

Theorem (Hajdu, V, 2022)

Let $f(x) \in P_S$ with $S = \emptyset$ (i.e. $f(x)$ is a Littlewood polynomial, with all coefficients being ± 1). Assume further that $\deg f \geq 3$, and let b be a non-zero rational number. Then all solutions $x, y, n \in \mathbb{Z}$ of the equation

$$f(x) = by^n \tag{2}$$

with $n \geq 2$, satisfy

$$\max(|x|, |y|, n) \leq C_3,$$

except when $n = 2$ and f is one of the forms

$$f(x) = \pm(x^{2k+1} + \ldots + x^{k+1} - x^k - \ldots - 1),$$
$$\pm(x^{2k+1} - x^{2k} + \ldots + (-1)^{k+2}x^{k+1} + (-1)^k x^k + \cdots + 1)$$

with some $k \geq 1$. Here $C_3 = C_3(b, d)$ is an effectively computable constant depending only on b and the degree d of f.

Theorem 3

Theorem (Hajdu, Tijdeman, V, 2023)

Let $f(x)$ be a Littlewood polynomial of degree n with $n \geq 4$ and $a, b \in \mathbb{Q}$ with $a \neq 0$. Then all solutions $x, y, m \in \mathbb{Z}$ of the equation

$$f(x) = ay^m + b \tag{3}$$

with $m \geq 2$, satisfy

$$\max(|x|, |y|, m) \leq C_4,$$

except when

Theorem 3

Theorem

except when $m = 2$ *and*

$$f(x) \in \{f^*(x),\ f^*(x) - 2f^*(0),\ xf^*(x) \pm 1\} \qquad (4)$$

with $b = 0, -2f^*(0), \pm 1$, *respectively, where*

$$f^*(x) = \pm(x^{2\ell+1} + x^{2\ell} + \ldots + x^{\ell+1} - x^{\ell} - \ldots - 1), \quad \text{or}$$
$$f^*(x) = \pm((-x)^{2\ell+1} + (-x)^{2\ell} + \ldots + (-x)^{\ell+1} - (-x)^{\ell} + \cdots - 1)$$

with $\ell = \lfloor (n-1)/2 \rfloor$ *and the solutions are given by* $y = Q(x)$ *with* $Q(\pm x) = \pm(x^k + \ldots + x + 1)$. *Here* C_4 *depends only on* n, a, b *and we use the convention that* $m \leq 3$ *if* $|y| \leq 1$.

Theorem 4

Theorem (Hajdu, Tijdeman, V, 2023)

Let $f(x)$ *be a Littlewood polynomial of degree* n *with* $n \geq 4$ *and* $g(x) \in \mathbb{Z}[x]$. *Then the equation*

$$f(x) = g(y) \tag{5}$$

has only finitely many solutions in integers x, y, *except when* $g(y) = f(T(y))$ *with some polynomial* $T(y)$ *of degree* ≥ 1 *having rational coefficients, or if* $f(x)$ *is of the shape (4) and* $g(y) = a(cy + d)^2 + b$ *for* a, b *as in Theorem 3 and* $c, d \in \mathbb{Q}, c \neq 0$.

- Introduction
- New theorems
- **Auxiliary results from others**
- New lemmas
- Sketch of proofs

Lemma-Gy

Lemma (Győry, 1972)

Let S be as above, and A, B be non-zero rational numbers. Then the solutions $x, y \in \mathbb{Z}_S$ of the equation

$$Ax - By = 1$$

satisfy

$$\max(|x|, |y|) < C_5,$$

where $C_5 = C_5(A, B, p_k)$ is an effectively computable constant depending only on A, B and p_k.

The statement is an immediate consequence of a classical result of Győry (1972).

Lemma-ST

Lemma (Schinzel, Tijdeman, 1976)

Let $F(x) \in \mathbb{Z}[x]$ having two distinct (complex) roots of degree D and height H, and B be a non-zero rational number. Then the equality

$$F(x) = By^n$$

with $x, y \in \mathbb{Z}$, $|y| > 1$ implies that $n < C_6$, where $C_6 = C_6(B, D, H)$ is an effectively computable constant depending only on B, D and H.

The statement immediately follows from the Schinzel-Tijdeman (1976) theorem.

Lemma-B

- For any finite set S of primes, write $\mathbb{Q}_S$ for those rationals whose denominators (in their primitive forms) are composed exclusively from the primes in S.
- By the height $h(s)$ of a rational number s we mean the maximum of the absolute values of the numerator and the denominator of s (written again in primitive form).
- The following Lemma is a theorem of Brindza (1984).

Lemma-B

Lemma (Brindza, 1984)

Let $F(x) \in \mathbb{Z}[x]$ of degree D and height H, and write $F(x) = A\prod_{i=1}^{\ell}(x-\gamma_i)^{r_i}$, where A is the leading coefficient of F, and $\gamma_1, \ldots, \gamma_\ell$ are the distinct complex roots of $F(x)$, with multiplicities $r_1, \ldots, r_\ell$, respectively. Further, let n be an integer with $n \geq 2$, and put $q_i = \frac{n}{(n, r_i)} \quad (i = 1, \ldots, \ell)$.
Suppose that $(q_1, \ldots, q_\ell)$ is not a permutation of any of the ℓ-tuples $(q, 1, \ldots, 1)$ $(q \geq 1)$, $\quad (2, 2, 1, \ldots, 1)$.
Then for any finite set S of primes and non-zero rational B, the solutions $x, y \in \mathbb{Q}_S$ of the equation

$$F(x) = By^n$$

satisfy

$$\max(h(x), h(y)) < C_7(B, n, D, H, S),$$

where $C_7(B, n, D, H, S)$ is an effectively computable constant depending only on B, n, D, H, S.

Lemma-BT

Lemma (Bilu, Tichy, 2000)

Let $f(x), g(x) \in \mathbb{Q}[x]$ be non-constant polynomials. Then the following two statements are equivalent.

(I) *The equation $f(x) = g(y)$ has infinitely many rational solutions x, y with a bounded denominator.*

(II) *We have $f = \varphi(F(\kappa))$ and $g = \varphi(G(\lambda))$, where $\kappa(x), \lambda(x) \in \mathbb{Q}[x]$ are linear polynomials, $\varphi(x) \in \mathbb{Q}[x]$, and $F(x), G(x)$ form a standard pair over $\mathbb{Q}$ such that the equation $F(x) = G(y)$ has infinitely many rational solutions with a bounded denominator.*

Lemma-DG

In the proof of Theorem 4, the decomposability of polynomials will play an important role. We call $F(x) \in \mathbb{Q}[x]$ decomposable over $\mathbb{Q}$ if there exist $G(x), H(x) \in \mathbb{Q}[x]$ with $\deg(G) > 1$, $\deg(H) > 1$ such that $F = G(H)$, and otherwise indecomposable.

Lemma (Dujella, Gusić, 2006)

Let $F(x) \in \mathbb{Z}[x]$, of the form

$$F(x) = x^n + u_1 x^{n-1} + \cdots + u_{n-1}x + u_n.$$

If $\gcd(u_1, n) = 1$ then $F(x)$ is indecomposable over $\mathbb{Q}$.

- Introduction
- New theorems
- Auxiliary results from others
- **New lemmas**
- Sketch of proofs

Lemma 1

Lemma (Hajdu, V, 2022)

Let m be a non-negative integer and let

$$G(x) = b_0x^t + b_1x^{t-1} + \ldots + b_{t-1}x + b_t \tag{6}$$

with $b_0, b_1, \ldots, b_t \in \mathbb{Z}$, such that all the coefficients of the polynomial $(x-1)^m G(x)$ belong to $\{-1, 1\}$. Then $b_1 = 0$ implies $m = 1$.

Lemma 2

Lemma (Hajdu, V, 2022)

Let $G(x) \in \mathbb{Z}[x]$ *and* m *be a non-negative integer. If all the coefficients of* $(x-1)^m G(x)$ *belong to* $\{-1, 1\}$ *then, writing*

$$G(x) = b_0 x^t + b_1 x^{t-1} + \ldots + b_{t-1} x + b_t,$$

for all $i = 0, 1, \ldots, t$ *we have*

$$-\min\left(\binom{m+i}{m}, \binom{m+t-i}{m}\right) \leq b_i \leq \min\left(\binom{m+i}{m}, \binom{m+t-i}{m}\right).$$

Here we use the convention $\binom{0}{0} = 1$.

Lemma 3 and 4

Lemma (Hajdu, V, 2022)

Let $n \geq 2$ *and* $g(x) \in \mathbb{Z}[x]$ *be non-zero polynomial. If all the coefficients of* $(x-1)^{n-1}g^n(x)$ *belong to* $\{-1, 1\}$ *then we have* $n = 2$.

Lemma 3 and 4

Lemma (Hajdu, V, 2022)

Let $n \geq 2$ and $g(x) \in \mathbb{Z}[x]$ be non-zero polynomial. If all the coefficients of $(x-1)^{n-1}g^n(x)$ belong to $\{-1, 1\}$ then we have $n = 2$.

Lemma (Hajdu, V, 2022)

Let $g(x) \in \mathbb{Z}[x]$ be a non-constant polynomial and m, n be integers with $0 \leq m < n$. If all the coefficients of the polynomial $(x-1)^m(g(x))^n$ belong to $\{-1, 1\}$ then $n = 2$, $m = 1$ and $g(x)$ is of the form

$$g(x) = \pm(x^\ell + \ldots + x + 1)$$

with some $\ell \geq 1$.

Lemma 5 and 6

A multiple root is a root of multiplicity > 1.

Lemma (Hajdu, Tijdeman, V, 2023)

Let $f(x)$ be a Littlewood polynomial and $b \in \mathbb{Q}$. If $f(x) - b$ has a root of multiplicity ≥ 3, or has at least two roots of multiplicities ≥ 2, then $b \in \mathbb{Z}$. Further, in both cases the multiple roots of $f(x) - b$ are units.

Lemma 5 and 6

A multiple root is a root of multiplicity > 1.

Lemma (Hajdu, Tijdeman, V, 2023)

Let $f(x)$ be a Littlewood polynomial and $b \in \mathbb{Q}$. If $f(x) - b$ has a root of multiplicity ≥ 3, or has at least two roots of multiplicities ≥ 2, then $b \in \mathbb{Z}$. Further, in both cases the multiple roots of $f(x) - b$ are units.

Lemma (Hajdu, Tijdeman, V, 2023)

Let $f(x)$ be a Littlewood polynomial of degree n and let $b \in \mathbb{Z}$. Then for any root α of $f(x) - b$ with $|\alpha| > 2$ we have

$$\frac{|\alpha| - 2}{|\alpha| - 1} |\alpha|^n < |b|.$$

- Introduction
- New theorems
- Auxiliary result from others
- New lemmas
- **Sketch of proofs**

Proof of Theorem 1 — steps

- The statement immediately follows by Lemma-ST, as soon as $f(x)$ has two distinct roots.
- Thus we can assume that $f(x)$ is of the form $f(x) = u(x+v)^d$, with some $u \in \mathbb{Z}$ and $v \in \mathbb{Q}$.
- Investigating the value of u, v, d and the coefficients of f we have two cases:
  In the first case $d, d-1 \in \mathbb{Z}_S$ satisfy the equation $w_1 - w_2 = 1$, while in the second case $d, (d-1)/2 \in \mathbb{Z}_S$ are solution to the $w_1 - 2w_2 = 1$ in $w_1, w_2 \in \mathbb{Z}_S$.
- Using Lemma-Gy we get that for the solutions of the above equations $\max(|w_1|, |w_2|) < C_8$ holds, where $C_8 = C_8(p_k)$.
- So if $d > C_8$, then d cannot come from a solution of the above equations, which implies that $f(x)$ is not of the form $u(x+v)^d$.

Proof of Theorem 2 — steps

- We show that n can be bounded in the required way. Following the lines of the proof of Theorem 1, we see that it is sufficient to exclude the case when $f(x)$ is of the form $(x \pm 1)^d$. However, this is clearly impossible.

- We may suppose that $n \geq 2$ is fixed. Thus our statement immediately follows from Lemma-B, except in the following two cases:

  i) $n = 2$ and $f(x) = h(x)(g(x))^2$ where $\deg h = 2$ and $h(x), g(x) \in \mathbb{Z}[x]$;

  ii) n is arbitrary and $f(x) = (h(x))^m(g(x))^n$, where $\deg h \leq 1$, $0 \leq m < n$ and $h(x), g(x) \in \mathbb{Z}[x]$.

Proof of Theorem 2 — steps

- In the case i) write $h(x) = x^2 + v_1x + v_2$ and

$$g(x) = x^\ell + u_1x^{\ell-1} + \ldots + u_\ell.$$

  Case i) cannot hold.

- Consider the case ii). We can be suppose that the polynomials f, g, h are monic and $h(x) = x - 1$. The statement follows from Lemma 4.

Proof of Theorem 3 — sketch

- bound for m follows from Lemma-ST unless $f(x) - b$ is of the shape $f(x) = (x - s)^n$ with $s \in \mathbb{Q}$
- by Lemma-ST, we may assume that m is fixed
- our claim follows from Lemma-B, except for the following two cases:

  i) $m \geq 2$ is arbitrary and $f(x) - b = (P(x))^r (Q(x))^t$ with $0 \leq r < t$, $t \geq 2$ and $P, Q \in \mathbb{Q}[x]$, $\deg(P) \leq 1$;

  ii) $m = 2$ and $f(x) - b = P(x)(Q(x))^2$ with $P, Q \in \mathbb{Q}[x]$, $\deg(P) = 2$.

- $n = \deg(f) = 4$
- $n \geq 5$
  - case (i): possible values of r and then s
    investigation of coefficients
    (Lemma 4', 5, 6)
  - case (ii): $P(x) = x^2 + ux + w$
    parity and possible values of u, w then
    $P(x) = x^2 \pm 3x + 4,\ x^2 \pm x + 4,\ x^2 \pm x - 2,\ x^2 \pm 3x + 2,\ x^2 \pm x + 2.$

    we get these cases cannot occur
  - (Lemma 4', 5 and 6)

Proof of Theorem 4

- by Lemma-DG: $f(x)$ is indecomposable over $\mathbb{Q}$
- thus, if equation $f(x) = g(y)$ has infinitely many solutions in integers x, y, then by Lemma-BT we have only two options:
  - i) $g(x)$ is of the form $g(x) = f(T(x))$ with some $T(x) \in \mathbb{Z}[x]$
  - ii) $f(x)$ is of the shape $f(x) = AF(ux + w) + B$ with some $A, B, u, w \in \mathbb{Q}$, $Au \neq 0$, where F belongs to a standard pair.

- L. Hajdu - N. Varga: *Diophantine equations for polynomials with restricted coefficients, I (Power values)*. Bulletin of the Australian Math. Soc. 106/2 (2022), 254-263.
- L. Hajdu - R. Tijdeman - N. Varga: *Diophantine equations for Littlewood polynomials.* Acta Arithmetica, accepted