FINITENESS RESULTS FOR SOME FAMILIES OF POLYNOMIAL DIOPHANTINE EQUATIONS

Thesis for the Degree of Doctor of Philosophy (PhD)

Orsolya Szilágyi-Herendi
Supervisor: Dr. Lajos Hajdu

UNIVERSITY OF DEBRECEN
Doctoral Council for Natural Sciences and Engineering
Doctoral School of Mathematical and Computional Sciences
Debrecen, 2025

Hereby I declare that I prepared this thesis within the Doctoral Council for Natural Sciences and Engineering, Doctoral School of Mathematical and Computional Sciences, University of Debrecen in order to obtain a PhD Degree in Natural Sciences at Debrecen University.
The results published in the thesis are not reported in any other PhD theses.

Debrecen, 2025.10.01.

……………………….
signature of the candidate

Hereby I confirm that Orsolya Szilágyi-Herendi candidate conducted her studies with my supervision within the Constructive and Diophantine Doctoral Program of the Doctoral School of Mathematical and Computional Sciences between 2020 and 2024. The independent studies and research work of the candidate significantly contributed to the results published in the thesis. I also declare that the results published in the thesis are not reported in any other theses.
I support the acceptance of the thesis.

Debrecen, 2025.10.01.

……………………………
signature of the supervisor

FINITENESS RESULTS FOR SOME FAMILIES OF POLYNOMIAL DIOPHANTINE EQUATIONS

Dissertation submitted in partial fulfilment of the requirements for the doctoral (PhD) degree
in Mathematics and Computing

Written by Orsolya Szilágyi-Herendi certified mathematician

Prepared in the framework of the Doctoral School of Mathematical and Computional Sciences of the University of Debrecen
(Constructive and Diophantine Number Theory programme)

Dissertation supervisor: Dr. Lajos Hajdu

The official opponents of the dissertation:

Dr. ....
Dr. ....

The evaluation board:
chairperson: Dr. ....
members: Dr. ....
Dr. ....
Dr. ....
Dr. ....

The date and venue of the dissertation defence: Debrecen 2025.

Köszönetnyílvánítás

Köszönöm a témavezetőmnek az egyetemi éveim során nyújtott rengeteg segítségét és támogatását. Hálás vagyok tanáraimnak, akik motiváltak és végig hittek bennem. Köszönöm az egyetemi csoporttársaimnak, akik megmutatták, hogy együtt könnyebb.

Köszönöm a szüleimnek, hogy a tanulmányaim során végig támogattak, segítettek a céljaim kiválasztásában és teljesítésében.

Köszönöm a férjemnek a türelmét, lelkesítését, megértését és folyamatos támogatását.

Contents

Chapter 1

Introduction

The main theme of this dissertation is the study of various polynomial Diophantine equations, where the polynomials considered belong to some specific family with some interesting and/or important feature. Polynomial Diophantine equations form a classical field of Diophantine number theory, however, at the same time, being in the focus of recent interest, as well. As classical examples of such equations one can mention, for example Thue-equations and elliptic, hyperelliptic and superelliptic equations. For a history and a summary of some of the most important results related to these equations, one can read e.g. the corresponding chapters of the book of Shorey and Tijdeman [57].

In what follows, we only concentrate on those topics in the field of polynomial Diophantine equations which appear in our present studies. At this point we only shortly discuss these topics, and briefly summarize our results and their background. A precise and detailed description of the studied problems and our new results, together with a survey of the related literature, will be provided in the corresponding chapters.

The first topic we study is the following: what can we say about the number of integral points in some 'interesting' sets (e.g., in certain regular solids)? In particular, we focus on the following solids: n-dimensional cube, pyramid and simplex. Counting the integral points in these objects, one finds (see [17]) that the following polynomials arise, respectively:

$$(x+1)^n, \quad S_{n-1}(x) := 1^{n-1} + \cdots + (x+1)^{n-1}, \quad \binom{x+n}{n}. \tag{1.1}$$

Here n is the dimension, and x describes the size of the solid. Equations of the type

$$f(x) = g(y) \tag{1.2}$$

where $f(x)$ belongs to one of the families in (1.1) and $g(y)$ is a polynomial with integer coefficients, have been heavily studied in the literature, by several authors. A thorough overview of the corresponding literature will be given in the third chapter of the dissertation, here we only make some notes related to the most general cases (i.e., when there is no further restriction imposed on $g(y)$). For $f(x) = (x+1)^n$ equation (1.2) is just a hyperelliptic equation (see e.g. the corresponding chapter of Shorey and Tijdeman [57] or the theorem of Brindza [14], also given in the next chapter); for $f(x) = S_{n-1}(x)$ equation (1.2) has been considered by Rakaczki [49]; when $f(x) = \binom{x+n}{n}$ then (1.2) has been studied by Kulkarni and Sury [42]. In every case it turns out that (apart from certain well-described cases), (1.2) has only finitely many solutions. (More, and more precise discussion will follow in the third chapter.) Here we consider the problem of counting integral points not *in the interior*, rather *on the surface* of these solids. As it will turn out, the number of such integral points (in the above settings) are described by the polynomials

$$(x+1)^n - (x-1)^n, \quad (x+1)^{n-1} + x^{n-1}, \quad \binom{x+n}{n} - \binom{x-1}{n},$$

respectively. We study equation (1.2) for polynomials coming from the above families. We prove that (apart from certain special, completely described cases) (1.2) allows only finitely many integer solutions x, y, moreover, if $g(y)$ is of the shape $g(y) = Ay^\ell + B$, then $\max(\ell, |x|, |y|)$ is bounded by a constant depending only on the parameters involved.

The starting point of the next topic we study is a classical theorem of Erdős and Selfridge [20]: the product of two or more consecutive positive integers cannot be a perfect power. This problem has been extended into various directions. One of the most important generalizations concerns the problem of perfect powers in products of consecutive terms of arithmetic progressions. There are a huge amount of papers devoted to this question (see, for example, the paper by Győry, Hajdu and Pintér [27] for the case of at most 34 terms, and the references given there) - however, it is still unsolved. In most related results, naturally, the strong structure of the underlying arithmetic progression is of utmost importance. It is an interesting question how far one can 'disturb' this structure still to have definitive (finiteness) results. See for example a recent paper by Hajdu, Papp and Tijdeman [36] where equation (1.2) is studied for polynomials f having roots from an arithmetic progressions - however, these roots are not (necessarily) consecutive terms, some terms of the progression are omitted. (In the literature one can find various related results, see e.g. the references in [36].) In the fourth chapter of the dissertation we approach the problem from another, new direction. Namely, we keep the symmetry of the roots of $f(x)$, however, we allow arbitrarily large gaps among them. More precisely, we prove that if the roots of $f(x)$ form a symmetric, convex set then (1.2) has only finitely many integer solutions x, y.

Finally, in the fifth chapter of the dissertation we study square values of Littlewood polynomials, i.e. polynomials with all coefficients equal to ± 1. In fact, this means that we consider equation (1.2) for $f(x)$ being a Littlewood polynomial and $g(y) = y^2$. The polynomial values of Littlewood polynomials, from the viewpoint of finiteness of solutions, have already been studied by Hajdu, Tijdeman and Varga [37]. Further, the problem is a generalization of the famous Nagell-Ljunggren equation

$$\frac{x^n - 1}{x - 1} = y^\ell$$

in the case $\ell = 2$. The above equation has been studied by many mathematicians, in several papers. A classical result of Ljunggren [44] gives that for $\ell = 2$ the only solutions are $(x, y, n) = (7, \pm 20, 4)$. Here we shall be interested in finding *all solutions* of the equation. Combining various methods (e.g. the theory of elliptic curves, hyperelliptic curves and Runge's method), we succeed to list all solutions in cases $n = 3, 5$ and $2 \leq n \leq 24$, n even. Beside this, we gather some information for the case of n odd with $n \leq 17$. Based upon the data obtained, we can formulate some striking questions for further research, as well.

In the proofs of our results, we need to combine several deep tools, among others Baker's method and a celebrated theorem of Bilu and Tichy [12], guaranteeing the finiteness of the number of integral solutions of equations of the shape $f(x) = g(y)$.

The dissertation is structured in the following way. In the second chapter we collect the most important tools we use at several points later on. Namely, we provide a famous theorem of Schinzel and Tijdeman [56] giving an upper bound for the exponent of the powers in the value sets of polynomials, and a classical result of Brindza [14] yielding an upper bound for the solutions of superelliptic equations. Note that both results are based upon Baker's method. We also formulate the above mentioned theorem of Bilu and Tichy [12]. The forthcoming three chapters contain our results, in the order indicated above.

Chapter 2

Methods and tools

In this chapter we introduce some notation and lemmas. They will be used multiple times in our dissertation so we give them here. They are our main tools in giving effective and ineffective finiteness results for various polynomial Diophantine equations.

Let $T(x) \in \mathbb{Z}[x]$. By the height H of the polynomial $T(x)$ we mean the maximum of the absolute value of its coefficients. Let A be an integer with $A \neq 0$, and consider the equation

$$T(x) = Ay^m, \tag{2.1}$$

in unknown integers x, y, m with $m \geq 2$, under the convention that $m \leq 3$ if $|y| \leq 1$.

The next result is due to Schinzel and Tijdeman [56] (see also Tijdeman [65]).

Lemma 2.1. *If $T(x)$ has at least two different roots, then for all solutions of* (2.1)

$$m < C_1(A, d, H)$$

holds. Here $C_1(A, d, H)$ is an effectively computable constant depending only on A, the degree d and the height H of $T(x)$.

The following lemma is a special case of the main result of Brindza [14]. Ultimately, it is based on Baker's method. In order to formulate it we need some new notation. Let S be a finite set of primes, and let $\mathbb{Z}_S$ be the set of those rationals whose denominators are composed exclusively of primes from S. By the height $h(q)$ of a rational number q we mean the maximum of the absolute value of its denominator and numerator.

Lemma 2.2. *Let $T(x) \in \mathbb{Z}[x]$, and write*

$$T(x) = a \prod_{i=1}^{k} (x - \gamma_i)^{r_i},$$

where a is the leading coefficient of T, and $\gamma_1, \ldots, \gamma_k$ are the distinct complex roots of $T(x)$, with multiplicities $r_1, \ldots, r_k$, respectively. Further, fix m with $m \geq 2$, and put

$$t_i = \frac{m}{(m, r_i)} \qquad (i = 1, \ldots, k).$$

Suppose that $(t_1, \ldots, t_k)$ is not a permutation of any of the k-tuples

$$(t, 1, \ldots, 1) \ (t \geq 1), \quad (2, 2, 1, \ldots, 1).$$

Then for any finite set S of primes, the solutions $x, y \in \mathbb{Z}_S$ of (2.1) *satisfy*

$$\max\left(h(x), h(y)\right) < C_2(A, m, d, H, S),$$

where $C_2(A, m, d, H, S)$ is an effectively computable constant depending only on A, m, d, H, S, where d is the degree and H is the height of $T(x)$.

The next lemma is a deep result of Bilu and Tichy [12]. To formulate it we need some more notation.

By the *decomposition* of a polynomial $T(x)$ over a field K we mean a composition of the form $T(x) = U_1(U_2(x))$, where $U_1(x), U_2(x) \in K[x]$. We say that the decomposition is *nontrivial* if $\deg(U_1) > 1$ and $\deg(U_2) > 1$. Two decompositions $T(x) = U_1(U_2(x))$ and $T(x) = V_1(V_2(x))$ are *equivalent* if there exists a linear polynomial $t(x) \in K[x]$ such that $U_1(x) = V_1(t(x))$ and $V_2(x) = t(U_2(x))$. If $T(x)$ has at least one nontrivial decomposition over K then we say that $T(x)$ is *decomposable*; otherwise $T(x)$ is *indecomposable.*

Let α, β, $\delta \in \mathbb{Q} \setminus \{0\}$, μ, ν, q be positive integers, r be a non-negative integer, and $v(x) \in \mathbb{Q}[x]$ a polynomial, which is not identically zero. Write $D_\mu(x, \delta)$ for the μ-th Dickson polynomial, that is

$$D_\mu(x, \delta) = \sum_{i=0}^{\lfloor \mu/2 \rfloor} d_{\mu,i} x^{\mu - 2i},$$

where

$$d_{\mu,i} = \frac{\mu}{\mu - i} \binom{\mu - i}{i} (-\delta)^i.$$

We say that the polynomials $F(x)$ and $G(x)$ form a standard pair over $\mathbb{Q}$, if $(F(x), G(x))$ or $(G(x), F(x))$ appears in Table 2.1.

The following lemma is the main result of Bilu and Tichy [12].

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

Table 2.1: Standard pairs

Lemma 2.3. *Let $f(x), g(x) \in \mathbb{Q}[x]$ be non-constant polynomials. Then the following two assertions are equivalent.*

i) The equation

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

has infinitely many solutions with a bounded denominator.

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

Chapter 3

Polynomial values of surface point counting polynomials

3.1 Introduction

There are many problems related to the description and various properties of polynomials providing the number of lattice points in certain regular bodies.

In the present chapter, among such bodies we focus on the n-dimensional cube, pyramid and simplex. As it is well known [17], the number of integral points in the interior of these bodies in $\mathbb{R}^n$ (in case of their usual placement) is given by the polynomials

$$(x+1)^n, \quad 1^{n-1}+2^{n-1}+\cdots+(x+1)^{n-1}, \quad \binom{x+n}{n}, \tag{3.1}$$

respectively.

The polynomial values of the first polynomial in (3.1), namely the so called superelliptic equation

$$(x+1)^n = g(y)$$

has been studied by many mathematicians. Here g is a polynomial with rational coefficients and x, y are integral unknowns. Results of Tijdeman [65] and Schinzel and Tijdeman [56] imply that under certain necessary assumptions here n can be effectively bounded. Baker (see [1, 2]) and Brindza [14] showed that given n, under some assumptions one can also bound the absolute values of x, y, as well. For further related results see the book of Shorey and Tijdeman [57].

The second polynomial in (3.1) is denoted by $S_{n-1}(x+1)$. The polynomial values of this polynomial, i.e. the equation

$$S_{n-1}(x+1) = g(y)$$

where g is a polynomial with rational coefficients and x, y are integral unknowns, has also been intensively studied. In the special case where g is of the form $g(y) = y^\ell$, a classical result of Schäffer [55] shows that (apart from certain completely described exceptions) the above equation has only finitely many solutions for n fixed. When $g(y)$ is a shifted power, or more generally it is of the shape $g(y) = Ay^\ell + B$ with $A, B \in \mathbb{Q}$, $A \neq 0$, Győry, Tijdeman and Voorhoeve [30] obtained deep finiteness results - again, with n fixed. Later, the same authors derived even more general finiteness results concerning shifts of $S_{n-1}(x+1)$ with polynomials (see [66]). The general case has been taken up by Rakaczki [49]. He proved that the previous equation for any fixed n, apart from certain well-described exceptions, has only finitely many solutions in integers x, y. For more related results see e.g. the papers Bennett, Győry and Pintér [6], Győry and Pintér [29], Bazsó [4] and Hajdu [31] and the references given there.

Finally, the investigation of the third polynomial in (3.1) reduces to the equation

$$\binom{x+n}{n} = g(y)$$

in integers x, y, where g is a polynomial with rational coefficients again. This is also a famous equation, studied by several authors. In the case where $g(y) = y^\ell$, the equation has been completely solved by Erdős [19] (for $n \geq 4$) and Győry [26] (for $n = 2, 3$). When g is of the shape $g(y) = Ay^\ell + B$ with $A, B \in \mathbb{Q}$, $A \neq 0$, Yuan [69] gave effective upper bounds for the absolute values of x, y. In the general case, Kulkarni and Sury [42] gave an ineffective finiteness theorem for the solutions of the previous equation.

Besides the above mentioned results, there are many more related papers in the literature. The interested reader may consult e.g. the paper of Bilu, Brindza, Kirschenhofer, Pintér and Tichy [11] or the survey paper of Győry, Kovács, Péter and Pintér [28] and the references therein.

In the present chapter we study the polynomials describing the number of lattice points on the *surfaces* of the above mentioned regular bodies. These polynomials can be obtained by certain differences of the polynomials in (3.1). Namely, one can easily check that the number of integral points on the surfaces of the n-dimesional cube, pyramid and simplex (for arbitrary $n \geq 1$) can be given by the polynomials

$$\begin{aligned} F_n(x) =& (x+1)^n - (x-1)^n, \\ G_n(x) =& (x+1)^{n-1} + x^{n-1}, \\ H_n(x) =& \binom{x+n}{n} - \binom{x-1}{n}, \end{aligned} \tag{3.2}$$

respectively. We provide various finiteness results for the polynomial values of $F_n(x)$,

$G_n(x)$, $H_n(x)$, that is for the integer solutions of the equations

$$F_n(x) = g(y), \quad G_n(x) = g(y), \quad H_n(x) = g(y)$$

where g is a polynomial with rational coefficients. In the general case our theorems are ineffective. However, in the case where g is of the form $g(y) = Ay^\ell + B$ with $A, B \in \mathbb{Q}$, $A \neq 0$ then we can provide effective finiteness results. In our proofs (among others) we combine Baker's method and the Bilu-Tichy theorem [12]. To apply these methods (as we shall see) we need to get precise information on the root structures of the polynomials, their derivatives and their shifts from (3.2). We shall also have to understand the decomposability properties of these polynomials. It is worth to mention that to prove the related properties of the difference polynomials (3.2) in many cases is significantly more difficult than in case of the original polynomials (3.1). Finally, we note that related investigations (i.e. papers concerned with differences of combinatorial polynomials) are known in the literature: see e.g. the paper of Liptai, Luca, Pintér and Szalay [43] (and the references there), where the equation $S_k(x-1) = S_\ell(y-1) - S_\ell(x)$ has been studied.

The structure of the chapter is the following. In the next section we give our main results. In Section 3.3 we describe the root structures of the polynomials (3.2) and of their derivatives and shifts, together with their decomposability properties. Then we provide the proofs of our effective statements. Finally, we give the proofs of our ineffective results.

3.2 Main results

In this chapter we examine the equation

$$W(x) = g(y) \tag{3.3}$$

where $W(x)$ is one of the polynomials $F_n(x)$, $G_n(x)$, $H_n(x)$ ($n \geq 1$) from (3.2), and $g(y) \in \mathbb{Q}[y]$. Our purpose is to prove finiteness results for the integer solutions x, y of (3.3). First we provide a general theorem for the problem considered. This result is ineffective, so it only shows the finiteness of the number of solutions, it does not give bounds for the solutions themselves.

Theorem 3.2.1 (L. Hajdu, O. Herendi [32]). *Let $n \geq 6$ and $\deg(g) \geq 2$. If equation (3.3) has infinitely many solutions in integers x, y then either*

$$g(y) = W(P(y))$$

where $P(y) \in \mathbb{Q}[y]$, or

$$g(y) = \hat{W}(Q(y))$$

where $Q(y) \in \mathbb{Q}[y]$ with at most two roots of odd multiplicity, n is odd, and in case of $W(x) = F_n(x)$, $G_n(x)$, $H_n(x)$ the polynomial $\hat{W}$ is φ_1, φ_2, φ_3, respectively, with

$$\varphi_1(x) = 2\binom{n}{1}x^{\frac{n-1}{2}} + 2\binom{n}{3}x^{\frac{n-3}{2}} + \cdots + 2\binom{n}{n-2}x + 2,$$

$$\varphi_2(x) = 2x^{\frac{n-1}{2}} + \frac{1}{2}\binom{n-1}{2}x^{\frac{n-3}{2}} + \cdots + \frac{1}{2^{n-4}}\binom{n-1}{n-3}x + \frac{1}{2^{n-2}},$$

$$\varphi_3(x) = \frac{2}{n!}(s_1 x^{\frac{n-1}{2}} + \cdots + s_n) \quad \text{where } s_j = \sum_{\substack{A \subseteq \{1,\ldots,n\} \\ |A| = j}} \prod_{a \in A} a \quad (j = 1, \ldots, n).$$

Remark 3.2.1. Clearly, we have to exclude polynomials g with $\deg(g) = 1$, so the assumption $\deg(g) \geq 2$ is necessary. The condition $n \geq 6$ is necessary, too. For $n \leq 5$ one can easily find counterexamples (which is not surprising in view of the many free parameters involved; see the proof of the theorem).

In the case where $g(y) = Ay^\ell + B$ with $A, B \in \mathbb{Q}$ with $A \neq 0$, we can give an effective upper bound for the absolute values of the integer solutions x, y of the equation (3.3).

Theorem 3.2.2 (L. Hajdu, O. Herendi [32])**.** *Let $n \geq 1$ and consider the equation*

$$W(x) = Ay^\ell + B \tag{3.4}$$

where $W(x)$ is one of the polynomials $F_n(x), G_n(x), H_n(x)$ from (3.2), A, B are given rationals with $A \neq 0$, and x, y and $\ell \geq 2$ are integer unknowns.

i) Let $n \geq 4$. Then there exists an effectively computable constant $C_3(A, B, n)$, depending only on A, B, n such that

$$\ell < C_3(A, B, n)$$

for every solutions of (3.4) with $|y| > 1$.

ii) Let $\ell \geq 2$ be arbitrary but fixed and $n \geq 8$. Then there exists an effectively computable constant $C_4(A, B, n)$, depending only on A, B, n such that

$$\max(|x|, |y|) \leq C_4(A, B, n)$$

for every integer solution x, y of (3.4).

Remark 3.2.2. Also in this case, the assumptions made for n are all necessary; one could easily find counterexamples in the excluded cases.

In the proof of our ineffective results the following theorem plays an important role. It completely describes the decompositions of the polynomial families $F_n(x)$, $G_n(x)$, $H_n(x)$.

Theorem 3.2.3 (L. Hajdu, O. Herendi [32]). *Let $n \geq 2$. If n is even then the polynomials $F_n(x)$, $G_n(x)$, $H_n(x)$ are indecomposable. If n is odd, then all the decompositions of these polynomials are equivalent with*

$$F_n(x) = \varphi_1(x^2), \quad G_n(x) = \varphi_2\left(\left(x + \frac{1}{2}\right)^2\right), \quad H_n(x) = \varphi_3(x^2),$$

respectively. Here φ_1, φ_2, φ_3 are the same polynomials as in Theorem 3.2.1.

3.3 Root structures and decompositions

In this section we describe the root structures of the studied polynomial families, of their derivatives and of their shifts. We also prove Theorem 3.2.3 in this section, characterizing the decompositions of the polynomials $F_n(x)$, $G_n(x)$, $H_n(x)$.

We note that obviously

$$\deg(F_n) = \deg(G_n) = \deg(H_n) = n - 1 \quad (n \geq 1).$$

3.3.1 The polynomial family $F_n(x)$

In this subsection we describe the root structure of $F_n(x)$, of its derivative and of its shifts. We start with $F_n(x)$ itself.

Lemma 3.3.1. *Let $n \geq 2$. Then all the roots of $F_n(x) = (x+1)^n - (x-1)^n$ are simple.*

Proof. Taking derivative we get

$$F_n'(x) = n(x+1)^{n-1} - n(x-1)^{n-1}$$

whence

$$nF_n(x) - (x+1)F_n'(x) = 2n(x-1)^{n-1}.$$

Thus the common roots of $F_n(x)$ and $F_n'(x)$ are also roots of $(x-1)^{n-1}$. As clearly there are no such roots, our claim follows. □

As a simple consequence we obtain the following statement concerning $F_n'(x)$.

Corollary 3.3.1. *Let $n \geq 3$. Then all the roots of $F_n'(x)$ are simple.*

Proof. Since $F_n'(x) = nF_{n-1}(x)$, the statement immediately follows from Lemma 3.3.1. □

In the next lemma we examine the root structure of the shifted polynomials of $F_n(x)$.

Lemma 3.3.2. *Let $n \geq 2$. Then for any $r \in \mathbb{C}$ the polynomial $F_n(x) + r$ has at most two multiple roots, which are at most double.*

Proof. By Lemma 3.3.1 we may assume that $r \neq 0$. Differentiating $F_n(x) + r$ we obtain

$$(F_n(x) + r)' = n(x + 1)^{n-1} - n(x - 1)^{n-1}.$$

Thus

$$n(F_n(x) + r) - (x - 1)(F_n(x) + r)' = 2n(x + 1)^{n-1} + nr.$$

So any common root α of $F_n(x) + r$ and $(F_n(x) + r)'$ is a root of $2(x + 1)^{n-1} + r$, which implies that

$$|\alpha + 1| = \sqrt[n-1]{\left|\frac{r}{2}\right|}. \tag{3.5}$$

On the other hand, we also have

$$n(F_n(x) + r) - (x + 1)(F_n(x) + r)' = 2n(x - 1)^{n-1} + nr.$$

So α is also a root of $2(x - 1)^{n-1} + r$ whence

$$|\alpha - 1| = \sqrt[n-1]{\left|\frac{r}{2}\right|}. \tag{3.6}$$

Combining (3.5) and (3.6) we see that the multiple roots of $F_n(x)+r$ are on the intersection of two distinct circles on the complex plane. This shows that there are at most two such roots. The multiplicity of these roots (if they exist) cannot be greater than two, since by Corollary 3.3.1 all the roots of $(F_n(x) + r)' = F_n'(x)$ are simple. □

Finally, we need the following assertion to prove the corresponding part of Theorem 3.2.3.

Lemma 3.3.3. *Let $n \geq 2$. Then* $\max_{\lambda \in \mathbb{C}} \deg(\gcd(F_n(x) - \lambda, F_n'(x))) \leq 2$.

Proof. We know from Lemma 3.3.2 that for any $\lambda \in \mathbb{C}$ the polynomial $F_n(x) - \lambda$ has at most two multiple roots, which are at most double. Hence $\deg(\gcd(F_n(x)-\lambda, F_n'(x))) \leq 2$, and our claim follows. □

3.3.2 The polynomial family $G_n(x)$

Now we examine the polynomials $G_n(x)$. Since this family is similar to $F_n(x)$, the proofs here are very similar to those in the previous subsection.

Lemma 3.3.4. *For any $n \geq 2$ the roots of the polynomial $G_n(x) = (x+1)^{n-1} + x^{n-1}$ are all simple.*

Proof. By taking derivative, we get that

$$G'_n(x) = (n-1)(x+1)^{n-2} + (n-1)x^{n-2}$$

and

$$(n-1)G_n(x) - (x+1)G'_n(x) = -(n-1)x^{n-2}.$$

Thus the common roots of $G_n(x)$ and $G'_n(x)$ are also roots of x^{n-2}. As 0 is not a root of $G_n(x)$ neither of $G'_n(x)$, our claim follows. □

By the previous statement we can easily describe the root structure of $G'_n(x)$, as well.

Corollary 3.3.2. *For any $n \geq 3$ the roots of the polynomial $G'_n(x)$ are all simple.*

Proof. As $G'_n(x) = (n-1)G_{n-1}(x)$, the statement immediately follows from Lemma 3.3.4. □

Now we examine the root structure of the shifts of $G_n(x)$.

Lemma 3.3.5. *Let $n \geq 2$. Then in case of any $r \in \mathbb{C}$ the polynomial $G_n(x) + r$ has at most two multiple roots, which are at most double.*

Proof. By Lemma 3.3.4 we may assume that $r \neq 0$. Differentiating $G_n(x) + r$ we obtain

$$(G_n(x) + r)' = (n-1)(x+1)^{n-2} + (n-1)x^{n-2}.$$

Thus

$$(n-1)(G_n(x) + r) - x(G_n(x) + r)' = (n-1)(x+1)^{n-2} + (n-1)r.$$

So any common root α of $G_n(x) + r$ and $(G_n(x) + r)'$ is a root of $(x+1)^{n-2} + r$, which implies that

$$|\alpha + 1| = \sqrt[n-2]{|r|}. \tag{3.7}$$

On the other hand, we also have

$$(n-1)(G_n(x) + r) - (x+1)(G_n(x) + r)' = -(n-1)x^{n-2} + (n-1)r.$$

So α is also a root of $-x^{n-2} + r$ whence

$$|\alpha| = \sqrt[n-2]{|r|}. \tag{3.8}$$

Combining (3.7) and (3.8) we see that the multiple roots of $G_n(x)+r$ are on the intersection of two distinct circles on the complex plane. This shows that there are at most two such roots. The multiplicity of these roots (if they exist) cannot be greater than two, since by Corollary 3.3.2 all the roots of $(G_n(x)+r)' = G'_n(x)$ are simple.

□

To prove the corresponding part of Theorem 3.2.3 we also need the following lemma.

Lemma 3.3.6. *Let* $n \geq 2$*. Then* $\max_{\lambda\in\mathbb{C}} \deg(\gcd(G_n(x)-\lambda, G'_n(x))) \leq 2$.

Proof. We know from Lemma 3.3.5 that for any $\lambda \in \mathbb{C}$ the polynomial $G_n(x)-\lambda$ has at most two multiple roots, which are at most double. Hence $\deg(\gcd(G_n(x)-\lambda, G'_n(x))) \leq 2$, and our claim follows. □

3.3.3 The polynomial family $H_n(x)$

Finally, we examine the family $H_n(x)$.

Lemma 3.3.7. *For all* $n \geq 2$*, all the roots of*

$$H_n(x) = \frac{1}{n!}\left((x+1)\dots(x+n)-(x-1)\dots(x-n)\right)$$

are simple. Further, the real part of any root of $H_n(x)$ *is zero.*

Proof. We distinguish two cases, according to the parity of n.

Assume first that n is odd. Observe that then the coefficients of the odd powers of $H_n(x)$ are zero. In particular, we easily see that $\deg(H_n) = n-1$ and 0 is not a root of $H_n(x)$. It is also obvious that if α is a root of $H_n(x)$, so is $-\alpha$. Thus it is sufficient to show that $H_n(x)$ has roots of the form $a_k i$ with distinct positive real numbers a_k $(k = 1,\dots,(n-1)/2)$. For arbitrary positive real a, we have

$$n!H_n(ai) = |ai+1|\dots|ai+n|(\cos(\alpha_1+\dots+\alpha_n)+i\sin(\alpha_1+\dots+\alpha_n))$$
$$-|ai-1|\dots|ai-n|(\cos(n\pi-\alpha_1-\dots-\alpha_n)+i\sin(n\pi-\alpha_1+\dots-\alpha_n))$$
$$= 2|ai+1|\dots|ai+n|\cos\left(\sum_{j=1}^{n}\arctan\left(\frac{a}{j}\right)\right).$$

Here we wrote α_j for the argument of $ai+j$, and used that $\alpha_j = \arctan(a/j)$ $(j = 1,\dots,n)$. Put

$$s(a) = \sum_{j=1}^{n}\arctan\left(\frac{a}{j}\right).$$

Observe that $s(a)$ is strictly monotone increasing in a, and

$$0 < s(a) < n\arctan(a) < \frac{\pi}{2}$$

if $\arctan(a) < \pi/2n$, and

$$(n-1)\frac{\pi}{2} < n\arctan\left(\frac{a}{n}\right) < s(a)$$

if $(n-1)\pi/2n < \arctan(a/n)$. So by the continuity of $s(a)$, we get that there exist distinct positive real numbers a_k such that

$$s(a_k) = (2k-1)\pi/2 \quad (k = 1, \dots, (n-1)/2). \tag{3.9}$$

However, then we have $H_n(a_k i) = 0$ $(k = 1, \dots, (n-1)/2)$, and the statement follows in this case.

Assume now that n is even. Observe that then the coefficients of the even powers of $H_n(x)$ are zero. In particular, we easily see that $\deg(H_n) = n-1$ and 0 is a simple root of $H_n(x)$. Again, if α is a root of $H_n(x)$, so is $-\alpha$. Thus it is sufficient to show that $H_n(x)$ has roots of the form $a_k i$ with distinct positive real numbers a_k $(k = 1, \dots, (n-2)/2)$. Similarly as for n odd, for arbitrary positive real a, we have

$$n!H_n(ai) = 2i|ai+1|\dots|ai+n|\sin\left(\sum_{j=1}^{n}\arctan\left(\frac{a}{j}\right)\right).$$

Now we get that there exist distinct positive real numbers a_k such that $s(a_k) = k\pi$ $(k = 1, \dots, (n-2)/2)$. However, then we have $H_n(a_k i) = 0$ $(k = 1, \dots, (n-2)/2)$, and the statement follows also in this case. ☐

The characterization of the root structure of $H_n'(x)$ is much more complicated then for $F_n'(x)$ and $G_n'(x)$.

Lemma 3.3.8. *For all $n \geq 2$, all the roots of $H_n'(x)$ are simple.*

Proof. According to the parity of n we distinguish two cases again.

Assume first that n is odd. Then $H_n(x)$ can be written in the form

$$H_n(x) = u_{n-1}x^{n-1} + u_{n-3}x^{n-3} + \dots + u_2x^2 + u_0.$$

We know, that the roots of $H_n(x)$ are on the imaginary axis: $(n-1)/2$ roots are on its positive part and $(n-1)/2$ roots are on its negative part. We introduce the polynomials $H_n^*(x) := H_n(ix)$. Then we have

$$H_n^*(x) = (-1)^{\frac{n-1}{2}}u_{n-1}x^{n-1} + (-1)^{\frac{n-3}{2}}u_{n-3}x^{n-3} + \dots - u_2x^2 + u_0.$$

It is easy to check that $H_n^*(x) \in \mathbb{R}[x]$ and $H_n^*(a) = 0$ if and only if $H_n(ia) = 0$ $(a \in \mathbb{R})$. Since the roots of $H_n(x)$ have the shape $\pm a_k i$ $(k = 1, \dots, (n-1)/2)$ with $0 < a_1 < \dots < a_{(n-1)/2}$, the roots of $H_n^*(x)$ are $\pm a_k$ $(k = 1, \dots, (n-1)/2)$. Applying Rolle's theorem, we get that $(H_n^*)'(x)$ has a root in every interval $[-a_{j+1}, -a_j]$ and $[a_j, a_{j+1}]$ $(j = 1, \dots, (n-3)/2)$, so every root of $(H_n^*)'(x)$ is simple and real. Observe that

$$(H_n^*)'(x) = x\left((-1)^{\frac{n-1}{2}}(n-1)u_{n-1}x^{n-3} + \dots + 4u_4x^2 - 2u_2\right), \tag{3.10}$$

hence 0 is a root of $(H_n^*)'(x)$, and if b is a root of $(H_n^*)'(x)$, then so is $-b$. Thus the roots of $(H_n^*)'(x)$ are given by

$$b_0, \pm b_1, \dots, \pm b_{\frac{n-3}{2}}$$

with

$$0 = b_0 < b_1 < \dots < b_{\frac{n-3}{2}}$$

and

$$\begin{aligned} -a_{\frac{n-1}{2}} < -b_{\frac{n-3}{2}} < -a_{\frac{n-3}{2}} < \dots < -b_1 < -a_1 < b_0 < a_1 < \\ < b_1 < a_2 < \dots < a_{\frac{n-3}{2}} < b_{\frac{n-3}{2}} < a_{\frac{n-1}{2}}. \end{aligned} \tag{3.11}$$

Also, $(H_n')^*(b) = 0$ if and only if $H_n'(ib) = 0$. (Here * stands for the earlier transformation: in case of $g(x) \in \mathbb{C}[x]$, $g^*(x) = g(ix)$.) We show that $(H_n')^*(x) = (-i)(H_n^*)'(x)$. It easily follows, since

$$H_n'(x) = x\left((n-1)u_{n-1}x^{n-3} + (n-3)u_{n-3}x^{n-5} + \dots + 4u_4x^2 + 2u_2\right)$$

and thus

$$(H_n')^*(x) = ix\left((-1)^{\frac{n-3}{2}}(n-1)u_{n-1}x^{n-3} + \dots - 4u_4x^2 + 2u_2\right)$$

which by (3.10) gives our claim. Hence the roots of $H_n'(x)$ are given by

$$0 = b_0,\ \pm b_j i \quad \left(j = 1, \dots, \frac{n-3}{2}\right). \tag{3.12}$$

So the statement is true for n odd.

Assume next that n is even. Using the transformation $H_n^\times(x) := iH_n(ix)$ in place of $H_n^*(x)$, a very similar argument works as in case of n odd. Here

$$H_n^\times(x) = (-1)^{\frac{n}{2}}u_{n-1}x^{n-1} + (-1)^{\frac{n-2}{2}}u_{n-3}x^{n-3} + \dots + u_3x^3 - u_1x.$$

It is easy to check that $H_n^\times(x) \in \mathbb{R}[x]$ and $H_n^\times(a) = 0$ if and only if $iH_n(ia) = 0$ $(a \in \mathbb{R})$. Since the roots of $H_n(x)$ are $a_0 = 0$ and the others have the shape $\pm a_k i$ $(k = 1, \dots, (n-2)/2)$ with $0 < a_1 < \dots < a_{(n-2)/2}$, the roots of $H_n^\times(x)$ are $0, \pm a_k$ $(k = 1, \dots, (n-2)/2)$. Applying Rolle's theorem, we get that $(H_n^\times)'(x)$ has a root in every interval $[-a_{j+1}, -a_j]$ and $[a_j, a_{j+1}]$ $(j = 0, \dots, (n-4)/2)$, so every root of $(H_n^\times)'(x)$ is simple and real. Observe that

$$(H_n^\times)'(x) = (-1)^{\frac{n}{2}}(n-1)u_{n-1}x^{n-3} + \dots + 3u_3x^2 - u_1, \tag{3.13}$$

hence if b is a root of $(H_n^\times)'(x)$, then so is $-b$. Thus the roots of $(H_n^\times)'(x)$ are given by

$$\pm b_1, \dots, \pm b_{\frac{n-1}{2}}$$

with

$$0 < b_1 < \dots < b_{\frac{n-1}{2}}$$

and

$$\begin{aligned} -a_{\frac{n-1}{2}} < -b_{\frac{n-1}{2}} < -a_{\frac{n-3}{2}} < \dots < -a_1 < -b_1 < a_0 < b_1 < \\ < a_1 < b_2 < \dots < a_{\frac{n-3}{2}} < b_{\frac{n-3}{2}} < a_{\frac{n-1}{2}}. \end{aligned} \tag{3.14}$$

We show that $(H_n')^\times(x) = i(H_n^\times)'(x)$. (Here $^\times$ stands for the earlier transformation: in case of $g(x) \in \mathbb{C}[x]$, $g^\times(x) = ig(ix)$.) It easily follows, since

$$H_n'(x) = (n-1)u_{n-1}x^{n-2} + (n-3)u_{n-3}x^{n-4} + \dots + 3u_3x^2 + u_1$$

and thus

$$(H_n')^\times(x) = i\left(i^{n-2}(n-1)u_{n-1}x^{n-2} + \dots - 3u_3x^2 + u_1\right)$$

which by (3.13) gives our claim. Hence the roots of $H_n'(x)$ are given by

$$\pm b_j i \quad \left(j = 1, \dots, \frac{n-1}{2}\right). \tag{3.15}$$

So the statement is also true for n even. □

Now we examine the root structures of the shifts of $H_n(x)$.

Corollary 3.3.3. *For any $n \geq 2$ and for all $r \in \mathbb{C}$, the multiplicities of the roots of $H_n(x) + r$ are at most two.*

Proof. The statement is an immediate consequence of Lemma 3.3.8. □

To prove the corresponding part of Theorem 3.2.3 we need one more lemma, similar to Lemmas 3.3.3 and 3.3.6.

Lemma 3.3.9. *Let $n \geq 2$. Then* $\max_{\lambda \in \mathbb{C}} \deg(\gcd(H_n(x) - \lambda, H_n'(x))) \leq 2$.

Proof. We split the proof into two parts, according to the parity of n again.

If n is odd then recalling (3.12) from the proof of Lemma 3.3.8, we know that the roots of $H_n'(x)$ can be written in the form

$$b_0, \ \pm b_k i \quad (k = 1, \dots, (n-3)/2)$$

where $0 = b_0 < b_1 < \ldots < b_{(n-3)/2}$ are real numbers. Also, by (3.11) here

$$0 = b_0 < a_1 < b_1 < a_2 < b_2 < \ldots < a_{\frac{n-3}{2}} < b_{\frac{n-3}{2}} < a_{\frac{n-1}{2}}$$

holds, where $\pm a_k i$ $(k = 1, \ldots, (n-1)/2)$ are the roots of $H_n(x)$. Furthermore, for all

$$a_{k-1} \leq t \leq a_k \quad \left(k = 2, \ldots, \frac{n-1}{2}\right)$$

we have

$$|H_n(ti)| \leq |H_n(b_{k-1}i)|.$$

Recall that by (3.9)

$$\sum_{j=1}^{n} \arctan\left(\frac{a_k}{j}\right) = (2k-1)\frac{\pi}{2} \quad \left(k = 1, \ldots, \frac{n-1}{2}\right)$$

also holds. Now, let $\hat{b}_k \in [a_k, a_{k+1}]$ $(k = 1, \ldots, (n-3)/2)$ be that unique real number for which

$$\sum_{j=1}^{n} \arctan\left(\frac{\hat{b}_k}{j}\right) = k\pi.$$

With this notation, since

$$\prod_{j=1}^{n} |\hat{b}_k i + j| > \prod_{j=1}^{n} |b_{k-1} i + j| \quad \left(k = 1, \ldots, \frac{n-3}{2}\right)$$

is obviously true, we obtain

$$|H_n(b_{k-1}i)| < |H_n(\hat{b}_k i)| \leq |H_n(b_k i)|.$$

It can be similarly proved (in fact, it also follows by symmetry) that

$$|H_n(-b_{k-1}i)| < |H_n(-b_k i)| \quad \left(k = 1, \ldots, \frac{n-3}{2}\right).$$

This implies that H_n' cannot have three different roots $\beta_1, \beta_2, \beta_3$ with

$$H_n'(\beta_1) = H_n'(\beta_2) = H_n'(\beta_3).$$

As the roots of H_n' are simple, we get that for any $\lambda \in \mathbb{C}$

$$\deg(\gcd(H_n'(x), H_n(x) - \lambda)) \leq 2,$$

and the statement is proved for n odd.

In case of n even our claim follows by a rather similar argument. If n is even then recalling (3.15) from the proof of Lemma 3.3.8, we know that the roots of $H_n'(x)$ can be written in the form

$$\pm b_k i \quad (k = 1, \ldots, (n-2)/2)$$

where $0 < b_1 < \ldots < b_{(n-2)/2}$ are real numbers. Also, by (3.14) here

$$0 = a_0 < b_1 < a_1 < b_2 < a_2 < \ldots < a_{\frac{n-4}{2}} < b_{\frac{n-2}{2}} < a_{\frac{n-2}{2}}$$

holds, where $a_0 = 0$, $\pm a_k i$ $(k = 1, \ldots, (n-2)/2)$ are the roots of $H_n(x)$. Furthermore, for all

$$a_{k-1} \le t \le a_k \qquad \left(k = 1, \ldots, \frac{n-2}{2}\right)$$

we have

$$|H_n(ti)| \le |H_n(b_k i)|.$$

Recall that from the proof of Lemma 3.3.7 when n is even that

$$\sum_{j=1}^{n} \arctan\left(\frac{a_k}{j}\right) = k\pi \qquad \left(k = 0, \ldots, \frac{n-2}{2}\right).$$

Now, let $\hat{b}_k \in [a_s, a_{s+1}]$ $(s = 1, \ldots, (n-4)/2)$ be that uniqe real number for which

$$\sum_{j=1}^{n} \arctan\left(\frac{\hat{b}_k}{j}\right) = (2k-1)\frac{\pi}{2}$$

holds. With this notation, since

$$\prod_{j=1}^{n} |\hat{b}_k i + j| > \prod_{j=1}^{n} |b_{k-1} i + j| \qquad \left(k = 2, \ldots, \frac{n-2}{2}\right)$$

is obviously true, we get that

$$|H_n(b_{k-1}i)| < |H_n(\hat{b}_k i)| \le |H_n(b_k i)|$$

holds. It can be similarly proved that

$$|H_n(-b_{k-1}i)| < |H_n(-b_k i)| \qquad \left(k = 2, \ldots, \frac{n-2}{2}\right).$$

In this case we also get that the degree of the greatest common divisor of $H_n'(x)$ and $H_n(x) - \lambda$ is at most two.

□

3.3.4 The decomposition properties of $F_n(x)$, $G_n(x)$, $H_n(x)$

In this subsection we prove Theorem 3.2.3.

Proof of Theorem 3.2.3. Let the polynomial $W(x)$ be one of $F_n(x)$, $G_n(x)$, $H_n(x)$ $(n \geq 2)$ and suppose that it is decomposable. Then $W(x)$ is of the shape $W(x) = T_1(T_2(x))$ with some $T_1, T_2 \in \mathbb{Q}[x]$, $\deg(T_1), \deg(T_2) > 1$. It is well-known (see e.g. the proof of Theorem 4.3 in [11]) that we have

$$\deg(T_2) \leq \max_{\lambda \in \mathbb{C}} \deg(\gcd(W(x) - \lambda, W'(x))).$$

Thus based on Lemmas 3.3.3, 3.3.6 and 3.3.9 we obtain $\deg(T_2) \leq 2$. This immediately shows that $n-1$ (the common degree of F_n, G_n, H_n) must be even, or in other words, that our polynomials are indecomposable for n even.

So assume that n is odd. Then by direct checking we get

$$\begin{aligned} F_n(x) &= (x+1)^n - (x-1)^n = \\ &= 2\binom{n}{1}x^{n-1} + 2\binom{n}{3}x^{n-3} + \cdots + 2\binom{n}{n-2}x^2 + 2 = \varphi_1(x^2) \end{aligned}$$

with

$$\varphi_1(t) = 2\binom{n}{1}t^{\frac{n-1}{2}} + 2\binom{n}{3}t^{\frac{n-3}{2}} + \cdots + 2\binom{n}{n-2}t + 2,$$

$$\begin{aligned} G_n(x) &= (x+1)^{n-1} + x^{n-1} = \\ &= \left(\left(x+\frac{1}{2}\right)+\frac{1}{2}\right)^{n-1} + \left(\left(x+\frac{1}{2}\right)-\frac{1}{2}\right)^{n-1} = \\ &= 2\left(x+\frac{1}{2}\right)^{n-1} + \frac{1}{2}\binom{n-1}{2}\left(x+\frac{1}{2}\right)^{n-3} + \cdots \\ &\quad \cdots + \frac{1}{2^{n-4}}\binom{n-1}{n-3}\left(x+\frac{1}{2}\right)^2 + \frac{1}{2^{n-2}} = \varphi_2\left(\left(x+\frac{1}{2}\right)^2\right), \end{aligned}$$

with

$$\varphi_2(t) = 2t^{\frac{n-1}{2}} + \frac{1}{2}\binom{n-1}{2}t^{\frac{n-3}{2}} + \cdots + \frac{1}{2^{n-4}}\binom{n-1}{n-3}t + \frac{1}{2^{n-2}}$$

and

$$\begin{aligned} H_n(x) =& \frac{1}{n!}((x+1)\cdots(x+n) - (x-1)\cdots(x-n)) \\ =& \frac{2}{n!}(s_1x^{n-1} + s_3x^{n-3} + \cdots + s_n), \end{aligned}$$

where

$$s_j = \sum_{\substack{A \subseteq \{1,\ldots,n\} \\ |A|=j}} \prod_{a \in A} a \quad (j = 1, \ldots, n),$$

so $H_n(x) = \varphi_3(x^2)$ with

$$\varphi_3(t) = \frac{2}{n!}(s_1 t^{\frac{n-1}{2}} + s_3 t^{\frac{n-3}{2}} + \cdots + s_{n-2}t + s_n).$$

We only need to show that if n is odd then all decompositions of $F_n(x)$, $G_n(x)$ and $H_n(x)$ are equivalent to the above ones, respectively. We only check it for $F_n(x)$, the two other cases can be handled similarly. Since in any decomposition we must have $\deg(T_2) = 2$, we can write $T_2(x) = \alpha(x-\beta)^2 + \gamma$ with some $\alpha, \beta, \gamma \in \mathbb{C}$. Then the decomposition

$$F_n(x) = T_1(\alpha(x-\beta)^2 + \gamma)$$

is equivalent to a decomposition of the form $F_n(x) = P((x-\beta)^2)$ with some $P(x) \in \mathbb{C}[x]$. Thus the roots of $F_n(x)$ are symmetric about β. So necessarily $\beta = 0$, which proves our statement. □

3.4 Proofs of our effective results

In this section we prove our effective results. For this, we will use Lemma 2.1 and Lemma 2.2 (which will be also used in the proofs of the ineffective theorems).

Remark 3.4.1. Note that if $\ell \geq 3$ and $W(x)$ has at least two simple roots, or if $\ell = 2$ and $W(x)$ has at least three simple roots, then the conditions of Lemma 2.2 are satisfied.

Proof of Theorem 3.2.2. Recall that for any $B \in \mathbb{Q}$, we have $\deg(W(x) - B) = n - 1$. If $n \geq 4$ then by Lemmas 3.3.2, 3.3.5 and Corollary 3.3.3 the polynomial $W(x) - B$ has at least two distinct roots. Hence by Lemma 2.1 part i) of the theorem follows.

To prove part ii) of the statement, we examine the cases $W(x) = F_n(x), G_n(x), H_n(x)$ separately. We shall always assume that $n \geq 8$. Further, note that by part i), ℓ is bounded in terms of A, d, H, unless $|y| \leq 1$ - but in that case the statement is obvious.

Lemmas 3.3.2 and 3.3.5 yield that the polynomials $F_n(x) - B$ and $G_n(x) - B$ have at least three simple roots. Thus Lemma 2.2 immediately shows that the statement is true for $W(x) = F_n(x), G_n(x)$.

So finally, let $W(x) = H_n(x)$. If $\ell \geq 3$ then Corollary 3.3.3 gives that $H_n(x) - B$ has at least three distinct roots, and the multiplicity of these roots cannot be larger than two. Thus our statement follows from Lemma 2.2 also in this case. Let now $\ell = 2$. Clearly, our statement follows from Lemma 2.2 also in this case, unless we have

$$H_n(x) - B = u(x)(v(x))^2$$

with some $u(x), v(x) \in \mathbb{Q}[x]$ with $\deg(u) \leq 2$. However, if $H_n(x) - B$ is of the above shape, then we have

$$(H_n(x) - B)' = v(x)\left(u'(x)v(x) + 2u(x)v'(x)\right).$$

Hence the roots of $v(x)$ are also roots of $H'_n(x)$. However, these are roots of the polynomial $H_n(x) - B$ as well. According to Lemma 3.3.9, we know that the degree of the greatest common divisor of $H'_n(x)$ and $H_n(x) - B$ is at most two. Hence $\deg(v) \le 2$, so $n \le 7$. This contradicts our assumption $n \ge 8$, and our statement follows. □

3.5 Proofs of our ineffective results

Now we give the proof of Theorem 3.2.1. We mention that the polynomials F_n and G_n ($n \ge 1$) form so-called Appell families. Thus in the proof we could use some results of Bazsó and Pink [5]. However, as we should handle certain cases separately anyhow, to keep the presentation coherent, we proceed differently.

Proof of Theorem 3.2.1. Suppose that (3.3) has infinitely many solutions in integers x, y. Then according to Lemma 2.3 we have $W = \varphi \circ F \circ \lambda$ and $g = \varphi \circ G \circ \kappa$, where $\varphi, \lambda, \kappa \in \mathbb{Q}[x], \deg(\lambda) = \deg(\kappa) = 1$ and F, G form a standard pair. Thus using Theorem 3.2.3 we obtain that only one of the following cases is possible:

- $\deg(\varphi) = n - 1$ and $\deg(F) = 1$,
- $n - 1$ is even, $\deg(\varphi) = (n-1)/2$, $\deg(F) = 2$, and φ is one of the polynomials φ_1, φ_2, φ_3,
- $\deg(\varphi) = 1$ and $\deg(F) = n - 1$.

In the first case we get that $\varphi(x) = W(\tau(x))$, where $\tau(x) \in \mathbb{Q}[x]$ is a linear polynomial. Thus we have $g(y) = W(P(y))$, where $P(y) \in \mathbb{Q}[y]$, and our statement follows.

In the second case we have one of

$$W(x) = \varphi_1(x^2),\ \varphi_2\left(\left(x + \frac{1}{2}\right)^2\right),\ \varphi_3(x^2).$$

Hence now $g(y) = \hat{W}(Q(y))$ holds, where $\hat{W}$ is one of φ_1, φ_2, φ_3. Furthermore, Lemma 2.3 implies that the equation

$$x^2 = Q(y), \quad \left(x + \frac{1}{2}\right)^2 = Q(y), \quad x^2 = Q(y),$$

respectively, must have infinitely many solutions in rational numbers with bounded denominators. So by Lemma 2.2 we deduce that $Q(y)$ can have at most two roots with odd multiplicity. This proves our claim also in this case.

Finally, assume that we are in the third case, that is $\deg(\varphi) = 1$ and $\deg(F) = n - 1$. Then we can write

$$W(x) = AF(ax + b) + B$$

with some $A, B, a, b \in \mathbb{Q}$, $Aa \neq 0$, were F is a member of one of the five standard pairs. We shall check all the five standard pairs in turn. Recall that by our assumption we have $n \geq 6$. Further, one can easily see that the theorem for $\deg(g) = 2$ follows from the case $\ell = 2$ of Theorem 3.2.2. Hence we may also assume that $\deg(g) \geq 3$.

We start with the case where $F(x)$ is from a standard pair of the fifth kind. It can be easily seen that then $W'(x)$ has multiple roots. However, this is not possible because of Corollaries 3.3.1, 3.3.2 and Lemma 3.3.8. So this possibility cannot hold.

Assume next that $F(x)$ is from a standard pair of the first kind. If

$$W(x) = A \cdot (ax + b)^q + B,$$

then

$$W'(x) = A \cdot aq(ax + b)^{q-1}.$$

However, by Corollaries 3.3.1, 3.3.2 and Lemma 3.3.8 we know that the roots of $W'(x)$ are simple. Thus we get $q \leq 2$, contradicting $n \geq 6$. If W is of the form

$$W(x) = A\alpha(ax + b)^r v(ax + b)^q + B$$

where $0 \leq r < q$, $(r, q) = 1$, $r + \deg(v) > 0$, then

$$W'(x) = A\alpha a(ax + b)^{r-1} v(ax + b)^{q-1}(rv(ax + b) + q(ax + b)v'(ax + b)).$$

This similarly as above yields that $r \leq 2$, and either $q \leq 2$ or $\deg(v) = 0$. If $\deg(v) = 0$ then we get back to the previous case, which has already been excluded. Thus we may assume that $\deg(v) > 0$, and by $r < q$ and $\gcd(r, q) = 1$ also that $(r, q) = (0, 1), (1, 2)$. Now as

$$g = \varphi \circ G \circ \kappa$$

where $\deg(\varphi) = \deg(\kappa) = 1$ and $\deg(G) = q$, we get $\deg(g) \leq 2$, which is excluded. Thus our theorem follows also in this case.

Consider now the case where $F(x)$ is a member of a standard pair of the second kind. Now we easily get that either $\deg(W) = 2$, contradicting our assumption $n \geq 6$, or $\deg(g) = 2$, contradicting the condition $\deg(g) \geq 3$.

Finally, assume that $F(x)$ is from a standard pair of the third or fourth kind. We give detailed arguments only for the case $W(x) = F_n(x)$, since $W(x) = G_n(x), H_n(x)$ can be handled similarly. So let $W(x) = F_n(x)$. Then

$$F_n(x) = AD_{n-1}(ax + b) + B,$$

where $D_{n-1}(x)$ is a Dickson-polynomial, with some parameter δ. So

$$2\binom{n}{1}x^{n-1} + 2\binom{n}{3}x^{n-3} + 2\binom{n}{5}x^{n-5} + 2\binom{n}{7}x^{n-7} + \dots$$
$$= Ad_0(ax+b)^{n-1} + Ad_1(ax+b)^{n-3} + Ad_2(ax+b)^{n-5} + \dots$$

with

$$d_i = \frac{n-1}{n-1-i}\binom{n-1-i}{i}(-\delta)^i \quad (i \geq 0).$$

Comparing the leading coefficients, we get that $Aa^{n-1} = 2n$, and from the coefficients of x^{n-2} we immediately see that $b = 0$. Now checking the coefficients of x^{n-3}, we obtain

$$-\frac{\delta}{a^2} = \frac{n-2}{6}.$$

Then the comparison of the coefficients of x^{n-5} yields a contradiction, and our theorem follows in this case. As we mentioned, in the case of the other two polynomial families a similar argument applies, and thus the proof of our theorem is complete. □

Chapter 4

Extrema of polynomials with real roots and Diophantine equations

4.1 Introduction

There are many results in the literature concerning polynomial values and (shifted) power values of polynomials with consecutive integer roots, or more generally, with roots forming an arithmetic progression. We only mention a classical result of Erdős and Selfridge [20] saying that the product of consecutive integers can never be a perfect power, a theorem of Győry, Hajdu and Pintér [27] giving an alike result concerning arithmetic progressions up to 34 terms, and a paper by Kulkarni and Sury [42] providing finiteness results for the polynomial values of products of consecutive integers. It is an interesting question that how far one can 'disturb' the structure of the roots such that the finiteness results still remain valid. Also there are many results into this direction, with adding or removing one or more terms (roots). Here we only recall results of Saradha and Shorey [53, 54] concerning power values of products of consecutive integers with one term missing, Hajdu and Papp [35] and Hajdu, Papp and Tijdeman [36] about polynomial values and shifted power values of products of consecutive terms of arithmetic progressions with one and with several missing terms, respectively, and Hajdu and Varga [38] with one term added. We suggest the interested reader to consult the references of the mentioned papers, as well.

In this chapter we study a case where (part of) the symmetric root structure is preserved, however, having increasing (possibly large) gaps between the roots. We prove that the finiteness of the solutions can also be guaranteed under these generalized circumstances. Our results can be considered to be generalizations of the corresponding finiteness results, e.g. from [42]. (This will be explained in Remark 4.2.1.) In our proofs we combine

Baker's method and the Bilu-Tichy theorem with a new result guaranteeing an increasing property for the extremal values of polynomials, with distinct real roots satisfying certain symmetry and increasing gap properties. The structure of the chapter is the following. In the next section we provide our main results. Then we give their proofs (together with the corresponding lemmas and auxiliary results) in separate sections. The reason of this is that we need different tools in the proofs of our results, and we would like to present the necessary tools close to their actual use (as much as possible). We note that we give the proofs of our results not in the order of stating the theorems, but in the 'logical' order (which in fact is just the opposite order).

4.2 Main results

We say that a finite sequence $b_1, \dots, b_k$ in $\mathbb{R}$ with $b_1 < \dots < b_k$ is symmetric, if there exists a $c \in \mathbb{R}$ such that $b_i + b_{k+1-i} = 2c$ for $i = 1, 2, \dots, k$. We say that c is the center of symmetry for the sequence. A symmetric sequence is called centrally convex, if writing $\ell = \left\lceil \frac{k}{2} \right\rceil$, $b_\ell, b_{\ell+1}, \dots, b_k$ form a convex sequence, that is

$$b_i - b_{i-1} \leq b_{i+1} - b_i \quad (\ell < i < k) \tag{4.1}$$

holds. For example, $-2, 0, 1, 2, 4$ is a centrally convex symmetric sequence: the center of symmetry is $c = 1$, and we have

$$2 - 1 \leq 4 - 2.$$

To see an example of a centrally convex symmetric sequence with an even number of elements, consider $-10, -2, 1, 4, 6, 9, 12, 20$: now the center of symmetry is $c = 5$ and we have

$$6 - 4 \leq 9 - 6 \leq 12 - 9 \leq 20 - 12.$$

Remark 4.2.1. Our results concern polynomials with simple real roots forming a centrally convex symmetric sequence. We find it important to emphasize a few points here. In the first place, any arithmetic progression $h_1, \dots, h_N$ forms a centrally convex symmetric sequence. Indeed, the sequence is symmetric to the point $c := (h_1 + h_N)/2$ (i.e. $h_i + h_{N+1-i} = 2c$ for all $i = 1, \dots, N$), and since the gaps between the terms after the middle point are non-decreasing (certainly, the gap is constant), the centrally convex property (4.1) is also satisfied. So our Theorem 4.2.1 below provides an extension of the main result of [42]. However, in fact our results are much more general than that. For example, as one can easily check, the numbers

$$-k^2, -(k-1)^2, \dots, -4, -1, 0, 1, 4, \dots, (k-1)^2, k^2$$

also form a centrally convex symmetric sequence, so our results provide finiteness conditions for the equations appearing in Theorems 4.2.1 and 4.2.2 involving the corresponding polynomial

$$f(x) = x\prod_{j=1}^{k}(x-j^2)(x+j^2).$$

First we provide a general, ineffective theorem for the common integer values of a polynomial $f(x) \in \mathbb{Q}[x]$ having distinct roots forming a centrally convex symmetric sequence with any polynomial $g(x) \in \mathbb{Q}[x]$.

Theorem 4.2.1 (L. Hajdu, O. Herendi [33])**.** *Let $f(x) \in \mathbb{Q}[x]$ have distinct real roots forming a centrally convex symmetric sequence,* $\deg(f) > 6$ *and let $g(x) \in \mathbb{Q}[x]$ with* $\deg(g) \geq 2$. *If the equation*

$$f(x) = g(y) \tag{4.2}$$

has infinitely many solutions in integers x, y then either

$$g(y) = f(P(y))$$

with some $P(y) \in \mathbb{Q}[y]$ of degree ≥ 1, or $\deg(f) = 2k$ *is even and*

$$g(y) = \hat{f}(Q(y))$$

with some $Q(y) \in \mathbb{Q}[y]$ having at most two roots of odd multiplicity, where

$$\hat{f}(x) = b_0(x-(b_1-c)^2)\cdots(x-(b_k-c)^2).$$

Here b_0 is the leading coefficient of f, b_i $(i = 1, \ldots, 2k)$ are the roots of f in increasing order, and c is the center of symmetry for them.

Remark 4.2.2. It is easy to see that $\hat{f}(x) \in \mathbb{Q}[x]$. We shall show this in the proof of the theorem.

If we have $g(x) = Ax^m + B$ with some fixed $A, B \in \mathbb{Q}$ $(A \neq 0)$ and m is an integer variable with $m \geq 2$, we are able to provide an effective upper bound for the absolute values of the integer solutions x, y and also of m in equation (4.2). By the height of a polynomial in $\mathbb{Q}[x]$ we mean the maximum of the absolute values of the numerators and denominators of its coefficients.

Theorem 4.2.2 (L. Hajdu, O. Herendi [33])**.** *Let $f(x) \in \mathbb{Q}[x]$ have distinct real roots forming a centrally convex symmetric sequence and suppose that* $\deg(f) > 6$. *Let A, B be given rationals with $A \neq 0$, and consider the equation*

$$f(x) = Ay^m + B \tag{4.3}$$

in integers x, y, m with $m \geq 2$, with the convention that $m \leq 3$ if $|y| \leq 1$. Then there exists an effectively computable constant $C_5(A, B, d, H)$, depending only on A, B and the degree d and height H of f such that

$$\max(|x|, |y|, m) \leq C_5(A, B, d, H)$$

for every integer solution x, y, m of (4.3).

Remark 4.2.3. The assumptions of Theorems 4.2.1 and 4.2.2 are necessary. Clearly, we need to exclude the case $\deg(g) = 1$ in Theorem 4.2.1. To see an example with $\deg(f) = 6$ such that both (4.2) and (4.3) have infinitely many solutions, put

$$f(x) = (x + 8)(x + 4)(x + 1)(x - 1)(x - 4)(x - 8)$$

and

$$g(y) = Ay^m + B = 29y^2 + 3136.$$

(Observe that the roots $-8, -4, -1, 1, 4, 8$ form a centrally convex symmetric sequence.) Then both (4.2) and (4.3) can be written as

$$(x^2 - 65)(x^2 - 8)^2 = 29y^2.$$

Since the generalized Pell equation

$$u^2 - 29v^2 = 65$$

has infinitely many integer solutions u, v (the 'smallest' one is given by $(u, v) = (23, 4)$), (4.2) and (4.3) admit infinitely many solutions $x, y \in \mathbb{Z}$. However, we mention that the condition $\deg(f) > 6$ is necessary only for $m = 2$. When $m \geq 3$, in fact the assumption $\deg(f) > 2$ is sufficient. This can be easily seen from the proof of Theorem 4.2.2.

We also note that requiring only distinct real roots for f is certainly not necessary: see e.g. the identities involving Dickson polynomials in [12]. That is, some further requirement for the roots is necessary.

In the proof of Theorem 4.2.1 the following result plays an important role. It gives a complete description of the decompositions of polynomials over $\mathbb{Q}$ with simple real roots forming a centrally convex symmetric sequence.

Theorem 4.2.3 (L. Hajdu, O. Herendi [33])**.** *Let $f(x) \in \mathbb{Q}[x]$ have distinct real roots forming a centrally convex symmetric sequence. If $\deg(f)$ is odd or $\deg(f) = 2$ then f is indecomposable over $\mathbb{Q}$. If $\deg(f) \geq 4$ is even then f is decomposable over $\mathbb{Q}$, and all the decompositions of f over $\mathbb{Q}$ are equivalent to*

$$f(x) = b_0((x - c)^2 - (b_1 - c)^2) \dots ((x - c)^2 - (b_k - c)^2),$$

where b_0 is the leading coefficient of f, $b_1, \dots, b_{2k}$ are the roots of f in increasing order, and c is their center of symmetry.

Remark 4.2.4. Using the notation introduced in Theorem 4.2.1, the above decomposition can also be written as

$$f(x) = \hat{f}((x - c)^2).$$

So (for $\deg(f) \geq 4$ even) this decomposition is over $\mathbb{Q}$, indeed.

Finally, we give a theorem providing information about the extrema of polynomials having simple real roots forming a centrally convex symmetric sequence. As we shall see, this result will play a key role in the proofs of our theorems given above - however, we find it of possible independent interest.

Theorem 4.2.4 (L. Hajdu, O. Herendi [33])**.** *Let $f(x) \in \mathbb{R}[x]$ have distinct real roots, which form a centrally convex symmetric sequence. Then the extremal values of f are strictly increasing in absolute value moving away from the center of symmetry of the roots.*

Remark 4.2.5. In the statement neither the centrally convex nor the symmetric properties can be dropped. We illustrate it with two examples.

Take first

$$f(x) = (x+3)(x+2)(x+1)(x-1)(x-2)(x-3).$$

We see that the roots form a symmetric sequence (with center of symmetry being 0), and for the gaps only one 'centrally convex inequality' is violated (namely, $1-(-1) \leq 2-1$ does not hold). However, a simple calculation with Maple shows that the roots of $f'(x)$ are given by

$$-\sqrt{7}, \quad -\sqrt{\frac{7}{3}}, \quad 0, \quad \sqrt{\frac{7}{3}}, \quad \sqrt{7},$$

and the extremal values of $f(x)$ are

$$-36, \quad \frac{400}{27}, \quad -36, \quad \frac{400}{27}, \quad -36$$

at these values, respectively. So we see that the strictly monotone increasing property of the absolute values of the extremal values (moving away from the center of symmetry) does not hold in this case.

Let now

$$f(x) = (x+9)(x+6)(x+3)x(x-1)(x-2)(x-3).$$

We see that the roots satisfy an 'increasing gap property' starting from the middle root (which is 0), into both the positive and the negative direction. (Since we dropped symmetry here, certainly we cannot use a 'center of symmetry'.) However, a simple calculation with Maple shows that the extremal value of f between the roots 0 and 1 is larger in absolute value than that between the roots 1 and 2. (Since the data are non-rational and cannot be expressed easily, we suppress the details.) So, the strictly increasing extremal value property does not hold in this case either.

4.3 Proof of Theorem 4.2.4

As we shall see, Theorem 4.2.4 is a simple consequence of the following two propositions. They are rather similar, but because of technical reasons it is worth to formulate them separately.

Proposition 4.3.1. *Let* $0 = a_0 < a_1 < \cdots < a_n$ *be real numbers with*

$$a_i - a_{i-1} \leq a_{i+1} - a_i \quad (1 \leq i \leq n-1), \tag{4.4}$$

and let

$$f_1(x) = x \prod_{i=1}^{n} (x - a_i)(x + a_i).$$

Let α_i *be the extremum of* f_1 *between* a_i *and* a_{i+1} *for* $i = 0, \ldots, n-1$. *Then we have*

$$|f_1(\alpha_0)| < |f_1(\alpha_1)| < \cdots < |f_1(\alpha_{n-1})|.$$

Proposition 4.3.2. *Let* $0 < a_1 < \cdots < a_n$ *be real numbers with*

$$3a_1 \leq a_2 \quad \textit{and} \quad a_i - a_{i-1} \leq a_{i+1} - a_i \quad (2 \leq i \leq n-1), \tag{4.5}$$

and let

$$f_2(x) = \prod_{i=1}^{n} (x - a_i)(x + a_i).$$

Let α_i *be the extremum of* f_2 *between* a_i *and* a_{i+1} *for* $i = 1, \ldots, n-1$. *Then we have*

$$|f_2(0)| < |f_2(\alpha_1)| < \cdots < |f_2(\alpha_{n-1})|.$$

Remark 4.3.1. Note that by Rolle's theorem the extrema of f_1 and f_2 are situated in the way indicated in Propositons 4.3.1 and 4.3.2, respectively - that is, they are between the roots.

To prove Propositions 4.3.1 and 4.3.2 we shall need some lemmas. The first one concerns certain properties of the Γ function, defined by

$$\Gamma(z) = \frac{1}{z} \prod_{n=1}^{\infty} \frac{\left(1 + \frac{1}{n}\right)^z}{1 + \frac{z}{n}} \quad (z \in \mathbb{C} \setminus \mathbb{Z}_{\leq 0}),$$

where $\mathbb{Z}_{\leq 0}$ is the set of non-positive integers. Note that there are many other possibilities to define $\Gamma(z)$, the above form is called Euler's formula.

Lemma 4.3.1. *The following assertions hold.*

i) For any $z \in \mathbb{C} \setminus \mathbb{Z}_{\leq 0}$ *we have*

$$z\Gamma(z) = \Gamma(z+1).$$

ii) For any $z \in \mathbb{C} \setminus \mathbb{Z}$ we have

$$\Gamma(z)\Gamma(1-z) = \frac{\pi}{\sin \pi z}.$$

iii) For any $u_1, u_2, v_1, v_2 \in \mathbb{C} \setminus \mathbb{Z}_{\leq 0}$ with $u_1 + u_2 = v_1 + v_2$ we have

$$\prod_{k=0}^{\infty} \frac{(k+u_1)(k+u_2)}{(k+v_1)(k+v_2)} = \frac{\Gamma(v_1)\Gamma(v_2)}{\Gamma(u_1)\Gamma(u_2)}.$$

Proof. The assertions i), ii) and iii) can be found in Sections 12.12, 12.14 and 12.13 of [67], respectively. □

In the proof of Proposition 4.3.1 we shall need the following assertion.

Lemma 4.3.2. *Let $0 < a_1 < \cdots < a_n$ be real numbers with*

$$a_i - a_{i-1} \leq a_{i+1} - a_i \quad (2 \leq i \leq n-1).$$

Then for every i_1, i_2 with $1 \leq i_1 \leq i_2 \leq n$ we have

$$\frac{a_{i_2}}{a_{i_1}} \geq \frac{i_2}{i_1}.$$

Proof. We prove the statement by induction on i_2. For $i_2 = 1$ the assertion is obvious. Assume that the statement holds for some i_2 with $1 \leq i_2 < n$. Observe that using the assertion concerning the gaps between the a_i, we have

$$\frac{a_{i_2+1}}{a_{i_2}} = \frac{a_{i_2+1} - a_{i_2}}{a_{i_2}} + 1 \geq \frac{a_{i_2} - a_{i_2-1}}{a_{i_2}} + 1 = 2 - \frac{a_{i_2-1}}{a_{i_2}} \geq 2 - \frac{i_2 - 1}{i_2} = \frac{i_2 + 1}{i_2}.$$

Here, we also used the induction hypothesis. Now take any i_1 with $1 \leq i_1 < i_2$. Then using the above assertion and the induction hypothesis we have

$$\frac{a_{i_2+1}}{a_{i_1}} = \frac{a_{i_2+1}}{a_{i_2}} \cdot \frac{a_{i_2}}{a_{i_1}} \geq \frac{i_2+1}{i_2} \cdot \frac{i_2}{i_1} = \frac{i_2+1}{i_1}.$$

Hence, the lemma follows. □

In the proof of Proposition 4.3.2 we shall need the following variant of Lemma 4.3.2.

Lemma 4.3.3. *Let $0 < a_1 < \cdots < a_n$ be real numbers with*

$$3a_1 \leq a_2$$

and

$$a_i - a_{i-1} \leq a_{i+1} - a_i \quad (2 \leq i \leq n-1).$$

Then for every i_1, i_2 with $1 \leq i_1 \leq i_2 \leq n$ we have

$$\frac{a_{i_2}}{a_{i_1}} \geq \frac{2i_2 - 1}{2i_1 - 1}.$$

Proof. The proof is similar to that of Lemma 4.3.2. However, for the convenience of the reader we summarize the main steps, but we give less details.

We apply induction on i_2. For $i_2 = 1$ the statement is clear. Assume that the statement holds for some i_2 with $1 \leq i_2 < n$. Using the assumption on the gaps between the a_i and the induction hypothesis, we have

$$\frac{a_{i_2+1}}{a_{i_2}} \geq 2 - \frac{a_{i_2-1}}{a_{i_2}} \geq \frac{2i_2+1}{2i_2-1}.$$

Now for any i_1 with $1 \leq i_1 < i_2$ we obtain

$$\frac{a_{i_2+1}}{a_{i_1}} = \frac{a_{i_2+1}}{a_{i_2}} \cdot \frac{a_{i_2}}{a_{i_1}} \geq \frac{2i_2+1}{2i_1-1},$$

and the lemma follows. □

Now we give the proof of Proposition 4.3.1.

Proof of Proposition 4.3.1. Let i be fixed with $1 \leq i \leq n-1$. First we show that for any t with $0 < t < 1$ we have

$$f^*(t) := \left| \frac{f_1(a_i - t(a_i - a_{i-1}))}{f_1(a_i + t(a_i - a_{i-1}))} \right| < 1, \tag{4.6}$$

from which the assertion will easily follow. Note that by our assumption on the gaps between the a_j, we have

$$a_{i-1} < a_i - t(a_i - a_{i-1}) < a_i < a_i + t(a_i - a_{i-1}) < a_{i+1} \quad (0 < t < 1).$$

Putting

$$d = \frac{a_i - a_{i-1}}{a_i} \quad \text{and} \quad s_j = \frac{a_j}{a_i} \quad (1 \leq j \leq n)$$

we can write (4.6) as

$$f^*(t) = \left(\frac{1-td}{1+td} \cdot \frac{2-td}{2+td} \right) \times \prod_{j=1}^{i-1} \left(\frac{1-s_j-td}{1-s_j+td} \cdot \frac{1+s_j-td}{1+s_j+td} \right) \times$$
$$\times \prod_{j=i+1}^{n} \left(\frac{s_j-1+td}{s_j-1-td} \cdot \frac{s_j+1-td}{s_j+1+td} \right). \tag{4.7}$$

Here, the first block corresponds to the roots $a_0 = 0$ and $\pm a_i$ of f_1. Further, note that we have $1 - s_j > td > 0$ for $j = 1, \ldots, i-1$ and $0 < td < s_j - 1$ for $j = i+1, \ldots, n$. (That is why it is worth to split the product for $j \geq 0$, $j \neq i$ according as $j < i$ or $j > i$.) Now we deal with the second and third terms on the right hand side of (4.7) in turn. We start with the second term. First observe that

$$\frac{X-Y}{X+Y} \text{ is strictly monotone increasing in } X > 0, \text{ for any } Y > 0. \tag{4.8}$$

Further, in view of the gap property of the a_j we have

$$1 - s_j = \frac{a_i - a_j}{a_i} = \frac{(a_i - a_{i-1}) + \cdots + (a_{j+1} - a_j)}{a_i} \leq (i-j)d,$$

and by Lemma 4.3.2 we see that

$$s_j \leq \frac{j}{i}$$

for all j with $1 \leq j < i$. Combining the above assertions, we obtain

$$\prod_{j=1}^{i-1} \left(\frac{1 - s_j - td}{1 - s_j + td} \cdot \frac{1 + s_j - td}{1 + s_j + td} \right) \leq \prod_{j=1}^{i-1} \left(\frac{i - j - t}{i - j + t} \cdot \frac{j + i - itd}{j + i + itd} \right). \tag{4.9}$$

Now we estimate the third product in (4.7). For this, observe that

$$\frac{s_j - 1 + td}{s_j - 1 - td} \cdot \frac{s_j + 1 - td}{s_j + 1 + td} = \frac{s_j^2 - (1 - td)^2}{s_j^2 - (1 + td)^2}$$

and that the function

$$\frac{X^2 - (1 - td)^2}{X^2 - (1 + td)^2}$$

is strictly decreasing in X for $X > 1 + td$. Hence in view of the inequality

$$s_j = 1 + \frac{a_j - a_i}{a_i} = 1 + \frac{(a_j - a_{j-1}) + \cdots + (a_{i+1} - a_i)}{a_i} \geq 1 + (j-i)d$$

valid for any $j > i$ obtained by the gap property of the a_j, we get

$$\prod_{j=i+1}^{n} \left(\frac{s_j - 1 + td}{s_j - 1 - td} \cdot \frac{s_j + 1 - td}{s_j + 1 + td} \right) \leq \prod_{j=i+1}^{n} \left(\frac{j - i + t}{j - i - t} \cdot \frac{j - i + \frac{2}{d} - t}{j - i + \frac{2}{d} + t} \right). \tag{4.10}$$

On combining (4.7), (4.9) and (4.10), we obtain

$$f^*(t) \leq \left(\frac{1 - td}{1 + td} \cdot \frac{2 - td}{2 + td} \right) \times \prod_{j=1}^{i-1} \left(\frac{i - j - t}{i - j + t} \cdot \frac{j + i - itd}{j + i + itd} \right) \times$$
$$\times \prod_{j=i+1}^{n} \left(\frac{j - i + t}{j - i - t} \cdot \frac{j - i + \frac{2}{d} - t}{j - i + \frac{2}{d} + t} \right). \tag{4.11}$$

In view of (4.8),

$$\frac{j - i + \frac{2}{d} - t}{j - i + \frac{2}{d} + t}$$

is monotone increasing in $2/d$ - so it is monotone decreasing in d. On the other hand, using (the negative of) (4.8) again, we see that all the terms in the first and second terms on the right hand side of (4.11) (which depend on d) are strictly monotone decreasing in

d. Altogether, we obtain that the right hand side of (4.11) is monotone decreasing in d (for any fixed t). In view of

$$d = \frac{a_i - a_{i-1}}{a_i} = 1 - \frac{a_{i-1}}{a_i} \geq 1 - \frac{i-1}{i} = \frac{1}{i}$$

obtained by Lemma 4.3.2, substituting $d = 1/i$ in (4.11) gives

$$f^*(t) \leq -\frac{i-t}{i+t} \cdot \prod_{j=1}^{n} \left(\frac{j-i+t}{j-i-t} \cdot \frac{j+i-t}{j+i+t} \right).$$

(The negative sign comes from the factor $t/(-t)$ in case $j = i$.) Now using parts iii), i) and ii) of Lemma 4.3.1 (in this order), in view of that

$$\frac{j-i+t}{j-i-t} \cdot \frac{j+i-t}{j+i+t} > 1 \quad \text{for } j > n$$

we obtain

$$\begin{aligned} f^*(t) < -\frac{i-t}{i+t} \cdot \prod_{j=1}^{\infty} \left(\frac{j-i+t}{j-i-t} \cdot \frac{j+i-t}{j+i+t} \right) = \\ = -\frac{i-t}{i+t} \cdot \frac{\Gamma(1-i-t)\Gamma(1+i+t)}{\Gamma(1-i+t)\Gamma(1+i-t)} = -\frac{\Gamma(1-i-t)\Gamma(i+t)}{\Gamma(1-i+t)\Gamma(i-t)} = \\ = -\frac{\sin \pi(i-t)}{\sin \pi(i+t)} = \frac{\sin \pi(t-i)}{\sin \pi(t+i)} = 1. \end{aligned}$$

Thus

$$f^*(t) < 1 \quad \text{for all } t \in (0,1),$$

and our claim (4.6) follows.

Put now

$$t_0 := \frac{a_i - \alpha_{i-1}}{a_i - a_{i-1}}.$$

Observe that $0 < t_0 < 1$ and that

$$\alpha_{i-1} = a_i - t_0(a_i - a_{i-1}) < a_i < a_i + t_0(a_i - a_{i-1}) < a_{i+1}.$$

Thus (4.6) implies

$$|f_1(\alpha_i)| = |f_1(a_i - t_0(a_i - a_{i-1}))| < |f_1(a_i + t_0(a_i - a_{i-1}))| \leq |f_1(\alpha_{i+1})|,$$

and the proposition follows. □

Now we give the proof of Proposition 4.3.2. It is rather similar to that of Proposition 4.3.1, however, with considerable technical differences. So we indicate all the important steps, but we suppress some details.

Proof of Proposition 4.3.2. Fix i with $2 \le i \le n-1$. First we prove that for any t with $0 < t < 1$ we have

$$f^*(t) := \left| \frac{f_2(a_i - t(a_i - a_{i-1}))}{f_2(a_i + t(a_i - a_{i-1}))} \right| < 1. \tag{4.12}$$

Put

$$d = \frac{a_i - a_{i-1}}{a_i} \quad \text{and} \quad s_j = \frac{a_j}{a_i} \quad (1 \le j \le n)$$

and rewrite (4.12) as

$$f^*(t) = \frac{2 - td}{2 + td} \times \prod_{j=1}^{i-1} \left(\frac{1 - s_j - td}{1 - s_j + td} \cdot \frac{1 + s_j - td}{1 + s_j + td} \right) \times \\ \times \prod_{j=i+1}^{n} \left(\frac{s_j - 1 + td}{s_j - 1 - td} \cdot \frac{s_j + 1 - td}{s_j + 1 + td} \right). \tag{4.13}$$

The first term corresponds to the root a_i of f_2. Note that $1 - s_j > td > 0$ for $j = 1, \dots, i-1$ and $0 < td < s_j - 1$ for $j = i+1, \dots, n$. To estimate the second term we follow the arguments in the proof of Proposition 4.3.1. Applying

$$1 - s_j = \frac{a_i - a_j}{a_i} = \frac{(a_i - a_{i-1}) + \cdots + (a_{j+1} - a_j)}{a_i} \le (i - j)d$$

again, but now combining it with

$$s_j \le \frac{2j - 1}{2i - 1} \quad (i < j \le n)$$

obtained by Lemma 4.3.2, we get

$$\prod_{j=1}^{i-1} \left(\frac{1 - s_j - td}{1 - s_j + td} \cdot \frac{1 + s_j - td}{1 + s_j + td} \right) \le \prod_{j=1}^{i-1} \left(\frac{i - j - t}{i - j + t} \cdot \frac{2j - 1 + (2i - 1)(1 - td)}{2j - 1 + (2i - 1)(1 + td)} \right). \tag{4.14}$$

On the other hand, in the same way as in the proof of Proposition 4.3.1, for the third term of (4.13) we obtain

$$\prod_{j=i+1}^{n} \left(\frac{s_j - 1 + td}{s_j - 1 - td} \cdot \frac{s_j + 1 - td}{s_j + 1 + td} \right) \le \prod_{j=i+1}^{n} \left(\frac{j - i + t}{j - i - t} \cdot \frac{j - i + \frac{2}{d} - t}{j - i + \frac{2}{d} + t} \right). \tag{4.15}$$

Combining (4.13), (4.14) and (4.15), we conclude

$$f^*(t) \le \frac{2 - td}{2 + td} \times \prod_{j=1}^{i-1} \left(\frac{i - j - t}{i - j + t} \cdot \frac{2j - 1 + (2i - 1)(1 - td)}{2j - 1 + (2i - 1)(1 + td)} \right) \times \\ \times \prod_{j=i+1}^{n} \left(\frac{j - i + t}{j - i - t} \cdot \frac{j - i + \frac{2}{d} - t}{j - i + \frac{2}{d} + t} \right). \tag{4.16}$$

Similarly as in the proof of Proposition 4.3.1, we can check that the right hand side of (4.16) is monotone decreasing in d (for any fixed t). Since

$$d = \frac{a_i - a_{i-1}}{a_i} = 1 - \frac{a_{i-1}}{a_i} \geq 1 - \frac{2i-3}{2i-1} = \frac{2}{2i-1}$$

by Lemma 4.3.3, substituting $d = 2/(2i-1)$ in (4.16) we obtain

$$f^*(t) \leq -\prod_{j=1}^{n} \left(\frac{j-i+t}{j-i-t} \cdot \frac{j+i-1-t}{j+i-1+t} \right).$$

Now using parts iii), i) and ii) of Lemma 4.3.1 (in this order) we obtain

$$f^*(t) < -\prod_{j=1}^{\infty} \left(\frac{j-i+t}{j-i-t} \cdot \frac{j+i-1-t}{j+i-1+t} \right) = -\frac{\Gamma(1-i-t)\Gamma(i+t)}{\Gamma(1-i+t)\Gamma(i-t)} =$$

$$= -\frac{\sin \pi(i-t)}{\sin \pi(i+t)} = \frac{\sin \pi(t-i)}{\sin \pi(t+i)} = 1.$$

Thus,

$$f^*(t) < 1 \quad \text{for all } t \in (0,1),$$

and our claim (4.12) follows. From this, just as in the proof of Proposition 4.3.1 we get

$$|f_2(\alpha_i)| < |f_2(\alpha_{i+1})|,$$

implying

$$|f_2(\alpha_1)| < \cdots < |f_2(\alpha_{n-1})|.$$

Thus, to prove the statement, it remains to show that

$$|f_2(0)| < |f_2(\alpha_1)|.$$

For this, first we show that

$$|f_2(0)| < |f_2(2a_1)|.$$

Plainly, we have

$$f_2(0) = \prod_{j=1}^{n} a_j^2.$$

On the other hand,

$$|f_2(2a_1)| = \left| \prod_{j=1}^{n} (2a_1 - a_j)(2a_1 + a_j) \right| = 3a_1^2 \prod_{j=2}^{n} (a_j^2 - 4a_1^2).$$

Thus,

$$\left| \frac{f_2(0)}{f_2(2a_1)} \right| = \frac{1}{3} \prod_{j=2}^{n} \frac{\delta_j^2}{\delta_j^2 - 4},$$

where

$$\delta_j = \frac{a_j}{a_1} \quad (2 \le j \le n).$$

Since the function

$$\frac{X^2}{X^2 - 4}$$

is strictly decreasing in $X \ge 3$ and

$$\delta_j \ge 2j - 1 \quad (2 \le j \le n),$$

we obtain

$$\left| \frac{f_2(0)}{f_2(2a_1)} \right| < \frac{1}{3} \cdot \prod_{j=2}^{\infty} \frac{(2j-1)^2}{(2j-1)^2 - 4} = \frac{1}{3} \cdot \prod_{j=2}^{\infty} \frac{\left(j - \frac{1}{2}\right)^2}{\left(j - \frac{3}{2}\right)\left(j + \frac{1}{2}\right)} = \frac{1}{3} \cdot \frac{\Gamma\left(\frac{1}{2}\right)\Gamma\left(\frac{5}{2}\right)}{\Gamma\left(\frac{3}{2}\right)\Gamma\left(\frac{3}{2}\right)} = 1.$$

Here we used part iii) of Lemma 4.3.1. From this, by $a_1 < 2a_1 < a_2$, we get

$$|f_2(0)| < |f_2(2a_1)| \le f_2(\alpha_1)|$$

and hence the proposition follows. □

Now we are ready to give the proof of Theorem 4.2.4.

Proof of Theorem 4.2.4. Let b_0 be the leading coefficient of $f(x)$, write $b_1, \dots, b_k$ for the roots of f in increasing order, and let c be the center of symmetry of them. Observe that then $b_1 - c, \dots, b_k - c$ can be written as

$$-a_n, \dots, -a_1, (a_0 = 0), a_1, \dots, a_n$$

with $k = 2n + 1$ or $k = 2n$, according as k is odd or k is even. Thus, we have

$$f(x + c) = \begin{cases} b_0 f_1(x) & \text{if } n \text{ is odd,} \\ b_0 f_2(x) & \text{if } n \text{ is even,} \end{cases}$$

with $f_1(x)$ and $f_2(x)$ defined in Propositions 4.3.1 and 4.3.2, respectively. Further, by the centrally convex property of $b_1, \dots, b_k$, we see that (4.4) in Proposition 4.3.1 or (4.5) in Proposition 4.3.2 is also satisfied, respectively. (Note that $3a_1 \le a_2$ in (4.5) can be written as $a_1 - (-a_1) \le a_2 - a_1$.) Since $f_1(x)$ and $f_2(x)$ are symmetric with respect to 0, and $f(x + c)$ is just a shift of $f(x)$ along the x axis, the statement immediately follows from Propositions 4.3.1 and 4.3.2. □

4.4 Proof of Theorem 4.2.3

As we shall see, Theorem 4.2.3 follows from Theorem 4.2.4 after some simple considerations.

Proof of Theorem 4.2.3. Suppose that f is decomposable over $\mathbb{Q}$. Then we can write $f(x) = T_1(T_2(x))$ with some polynomials $T_1, T_2 \in \mathbb{Q}[x]$ where $\deg(T_1) > 1$ and $\deg(T_2) > 1$. As one can easily check (or see e.g. the proof of Theorem 4.3 in [11]) we have

$$\deg(T_2) \leq \max_{\lambda \in \mathbb{C}} \deg(\gcd(f(x) - \lambda, f'(x))).$$

Observe that since $f(x) \in \mathbb{Q}[x]$ and the roots of $f'(x)$ are simple and real, if $\deg(\gcd(f(x) - \lambda, f'(x))) \geq 1$, then λ is an extremal value of f (in particular, $\lambda \in \mathbb{R}$). However, Theorem 4.2.4 shows that there are no three (or more) extremal values of f which are equal. Hence, $\deg(T_2) = 2$. So, if $\deg(f)$ is odd, then f is indecomposable. On the other hand, if $\deg(f)$ is even then we have

$$f(x) = b_0((x-c)^2 - (b_1 - c)^2) \cdots ((x-c)^2 - (b_k - c)^2). \tag{4.17}$$

Indeed, the degree and the leading coefficient of the right hand side in (4.17) are the same as those of f. Further, $b_1, \ldots, b_k$ are obviously roots of the right hand side - and by

$$(b_i - c)^2 = (b_{2k+1-i} - c)^2 \quad (i = 1, \ldots, k)$$

the same is true for $b_{k+1}, \ldots, b_{2k}$.

Write

$$\hat{f}(x) = b_0(x - (b_1 - c)^2) \cdots (x - (b_k - c)^2).$$

(Note that this is the same polynomial that appears in Theorem 4.2.2.) We show that this polynomial has rational coefficients. First observe that we have

$$2kc = b_1 + \cdots + b_{2k}.$$

Since the right hand side above is just the negative of the coefficient of x^{2k-1} in $f(x)$, this implies that $c \in \mathbb{Q}$. Thus $f(x + c) = \hat{f}(x^2) \in \mathbb{Q}[x]$. But then we also have $\hat{f}(x) \in \mathbb{Q}[x]$.

Finally, it is easy to check that any other decomposition of $f(x)$ over $\mathbb{Q}$ is equivalent to (4.17), and the theorem follows.

□

4.5 Proof of Theorem 4.2.2

Now we can give the proof of Theorem 4.2.2.

Proof of Theorem 4.2.2. Since $\deg(f) > 6$ and $f'(x) = (f(x) - B)'$ has simple roots, it is clear that $f(x) - B$ has at least two distinct roots. Hence, we can apply Lemma 2.1 to get an effective upper bound for m as claimed.

In particular, from this point on we may assume that $m \geq 2$ is fixed. Using again that $f'(x) = (f(x) - B)'$ has simple roots, we see that $f(x) - B$ has at most double roots. Thus the second part of the statement immediately follows from Lemma 2.2 for $m \geq 3$.

So we may assume that $m = 2$. Then, the second part of the theorem also follows from Lemma 2.2, unless we have

$$f(x) - B = p(x)(q(x))^2 \tag{4.18}$$

with some $p, q \in \mathbb{Q}[x]$, $\deg(p) \leq 2$. Differentiating both sides of (4.18) we get

$$f'(x) = q(x)(p'(x)q(x) + 2p(x)q'(x)).$$

So writing $\alpha_1, \ldots, \alpha_{d-1}$ for the (real, simple) roots of $f'(x)$, we see that the roots of $q(x)$ are among them. However, if α_i is a root of $q(x)$, then (4.18) yields $f(\alpha_i) = B$. However, this may hold at most for two α_i-s. That is, $\deg(q) \leq 2$. Hence, $d \leq 6$, which is excluded, and the theorem follows. □

4.6 Proof of Theorem 4.2.1

Now we give the proof of Theorem 4.2.1.

Proof of Theorem 4.2.1. First observe that if $\deg(g) = 2$, then by a linear substitution we may get rid of the coefficient of the linear term in g, and hence the statement follows from Theorem 4.2.2. So, from this point on we shall assume that $\deg(g) \geq 3$.

Suppose that (4.2) has infinitely many solutions in integers x, y. Then according to Lemma 2.3 we have $f(x) = \varphi(F(\lambda(x)))$ and $g(x) = \varphi(G(\kappa(x)))$, where $\lambda(x)$ and $\kappa(x)$ are linear polynomials in $\mathbb{Q}[x]$, $\varphi(x) \in \mathbb{Q}[x]$ and $(F(x), G(x))$ is a standard pair over $\mathbb{Q}$. Based on Theorem 4.2.3 we have three possible cases:

1. $\deg(\varphi) = \deg(f)$ and $\deg(F) = 1$,
2. $\deg(f) = 2k$ even, $\deg(\varphi) = k$ and $\deg(F) = 2$,

3. $\deg(\varphi) = 1$ and $\deg(F) = \deg(f)$.

In the first case $\varphi(x) = f(\tau(x))$, where τ is a rational linear polynomial. Hence, we have $g(y) = f(P(y))$, where $P(y) \in \mathbb{Q}[y]$ is arbitrary with degree ≥ 1, and the theorem follows in this case.

In the second case we have $\varphi = \hat{f}$ and $f(x) = \hat{f}((x-c)^2)$. (Note that from the proof of Theorem 4.2.2 we already know that $\hat{f}(x) \in \mathbb{Q}[x]$.) Thus, we have $g(y) = \hat{f}(Q(y))$ with some $Q(y) \in \mathbb{Q}[y]$. Lemma 2.3 implies that the equation

$$(x-c)^2 = Q(y)$$

must have infinitely many solutions in $x, y \in \mathbb{Q}$ with a bounded denominator. Thus, according to Lemma 2.2, $Q(y)$ can have at most two roots with odd multiplicity. So the statement is proved also in this case.

In the third case, we have

$$f(x) = AF(ax+b) + B \tag{4.19}$$

with $A, B, a, b \in \mathbb{Q}$ with $Aa \neq 0$, and F is a member of one of the five standard pairs from Table 2.1. We check the cases of the five standard pairs in turn.

Assume first that F comes from a standard pair of the fifth kind. Then differentiating both sides of (4.19) we see that $f'(x)$ has a double root. However, this contradicts the fact that the roots of $f'(x)$ are simple (and real). So, this case cannot occur.

Suppose next that F belongs to a standard pair of the first kind. By our conditions $\deg(f) > 6$ and $\deg(g) \geq 3$ we see that $q \geq 3$. Further, as $f'(x)$ has simple (real) roots, we obtain that $F(x) = \alpha x^r v(x)^q$ must be valid, but with $v(x)$ being constant and $r \leq 2$. However, this contradicts $\deg(f) > 6$, so this case also cannot occur.

The case that F belongs to a standard pair of the second kind also cannot hold, since then we would get $\deg(f) = 2$ or $\deg(g) = 2$, which are excluded.

So we are left with the possibilities where $F(x)$ comes from a standard pair of the third or fourth kind. In both cases, (4.19) yields an equality of the form

$$f(x) = AD_n(ax+b, \delta) + B$$

where $n \geq 3$ and δ is a non-zero rational. By Proposition 3.3 of Bilu [10] we see that $D_n(x, \delta)$ has precisely two different extremal values, and this property is certainly inherited to $AD_n(ax+b, \delta) + B$. However, Theorem 4.2.4 shows that f has at least three extremal values already for $\deg(f) > 4$. Hence, this case also cannot occur, and the theorem is proved. □

Chapter 5

Square values of Littlewood polynomials

5.1 Introduction

Littlewood polynomials, that is polynomials with only ± 1 coefficients, have an extensive literature. Their aggregated set of zeroes, that is the set

$$\mathcal{L} = \{\alpha \in \mathbb{C} : \alpha \text{ is a root of a Littlewood polynomial}\}$$

has a lot of interesting properties, and has attracted a lot of attention. We only mention a few related recent papers, and suggest the interested reader to study them and their references. Peled, Sen and Zeitouni [48] studied double roots of random Littlewood polynomials. Recently, Balister, Bollobás, Morris, Sahasrabudhe and Tiba [3] solved an old conjecture of Littlewood, by showing that there exist so called flat Littlewood polynomials of any degree $n \geq 2$. Han and Schied [40] (among others) investigated so-called step roots of such polynomials, and provided some applications. Hare and Jankauskas [41] and Yakir [68] investigated the roots of Littlewood polynomials inside the unit disk. Beside this, certain divisibility properties of Littlewood polynomials are also of interest; see e.g. Dubickas and Jankauskas [18] who studied the problem of Newman polynomials not dividing any Littlewood polynomial, or Mossinghoff [46] for a study of Littlewood polynomials with prescribed cyclotomic factors. Recently, Diophantine properties of Littlewood polynomials have also been investigated. Hajdu and Varga [39] and Hajdu, Tijdeman and Varga [37] provided various finiteness results for the power values, shifted power values and polynomial values of such polynomials. It is important to mention that the famous Nagell-Ljunggren equation

$$\frac{x^n - 1}{x - 1} = y^\ell \tag{5.1}$$

in integers x, y, n, ℓ with $|x| > 1$, $|y| > 1$, $n > 2$, $\ell \geq 2$ is an important, particular case of this problem, studied by many mathematicians. Indeed, the polynomial on the left hand side of (5.1) is a particular Littlewood polynomial, with all coefficients equal to one. Equation (5.1) has a huge literature. We only mention a classical result of Ljunggren [44], stating that the only solution of (5.1) with $\ell = 2$ is given by $(x, y, n) = (7, \pm 20, 4)$. Since we shall be concerned with square values of Littlewood polynomials, this result is of particular interest for us. We mention already at this point that based upon our new results, the set of solutions seems to be rather restricted in case of general Littlewood polynomials, as well. For further related results and surveys on the Nagell-Ljunggren equation we refer the interested reader to the book Shorey and Tijdeman [57] and the recent paper Bennett and Levin [7], and the references there.

In this chapter we explicitly give all square values of Littlewood polynomials of degrees $n = 3, 5$ and $n \leq 24$ even. For this, we need to combine several tools, including elliptic- and higher genus curves, Chabauty's method and Runge's method. To be able to handle the higher degree cases (say with $n \geq 14$), because of the huge number of polynomials to be studied, we need careful considerations and a delicate approach. Beside this, we gather computational data (by providing all solutions in a certain range) for n odd with $n \leq 17$. Based upon our results, we formulate some striking problems for further research, as well.

5.2 The main theorem

Our main theorem is the following.

Theorem 5.2.1 (L. Hajdu, O. Herendi, Sz. Tengely, N. Varga [34]). *Let $f(x)$ be a Littlewood polynomial of degree n with $n = 3, 5$ or $2 \leq n \leq 24$ even. Then all solutions of the equation*

$$f(x) = y^2 \tag{5.2}$$

in integers x, y with $|x| > 2$ and $y \geq 0$ are precisely those appearing in Tables 5.1 and 5.2.

$f(x)$	(x, y)
$\pm x^3 + x^2 \pm x - 1$	$(\pm(t^2+1), t(t^2+2))$ $(t \in \mathbb{Z}_{>1})$
$\pm x^3 - x^2 \pm x + 1$	$(\pm(t^2-1), t(t^2-2))$ $(t \in \mathbb{Z}_{>1})$
$\pm x^3 + x^2 \pm x + 1$	$(\pm 7, 20)$
$\pm x^5 + x^4 \pm x^3 - x^2 \mp x - 1$	$(\pm(t^2+1), t(t^4+3t^2+3))$ $(t \in \mathbb{Z}_{>1})$
$\pm x^5 - x^4 \pm x^3 + x^2 \mp x + 1$	$(\pm(t^2-1), t(t^4-3t^2+3))$ $(t \in \mathbb{Z}_{>1})$

Table 5.1: All solutions of equation (5.2) with $|x| > 2$ and $y \geq 0$ for $n = 3, 5$. The $\pm$ and $\mp$ signs change together in every row.

$f(x)$	(x,y)
$x^4 \pm x^3 - x^2 \mp x + 1$	$(\mp 3, 7)$
$x^4 \pm x^3 - x^2 \pm x - 1$	$(\pm 5, 27)$
$x^4 \pm x^3 + x^2 \mp x - 1$	$(\mp 5, 23)$
$x^4 \pm x^3 + x^2 \pm x + 1$	$(\pm 3, 11)$
$x^6 \pm x^5 - x^4 \mp x^3 - x^2 \mp x + 1$	$(\mp 9, 683)$
$x^6 \pm x^5 - x^4 \mp x^3 + x^2 \pm x + 1$	$(\pm 7, 363)$
$x^6 \pm x^5 + x^4 \pm x^3 - x^2 \pm x + 1$	$(\mp 3, 23)$
$x^{12} \pm x^{11} - x^{10} \mp x^9 - x^8 \pm x^7 - x^6 \mp x^5 + x^4 \mp x^3 + x^2 \pm x + 1$	$(\mp 3, 553)$
$x^{12} \pm x^{11} - x^{10} \pm x^9 + x^8 \mp x^7 + x^6 \mp x^5 - x^4 \pm x^3 + x^2 \pm x + 1$	$(\pm 3, 821)$
$x^{12} \pm x^{11} + x^{10} \mp x^9 - x^8 \mp x^7 + x^6 \pm x^5 - x^4 \pm x^3 - x^2 \mp x + 1$	$(\mp 3, 655)$
$x^{14} \pm x^{13} - x^{12} \mp x^{11} - x^{10} \pm x^9 + x^8 \pm x^7 - x^6 \pm x^5 - x^4 \pm x^3 + x^2 \pm x + 1$	$(\mp 3, 1661)$
$x^{14} \pm x^{13} - x^{12} \pm x^{11} - x^{10} \mp x^9 - x^8 \pm x^7 - x^6 \mp x^5 + x^4 \mp x^3 - x^2 \pm x + 1$	$(\pm 3, 2437)$
$x^{14} \pm x^{13} - x^{12} \pm x^{11} + x^{10} \mp x^9 - x^8 \pm x^7 + x^6 \pm x^5 - x^4 \pm x^3 - x^2 \pm x + 1$	$(\mp 3, 1597)$
$x^{14} \pm x^{13} + x^{12} \mp x^{11} - x^{10} \pm x^9 + x^8 \pm x^7 - x^6 \pm x^5 + x^4 \mp x^3 + x^2 \mp x + 1$	$(\mp 3, 1955)$
$x^{14} \pm x^{13} + x^{12} \pm x^{11} - x^{10} \pm x^9 - x^8 \pm x^7 + x^6 \pm x^5 - x^4 \mp x^3 - x^2 \pm x + 1$	$(\mp 3, 1859)$
$x^{14} \pm x^{13} + x^{12} \pm x^{11} + x^{10} \mp x^9 - x^8 \pm x^7 + x^6 \mp x^5 - x^4 \pm x^3 + x^2 \mp x + 1$	$(\mp 3, 1901)$
$x^{16} \pm x^{15} - x^{14} \mp x^{13} - x^{12} \mp x^{11} - x^{10} \mp x^9 - x^8 \mp x^7 - x^6 \pm x^5 - x^4 \mp x^3 + x^2 \mp x + 1$	$(\mp 3, 5011)$
$x^{16} \pm x^{15} - x^{14} \mp x^{13} - x^{12} \mp x^{11} - x^{10} \mp x^9 - x^8 \pm x^7 - x^6 \mp x^5 - x^4 \mp x^3 + x^2 \mp x + 1$	$(\pm 3, 7087)$
$x^{16} \pm x^{15} - x^{14} \mp x^{13} - x^{12} \pm x^{11} + x^{10} \mp x^9 + x^8 \mp x^7 + x^6 \pm x^5 - x^4 \mp x^3 - x^2 \pm x + 1$	$(\pm 3, 7121)$
$x^{16} \pm x^{15} - x^{14} \mp x^{13} + x^{12} \mp x^{11} - x^{10} \mp x^9 + x^8 \pm x^7 + x^6 \mp x^5 - x^4 \mp x^3 + x^2 \pm x + 1$	$(\mp 3, 5117)$
$x^{16} \pm x^{15} - x^{14} \mp x^{13} + x^{12} \pm x^{11} + x^{10} \pm x^9 - x^8 \mp x^7 - x^6 \mp x^5 - x^4 \mp x^3 + x^2 \pm x + 1$	$(\mp 3, 5089)$
$x^{16} \pm x^{15} - x^{14} \pm x^{13} + x^{12} \mp x^{11} + x^{10} \pm x^9 - x^8 \pm x^7 - x^6 \pm x^5 + x^4 \pm x^3 + x^2 \pm x + 1$	$(\pm 5, 422409)$
$x^{16} \pm x^{15} + x^{14} \pm x^{13} + x^{12} \mp x^{11} - x^{10} \pm x^9 - x^8 \mp x^7 + x^6 \pm x^5 - x^4 \pm x^3 + x^2 \mp x + 1$	$(\pm 3, 8005)$
$x^{16} \pm x^{15} + x^{14} \pm x^{13} + x^{12} \mp x^{11} + x^{10} \pm x^9 + x^8 \pm x^7 - x^6 \mp x^5 + x^4 \pm x^3 + x^2 \mp x + 1$	$(\mp 3, 5713)$
$x^{16} \pm x^{15} + x^{14} \pm x^{13} + x^{12} \pm x^{11} + x^{10} \mp x^9 + x^8 \pm x^7 - x^6 \pm x^5 - x^4 \pm x^3 + x^2 \mp x + 1$	$(\pm 3, 8033)$
$x^{18} \pm x^{17} - x^{16} \mp x^{15} - x^{14} \mp x^{13} - x^{12} \mp x^{11} + x^{10} \mp x^9 - x^8 \pm x^7 + x^6 \pm x^5 + x^4 \mp x^3 + x^2 \mp x + 1$	$(\pm 3, 21263)$
$x^{18} \pm x^{17} - x^{16} \mp x^{15} - x^{14} \pm x^{13} - x^{12} \mp x^{11} - x^{10} \mp x^9 + x^8 \pm x^7 - x^6 \mp x^5 - x^4 \pm x^3 - x^2 \pm x + 1$	$(\mp 3, 14927)$
$x^{18} \pm x^{17} - x^{16} \mp x^{15} + x^{14} \mp x^{13} + x^{12} \mp x^{11} - x^{10} \mp x^9 + x^8 \mp x^7 - x^6 \pm x^5 - x^4 \pm x^3 - x^2 \mp x + 1$	$(\mp 3, 15383)$
$x^{18} \pm x^{17} - x^{16} \mp x^{15} + x^{14} \pm x^{13} - x^{12} \pm x^{11} + x^{10} \pm x^9 + x^8 \pm x^7 - x^6 \pm x^5 - x^4 \pm x^3 - x^2 \mp x + 1$	$(\mp 3, 15235)$
$x^{18} \pm x^{17} - x^{16} \pm x^{15} - x^{14} \mp x^{13} + x^{12} \mp x^{11} - x^{10} \pm x^9 + x^8 \pm x^7 + x^6 \pm x^5 + x^4 \mp x^3 + x^2 \mp x + 1$	$(\mp 3, 14083)$
$x^{18} \pm x^{17} + x^{16} \pm x^{15} - x^{14} \mp x^{13} + x^{12} \pm x^{11} + x^{10} \mp x^9 + x^8 \pm x^7 - x^6 \pm x^5 - x^4 \mp x^3 + x^2 \mp x + 1$	$(\mp 3, 16859)$
$x^{18} \pm x^{17} + x^{16} \pm x^{15} + x^{14} \pm x^{13} + x^{12} \mp x^{11} - x^{10} \pm x^9 + x^8 \mp x^7 - x^6 \mp x^5 - x^4 \pm x^3 + x^2 \mp x + 1$	$(\mp 3, 17053)$
$x^{20} \pm x^{19} - x^{18} \mp x^{17} - x^{16} \pm x^{15} + x^{14} \pm x^{13} - x^{12} \mp x^{11} - x^{10} \pm x^9 + x^8 \mp x^7 + x^6 \mp x^5 - x^4 \pm x^3 - x^2 \pm x + 1$	$(\mp 3, 44851)$
$x^{20} \pm x^{1}9 - x^{18} \mp x^{17} + x^{16} \mp x^{15} + x^{14} \mp x^{13} + x^{12} \mp x^{11} - x^{10} \pm x^9 + x^8 \mp x^7 - x^6 \pm x^5 + x^4 \mp x^3 + x^2 \mp x + 1$	$(\mp 3, 46159)$
$x^{20} \pm x^{19} - x^{18} \pm x^{17} + x^{16} \pm x^{15} - x^{14} \mp x^{13} + x^{12} \mp x^{11} - x^{10} \pm x^9 - x^8 \mp x^7 - x^6 \mp x^5 + x^4 \pm x^3 + x^2 \mp x + 1$	$(\pm 3, 66649)$
$x^{20} \pm x^{19} + x^{18} \mp x^{17} + x^{16} \mp x^{15} + x^{14} \mp x^{13} + x^{12} \mp x^{11} - x^{10} \mp x^9 + x^8 \mp x^7 - x^6 \pm x^5 - x^4 \pm x^3 + x^2 \mp x + 1$	$(\mp 3, 53903)$
$x^{20} \pm x^{19} + x^{18} \pm x^{17} + x^{16} \mp x^{15} + x^{14} \mp x^{13} + x^{12} \pm x^{11} + x^{10} \mp x^9 - x^8 \pm x^7 - x^6 \pm x^5 + x^4 \mp x^3 + x^2 \pm x + 1$	$(\mp 3, 51449)$
$x^{20} \pm x^{19} + x^{18} \pm x^{17} + x^{16} \pm x^{15} + x^{14} \mp x^{13} + x^{12} \pm x^{11} + x^{10} \pm x^9 - x^8 \mp x^7 - x^6 \pm x^5 - x^4 \pm x^3 - x^2 \pm x + 1$	$(\mp 3, 51169)$
$x^{22} \pm x^{21} - x^{20} \mp x^{19} - x^{18} \pm x^{17} + x^{16} \mp x^{15} + x^{14} \mp x^{13} + x^{12} \pm x^{11} + x^{10} \mp x^9 - x^8 \pm x^7 + x^6 \pm x^5 + x^4 \mp x^3 - x^2 \pm x + 1$	$(\mp 3, 134699)$

$x^{22} \pm x^{21} - x^{20} \mp x^{19} + x^{18} \mp x^{17} - x^{16} \pm x^{15} - x^{14} \mp x^{13} + x^{12} \pm x^{11} + x^{10} \pm x^9 + x^8 \pm x^7 - x^6 \pm x^5 + x^4 \pm x^3 - x^2 \mp x + 1$	$(\mp 3, 138031)$
$x^{22} \pm x^{21} - x^{20} \mp x^{19} + x^{18} \mp x^{17} - x^{16} \pm x^{15} - x^{14} \pm x^{13} - x^{12} \mp x^{11} + x^{10} \mp x^9 - x^8 \mp x^7 + x^6 \mp x^5 + x^4 \pm x^3 - x^2 \mp x + 1$	$(\mp 3, 138017)$
$x^{22} \pm x^{21} - x^{20} \mp x^{19} + x^{18} \pm x^{17} + x^{16} \mp x^{15} + x^{14} \mp x^{13} + x^{12} \mp x^{11} + x^{10} \pm x^9 - x^8 \mp x^7 + x^6 \mp x^5 + x^4 \pm x^3 - x^2 \mp x + 1$	$(\mp 3, 137545)$
$x^{22} \pm x^{21} - x^{20} \mp x^{19} + x^{18} \pm x^{17} + x^{16} \mp x^{15} + x^{14} \pm x^{13} - x^{12} \mp x^{11} + x^{10} \mp x^9 + x^8 \pm x^7 - x^6 \pm x^5 + x^4 \pm x^3 - x^2 \mp x + 1$	$(\mp 3, 137531)$
$x^{22} \pm x^{21} - x^{20} \pm x^{19} - x^{18} \pm x^{17} + x^{16} \pm x^{15} + x^{14} \pm x^{13} - x^{12} \mp x^{11} + x^{10} \pm x^9 - x^8 \mp x^7 - x^6 \pm x^5 - x^4 \mp x^3 + x^2 \pm x + 1$	$(\mp 3, 125645)$
$x^{22} \pm x^{21} - x^{20} \pm x^{19} + x^{18} \mp x^{17} + x^{16} \pm x^{15} + x^{14} \pm x^{13} - x^{12} \mp x^{11} - x^{10} \mp x^9 + x^8 \pm x^7 - x^6 \pm x^5 - x^4 \pm x^3 + x^2 \pm x + 1$	$(\pm 3, 199595)$
$x^{22} \pm x^{21} - x^{20} \pm x^{19} + x^{18} \pm x^{17} + x^{16} \pm x^{15} - x^{14} \pm x^{13} + x^{12} \pm x^{11} + x^{10} \pm x^9 + x^8 \mp x^7 - x^6 \pm x^5 + x^4 \pm x^3 + x^2 \pm x + 1$	$(\pm 3, 200221)$
$x^{22} \pm x^{21} + x^{20} \mp x^{19} - x^{18} \mp x^{17} - x^{16} \mp x^{15} - x^{14} \mp x^{13} - x^{12} \pm x^{11} + x^{10} \pm x^9 + x^8 \mp x^7 - x^6 \pm x^5 - x^4 \pm x^3 - x^2 \pm x + 1$	$(\pm 3, 208771)$
$x^{22} \pm x^{21} + x^{20} \pm x^{19} - x^{18} \pm x^{17} - x^{16} \pm x^{15} + x^{14} \pm x^{13} + x^{12} \mp x^{11} + x^{10} \mp x^9 - x^8 \pm x^7 - x^6 \mp x^5 + x^4 \mp x^3 - x^2 \pm x + 1$	$(\mp 3, 150583)$
$x^{22} \pm x^{21} + x^{20} \pm x^{19} + x^{18} \pm x^{17} - x^{16} \pm x^{15} - x^{14} \mp x^{13} + x^{12} \mp x^{11} - x^{10} \mp x^9 - x^8 \mp x^7 + x^6 \pm x^5 + x^4 \pm x^3 - x^2 \pm x + 1$	$(\mp 3, 153113)$
$x^{24} \pm x^{23} - x^{22} \mp x^{21} - x^{20} \mp x^{19} - x^{18} \mp x^{17} - x^{16} \mp x^{15} + x^{14} \pm x^{13} - x^{12} \mp x^{11} - x^{10} \mp x^9 - x^8 \pm x^7 - x^6 \mp x^5 + x^4 \pm x^3 + x^2 \mp x + 1$	$(\pm 3, 574033)$
$x^{24} \pm x^{23} - x^{22} \mp x^{21} + x^{20} \pm x^{19} - x^{18} \pm x^{17} + x^{16} \pm x^{15} + x^{14} \pm x^{13} + x^{12} \mp x^{11} + x^{10} \pm x^9 - x^8 \mp x^7 + x^6 \mp x^5 - x^4 \mp x^3 - x^2 \pm x + 1$	$(\pm 3, 582397)$
$x^{24} \pm x^{23} - x^{22} \mp x^{21} + x^{20} \pm x^{19} + x^{18} \mp x^{17} - x^{16} \pm x^{15} + x^{14} \pm x^{13} - x^{12} \mp x^{11} - x^{10} \mp x^9 - x^8 \pm x^7 - x^6 \mp x^5 + x^4 \pm x^3 + x^2 \mp x + 1$	$(\mp 3, 412495)$
$x^{24} \pm x^{23} - x^{22} \pm x^{21} - x^{20} \mp x^{19} + x^{18} \mp x^{17} - x^{16} \pm x^{15} - x^{14} \mp x^{13} - x^{12} \pm x^{11} - x^{10} \mp x^9 - x^8 \mp x^7 - x^6 \mp x^5 - x^4 \pm x^3 - x^2 \pm x + 1$	$(\pm 3, 592643)$
$x^{24} \pm x^{23} - x^{22} \pm x^{21} - x^{20} \mp x^{19} + x^{18} \pm x^{17} + x^{16} \mp x^{15} - x^{14} \pm x^{13} + x^{12} \pm x^{11} + x^{10} \pm x^9 + x^8 \mp x^7 + x^6 \pm x^5 + x^4 \mp x^3 - x^2 \pm x + 1$	$(\pm 3, 592913)$
$x^{24} \pm x^{23} - x^{22} \pm x^{21} + x^{20} \pm x^{19} - x^{18} \mp x^{17} - x^{16} \mp x^{15} - x^{14} \mp x^{13} + x^{12} \mp x^{11} - x^{10} \mp x^9 + x^8 \mp x^7 + x^6 \pm x^5 + x^4 \mp x^3 + x^2 \pm x + 1$	$(\mp 3, 385331)$
$x^{24} \pm x^{23} - x^{22} \pm x^{21} + x^{20} \pm x^{19} + x^{18} \mp x^{17} + x^{16} \mp x^{15} + x^{14} \mp x^{13} + x^{12} \pm x^{11} - x^{10} \mp x^9 - x^8 \mp x^7 + x^6 \mp x^5 - x^4 \mp x^3 + x^2 \mp x + 1$	$(\pm 3, 600493)$
$x^{24} \pm x^{23} - x^{22} \pm x^{21} + x^{20} \pm x^{19} + x^{18} \pm x^{17} - x^{16} \mp x^{15} - x^{14} \mp x^{13} - x^{12} \pm x^{11} + x^{10} \mp x^9 - x^8 \mp x^7 + x^6 \pm x^5 + x^4 \mp x^3 - x^2 \mp x + 1$	$(\mp 3, 385999)$
$x^{24} \pm x^{23} + x^{22} \mp x^{21} - x^{20} \pm x^{19} - x^{18} \pm x^{17} + x^{16} \pm x^{15} - x^{14} \pm x^{13} - x^{12} \mp x^{11} + x^{10} \mp x^9 - x^8 \mp x^7 + x^6 \mp x^5 + x^4 \mp x^3 + x^2 \mp x + 1$	$(\mp 3, 474325)$
$x^{24} \pm x^{23} + x^{22} \mp x^{21} + x^{20} \mp x^{19} - x^{18} \mp x^{17} + x^{16} \mp x^{15} + x^{14} \pm x^{13} - x^{12} \pm x^{11} + x^{10} \pm x^9 + x^8 \pm x^7 - x^6 \mp x^5 - x^4 \mp x^3 - x^2 \mp x + 1$	$(\mp 3, 484333)$
$x^{24} \pm x^{23} + x^{22} \mp x^{21} + x^{20} \mp x^{19} + x^{18} \mp x^{17} - x^{16} \pm x^{15} + x^{14} \mp x^{13} - x^{12} \mp x^{11} - x^{10} \mp x^9 - x^8 \pm x^7 + x^6 \pm x^5 - x^4 \pm x^3 - x^2 \pm x + 1$	$(\pm 3, 632495)$
$x^{24} \pm x^{23} + x^{22} \pm x^{21} - x^{20} \mp x^{19} - x^{18} \pm x^{17} - x^{16} \mp x^{15} - x^{14} \mp x^{13} + x^{12} \mp x^{11} + x^{10} \mp x^9 + x^8 \pm x^7 + x^6 \pm x^5 - x^4 \pm x^3 - x^2 \mp x + 1$	$(\mp 3, 454241)$
$x^{24} \pm x^{23} + x^{22} \pm x^{21} - x^{20} \mp x^{19} + x^{18} \mp x^{17} + x^{16} \pm x^{15} + x^{14} \mp x^{13} - x^{12} \mp x^{11} - x^{10} \mp x^9 + x^8 \mp x^7 - x^6 \mp x^5 + x^4 \mp x^3 + x^2 \pm x + 1$	$(\mp 3, 455449)$
$x^{24} \pm x^{23} + x^{22} \pm x^{21} - x^{20} \pm x^{19} - x^{18} \pm x^{17} - x^{16} \mp x^{15} - x^{14} \mp x^{13} + x^{12} \pm x^{11} + x^{10} \pm x^9 - x^8 \mp x^7 - x^6 \mp x^5 + x^4 \mp x^3 + x^2 \mp x + 1$	$(\pm 3, 644801)$

$x^{24} \pm x^{23} + x^{22} \pm x^{21} + x^{20} \pm x^{19} + x^{18} \mp x^{17} - x^{16} \pm x^{15} + x^{14} \pm x^{13} + x^{12} \pm x^{11} + x^{10} \mp x^9 - x^8 \pm x^7 + x^6 \pm x^5 - x^4 \mp x^3 - x^2 \mp x + 1$	$(\pm 3, 650615)$
$x^{24} \pm x^{23} + x^{22} \pm x^{21} + x^{20} \pm x^{19} + x^{18} \pm x^{17} + x^{16} \pm x^{15} - x^{14} \pm x^{13} + x^{12} \pm x^{11} + x^{10} \pm x^9 - x^8 \pm x^7 + x^6 \pm x^5 + x^4 \mp x^3 + x^2 \mp x + 1$	$(\mp 3, 460231)$

Table 5.2: All solutions of equation (5.2) with $|x| > 2$ and $y \geq 0$ for n even with $2 \leq n \leq 24$. The $\pm$ and $\mp$ signs change together in every row.

For the sake of completeness, and in particular, to gather more substantial numerical data also in case of odd exponents, we provide an alike statement for n odd. Note however, that in this case we are not able to find all solutions of (5.2), our purpose is only to get some computational insight in this case, as well.

Proposition 5.2.1. *Let $f(x)$ be a Littlewood polynomial of degree n with $7 \leq n \leq 17$ odd. Suppose further that $f(x)$ does not belong to any of the families*

$$\pm(x^{2k+1} + \ldots + x^{k+1} - x^k - \ldots - 1) = \pm(x-1)(x^k + \cdots + x + 1)^2, \tag{5.3}$$

$$\pm\,(x^{2k+1} - x^{2k} + \ldots + (-1)^{k+2}x^{k+1} + (-1)^k x^k + \cdots + 1) = \\ = \pm(x+1)(x^k - x^{k-1} + \cdots + (-1)^k)^2, \tag{5.4}$$

$$\pm\,(x^{4k+3} + x^{4k+2} - x^{4k+1} - x^{4k} + \ldots + (-1)^k x^{2k+3} + (-1)^k x^{2k+2} \\ + (-1)^k x^{2k+1} + (-1)^k x^{2k} + \ldots + x + 1) = \\ = \pm(x+1)(x^2+1)(x^{2k} - x^{2k-2} + \ldots + (-1)^k)^2, \tag{5.5}$$

$$\pm\,(x^{4k+3} - x^{4k+2} - x^{4k+1} + x^{4k} + \ldots + (-1)^k x^{2k+3} - (-1)^k x^{2k+2} \\ + (-1)^k x^{2k+1} - (-1)^k x^{2k} + \ldots + x - 1) = \\ = \pm(x-1)(x^2+1)(x^{2k} - x^{2k-2} + \ldots + (-1)^k)^2. \tag{5.6}$$

Then all solutions of equation (5.2) in integers x, y with $100 \geq |x| > 2$ and $y \geq 0$ are precisely those appearing in Table 5.3.

$f(x)$	(x,y)
$\pm x^7 - x^6 \mp x^5 - x^4 \pm x^3 - x^2 \pm x + 1$	$(\pm 3, 34)$
$\pm x^9 - x^8 \pm x^7 + x^6 \pm x^5 + x^4 \pm x^3 - x^2 \pm x + 1$	$(\pm 3, 128)$
$\pm x^9 + x^8 \mp x^7 + x^6 \pm x^5 - x^4 \pm x^3 - x^2 \mp x + 1$	$(\pm 3, 158)$
$\pm x^9 + x^8 \pm x^7 - x^6 \mp x^5 + x^4 \pm x^3 - x^2 \mp x + 1$	$(\pm 3, 166)$
$\pm x^{11} - x^{10} \mp x^9 + x^8 \mp x^7 - x^6 \pm x^5 + x^4 \pm x^3 - x^2 \mp x + 1$	$(\pm 3, 320)$
$\pm x^{11} - x^{10} \mp x^9 + x^8 \pm x^7 + x^6 \mp x^5 - x^4 \pm x^3 - x^2 \mp x + 1$	$(\pm 3, 328)$
$\pm x^{11} - x^{10} \pm x^9 - x^8 \mp x^7 - x^6 \mp x^5 + x^4 \pm x^3 - x^2 \pm x + 1$	$(\pm 3, 358)$
$\pm x^{11} - x^{10} \pm x^9 + x^8 \pm x^7 - x^6 \pm x^5 - x^4 \mp x^3 - x^2 \mp x + 1$	$(\pm 3, 382)$
$\pm x^{13} - x^{12} \mp x^{11} + x^{10} \pm x^9 + x^8 \pm x^7 - x^6 \mp x^5 - x^4 \pm x^3 + x^2 \mp x + 1$	$(\pm 3, 986)$
$\pm x^{13} - x^{12} \pm x^{11} - x^{10} \mp x^9 - x^8 \pm x^7 + x^6 \pm x^5 - x^4 \mp x^3 - x^2 \mp x + 1$	$(\pm 3, 1076)$
$\pm x^{13} - x^{12} \pm x^{11} - x^{10} \pm x^9 + x^8 \pm x^7 + x^6 \mp x^5 + x^4 \pm x^3 - x^2 \pm x + 1$	$(\pm 3, 1100)$
$\pm x^{13} + x^{12} \mp x^{11} - x^{10} \mp x^9 - x^8 \pm x^7 + x^6 \mp x^5 - x^4 \pm x^3 + x^2 \pm x + 1$	$(\pm 3, 1366)$
$\pm x^{13} + x^{12} \pm x^{11} + x^{10} \mp x^9 + x^8 \mp x^7 + x^6 \mp x^5 - x^4 \mp x^3 - x^2 \pm x + 1$	$(\pm 3, 1532)$
$\pm x^{15} - x^{14} \pm x^{13} - x^{12} \mp x^{11} - x^{10} \pm x^9 - x^8 \pm x^7 - x^6 \mp x^5 + x^4 \pm x^3 + x^2 \mp x + 1$	$(\pm 3, 3226)$
$\pm x^{15} - x^{14} \pm x^{13} - x^{12} \pm x^{11} - x^{10} \mp x^9 - x^8 \mp x^7 + x^6 \mp x^5 + x^4 \pm x^3 - x^2 \pm x + 1$	$(\pm 3, 3274)$
$\pm x^{15} - x^{14} \pm x^{13} - x^{12} \pm x^{11} + x^{10} \pm x^9 - x^8 \mp x^7 + x^6 \pm x^5 - x^4 \mp x^3 - x^2 \mp x + 1$	$(\pm 3, 3298)$
$\pm x^{15} - x^{14} \pm x^{13} + x^{12} \mp x^{11} - x^{10} \pm x^9 + x^8 \mp x^7 - x^6 \mp x^5 - x^4 \pm x^3 + x^2 \mp x + 1$	$(\pm 3, 3388)$
$\pm x^{17} - x^{16} \mp x^{15} - x^{14} \pm x^{13} + x^{12} \mp x^{11} - x^{10} \mp x^9 - x^8 \mp x^7 + x^6 \pm x^5 - x^4 \pm x^3 - x^2 \pm x + 1$	$(\pm 3, 8296)$
$\pm x^{17} - x^{16} \mp x^{15} + x^{14} \mp x^{13} + x^{12} \mp x^{11} - x^{10} \pm x^9 - x^8 \mp x^7 - x^6 \mp x^5 - x^4 \mp x^3 - x^2 \pm x + 1$	$(\pm 3, 8674)$
$\pm x^{17} - x^{16} \mp x^{15} + x^{14} \pm x^{13} + x^{12} \pm x^{11} - x^{10} \pm x^9 - x^8 \mp x^7 + x^6 \pm x^5 + x^4 \pm x^3 - x^2 \pm x + 1$	$(\pm 3, 8876)$
$\pm x^{17} - x^{16} \pm x^{15} - x^{14} \pm x^{13} - x^{12} \mp x^{11} - x^{10} \pm x^9 + x^8 \mp x^7 + x^6 \pm x^5 - x^4 \mp x^3 - x^2 \mp x + 1$	$(\pm 3, 9824)$
$\pm x^{17} - x^{16} \pm x^{15} - x^{14} \pm x^{13} - x^{12} \pm x^{11} + x^{10} \pm x^9 + x^8 \mp x^7 + x^6 \mp x^5 + x^4 \pm x^3 - x^2 \pm x + 1$	$(\pm 3, 9848)$
$\pm x^{17} - x^{16} \pm x^{15} - x^{14} \pm x^{13} + x^{12} \pm x^{11} - x^{10} \pm x^9 + x^8 \pm x^7 - x^6 \mp x^5 + x^4 \pm x^3 + x^2 \mp x + 1$	$(\pm 3, 9896)$
$\pm x^{17} - x^{16} \pm x^{15} + x^{14} \mp x^{13} - x^{12} \pm x^{11} + x^{10} \pm x^9 - x^8 \mp x^7 + x^6 \pm x^5 - x^4 \mp x^3 + x^2 \mp x + 1$	$(\pm 3, 10166)$
$\pm x^{17} + x^{16} \mp x^{15} + x^{14} \pm x^{13} - x^{12} \pm x^{11} + x^{10} \mp x^9 - x^8 \mp x^7 - x^6 \pm x^5 + x^4 \pm x^3 - x^2 \mp x + 1$	$(\pm 3, 12802)$
$\pm x^{17} + x^{16} \pm x^{15} - x^{14} \mp x^{13} - x^{12} \pm x^{11} - x^{10} \pm x^9 + x^8 \pm x^7 + x^6 \pm x^5 - x^4 \mp x^3 + x^2 \pm x + 1$	$(\pm 3, 13408)$
$\pm x^{17} + x^{16} \pm x^{15} - x^{14} \mp x^{13} + x^{12} \pm x^{11} + x^{10} \mp x^9 - x^8 \pm x^7 + x^6 \mp x^5 - x^4 \pm x^3 - x^2 \mp x + 1$	$(\pm 3, 13450)$
$\pm x^{17} + x^{16} \pm x^{15} + x^{14} \pm x^{13} - x^{12} \pm x^{11} - x^{10} \mp x^9 + x^8 \pm x^7 - x^6 \mp x^5 + x^4 \mp x^3 - x^2 \mp x + 1$	$(\pm 3, 13874)$

Table 5.3: All solutions of equation (5.2) excluding polynomials $f(x)$ with (5.3), (5.4), (5.5), (5.6), with $100 \geq |x| > 2$ and $y \geq 0$ for $7 \leq n \leq 17$ odd. The $\pm$ and $\mp$ signs change together in every row.

Note that it is obvious that if $f(x)$ is of the shape (5.3) or (5.4) then (5.2) has infinitely many solutions. Further, by the procedure `IntegralPoints` of Magma [13], we get that the solutions of the equations

$$\pm(x+1)(x^2+1) = y^2 \quad \text{and} \quad \pm(x-1)(x^2+1) = y^2$$

are given by $(x,y) = (0,\pm 1), (\pm 1, 0), (\pm 7, \pm 20)$. So if $f(x)$ is of the shape (5.5) or (5.6) then (5.2) has a solution with $x = \pm 7$ (with $+$ and $-$ signs on the left hand side, respectively) for any n with $n \equiv 3 \pmod 4$.

Remark. We can exclude the cases $|x| \leq 2$, even if we do not prescribe an upper bound for n. (Note that, clearly, the square values of Littlewood polynomials of any fixed degree at places x with $|x| \leq 2$ can be listed without any trouble.) The case $x = 0$ is trivial, and the cases $x = \pm 1$ are also easy. The cases $x = \pm 2$ require a little more attention. Since if $f(x)$ is a Littlewood polynomial then so is $f(-x)$, thus talking about the values of Littlewood polynomials at ± 2, it is sufficient to consider the values at 2. As one can readily check, any odd integer r with $-2^{n+1} + 1 \leq r \leq 2^{n+1} - 1$ can be represented in the form $f(2)$ with a unique Littlewood polynomial f of degree n, in precisely one way. Indeed, these numbers r are just given by

$$-2^n - 2^{n-1} - \ldots - 2 - 1, -2^n - 2^{n-1} - \ldots - 2 + 1, \ldots, 2^n + 2^{n-1} + \ldots + 2 + 1,$$

and obviously the representation (for fixed n) is unique. This shows that the solutions of (5.2) with $|x| = 2$ are also completely understood and described.

Based upon our results, we think that the solution set to (5.2) is very restricted. We propose the following problems. The first two problems ask about the existence of bounds for the solutions in a general sense. The third problem offers a possible complete description of all solutions with $|x| > 3$. Note that an affirmative answer to the first question in Problem 3 would certainly yield an affirmative answer to the first two problems, in an explicit form.

Problem 1. Is it true that there exists an absolute constant c_1 such that for all solutions x, y of (5.2) with any Littlewood polynomial f of degree $n \geq 2$ not of the shape (5.3) and (5.4) we have $|x| \leq c_1$?

Problem 2. Is it true that there exists an absolute constant c_2 such that if $n > c_2$ then for all solutions x, y of (5.2) with any Littlewood polynomial f of degree n not of the shape (5.3), (5.4), (5.5), (5.6), we have $|x| \leq 3$? On the other hand, is it true that there exist infinitely many Littlewood polynomials $f(x)$ not of the shape (5.4) such that $f(3)$ is a square? Even more, is it true that for every $n > 10$ there exists a Littlewood polynomial $f(x)$ of degree n not of the shape (5.4) such that $f(3)$ is a square?

Problem 3. Is it true that if (x, y) is a solution of (5.2) with $|x| > 3$ and $y \geq 0$ for some Littlewood polynomial f of degree $n \geq 2$ not of the form (5.3), (5.4), (5.5), (5.6), then

$$(x, y, n) = (\pm 5, 23, 4), (\pm 5, 27, 4), (\pm 7, 363, 6), (\pm 9, 683, 6), (\pm 5, 422409, 16)$$

holds? In particular, is it true that for all solutions of (5.2) with x even with any Littlewood polynomial f not of the shape (5.3), (5.4) we have $|x| \leq 2$?

Now we give some heuristics which shed some light on the problems, in particular, support that solutions with $|x| > 3$ should be extremely rare.

Some heuristics behind the problems. We have already argued that solutions with $|x| \leq 2$ will appear infinitely often. So let z be an integer with $|z| \geq 3$, and consider the question whether $f(z)$ is a square for some Littlewood polynomial of degree n. Using symmetry as earlier, we may restrict our attention to positive integers z and Littlewood polynomials f of degree n with leading coefficient 1. Observe that for fixed n, we have

$$z^n - \frac{z^n - 1}{z - 1} \leq f(z) \leq z^n + \frac{z^n - 1}{z - 1}.$$

So $f(z)$ belongs to an interval of length approximately

$$\ell = \frac{2z^n}{z - 1}. \tag{5.7}$$

(It will be clear that the points where we work 'approximately', do not change the general argument.) Further, the number of squares S in this interval is given by

$$\sqrt{z^n + \frac{z^n - 1}{z - 1}} - \sqrt{z^n - \frac{z^n - 1}{z - 1}} = \frac{2z^n}{\sqrt{z^n + \frac{z^n-1}{z-1}} + \sqrt{z^n - \frac{z^n-1}{z-1}}},$$

so approximately

$$S = (\sqrt{z})^n. \tag{5.8}$$

The number of Littlewood polynomials of degree n (with leading coefficient 1) is 2^n. Considering the values of these polynomials at z as independent random variables, in view of (5.7) and (5.8) we get that the probability that none of them is a square, is approximately given by

$$P_n(z) := \left(1 - \frac{1}{(\sqrt{z})^n}\right)^{2^n} = \left(\left(1 - \frac{1}{(\sqrt{z})^n}\right)^{(\sqrt{z})^n}\right)^{\left(\frac{2}{\sqrt{z}}\right)^n}.$$

As

$$\lim_{n\to\infty} \left(1 - \frac{1}{(\sqrt{z})^n}\right)^{(\sqrt{z})^n} = \frac{1}{e}$$

we see that $P_n(3)$ tends to 0, while $P_n(z)$ tends to 1 for $z \geq 5$ as n tends to infinity. This suggests that for n 'large enough', for $z = 3$ there is a Littlewood polynomial with $f(z)$ being a square, while for $z \geq 5$ just the opposite statement is valid. We are left with the case $z = 4$. However, then (5.2) implies that $\pm 4 \pm 1 \equiv y^2 \pmod 8$ should be valid, which cannot hold. That is, $z = 4$ never yields a solution to (5.2).

Altogether, it seems that the above heuristics suggest that the answers to the problems might be affirmative.

Remark. As we have seen, for n odd we have the identities (5.3), (5.4), (5.5), (5.6). The latter two are easy to handle; we did that already after Proposition 5.2.1. On the other hand, in case of (5.3), (5.4) there are infinitely many solutions for (5.2). Note that the existence of these solutions does not 'contradict' our heuristics above: special structures will certainly skip through such a probabilistic argument. There are no further identities similar to (5.3) and (5.4) (taken from [39]). In case of n even, any Littlewood polynomial of degree n is congruent to $(x^{n+1}-1)/(x-1)$ modulo 2, which has a square-free numerator. Further, the proof of Theorem 2.2 of [39] shows that a Littlewood polynomial of odd degree is of the form $g(x)(h(x))^2$ with $\deg(g) = 1$ if and only if $f(x)$ appears in (5.3) or (5.4). So altogether, the above problems (after excluding the special polynomials in (5.3), (5.4), (5.5), (5.6)) might be answered to the affirmative.

5.3 Proof of Theorem 5.2.1

As in the proof of our theorem we use different tools in the different cases, we give our argument in different subsections. We made available the codes we used at `https://shrek.unideb.hu/~tengely/LittleWood.html`.

5.3.1 Proof of Theorem 5.2.1 for $n = 3$

Consider the Littlewood polynomials $f(x) = \pm x^3 \pm x^2 \pm x \pm 1$, and investigate (5.2) for them. There are 16 equations to study, however, using the substitution $x \to -x$ it is sufficient to consider only those where the leading coefficient of $f(x)$ is positive. Indeed, (x, y) is a solution to $f(x) = y^2$ if and only if $(-x, y)$ is a solution to $f(-x) = y^2$. Two of the curves implied by (5.2) are singular. Namely, for

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

and

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

(5.2) has infinitely many solutions. These solutions are trivial to describe: they are given by

$$(x, y) = (t^2 + 1, \pm t(t^2 + 2)) \quad \text{and} \quad (x, y) = (t^2 - 1, \pm t(t^2 - 2)),$$

respectively. By our assumptions $|x| > 2$ and $y \geq 0$, we can omit the $\pm$ signs, and we may assume that $t > 1$. In the other cases (5.2) is an elliptic curve, and we may apply the procedure `IntegralPoints` of Magma [13] (based upon methods of Gebel, Pethő, Zimmer [25] and Stroeker, Tzanakis [62]) to obtain the integral points (solutions). We get that (5.2) has an integral solution with $|x| > 2$ only for $f(x) = x^3 + x^2 + x + 1$, when the only such solutions are given by $(x, y) = (7, \pm 20)$. So our theorem follows in this case. The solutions (with $|x| > 2$ and $y \geq 0$, taking into consideration the substitution $x \to -x$ as well) are given in the first three rows of Table 5.1.

5.3.2 Proof of Theorem 5.2.1 for $n = 5$

We need to study equation (5.2) for $f(x) = \pm x^5 \pm x^4 \pm x^3 \pm x^2 \pm x \pm 1$, which now is a hyperelliptic equation. Similarly as in case $n = 3$, we may restrict to polynomials $f(x)$ with positive leading coefficient, so we need to consider 32 equations. We shall use Chabauty's method [16] and the hyperelliptic logarithm method [23] to handle these equations.

We have two reducible cases that are not square-free, these are as follows:

$$\begin{aligned} x^5 + x^4 + x^3 - x^2 - x - 1 &= (x-1)(x^2+x+1)^2, \\ x^5 - x^4 + x^3 + x^2 - x + 1 &= (x+1)(x^2-x+1)^2. \end{aligned}$$

In these cases we can easily describe all solutions of (5.2). These are given by

$$(x, y) = (t^2 + 1, t(t^4 + 3t^2 + 3)) \ (t \in \mathbb{Z})$$

and

$$(x, y) = (t^2 - 1, t(t^4 - 3t^2 + 3)) \ (t \in \mathbb{Z}),$$

respectively.

In the remaining cases we need to consider genus 2 curves. By using Magma [13] we can compute the ranks of the Jacobians and determine generators of the Mordell-Weil groups based on Stoll's papers [58], [59], [60].

The rank of the Jacobian is 0 for the hyperelliptic curves related to the following polynomials:

$$x^5 + x^4 - x^3 - x^2 - x - 1,\ x^5 + x^4 - x^3 - x^2 + x - 1,\ x^5 - x^4 + x^3 - x^2 - x - 1,$$

$$x^5 - x^4 + x^3 - x^2 + x - 1,\ x^5 + x^4 - x^3 + x^2 - x - 1,\ x^5 - x^4 - x^3 + x^2 + x - 1,$$

$$x^5 + x^4 + x^3 + x^2 - x - 1,\ x^5 + x^4 - x^3 + x^2 + x - 1,\ x^5 - x^4 - x^3 - x^2 + x - 1.$$

Computing the rational points on the curves (5.2) by the procedure `Chabauty0` of Magma, we obtained only solutions with $x = \pm 1$ and $y = 0$ in these cases.

Consider now the polynomials that yield rank 1 Mordell-Weil groups. These are given by

$$x^5 - x^4 - x^3 - x^2 - x - 1,\ x^5 - x^4 + x^3 - x^2 - x + 1,\ x^5 - x^4 - x^3 + x^2 - x - 1,$$

$$x^5 + x^4 + x^3 - x^2 - x + 1,\ x^5 - x^4 + x^3 + x^2 - x - 1,\ x^5 - x^4 - x^3 + x^2 - x + 1,$$

$$x^5 + x^4 + x^3 - x^2 + x - 1,\ x^5 - x^4 - x^3 - x^2 + x + 1,\ x^5 - x^4 + x^3 + x^2 + x - 1,$$

$$x^5 + x^4 - x^3 - x^2 + x + 1,\ x^5 + x^4 + x^3 + x^2 + x - 1,\ x^5 - x^4 + x^3 - x^2 + x + 1,$$

$$x^5 - x^4 - x^3 - x^2 - x + 1, \quad x^5 - x^4 - x^3 + x^2 + x + 1,$$
$$x^5 + x^4 - x^3 - x^2 - x + 1, \quad x^5 + x^4 + x^3 + x^2 + x + 1.$$

Now the Magma procedure `Chabauty` gives all the rational solutions of (5.2) in these cases. We obtain that only solutions with $|x| \le 2$ exist.

It remains to study the hyperelliptic curves defined by the polynomials

$$x^5 + x^4 - x^3 + x^2 - x + 1,\ x^5 + x^4 - x^3 + x^2 + x + 1,\ x^5 + x^4 + x^3 + x^2 - x + 1,$$
$$x^5 - x^4 + x^3 + x^2 + x + 1, \quad x^5 + x^4 + x^3 - x^2 + x + 1.$$

In all these cases the curves (5.2) have rank 2 Mordell-Weil groups, therefore classical Chabauty's method cannot be applied. In these cases we shall use the hyperelliptic logarithm method from [23]. We provide details only in case of the polynomial $x^5 + x^4 + x^3 + x^2 - x + 1$, all the other polynomials can be handled similarly. In this case the hyperelliptic curve (5.2) is given by

$$C: \quad y^2 = f(x) := x^5 + x^4 + x^3 + x^2 - x + 1. \tag{5.9}$$

A Magma computation using the procedures `TorsionSubgroup` and `MordellWeilGroupGenus2` yields that the Jacobian of C has trivial torsion, and it has a Mordell-Weil basis given by

$$D_1 = (0, -1) - \infty, \quad D_2 = (1, -2) - \infty.$$

As a next step, by means of Baker's method [1] we derive a (large) bound for $\log|x|$. Here we use the following improved version from [23].

Lemma 5.3.1 (Proposition 2.1 in [23])**.** *Let α be a root of $f(x)$. Assuming the knowledge of explicit generators for the Mordell–Weil group $J(C)(\mathbb{Q})$, there is a finite computable set $\mathcal{K}$ consisting of integers of $\mathbb{Q}[\alpha]$ such that if (x, y) is an integral solution to C, then $x - \alpha = \kappa\xi^2$ for some $\kappa \in \mathcal{K}$ and $\xi \in \mathbb{Q}[\alpha]$.*

Moreover, suppose $\kappa \in \mathcal{K}$. Let $\alpha_1, \alpha_2, \alpha_3$ be different conjugates of α, and let $\kappa_1, \kappa_2, \kappa_3$ be the corresponding conjugates of κ. Let $K_1 = \mathbb{Q}(\alpha_1, \alpha_2, \sqrt{\kappa_1\kappa_2})$, $K_2 = \mathbb{Q}(\alpha_1, \alpha_3, \sqrt{\kappa_1\kappa_3})$, $K_3 = \mathbb{Q}(\alpha_2, \alpha_3, \sqrt{\kappa_2\kappa_3})$ and $L = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \sqrt{\kappa_1\kappa_2}, \sqrt{\kappa_1\kappa_3})$. Then there is an explicitly computable constant B_κ depending on α and κ and the degrees, regulators, class numbers and unit ranks of the K_is, and the degree of L such that if $x \neq 0$ is an integer satisfying $x - \alpha = \kappa\xi^2$ for some $\xi \in \mathbb{Q}[\alpha]$, then $\log|x| \le B_\kappa$.

Hence, if (x, y) is an integral solution of C, then $\log|x| \le B := \max_{\kappa\in\mathcal{K}} B_\kappa$.

Importantly, the methods developed in [23] provide B in Lemma 5.3.1 explicitly indeed. To make the actual calculations, the worked out example [24] provided by Gallegos-Ruiz can be followed, as well. In case of our equation (5.9) we obtain the bound

$$\log|x| \le 4.56 \times 10^{319}.$$

If P is an integral point on C, then the image of P on the Jacobian of C can be expressed as

$$P - \infty = n_1 D_1 + n_2 D_2.$$

There are only finitely many integral points on C, so we may define M as

$$M = \max_{P \in C(\mathbb{Z})} \|n_P\| = \max_{P \in C(\mathbb{Z})} \sqrt{n_1^2 + n_2^2}.$$

To obtain an upper bound for M from the Baker bound we computed above we make use of Corollary 3.2 in [23]. To state the result we need to define μ_1, μ_2. From [21, Theorem 4] we can compute a lower bound for the height difference

$$\mu_1 \le h(D) - \hat{h}(D), \quad D \in J(C)(\mathbb{Q}).$$

(Here, as usual, h and $\hat{h}$ stand for the naive height and canonical height on $J(C)(\mathbb{Q})$, respectively.) Let us denote the eigenvalues of the height pairing matrix of the Mordell-Weil basis $\{D_1, D_2\}$ by λ_1, λ_2. Set $\mu_2 = \min\{\lambda_1, \lambda_2\}$. In our case the coefficient of x^5 is 1, so we have the following simplified version of Corollary 3.2 from [23].

Lemma 5.3.2 (simplified version of Corollary 3.2 in [23])**.** *Let B be an upper bound for the logarithmic height of integral points on C. Then*

$$M \le \sqrt{\mu_2^{-1}(2B - \mu_1)}.$$

The application of Lemma 5.3.2 to (5.9) yields that $M \le 1.28 \times 10^{160}$. It remains to reduce the bound following [23, Section 6] based on the LLL-algorithm (which results in many cases in a logarithmic improvement). To reduce the bound we set $K = 10^{600}$. The 6×6 matrix $\mathcal{A}_K$ mentioned in Proposition 6.2 in [23] is given by (with 800 digits of precision - here only the first three digits after the decimal point are indicated)

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ -1.097 \times K & -4.253 \times K & -2.893 \times K & 2.620 \times K & -1.173 \times K & -2.346 \times K \\ 0.679 \times K & -1.590 \times K & -4.538 \times K & -0.679 \times K & 2.269 \times K & 1.358 \times K \\ 5.308 \times K & 0.345 \times K & -8.490 \times K & 1.122 \times K & 3.123 \times K & 6.246 \times K \\ -2.180 \times K & -0.847 \times K & 2.664 \times K & 2.180 \times K & -1.332 \times K & -4.360 \times K \end{pmatrix}.$$

Proposition 6.2 yields a new bound 70.25 for $\|n_P\|$. Further reductions are applied with $K = 10^{20}$, 10^{14} and 10^{12} to get bounds 13.73, 11.88 and 11.06, respectively. After this procedure, it remains to enumerate all integral points with

$$\|n_P\| \le 11.06,$$

which can be done easily. These points are as follows:

$$(x, y) \in \{(0, \pm 1), (1, \pm 2)\}.$$

Altogether, we obtained that (5.2) with $n = 5$ has the only solutions given in the last two rows of Table 5.1.

5.3.3 Proof of Theorem 5.2.1 for n even with $2 \leq n \leq 24$

Let $f(x)$ be a Littlewood polynomial of even degree $n = 2k$ with $2 \leq n \leq 24$, and consider (5.2). In principle we have 2^{n+1} equations to solve. However, since $|x|^n > |x|^{n-1} + \ldots + |x| + 1$ when $|x| > 2$, we can immediately exclude the cases where the leading coefficient of $f(x)$ is -1, as otherwise there are no solutions with $|x| > 2$. Further, similarly as in cases $n = 3, 5$, using the substitution $x \to -x$ we can get rid of half of the equations. Namely, it is sufficient to study (5.2) only when $f(x)$ is of the shape

$$f(x) = x^n + x^{n-1} + e_2 x^{n-2} + \cdots + e_{n-1}x + e_n$$

with $e_2, \ldots, e_n \in \{-1, 1\}$. This means that we need to consider 2^{n-1} equations only. To solve these equations, we shall follow Runge's method. We do not outline the general method here, however, we shall give all the details required to keep the presentation self-contained. Beside this, we shall illustrate our method by an example, too. For more details on Runge's method, its implementation and its applications, see e.g. [63], [9], Chapter 2 of [64] and Chapter 4 of [45] and the references there. We used the program package SageMath [51] for our computations.

First, we shall need the polynomial part of the Puiseux expansion of $\sqrt{f(x)}$ at ∞. The following statement, which we hope to be useful in later investigations as well, provides this in a general form.

Proposition 5.3.1. *Let*

$$f(x) = x^n + e_1 x^{n-1} + \cdots + e_{n-1}x + e_n \tag{5.10}$$

be a Littlewood polynomial of even degree $n = 2k$. Then there exists a uniquely determined polynomial

$$u(x) = u_0 x^k + u_1 x^{k-1} + \cdots + u_{k-1}x + u_k \tag{5.11}$$

with $u_0 = 1$ and $u_i \in \mathbb{Q}$ $(i = 1, \ldots, k)$ such that the coefficients of the terms x^i in $f(x)$ and $u^2(x)$ are the same for $i = k, k+1, \ldots, n$. Further, for the denominators d_i of the coefficients u_i of $u(x)$ we have

$$d_i = 2^{\nu_2((2i)!)} \quad (i = 0, 1, \ldots, k), \tag{5.12}$$

where $\nu_2(\ell)$ denotes the exponent of 2 in the prime factorization of a positive integer ℓ.

Proof. By formula (3.1) on p. 481 of [52] the coefficients of $u(x)$ are uniquely determined, and are given by

$$u_i = \sum_{s=1}^{i} \binom{1/2}{s} {\sum}' \frac{s!}{j_1! \ldots j_n!} e_1^{j_1} \ldots e_n^{j_n} \quad (i = 0, 1, \ldots, k),$$

where $\sum'$ is taken over all tuples $(j_1, \dots, j_n)$ such that $j_1 + \dots + j_n = s$ and $j_1 + 2j_2 + \dots + nj_n = i$. (Here, as usual, $\binom{r}{s}$ is defined as $r(r-1)\dots(r-s+1)/s!$ for $r \in \mathbb{R}$.) This shows that the u_i are rational numbers. Observe that the terms in the inner sum $\sum'$ are integers. In particular, as for $s = i$ we must have $j_1 = i$ and $j_2 = \dots = j_n = 0$, this integer is ± 1 in this case. Thus the denominator d_i of u_i is the same as that of $\binom{1/2}{i}$ $(i = 0, 1, \dots, k)$. As one can easily check, this denominator is given by $2^{\nu_2(i!)+i} = 2^{\nu_2((2i)!)}$. Hence our claim follows. □

Observe that writing $f(x)$ as

$$f(x) = F(x) + g(x) \tag{5.13}$$

with

$$F(x) = x^n + x^{n-1} + e_2 x^{n-2} + \dots + e_{n-k}x^k, \ g(x) = e_{n-k+1}x^{k-1} + \dots + e_{n-1}x + e_n,$$

the polynomial $u(x)$ provided by Proposition 5.3.1 depends only on $F(x)$, it is independent of $g(x)$. This is extremely important for our purposes. Indeed, in this way we shall need to loop through only the possible choices of $F(x)$, which means that we can reduce the number of cases to be considered down to 2^{k-1}. (Though certainly, we also need to take care of the polynomials $g(x)$ appearing in (5.13). However, as we shall see, this can be done relatively easily.)

Let $t = 2^{-\nu_2(n!)}$. Observe that the polynomials $(u(x) - t)^2 - f(x)$ and $(u(x) + t)^2 - f(x)$ are of degree k, with leading coefficients $-2t$ and $2t$, respectively. This implies that there is a constant C (to be discussed later) such that for $|x| > C$ we have that either

$$(u(x) - t)^2 < f(x) < (u(x) + t)^2 \tag{5.14}$$

or

$$(u(x) + t)^2 < f(x) < (u(x) - t)^2 \tag{5.15}$$

is valid. Multiplying by $2^{2\nu_2(n!)-2}$, (5.14) and (5.15) yield

$$(2^{\nu_2(n!)-1}u(x) - 2^{\nu_2(n!)-1}t)^2 < 2^{2\nu_2(n!)-2}f(x) < (2^{\nu_2(n!)-1}u(x) + 2^{\nu_2(n!)-1}t)^2$$

and

$$(2^{\nu_2(n!)-1}u(x) + 2^{\nu_2(n!)-1}t)^2 < 2^{2\nu_2(n!)-2}f(x) < (2^{\nu_2(n!)-1}u(x) - 2^{\nu_2(n!)-1}t)^2,$$

respectively. By Proposition 5.3.1 we see that $1/t$ is just the denominator of u_k, and that the denominators of all the other coefficients of $u(x)$ are powers of 2, with exponents strictly less than $\nu_2(n!)$. Thus the left and right hand sides of the above inequalities are integer polynomials of x. Further, we have

$$(2^{\nu_2(n!)-1}u(x) + 2^{\nu_2(n!)-1}t) - (2^{\nu_2(n!)-1}u(x) - 2^{\nu_2(n!)-1}t) = 1.$$

That is, $2^{2\nu_2(n!)-2}f(x)$ is between two consecutive (integer) squares in both cases, thus it cannot be a square. But then the same is true for $f(x)$. That is, $f(x)$ cannot be a square for $|x| > C$, or in other words, (5.2) has no solutions with $|x| > C$.

So we are left with the following tasks: find an appropriate C, and check the integer values of x with $2 < |x| \leq C$. For this, we may assume that neither (5.14), nor (5.15) is valid. (Indeed, if either (5.14) or (5.15) holds, then as we have seen, x cannot yield a solution to (5.2).) Fix $F(x)$ in (5.13). Then, as we have pointed out earlier, $u(x)$ is also fixed. Think of $g(x)$ in (5.13) as an arbitrary, but fixed Littlewood polynomial of degree $k-1$. Put

$$h_1(x) = (u(x) - t)^2 - F(x) - g(x),\ h_2(x) = (u(x) + t)^2 - F(x) - g(x). \tag{5.16}$$

Then $h_1(x), h_2(x)$ are polynomials of degree k, with leading coefficients $-2t$ and $2t$, respectively. Since (5.14) is not valid, we have

$$h_1(x) \geq 0 \quad \text{or} \quad h_2(x) \leq 0,$$

and as (5.15) is false,

$$h_1(x) \leq 0 \quad \text{or} \quad h_2(x) \geq 0.$$

From these we easily see that $|x| \leq \max(C_1, C_2)$, where C_i is the maximum of the absolute values of the roots of $h_i(x)$ for $i = 1, 2$. So we can take $C = \max(C_1, C_2)$. To get upper bounds for the values of C_1 and C_2, we use the following lemma.

Lemma 5.3.3. *Let $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be a polynomial with complex coefficients, with $a_n \neq 0$. The absolute values of all the roots of this polynomial can be bounded from above both by*

$$1 + \max\left\{\left|\frac{a_{n-1}}{a_n}\right|, \left|\frac{a_{n-2}}{a_n}\right|, \ldots, \left|\frac{a_0}{a_n}\right|\right\}.$$

and by

$$2\max\left\{\left|\frac{a_{n-1}}{a_n}\right|, \left|\frac{a_{n-2}}{a_n}\right|^{\frac{1}{2}}, \ldots, \left|\frac{a_1}{a_n}\right|^{\frac{1}{n-1}}, \left|\frac{a_0}{2a_n}\right|^{\frac{1}{n}}\right\}.$$

The bound above is due to Cauchy [15]. Certainly there exist other bounds for the roots of real zeros of polynomials like the one obtained by Fujiwara [22]. 'In general', Fujiwara's bound is better. However, our computations show that for our purposes the factor 2 in Fujiwara's bound makes the bound of Cauchy much better for us in the considered range. So to get C_1 and C_2 (and then C) we apply the following procedure. Fix $F(x)$; then t and $u(x)$ are also fixed, as well as the polynomials $(u(x) - t)^2 - F(x)$ and $(u(x) + t)^2 - F(x)$. Thus the absolute values of the coefficients of $h_1(x)$ and $h_2(x)$ defined by (5.16) can be easily bounded: the leading coefficients are $-2t$ and $2t$, respectively, while the absolute values of the coefficients of x^j with $0 \leq j < k$ are at most one larger than those of the polynomials $(u(x) - t)^2 - F(x)$ and $(u(x) + t)^2 - F(x)$, respectively. So fixing $F(x)$, we can get an upper bound for the Cauchy bound both in case of h_1 and h_2. In this way we obtain a constant C such that if x, y is a solution to equation (5.2), then $|x| \leq C$ must be valid. Importantly, observe that this C is uniformly valid for any $f(x)$ having the fixed $F(x)$ part in (5.13). We illustrate what we did so far with an example.

Example. Let $n = 6$, and take a Littlewood polynomial $f(x)$ with $F(x) = x^6+x^5-x^4-x^3$. Then by (5.13) we have

$$f(x) = x^6 + x^5 - x^4 - x^3 + g(x),$$

where $g(x)$ is a Littlewood polynomial of degree 2. Proposition 5.3.1 gives

$$u(x) = x^3 + \frac{1}{2}x^2 - \frac{5}{8}x - \frac{3}{16}.$$

So we have $t = 1/16$, while (5.14) and (5.15) read as

$$\left(x^3 + \frac{1}{2}x^2 - \frac{5}{8}x - \frac{2}{8}\right)^2 < x^6 + x^5 - x^4 - x^3 + g(x) < \left(x^3 + \frac{1}{2}x^2 - \frac{5}{8}x - \frac{1}{8}\right)^2$$

and

$$\left(x^3 + \frac{1}{2}x^2 - \frac{5}{8}x - \frac{1}{8}\right)^2 < x^6 + x^5 - x^4 - x^3 + g(x) < \left(x^3 + \frac{1}{2}x^2 - \frac{5}{8}x - \frac{2}{8}\right)^2,$$

respectively. Expanding the above inequalities, we obtain

$$-\frac{1}{8}x^3 + \frac{9}{64}x^2 + \frac{5}{16}x + \frac{1}{16} < g(x) < \frac{1}{8}x^3 + \frac{17}{64}x^2 + \frac{5}{32}x + \frac{1}{64}$$

or

$$\frac{1}{8}x^3 + \frac{17}{64}x^2 + \frac{5}{32}x + \frac{1}{64} < g(x) < -\frac{1}{8}x^3 + \frac{9}{64}x^2 + \frac{5}{16}x + \frac{1}{16}.$$

By $\deg(g) = 2$ one of them is certainly valid if $|x| > C$ for some C. However, multiplying them by $2^{2\nu_2(n!)-2} = 8^2$, we get

$$(8x^3 + 4x^2 - 5x - 2)^2 < 64(x^6 + x^5 - x^4 - x^3 + g(x)) < (8x^3 + 4x^2 - 5x - 1)^2$$

or

$$(8x^3 + 4x^2 - 5x - 1)^2 < 64(x^6 + x^5 - x^4 - x^3 + g(x)) < (8x^3 + 4x^2 - 5x - 2)^2$$

respectively. This shows that $64f(x)$ cannot be a square, whence $f(x)$ cannot be a square - so (5.2) has no solutions with $|x| > C$. Now we need to find an appropriate C. For the polynomials h_1, h_2 defined by (5.16) we obtain

$$h_1(x) = -\frac{1}{8}x^3 + \frac{9}{64}x^2 + \frac{5}{16}x + \frac{1}{16} - g(x)$$

and

$$h_2(x) = \frac{1}{8}x^3 + \frac{17}{64}x^2 + \frac{5}{32}x + \frac{1}{64} - g(x).$$

For the Cauchy bounds of h_1, h_2 we get

$$11.5, \quad 11.125,$$

respectively. Hence

$$C = \max(11.5, 11.25) = 11.5.$$

This bound can be used for all $f(x)$ with $F(x)$ part $F(x) = x^6 + x^5 - x^4 - x^3$ in (5.13).

After establishing C, the only remaining task is to check the integers x with $2 < |x| \leq C$ whether they yield a solution to (5.2). For this, one may use Stoll's `ratpoints` code [61] to compute all "small" points on a hyperelliptic curve. We used the function `hyperellratpoints` the PARI [47] implementation of Stoll's code.

We mention that the total running times (and also the largest Cauchy's bound) on a HPC supercomputer using 128 cores parallel for each degree (between 12 and 24, we omit the low degree cases) were the following:

n (degree)	12	14	16	18	20	22	24
running time	1.04 s	1.3 s	2.67 s	10.5 s	39.7 s	2 min 42 s	28 min 28 s
the largest bound C	5374	19712	671205	3341457	36063346	204015976	4792168585

5.4 The proof of Proposition 5.2.1

Here we directly applied the previously mentioned PARI version of Stoll's `ratpoints` code on a HPC supercomputer using 128 cores. We mention that the total running times for each degree (between 7 and 17) were the following:

n (degree)	7	9	11	13	15	17
running time	529 ms	2.19 s	9.55 s	41.9 s	3 min 32 s	24 min 17 s

The code and the outputs can be downloaded from `https://shrek.unideb.hu/~tengely/LittleWoodOdd.html`.

Chapter 6

Summary

In this dissertation we studied various polynomial Diophantine equations, where the polynomials considered belong to some specific family with some interesting and/or important feature.

Our research can be divided into three parts. Here we briefly summarize our results and their background.

The first topic we studied is the following: what can we say about the number of integral points in some 'interesting' sets (e.g., in certain regular solids)? In particular, we focused on the following solids: n-dimensional cube, pyramid and simplex. Counting the integral points in these objects, one finds (see [17]) that the following polynomials arise, respectively:

$$(x+1)^n, \quad S_{n-1}(x) := 1^{n-1} + \cdots + (x+1)^{n-1}, \quad \binom{x+n}{n}. \tag{6.1}$$

Here n is the dimension, and x describes the size of the solid. Equations of type

$$f(x) = g(y) \tag{6.2}$$

where $f(x)$ belongs to one of the families in (6.1) and $g(y)$ is a polynomial with integer coefficients, have been heavily studied in the literature, by several authors. For $f(x) = (x+1)^n$ equation (6.2) is just a hyperelliptic equation (see e.g. the corresponding chapter of Shorey and Tijdeman [57] or the theorem of Brindza [14]; for $f(x) = S_{n-1}(x)$ equation (6.2) has been considered by Rakaczki [49]; when $f(x) = \binom{x+n}{n}$ then (6.2) has been studied by Kulkarni and Sury [42]. In every case it turns out that (apart from certain well-described cases), (6.2) has only finitely many solutions. Here we considered the problem of counting integral points not *in the interior*, rather *on the surface* of these solids. As it turned out, the number of such integral points (in the above settings) are described by the polynomials

$$(x+1)^n - (x-1)^n, \quad (x+1)^{n-1} + x^{n-1}, \quad \binom{x+n}{n} - \binom{x-1}{n},$$

respectively. We studied equation (6.2) for polynomials coming from the above families. We proved that (apart from certain special, completely described cases) (6.2) allows only finitely many integer solutions x, y, moreover, if $g(y)$ is of the shape $g(y) = Ay^\ell + B$, then $\max(\ell, |x|, |y|)$ is bounded by a constant depending only on the parameters involved.

The starting point of the next topic we studied is a classical theorem of Erdős and Selfridge [20]: the product of two or more consecutive positive integers cannot be a perfect power. This problem has been extended into various directions. One of the most important generalizations concerns the problem of perfect powers in products of consecutive terms of arithmetic progressions. There are a huge amount of papers devoted to this question (see, for example, the paper by Győry, Hajdu and Pintér [27] for the case of at most 34 terms, and the references given there) - however, it is still unsolved. In most related results, naturally, the strong structure of the underlying arithmetic progression is of utmost importance. It is an interesting question how far one can 'disturb' this structure still to have definitive (finiteness) results. See for example a recent paper by Hajdu, Papp and Tijdeman [36] where equation (6.2) is studied for polynomials f having roots from an arithmetic progressions - however, these roots are not (necessarily) consecutive terms, some terms of the progression are omitted. (In the literature one can find various related results, see e.g. the references in [36].) In the fourth chapter of the dissertation we approached the problem from another, new direction. Namely, we kept the symmetry of the roots of $f(x)$, however, we allowed arbitrarily large gaps among them. More precisely, we proved that if the roots of $f(x)$ form a symmetric, convex set then (6.2) has only finitely many integer solutions x, y.

Finally, in the fifth chapter of the dissertation we studied square values of Littlewood polynomials, i.e. polynomials with all coefficients equal to ± 1. In fact, this means that we consider equation (6.2) for $f(x)$ being a Littlewood polynomial and $g(y) = y^2$. The polynomial values of Littlewood polynomials, from the point of finiteness of solutions, have already been studied by Hajdu, Tijdeman and Varga [37]. Further, the problem is a generalization of the famous Nagell-Ljunggren equation

$$\frac{x^n - 1}{x - 1} = y^\ell$$

in the case $\ell = 2$. The above equation has been studied by many mathematicians, in several papers. A classical result of Ljunggren [44] gives that for $\ell = 2$ the only solutions are $(x, y, n) = (7, \pm 20, 4)$. Here we shall be interested in finding *all solutions* of the equation. Combining various methods (e.g. the theory of elliptic curves, hyperelliptic curves and Runge's method), we succeeded to list all solutions in cases $n = 3, 5$ and $2 \leq n \leq 24$, n even. Beside this, we gathered some information for the case of n odd with

$n \leq 17$. Based upon the data obtained, we could formulate some striking questions for further research, as well.

In the proofs of our results, we needed to combine several deep tools, among others Baker's method and a celebrated theorem of Bilu and Tichy [12], guaranteeing the finiteness of the number of integral solutions of equations of the shape $f(x) = g(y)$.

Chapter 7

Összefoglaló

(Hungarian summary)

A disszertációban különböző polinomiális diofantikus egyenleteket tanulmányoztunk, ahol a vizsgált polinomok valamilyen specifikus, érdekes és/vagy fontos tulajdonsággal rendelkező családhoz tartoznak.

Kutatásunk három részre osztható. A következőkben áttekintjük eredményeinket és ezek hátterét.

Az első téma, amit tanulmányoztunk, a következő: mit mondhatunk az egész pontok számáról bizonyos „érdekes" halmazokban (például egyes szabályos testekben)? Leginkább az n-dimenziós kockára, gúlára és szimplexre koncentráltunk. Ezeket a testeket vizsgálva azt kapjuk (lásd [17]), hogy a testekben lévő egész pontok száma rendre a

$$(x+1)^n, \quad S_{n-1}(x) := 1^{n-1} + \cdots + (x+1)^{n-1}, \quad \binom{x+n}{n} \tag{7.1}$$

polinomokkal írható le, ahol n a dimenzió és x a test méretét írja le. Sokan tanulmányozták már az

$$f(x) = g(y) \tag{7.2}$$

egyenletet, ahol $f(x)$ a (7.1) polnomcsaládok egyike, $g(y)$ pedig egész együtthatós polinom. A (7.2) egyenlet $f(x) = (x+1)^n$-re a hiperelliptikus egyenlet (lásd például Shorey és Tijdeman [57] könyvének kapcsolódó fejezeteit vagy Brindza [14] tételét). Amikor $f(x) = S_{n-1}(x)$, a (7.2) egyenletet Rakaczki [49] tanulmányozta. Abban az esetben pedig, amikor $f(x) = \binom{x+n}{n}$, a (7.2) egyenletet Kulkarni and Sury [42] vizsgálta. Minden esetben (pár jól meghatározott kivételtől eltekintve) a (7.2) egyenletnek csak véges sok megoldása van. Mi most ezeknek a testeknek nem a *belsejében* hanem a *felületén* található egész pontok számlálásának a problémájával foglalkoztunk. Az említett testeket vizsgálva azt kaptuk, hogy az egész pontok száma rendre az

$$(x+1)^n-(x-1)^n, \quad (x+1)^{n-1}+x^{n-1}, \quad \binom{x+n}{n}-\binom{x-1}{n}$$

polinomokkal írható le. A (7.2) egyenletet olyan polinomokra vizsgáltuk, melyek a fenti polinomcsaládok valamelyikének a tagjai. Igazoltuk, hogy (pár, jól meghatározott kivételtől eltekintve) a (7.2) egyenletnek csak véges sok megoldása lehet x, y egészekre. Továbbá, ha $g(y)$ pedig $g(y) = Ay^\ell + B$ alakú, akkor $\max(\ell, |x|, |y|)$ is korlátozható egy konstanssal, mely csak az egyenletben szereplő paraméterektől függ.

A következő témánk kiindulópontja Erdős és Selfridge [20] egy klasszikus tétele: két vagy több egymást követő pozitív egész szám szorzata nem lehet teljes hatvány. Ennek a problémának több különböző kiterjesztése is ismert. Az egyik legfontosabb általánosítása a teljes hatványok meghatározása számtani sorozatok egymást követő tagjainak szorzatában. Számtalan cikk született a kérdés kutatása során (lásd például legfeljebb 34 tagú szorzatok esetére Győry, Hajdu és Pintér [27] cikkét és az ott szereplő hivatkozásokat) - azonban a probléma megoldatlan maradt. Értelemszerűen, a legtöbb kapcsolódó kutatásban kiemelt jelentőségű a probléma hátterét adó számtani sorozatok erős struktúrája. Érdekes lehet az a kérdés is, hogy mennyire lehet „megzavarni” ezt a struktúrát úgy, hogy hasonló végességi eredményeket kapjunk. Lásd pédául Hajdu, Papp és Tijdeman [36] egy friss cikkét, amiben a (7.2) egyenletet olyan f polinomokra vizsgálták, melyek gyökei egy számtani sorozat tagjai - azonban, ezek a gyökök nem feltétlen egymást követő tagok, a sorozat pár tagját elhagyják. (Az irodalomban több, ehhez hasonló eredmény található, lásd például a [36]-ban szereplő hivatkozásokat.) A disszertáció negyedik fejezetében egy másfajta, új irányból közelítettük meg a problémát. Tettük ezt úgy, hogy megtartottuk az $f(x)$ gyökeinek a szimmetriáját, de megengedtünk tetszőlegesen nagy különbségeket közöttük. Pontosabban, azt igazoltuk, hogy ha $f(x)$ gyökei szimmetrikus, konvex halmazt alkotnak, akkor a (7.2) egyenletnek csak véges sok megoldása van x, y egészekben.

Végül, a disszertáció ötödik fejezetében a Littlewood polinomok, azaz a ± 1 együtthatójú polinomok négyzet értékeit vizsgáltuk. Valójában ez a (7.2) egyenletet vizsgálatát jelenti, ahol $f(x)$ egy Littlewood polinom és $g(y) = y^2$. A megoldások számának végessége szempontjából a Littlewood polinomok polinomértékeit Hajdu, Tijdeman és Varga [37] már tanulmányozták. Továbbá, a probléma a híres

$$\frac{x^n-1}{x-1} = y^\ell$$

Nagell-Ljunggren egyenlet egy általánosítása $\ell = 2$ esetben. A fenti egyenletet sok matematikus vizsgálta már. Ljunggren [44] egy klasszikus eredménye szerint $\ell = 2$ esetén az egyedüli megoldás $(x, y, n) = (7, \pm 20, 4)$. Mi az egyenlet összes megoldásának leírására törekedtünk. Különböző módszerek (például elliptikus görbék, hiperelliptikus görbék, Runge-módszer) kombinálásával sikerült megadnunk az összes megoldást abban az esetben, amikor $n = 3, 5$, illetve $2 \leq n \leq 24$ és n páros. Emellett, $n \leq 17$ és n páratlan estén is hasznos információkat gyűjtöttünk össze. A vizsgálatok során nyert eredmények alapján több kérdést is meg tudtunk fogalmazni, melyek további kutatások tárgyát képezhetik.

Eredményeink igazolása során, több mély módszer kombinálására volt szükségünk. Többek között a Baker módszerre és Bilu és Tichy [12] híres tételére, amely az $f(x) = g(y)$ alakú egyenletek egész megoldásai számának végességét garantálja.

References

[1] A. Baker, *Bounds for the solutions of hyperelliptic equations*, Proc. Camb. Phil. Soc. **65** (1969), 439–444.

[2] A. Baker, *Transcendental Number Theory*, Cambridge University Press, 1975.

[3] P. Balister, B. Bollobás, R. Morris, J. Sahasrabudhe, M. Tiba, *Flat Littlewood polynomials exist*, Annals Math. **19** (2020), 977–1004.

[4] A. Bazsó, *Polynomial values of (alternating) power sums*, Acta Math. Hung. **146** (2015), 202–219.

[5] A. Bazsó, I. Pink, *Diophantine equations with Appell sequences*, Period. Math. Hung. **69** (2014), 222–230.

[6] M. A. Bennett, K. Győry, Á. Pintér, *On the Diophantine equation* $1^k+2^k+\cdots+x^k = y^n$, Compositio Math. **140** (2004), 1417–1431.

[7] M. A. Bennett, A. Levin, *The Nagell–Ljunggren equation via Runge's method*, Monatsh. Math. **177** (2015), 15–31.

[8] A. Bérczes, B. Brindza, L. Hajdu, On the power values of polynomials, Publ. Math. Debrecen **53** (1998), 375–381.

[9] F. Beukers, Sz. Tengely, *An implementation of Runge's method for Diophantine equations*, arXiv:math/0512418 [math.NT], 2005.

[10] Yu. Bilu, *Quadratic factors of* $f(x) = g(y)$, Acta Arith. **90** (1999), 341–355.

[11] Yu. Bilu, B. Brindza, P. Kirschenhofer, Á. Pintér, R. F. Tichy, *Diophantine equations and Bernoulli polynomials. With an appendix by A. Schinzel*, Compositio Math. **131** (2002), 173–188.

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

[13] W. Bosma, J. Cannon, C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), 235–265.

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

[15] A.-L. Cauchy, *Exercices de mathématique*, Œuvres **2(9)** (1829), p.122.

[16] C. Chabauty, *Sur les points rationnels des courbes algébriques de genre supérieur à l'unité*, C. R. Acad. Sci. Paris **212** (1941), 882–885.

[17] M. Deza, E. Deza, *Encyclopedia of distances*, Springer, 2009

[18] A. Dubickas, J. Jankauskas, *On Newman polynomials which divide no Littlewood polynomial*, Math. Comp. **78** (2009), 327–344.

[19] P. Erdős, *On a Diophantine equation*, J. London Math. Soc. **26** (1951), 176–178.

[20] P. Erdős, J. L. Selfridge, *The product of consecutive integers is never a power*, Ill. J. Math. **19** (1975), 292–301.

[21] E. V. Flynn and N. P. Smart, *Canonical heights on the Jacobians of curves of genus 2 and the infinite descent*, Acta Arith. **79(4)** (1997), 333–352.

[22] M. Fujiwara, M. *Über die obere Schranke des absoluten Betrages der Wurzeln einer algebraischen Gleichung*, Tohoku Math. J. (first series) **10** (1916), 167–171.

[23] H. R. Gallegos-Ruiz, *Computing integral points on genus 2 curves estimating hyperelliptic logarithms*, Acta Arith. **187** (2019), 329–344.

[24] H. R. Gallegos-Ruiz, *Worked out example for my paper: Computing integral points on genus 2 curves estimating hyperelliptic logarithms*, http://personal.cimat.mx:8181/~hgallegos/programs/hyperlogs/WorkedExample.pdf.

[25] J. Gebel, A. Pethő, H. G. Zimmer, *Computing integral points on elliptic curves*, Acta Arith. **68** (1994), 171–192.

[26] K. Győry, *On the Diophantine equation $\binom{n}{k} = x^\ell$*, Acta Arith. **80** (1997), 289–295.

[27] K. Győry, L. Hajdu, Á. Pintér, *Perfect powers from products of consecutive terms in arithmetic progression*, Compositio Math. **145** (2009), 845–864.

[28] K. Győry, T. Kovács, Gy. Péter, Á. Pintér, *Equal values of standard counting polynomials*, Publ. Math. Debrecen **84** (2014), 259–277.

[29] K. Győry, Á. Pintér, *On the equation $1^k + 2^k + \cdots + x^k$*, Publ. Math. Debrecen **62** (2003), 403–414.

[30] K. Győry, R. Tijdeman, M. Voorhoeve, *On the equation $1^k + 2^k + \cdots + x^k = y^z$*, Acta Arith. **37** (1980), 233–240.

[31] L. Hajdu, *On a conjecture of Schäffer concerning the equation* $1^k + ... + x^k = y^n$, J. Number Theory **155** (2015), 129–138. Corrigendum: ibid **164** (2016) 429–432.

[32] L. Hajdu, O. Herendi, *Polynomial values of surface point counting polynomials*, Int. J. Number Theory **17/01** (2021), 15–32.

[33] L. Hajdu, O. Herendi, *Extrema of polynomials with real roots and diophantine equations*, J. Number Theory **242** (2023), 626–646.

[34] L. Hajdu, O. Herendi, Sz. Tengely, N. Varga, *Square values of Littlewood polynomials*, The Ramanujan Journal **65(3)** (2024), 1205–1226.

[35] L. Hajdu, Á. Papp, *Polynomial values of products of terms from an arithmetic progression*, Monatsh. Math. **193** (2020), 637–655.

[36] L. Hajdu, Á. Papp, R. Tijdeman, *The Prouhet-Tarry-Escott problem, indecomposability of polynomials and Diophantine equations*, Ramanujan J. **58** (2022), 1075–1093.

[37] L. Hajdu, R. Tijdeman, N. Varga, *Diophantine equations for Littlewood polynomials*, Acta Arith. **210** (2023), 223–234.

[38] L. Hajdu, N. Varga, *Polynomial values of figurate numbers*, J. Number Theory **214** (2020), 79–99.

[39] L. Hajdu, N. Varga, *Diophantine equations for polynomials with restricted coefficients, I (power values)*, Bull. Austral. Math. Soc. **106** (2022), 254–263.

[40] X. Han, A. Schied, *Step roots of Littlewood polynomials and the extrema of functions in the Takagi class*, Math. Proc. Cambridge Phil. Soc. **173** (2022), 591–618.

[41] K. G. Hare, J. Jankauskas, *On Newman and Littlewood polynomials with a prescribed number of zeros inside the unit disk*, Math. Comp. **90** (2021), 831–870.

[42] M. Kulkarni, B. Sury, *On the Diophantine equationv*$x(x+1)(x+2)\dots(x+(m-1)) = g(y)$, Indag. Math. (N.S.) **14** (2003), 35–44.

[43] K. Liptai, F. Luca, Á. Pintér, L. Szalay, *Generalized balancing numbers*, Indag. Math. (N.S.) **20** (2009), 87–100.

[44] W. Ljunggren, *Noen Setninger om ubestemte likninger av formen* $(x^n-1)/(x-1) = y^q$, Norsk. Mat. Tidsskr. **25** (1943), 17–20.

[45] D. Masser, *Auxiliary Polynomials in Number Theory*, Cambridge University Press, 2016.

[46] M. J. Mossinghoff, *Polynomials with Restricted Coefficients and Prescribed Noncyclotomic Factors*, LMS J. Comp. Math. **6** (2003), 314–325.

[47] The PARI Group, PARI/GP version `2.15.4`, Univ. Bordeaux, 2023, `http://pari.math.u-bordeaux.fr/`.

[48] R. Peled, A. Sen, O. Zeitouni, *Double roots of random Littlewood polynomials*, Israel J. Math. **213** (2016), 55–77.

[49] Cs. Rakaczki, *On the Diophantine equation $S_m(x) = g(y)$*, Publ. Math. Debrecen **65** (2004), 439–460.

[50] C. Runge, *Über ganzzahlige Lösungen von Gleichungen zwischen zwei Veränderlichen*, J. reine angew. Math. **100** (1887), 425–435.

[51] SageMath, the Sage Mathematics Software System (Version 9.8), The Sage Developers, 2023, https://www.sagemath.org.

[52] A. Sankaranarayanan, N. Saradha, *Estimates for the solutions of certain Diophantine equations by Runge's method*, Int. J. Number Theory **4** (2008), 475–493.

[53] N. Saradha, T. N. Shorey, *Almost perfect powers in arithmetic progression*, Acta Arith. **99** (2001), 363–388.

[54] N. Saradha, T. N. Shorey, *Almost squares and factorizations in consecutive integers*, Compositio Math. **138** (2003), 113–124.

[55] J. J. Schäffer, *The equation $1^p + 2^p + \cdots + n^p = m^q$*, Acta Math. **95** (1956), 155–189.

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

[57] T. N. Shorey and R. Tijdeman, *Exponential Diophantine equations*, Cambridge University Press, Cambridge, 1986.

[58] M. Stoll, *On the height constant for curves of genus two*, Acta Arith. **90** (1999), 183–201.

[59] M. Stoll, *Implementing 2-descent for Jacobians of hyperelliptic curves*, Acta Arith. **98** (2001), 245–277.

[60] M. Stoll, *On the height constant for curves of genus two. II*, Acta Arith. **104** (2002), 165–182.

[61] M. Stoll, *Documentation for the ratpoints program*, arXiv 0803.3165 (2022).

[62] R. J. Stroeker, N. Tzanakis, *Solving elliptic diophantine equations by estimating linear forms in elliptic logarithms*, Acta Arith. **67** (1994), 177–196.

[63] Sz. Tengely, *On the Diophantine equation $F(x) = G(y)$*, Acta Arith. **110** (2003), 185–200.

[64] Sz. Tengely, *Effective Methods for Diophantine Equations*, Ph.D. thesis, Leiden University, The Netherlands, 2005.

[65] R. Tijdeman, *Applications of the Gel'fond-Baker method to rational number theory*, Topics in Number Theory, Proceedings of the Conference at Debrecen 1974, Colloq. Math. Soc. János Bolyai **13**, pp. 399–416, North-Holland, Amsterdam, 1976.

[66] M. Voorhoeve, K. Győry, R. Tijdeman, *On the Diophantine equation* $1^k + 2^k + \cdots + x^k + R(x) = y^z$, Acta Math. **143** (1979), 1–8.

[67] E.T. Whittaker, G.N. Watson, *A Course of Modern Analysis*, 4th ed., Cambridge Univ. Press, Cambridge, 1927.

[68] O. Yakir, *Approximately half of the roots of a random Littlewood polynomial are inside the disk*, Studia Math. **261** (2021), 227–240.

[69] P. Z. Yuan, *On a special Diophantine equation* $a\binom{x}{n} = by^r + c$, Publ. Math. Debrecen **44** (1994), 137–143.

Publications and conference talks of Orsolya Herendi

Publications

1. L. Hajdu, O. Herendi, *Polynomial values of surface point counting polynomials*, Int. J. Number Theory **17/01** (2021), 15–32.
2. L. Hajdu, O. Herendi, *Extrema of polynomials with real roots and diophantine equations*, J. Number Theory **242** (2023), 626–646.
3. L. Hajdu, O. Herendi, Sz. Tengely, N. Varga, *Square values of Littlewood polynomials*, The Ramanujan Journal **65(3)** (2024), 1205–1226.

Conference talks

1. TDK (Scientific Student Association) Conference 2018, Debrecen, *Polynomial values of surface point counting polynomials*
2. OTDK (National Scientific Student Association) Conference 2019, Eger, *Polynomial values of surface point counting polynomials*
3. 24th CENT 2019, Komarno, *Polynomial values of surface point counting polynomials*
4. Number Theory Seminar 2019, *Polynomial values of surface point counting polynomials*
5. Research Seminar 'Diophantine Number Theory' 2021, *Finiteness results for polynomial values of surface point counting polynomials*