DIOPHANTINE EQUATIONS FOR LITTLEWOOD POLYNOMIALS

LAJOS HAJDU, ROBERT TIJDEMAN, AND NÓRA VARGA

Dedicated to the memory of Andrzej Schinzel.

Abstract. In this paper we give finiteness results for the shifted power values and polynomial values of Littlewood polynomials.

1. Introduction

There are many papers in the literature concerning polynomials with coefficients belonging to the set $\{-1, 0, 1\}$. For a short survey, we refer to the introduction of the paper [4] and the references there. If the coefficients are only ± 1, the polynomials are called Littlewood polynomials. In [4], under certain necessary assumptions, an effective bound for $\max(|x|, |y|, m)$ in the equation

$$f(x) = y^m$$

is given in case f is a Littlewood polynomial and x, y, m are integral unknowns with $m \geq 2$. In this paper we give effective upper bounds for the solutions of the more general equation

$$f(x) = ay^m + b$$

where $a, b \in \mathbb{Q}$. Further, we describe all cases where a Littlewood polynomial can have infinitely many common values with another polynomial. In particular, we show that for any $g(x) \in \mathbb{Q}[x]$, the equation

$$f(x) = g(y)$$

can have only finitely many solutions in integers x, y, except for certain explicitly given cases.

Date: November 3, 2022.

2010 *Mathematics Subject Classification.* 11D41, 11R09.

Key words and phrases. Littlewood polynomials, shifted power values, polynomial values.

Research supported in part by the Eötvös Loránd Research Network (ELKH), by the NKFIH grants 128088 and 130909, and the project EFOP-3.6.1-16-2016-00022 co-financed by the European Union and the European Social Fund.

2. The theorems

Theorem 2.1. *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*

$$f(x) = ay^m + b \tag{1}$$

with $m \geq 2$, satisfy

$$\max(|x|, |y|, m) \leq C_1,$$

except when $m = 2$ and

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

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

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

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_1 is an effectively computable constant depending only on n, a, b, and we use the convention that $m \leq 3$ if $|y| \leq 1$.

Theorem 2.2. *Let $f(x)$ be a Littlewood polynomial of degree n with $n \geq 4$ and $g(x) \in \mathbb{Z}[x]$. Then the equation*

$$f(x) = g(y) \tag{3}$$

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 (2) and $g(y) = a(cy + d)^2 + b$ for a, b as in Theorem 2.1 and $c, d \in \mathbb{Q}, c \neq 0$.

Remark 1. In both theorems the assumption $\deg(f) \geq 4$ is necessary. The case $\deg(f) = 1$ is trivial. It is easy to construct infinitely many f, a, b with $\deg(f) = 2$, and $g(y) = ay^2 + b$ such that equation (1) becomes a Pell equation having infinitely many integer solutions x, y. Finally, also for $\deg(f) = 3$ there exist cases not fitting in the families described in the theorems. For example, taking

$$f(x) = x^3 + x^2 - x + 1, \quad a = \frac{1}{27} \quad b = \frac{22}{27},$$

in view of

$$f(x) - b = a(3x + 5)(3x - 1)^2$$

we see that equation (1) has infinitely many integer solutions x, y.

It is also necessary that $f(x)$ is not of the shape (2). We demonstrate it only for one case. The other cases can be checked similarly. Take

$$f(x) = x(x^{2\ell+1} + \ldots + x^{\ell+1} - x^{\ell} - \ldots - 1) + 1 = \\ = x^n + \ldots + x^{n/2+1} - x^{n/2} - \ldots - x + 1.$$

One can readily check that

$$f(x) - 1 = x(x-1)(x^{n/2-1} + \cdots + x + 1)^2.$$

As the Pell equation $x(x-1) = 2y^2$ has infinitely many solutions, equation (1) has infinitely many solutions in integers x, y when taking $m = 2$, $a = 2$, $b = 1$.

Remark 2. Let $f(x)$ be a Littlewood polynomial and write

$$f(x) = \varepsilon_0 x^n + \varepsilon_1 x^{n-1} + \varepsilon_2 x^{n-2} + \cdots + \varepsilon_{n-1} x + \varepsilon_n$$

with $\varepsilon_i \in \{-1, 1\}$ $(i = 0, 1, \ldots, n)$. Applying the transformation $x \to -x$ if necessary, we may assume that $\varepsilon_0 = \varepsilon_1$. Then, taking out a factor -1 if necessary, we may suppose that $\varepsilon_0 = \varepsilon_1 = 1$. Since our statements concern the root structure of $f(x)$ and $f'(x)$, and equations involving $f(x)$, we can clearly do this in our arguments without loss of generality. So from this point on, we shall assume that $f(x)$ is of the shape

$$f(x) = x^n + x^{n-1} + \varepsilon_2 x^{n-2} + \cdots + \varepsilon_{n-1} x + \varepsilon_n. \tag{4}$$

3. Auxiliary results

We present some lemmas which we shall use in the proofs of the theorems. By the height $H(F(x))$ of a polynomial $F(x)$ with integer coefficients we mean the maximum of the absolute values of its coefficients.

Lemma 3.1. *Let $F(x) \in \mathbb{Z}[x]$ of degree D and height H have two distinct (complex) roots, and B a non-zero rational number. Then the equation*

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

with $x, y \in \mathbb{Z}$, $|y| > 1$ implies that $m < C_2$, where C_2 is effectively computable and depends only on B, D and H.

Proof. The statement follows from the Schinzel-Tijdeman theorem [6]. □

The following lemma is a theorem of Brindza [2]. 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 height of its minimal defining polynomial.

Lemma 3.2. *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 $\gamma_1, \dots, \gamma_\ell$ are the distinct complex roots of $F(x)$, with multiplicities $r_1, \dots, r_\ell$, respectively. Further, let m be an integer with $m \geq 2$, and put

$$q_i = \frac{m}{(m, r_i)} \quad (i = 1, \dots, \ell).$$

Suppose that $(q_1, \dots, q_\ell)$ is not a permutation of any of the ℓ-tuples

$$(q, 1, \dots, 1) \ (q \geq 1), \quad (2, 2, 1, \dots, 1).$$

Then for any finite set S of primes and non-zero rational B, the solutions $x, y \in \mathbb{Q}_S$ of the equation

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

satisfy

$$\max(h(x), h(y)) < C_3,$$

where C_3 is effectively computable and depends only on B, m, D, H, S.

In the proof of Theorem 2.2, 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 3.3. *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 $\mathbb{Q}$.

Proof. The statement is a simple consequence of Theorems 2 and 3 of [3]. □

We further apply a deep result of Bilu and Tichy. Let δ be a non-zero rational number and μ be a positive integer. Then the μ-th Dickson polynomial is defined by

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

Kind	Standard pair (unordered)	Parameter restrictions
First	$(x^q, \alpha x^p v(x)^q)$	$0 \leq p < q$, $(p, q) = 1$, $p + \deg(v) > 0$
Second	$(x^2, (\alpha x^2 + \beta) v(x)^2)$	-
Third	$(D_\mu(x, \alpha^\nu), D_\nu(x, \alpha^\mu))$	$\gcd(\mu, \nu) = 1$
Fourth	$(\alpha^{-\mu/2} D_\mu(x, \alpha), -\beta^{-\nu/2} D_\nu(x, \beta))$	$\gcd(\mu, \nu) = 2$
Fifth	$((\alpha x^2 - 1)^3, 3x^4 - 4x^3)$	-

TABLE 1. Standard pairs. Here α, β are non-zero rational numbers, μ, ν, q are positive integers, p is a non-negative integer, $v(x) \in \mathbb{Q}[x]$ is a non-zero, but possibly constant polynomial.

For properties of Dickson polynomials see e.g. [5]. The polynomials $F, G \in \mathbb{Q}[x]$ form a standard pair over $\mathbb{Q}$ if either $(F(x), G(x))$ or $(G(x), F(x))$ appears in Table 1.

Lemma 3.4 (Bilu, Tichy [1], Theorem 1.1)**.** *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.*

A multiple root is a root of multiplicity > 1.

Lemma 3.5. *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.*

Proof. Let $f(x)$ be given by (4) as in Remark 2. For any root α of $f(x) - b$ let $v_\alpha(x)$ denote the monic minimal defining polynomial of α over $\mathbb{Q}$. If α is a triple (or higher multiplicity) root of $f(x) - b$, then let $v(x) = v_\alpha(x)$. Similarly, if α is a double root of $f(x) - b$ with $\deg(v_\alpha) \geq 2$, then let $v(x) = v_\alpha(x)$. Finally, if $\deg(v_\alpha) = 1$ in the case of at least two roots of multiplicities ≥ 2, then take any other multiple root β of $f(x) - b$ and let $v(x) = v_\alpha(x) v_\beta(x)$. Observe that in each case, we can write

$$f(x) - b = g(x)(v(x))^\ell \tag{5}$$

with a monic $g \in \mathbb{Q}[x]$ and $\ell \geq 2$, and either $k := \deg(v) \geq 2$ or $\ell \geq 3$. Write $b = q_1/q_2$ with coprime integers q_1, q_2 ($q_2 > 0$), and $v(x) = v^*(x)/v_0$, $g(x) = g^*(x)/g_0$ with $v^*, g^* \in \mathbb{Z}[x]$ primitive polynomials, v_0, g_0 positive integers. (Since v and g are monic, such v^*, g^*, v_0, g_0 exist.) Rewrite (5) as

$$q_2 f(x) - q_1 = \frac{q_2}{g_0 v_0^\ell} g^*(x)(v^*(x))^\ell. \tag{6}$$

Since $q_2 f(x) - q_1$ and $g^*(x)(v^*(x))^\ell$ are primitive polynomials in $\mathbb{Z}[x]$ (the latter one by the Gauss lemma), we see that $q_2/g_0 v_0^\ell = 1$ in (6). Suppose that $q_2 \neq 1$. Let p be any prime with $p \mid q_2$. Then taking (6) modulo p, we see that

$$v^*(x) \equiv c \pmod{p} \tag{7}$$

for some integer c with $p \nmid c$. Taking now derivatives in (5) we obtain

$$f'(x) = (v(x))^{\ell-1} h(x) \tag{8}$$

with

$$h(x) = g'(x)v(x) + \ell g(x) v'(x).$$

Note that $\deg(f') = n-1$, $\deg(h) = n-1-k(\ell-1)$. There exist coprime positive integers h_0, h_1 and a primitive polynomial $h^*(x) \in \mathbb{Z}[x]$ such that $h(x) = h_1 h^*(x)/h_0$. Thus we can rewrite (8) as

$$f'(x) = \frac{h_1}{v_0^{\ell-1} h_0} v^*(x)^{\ell-1} h^*(x). \tag{9}$$

Recall Remark 2. Since

$$f'(x) = nx^{n-1} + (n-1)x^{n-2} + \ldots + 2\varepsilon_{n-2}x + \varepsilon_{n-1}$$

as well as $v^*(x)^{\ell-1} h^*(x)$ are primitive polynomials in $\mathbb{Z}[x]$, we see that $h_1/v_0^{\ell-1} h_0 = 1$. Taking (9) modulo p with the above prime $p \mid q_2$, we obtain by (7) that

$$\deg(f'(x) \pmod{p}) \leq n - 1 - k(\ell - 1).$$

However, since the coefficients of the first two terms of $f'(x)$ are n and $n-1$ which are coprime, we see that

$$\deg(f'(x) \pmod{p}) \geq n - 2.$$

As $k \geq 2, \ell \geq 2$ or $\ell \geq 3$ this is a contradiction. Hence we conclude that $q_2 = 1$, hence $b \in \mathbb{Z}$.

Next we show that under the assumptions of the statement, the multiple roots of $f(x) - b$ are units. Let α be any such root. Then, since $b \in \mathbb{Z}$, α is an algebraic integer. Thus $v_\alpha(x) \in \mathbb{Z}[x]$ and $(v_\alpha(x))^2 \mid f(x) - b$ over $\mathbb{Z}$, whence $v_\alpha(x) \mid f'(x)$ over $\mathbb{Z}$. As $f'(0) = \pm 1$, our claim follows. $\square$

We shall also apply the following information concerning the roots of shifted Littlewood polynomials.

Lemma 3.6. *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*

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

Proof. We have

$$|\alpha|^n \leq |\alpha|^{n-1} + |\alpha|^{n-2} + \ldots + |\alpha| + 1 + |b| = \frac{|\alpha|^n - 1}{|\alpha| - 1} + |b| < \frac{|\alpha|^n}{|\alpha| - 1} + |b|.$$

From this the statement follows. □

Finally, we shall also use the following result from [4].

Lemma 3.7. *Let $Q(x) \in \mathbb{Z}[x]$ be a non-constant polynomial and r, t be integers with $0 \leq r < t$, $t \geq 2$. If all the coefficients of the polynomial $(x-1)^r(Q(x))^t$ belong to $\{-1, 1\}$, then $t = 2$, $r = 1$ and $Q(x)$ is of the form*

$$Q(x) = \pm(x^k + \ldots + x + 1) \tag{10}$$

with some $k \geq 1$. If all the coefficients of the polynomial $(x+1)^r(Q(x))^t$ belong to $\{-1, 1\}$, then $t = 2$, $r = 1$ and $Q(x)$ is of the form

$$Q(-x) = \pm(x^k + \ldots + x + 1) \tag{11}$$

with some $k \geq 1$.

Proof. The first statement is Lemma 3.6 in [4]. The second statement follows by the substitution $x \to -x$. □

4. Proofs of the theorems

Proof of Theorem 2.1. Let $f(x)$ be given by (4). The bound for m follows from Lemma 3.1, unless $f(x) - b$ is of the shape $f(x) = (x - s)^n$ with $s \in \mathbb{Q}$. Since Lemma 3.5 implies $b \in \mathbb{Z}$, we have $s \in \mathbb{Z}$. However, we get a contradiction with the fact that the coefficient of x^{n-1} is 1 in $f(x) - b$.

Thus, by Lemma 3.1, we may assume that m is fixed. Now our claim follows from Lemma 3.2, 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 $P, Q \in \mathbb{Q}[x]$, $\deg(P) = 2$.

Throughout the proof we suppose without loss of generality that P, Q are both monic.

For $n = 4$ a simple computer calculation shows that i) is impossible, while ii) can occur only when we have

$$(f(x), b)) = (x^4 + x^3 - x^2 - x \pm 1, \pm 1).$$

Since this possibility is among the exceptional cases (2), we may assume that $n \geq 5$. Lemma 3.5 implies $b \in \mathbb{Z}$, so we infer that $P, Q \in \mathbb{Z}[x]$. We consider cases i) and ii) in turn.

Assume first that i) holds. If $r = 0$ or $P(x)$ is constant then, since the coefficient of x^{n-1} is 1 on the left-hand side, while it is divisible by t on the right-hand side, we get a contradiction. So $r \geq 1$ and $P(x)$ is linear. We write $P(x) = x - s$ with $s \in \mathbb{Z}$. Since either $t \geq 3$ or $\deg(Q) \geq 2$, and the roots of Q are multiple roots of $f(x) - b$, by Lemma 3.5 we obtain $Q(0) = \pm 1$. Further, the same lemma yields that for $r \geq 2$ we have $s = \pm 1$. We apply Lemma 3.7 and obtain a contradiction. We conclude that the statement of Theorem 2.1 holds if $r \geq 2$.

So we may assume that $r = 1$. Comparing the constant terms, we see that $b = \varepsilon_n \pm s$. Lemma 3.6 with $n \geq 5, |b| \leq 3$ yields $|s| < 3$.

If $|s| = 1$ then Lemma 3.7 implies that $Q(x)$ is of the form (10) or (11). This leads to the first two options of (2).

If $s = 0$ then comparing the coefficients of x^{n-1} on both sides we get a contradiction: it is 1 on the left-hand side, while it is a multiple of t on the right-hand side.

Hence we are left with $s = \pm 2$. Since s is a root of $f(x) - b$, we have (recall Remark 2)

$$f(s) - b = s^n + s^{n-1} + \varepsilon_2 s^{n-2} + \cdots + \varepsilon_{n-1} s + \varepsilon_n - b = 0. \tag{12}$$

In view of $|s^n + s^{n-1}| \geq 2^{n-1}$, and as by $\varepsilon_n - b = \pm 2$ we have

$$|\varepsilon_2 s^{n-2} + \cdots + \varepsilon_{n-1} s + \varepsilon_n - b| \leq 2^{n-2} + 2^{n-3} + \cdots + 2^1 + 2 = 2^{n-1},$$

(12) is only possible if $s = -2$ and all other terms in (12) have signs opposite to that of s^n. Thus we conclude

$$f(x) - b = x^n + x^{n-1} - x^{n-2} + \ldots + (-1)^{n-2} x + (-1)^{n-1} \cdot 2. \tag{13}$$

Hence we easily get

$$(Q(x))^t = x^{n-1} - x^{n-2} + \ldots .$$

However, it is not possible, since the coefficient of x^{n-2} is not divisible by t. Thus the theorem is true in case i).

Suppose that ii) holds. Write $P(x) = x^2 + ux + w$. Recall that $n = \deg(f) \geq 5$ - thus now in fact $n \geq 6$. First we clarify the parity of

u and w. Taking the equation in ii) modulo 2 we obtain

$$x^n + x^{n-1} + x^{n-2} + x^{n-3} + \ldots \equiv$$
$$\equiv (x^2 + ux + w)(x^{n-2} + \delta_1 x^{n-4} + \delta_2 x^{n-6} + \ldots) \pmod 2.$$

Here *a priori* $\delta_1, \delta_2 \in \{0, 1\}$. Comparing the coefficients of x^{n-1}, x^{n-3}, x^{n-2} (in this order) on both sides, we successively get that u is odd, $\delta_1 = 1$ and w is even.

Since $n \geq 6$, Lemma 3.5 implies (as in case $r \geq 2$ of i)) that $Q(0) = \pm 1$, and consequently $f(0) - b = w$. Observe that $P(x)$ has a root α with $|\alpha| \geq \sqrt{|w|}$. Since $b = -w \pm 1$, for $n \geq 6$ Lemma 3.6 yields that

$$\frac{\sqrt{|w|} - 2}{\sqrt{|w|} - 1} |w|^3 < |w| + 1.$$

This implies $|w| \leq 4$. Hence by the parity condition above, we obtain $w \in \{0, \pm 2, \pm 4\}$. Assume first that $w = 0$. Then $f(0) - b = 0$, and taking out a factor x the equality in ii) simplifies to

$$\frac{f(x) - b}{x} = (x + u)(Q(x))^2.$$

Observe that the polynomial on the left hand side is a Littlewood polynomial. So $u = \pm 1$, and by Lemma 3.7 we obtain (similarly as in case $r = 1, s = \pm 1$ of Case i)) that $Q(x)$ is of the form (10) or (11). This yields the third option of (2) and

$$\frac{f(x) - b}{x} = (x - 1)(x^k + \ldots + x + 1)^2.$$

From this our claim follows in case $w = 0$. For the remaining values of w, Lemma 3.6 implies

$$\frac{|\alpha_{1,2}| - 2}{|\alpha_{1,2}| - 1} |\alpha_{1,2}|^6 < |w| + 1 \leq 5$$

for any of

$$\alpha_{1,2} = \frac{-u \pm \sqrt{u^2 - 4w}}{2}$$

with absolute value > 2. A simple calculation gives that then $|\alpha_{1,2}| < 2.1$. A further calculation yields that both roots are below this bound in absolute value only if $u = 0$ for $w = -4$; $|u| \leq 4$ for $w = 4$; $|u| \leq 1$ for $w = -2$; $|u| \leq 3$ for $w = 2$. Since u must be odd, we are left with the following polynomials:

$$P(x) = x^2 \pm 3x + 4,\ x^2 \pm x + 4,\ x^2 \pm x - 2,\ x^2 \pm 3x + 2,\ x^2 \pm x + 2.$$

We handle these possibilities in turn.

Let α be a root of any of the polynomials $P(x) = x^2 \pm 3x + 4$, $x^2 \pm x + 4$. Then $|\alpha| = 2$, and α is a root of $f(x) - b$. Since the constant term of $f(x) - b$ is 4, we obtain

$$2^n = |\alpha|^n \leq |\alpha|^{n-1} + \cdots + |\alpha|^4 + M = 2^n - 16 + M,$$

where

$$M = \max_{\varepsilon_1,\varepsilon_2,\varepsilon_3 \in \{-1,1\}} |\varepsilon_3\alpha^3 + \varepsilon_2\alpha^2 + \varepsilon_1\alpha + 4|.$$

However, a computer calculation shows that $M < 16$ for these choices of $P(x)$. Hence these cases cannot occur.

Consider now the polynomials $P(x) = x^2 \pm x - 2$, $x^2 \pm 3x + 2$. Observe that -2 or 2 is a root of these polynomials. Further, the constant term of $f(x) - b$ equals ± 2 in these cases. Thus we get (similar to (13), recall that $f(x)$ is of the form (4), and that n is even)

$$f(x) - b = x^n + x^{n-1} - x^{n-2} + x^{n-3} - x^{n-4} + \ldots - x^2 + x - 2$$

with a root -2. This, in view of the signs of the constant terms, rules out the polynomials $P(x) = x^2 \pm 3x + 2$. In case $P(x) = x^2 \pm x - 2$ we get, since f is a Littlewood polynomial,

$$(Q(x))^2 = x^{n-2} + x^{n-4} + \ldots + x^2 + 1.$$

Then, writing

$$Q(x) = x^{\frac{n-2}{2}} + q_1 x^{\frac{n-4}{2}} + q_2 x^{\frac{n-6}{2}} + \ldots,$$

from the coefficients of x^{n-3} we see that $q_1 = 0$, and then from the coefficients of x^{n-4} that $2q_2 = 1$. This contradicts $Q(x) \in \mathbb{Z}[x]$. So these cases are not possible either.

Thus we are left with $P(x) = x^2 \pm x + 2$. Write

$$Q(x) = x^k + q_1 x^{k-1} + \ldots + q_{k-1}x + q_k$$

with $n = 2k + 2$. Recall that $q_1, \ldots, q_k \in \mathbb{Z}$ with $q_k = \pm 1$. First we argue that the equality

$$f(x) - b = (x^2 \pm x + 2)(Q(x))^2 \tag{14}$$

implies that $q_1, \ldots, q_k$ are all odd. Indeed, if i is the smallest index with q_i is even, then the coefficients of x^{2i-1}, x^{2i}, x^{2i+1} would all be even in $(Q(x))^2$, so the coefficient of x^{2i+1} would be even in $f(x) - b$, a contradiction. Expanding the first few coefficients on the right-hand side of (14) we get

$$\begin{aligned} x^n + x^{n-1} + \varepsilon_2 x^{n-2} + \ldots &= \\ &= x^n + (2q_1 \pm 1)x^{n-1} + (2q_2 + q_1^2 \pm 2q_1 + 2)x^{n-2} + \ldots . \end{aligned}$$

Hence, using that q_1 and q_2 are odd, we obtain successively

$$q_1 = 1, \quad P(x) = x^2 - x + 2, \quad q_2 = -1, \quad \varepsilon_2 = -1.$$

Write α for a root of $x^2 - x + 2$. Since α is a root of $f(x) - b$, we obtain

$$|\alpha^n + \alpha^{n-1} - \alpha^{n-2}| \leq |\alpha|^{n-3} + \cdots + |\alpha| + |f(0) - b|.$$

Note that $|\alpha| = \sqrt{2}$ and $|\alpha^2 + \alpha - 1| > 6$. Since the constant term $f(0) - b$ of $f(x) - b$ is 2, we obtain

$$6 \cdot (\sqrt{2})^{n-2} < \frac{(\sqrt{2})^{n-2} - 1}{\sqrt{2} - 1} + 1.$$

This gives a contradiction, which shows that $P(x) = x^2 - x + 2$ is also impossible. Hence the theorem is proved. □

Proof of Theorem 2.2. Let $f(x)$ be of the form (4). Then Lemma 3.3 implies that $f(x)$ is indecomposable over $\mathbb{Q}$. Thus, if equation (3) has infinitely many solutions in integers x, y, then by Lemma 3.4 we have only two options. Either $g(x)$ is of the form $g(x) = f(T(x))$ with some $T(x) \in \mathbb{Z}[x]$ (in which case (3) clearly has infinitely many integer solutions indeed) or $f(x)$ is of the shape

$$f(x) = AF(ux + w) + B, \tag{15}$$

with some $A, B, u, w \in \mathbb{Q}$, $Au \neq 0$, where F belongs to a standard pair from Table 1. Only the latter case needs more investigation.

Suppose first that $F(x)$ belongs to case I or II of Table 1. Since a Littlewood polynomial cannot be a perfect power of another polynomial, in these cases $G(x)$ is a perfect power of x and $F(x)$ is the other possibility in Table 1. Therefore $f(x)$ is of the shape occurring as i) or ii) in the proof of Theorem 2.1 and $g(x) = P(cx + d)$ for some $c, d \in \mathbb{Q}, c \neq 0$. So the statement follows Theorem 2.1 in the cases I and II.

Now assume that we are in case III or IV of Table 1. Then $F(x)$ is a constant multiple of a Dickson polynomial in (15). Clearly, (15) is equivalent to

$$f\left(\frac{x - w}{u}\right) = AD_n(x, \delta) + B \tag{16}$$

with some non-zero $\delta \in \mathbb{Q}$, where n is the degree of f. (Here in case III, A is replaced by another constant.) Recall that $n \geq 4$. Since D_n is either an odd or an even polynomial (depending on the parity of n), comparing the coefficients of x^{n-1} and x^{n-3} in (16), we get

$$-\frac{nw}{u^n} + \frac{1}{u^{n-1}} = 0,$$

$$-\binom{n}{3}\frac{w^3}{u^n}+\binom{n}{2}\frac{w^2}{u^{n-1}}-\varepsilon_2\frac{nw}{u^{n-2}}+\varepsilon_3\frac{1}{u^{n-3}}=0,$$

respectively. These equalities imply

$$(3\varepsilon_3-3\varepsilon_2+1)n^2-1=0.$$

Hence $n=\pm 1$, which is excluded.

Finally, suppose that $F(x)$ comes from case V of Table 1. The polynomial $(\alpha x^2-1)^3$ is an even polynomial of degree 6 and it can be handled and excluded in the same way as the possibilities in the cases III and IV. If $F(x)=3x^4-4x^3$, then (15) gives

$$f(x)=A(3(ux+w)^4-4(ux+w)^3)+B.$$

A simple calculation shows that $f(x)$ cannot be a Littlewood polynomial. Hence the theorem is proved. □

Acknowledgements

The authors are grateful to the referee for her/his work and for the helpful remarks.

References

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

[2] B. Brindza, *On S-integral solutions of the equation $y^m=f(x)$*, Acta Math. Hungar. **44** (1984), 133–139.

[3] A. Dujella and I. Gusić, *Indecomposability of polynomials and related Diophantine equations*, Q. J. Math. **57** (2006), 193–201.

[4] L. Hajdu, N. Varga, *Diophantine equations for polynomials with restricted coefficients, I (power values)*, Bull. Austral. Math. Soc. (to appear), https://doi.org/10.1017/S0004972722000132.

[5] R. Lidl, G. Mullen, G. Turnwald, *Dickson polynomials*, Pitman Monographs and Surveys in Pure and Applied Mathematics **65**, Longman Scientific & Technical, Harlow, 1993.

[6] A. Schinzel, R. Tijdeman, *On the equation $y^m=P(x)$*, Acta Arith. **31** (1976), 199–204.

Institute of Mathematics, University of Debrecen,
P. O. Box 400, H-4002 Debrecen, Hungary
and ELKH-DE Equations, Functions, Curves and their Applications Research Group
Email address: hajdul@science.unideb.hu

Mathematical Institute, Leiden University,
Postbus 9512, 2300 RA Leiden, The Netherlands
Email address: tijdeman@math.leidenuniv.nl

Institute of Mathematics, University of Debrecen,
P. O. Box 400, H-4002 Debrecen, Hungary
and ELKH-DE Equations, Functions, Curves and their Applications Research Group
Email address: nvarga@science.unideb.hu