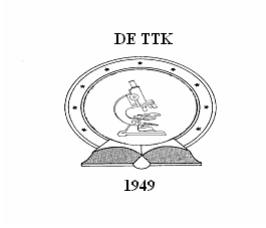


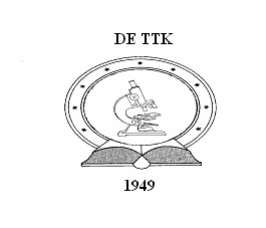
Combinatorial Diophantine equations

Egyetemi doktori (PhD) értekezés

Szerző: Kovács Tünde

Témavezető: Dr. Hajdu Lajos

Debreceni Egyetem
Természettudományi Doktori Tanács
Matematika- és Számítástudományok Doktori Iskola
Debrecen, 2011.



Combinatorial Diophantine equations

Egyetemi doktori (PhD) értekezés

Szerző: Kovács Tünde

Témavezető: Dr. Hajdu Lajos

Debreceni Egyetem
Természettudományi Doktori Tanács
Matematika- és Számítástudományok Doktori Iskola
Debrecen, 2011.

Ezen értekezést a Debreceni Egyetem Természettudományi Doktori Tanács *Matematika- és Számítástudományok* Doktori Iskola *Diofantikus és Konstruktív Számelmélet* programja keretében készítettem a Debreceni Egyetem természettudományi doktori (PhD) fokozatának elnyerése céljából.

Debrecen, 2011. június 20.

_____

a jelölt aláírása

Tanúsítom, hogy *Kovács Tünde* doktorjelölt 2008. szeptember – 2011. június között a fent megnevezett Doktori Iskola *Diofantikus és Konstruktív Számelmélet* programjának keretében irányításommal végezte munkáját. Az értekezésben foglalt eredményekhez a jelölt önálló alkotó tevékenységével meghatározóan hozzájárult. Az értekezés elfogadását javaslom.

Debrecen, 2011. június 20.

_____

a témavezető aláírása

Combinatorial Diophantine equations

Értekezés a doktori (PhD) fokozat megszerzése érdekében
a matematika tudományágban

Írta: Kovács Tünde okleveles alkalmazott matematikus és angol-magyar szakfordító

Készült a Debreceni Egyetem Matematika- és Számítástudományok Doktori Iskola Diofantikus és Konstruktív Számelmélet programja keretében

Témavezető: Dr. Hajdu Lajos

A doktori szigorlati bizottság:

elnök:	Dr.	.....
tagok:	Dr.	.....
	Dr.	.....

A doktori szigorlat időpontja: 201... ....

Az értekezés bírálói:

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

A bírálóbizottság:

elnök:	Dr.	.....
tagok:	Dr.	.....
	Dr.	.....
	Dr.	.....
	Dr.	.....

Az értekezés védésének időpontja: 201... ....

Köszönetnyilvánítás

Ezúton szeretnék köszönetet mondani mindazoknak, akik bármi módon hozzájárultak a disszertációm elkészítéséhez.

Szüleimnek, akik felneveltek és elindítottak az életben.

Témavezetőmnek, Dr. Hajdu Lajosnak, aki megszerettette velem a számelméletet, azért a rengeteg hasznos tanácsért, útmutatásért és bátorításért, amely nélkül ez a dolgozat nem jöhetett volna létre.

Tanáraimnak, Dr. Győry Kálmánnak, Dr. Pethő Attilának, Dr. Gaál Istvánnak és Dr. Pintér Ákosnak, akiktől nagyon sokat tanultam és tanulok.

Kollégáimnak az Algebra és Számelmélet Tanszéken, Dr. Bérczes Attilának és Dr. Tengely Szabolcsnak, akikhez bármikor fordulhattam szakmai segítségért.

Contents

Introduction

Our PhD dissertation consists of five chapters each containing new results concerning Diophantine equations and Diophantine problems. Most problems have certain combinatorial background. In the first chapter we present the main method used in our studies namely the $\mathcal{E}llog$ method together with an improvement of ours [50]. In the second chapter we apply the $\mathcal{E}llog$ method to solve several Diophantine equations having certain combinatorial background. These results can be found in [58]. In the third chapter we give several effective and explicit results concerning the values of some polynomials in binary recurrence sequences. These results are published in [59]. In the fourth chapter we introduce the concept of balancing numbers in arithmetic progressions, and prove several effective finiteness and explicit results about them. The results of Chapter 4 are published in [60]. In the fifth chapter we prove that the product of k consecutive terms of a primitive arithmetic progression is never a perfect fifth power when $3 \leq k \leq 54$. We also provide a more precise statement, concerning the case where the product is an "almost" fifth power. These results are published in [51]. In what follows, we give an overview of the contents of the chapters one by one.

I

Though we shall apply and combine several techniques to prove our results, our main tool will be elliptic curves and elliptic equations. In particular, we shall be interested in finding the integer points on such equations. The search for integral solutions of elliptic equations has been initiated by Mordell. By Siegel's famous theorem [100], we know that any given elliptic equation has at most finitely many integral solutions. Since this result is ineffective, the determination of the solutions remained a challenge. Baker's famous work on linear forms in logarithms of algebraic numbers made Siegel's theorem effective.

Since then several improvements have been achieved, see e.g. [4], [19], [99], [102], [27], [49] and the references given there. Besides these results a great variety of methods and techniques have been successfully applied to solve particular equations (see e.g. [71], [72], [2], [66], [3], [18], [119], [86] and the references given there) until a powerful, general method has been developed simultaneously and independently by Stroeker, Tzanakis [103] and Gebel, Pethő, Zimmer [41]. This approach uses the arithmetic properties of elliptic curves and combines many deep ingredients, due to several authors, including an effective bound for linear forms in elliptic logarithms obtained by David [36]. The most recent version of the method, the so-called *Ellog* method is already capable to find (at least in principle) all integral points on genus 1 curves (see [105], and also the references given there). In Chapter 1, we describe in details the *Ellog* method and present an improvement due to Hajdu and Kovács [50]. The method splits up into three distinct parts. In the initial stage the basic characteristics of the corresponding elliptic curve are gathered, like the torsion group, the rank r and a basis $(P_1, \ldots, P_r)$ for the free part of the Mordell-Weil group. Each rational point $P \in E(\mathbb{Q})$ has a unique representation of the form

$$P = P_0 + n_1 P_1 + \ldots + n_r P_r, \tag{1}$$

where P_0 is a torsion point and $n_i \in \mathbb{Z}$ $(i = 1, \ldots, r)$. Put $N = \max_{1 \leq i \leq r}\{|n_i|\}$. The first main step of the method is to derive an initial upper bound for N. At this stage beside certain standard height estimates the above mentioned result of David [36] plays a crucial role. Once an upper bound for N is obtained, all points P satisfying relation (1) can be explicitly computed, at least in principle.

Typically, the initial upper bound obtained for N is rather huge, so it cannot be used for practical purposes. In the second stage of *Ellog* this initial upper bound is reduced drastically. At this step the key method relies on a result of de Weger [120] which is based upon the LLL-algorithm.

The third step of the method seems to be trivial: using the final bound for N (which is typically around 10 say) we simply enumerate all the possibilities and then check whether they are solutions or not. However, this innocent looking part may be the most troublesome point of the method. Indeed, if the rank r is large then the size of the region to be checked for solutions can be extremely huge. (At this point it is worth to mention that by a folklore conjecture there exist elliptic curves of arbitrarily high rank.) So any further reduction of the "final" bound for N or shrinking the region of possible solutions can be very important in solving a particular equation completely. Hence this point deserves extra attention.

In [104], Stroeker and Tzanakis observed and gave convincing numerical and heuristic evidence for that in their $\mathcal{E}llog$ method a certain parameter λ plays a decisive role in the size of the final bound N_{final} for the integral points on elliptic curves. In fact this λ is the smallest eigenvalue of the height-pairing matrix of the underlying Mordell-Weil basis. Further, they provided an algorithm to determine that Mordell-Weil basis of the curve which corresponds to the optimal choice of λ. Hence to minimize the final bound for the solutions, one should use such a "best" basis of the curve. We shall call such a basis Stroeker-Tzanakis basis, or shortly ST-basis. In [104] it is shown through several examples that using an ST-basis one can get a (much) better bound N_{final} than with other bases. In Chapter 1 we show that even the "best" final bound N_{final} received by using an ST-basis, can be further improved if one uses more bases simultaneously, and combines the information obtained for the solutions in the different bases. The results of the first chapter are published in [50].

II

Many Diophantine equations possess combinatorial background. A lot of deep finiteness (both effective and ineffective) results are known about the solutions of such equations. We refer to the papers [15], [16], [21], [88], [89] and the references given there. One of the first results giving all integer solutions of a combinatorial Diophantine equation is a theorem of Mordell [71], which provides all integer solutions of the equation $y(y+1) = x(x+1)(x+2)$. Later Avanesov [2] resolved the equation $\binom{y}{2} = \binom{x}{3}$. MacLeod and Barrodale [66] considered the problem when the product of two consecutive integers is equal to the product of six consecutive integers, i.e. resolved the equation $y(y+1) = x(x+1)\cdots(x+5)$. A similar result is due to Boyd and Kisilevsky [18]. They determined all integral solutions of the equation $y(y+1)(y+2) = x(x+1)(x+2)(x+3)$. Later among others, mixed equations were considered, i.e. on one side there is a binomial coefficient and on the other side there is the product of l consecutive integers. For example Tzanakis and de Weger [118] resolved the equation $\binom{y}{2} = x(x+1)(x+2)$ and Pintér [82] (see also [43], p. 225) found all integral solutions of the equation $\binom{y}{2} = x(x+1)(x+2)(x+3)$. Other scattered equations have been investigated by several authors, see for example [3], [66], [86], [103], [119], [122]. Hajdu and Pintér [52] systematically collected and solved those combinatorial equations of the above types that can be reduced to Mordell-type equations. Our purpose is to extend this result to more general combinatorial equations that can be reduced to general elliptic equations. Namely, we collect those equations that can be reduced to equations of genus 1 and then resolve them by the above

described $\mathcal{E}llog$ method. We mention that beside a lot of sparse results (see e.g. [82], [83], [86], [106] and [121]), Stroeker and de Weger [107] solved all such equations involving binomial coefficients. The results of the second chapter are published in [58].

III

There are many papers about values of a polynomial $p(x) \in \mathbb{Q}[x]$ (taken at integer values of x) in a binary linear recurrence sequence U. The first such results dealt with the case where U is a special sequence and $p(x) = x^m$ with some $m \geq 2$. That is, we are interested in terms of U which are perfect powers. In 1962 Ogilvy [77], one year later Moser and Carlitz [73], and Rollett [92] proposed the following problem: determine all squares in the Fibonacci sequence F. The problem was solved by Cohn [29, 30] and Wyler [125] who independently proved with elementary methods that the only squares in the Fibonacci sequence are $F_0 = 0, F_1 = F_2 = 1, F_{12} = 144$. Later, Alfred [1] and Cohn [31] determined the squares in the Lucas sequence L. Pethő [80] and Cohn [32] independently determined the perfect powers in the Pell sequence. Recently, Bugeaud, Mignotte and Siksek [28] showed that the perfect powers in the Fibonacci and Lucas sequences are exactly $F_0 = 0, F_1 = F_2 = 1, F_6 = 8, F_{12} = 144$, and $L_1 = 1, L_3 = 4$, respectively.

Another branch of problems is about triangular numbers in recurrence sequences, i.e. we take the polynomial $p(x) = \frac{x(x+1)}{2}$. Hoggatt stated the conjecture that there are only five triangular Fibonacci numbers. In 1989 Ming [69] proved that this conjecture is true. Furthermore, Ming [70] and McDaniel [68] determined the triangular numbers in the Lucas and Pell sequences, respectively. In [108] Szalay described all values of the polynomials $S_2(x)$ and $S_3(x)$ in the Fibonacci, Lucas and Pell sequences, where $S_k(x)$ denotes the sum of the first $x-1$ kth powers ($x \in \mathbb{N}$). Further, he listed all numbers of the form $\binom{x}{4}$ in the Fibonacci and Lucas sequences, as well. As a generalization of the previous results, Tengely [114] determined the g-gonal numbers in the Fibonacci, Lucas, Pell and Associated Pell sequences for $g \leq 20$. Recently, Tengely [115] showed that the only term of the form $\binom{x}{5}$ of the Lucas sequence is $L_1 = 1$.

The above mentioned results give complete solutions of the problem in case of certain sequences U and polynomials p. Beside them there are several results in the literature which provide effective upper bounds for the solutions under certain assumptions. The most extensively investigated situation is again the case of perfect powers, i.e. where $p(x) = x^m$ with some $m \geq 2$. Instead of trying to survey the extremely huge literature we only refer to the book [99]

and the references given there. Finally, we mention that Szalay [108] provided an algorithm for the complete description of the values of a polynomial $p(x)$ of degree 3 in a binary recurrence sequence U under some assumptions.

In Chapter 3 we prove three theorems concerning the values of some polynomials in binary recurrence sequences. First we provide an effective finiteness theorem for certain combinatorial numbers, namely for binomial coefficients, products of consecutive integers, power sums and alternating power sums in binary recurrence sequences, under some assumptions. The proof of this theorem is based on Baker's method and results of Brindza [19], Ping-Zhi [81], Pintér and Rakaczki [85] and Rakaczki [90]. Our second theorem is an extension of the above mentioned result of Szalay. More precisely, it provides an efficient algorithm for determining the values of certain degree 4 polynomials in binary recurrence sequences, under some assumptions. We note that we implemented our algorithm in Magma [17] as well. Finally, partly by the help of this algorithm we give all combinatorial numbers mentioned above for the small values of the parameter involved in the Fibonacci, Lucas, Pell and Associated Pell sequences. To prove the latter result we reduce the problem to elliptic and more generally to genus 1 equations. We use the $\mathcal{E}llog$ method and the program package Magma to resolve our particular equations. The results of the third chapter are published in [59].

IV

A positive integer n is called a balancing number if

$$1 + \cdots + (n-1) = (n+1) + \cdots + (n+r)$$

holds for some positive integer r (see [7] and [39]). The sequence of balancing numbers is denoted by B_m $(m = 1, 2, \dots)$. It is easily checked that $B_1 = 6$ and $B_2 = 35$. By a result of Behera and Panda [7], we have the recurrence relation

$$B_{m+1} = 6B_m - B_{m-1} \qquad (m > 1).$$

In particular, there are infinitely many balancing numbers.

The literature of balancing numbers is very rich. In [62] and [63] Liptai proved that there are no Fibonacci and Lucas balancing numbers, respectively. Later, Szalay [111] derived the same results by a different method.

In [64] Liptai, Luca, Pintér and Szalay generalized the concept of balancing numbers in the following way. Let y, k, l be fixed positive integers with $y \geq 4$.

A positive integer x with $x \leq y-2$ is called a (k,l)-power numerical center for y if

$$1^k + \cdots + (x-1)^k = (x+1)^l + \cdots + (y-1)^l.$$

In [64] several effective and ineffective finiteness results were proved for (k,l)-power numerical centers.

Recently, the "balancing" property has been investigated in recurrence sequences (see [14]). In this chapter we extend the concept of balancing numbers to arithmetic progressions. Let $a > 0$ and $b \geq 0$ be coprime integers. If for some positive integers n and r we have

$$(a+b) + \cdots + (a(n-1)+b) = (a(n+1)+b) + \cdots + (a(n+r)+b)$$

then we say that $an+b$ is an (a,b)-balancing number. The sequence of (a,b)-balancing numbers is denoted by $B_m^{(a,b)}$ $(m = 1, 2, \dots)$. We mention that since $B_m^{(1,0)} = B_m$ for all m, we obtain a generalization of balancing numbers.

In Chapter 4 we prove several effective finiteness and explicit results concerning polynomial values in the sequences $B_m^{(a,b)}$. That is, we consider the equation

$$B_m^{(a,b)} = f(x)$$

in integers m and x with $m \geq 1$, where f is some polynomial with rational coefficients, taking only integral values at integers. To prove our theorems, beside the earlier mentioned results of Ping-Zhi [81], Pintér and Rakaczki [85] and Rakaczki [90], we further need the modular method developed by Wiles [124] and others and a deep result of Bennett [8] concerning binomial Thue equations. Our results from Chapter 4 are published in [60].

V

A celebrated theorem of Erdős and Selfridge [38] states that the product of consecutive positive integers is never a perfect power. A natural generalization is the Diophantine equation

$$x(x+d)\dots(x+(k-1)d) = by^n \tag{2}$$

in non-zero integers x, d, k, b, y, n with $\gcd(x,d) = 1$, $d \geq 1$, $k \geq 3$, $n \geq 2$ and $P(b) \leq k$. Here $P(u)$ stands for the largest prime divisor of a non-zero integer u, with the convention $P(\pm 1) = 1$.

This equation has a long history with an extensive literature. For $d = 1$, equation (2) has been completely solved by Saradha [94] (case $k \geq 4$) and

Győry [44] (case $k < 4$). Instead of trying to overview the huge number of related results for $d > 1$, we refer to the excellent survey papers of Győry [45], Shorey [96], [97] and Tijdeman [116]. Here we concentrate only on results where all solutions of (2) have been determined when the number k of terms is fixed.

If $(k, n) = (3, 2)$, equation (2) has infinitely many solutions even with $b = 1$ (c.f. [116]). Euler (see [37]) showed that (2) has no solutions if $b = 1$ and $(k, n) = (3, 3)$ or $(4, 2)$. Obláth [75], [76] obtained similar results for $(k, n) = (3, 4)$, $(3, 5)$ and $(5, 2)$.

By a conjecture of Erdős, equation (2) has no solutions in positive integers when $k > 3$ and $b = 1$. In other words, the product of k consecutive terms of a primitive positive arithmetic progression with $k > 3$ should never be a perfect power. By primitive arithmetic progression we mean one of the form

$$x, x + d, \ldots, x + (k - 1)d,$$

with $\gcd(x, d) = 1$. Erdős' conjecture has recently been verified for certain values of k in a more general form; see the papers [45], [46], [10], [47]. Now we focus on the case $n = 5$. We give only the best known result for this particular exponent. (Though the results mentioned are valid for any $n \geq 2$.) The following statement is a combination of results from [45] (case $k = 3$), [46] (cases $k = 4, 5$), [10] (cases $k = 6, 7$) and [47] (cases $8 \leq k \leq 34$).

Theorem A. *The only solutions to equation* (2) *with* $n = 5$, $3 \leq k \leq 34$ *and* $P(b) \leq P_k$, *with*

$$P_k = \begin{cases} 2, & \text{if } k = 3, 4, \\ 3, & \text{if } k = 5, \\ 5, & \text{if } k = 6, 7, \\ 7, & \text{if } 8 \leq k \leq 22, \\ \frac{k-1}{2}, & \text{if } 23 \leq k \leq 34 \end{cases}$$

are given by

$$(k, d) = (8, 1),\ x \in \{-10, -9, -8, 1, 2, 3\}; \quad (k, d) = (8, 2),\ x \in \{-9, -7, -5\};$$

$$(k, d) = (9, 1),\ x \in \{-10, -9, 1, 2\}; \quad (k, d) = (9, 2),\ x \in \{-9, -7\};$$

$$(k, d) = (10, 1),\ x \in \{-10, 1\}; \quad (k, d, x) = (10, 2, -9).$$

Note that knowing the values of k, d and x, all solutions (x, d, k, b, y, n) of (2) can be easily listed.

Now we explain why the case $n = 5$ in equation (2) is special. In order to do that, we need to give some insight into the method of solving (2) for fixed k, in the general case $n \geq 2$. One of the most important tools is the modular method, developed by Wiles [124]. In [45], [46], [10], [47] all three types of ternary equations (i.e. of signatures $(n, n, 2), (n, n, 3), (n, n, n)$) and related results of Wiles [124], Darmon and Merel [35], Ribet [91], Bennett and Skinner [12], Bennett, Vatsal and Yazdani [13] and others are used. However, the modular technique works effectively only for "large" exponents, typically for $n \geq 7$. Thus the "small" exponents $n = 2, 3, 5$ must be handled separately. In fact these cases are considered in distinct sections, or are covered by separate theorems in the above mentioned papers.

Further, the exponents $n = 2, 3$ has already been considered in separate papers. Equation (2) with $n = 2$ has a broad literature in itself; see e.g. [57] and the references given there. Here we focus only on the resolution of (2) with fixed k again. For $n = 2$ and positive x, equation (2) has been completely solved up to a few exceptional cases by Hirata-Kohno, Laishram, Shorey and Tijdeman [57] for $k \leq 100$, and in case of $b = 1$, even for $k \leq 109$. Their main tools were elliptic curves and quadratic residues. Later, the exceptional remaining cases have been handled by Tengely [113], by the help of the Chabauty method. At this point we note that we shall refer to the Chabauty method frequently later on. For the description of the method, and in particular how to use it in the frame of the program package Magma [17], we refer to the papers of Bruin [23], [24] and the references given there.

When $n = 3$, working mainly with cubic residues, however making use of elliptic curves and the Chabauty method as well, Hajdu, Tengely and Tijdeman [54] obtained all solutions to equation (2) with $k < 32$ such that $P(b) \leq k$ if $4 \leq k \leq 12$ and $P(b) < k$ if $k = 3$ or $k \geq 13$. Further, if $b = 1$ then they could solve (2) for $k < 39$.

The case $n = 5$ has not yet been closely investigated. In this case (in the above mentioned papers considering equation (2) for general exponent n) mainly classical methods were used, due to Dirichlet and Lebesgue (see e.g. [47]). Apparently, for $n = 5$ elliptic curves are not applicable. In Chapter 5 we show that in this case the Chabauty method (both the classical and the elliptic versions) can be applied very efficiently. As we mentioned, the Chabauty method has been already used for the cases $n = 2, 3$ in [10], [113], [54]. However, it has been applied only for some particular cases and equations. In our results we solve a large number of genus 2 equations by Chabauty method, and then build a kind of sieve system based upon them. The results of Chapter 5 are published in [51].

Chapter 1

The $\mathcal{E}llog$ method and an improvement

1.1 Introduction

As we have already mentioned in the introduction, the effective theory of elliptic Diophantine equations has been started by the classical result of Baker [4]. However, since the bound provided for the solutions by this result is too large, to solve a concrete elliptic equation some further or alternative considerations are needed. For a long time, a great variety of methods and techniques have been successfully applied to solve individual elliptic equations, see e.g. [72], [99] until a new method was developed simultaneously and independently by Stroeker, Tzanakis [103] and Gebel, Pethő, Zimmer [41]. This approach uses the arithmetic properties of elliptic curves and combines many deep ingredients, due to several authors. The most recent version of this so-called $\mathcal{E}llog$ method is already capable to find (at least in principle) all integral points on genus 1 curves (see [105], and also the references given there). In Section 1.2, we describe in details the $\mathcal{E}llog$ method. We follow the discussion and terminology of [105]. In Section 1.3, we present an improvement of the $\mathcal{E}llog$ method due to Hajdu and Kovács [50]. The $\mathcal{E}llog$ method splits up into three distinct parts. In the initial stage essential characteristics of the corresponding elliptic curve are gathered, like the torsion group, the rank r and a basis $(P_1, \ldots, P_r)$ for the free part of the Mordell-Weil group. Each rational point $P \in E(\mathbb{Q})$ has a unique representation

of the form

$$P = P_0 + n_1 P_1 + \ldots + n_r P_r, \tag{1.1}$$

where P_0 is a torsion point and $n_i \in \mathbb{Z}$ $(i = 1, \ldots, r)$. Put $N = \max_{1 \le i \le r}\{|n_i|\}$.

The first main step of the method is to derive an initial upper bound for N. At this stage beside certain standard height estimates a deep result of David [36] concerning linear forms in elliptic logarithms plays a crucial role. Once an upper bound for N is obtained, all points P satisfying relation (1) can be explicitly computed, at least in principle.

Typically, the initial upper bound obtained for N is rather huge, so it cannot be used for practical purposes. In the second stage of $\mathcal{E}llog$ this initial upper bound is reduced drastically. At this step the key method relies on a result of de Weger [120] which is based upon the LLL-algorithm.

The third step of the method seems to be trivial: using the final bound for N (which is typically around 10 say) we simply enumerate all the possibilities and then check whether they are solutions or not. However, this innocent looking part may be the most troublesome point of the method. Indeed, if the rank r is large then the size of the region to check for solutions can be extremely huge. (At this point it is worth to mention that by a folklore conjecture there exist elliptic curves of arbitrarily high rank.) So any further reduction of the "final" bound for N or shrinking the region of possible solutions can be very important in solving a particular equation. Hence this point deserves extra attention.

In [104], Stroeker and Tzanakis observed and gave convincing numerical and heuristic evidence for that in the $\mathcal{E}llog$ method a certain parameter λ plays a decisive role in the size of the final bound N_{final} for the integral points on elliptic curves. Further, they provided an algorithm to determine that Mordell-Weil basis of the curve which corresponds to the optimal choice of λ. Hence to minimize the final bound for the solutions, one should use such a "best" basis of the curve. We shall call such a basis Stroeker-Tzanakis basis, or shortly ST-basis. In Section 1.3 we show that even the "best" final bound N_{final} received by using an ST-basis, can be further improved if one uses more bases simultaneously, and combines the information obtained for the solutions in the different bases. The results of this chapter are published in [50].

1.2 The $\mathcal{E}llog$ method

Let $f \in \mathbb{Z}[u, v]$ be irreducible over $\mathbb{Z}$, and consider the Diophantine equation

$$f(u, v) = 0 \tag{1.2}$$

and the corresponding curve

$$C = \left\{(u, v) \in \mathbb{Q}^2 \mid f(u, v) = 0\right\}.$$

If C is of genus 1 and non-empty, then (1.2) can be transformed into a short Weierstrass equation

$$y^2 = x^3 + Ax + B =: q(x) \tag{1.3}$$

with a birational transformation. Here $A, B \in \mathbb{Z}$, and the discriminant of $q(x)$, i.e. $4A^3 + 27B^2$ is non-zero. We define

$$E(K) = \{(x, y) \in K^2 \mid y^2 = x^3 + Ax + B\},$$

where $K \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$. The birational transformation and its inverse between C and $E(\mathbb{Q})$ can be written in the form

$$\begin{aligned} x &= X(u, v), \quad & y &= Y(u, v), \\ u &= U(x, y), \quad & v &= V(x, y), \end{aligned}$$

where

$$(X, Y) : C \longrightarrow E(\mathbb{Q}) \quad \text{and} \quad (U, V) = (X, Y)^{-1} : E(\mathbb{Q}) \longrightarrow C.$$

Here X, Y, U, V are rational functions which can be explicitly computed.

In what follows, we recall some well-known facts and results about $E(\mathbb{Q})$, $E(\mathbb{R})$ and $E(\mathbb{C})$. For the basic properties of these structures we refer to [101] and the references given there.

$E(\mathbb{Q})$ is a finitely generated group, more precisely

$$E(\mathbb{Q}) \cong E_{tors}(\mathbb{Q}) \times \mathbb{Z}^r,$$

where $E_{tors}(\mathbb{Q})$ is the torsion group, and r is the rank of $E(\mathbb{Q})$. Note that by a famous theorem of Mazur, the order of any torsion point is at most 12, and by the Nagell-Lutz theorem the torsion points can be easily computed. Let $P_1, \ldots, P_r$ denote a Mordell-Weil basis of $E(\mathbb{Q})$. Then each rational point $P \in E(\mathbb{Q})$ has a unique representation of the form

$$P = P_0 + n_1 P_1 + \ldots + n_r P_r, \tag{1.4}$$

where $P_0 \in E_{tors}(\mathbb{Q})$ is a torsion point and $n_i \in \mathbb{Z}$ $(i = 1, \ldots, r)$.

The group $E(\mathbb{R})$ has the so-called identity component E_0 and in the real case – when $q(x)$ has three real roots: $e_1 > e_2 > e_3$ – also a bounded component E_1. The components are given by

$$E_0 = \{(x, y) \in E(\mathbb{R}) \mid e_1 \leq x\},$$

$$E_1 = \{(x, y) \in E(\mathbb{R}) \mid e_3 \leq x \leq e_2\}.$$

Consider the isomorphism $\Phi : E_0 \to \mathbb{R}/\mathbb{Z}$ defined by

$$\Phi \equiv \begin{cases} 0 \pmod 1, & \text{if } P = \mathcal{O}, \\ \frac{1}{\omega} \int_{x(P)}^{\infty} \frac{dt}{\sqrt{q(t)}} \pmod 1, & \text{if } y(P) \geq 0, \\ -\Phi(-P) \pmod 1, & \text{if } y(P) < 0, \end{cases}$$

where $\omega = 2\int_{e_1}^{\infty} \frac{dx}{\sqrt{q(x)}}$ is the fundamental real period of $E(\mathbb{C})$. In the complex case – that is when $q(x)$ has a single real root – $E_0 = E(\mathbb{R})$ and Φ is defined on the whole $E(\mathbb{R})$. In the real case Φ can be extended to a two-to-one epimorphism $\tilde{\Phi}$, defined by

$$\tilde{\Phi}(R) = \begin{cases} \Phi(R), & \text{if } R \in E_0, \\ \Phi(R'), & \text{if } R \in E_1, \end{cases}$$

where $R' = R + (e_2, 0)$. In the complex case simply set $\tilde{\Phi} = \Phi$. We have

$$\omega \cdot \tilde{\Phi}(R) = \begin{cases} \text{elliptic logarithm of } R, & \text{if } R \in E_0, \\ \text{elliptic logarithm of } R', & \text{if } R \in E_1. \end{cases}$$

Let

$$G(u, v) = 2\frac{\partial_u Y(u, v) \cdot \partial_v f(u, v) - \partial_v Y(u, v) \cdot \partial_u f(u, v)}{3X^2(u, v) + A}.$$

The relation between the original equation (1.2) and the short Weierstrass equation (1.3) is given by

$$\int_{U(P)}^{\infty} \frac{G(u, v)}{\partial_v f(u, v)} du = \int_{x(P)}^{x_0} \frac{dx}{\varepsilon\sqrt{q(x)}} \tag{1.5}$$

under the assumption that $U(P)$ is greater than the poles of X and Y. Here $x(P)$ is the first coordinate of the point P on the curve E, $U(P)$ is the first coordinate of the inverse of the point P on C, $\varepsilon = \pm 1$, and $x_0 = \lim_{u\to\infty} X(u, v)$. It can be easily seen that either $x_0 = \infty$, or x_0 is a real algebraic number that can be

explicitly computed. In the latter case, let R_0 denote the point of $E(\mathbb{R})$ with first coordinate x_0, and non-negative second coordinate. The integral on the right side of (1.5) can be expressed by (1.4) as a linear form in elliptic logarithms in the following way:

$$\int_{x(P)}^{x_0} \frac{dx}{\varepsilon\sqrt{q(x)}} = u_0 + n_1u_1 + \ldots + n_ru_r - u_{r+1} + n_0\omega =: \mathcal{L}(P). \tag{1.6}$$

Here $P = (x, y) \in E(\mathbb{Q})$, u_i denotes the elliptic logarithm of the points P_i $(i = 0, 1, \ldots, r)$, u_{r+1} is the elliptic logarithm of R_0 and n_0 is a rational integer. Put $N = \max_{1\leq i\leq r}\{|n_i|\}$. Note that $n_0 \leq rN + 1$. We derive an upper bound for the linear form $\mathcal{L}(P)$ in terms of N. First, in a standard way (using e. g. elliptic integrals and Puiseux-expansions) we obtain an inequality of the form

$$|\mathcal{L}(P)| < c_1 \cdot |u|^{-\delta},$$

where δ and c_1 (and later c_2, c_3, etc.) are explicitly computable positive constants depending only on the parameters of the curve. At this point we need some further notation. Let $h(\alpha)$ denote the logarithmic height of an algebraic number α (see for example [61]). We mention that if $p, q \in \mathbb{Z}$, $q \neq 0$, $\gcd(p, q) = 1$, then $h(p/q) = \log\max(|p|, |q|)$. With a simple calculation from equation (1.2) we deduce that

$$h(X(u, v)) \leq c_2 + c_3 \log|u|.$$

It is well-known (see for example [34] and the references there), that

$$\hat{h}(P) - \frac{1}{2}h(X(u, v)) \leq c_4$$

for all $P = (x, y) \in E(\mathbb{Q})$, where $\hat{h}$ is the so-called Néron-Tate height function, that is

$$\hat{h}(P) = \frac{1}{2}\lim_{n\to\infty}\frac{h(2^nP)}{2^{2n}}.$$

(Here and later on we use the convention $h(Q) = h(x(Q))$ for all algebraic points $Q \in E(\mathbb{C})$.) On the other hand, since $\hat{h}$ is a positive semidefinite quadratic form on $E(\mathbb{R})$, we obtain the lower estimate

$$\hat{h}(P) \geq \lambda N^2,$$

where $\lambda > 0$ is the smallest eigenvalue of the matrix of $\hat{h}$ with respect to the basis $P_1, \ldots, P_r$ of $E(\mathbb{Q})$. On combining the latter four inequalities, we get the estimate

$$|\mathcal{L}(P)| < c_5 \exp\left(c_6 - c_7 \lambda N^2\right). \tag{1.7}$$

To get a lower estimation for $|\mathcal{L}(P)|$, one needs a deep result of David [36] providing a lower bound for linear forms in elliptic logarithms. In the following lemma we formulate Tzanakis' variant of this result from [117]. Before that, we need to introduce some new notation. First note that it is always possible to choose a pair of fundamental periods ω_1, ω_2 of the curve E in a way that $\tau := \omega_2/\omega_1$ satisfies

$$|\tau| \geq 1\ , \quad \Im\tau > 0\ , \quad -\tfrac{1}{2} < \Re\tau \leq \tfrac{1}{2} \quad \text{with } 0 \leq \Re\tau \quad \text{if } |\tau| = 1.$$

The height of $E(\mathbb{Q})$ is defined by $h_E = \max\left(1, h\left(\frac{A}{4}, \frac{B}{16}\right), h(j_E)\right)$, where $j_E = 2^8 3^3 A^3/\left(4A^3 + 27B^2\right)$ is the modular invariant of $E(\mathbb{Q})$. Let D denote the degree of the number field generated by the coordinates of R_0, and let $k = r + 1$ if $\Phi(R_0)$ is linearly independent of $\Phi(P_1), \ldots, \Phi(P_r)$ over $\mathbb{Q}$, else set $k = r$. Finally, choose real numbers A_i $(i = 0, \ldots, r+1)$ such that $A_0 \geq \max\left(h_E, \frac{3\pi|\omega|^2}{D|\omega_1|^2\Im\tau}\right)$, $A_i \geq \max\left(h_E, \frac{3\pi|\omega|^2\Phi(P_i)^2}{D|\omega_1|^2\Im\tau}, \hat{h}(P_i)\right)$ $(i = 1, \ldots, r)$, $A_{r+1} \geq \max\left(h_E, \frac{3\pi|\omega|^2\Phi(R_0)^2}{D|\omega_1|^2\Im\tau}, \hat{h}(R_0)\right)$.

Lemma 1.2.1 (Tzanakis [117])**.** *By the above notation we have*

$$|\mathcal{L}(P)| > \exp\left(-c_8 \left(\log N' + c_9\right)\left(\log\log N' + c_{10}\right)^{k+2}\right), \tag{1.8}$$

where

$$c_8 = 2.9 \cdot 10^{6k+12} D^{2k+4} 4^{2(k+1)^2} (k+2)^{2k^2+13k+23.3} \prod_{i=0}^{k} A_i,$$

$$c_9 = \log De, \quad c_{10} = \log De + h_E,$$

and $N' = \max\{|n_0|, N\}$.

Combining the upper bound (1.7) and the lower bound (1.8) for the linear form, using $N' \leq rN + 1$ we obtain an upper estimate for N. This initial bound according to a heuristic argument of Stroeker and Tzanakis [104] is approximately around $10^{\left(5r^2+15r+28\right)/2}$, so it is too large to determine all integer solutions of

the original equation. We use de Weger's method [120] based upon the LLL-algorithm to reduce this bound. Using the inverse of the birational transformation, after the reduction we can compute all integer solutions of equation (1.2). Put $\rho_i = \Phi(P_i)$ $(i = 1, \ldots, r)$ and $\rho_{r+1} = \Phi(R_0)$. In general, ρ_{r+1} is linearly independent of $\rho_1, \ldots, \rho_r$ over $\mathbb{Q}$. In the opposite case, a simpler version of the reduction can be used. Now we outline the main steps of the reduction algorithm. Consider the $(r+1)$-dimensional lattice Γ generated by the coloumns of the matrix

$$A = \begin{pmatrix} 1 & \ldots & 0 & 0 \\ 0 & \ldots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1 & 0 \\ [K_0\rho_1] & \cdots & [K_0\rho_r] & K_0 \end{pmatrix},$$

where K_0 is a conveniently chosen integer, to be specified later. Compute the LLL-reduced basis of the lattice, and denote by b_1 the shortest vector of this basis. Write

$$\begin{pmatrix} x_1 \\ \vdots \\ x_{r+1} \end{pmatrix} = B^{-1} \cdot \mathbf{x} \quad \text{with} \quad \mathbf{x} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ -[K_0\rho_{r+1}] \end{pmatrix} \in \mathbb{R}^{r+1},$$

where B denotes the matrix whose columns are the vectors of the reduced basis. By Lemma 3.5 of de Weger [120]

$$d(\mathbf{x}, \Gamma) \geq 2^{r/2} \|x_{i_0}\| |b_1|$$

holds, where $\|\cdot\|$ denotes the distance to the nearest integer, $i_0 \in \{1, \ldots, r+1\}$ is chosen so that $\|x_{i_0}\|$ is minimal among $\|x_1\|, \ldots, \|x_{r+1}\|$. Then we have the following result.

Lemma 1.2.2 (Tzanakis [117]). *Let $K_1 = \frac{c_5}{\omega} \exp c_6$, $K_2 = c_7$. Then by the above notation,*

$$\|x_{i_0}\| |b_1| > 2^{r/2} \sqrt{(r^2 + r) K_3^2 + 2rK_3 + 1}$$

implies that

$$N^2 \leq K_2^{-1} \left(\log K_0 K_1 - \log \sqrt{2^{-r} \|x_{i_0}\|^2 |b_1|^2 - rK_3^2} - rK_3 - 1 \right).$$

To use this result, we choose K_0 somewhat larger than $(2^{r/2}K_3\sqrt{r^2+r})^{r+1}$. Then by Lemma 1.2.2 (if the condition is satisfied) we get a new bound for N of the size $(K_2^{-1}\log K_3)^{1/2}$. We iterate this process (always with the new values of K_0 and K_3), until the new bound cannot be improved. Using this reduced bound we can determine the integer points of the curve C by the help of the inverse of the birational transformation, and hence all integer solutions of the equation (1.2).

1.3 An improvement of the $\mathcal{E}llog$ method - Parallel LLL-reduction for bounding the integral solutions of elliptic Diophantine equations

In [104], Stroeker and Tzanakis observed and gave convincing numerical and heuristic evidence for that in their $\mathcal{E}llog$ method a certain parameter λ plays a decisive role in the size of the final bound N_{final} for the integral points on elliptic curves. This λ is the smallest eigenvalue of the height-pairing matrix of the underlying Mordell-Weil basis. Further, they provided an algorithm to determine that Mordell-Weil basis of the curve which corresponds to the optimal choice of λ. Hence to minimize the final bound for the solutions, one should use such a "best" basis of the curve. We shall call such a basis Stroeker-Tzanakis basis, or shortly ST-basis. In [104] it is shown through several examples that using an ST-basis one can get a (much) better bound N_{final} than with other bases. This point is important in particular if the rank of the elliptic curve is "large", as then already a small improvement of the final bound can considerably shrink the region of possible solutions, and hence the final search can be done much faster. In this section we show that even the "best" final bound N_{final} received by using an ST-basis, can be further improved if one uses more bases simultaneously, and combines the information obtained for the solutions in the different bases. As we will also see, elementary linear algebra tells us that it takes only a very little extra time to get this improvement.

In the first subsection we explain our method. In the second subsection we give some examples to illustrate how our method works. These result are published in [50].

1.3.1 Bounding integral solutions of genus 1 equations

All constants $c_5, c_6, c_7, c_8, c_9, c_{10}$ occurring in the upper and lower bounds (1.7) and (1.8) obtained for $\mathcal{L}(P)$ depend only on C and E. However, most importantly from our point of view, in (1.7) λ is the smallest eigenvalue of the height pairing matrix of the basis $P_1, \ldots, P_r$ occurring in (1.4). That is, λ certainly depends on the choice of the Mordell-Weil basis. As it is demonstrated by Stroeker and Tzanakis [104], the size of λ has a great impact on the final bound N_{final} for N. As it turns out, N_{final} is almost linear in $\lambda^{-1/2}$ so it is worth to pay attention to this point. We shall return here a little later.

As it was described before, in Section 1.2, combining estimates (1.8) and (1.7) we get an initial upper bound N_0 for N. However, this upper bound is usually extremely huge. Due to an observation of Stroeker and Tzanakis [104], N_0 should be around $10^{(5r^2+5r+28)/2}$. Hence to explicitly determine the integral points on C, this initial bound N_0 should be reduced. This is the final stage of $\mathcal{E}llog$ and can be done by lattice reduction techniques due to de Weger [120], based on the LLL-algorithm. We use Lemma 1.2.2 due to Tzanakis [117]. To apply this result, one starts with (1.7), together with the inequality $N < N_0$. Using the appropriate Proposition from Section 5 of Tzanakis [117], one gets a new lower bound of the shape

$$N < \frac{c_{11}}{\sqrt{c_7 \lambda}}$$

for N, where c_{11} is an explicitly computable constant depending on some parameters of E, and also on the length of the shortest vector of an LLL-reduced basis of a certain lattice. As one can see, this new bound is linear in $\lambda^{-1/2}$, which shows the importance of this parameter. Stroeker and Tzanakis [104] have considered several examples which indicate this phenomenon in a rather convincing way. Summarizing the results in [104], to get the best possible reduced bound N_{final} for N one should definitely choose an ST-basis of the curve E in (1.4). Subsequently, Stroeker and Tzanakis [104] have also worked out an efficient algorithm for finding an ST-basis of the curve.

However, in the sequel it turns out that the bound obtained by using an ST-basis, can still be improved further, if one works with several Mordell-Weil bases simultaneously. It is important to note that following our method the use of more bases shall increase only by a fraction the total time needed to get a better N_{final}. As we mentioned earlier, already a small gain in N_{final} may lead to a large improvement in the searching time for finding the small solutions - in particular, if r is large. The reason is simply that the region where we have to

look for the small solutions is of size $(2N_{final}+1)^r$. Note that a similar "size" notion was used also in [104] to compare the final bounds obtained in different Mordell-Weil bases.

Now we briefly outline how to work in several bases simultaneously. To explain our ideas in fact it is sufficient to use two bases. So assume that $B_1 = (P_1, \ldots, P_r)$ is a Mordell-Weil basis of E, and let S be an integral unimodular matrix of size $r \times r$. Let $B_2 = (Q_1, \ldots, Q_r)$ be the basis of E obtained from B_1 by using S as a basis transformation matrix. Let P be a rational point on E with the representation (1.4), and assume that we also have

$$P = Q_0 + m_1 Q_1 + \ldots + m_r Q_r, \tag{1.9}$$

with some torsion point Q_0 and integers $m_1, \ldots, m_r$. Put $M = \max_{1 \le i \le r} |m_i|$, and recall that by elementary linear algebra we have

$$S^{-1} \begin{pmatrix} n_1 \\ \vdots \\ n_r \end{pmatrix} = \begin{pmatrix} m_1 \\ \vdots \\ m_r \end{pmatrix}. \tag{1.10}$$

This implies $M \le sN$, where $s = ||S^{-1}||$ is the row norm of S^{-1}. (The row norm of a $k \times \ell$ type real matrix $A = (a_{ij})_{\substack{1 \le i \le k \\ 1 \le j \le \ell}}$ is defined by $||A|| = \max_{1 \le i \le k} \sum_{j=1}^{\ell} |a_{ij}|$.) In particular, this means that one does not have to go through the $\mathcal{E}llog$ method both for B_1 and B_2, it is sufficient to use it with B_1 say. Indeed, take for example B_1 to be an ST-basis of E, and suppose that after applying the $\mathcal{E}llog$ method (together with the reduction stage) we have the bound $N < N_{final}$. Then by $M \le sN$, we automatically have $M \le M_0 := sN_{final}$. As s is typically "small" (it will be at most around ten), M_0 is not too large - and of course, it can also be reduced. Importantly, we can get the final bound M_{final} very easily and quickly. The reason is that the reduction steps are difficult and time consuming only if the initial bound is large, as then e.g. high precision is needed. However, as s will be small, the reduction steps leading from M_0 to M_{final} are made very easily. The final bounds N_{final} and M_{final} yield simultaneous upper bounds for the coefficients of P, in two different bases. Combining these two bounds by (1.10), we can decrease the domain where the final search has to be done. As one may predict (which turns out to be true), the gain starts getting more and more significant as the rank r is getting larger and larger.

In our calculations we choose B_1 to be an ST-basis of E, and we choose the other bases according to two different strategies.

Strategy 1. We try to decrease $N^{(1)}_{final}$ (corresponding to B_1), componentwise. For this purpose, choose distinct indices i, j with $1 \leq i, j \leq r$ and a positive integer t, and consider the bases B_2 and B_3 obtained by replacing P_i by $P_i + tP_j$ and $P_i - tP_j$ in B_1, respectively (leaving the other basis elements untouched). With the bases B_2 and B_3 the reduction process starts from the quite small bound $(t+1)N^{(1)}_{final}$ and gives, respectively, the final bounds, say, $N^{(2)}_{final}$ and $N^{(3)}_{final}$. Then a simple calculation yields that

$$|n_i| \leq \frac{N^{(2)}_{final} + N^{(3)}_{final}}{2t}$$

holds. If the right hand side happens to be less than $N^{(1)}_{final}$, then we get a new, improved bound for $|n_i|$. To make this principle work, for each fixed i we (heuristically) choose that j, for which the sum of the λ values (corresponding to B_2 and B_3) is maximal with $t = 1$. Then for simplicity (and also because we try to keep the time consumption of the method low), instead of checking several values, we take the fixed value $t = 10$ in the computations. The procedure can be iterated, and the iteration leads to further improvement in some cases.

Note that the "one-sided" version of this approach could also be used (i.e. when we work only with one of B_2 or B_3), but our experiences suggest that this "two-sided" version is more efficient. Further, we have some reasons for the choice of $t = 10$. If λ_t denotes the value of λ corresponding to t (either in B_2 or in B_3), then $\frac{t+1}{t}\sqrt{\frac{\lambda_t}{\lambda_{t+1}}}$ is close to 1, if t is "large". The value $t = 10$ seems to be large enough to make the λ-s corresponding to B_2 and B_3 more or less close to each other, and it seems to have some good effect on the outcome. Still, obviously at this point the method can have many variants.

Strategy 2. Using the algorithm of Stroeker and Tzanakis [104], we determine the "best" ten Mordell-Weil bases B_j $(j = 1, \ldots, 10)$ i.e. ten Mordell-Weil basis corresponding to the ten largest λ-values. (Note that by the algorithm we get all the basis transformation matrices with respect to B_1, as well, and also that the calculation of ten basis takes only a little extra time than calculating only B_1.) Then we compute the initial upper bounds $N^{(j)}_0$ $(j = 1, \ldots, 10)$ for the coordinates of the integral points in these bases, respectively. (As we mentioned, out of these only the calculation of $N^{(1)}_0$ is time consuming (but it has to be calculated even if we use only B_1), the other bounds come very quickly and easily.) Having these bounds, using the basis transformation matrices, we get several extra information for the coefficients of P in B_1. In fact we get a system

of inequalities defining a convex body, which contains much less integral points than the one implied by $|n_i| \leq N_{final}^{(1)}$ $(i = 1, \ldots, r)$.

Finally, we mention that altogether it seems that *Strategy 2* yields more improvement than *Strategy 1*.

1.3.2 Examples

In this subsection we give some examples, to illustrate how *Strategy 1* and *Strategy 2* work. For this purpose we borrow some curves from the papers [104] and [58]. As we mentioned, the problem discussed in the paper is interesting when the rank of the underlying elliptic curve is not too small, so we consider curves of ranks 5 and 6. In fact we have worked out a number of other examples (from [107], [104] and [58]), which can be found on the homepage http://www.math.klte.hu/algebra/hajdu.htm.

In each example we illustrate both *Strategy 1* and *Strategy 2*. We always start with giving the underlying curve and the basic information corresponding to it. In case of *Strategy 1*, we give the index j for each i, the two corresponding linear inequalities (with $t = 10$, using the notation (1.4)), and also indicate the final bound obtained for $|n_i|$. Finally, we calculate the improvement ratio, as well.

In case of *Strategy 2* we provide the following data. We give the best ten Mordell-Weil bases (in the sense explained above), by using the algorithm of Stroeker and Tzanakis [104]. (Note that the best basis is of course an ST-basis.) The bases are represented by the basis transformation matrices (with respect to the ST-basis). We indicate the corresponding λ values, as well. Finally, we list the final bounds in the corresponding bases, obtained by the above mentioned reduction results from [117]. After that we summarize the information in a system of linear inequalities (of the form $-\underline{b} \leq A\underline{x} \leq \underline{b}$). Using Barvinok's algorithm [6] the number N^* of the integral points in the corresponding convex body can be computed by the program package Latte [65]. Hence we can calculate the "improvement ratio" defined in the natural way, by $N^*/(2N_{final} + 1)^r$, where N_{final} corresponds to the ST-basis. Note that here we may use the reduced bounds obtained for $|n_i|$ by *Strategy 1*.

We give a detailed description only in the first example. In case of the other examples, we present the data in a brief form, following the previous notation. We start with two curves of rank 5, and we conclude with a rank 6 curve.

Example 1. This example is from [104]. We would like to determine the integral

points on the curve

$$E: \quad x^3 - 203472x + 18487440 = y^2.$$

The rank of E is $r = 5$, and an ST-basis of E (obtained by the method in [104]) is given by

$$P_1 = (468, 5076), P_2 = (-216, 7236), P_3 = (432, 3348),$$

$$P_4 = (-36, 5076), P_5 = (36, 3348).$$

The final bound obtained for the coordinates of the integral points of E is $N_{final} = 9$ in this basis (see [104]).

Strategy 1. Using the above explained methods, we get the following table.

i	j	bound for $\lvert 10n_i \pm n_j\rvert$	bound for $\lvert n_i\rvert$
1	4	(77,82)	7
2	1	(85,79)	8
3	5	(76,81)	7
4	5	(84,88)	8
5	1	(75,81)	7

Based upon the table, the improvement is given by

$$\frac{(2\cdot 7+1)(2\cdot 8+1)(2\cdot 7+1)(2\cdot 8+1)(2\cdot 7+1)}{(2\cdot 9+1)^5} = 0.393916.$$

Strategy 2. The basis transformation matrices (with respect to the ST-basis) of the best ten bases (obtained by the method of Stroeker and Tzanakis [104]) are given by

$$\begin{pmatrix} 1&0&0&0&0\\ 0&1&0&0&0\\ 0&0&1&0&0\\ 0&0&0&1&0\\ 0&0&0&0&1 \end{pmatrix}, \begin{pmatrix} 1&0&0&0&0\\ 0&1&0&0&0\\ 0&0&1&0&0\\ 0&0&0&1&0\\ -1&-1&1&1&1 \end{pmatrix}, \begin{pmatrix} 1&1&1&1&1\\ 0&0&0&1&-1\\ 1&0&0&0&0\\ 0&1&0&0&0\\ 0&0&0&-1&0 \end{pmatrix}, \begin{pmatrix} 1&0&0&0&0\\ 0&1&0&0&0\\ 0&0&1&0&0\\ 1&1&-1&1&0\\ 0&0&0&0&1 \end{pmatrix},$$

$$\begin{pmatrix} 1&0&0&0&0\\ 0&1&0&0&0\\ 0&0&1&0&0\\ 1&1&-1&1&0\\ 1&1&-1&1&1 \end{pmatrix}, \begin{pmatrix} 0&0&0&0&-1\\ -1&-1&1&1&2\\ 0&-1&1&1&1\\ -1&0&1&1&1\\ 0&0&1&0&0 \end{pmatrix}, \begin{pmatrix} 0&0&0&0&1\\ 1&0&0&0&-1\\ 0&1&0&0&0\\ 1&-1&1&0&0\\ 1&-1&1&1&0 \end{pmatrix},$$

$$\begin{pmatrix} 0&0&0&0&1\\ 1&0&0&0&-1\\ 1&1&1&1&0\\ 0&0&-1&-1&0\\ 0&0&0&-1&0 \end{pmatrix}, \begin{pmatrix} 1&1&1&0&1\\ 0&0&0&0&-1\\ 1&0&0&0&0\\ 0&1&0&0&0\\ 0&0&0&1&0 \end{pmatrix}, \begin{pmatrix} 1&0&0&0&0\\ 0&1&0&0&0\\ 1&1&1&1&0\\ 0&0&0&-1&0\\ 0&0&0&0&1 \end{pmatrix}.$$

The corresponding λ values are

$$0.46493, 0.45844, 0.45792, 0.44837, 0.44736,$$

$$0.42425, 0.41358, 0.41295, 0.41229, 0.41173,$$

and the final bounds N_{final} obtained after the reduction are

$$9, 9, 9, 9, 9, 10, 10, 10, 10, 10,$$

respectively. Combining these data, using the notation (1.4) (with respect to the ST-basis) we get the system of linear inequalities

$$\begin{pmatrix} -7 \\ -8 \\ -7 \\ -8 \\ -7 \\ -9 \\ -9 \\ -9 \\ -10 \\ -10 \\ -10 \\ -10 \end{pmatrix} \leq \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & -1 & -1 & 1 \\ -1 & -1 & 1 & 1 & 0 \\ 0 & 0 & 0 & -1 & 1 \\ -1 & -1 & 1 & 0 & 0 \\ -1 & -1 & 0 & 1 & 0 \\ 0 & -1 & 1 & 1 & -1 \\ 1 & 1 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} n_1 \\ n_2 \\ n_3 \\ n_4 \\ n_5 \end{pmatrix} \leq \begin{pmatrix} 7 \\ 8 \\ 7 \\ 8 \\ 7 \\ 9 \\ 9 \\ 9 \\ 10 \\ 10 \\ 10 \\ 10 \end{pmatrix}. \tag{1.11}$$

Note that because of some (natural) redundancy, here and also in the other examples not all the ten basis transformation matrices are needed to derive (1.11). We also mention that here we could already use the improved upper bounds obtained by *Strategy 1* for the $|n_i|$. Using Latte [65], we get that the above inequality (1.11) has precisely $N^* = 396785$ integral solutions in $(n_1, n_2, n_3, n_4, n_5)$. Hence the "improvement ratio" is

$$N^*/(2N_{final} + 1)^5 = 396785/(2 \cdot 9 + 1)^5 = 0.160246,$$

where $N_{final} = 9$ corresponds to the ST-basis P_1, P_2, P_3, P_4, P_5.

Example 2. This example is from [104]. The problem is to find the integral points on the curve

$$E: \quad x^3 - 879984x + 319138704 = y^2.$$

The rank of E is $r = 5$, and an ST-basis of E is given by

$$P_1 = (468, 3132), P_2 = (-684, -24516), P_3 = (720, -7668),$$

$$P_4 = (432, -4428), P_5 = (540, -1188).$$

i	j	bound for $\lvert 10n_i \pm n_j\rvert$	bound for $\lvert n_i\rvert$
1	5	(83,79)	8
2	1	(76,82)	7
3	5	(77,78)	7
4	3	(94,89)	9
5	1	(79,77)	7

The final bound obtained for the coordinates of the integral points of E is $N_{final} = 9$ in this basis (cf. [104]).

Strategy 1. We obtain the table
Hence the improvement is given by

$$\frac{(2\cdot 8+1)(2\cdot 7+1)(2\cdot 7+1)(2\cdot 9+1)(2\cdot 7+1)}{(2\cdot 9+1)^5} = 0.440259.$$

Strategy 2. The basis transformation matrices of the best ten bases:

$$\begin{pmatrix} 1&0&0&0&0\\ 0&1&0&0&0\\ 0&0&1&0&0\\ 0&0&0&1&0\\ 0&0&0&0&1 \end{pmatrix}, \begin{pmatrix} 1&0&1&1&1\\ 0&0&1&0&0\\ 0&0&0&0&-1\\ 0&0&0&-1&0\\ 0&-1&0&0&0 \end{pmatrix}, \begin{pmatrix} 1&1&1&1&0\\ 0&0&0&0&1\\ 1&0&0&0&0\\ -1&0&-1&-1&1\\ 0&0&0&-1&0 \end{pmatrix}, \begin{pmatrix} 0&1&0&0&0\\ 0&0&0&1&0\\ -1&1&1&0&1\\ 0&-1&0&1&-1\\ 0&0&1&0&0 \end{pmatrix},$$

$$\begin{pmatrix} 0&1&0&0&0\\ 0&0&0&1&0\\ 0&0&0&0&1\\ -1&0&1&1&-1\\ 0&0&1&0&0 \end{pmatrix}, \begin{pmatrix} 0&0&1&0&0\\ 0&0&0&0&1\\ 1&0&0&0&0\\ 0&1&-1&0&1\\ 0&0&0&1&0 \end{pmatrix}, \begin{pmatrix} 0&1&0&0&0\\ -1&1&0&1&1\\ 0&0&0&1&0\\ 0&0&0&0&1\\ 0&0&1&0&0 \end{pmatrix},$$

$$\begin{pmatrix} 0&0&0&1&0\\ 0&0&0&0&1\\ 1&0&0&0&0\\ 0&1&0&-1&1\\ 1&1&1&-1&0 \end{pmatrix}, \begin{pmatrix} 0&1&0&0&0\\ 0&0&0&1&0\\ 1&-1&0&1&1\\ 0&0&0&0&-1\\ 0&0&1&0&0 \end{pmatrix}, \begin{pmatrix} 0&1&0&0&0\\ 0&0&0&1&0\\ 0&0&0&0&1\\ 1&-1&0&1&-1\\ 0&0&1&0&0 \end{pmatrix}.$$

The corresponding λ values are

$$0.492063, 0.462853, 0.457636, 0.454803, 0.454749,$$

$$0.453727, 0.451024, 0.450503, 0.448775, 0.431040,$$

and the final bounds N_{final} obtained after reduction are

$$9, 9, 9, 9, 9, 9, 9, 9, 9, 9,$$

respectively. Thus we get the system of linear inequalities

$$\begin{pmatrix} -8\\ -7\\ -7\\ -9\\ -7\\ -9\\ -9\\ -9 \end{pmatrix} \le \begin{pmatrix} 1&0&0&0&0\\ 0&1&0&0&0\\ 0&0&1&0&0\\ 0&0&0&1&0\\ 0&0&0&0&1\\ 1&-1&1&1&0\\ 1&-1&0&1&0\\ 0&1&-1&-1&1 \end{pmatrix} \begin{pmatrix} n_1\\ n_2\\ n_3\\ n_4\\ n_5 \end{pmatrix} \le \begin{pmatrix} 8\\ 7\\ 7\\ 9\\ 7\\ 9\\ 9\\ 9 \end{pmatrix}.$$

By Latte [65] we obtain that the above inequality has precisely $N^* = 513939$ integral solutions in $(n_1, n_2, n_3, n_4, n_5)$. Hence the "improvement ratio" is

$$513939/(2 \cdot 9 + 1)^5 = 0.207560.$$

Example 3. This example is from [58]. The original problem is to find the integral points on the curve

$$C: \quad 2u^3 + 3u^2 + u = 6v^3 + 60v^2 + 144v.$$

The curve is birationally equivalent to

$$E: \quad x^3 - 1008x + 2985993 = y^2.$$

The rank of E is $r = 6$, and an ST-basis of E is

$$P_1 = (-36, 1725), P_2 = (298, 5399), P_3 = (243, 4134),$$

$$P_4 = (-138, -705), P_5 = (24, 1725), P_6 = (-41, 1720).$$

The final bound obtained for the coordinates of the images of the integral points of C on E is $N_{final} = 7$ in this basis (see [58]).

Strategy 1. We get the table

i	j	bound for $\lvert 10n_i \pm n_j \rvert$	bound for $\lvert n_i \rvert$
1	3	(70,68)	6
2	6	(69,64)	6
3	4	(64,61)	6
4	3	(64,60)	6
5	6	(68,71)	6
6	5	(59,63)	6

Hence the improvement is given by

$$\frac{(2 \cdot 6 + 1)(2 \cdot 6 + 1)(2 \cdot 6 + 1)(2 \cdot 6 + 1)(2 \cdot 6 + 1)(2 \cdot 6 + 1)}{(2 \cdot 7 + 1)^6} = 0.423753.$$

Strategy 2. The basis transformation matrices of the best ten bases:

$$\begin{pmatrix} 1&0&0&0&0&0\\ 0&1&0&0&0&0\\ 0&0&1&0&0&0\\ 0&0&0&1&0&0\\ 0&0&0&0&1&0\\ 0&0&0&0&0&1 \end{pmatrix}, \begin{pmatrix} -1&-2&1&-1&1&1\\ 0&0&1&0&0&0\\ 0&0&0&1&0&0\\ 0&0&0&0&0&-1\\ 0&-1&0&0&1&0\\ 0&-1&0&0&0&0 \end{pmatrix}, \begin{pmatrix} 0&1&0&0&0&0\\ 0&0&1&0&0&0\\ 0&0&0&1&0&0\\ 0&0&0&0&0&-1\\ -1&0&0&0&1&0\\ -1&0&0&0&0&0 \end{pmatrix}, \begin{pmatrix} -1&-1&1&1&0&0\\ 0&0&0&-1&1&0\\ 0&0&0&0&0&1\\ 1&0&-1&-1&1&-1\\ 1&0&0&0&0&0\\ 0&0&0&1&0&0 \end{pmatrix},$$

$$\begin{pmatrix} 0 & -1 & 1 & 1 & 1 & 0 \\ -1 & 0 & 0 & -1 & -1 & 1 \\ 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 1 & -1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & -1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix},$$

$$\begin{pmatrix} -1 & -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & -1 & 1 & -1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & -1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ -2 & -1 & 1 & -1 & -1 & -1 \\ -1 & 0 & 0 & 0 & -1 & 0 \\ -1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

The corresponding λ values are

$$0.640325, 0.627020, 0.603695, 0.603010, 0.599688,$$

$$0.595452, 0.587593, 0.586898, 0.586647, 0.586371,$$

and the final bounds N_{final} obtained after reduction are

$$8, 8, 8, 8, 8, 8, 8, 8, 8, 8,$$

respectively. So we get the following system of linear inequalities

$$\begin{pmatrix} -6 \\ -6 \\ -6 \\ -6 \\ -6 \\ -6 \\ -8 \\ -8 \\ -8 \\ -8 \\ -8 \\ -8 \\ -8 \end{pmatrix} \leq \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ -1 & 1 & -1 & -1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & -1 \\ -1 & 1 & -1 & -1 & 0 & 1 \\ 0 & 1 & -1 & -1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ -1 & 1 & -1 & -1 & 1 & 0 \\ 0 & 1 & -1 & -1 & 1 & 1 \end{pmatrix} \begin{pmatrix} n_1 \\ n_2 \\ n_3 \\ n_4 \\ n_5 \\ n_6 \end{pmatrix} \leq \begin{pmatrix} 6 \\ 6 \\ 6 \\ 6 \\ 6 \\ 6 \\ 8 \\ 8 \\ 8 \\ 8 \\ 8 \\ 8 \\ 8 \end{pmatrix}.$$

Latte [65] gives that the above system has precisely $N^* = 1801039$ integral solutions in $(n_1, n_2, n_3, n_4, n_5, n_6)$. Thus the "improvement ratio" is

$$1801039/(2 \cdot 7 + 1)^6 = 0.158116.$$

Chapter 2

Combinatorial Diophantine equations of genus 1

2.1 Introduction

Many Diophantine equations possess combinatorial background. A lot of deep finiteness (both effective and ineffective) results are known about the solutions of such equations. We refer to the papers [15], [16], [21], [88], [89] and the references given there. One of the first results giving all integer solutions of a combinatorial Diophantine equation is a theorem of Mordell [71], which provides all integer solutions of the equation $y(y+1) = x(x+1)(x+2)$. Later Avanesov [2] resolved the equation $\binom{y}{2} = \binom{x}{3}$. MacLeod and Barrodale [66] considered the problem when the product of two consecutive integers is equal to the product of six consecutive integers, i.e. resolved the equation $y(y+1) = x(x+1)\cdots(x+5)$. A similar result is due to Boyd and Kisilevsky [18]. They determined all integral solutions of the equation $y(y+1)(y+2) = x(x+1)(x+2)(x+3)$. Later among others, mixed equations were considered, i.e. in one side there is a binomial coefficient and in the other side there is the product of l consecutive terms. For example Tzanakis and de Weger [118] resolved the equation $\binom{y}{2} = x(x+1)(x+2)$ and Pintér [82] (see also [43], p. 225) found all integral solutions of the equation $\binom{y}{2} = x(x+1)(x+2)(x+3)$. Other scattered equations have been investigated by several authors, see for example [3], [66], [86], [103], [119], [122]. Hajdu and Pintér [52] systematically collected and solved those combinatorial equations that can be reduced to Mordell-type equations. Our purpose is to extend this

result to more general combinatorial equations that can be reduced to general elliptic equations. Namely, we collect those equations that can be reduced to equations of genus 1. We mention that beside a lot of sparse results (see e.g. [82], [83], [86], [106] and [121]), Stroeker and de Weger [107] solved all such equations involving binomial coefficients. The results of Chapter 2 are published in [58].

2.2 New results

As we mentioned in the introduction, we systematically collect and solve those unsolved combinatorial Diophantine equations which can be reduced to equations of genus 1 or to Mordell-type equations (see the details later). We need some notation to formulate our results. For all $n, x \in \mathbb{N}$ let

$$S_n(x) = 1^n + 2^n + \ldots + (x-1)^n,$$

$$\Pi_n(x) = x(x+1)\cdots(x+n-1).$$

The formerly solved Diophantine equations which can be reduced to elliptic equations concerning $\Pi_n(x)$, $S_n(x)$ and $\binom{x}{n}$, are the followings:

$\Pi_2(k) = \Pi_3(l)$ (Mordell [71]),
$\binom{k}{2} = \binom{l}{3}$ (Avanesov [2]),
$\Pi_2(k) = \Pi_6(l)$ (MacLeod and Barrodale [66]),
$S_2(k) = \binom{l}{2}$ (Avanesov [3] and Uchiyama [119]),
$\Pi_3(k) = \Pi_4(l)$, $S_2(k) = \binom{l}{4}$ (Boyd and Kisilevsky [18]),
$\binom{k}{2} = \Pi_3(l)$ (Tzanakis and de Weger [118]),
$\binom{k}{2} = \Pi_4(l)$ (Pintér [82], see also [43], p. 225.),
$\binom{k}{4} = \binom{l}{2}$ (Pintér [83] and de Weger [121]),
$\binom{k}{3} = \binom{l}{4}$ (de Weger [122]),
$\binom{k}{4} = \Pi_2(l), \Pi_3(l)$ (Pintér and de Weger [86]),
$\binom{k}{m} = \Pi_n(l)$, where $(m,n) = (3,6;3,6)$ (Stroeker and de Weger [106]),
$\binom{k}{m} = \binom{l}{n}$, where $(m,n) = (2;3,4,6,8), (3;4,6), (4;6,8)$ (Stroeker and de Weger [107]),

Equation	Solutions
$S_3(k) = \Pi_2(l)$	$(k,l) = (-1,0;-1,0)$
$S_3(k) = \Pi_4(l)$	$(k,l) = (-1,0;-3,-2,-1,0)$
$S_3(k) = \Pi_8(l)$	$(k,l) = (-1,0;-7,-6,-5,-4,-3,-2,-1,0)$
$S_5(k) = \binom{l}{3}$	$(k,l) = (-1,0;0,1,2),(-2,1;3)$
$S_7(k) = \binom{l}{2}$	$(k,l) = (-1,0;0,1),(-2,1;-1,2)$
$P_2(k) = \Pi_4(l)$	$(k,l) = (-1,0;-3,-2,-1,0)$
$P_2(k) = \Pi_8(l)$	$(k,l) = (-1,0;-7,-6,-5,-4,-3,-2,-1,0)$
$P_3(k) = \Pi_6(l)$	$(k,l) = (-2,-1,0;-5,-4,-3,-2,-1,0),(8;-6,1)$
$P_4(k) = \Pi_8(l)$	$(k,l) = (-3,-2,-1,0;-7,-6,-5,-4,-3,-2,-1,0)$

Table 2.1: Equations which can be solved by Runge's method

$S_5(k) = \binom{l}{2}$, $S_5(k) = \binom{l}{4}$, $S_m(k) = \Pi_n(l)$, where $(m,n) = (2,5;2,4)$, $\binom{k}{m} = \Pi_n(l)$, where $(m,n) = (2,4;6),(3,6;2,4)$, $\Pi_4(k) = \Pi_6(l)$ (Hajdu and Pintér [52]).

Here and later on $(k,l) = (a_1,\dots,a_n;b_1,\dots,b_m)$ means that (k,l) can be any of the pairs (a_i,b_j), $i \in \{1,\dots,n\}$, $j \in \{1,\dots,m\}$.

We mention that $S_n(x)$ is a polynomial of degree $n+1$, and $\Pi_n(x)$ is a polynomial of degree n. For the sake of completeness we give all integer solutions of the investigated polynomial equations (although the negative solutions do not have combinatorial meanings). Our results are summarized in the next theorem. We distribute the equations considered into three tables, according to the methods used in their solutions.

Theorem 2.2.1. *All integral solutions of the equations in the first columns of Tables 2.1-2.3 are exactly the ones appearing in the second columns of the tables, respectively.*

2.3 Proof of Theorem 2.2.1

Proof of Theorem 2.2.1. The considered Diophantine equations can be divided into three groups.

Equations which can be solved by Runge's method. Consider the Diophantine equation $F(u) = G(v)$, where F and G are monic polynomials with integer coefficients, $F(u) - G(v)$ is irreducible in $\mathbb{Q}[u,v]$ and $\gcd(\deg F, \deg G) > 1$.

Equation	Solutions
$S_3(k) = \binom{l}{3}$	$(k,l) = (-1,0;0,1,2), (-2,1;3)$
$S_3(k) = \binom{l}{6}$	$(k,l) = (-1,0;0,1,2,3,4,5), (-2,1;-1,6)$
$S_3(k) = \Pi_3(l)$	$(k,l) = (-1,0;-2,-1,0)$
$S_3(k) = \Pi_6(l)$	$(k,l) = (-1,0;-5,-4,-3,-2,-2,-1,0)$
$S_5(k) = \binom{l}{2}$	$(k,l) = (-1,0;0,1), (-2,1;-1,2), (-4,3;-23,24),$ $(-9,8;-351,352)$
$S_5(k) = \binom{l}{4}$	$(k,l) = (-1,0;0,1,2,3), (-2,1;-1,4)$
$S_5(k) = \Pi_2(l)$	$(k,l) = (-1,0;-1,0)$
$S_5(k) = \Pi_4(l)$	$(k,l) = (-1,0;-3,-2,-1,0)$

Table 2.2: Equations which can be reduced to Mordell-type equations

We can use the method of Runge [93] for computing the integer solutions of such equations. Among the combinatorial Diophantine equations considered in Theorem 2.2.1, there are several ones which can be treated by this method. These equations are collected in Table 2.1. For example, using that

$$S_5(k) = \frac{1}{12}(2k^6 - 6k^5 + 5k^4 - k^2) = \frac{1}{12}(2(k^2-k)^3 - (k^2-k)^2),$$

the equation $S_5(k) = \binom{l}{3}$ can be transformed to the equation $u^3 - u^2 = v^3 - 6v^2 + 8v$ with the substitutions $u = 2k^2 - 2k$, $v = 2l$, and the method of Runge can be applied. There are several results and efficient algorithms for finding the integer solutions of Runge-type equations, see for example Masser [67], Schinzel and Grytschuk [42], Szalay [110], Tengely [112] and Walsh [123] and the references given there. Tengely implemented his algorithm from [112] in the Magma computational algebra system [17] and made it accessible on the internet site www.math.klte.hu/∼tengely. We computed all integer solutions of the equations in Table 2.1 with Tengely's program. The total running time of the program was only a few minutes.

Equations which can be reduced to Mordell-type equations. Under a Mordell-type equation we mean a Diophantine equation $F(u) = G(v)$ with $\deg F = 3$, $\deg G = 2$ or conversely. These equations can be simply solved with Magma by the procedure `IntegralPoints`. The algorithm is based upon a theorem obtained independently by Gebel, Pethő and Zimmer [41] and Stroeker and Tzanakis [103] that was mentioned in Section 1.2. We collected the equations which can be reduced to Mordell-type equations in Table 2.2. For example, the

Equation	Solutions
$S_1(k) = \binom{l}{4}$	$(k,l) = (-21,20;-7,10), (-6,5;-3,6),$ $(-2,1;-1,4), (-1,0;0,1,2,3)$
$S_1(k) = \binom{l}{8}$	$(k,l) = (-1,0;0,1,2,3,4,5,6,7), (-2,1;-1,8),$ $(-10,9;-3,10;), (-78,77;-7,14), (-221,220;-10,17)$
$S_1(k) = \Pi_4(l)$	$(k,l) = (-16,15;-5,2), (-1,0;-3,-2,-1,0))$
$S_1(k) = \Pi_8(l)$	$(k,l) = (-1,0;-7,-6,-5,-4,-3,-2,-1,0)$
$S_2(k) = \binom{l}{3}$	$(k,l) = (-1,0;0,1,2), (-2,-1), (1,3)$
$S_2(k) = \binom{l}{6}$	$(k,l) = (-1,0;0,1,2,3,4,5), (1;-1,6)$
$S_2(k) = \Pi_3(l)$	$(k,l) = (-1,0;-2,-1,0)$
$S_2(k) = \Pi_6(l)$	$(k,l) = (-1,0;-5,-4,-3,-2,-1,0)$
$S_3(k) = \binom{l}{2}$	$(k,l) = (-4,3;-8,9), (-2,1;-1,2), (-1,0;0,1)$
$S_3(k) = \binom{l}{4}$	$(k,l) = (-2,1;-1,4), (-1,0;0,1,2,3)$
$S_3(k) = \binom{l}{8}$	$(k,l) = (-1,0;0,1,2,3,4,5,6,7), (-3,2;-2,9),$ $(-2,1;-1,8)$
$S_5(k) = \binom{l}{6}$	$(k,l) = (-1,0;0,1,2,3,4,5), (-2,1;-1,6)$
$S_5(k) = \Pi_3(l)$	$(k,l) = (-1,0;-2,-1,0)$
$S_5(k) = \Pi_6(l)$	$(k,l) = (-1,0;-5,-4,-3,-2,-1,0)$
$S_7(k) = \binom{l}{4}$	$(k,l) = (-2,1;-1,4), (-1,0;0,1,2,3)$
$S_7(k) = \Pi_2(l)$	$(k,l) = (-1,0;-1,0)$
$S_7(k) = \Pi_4(l)$	$(k,l) = (-1,0;-3,-2,-1,0)$
$\binom{k}{2} = \Pi_8(l)$	$(k,l) = (0,1;-7,-6,-5,-4,-3,-2,-1,0)$
$\binom{k}{4} = \Pi_4(l)$	$(k,l) = (0,1,2,3;-3,-2,-1,0)$
$\binom{k}{4} = \Pi_8(l)$	$(k,l) = (0,1,2,3;-7,-6,-5,-4,-3,-2,-1,0)$
$\binom{k}{8} = \Pi_2(l)$	$(k,l) = (0,1,2,3,4,5,6,7;-1,0)$
$\binom{k}{8} = \Pi_4(l)$	$(k,l) = (0,1,2,3,4,5,6,7;-3,-2,-1,0)$

Table 2.3: Equations which can be reduced to genus 1 equations

equation $S_3(k) = \binom{l}{3}$ can be written as $3((k-1)k)^2 = 2l(l-1)(l-2)$, which reduces to the Mordell- type equation $3u^2 = 2v^3 - 6v^2 + 4v$ by the substitutions $u = (k-1)k$ and $v = l$. We determined all the integer solutions of these equations with Magma, and listed them in Table 2.2.

Equations which can be reduced to genus 1 equations. Table 2.3 contains equations that can be transformed into genus 1 equations with simple integral transformations. As finding the integer solutions of an equation of genus 1 is not at all automatic, we give some details at this point. The method we use is the $\mathcal{E}llog$ method of Stroeker and Tzanakis [105]. In the remaining part of this section, we follow the discussion and terminology of Section 1.2 without any further reference.
The algorithm discussed in Section 1.2 can always be used in cases when equation (1.2) has the form $F(u) = G(v)$, where $F, G \in \mathbb{Z}[x]$ with $\deg F = 4$, $\deg G = 2$ (quartic case) or $\deg F = \deg G = 3$ (cubic case). Among the equations in Table 2.3 the followings reduce to quartic ones:

$$
\begin{array}{llll}
S_1(k) = \binom{l}{4}, & S_1(k) = \binom{l}{8}, & S_1(k) = \Pi_4(l), & S_1(k) = \Pi_8(l), \\
S_3(k) = \binom{l}{2}, & S_3(k) = \binom{l}{4}, & S_3(k) = \binom{l}{8}, & S_7(k) = \binom{l}{4}, \\
S_7(k) = \Pi_2(l), & S_7(k) = \Pi_4(l), & \binom{k}{2} = \Pi_8(l), & \binom{k}{4} = \Pi_4(l), \\
\binom{k}{4} = \Pi_8(l), & \binom{k}{8} = \Pi_2(l), & \binom{k}{8} = \Pi_4(l). &
\end{array}
$$

To transform these equations to the desired shape, we make use of the fact that all of $S_{2i-1}(x)$, $\binom{x}{2i}$ and $\Pi_{2i}(x)$ can be written in the form $F(G(x))$, where $F, G \in \mathbb{Q}[x]$ with $\deg G = 2$, $\deg F = i$. For example, we have

$$S_7(k) = \frac{1}{24}(3k^8 - 12k^7 + 14k^6 - 7k^4 + 2k^2) = \frac{1}{24}(3(k^2-k)^4 - 4(k^2-k)^3 + 2(k^2-k)^2)$$

and

$$\Pi_4(l) = l(l+1)(l+2)(l+3) = (l^2+3l)(l^2+3l+2).$$

Hence, the equation $S_7(k) = \Pi_4(l)$ can be transformed to the equation $3u^4 - 4u^3 + 2u^2 = 6v^2 + 24v$ with the substitutions $u = k^2 - k$, $v = 2(l^2+3l)$.

Note that the program package Magma contains a procedure (namely `IntegralQuarticPoints`) which is able to locate all integral points on quartic equations in some cases. (For details see the Magma manual [17].) However, in

the previous versions of Magma this procedure apparently contains some error, and we solved all these equations following the $\mathcal{E}llog$ method step-by-step. In case of each equation, we obtained exactly the solutions listed in Table 2.3. Note that in the new version of Magma (V.2.13-9) distributed by the beginning of 2007 the procedure `IntegralQuarticPoints` seems to be correct, and by its help we have also solved the above quartic equations except for $\binom{k}{8} = \Pi_2(l)$, $\binom{k}{8} = \Pi_4(l)$ and $S_1(k) = \binom{l}{8}$. In these cases Magma is only able to guarantee that `IntegralQuarticPoints` gives all integral points in a subgroup of the curve of finite index. In the other cases we have obtained the same solutions as in Table 2.3.

Now we turn to the cubic case. From Table 2.3 the following equations belong to this group:

$$S_2(k) = \binom{l}{3}, \quad S_2(k) = \binom{l}{6}, \qquad S_2(k) = \Pi_3(l), \quad S_2(k) = \Pi_6(l),$$
$$S_5(k) = \binom{l}{6}, \quad S_5(k) = \Pi_3(l), \quad S_5(k) = \Pi_6(l).$$

In this case no implemented version of the procedure is available, and we follow the $\mathcal{E}llog$ method step-by-step for each equation. As an example, we illustrate the algorithm for finding the integer solutions of the equation $S_2(k) = \Pi_6(l)$. Substituting $u = k - 1$, $v = l^2 + 5l$, we get

$$f(u, v) = 2u^3 + 3u^2 + u - 6v^3 - 60v^2 - 144v = 0. \tag{2.1}$$

Put

$$C = \left\{(u, v) \in \mathbb{Q}^2 \mid f(u, v) = 0\right\}.$$

We use Magma to perform the following computations. Equation (2.1) can be transformed into the short Weierstrass equation

$$y^2 = x^3 - 1008x + 2985993$$

with the birational transformation

$$x = X(u, v) = 6\frac{1439v + 6902u + 10358}{144v - u}, y = Y(u, v) =$$
$$= 3\frac{124296v^2 - 414288uv + 1242960v + 1990654u + 2983104 + 2877u^2}{(u - 144v)u}.$$

Set

$$E = \left\{(x, y) \in \mathbb{Q}^2 \mid y^2 = x^3 - 1008x + 2985993\right\}.$$

It turns out that the rank of E is $r = 6$, and the only torsion point of E is $\mathcal{O}$. Further, a basis of the Mordell-Weil group of E is

$$\begin{array}{ll} P_1 = (24, 1725), & \hat{h}(P_1) = 1.717986\ldots, \\ P_2 = (-36, 1725), & \hat{h}(P_2) = 1.721482\ldots, \\ P_3 = (234, 3945), & \hat{h}(P_3) = 1.924237\ldots, \\ P_4 = (354, -6855), & \hat{h}(P_4) = 2.062256\ldots, \\ P_5 = (36, -1731), & \hat{h}(P_5) = 2.123124\ldots, \\ P_6 = (-144, 381), & \hat{h}(P_6) = 2.165316\ldots, \end{array}$$

where the Néron-Tate heights of the basis points are also indicated. Let

$$P = n_1P_1 + \ldots + n_6P_6 \quad (n_i \in \mathbb{Z}, i = 1, \ldots, 6)$$

be a point of E, which is the image of an integer point of C. In this case the linear form (1.6) is of the shape

$$\mathcal{L} = n_0\omega + n_1u_1 + n_2u_2 + n_3u_3 + n_4u_4 + n_5u_5 + n_6u_6 - u_7,$$

where ω is the fundamental real period, and u_i are the elliptic logarithms of the points P_i $(i = 1, \ldots, 6)$ and R_0, respectively. We have

$$R_0 = \left(6\frac{1439 + 6902 \cdot \sqrt[3]{3}}{144 - \sqrt[3]{3}}, 361\frac{\sqrt[3]{3}}{3} + 864\sqrt[3]{9} + 8649\right)$$

and

$$\omega = 0.704584\ldots, \ u_1 = 0.220969\ldots, u_2 = 0.255688\ldots, u_3 = 0.128958\ldots,$$
$$u_4 = 0.598701\ldots, u_5 = 0.490562\ldots, u_6 = 0.340110\ldots, u_7 = 0.091196\ldots.$$

We deduce an upper bound for $N = \max_{1 \le i \le 6} |n_i|$. With the previous notation we have

$$G(u, v) = 2\frac{\partial_u Y(u, v) \cdot \partial_v f(u, v) - \partial_v Y(u, v) \cdot \partial_u f(u, v)}{3X^2(u, v) - 1008} = -2.$$

If $U(P) \ge T$ then

$$\int_{U(P)}^{\infty} \frac{G(u, v)du}{\partial_v f(u, v)} = \int_{x(P)}^{x_{0i}} \frac{dx}{\varepsilon\sqrt{q(x)}},$$

where T is the maximum of the first coordinates of the poles of X and Y; now we have $T = 0$. Since

$$4.1u^2 < 9v^2 + 60v + 72$$

for all integer solutions u, v of (2.1)

$$\int_{U(P)}^{\infty} \frac{G(u,v)du}{\partial_v f(u,v)} = \int_{U(P)}^{\infty} \frac{1}{9v^2 + 60v + 72} du < \frac{1}{4.1\,|u|}$$

holds. Using the explicit form of $X(u,v)$, we obtain that

$$h(X(u,v)) < 11.953526 + \log|u|\,.$$

Furthermore, by a result of Cremona, Prickett and Siksek [34] we get that

$$\hat{h}(P) - \frac{1}{2}h(P) < 2.838410,$$

whence

$$\hat{h}(P) < 8.815173 + \frac{1}{2}\log|u|\,.$$

Additionally,

$$\hat{h}(P) \geq \lambda N^2$$

where $\lambda = 0.299043\ldots$ is the smallest eigenvalue of $\hat{h}$ with respect to the basis $P_1, \ldots, P_6$. From the above inequalities we obtain the upper bound

$$|\mathcal{L}| < 1.106568 \cdot 10^7 \cdot \exp(-0.598086N^2).$$

We deduce a lower bound for N by Lemma 1.2.1. We have

$$\omega_1 = 0.365010\ldots - i \cdot 0.201383\ldots, \quad \omega_2 = 0.365010\ldots + i \cdot 0.201383\ldots,$$

whence

$$\tau = 0.533276\ldots + i \cdot 0.845940\ldots,$$

and

$$j_E = \tfrac{-9710862336}{330222313475}, \quad A_i = h_E = 26.523031\ldots, \quad (i = 0, \ldots, 7),$$

$$D = 3, \quad c_8 = 1.227240 \cdot 10^{354}, \quad c_9 = 2.098612, \quad c_{10} = 28.621644.$$

Hence by Lemma 1.2.1 we obtain the lower bound

$$|\mathcal{L}| > \exp\left(-1.22724 \cdot 10^{354}(\log(N') + 2.09862)(\log(\log(N')) + 28.62165)^9\right).$$

Using that $N' \leq 6N + 1$ and combining the upper and lower bounds for the linear form $\mathcal{L}$, we get the initial bound

$$N < K_3 = 2.753 \cdot 10^{185}.$$

We reduce this bound by the LLL-algorithm, using Lemma 1.2.2. The constants K_1 and K_2 are given by

$$K_1 = 1.570524 \cdot 10^7, \quad K_2 = 0.598086.$$

The reduction steps are summarized in the following table:

bound for N	K_0	new bound for N
$2.753 \cdot 10^{185}$	$5.3 \cdot 10^{1322}$	67
67	$6.4 \cdot 10^{47}$	15
15	$5.5 \cdot 10^{16}$	9

After the third iteration we obtain $N \leq 9$, which cannot be improved further. The inverse of the birational transformation X and Y are

$$u = U(x, y) = \frac{-6\,(16x + 767)\,(36x + 431)}{10x^2 + 24xy + 206808x - 1439y + 5462793},$$

$$v = V(x, y) = \frac{-24x^2 + 992449x - 10358y + 29808030}{10x^2 + 24xy + 206808x - 1439y + 5462793}.$$

Using these functions, we can compute all the integer points of C. These are given by

$$(u, v) = (-1, 0; -6, -4, 0), (-33, -26), (-14, -13), (-11, -11), (2, -5).$$

In view of the original substitution, all integer solutions of the equation $S_2(k) = \Pi_6(l)$ are

$$(k, l) = (0, 1; -5, -4, -3, -2, -1, 0).$$

The integer solutions of all other cubic and quartic equations can be determined with a similar process and the solutions are exactly those which are summarized in Table 2.3. Hence Theorem 2.2.1 is proved. □

Chapter 3

Combinatorial numbers in binary recurrences

3.1 Introduction

There are many papers about values of a polynomial $p(x) \in \mathbb{Q}[x]$ (taken at integer values of x) in a binary linear recurrence sequence U. The first such results dealt with the case where U is a special sequence and $p(x) = x^m$ with some $m \geq 2$. That is, we are interested in terms of U which are perfect powers. In 1962 Ogilvy [77], one year later Moser and Carlitz [73], and Rollett [92] proposed the following problem: determine all squares in the Fibonacci sequence F. The problem was solved by Cohn [29, 30] and Wyler [125] who independently proved with elementary methods that the only squares in the Fibonacci sequence are $F_0 = 0, F_1 = F_2 = 1, F_{12} = 144$. Later, Alfred [1] and Cohn [31] determined the squares in the Lucas sequence L. Pethő [80] and Cohn [32] independently determined the perfect powers in the Pell sequence. Recently, Bugeaud, Mignotte and Siksek [28] showed that the perfect powers in the Fibonacci and Lucas sequences are exactly $F_0 = 0, F_1 = F_2 = 1, F_6 = 8, F_{12} = 144$, and $L_1 = 1, L_3 = 4$, respectively.

Another branch of problems is about triangular numbers in recurrence sequences, i.e. we take the polynomial $p(x) = \frac{x(x+1)}{2}$. Hoggatt stated the conjecture that there are only five triangular Fibonacci numbers. In 1989 Ming [69] proved that this conjecture is true. Furthermore, Ming [70] and McDaniel [68] determined the triangular numbers in the Lucas and Pell sequences, respec-

tively. In [108] Szalay described all values of the polynomials $S_2(x)$ and $S_3(x)$ in the Fibonacci, Lucas and Pell sequences, where $S_k(x)$ denotes the sum of the first $x-1$ kth powers ($x \in \mathbb{N}$). Further, he listed all numbers of the form $\binom{x}{4}$ in the Fibonacci and Lucas sequences, as well. As a generalization of the previous results, Tengely [114] determined the g-gonal numbers in the Fibonacci, Lucas, Pell and Associated Pell sequences for $g \leq 20$. Recently, Tengely [115] showed that the only term of the form $\binom{x}{5}$ of the Lucas sequence is $L_1 = 1$.

The above mentioned results give complete solutions of the problem in case of certain sequences U and polynomials p. Beside them there are several results in the literature which provide effective upper bounds for the solutions under certain assumptions. The most extensively investigated case is about perfect powers, i.e. where $p(x) = x^m$ with some $m \geq 2$. Instead of trying to survey the extremely huge literature we only refer to the book [99] and the references given there. Finally, we mention that Szalay [108] provided an algorithm for the complete description of the values of a polynomial $p(x)$ of degree 3 in a binary recurrence sequence U under some assumptions.

In this chapter we prove three theorems concerning the values of some polynomials in binary recurrence sequences. First we provide an effective finiteness theorem for certain combinatorial numbers, namely for binomial coefficients, products of consecutive integers, power sums and alternating power sums in binary recurrence sequences, under some assumptions. The proof of this theorem is based on Baker's method together with certain results of Brindza [19], Ping-Zhi [81], Pintér and Rakaczki [85] and Rakaczki [90]. Our second result is an extension of the above mentioned result of Szalay. More precisely, it provides an efficient algorithm for determining the values of certain degree 4 polynomials in binary recurrence sequences, under some assumptions. In particular, we implemented the main part of our algorithm in Magma [17]. Finally, partly by the help of this algorithm we give all combinatorial numbers mentioned above for the small values of the parameter involved in the Fibonacci, Lucas, Pell and Associated Pell sequences. We mention that to prove the latter result we reduce the problem to elliptic and more generally to genus 1 equations. We use the $\mathcal{E}llog$ method and the program package Magma to resolve our particular equations. The results of Chapter 3 are published in [59].

3.2 Notation

Let $U = \{U_n\}_{n=0}^{\infty}$ be a binary recurrence sequence defined by the initial terms $U_0, U_1 \in \mathbb{Z}$ and the recurrence relation

$$U_n = AU_{n-1} + BU_{n-2} \quad (n \geq 2)$$

where A, B are non-zero integers. Let α and β denote the zeros of the companion polynomial $x^2 - Ax - B$ of U. Further, let $D = A^2 + 4B$ be the discriminant of U and

$$a_u = U_1 - \beta U_0, \quad b_u = U_1 - \alpha U_0, \quad C = a_u b_u = U_1^2 - AU_0U_1 - BU_0^2.$$

The sequence U is called non-degenerate if $C \neq 0$ and α/β is not a root of unity. It is well-known that if U is non-degenerate then for all $n = 0, 1, \ldots$ we have

$$U_n = \frac{a_u\alpha^n - b_u\beta^n}{\alpha - \beta}.$$

From this point on we assume that $B = \pm 1$ and that U is non-degenerate. Then as it is also well-known, U has a so-called associate sequence $V = \{V_n\}_{n=0}^{\infty}$ for which

$$V_n^2 - DU_n^2 = 4C(-B)^n \tag{3.1}$$

holds for all $n = 0, 1, \ldots$. Observe that by our assumption $B = \pm 1$, we have $(-B)^n = \pm 1$. Further, note that $V_0 = 2U_1 - AU_0$, $V_1 = AU_1 + 2BU_0$ and V satisfies the same recurrence relation as U.

Beside dealing with general sequences U we consider combinatorial numbers in certain special famous sequences, too. Let F, L, P and Q denote the Fibonacci, Lucas, Pell and Associated Pell sequence, respectively. These sequences are defined by

$$\begin{array}{llll} F_0 = 0, & F_1 = 1, & F_n = F_{n-1} + F_{n-2} & (n \geq 2), \\ L_0 = 2, & L_1 = 1, & L_n = L_{n-1} + L_{n-2} & (n \geq 2), \\ P_0 = 0, & P_1 = 1, & P_n = 2P_{n-1} + P_{n-2} & (n \geq 2), \\ Q_0 = 1, & Q_1 = 1, & Q_n = 2Q_{n-1} + Q_{n-2} & (n \geq 2). \end{array}$$

Now we give what kind of combinatorial numbers we are interested in. Beside binomial coefficients, we consider power sums, alternating power sums and products of consecutive integers as well. In Chapter 2 we defined these polynomials except for the alternating power sum. That polynomial is defined for all $k, x \in \mathbb{N}$ as

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

We mention that $R_k(x)$ is a polynomial of degree k.

3.3 New results

We use the previous notation. Further, recall that $B = \pm 1$ and $U = \{U_n\}_{n=0}^{\infty}$ is non-degenerate. All our results concern the equation

$$U_n = p(x) \tag{3.2}$$

in integers n, x with $n \geq 0$. For the sake of completeness we also take care of the solutions with $x \leq 0$, although these solutions usually do not have combinatorial meanings.

First we give an effective result for the solutions of (3.2) which is valid for general U.

Theorem 3.3.1. *Let $k \geq 2$ and $p(x)$ be one of the polynomials $S_{k-1}(x)$, $R_k(x)$, $\Pi_k(x)$, $\binom{x}{k}$. If either $k = 2$ or $p(x)$ is one of $S_2(x), \Pi_3(x), \binom{x}{3}$, then further assume that $B = 1$. Then the solutions n, x of equation (3.2) satisfy $\max(n, |x|) < c_0(U, k)$, where $c_0(U, k)$ is an effectively computable constant depending only on U and k.*

Obviously, the assumption $k \geq 2$ cannot be omitted. The next proposition shows that the condition $B = 1$ in the special cases of the theorem is necessary as well.

Proposition 3.3.1. *Let U be the sequence defined by $B = -1$ and by the values U_0, U_1, A given in the ith row of Table 3.1, for any $i \in \{1, 2, 3, 4, 5\}$. Further, let $p(x)$ be a polynomial from the last column of the ith row of Table 3.1. Then equation (3.2) has infinitely many solutions.*

U_0	U_1	A	$p(x)$
1	253	254	$S_1(x), R_2(x), \binom{x}{2}$
2	506	254	$\Pi_2(x)$
1	3759787041401	3760028828350	$S_2(x)$
7770	455962704852690	58682458798	$\binom{x}{3}$
46620	2735776229116140	58682458798	$\Pi_3(x)$

Table 3.1: Settings where equation (3.2) has infinitely many solutions

Remark. If (3.2) has infinitely many solutions then these solutions have some special structure. This structure has been described by Nemes and Pethő [74], see Theorem 3 (cf. also [78], [79]). It turns out that the solutions x belong to certain recurrence sequences, while the solutions n come from some arithmetic progressions. For details see [74], [78] and [79]. Furthermore, to find the examples provided by Table 3.1, the above mentioned Theorem 3 of [74] can also be used. In the beginning of the proof of Proposition 3.3.1 we shall show that our examples do satisfy the conditions of Theorem 3 of [74]. Since the assumptions of Theorem 3 of [74] are not sufficient (see Remark 2 of [74]), it remains necessary to show that in these cases (3.2) really has infinitely many solutions. We also mention that for all polynomials that occur in Table 3.1 using the method in [74] many more binary recurrence sequences can be constructed with infinitely many solutions for equation (3.2).

As we mentioned above, Szalay [108] gave an algorithm for the resolution of (3.2) in the case when $p(x)$ is a polynomial of degree 3. We extend this result to the degree 4 case. For this purpose we need some further notation. Let $p(x) \in \mathbb{Q}[x]$ be a polynomial of degree 4 and write

$$p(x) = A_0x^4 + A_1x^3 + A_2x^2 + A_3x + A_4.$$

Suppose that the coefficients of p fulfill the relations

$$A_0 = \frac{a}{e}, A_1 = \frac{4ab}{e}, A_2 = \frac{6ab^2 + c}{e}, A_3 = \frac{4ab^3 + 2bc}{e}, A_4 = \frac{ab^4 + b^2c + d}{e},$$

with some integers a, b, c, d, e, $ae \neq 0$. Then we have

$$p(x) = \frac{a(x + b)^4 + c(x + b)^2 + d}{e}.$$

Write $x_1 = x + b$ and let $y = V_n$ where $V = \{V_n\}_{n=0}^{\infty}$ is the associate sequence of U. Then by (3.1) we get

$$y^2 - D\left(\frac{ax_1^4 + cx_1^2 + d}{e}\right)^2 = 4C(-B)^n,$$

which yields

$$Y^2 = h_4X^4 + h_3X^3 + h_2X^2 + h_1X + h_0, \tag{3.3}$$

where

$$Y = ey, \quad X = x_1^2, \quad h_4 = a^2D, \quad h_3 = 2acD,$$

$$h_2 = (c^2 + 2ad)D, \quad h_1 = 2cdD, \quad h_0 = d^2D + 4e^2C(-B)^n.$$

Equation (3.3) in general is of genus 1, therefore the $\mathcal{E}llog$ method can be used to determine all its integral solutions. In particular, using the program package Magma, equation (3.3) can be solved completely in concrete cases. If h_0 is a perfect square then (3.3) can be solved directly by the procedure `IntegralQuarticPoints`. Putting together some tools and results about genus 1 curves, we give an efficient method for the resolution of (3.3) in the general case. For the description of the method see the proof of Theorem 3.3.2. (Further, as we mentioned we implemented our algorithm in Magma, too.) From the solutions, the values x and the indices n can be easily determined.

Summarizing the above argument, we get

Theorem 3.3.2. *Using the previous notation, suppose that* $8aDd(2ad - c^2) \neq -64a^2C \pm e^2 - c^4D$. *Then equation* (3.2) *has only finitely many solutions* n, x *and these solutions can be effectively determined.*

Our final result completely describes the above type combinatorial numbers for the small values of the parameter k in some well-known binary recurrence sequences.

Theorem 3.3.3. *Let* $U \in \{F, L, P, Q\}$ *and* $p(x) \in \{S_1(x), S_2(x), S_3(x), R_2(x), R_4(x), \Pi_2(x), \Pi_3(x), \Pi_4(x), \binom{x}{2}, \binom{x}{3}, \binom{x}{4}\}$. *Then the solutions* n, x *of equation* (3.2) *are exactly those contained in Table 3.2. The sign "–" shows that the actual equation has no solution. Further, the references given in the table indicate that the corresponding equation was solved in the appropriate paper.*

Remark. The complete solution of the equation $U_n = R_3(x)$ remains open. In this case by relation (3.1) and with the substitution $y = V_n$ we get the equation

$$y^2 = D\frac{4x^6 - 12x^5 + 9x^4}{16} + 4C(-B)^n,$$

if x is even and

$$y^2 = D\frac{4x^6 - 12x^5 + 9x^4 + 4x^3 - 6x^2 + 1}{16} + 4C(-B)^n,$$

if x is odd. These equations are of genus 2 thus neither Szalay's method nor our algorithm given in the proof of Theorem 3.3.2 can be used to solve them.

$=$	F_n	L_n	P_n	Q_n
$S_1(x)$	[69]	[70]	[68]	$(0,-1),(0,2),$ $(1,-1),(1,2),$ $(2,-2),(2,3)$
$S_2(x)$	[108]	[108]	[108]	$(0,2),(1,2)$
$S_3(x)$	[108]	[108]	[108]	$(0,-1),(0,2),$ $(1,-1),(1,2)$
$T_2(x)$	$(0,0),(0,1),$ $(1,-1),(2,-1),$ $(4,3),(8,7),$ $(10,11)$	$(1,-1),(2,3),$ $(18,-107)$	$(1,-1)$	$(0,-1),(1,-1),$ $(2,3)$
$T_4(x)$	$(0,0),(0,1),$ $(1,-1),(2,-1)$	$(1,-1)$	$(0,0),(0,1),$ $(1,-1)$	$(0,-1),(1,-1)$
$\Pi_2(x)$	$(0,-1),(0,0),$ $(3,-2),(3,1)$	–	$(0,-1),(0,0),$ $(2,-2),(2,1),$ $(4,-4),(4,3)$	–
$\Pi_3(x)$	$(0,-2),(0,-1),$ $(0,0)$	–	$(0,-2),(0,-1),$ $(0,0)$	–
$\Pi_4(x)$	$(0,-3),(0,-2),$ $(0,-1),(0,0)$	–	$(0,-3),(0,-2),$ $(0,-1),(0,0)$	–
$\binom{x}{2}$	[69]	[70]	[68]	$(0,-1),(0,2),$ $(1,-1),(1,2),$ $(2,-2),(2,3)$
$\binom{x}{3}$	[109]	[109]	[109]	–
$\binom{x}{4}$	[108]	[108]	$(0,0),(0,1),$ $(0,2),(0,3),$ $(1,-1),(1,4),$ $(3,-2),(3,5),$ $(6,-5),(6,8)$	$(1,-1),(1,4)$

Table 3.2: Solutions of equation (3.2) with the particular settings

3.4 Proofs

We need some new concepts and also some lemmas for the proof of Theorem 3.3.1. A polynomial $f(x) \in \mathbb{C}[x]$ is called non-degenerate if it has at least three zeros of odd multiplicities.

Lemma 3.4.1 (Brindza [19]). *Let b be a non-zero rational number and $f(x) \in \mathbb{Q}[x]$ a non-degenerate polynomial. Then for the integral solutions x, y of the hyperelliptic equation*

$$f(x) = by^2$$

we have $\max(|x|, |y|) < c_1$, where c_1 is an effectively computable constant depending only on b and f.

Proof. This is a special case of the Theorem in [19]. □

Lemma 3.4.2 (Ping-Zhi [81]). *Let k be an integer with $k \geq 5$, b an algebraic number and put $f_k(x) = \binom{x}{k} - b$. Then apart from the cases when $k = 6, b = -\frac{10 \pm 7\sqrt{7}}{1215}$, the polynomial $f_k(x)$ is non-degenerate.*

Proof. See the proof of Theorem 2 in [81]. □

Further on, let $B_k(x)$ and $E_k(x)$ denote the kth Bernoulli and Euler polynomial, respectively (see e.g. [87]).

Lemma 3.4.3 (Pintér and Rakaczki [85]). *If k is an integer with $k \geq 5$ and a, b are complex numbers with $b \neq 0$ then the polynomial $(B_k(x) + a)^2 + b$ is non-degenerate.*

Proof. This is Lemma 5 in [85]. □

Lemma 3.4.4 (Rakaczki [90]). *If k is an integer with $k \geq 5$ and a, b are complex numbers with $b \neq 0$ then the polynomial $(E_k(x) + a)^2 + b$ is non-degenerate.*

Proof. This is Lemma 2 in [90]. □

Now we have all the tools to prove Theorem 3.3.1.

Proof of Theorem 3.3.1. We split the proof into three parts according to the value of k. In each part we investigate the possible choices for $p(x)$ in turn.

The case $k \geq 5$. Assume first that $p(x) = \binom{x}{k}$. By (3.1) with $y = V_n$, we get

$$y^2 = D\binom{x}{k}^2 + 4C(-B)^n,$$

for which by factoring the right-hand side we obtain

$$y^2 = D\left(\binom{x}{k} + 2\sqrt{\frac{-C(-B)^n}{D}}\right)\left(\binom{x}{k} - 2\sqrt{\frac{-C(-B)^n}{D}}\right). \tag{3.4}$$

Note that as $B = \pm 1$ and $C \neq 0$ the zeros of the two factors on the right-hand side of (3.4) must be distinct. Thus by Lemmas 3.4.1 and 3.4.2 it is enough to consider the cases where

$$k = 6, b = -\frac{10 \pm 7\sqrt{7}}{1215}.$$

Hence by a simple calculation we get that one of the factors of the right-hand side of (3.4) is non-degenerate. Thus by Lemma 3.4.1 the theorem follows.

Now let $p(x) = \Pi_k(x)$. By (3.1) with $y = V_n$ we obtain that

$$y^2 = D\Pi_k(x)^2 + 4C(-B)^n. \tag{3.5}$$

Since $\Pi_k(x) = k!\binom{x+k-1}{k}$, and a non-zero constant multiple of a non-degenerate polynomial is non-degenerate, by the previous argument the polynomial on the right-hand side of (3.5) is non-degenerate. Thus the theorem follows also in this case.

Assume that $p(x) = S_{k-1}(x)$. It is well-known that

$$S_{k-1}(x) = \frac{1}{k}(B_k(x) - B_k(0)),$$

where $B_k(x)$ is the kth Bernoulli polynomial. Thus by (3.1) with $y = V_n$ we have

$$y^2 = \frac{D}{k^2}\left((B_k(x) - B_k(0))^2 + \frac{4C(-B)^n k^2}{D}\right). \tag{3.6}$$

Applying Lemma 3.4.3 with $a = -B_k(0)$ and $b = \frac{4C(-B)^n k^2}{D} \neq 0$, the polynomial on the right-hand side of (3.6) is non-degenerate. So the theorem follows again by Lemma 3.4.1.

Finally, let $p(x) = R_k(x)$. It is well-known that for all $k \in \mathbb{N}$

$$R_k(x) = \frac{1}{2}(E_k(0) + (-1)^{x+1}E_k(x))$$

holds, where $E_k(x)$ is the kth Euler polnomial. In the usual manner, (3.1) gives

$$y^2 = \frac{D}{4}\left((E_k(x) + (-1)^{x+1}E_k(0))^2 + \frac{16C(-B)^n}{D}\right). \tag{3.7}$$

Using Lemma 3.4.4 with $a = (-1)^{x+1}E_k(0)$ and $b = \frac{16C(-B)^n}{D} \neq 0$, we obtain that the polynomial on the right-hand side of (3.7) is non-degenerate. Thus by Lemma 3.4.1 the theorem holds.

The case $k = 4$. Take first $p(x) = \binom{x}{4}$. Then (3.1) yields

$$y^2 = D\binom{x}{4}^2 + 4C(-B)^n,$$

where $y = V_n$. If the discriminant of the polynomial on the right-hand side is non-zero, then the polynomial is non-degenerate and the theorem is the consequence of Lemma 3.4.1. The discriminant of this polynomial is zero if and only if $4C(-B)^n = \frac{-9D}{16384}$, or $\frac{-D}{576}$, therefore we need to check only these two cases. In the first case we obtain the hyperelliptic equation

$$y^2 = D\binom{x}{4}^2 - \frac{9D}{16384} = \\ = \frac{D}{147456}(4x^2 - 12x - 1)(16x^4 - 96x^3 + 176x^2 - 96x + 9)(2x - 3)^2$$

and by Lemma 3.4.1 we are done. The second case gives the hyperelliptic equation

$$y^2 = D\binom{x}{4}^2 - \frac{D}{576} = \frac{D}{576}(x^4 - 6x^3 + 11x^2 - 6x - 1)(x^2 - 3x + 1)^2$$

and by Lemma 3.4.1 the theorem follows again.

When $p(x) \in \{\Pi_4(x), S_3(x), R_4(x)\}$ the theorem can be verified by a similar argument. We omit the details.

The case $k \leq 3$. First note that when $p(x) = R_3(x)$ by a similar argument as in case of $k = 4$ the theorem follows. Hence we may assume that either $k = 2$, or $k = 3$, $p(x) \in \{\binom{x}{3}, \Pi_3(x), S_2(x)\}$. Recall that in these cases we have $B = 1$. We only consider one example, all the other possibilities can be handled similarly. Let $p(x) = \binom{x}{2}$. Putting $y = V_n$ in (3.1) we get

$$y^2 = D\binom{x}{2}^2 + 4C(-1)^n. \tag{3.8}$$

The discriminant of the polynomial on the right-hand side is zero if and only if $4C(-1)^n = \frac{-D}{64}$. Thus this polynomial is non-degenerate, unless $256|D$ is valid. However, as now $D = A^2 + 4$, a simple calculation gives that it is impossible. Therefore the right-hand side of (3.8) is non-degenerate and by Lemma 3.4.1 the theorem follows. □

For the proof of Proposition 3.3.1 we need the following concept and lemma. Let $T_k(x)$ denote the Chebisev polynomial of degree k, i.e., $T_0(x) = 2$, $T_1(x) = x$, and $T_{n+1}(x) = xT_n(x) - T_{n-1}(x)$ for $n \geq 1$.

Lemma 3.4.5 (Nemes and Pethő [74])**.** *Let U_n be a non-degenerated binary recurrence sequence with $|B| = 1$, and $p(x)$ be a polynomial with integer coefficients of degree $k \geq 2$. Let be $q = -(-B)^m C/D$ and $E = 2(k-1)a_{k-1}^2 - 4ka_k a_{k-2}$. If (3.2) has infinitely many solutions n, x, then*

$$p(x) = \varepsilon\sqrt{q}T_k\left(\frac{2k|a_k|}{\eta\sqrt{E}}x + \frac{2a_{k-1}}{\eta\sqrt{E}}\right),$$

where ε and η are either 1 or -1. Furthermore, either x is an integer root of $p'(x)$ or $k|a_k|x + a_{k-1}$ is contained in the union of finitely many second order recurrence sequences with discriminants D_i, where D/D_i are squares of integers.

Proof. This is Theorem 3 in [74]. □

Proof of Proposition 3.3.1. We start the proof showing that our examples satisfy the conditions of Lemma 3.4.5. We consider only one example, the others can be handled similarly. Let $p(x) = \binom{x}{2}$. Then $p(x)$ can be written in the form

$$p(x) = \frac{1}{16}T_2(2\sqrt{2}x - \sqrt{2}) = \frac{1}{16}(8x^2 - 8x).$$

From this it follows that if equation (3.2) has infinitely many solutions then the parameters of the binary recurrence sequence U must satisfy $\frac{C}{D} = -\frac{1}{256}$. Choosing $U_0 = 1$, $U_1 = 253$, $A = 254$ with $B = -1$ we get that $\frac{C}{D} = \frac{-252}{64512} = -\frac{1}{256}$. Hence we can conclude that the binary recurrence sequence belonging to the parameters of the first row of Table 3.1 and the polynomial $p(x) = \binom{x}{2}$ satisfy the conditions of Lemma 3.4.5.

Now we prove that with these choices of the parameters, equation (3.2) actually has infinitely many solutions. Since the companion polynomial of U is $x^2 - 254x + 1$, we have

$$U_n = \tfrac{3\sqrt{7}+8}{16}(127 + 48\sqrt{7})^n - \tfrac{3\sqrt{7}-8}{16}(127 - 48\sqrt{7})^n \quad (n = 0, 1, \ldots).$$

Let $W = \{W_n\}_{n=0}^{\infty}$ be the ternary recurrence sequence defined by the initial values $W_0 = 2$, $W_1 = 23$, $W_2 = 359$ and by the recurrence relation $W_n = 17W_{n-1} - 17W_{n-2} + W_{n-3}$ $(n \geq 3)$. Then the companion polynomial of W is

$$x^3 - 17x^2 + 17x - 1 = (x^2 - 16x + 1)(x - 1).$$

Hence we have

$$W_n = \frac{3+\sqrt{7}}{4}(8+3\sqrt{7})^n + \frac{3-\sqrt{7}}{4}(8-3\sqrt{7})^n + \frac{1}{2}1^n.$$

Since U_n can be written as $U_n = \frac{1}{16}\left((8+3\sqrt{7})^{2n+1} + (8-3\sqrt{7})^{2n+1}\right)$, it can be easily verified that for all $n = 0, 1, \ldots$ we have $U_n = \binom{W_n}{2}$. Thus with the choice $x = W_n$ equation (3.2) has infinitely many solutions in n, x. □

Proof of Theorem 3.3.2. As we explained before formulating the theorem, to prove the statement it is sufficient to consider equation (3.3) with our special settings, i.e.

$$Y^2 = D\left(a^2X^4 + 2acX^3 + (c^2+2ad)X^2 + 2cdX + d^2\right) + 4C(-B)^n e^2.$$

The discriminant of the polynomial on the right-hand side is

$$\Delta = 256D^3a^4C^2e^4(16a^2Dd^2 + 64a^2C(-B)^n e^2 - 8aDc^2d + c^4D).$$

Since by our conditions $Dae \neq 0$, and U is non-degenerate therefore $C \neq 0$, thus if

$$8aDd(2ad - c^2) \neq -64a^2C(-B)^n e^2 - c^4D,$$

then $\Delta \neq 0$. Hence, by Lemma 3.4.1 the solutions n, x of (3.2) can be effectively determined.

The solutions can be determined explicitly in the following way. In what follows, we use certain procedures of the program package Magma and also Magma programs of Bruin and Stoll [26] and Tengely [112]. We emphasize that all the procedures we use or mention are known from the literature. The novelty at this point is only that we put them together in order to get a complete algorithm.

First, by the command `HyperellipticCurve` we define the hyperelliptic curve

$$Y^2 = h(X), \tag{3.9}$$

where $h(X) := h_4X^4 + h_3X^3 + h_2X^2 + h_1X + h_0$ is the right-hand side of (3.3). If h_4 is a perfect square then one can use Runge's method to solve (3.9). In fact, by the help of a Magma program of Tengely, all solutions can be determined in this case (see [112]). Otherwise, we try to determine some rational points on the curve (3.9) with the help of the procedure `Points`. If we cannot get any rational points, then most probably (3.9) has no rational solutions at all. This

can be very efficiently checked by the procedure `TwoCoverDescent` of Bruin and Stoll. (For the description of this procedure and some examples see [26].)

Assume now that with the procedure `Points` we obtained some rational points on (3.9). Suppose that there is a point (X_0, Y_0) among them such that $Y_0 = 0$. Let $(X_0, 0) = \left(\frac{x_1}{x_2}, 0\right)$ be such a point of the curve. Then using the substitutions $U = x_2X - x_1$ and $V = x_2^2Y$, noting that $h(X_0) = 0$, we obtain an equation of the shape

$$V^2 = t_4U^4 + t_3U^3 + t_2U^2 + t_1U$$

with some $t_i \in \mathbb{Z}$ $(i = 1, \ldots, 4)$. Factorizing the right-hand side we get that

$$sV_1^2 = U \tag{3.10}$$

and

$$sV_2^2 = t_4U^3 + t_3U^2 + t_2U + t_1 \tag{3.11}$$

with some integers s, V_1, V_2. Equation (3.10) implies that $s \mid U$, hence (3.11) yields that $s \mid t_1$. Thus to solve our original problem it is sufficient to find the integral points on finitely many elliptic curves given by (3.11). This can be done with the procedure `IntegralPoints`. Following the substitutions backwards we obtain all integer solutions of (3.9).

Finally, consider the case when the procedure `Points` finds only rational points on (3.9) with nonzero second coordinates. In this case by the help of certain birational transformations (3.9) can be transformed into an elliptic curve. For the theory of birational transformations see e.g. Harada and Lang [55], Connell [33], Tzanakis [117], Hermann [56] and the references given there. To resolve (3.9) completely, one can use the procedure `IntegralQuarticPoints` of Magma (which is actually based upon [117]). One needs to call the procedure `IntegralQuarticPoints` by (3.9) and one of the above mentioned points. In this way we can get all integral solutions of (3.9) also in this case.

We implemented our algorithm for the resolution of (3.9) in Magma.

From the solutions of equation (3.3) all solutions n, x of the original equation (3.2) can be easily determined. □

Proof of Theorem 3.3.3. We split the proof into three parts. We start with equations which turn to be unsolvable locally. Then we deal with equations which can be reduced to elliptic equations. Finally, we prove the theorem for those equations which can be reduced to genus 1 equations. In all cases we give the proof only for one equation as the other ones can be handled similarly.

Throughout the proof we shall use the well-known facts that L is the associate sequence of F and Q is the associate sequence of P.

Locally unsolvable equations. In this part of the proof we deal with those equations which turn out to be locally unsolvable for some prime. The following equations belong to this group: $Q_n = \Pi_2(x), \Pi_4(x)$.

As an example, take the equation $Q_n = \Pi_2(x)$. Writing $y = P_n$ in (3.1), we get the equations

$$y^2 = 8(x(x+1))^2 \mp 8.$$

A simple calculation modulo 16 leads to a contradiction. Hence equation $Q_n = \Pi_2(x)$ does not have any integer solutions. We note that our algorithm described in the proof of Theorem 3.3.2 provides the same conclusion.

Elliptic equations. In this part we handle those equations which can be reduced to elliptic equations. The following equations belong to this set: $Q_n = S_2(x)$, $\binom{x}{3}$ and $U_n = \Pi_3(x)$, with $U_n \in \{F_n, L_n, P_n, Q_n\}$.

As an example, consider the equation $P_n = \Pi_3(x)$. With the substitution $y = Q_n$, (3.1) yields

$$y^2 = 8(x(x+1)(x+2))^2 \pm 4.$$

With the substitution $x_1 = 2(x+1)^2$ the right-hand side can be transformed to a polynomial of degree 3, therefore we obtain the elliptic equations

$$y^2 = x_1^3 - 4x_1^2 + 4x_1 \pm 4.$$

With the procedure `IntegralPoints` of Magma one can compute the integer points of these curves, and then determine the solutions n, x of (3.2). The solutions are exactly the ones listed in Table 3.2.

Genus 1 equations. In this part we consider those equations which can be reduced to genus 1 equations. All the equations considered which are not mentioned so far belong to this group.

Consider the equation $F_n = \Pi_4(x)$. With $y = L_n$ and $x_1 = x^2 + 3x$ by (3.1) we get the equation

$$y^2 = 5x_1^4 + 20x_1^3 + 20x_1^2 + 4(-1)^n.$$

If n is even then directly, if n is odd then after the substitution $x_2 = x_1 + 1$ we can apply the procedure `IntegralQuarticPoints` of Magma to compute the integer solutions of this equation. Then we easily get the solutions n, x of the original equation (3.2). The solutions are exactly the ones listed in Table 3.2. □

Chapter 4

Results on (a, b)-balancing numbers

4.1 Introduction and main results

A positive integer n is called a balancing number if

$$1 + \cdots + (n-1) = (n+1) + \cdots + (n+r)$$

holds for some positive integer r (see [7] and [39]). The sequence of balancing numbers is denoted by B_m $(m = 1, 2, \dots)$. As one can easily check, we have $B_1 = 6$ and $B_2 = 35$. Note that by a result of Behera and Panda [7], we have

$$B_{m+1} = 6B_m - B_{m-1} \qquad (m > 1).$$

In particular, there are infinitely many balancing numbers.

The literature of balancing numbers is very rich. In [62] and [63] Liptai proved that there are no Fibonacci and Lucas balancing numbers, respectively. Later, Szalay [111] derived the same results by a different method.

In [64] Liptai, Luca, Pintér and Szalay generalized the concept of balancing numbers in the following way. Let y, k, l be fixed positive integers with $y \geq 4$. A positive integer x with $x \leq y - 2$ is called a (k, l)-power numerical center for y if

$$1^k + \cdots + (x-1)^k = (x+1)^l + \cdots + (y-1)^l.$$

In [64] several effective and ineffective finiteness results were proved for (k, l)-power numerical centers.

Recently, the "balancing" property has been investigated in recurrence sequences (see [14]). In this chapter we extend the concept of balancing numbers to arithmetic progressions. Let $a > 0$ and $b \geq 0$ be coprime integers. If for some positive integers n and r we have

$$(a + b) + \cdots + (a(n - 1) + b) = (a(n + 1) + b) + \cdots + (a(n + r) + b)$$

then we say that $an + b$ is an (a, b)-balancing number. The sequence of (a, b)-balancing numbers is denoted by $B_m^{(a,b)}$ $(m = 1, 2, \dots)$. We mention that since $B_m^{(1,0)} = B_m$ for all m, we obtain a generalization of balancing numbers.

We prove several effective finiteness and explicit results concerning polynomial values in the sequences $B_m^{(a,b)}$. That is, we consider the equation

$$B_m^{(a,b)} = f(x) \tag{4.1}$$

in integers m and x with $m \geq 1$, where f is some polynomial with rational coefficients, taking only integral values at integers. To prove our theorems, beside the above mentioned results of Ping-Zhi [81], Pintér and Rakaczki [85] and Rakaczki [90], we further need the modular method developed by Wiles [124] and others and a deep result of Bennett [8] concerning binomial Thue equations. The results of Chapter 4 are published in [60].

From this point on, when we refer to equation (4.1) we always assume that a and b are arbitrary, but fixed coprime integers such that $a > 0$ and $b \geq 0$. Our first result is the following.

Theorem 4.1.1. *Let $f(x)$ be a monic polynomial with integer coefficients, of degree ≥ 2. If a is odd, then for the solutions of (4.1) we have $\max(m, |x|) < c_0(f, a, b)$, where $c_0(f, a, b)$ is an effectively computable constant depending only on a, b and f.*

Our next result concerns the case where $f(x) = x^l$ with some $l \geq 2$. In this case solving equation (4.1) is equivalent to finding (a, b)-balancing numbers which are perfect powers.

Theorem 4.1.2. *If $a^2 - 4ab - 4b^2 = 1$, then there is no perfect power (a, b)-balancing number.*

Remark. One can easily check that the equation $a^2 - 4ab - 4b^2 = 1$ has infinitely many solutions in integers a, b with $a > 0$, $b \geq 0$. Hence Theorem 4.1.2 completely solves the proposed problem for infinitely many pairs (a, b).

The following theorem takes up the problem where the polynomial $f(x)$ in (4.1) has some combinatorial meaning. More precisely, we investigate binomial coefficients $\binom{x}{k}$, products of consecutive integers $\Pi_k(x)$, power sums $S_k(x)$ and alternating power sums $R_k(x)$. Note that the coefficients of $\binom{x}{k}$, $S_k(x)$ and $R_k(x)$ are not integers. Further, in the case $f(x) = \Pi_k(x)$ Theorem 4.1.1 yields a finiteness result, however, only for the odd values of the parameter a.

For these combinatorial choices of $f(x)$ our next statement yields a bound for the solutions of (4.1), without any assumptions for the parameters a and b.

Theorem 4.1.3. *Let $k \geq 2$ and $f(x)$ be one of the polynomials $\binom{x}{k}$, $\Pi_k(x)$, $S_{k-1}(x)$, $R_k(x)$. Then the solutions of equation (4.1) satisfy $\max(m, |x|) < c_1(a, b, k)$, where $c_1(a, b, k)$ is an effectively computable constant depending only on a, b and k.*

In our final result, under the assumption $a^2 - 4ab - 4b^2 = 1$, we provide the complete solution of (4.1) with the above choices of $f(x)$, for some small values of the parameter k. More precisely, we consider all cases where (4.1) can be reduced to an equation of genus 1. Further, we also solve a particular case of (4.1) which can be reduced to the resolution of a genus 2 equation.

Theorem 4.1.4. *Suppose that $a^2-4ab-4b^2 = 1$. Let $f(x) \in \{\binom{x}{2}, \binom{x}{3}, \binom{x}{4}, \Pi_2(x), \Pi_3(x), \Pi_4(x), S_1(x), S_2(x), S_3(x), S_5(x)\}$. Then the solutions (m, x) of equation (4.1) are those contained in Table 4.1. For the corresponding parameter values we have $(a, b) = (1, 0)$ in all cases.*

$f(x)$	Solutions (m, x) of (4.1)
$\binom{x}{2}$	$(1, -3), (1, 4)$
$\binom{x}{3}$	$(2, -5), (2, 7)$
$\binom{x}{4}$	$(2, -4), (2, 7)$
$\Pi_2(x)$	$(1, -3), (1, 2)$
$\Pi_3(x)$	$(1, -3), (1, 1)$
$\Pi_4(x)$	$--$
$S_1(x)$	$(1, -4), (1, 3)$
$S_2(x)$	$(3, -8), (3, 9), (5, -27), (5, 28)$
$S_3(x)$	$--$
$S_5(x)$	$--$

Table 4.1: Solutions of equation (4.1) with the particular polynomials

Remark. We considered some other related equations that lead to genus 2 equations. However, because of certain technical difficulties, we could not solve them by the Chabauty method. We checked that under the assumption $a^2 - 4ab - 4b^2 = 1$ equation (4.1) has no "small" solutions (i.e. solutions with $|x| \leq 10000$) in cases $f(x) \in \{\binom{x}{6}, \binom{x}{8}, \Pi_6(x), \Pi_8(x), S_7(x)\}$.

4.2 Proof of the theorems

For the proof of our theorems we need several lemmas. The first one is of principal importance, because it opens access to the application of deep methods.

Lemma 4.2.1. *For any $a > 0$, $b \geq 0$ and $m \geq 1$*

$$y^2 - 8\left(B_m^{(a,b)}\right)^2 = a^2 - 4ab - 4b^2 \tag{4.2}$$

holds with some $y \in \mathbb{Z}$.

Proof. Using the definition of $B_m^{(a,b)}$ and writing $B_m^{(a,b)} = an + b$, a simple calculation shows that

$$ar^2 + (a + 2B_m^{(a,b)})r - (n-1)(B_m^{(a,b)} + b) = 0.$$

The left hand side of this equality is a polynomial in r of degree two. Thus its discriminant must be a square in $\mathbb{Z}$. Since the discriminant in question is given by

$$8\left(B_m^{(a,b)}\right)^2 + a^2 - 4ab - 4b^2,$$

the statement follows. □

For the proof of Theorem 4.1.1 we need two lemmas. The first one is Lemma 3.4.1 from the previous chapter. For the second one, we need the following concept. If p is a prime and t is an integer, then by $p^\alpha || t$ we mean that $p^\alpha | t$ but $p^{\alpha+1} \nmid t$. The following result of Brindza and Pintér [20] provides information on the structure of zeros of certain polynomials.

Lemma 4.2.2. *Let $P(X) = a_n X^n + \cdots + a_1 X + a_0$ be a polynomial with integral coefficients, for which a_0 is odd, $4|a_i$ $(i = 1, \ldots, n)$ and $2^3 || a_n$. Then every zero of P is simple.*

Proof of Theorem 4.1.1. Using Lemma 4.2.1, from (4.1) we get the equation

$$8f^2(x) + a^2 - 4ab - 4b^2 = y^2.$$

It is easy to see that since a is odd, the left hand side of the above equation is a polynomial satisfying the conditions of Lemma 4.2.2. So, by Lemma 4.2.2 we know that the zeros of the left hand side are simple. Hence, by Lemma 3.4.1 the theorem follows. □

To prove Theorem 4.1.2, we need the following deep result of Bennett [8] about binomial Thue equations. Note that recently this result has been considerably generalized in certain sense (see e.g. the papers [9], [11] and the references given there). However, the following lemma is sufficient for our present purposes.

Lemma 4.2.3. *If A, B and n are integers with $AB \neq 0$ and $n \geq 3$, then the equation*

$$|Ax^n - By^n| = 1$$

has at most one solution in positive integers x, y.

Proof of Theorem 4.1.2. Using Lemma 4.2.1 and substituting $B_m^{(a,b)} = x^l$ into (4.2), by $a^2 - 4ab - 4b^2 = 1$ we obtain

$$y^2 - 8x^{2l} = 1, \tag{4.3}$$

with some $y \in \mathbb{Z}$. Rewrite (4.3) as

$$y^2 - 1 = 8x^t,$$

where $t = 2l$ with $t \geq 4$, as $l \geq 2$.

Obviously, y must be odd. Introducing the notation $y = 2k + 1$, we get

$$k(k+1) = 2x^t.$$

Thus we have $k = 2^\alpha x_1^t$ and $k + 1 = 2^\beta x_2^t$ with $\alpha\beta = 0$, $\alpha + \beta = 1$, where x_1, x_2 are some positive integers. This yields

$$|2^\beta x_2^t - 2^\alpha x_1^t| = 1. \tag{4.4}$$

Observe that $x_1 = x_2 = 1$ is a solution to (4.4). Hence by Lemma 4.2.3 there are no other solutions. Thus the only possible value for x is $x = 1$, which yields $B_m^{(a,b)} = 1$. Since this is impossible, the theorem follows. □

For the proof of Theorem 4.1.3, we need three more lemmas from the previous chapter, namely results of Ping-Zhi [81], Pintér and Rakaczki [85] and Rakaczki [90], respectively.

Proof of Theorem 4.1.3. Assume first that $k \geq 5$. Using Lemma 4.2.1 and (4.1), we get the equation

$$y^2 = 8\left(f(x)\right)^2 - C(a,b), \tag{4.5}$$

where $C(a,b) = -(a^2 - 4ab - 4b^2)$. Observe that $C(a,b) \neq 0$. We consider the possible choices for $f(x)$ in turn.

Let $f(x) = \binom{x}{k}$. Factorizing the right hand side of (4.5), we obtain

$$y^2 = 8\left(f(x) + \sqrt{\frac{C(a,b)}{8}}\right)\left(f(x) - \sqrt{\frac{C(a,b)}{8}}\right). \tag{4.6}$$

Since $C(a,b) \neq 0$, the zeros of the factors on the right hand side of equation (4.6) are distinct. Moreover, as one can readily check, $\pm\sqrt{\frac{C(a,b)}{8}} \neq \frac{10\pm7\sqrt{7}}{1215}$, since $C(a,b) \in \mathbb{Z}$. Thus, by Lemmas 3.4.1 and 3.4.2 the theorem follows in this case.

Now assume that $f(x) = \Pi_k(x)$. In this case Lemma 4.2.1 and (4.1) give

$$y^2 = 8\left(\Pi_k(x)\right)^2 - C(a,b).$$

Since $\Pi_k(x) = k!\binom{x+k-1}{k}$, we get

$$y^2 = 8(k!)^2\left(\binom{x+k-1}{k} + \sqrt{\frac{C(a,b)}{8(k!)^2}}\right)\left(\binom{x+k-1}{k} - \sqrt{\frac{C(a,b)}{8(k!)^2}}\right).$$

Since $C(a,b) \neq 0$, the zeros of the factors on the right hand side are distinct again. Moreover, it is easy to see that $\pm\sqrt{\frac{C(a,b)}{8k!^2}} \neq \frac{10\pm7\sqrt{7}}{1215}$. Hence using Lemmas 3.4.1 and 3.4.2 the theorem follows also in this case.

Next let $f(x) = S_k(x)$. We use again the well-known fact that

$$S_{k-1}(x) = \frac{1}{k}\left(B_k(x) - B_k(0)\right).$$

Then by Lemma 4.2.1 and (4.1) again, we obtain that

$$y^2 = \frac{8}{k^2}\left(\left(B_k(x) - B_k(0)\right)^2 - \frac{k^2C(a,b)}{8}\right).$$

Applying Lemma 3.4.3 with $A = -B_k(0)$ and $B = -\frac{k^2 C(a,b)}{8} \neq 0$, we see that the right hand side of this equation is non-degenerate. Thus, the theorem follows from Lemma 3.4.1.

Finally, let $f(x) = R_k(x)$. It is also well-known that for all $k \in \mathbb{N}$

$$R_k(x) = \frac{1}{2}\left(E_k(x) + (-1)^{x+1}E_k(0)\right)$$

is valid. Lemma 4.2.1 and (4.1) now yield

$$y^2 = 2\left((E_k(x) + (-1)^{x+1}E_k(0))^2 - \frac{C(a,b)}{2}\right).$$

Applying Lemma 3.4.4 with $A = (-1)^{x+1}E_k(0)$ and $B = -\frac{C(a,b)}{2} \neq 0$, we get that the right hand side of the above equation is non-degenerate. Again, the theorem follows from Lemma 3.4.1.

Consider now the cases when $2 \leq k \leq 4$. In all cases we get that the polynomial on the right hand side of (4.5) is non-degenerate because its discriminant is non-zero. We consider only one example, all the other cases can be handled similarly.

Let $f(x) = \binom{x}{2}$. In this case the discriminant of the polynomial on the right hand side of (4.5) is $D := -256C(a,b)^2(8C(a,b)-1)$. Since $C(a,b)$ is a non-zero integer, we get $D \neq 0$, indeed. Therefore, the polynomial on the right side of (4.5) is non-degenerate, and by Lemma 3.4.1 the theorem follows. □

As it was mentioned already, in our numerical results we consider all cases with the above choices of $f(x)$ and with $a^2 - 4ab - 4b^2 = 1$, where (4.1) can be reduced to an equation of genus 1. Further, we also solve a particular case of (4.1) which can be reduced to a genus 2 equation. To solve this equation, we shall use the Chabauty method by the help of explicit techniques developed by Bruin. We note that the Chabauty method has already been successfully used to solve certain other combinatorial Diophantine equations, see e.g. the corresponding results in the papers [25], [48], [53], [54], [98], [113] and the references given there.

Proof of Theorem 4.1.4. Using Lemma 4.2.1 and the assumption $a^2-4ab-4b^2 = 1$, equation (4.1) can be written as

$$y^2 = 8f(x)^2 + 1. \tag{4.7}$$

Actually, we solve equation (4.7) for all the cases of $f(x)$ listed in Theorem 4.1.4. We prove that the solutions are those contained in Table 4.2. Having the

solutions of (4.7), the solutions of the original equation (4.1) can be determined with simple calculations.

$f(x)$	Solutions (x, y) of (4.7)
$\binom{x}{2}$	$(-3, \pm 17), (-1, \pm 3), (0, \pm 1), (1, \pm 1), (2, \pm 3), (4, \pm 17)$
$\binom{x}{3}$	$(0, \pm 1), (1, \pm 1), (2, \pm 1), (-1, \pm 3), (3, \pm 3), (-5, \pm 99), (7, \pm 99)$
$\binom{x}{4}$	$(-4, \pm 99), (-1, \pm 3), (0, \pm 1), (1, \pm 1),$ $(2, \pm 1), (3, \pm 1), (4, \pm 3), (7, \pm 99)$
$\Pi_2(x)$	$(-3, \pm 17), (-1, \pm 1), (0, \pm 1), (2, \pm 17)$
$\Pi_3(x)$	$(-3, \pm 17), (-1, \pm 1), (0, \pm 1), (1, \pm 17)$
$\Pi_4(x)$	$(-3, \pm 1), (-2, \pm 1), (-1, \pm 1), (0, \pm 1)$
$S_1(x)$	$(-4, \pm 17), (-2, \pm 3), (-1, \pm 1), (0, \pm 1), (1, \pm 3), (3, \pm 17)$
$S_2(x)$	$(-27, \pm 19601), (-8, \pm 577), (-1, \pm 3), (0, \pm 1),$ $(1, \pm 1), (2, \pm 3), (9, \pm 577), (28, \pm 19601)$
$S_3(x)$	$(-1, \pm 3), (0, \pm 1), (1, \pm 1), (2, \pm 3)$
$S_5(x)$	$(-1, \pm 3), (0, \pm 1), (1, \pm 1), (2, \pm 3)$

Table 4.2: Solutions of equation (4.7) with the particular polynomials

As it will be clear from the presentation, it is worth to split the resolution of (4.10) into three parts. Assume first that $f(x) \in \{\binom{x}{3}, \Pi_3(x), S_2(x)\}$. Then the right hand side of equation (4.7) can be transformed into a polynomial of degree 3. As the computations are similar in all cases, we consider only one example. Let $f(x) = S_2(x)$. Then (4.7) is given by

$$y^2 = 8(S_2(x))^2 + 1.$$

Using the well-known fact $S_2(x) = x(x-1)(2x-1)/6$, we get

$$y^2 = \frac{32x^6 - 96x^5 + 104x^4 - 48x^3 + 8x^2 + 36}{36}.$$

This leads to the elliptic equation

$$Y^2 = X^3 + 2X^2 + 576,$$

where $X = 8(x^2 - x)$, $Y = 24y$. One can compute the integer solutions of this equation with the procedure `IntegralPoints` of Magma [17]. Following the substitutions backwards, we can determine the solutions x, y of the equation

(4.7). The solutions are exactly the ones listed in Table 4.2. In all the other cases we get the solutions of (4.7) by a similar calculation.

Assume next that $f(x) \in \{\binom{x}{2}, \binom{x}{4}, \Pi_2(x), \Pi_4(x), S_1(x), S_3(x)\}$. Then the right hand side of equation (4.7) can be transformed into a polynomial of degree 4. Since the different choices of f can be handled similarly, we consider only one example, again. Let $f(x) = \Pi_4(x)$. Then (4.7) has the form

$$y^2 = 8(\Pi_4(x))^2 + 1.$$

Using $\Pi_4(x) = x(x+1)(x+2)(x+3)$, introducing the notation $X = x^2 + 3x$, this yields

$$y^2 = 8X^4 + 32X^3 + 32X^2 + 1.$$

This equation is of genus 1 and can be solved using the Magma procedure `IntegralQuarticPoints`. Hence, we can find all integral solutions of equation (4.7), again. The solutions (x, y) are exactly the ones listed in Table 4.2. All the other cases are similar.

Finally, assume that $f(x) = S_5(x)$. In this case, equation (4.7) has the form

$$y^2 = 8(S_5(x))^2 + 1.$$

Hence, using the well-known assertion $S_5(x) = \frac{1}{12}(x-1)^2x^2(2x^2 - 2x - 1)$, we get

$$Y^2 = 8X^6 - 8X^5 + 2X^4 + 36, \tag{4.8}$$

where $X = x^2 - x$ and $Y = 6y$. Equation (4.8) defines a curve of genus 2 over $\mathbb{Q}$. All its solutions can be determined by applying recent explicit Chabauty techniques due to Bruin. Here we only indicate the main steps of the method without explaining the background theory. For details we refer to the papers of Bruin [22], [23], [24], and the references given there.

Since the Jacobian of the hyperelliptic curve determined by (4.8) has Mordell-Weil rank 3, the classical Chabauty-type method (see e.g. [40]) does not suffice to find the rational points on (4.8). To deal with this situation, we apply the elliptic Chabauty method, combined with Magma, following [24]. In the first step, we factorize the right-hand side of equation (4.8) over the number field $K = \mathbb{Q}(\alpha)$ where $\alpha = \sqrt{-2}$. For later use, we mention that $\{1, \alpha\}$ is an integral basis of K, and that the ring of integers O_K of K is a Euclidean ring. We obtain

$$Y^2 = (2\alpha X^3 - \alpha X^2 + 6)(-2\alpha X^3 + \alpha X^2 + 6). \tag{4.9}$$

This yields that

$$\delta Z^2 = 2\alpha X^3 - \alpha X^2 + 6 \tag{4.10}$$

is valid with some $\delta, Z \in O_K$, where δ is square-free in O_K. Observe that (4.9) and (4.10) imply that

$$\delta W^2 = -2\alpha X^3 + \alpha X^2 + 6$$

is also valid with some $W \in O_K$. Hence δ divides $(2\alpha X^3 - \alpha X^2 + 6) + (-2\alpha X^3 + \alpha X^2 + 6)$ in O_K, that is $\delta | 12$. Thus, using that the only units in O_K are ± 1, $\alpha^2 = -2$, and 3 is a prime in O_K, we get that $\delta = \pm \alpha^{t_1} 3^{t_2}$ with $t_1, t_2 \in \{0, 1\}$. Taking norms on both sides of (4.10), we obtain that $\delta \in \{-3, -1, 1, 3\}$. In the cases $\delta = \pm 1$, simple computations show that equation (4.10) has no solutions. We illustrate this only for $\delta = 1$. Write $Z = Z_1 + \alpha Z_2$ in (4.10) with $Z_1, Z_2 \in \mathbb{Z}$. Then comparing the coefficients of 1 and α on both sides of (4.10), we get $Z_1^2 - 2Z_2^2 = 6$. However, this is impossible modulo 16. The case of $\delta = -1$ can be excluded in a similar way.

Let now $\delta = 3$. Equation (4.10) defines a genus 1 curve over K that can be transformed into a Weierstrass-form elliptic curve E over K by the help of its point $P = (2, \alpha + 2)$. A minimal model of E is given by

$$ME: \quad v^2 = u^3 + 6u + (4\alpha - 1296).$$

Note that all these curves, together with the transformations among them can be handled by Magma. Now, as X, Y are known to be rational coordinates of the hyperelliptic curve defined by (4.8), one can apply the elliptic Chabauty method to solve (4.8) completely (following Bruin [24]). To have the method work, the rank of $ME(K)$ should be strictly less than the degree of K (which is 2). It turns out that the rank of $ME(K)$ is 1, so the elliptic Chabauty method is applicable. The procedure `PseudoMordellWeilGroup` of Magma is able to find a subgroup G of $ME(K)$ of finite odd index. Then using the procedure `Chabauty` with the prime 59, we get that $(X, Y) = (2, \pm 18)$ are the only solutions for equation (4.8) in this case. Substituting back, we obtain that the corresponding solutions to equation (4.7) are $(x, y) = (0, \pm 1), (1, \pm 1)$.

In case of $\delta = -3$ we can follow a similar argument. The rank of the corresponding elliptic curve is 1 again, so we can proceed as previously. The solutions for equation (4.8) can be found by using the prime 7 with `Aux:=19` in the procedure `Chabauty` of Magma. We obtain that all solutions of equation (4.8) are given by $(X, Y) = (0, \pm 6)$ in this case. Following the substitutions backwards, we get that the corresponding solutions to equation (4.7) are $(x, y) = (-1, \pm 3), (2, \pm 3)$.

From the solutions of equation (4.7), using (4.1) and $B_m^{(a,b)} = an + b$ with some integer $n > 0$, the parameters a, b, m can be found by simple calculations.

Thus we obtain all solutions (m, x) of (4.1). They are exactly the ones listed in Table 4.1, all corresponding to the parameters $(a, b) = (1, 0)$. □

Chapter 5

Almost fifth powers in arithmetic progression

5.1 Introduction

A classical theorem of Erdős and Selfridge [38] states that the product of consecutive positive integers is never a perfect power. A natural generalization is the Diophantine equation

$$x(x+d)\dots(x+(k-1)d) = by^n \tag{5.1}$$

in non-zero integers x, d, k, b, y, n with $\gcd(x,d) = 1$, $d \geq 1$, $k \geq 3$, $n \geq 2$ and $P(b) \leq k$. Here $P(u)$ stands for the largest prime divisor of a non-zero integer u, with the convention $P(\pm 1) = 1$.

This equation has a long history with an extremely rich literature. The complete solution of (5.1) in case of $d = 1$ is due to Saradha [94] (case $k \geq 4$) and Győry [44] (case $k < 4$).

For an overview of the huge number of related results for $d > 1$ we refer to survey papers of Győry [45], Shorey [96], [97] and Tijdeman [116]. Now we concentrate only on results where all solutions of (5.1) have been determined when the number k of terms is fixed.

In case of $(k,n) = (3,2)$ equation (5.1) has infinitely many solutions, already for $b = 1$ (c.f. [116]). Euler (see [37]) proved that (5.1) has no solutions with $b = 1$, and $(k,n) = (3,3)$ or $(4,2)$. Obláth [75], [76] obtained similar results for $(k,n) = (3,4)$, $(3,5)$ and $(5,2)$.

By a conjecture of Erdős, equation (5.1) has no solutions in positive integers when $k > 3$ and $b = 1$. In other words, the product of k consecutive terms of a primitive positive arithmetic progression with $k > 3$ is never a perfect power. By primitive arithmetic progression we mean one of the form

$$x, x + d, \ldots, x + (k - 1)d,$$

with $\gcd(x, d) = 1$. The conjecture of Erdős has recently been verified for certain values of k in a more general form; see the papers [45], [46], [10], [47]. Since now we focus on the case $n = 5$, we give only the best known result for this particular exponent. (Though the results mentioned are valid for any $n \geq 2$.) The following statement is a combination of results from [45] (case $k = 3$), [46] (cases $k = 4, 5$), [10] (cases $k = 6, 7$) and [47] (cases $8 \leq k \leq 34$).

Theorem A. *The only solutions to equation* (5.1) *with* $n = 5$, $3 \leq k \leq 34$ *and* $P(b) \leq P_k$, *with*

$$P_k = \begin{cases} 2, & \text{if } k = 3, 4, \\ 3, & \text{if } k = 5, \\ 5, & \text{if } k = 6, 7, \\ 7, & \text{if } 8 \leq k \leq 22, \\ \frac{k-1}{2}, & \text{if } 23 \leq k \leq 34 \end{cases}$$

are given by

$$(k, d) = (8, 1),\ x \in \{-10, -9, -8, 1, 2, 3\}; \quad (k, d) = (8, 2),\ x \in \{-9, -7, -5\};$$

$$(k, d) = (9, 1),\ x \in \{-10, -9, 1, 2\}; \quad (k, d) = (9, 2),\ x \in \{-9, -7\};$$

$$(k, d) = (10, 1),\ x \in \{-10, 1\}; \quad (k, d, x) = (10, 2, -9).$$

Note that knowing the values of k, d and x, all solutions (x, d, k, b, y, n) of (5.1) can be easily listed.

To explain why the case $n = 5$ in equation (5.1) is special, we need to give some insight into the method of solving (5.1) for fixed k, in the general case $n \geq 2$. One of the most important tools is the modular method, developed by Wiles [124]. In [45], [46], [10], [47] all three types of ternary equations (i.e. of signatures $(n, n, 2), (n, n, 3), (n, n, n)$) and related results of Wiles [124], Darmon and Merel [35], Ribet [91], Bennett and Skinner [12], Bennett, Vatsal and Yazdani [13] and others are used. However, the modular technique works effectively only

for "large" exponents, typically for $n \geq 7$. Thus the "small" exponents $n = 2, 3, 5$ must be handled separately. In fact these cases are considered in distinct sections, or are covered by separate theorems in the above mentioned papers.

Further, the exponents $n = 2, 3$ has already been considered in separate papers. Equation (5.1) with $n = 2$ has a broad literature in itself; see e.g. [57] and the references given there. Here we focus only on the resolution of (5.1) with fixed k. For $n = 2$ and positive x, equation (5.1) has been completely solved up to a few exceptional cases by Hirata-Kohno, Laishram, Shorey and Tijdeman [57] for $k \leq 100$, and in case of $b = 1$, even for $k \leq 109$. Their main tools were elliptic curves and quadratic residues. Later, the exceptional remaining cases have been handled by Tengely [113], by the help of the Chabauty method. At this point we note that we shall refer to the Chabauty method frequently later on. For the description of the method, and in particular how to use it in the frame of the program package Magma [17], we refer to the papers of Bruin [23], [24] and the references given there.

When $n = 3$, working mainly with cubic residues, however making use of elliptic curves and the Chabauty method as well, Hajdu, Tengely and Tijdeman [54] obtained all solutions to equation (5.1) with $k < 32$ such that $P(b) \leq k$ if $4 \leq k \leq 12$ and $P(b) < k$ if $k = 3$ or $k \geq 13$. Further, if $b = 1$ then they could solve (5.1) for $k < 39$.

The case $n = 5$ has not yet been closely investigated. In this case (in the above mentioned papers considering equation (5.1) for general exponent n) mainly classical methods were used, due to Dirichlet and Lebesgue (see e.g. [47]). Apparently, for $n = 5$ elliptic curves are not applicable. In this thesis we show that in this case the Chabauty method (both the classical and the elliptic version) can be applied very efficiently. As we mentioned, the Chabauty method has been already used for the cases $n = 2, 3$ in [10], [113], [54]. However, it has been applied only for some particular cases and equations. In our results we solve a large number of genus 2 equations by Chabauty method, and then build a kind of sieve system based upon them. The results of Chapter 5 are published in [51].

5.2 New results

Our first theorem considerably extends Theorem A, in the most interesting case of $b = 1$ in equation (5.1). We call an arithmetic progression of the form $x, x + d, \ldots, x + (k - 1)d$ *primitive*, if $\gcd(x, d) = 1$.

Theorem 5.2.1. *The product of k consecutive non-zero terms in a primitive arithmetic progression with $3 \le k \le 54$ is never a fifth power.*

In fact Theorem 5.2.1 follows directly from the next result. To formulate it, we need to introduce a new concept. An arithmetic progression $x, x + d, \ldots, x + (k-1)d$ is called *trivial* if $d \le 5$ and $|x + id| \le 15$ for some $i = 0, 1, \ldots, k-1$. Further, a solution to equation (5.1) is also called *trivial*, if the terms $x, x + d, \ldots, x + (k-1)d$ on the left-hand side of (5.1) form a trivial arithmetic progression. This concept is needed because of the huge number of trivial solutions; on the other hand, such solutions of (5.1) can be listed easily for any fixed k.

Theorem 5.2.2. *Equation* (5.1) *with $n = 5$, $3 \le k \le 24$ and $P(b) \le P_k$ has the only nontrivial solutions with*

$$(k,d) = (3,7),\ x \in \{-16,-8,-6,2\};$$

$$(k,d) = (4,7),\ x \in \{-16,-15,-12,-9,-6,-5\};$$

$$(k,d) = (4,11),\ x \in \{-27,-6\};\quad (k,d) = (5,7),\ x \in \{-16,-12\};$$

$$(k,d) = (5,11),\ x \in \{-36,-32,-12,-8\};$$

$$(k,d) = (5,13),\ x \in \{-40,-27,-25,-12\};$$

$$(k,d) = (6,7),\ x \in \{-32,-25,-10,-3\};$$

$$(k,d) = (6,9),\ x \in \{-25,-20\};\quad (k,d) = (6,13),\ x \in \{-40,-25\};$$

$$(k,d) = (7,7),\ x \in \{-39,-32,-27,-22,-20,-15,-10,-3\};$$

$$(k,d) = (8,7),\ x \in \{-39,-27,-22,-10\};$$

$$(k,d) = (9,7),\ x \in \{-39,-34,-32,-24,-22,-17\};$$

$$(k,d) = (10,7),\ x \in \{-39,-24\},$$

where the values of P_k are given by

k	3	4	5	6	7, 8
P_k	3	5	7	11	13
k	9, 10, 11, 12	13, 14, 15	16, 17	18, 19, 20, 21, 22, 23	24
P_k	17	19	23	29	31

Observe that $P_k > k$ for $k \geq 4$ in Theorem 5.2.2, which is a new feature about equation (5.1).

As a simple and immediate corollary of Theorem 5.2.2 we get the following statement, concerning the case $P(b) \leq k$. We mention that already this result yields considerable improvement of Theorem A, in particular with respect to the bound for $P(b)$.

Corollary 5.2.1. *For $n = 5$ and $3 \leq k \leq 36$ all nontrivial solutions of equation (5.1) with $P(b) \leq k$ are given by*

$$(k, d) = (3, 7),\ x \in \{-16, -8, -6, 2\}; \quad (k, d) = (5, 7),\ x \in \{-16, -12\}.$$

Our last theorem provides the key to the proof of Theorem 5.2.2 in case of $k \geq 4$. It has been proved by a kind of sieving procedure, based upon genus 2 equations and the Chabauty method.

Note that having an increasing arithmetic progression $z_1 < \ldots < z_l$, by symmetry we obtain that $-z_l < \ldots < -z_1$ is also an increasing arithmetic progression. Hence dealing with such arithmetic progressions it is sufficient to give only one progression from each symmetric pair.

Theorem 5.2.3. *Let $4 \leq t \leq 8$ and $z_0 < z_1 < \ldots < z_{t-1}$ be a non-trivial primitive arithmetic progression. Suppose that*

$$z_0 = b_0 x_0^5, z_{i_1} = b_{i_1} x_{i_1}^5, z_{i_2} = b_{i_2} x_{i_2}^5, z_{t-1} = b_{t-1} x_{t-1}^5,$$

with some indices $0 < i_1 < i_2 < t - 1$ such that $P(b_0 b_{i_1} b_{i_2} b_{t-1}) \leq 5$. Then the initial term z_0 and common difference $z_1 - z_0$ of the arithmetic progression $z_0, \ldots, z_{t-1}$ for the separate values of $t = 4, \ldots, 8$ up to symmetry is one of
$t = 4 : (-9, 7), (-6, 7), (-6, 11), (-5, 7);$

$t = 5 : (-32, 17), (-25, 13), (-20, 11), (-16, 13), (-12, 7), (-12, 11),$
$(-12, 13), (-10, 7), (-8, 7), (-8, 11), (-4, 7), (-3, 7), (-1, 7), (2, 7),$
$(4, 7), (4, 23);$

$t = 6 : (-125, 61), (-81, 17), (-30, 31), (-25, 8), (-25, 11), (-25, 13),$
$(-25, 17), (-20, 9), (-20, 13), (-20, 19), (-20, 29), (-15, 7), (-15, 11),$
$(-15, 13), (-15, 23), (-10, 7), (-10, 11), (-8, 7), (-5, 7), (-3, 7),$
$(-1, 11), (-1, 13), (1, 7), (5, 11);$

$t = 7 : (-54, 19), (-54, 29), (-48, 23), (-30, 11), (-30, 13), (-27, 17),$
$(-24, 13), (-18, 7), (-18, 11), (-18, 13), (-18, 19), (-16, 11), (-15, 7),$

$(-12,7),(-12,11),(-10,7),(-6,7),(-6,11),(-4,9),(-3,13),(-2,7),$
$(-2,17),(2,13),(3,7),(6,7),(8,7),(9,11),(18,7);$

$t=8:(-405,131),(-125,41),(-100,49),(-32,11),(-27,11),$
$(-27,13),(-25,19),(-24,7),(-16,13),(-10,13),(-9,7),(-5,11),$
$(-4,7),(-2,11),(-1,13),(-1,7),(1,7),(3,11),(4,11),(5,7),(6,17).$

5.3 Preliminaries

Before giving the proofs of our results, we explain some principles and techniques which shall be used rather frequently later on. We present these tools separately because in this way the structure of our proofs will be more transparent.

5.3.1 Reducing equation (5.1) to arithmetic progressions of "almost" fifth powers

In a standard way, as $\gcd(x,d)=1$ and $n=5$, any solution of equation (5.1) can be written as

$$x+id=a_ix_i^5 \quad (i=0,1,\dots,k-1) \tag{5.2}$$

where x_i is a non-zero integer and a_i is a fifth power free positive integer with $P(a_i)\le k$. This observation justifies the title of the chapter, as well: the members of the arithmetic progression $x,x+d,\dots,x+(k-1)d$ are "almost" n-th powers.

5.3.2 Listing the possible coefficient tuples

Suppose that

$$a_{i_1}x_{i_1}^5<a_{i_2}x_{i_2}^5<\cdots<a_{i_t}x_{i_t}^5 \tag{5.3}$$

are t (not necessarily consecutive) nonzero terms of a primitive arithmetic progression, with a_{i_j} as in (5.2). In this subsection we explain a method to list all the possible coefficient t-tuples $(a_{i_1},a_{i_2},\dots,a_{i_t})$ corresponding to (5.3).

Observe that knowing a_{i_j} is equivalent to knowing the exponents $\nu_p(a_{i_j})$ of the primes $p\le k$ in the factorization of a_{i_j}. Take an arbitrary prime $p\le k$ dividing one of the terms $a_{i_j}x_{i_j}^5$, and suppose that i_{j_0} is such an index that

$$\nu_p(a_{i_{j_0}}x_{i_{j_0}}^5)\ge\nu_p(a_{i_j}x_{i_j}^5) \quad \text{for all } j=1,\dots,t.$$

Since the arithmetic progression is assumed to be primitive, one can easily check that then for all $j = 1, \ldots, t$ with $j \neq j_0$ we have

$$\nu_p(a_{i_j} x_{i_j}^5) = \nu_p(j - j_0).$$

As we have $\nu_p(a_{i_{j_0}}) < 5$, we can simply list all possibilities for the exponents of the prime p in the coefficients $a_{i_1}, a_{i_2}, \ldots, a_{i_t}$. Then combining these possibilities for all primes $p \leq k$, we can list all the possible coefficient t-tuples $(a_{i_1}, a_{i_2}, \ldots, a_{i_t})$ which may occur in (5.3).

5.3.3 Local testing of coefficient tuples

As we will see, some of the coefficient tuples listed in the previous subsection in fact cannot occur as coefficients of fifth powers in arithmetic progressions. In many cases this can be shown already modulo m with some appropriate choice of m. We shall use the moduli $m = 11, 25$.

Let $0 \leq i_1 < i_2 < \cdots < i_t \leq k-1$ be t indices, and consider a coefficient t-tuple $(a_{i_1}, a_{i_2}, \ldots, a_{i_t})$, which in fact we would like to exclude - that is, we would like to show that no corresponding subsequence

$$a_{i_1} x_{i_1}^5, \ldots, a_{i_t} x_{i_t}^5 \tag{5.4}$$

of any appropriate arithmetic progression exists. For this purpose, consider (5.4) modulo m (with $m = 11$ or 25). Observe that to have such a sequence, we should find appropriate fifth powers modulo m. We check all the possibilities. (Since we work with $m = 11$ and $m = 25$, the fifth powers modulo m are only $\{0, \pm 1\}$ and $\{0, \pm 1, \pm 7\}$, respectively.) Observe that by coprimality, we know that $m \mid a_{i_{j_1}}, a_{i_{j_2}}$ yields that $m \mid j_1 - j_2$. If we find that no fifth powers modulo m exist having also the previous property, then the actual coefficient tuple $(a_{i_1}, \ldots, a_{i_t})$ is not valid in the sense that no underlying subsequence (5.4) exists. We shall indicate how to use this test later on.

5.3.4 Reducing the problem to genus 2 equations

We found two ways to get access to genus 2 equations.

Reduction method I

Suppose that $a_0 x_0^5, a_1 x_1^5, a_2 x_2^5$ is an arithmetic progression with nonzero terms, and with common difference d. Then we have

$$(a_1 x_1^5)^2 - a_0 x_0^5 \cdot a_2 x_2^5 = d^2$$

which after the substitutions $X = -x_0x_2/x_1^2$, $Y = d/x_1^5$ and $A = a_0a_2$, $B = a_1^2$ yields the genus 2 equation

$$AX^5 + B = Y^2$$

in $X, Y \in \mathbb{Q}$.

Reduction method II

Suppose that

$$a_ix_i^5, a_jx_j^5, a_ux_u^5, a_vx_v^5$$

are four terms of an arithmetic progression. Then we have

$$(j-u)a_ix_i^5 + (u-i)a_jx_j^5 = (j-i)a_ux_u^5$$

and

$$(j-v)a_ix_i^5 + (v-i)a_jx_j^5 = (j-i)a_vx_v^5.$$

Multiplying these identities we get an equation of the form

$$AX^{10} + BX^5Y^5 + CY^{10} = DZ^5, \tag{5.5}$$

where $A = (j-u)(j-v)a_i^2$, $B = ((j-u)(v-i) + (u-i)(j-v))a_ia_j$, $C = (u-i)(v-i)a_j^2$, $D = (j-i)^2a_ua_v$ and $X = x_i$, $Y = x_j$, $Z = x_ux_v$. Then from (5.5) we can easily get both genus 2 equations over $\mathbb{Q}$

$$A_1Z_1^5 + B_1 = X_1^2 \quad \text{and} \quad A_2Z_2^5 + B_2 = X_2^2$$

with the notation $A_1 = 4AD$, $B_1 = B^2 - 4AC$, $X_1 = 2AX^5/Y^5 + B$, $Z_1 = Z/Y^2$ and $A_2 = 4CD$, $B_2 = B^2 - 4AC$, $X_2 = 2CY^5/X^5 + B$, $Z_2 = Z/X^2$, respectively.

The rational points on the genus 2 curves obtained by both methods (under suitable assumptions) can be determined by the Chabauty method. Then, following the corresponding substitutions backwards we can determine the actual members of the original arithmetic progressions.

Note that in fact in case of $k = 3$ in the proof of Theorem 5.2.2 we also use genus 1 curves over some number fields, which can be treated by the elliptic Chabauty method. However, since these are particular cases, we do not include them in this "general" discussion.

5.4 Proofs

We give the proofs of our results in a specific order. First we prove the case $k = 3$ of Theorem 5.2.2. We do so because this result is needed in the proof of Theorem 5.2.3, which is the next step. The latter result gives the key to derive Theorem 5.2.2 for $k \geq 4$. Then we continue by proving the cases $k \geq 4$ of Theorem 5.2.2 and its corollary. Finally, we give the proof of Theorem 5.2.1, which easily follows from Theorem 5.2.2.

In the proof of case $k = 3$ of Theorem 5.2.2 we shall make use of two lemmas. The first one is due to Bennett, Bruin, Győry, Hajdu [10].

Lemma 5.4.1. *Let C be a positive integer with $P(C) \leq 5$. If the Diophantine equation*

$$X^5 + Y^5 = CZ^5$$

has solutions in nonzero coprime integers X, Y and Z, then $C = 2$ and $X = Y = \pm 1$.

Proof. See Proposition 6.1 in [10]. □

The second lemma is a result of Saradha and Shorey [95].

Lemma 5.4.2. *Let A and B be coprime positive integers with $AB = 2^\alpha 3^\beta$ for nonnegative integers α and β with $\alpha \geq 4$. Then the Diophantine equation*

$$AX^5 + BY^5 = Z^5$$

has no solutions in coprime nonzero integers X, Y and Z.

Proof. This is a special case of Lemma 13 in [95]. □

Proof of the case $k = 3$ of Theorem 5.2.2. First list all the possible coefficient triples (a_0, a_1, a_2) as in (5.2). This can be done by the method explained in Subsection 5.3.2. Altogether we obtain 182 such triples. Observe that $a_2x_2^5, a_1x_1^5, a_0x_0^5$ is also an arithmetic progression. Hence by symmetry it is sufficient to consider those 106 triples for which $a_0 \leq a_2$. (It will be clear from our method that we can do so without loss of generality indeed.)

Clearly, $a_0x_0^5, a_1x_1^5, a_2x_2^5$ is also an arithmetic progression modulo 11 and 25. So we can test the coefficient triples modulo 11 and 25, as explained in Subsection 5.3.3. After the modulo 11 test we are left with 88 triples; for example $(1, 1, 6)$ gets excluded by this method. The test modulo 25 excludes 6 more triples (e.g. $(1, 4, 3)$), and we are left with 82 ones.

Then we apply Lemmas 5.4.1 and 5.4.2, in this order, for the remaining set of triples. As an example for the application of Lemma 5.4.1 consider $(a_0, a_1, a_2) = (2, 1, 4)$. The identity $a_0x_0^5 + a_2x_2^5 = 2a_1x_1^5$ gives an equation of the shape

$$X^5 + Y^5 = 2Z^5,$$

with $X = -x_0$, $Y = x_2$, $Z = x_1$, hence with X, Y, Z coprime. Then Lemma 5.4.1 gives that the only solutions are given by $(X, Y, Z) = \pm(1, 1, 1)$. In view of our assumption that the arithmetic progression on the left hand side of (5.1) has a positive common difference, we get that in this case the progression must be given by $(x, d) = (-2, 3)$, i.e. $x_0 = -1$, $x_1 = x_2 = 1$. Note that here we can automatically handle the "symmetric" case $(a_0, a_1, a_2) = (4, 1, 2)$. For this triple we get the only arithmetic progression is defined by $(x, d) = (-4, 3)$, belonging to $x_0 = x_1 = -1$, $x_2 = 1$. By the help of Lemma 5.4.1 we can exclude 58 triples. (Note that from this step, as we have seen, some solutions are obtained.) To see an example also for the application of Lemma 5.4.2, take $(a_0, a_1, a_2) = (1, 1, 54)$. As one can easily check, this triple has not been excluded so far, by any of our previous filters. Observe that since $a_2x_2^5$ is even, $a_0x_0^5$ also must be even, i.e. $2 \mid x_0$. Thus using the identity $a_0x_0^5 + a_2x_2^5 = 2a_1x_1^5$ once again, we get an equation of the form

$$16X^5 + 27Y^5 = Z^5$$

with $X = x_0/2$, $Y = x_2$, $Z = x_1$, and $\gcd(X, Y, Z) = 1$. Then Lemma 5.4.2 shows that this equation has no solutions, so there is no arithmetic progression with coefficient triple $(1, 1, 54)$. By Lemma 5.4.2 we can exclude 6 more triples, so at this stage we are left with 18 ones.

Now we apply our Reduction method I explained in Subsection 5.3.4 to handle the remaining triples. Note that the Chabauty method for determining the rational points on a genus 2 curve is applicable only if the rank of the curve is at most one. We find that in 16 out of the 18 triples this is just the case. For example, when $(a_0, a_1, a_2) = (4, 1, 18)$ we get the curve

$$72X^5 + 1 = Y^2,$$

which is of rank 0. The rational points on this curve (and two more rank zero curves) can be determined by the procedure `Chabauty0` of Magma. It turns out that the above equation has the only rational solutions $(X, Y) = (0, \pm 1)$. Since there is no corresponding arithmetic progression on the left hand side of (5.1), this triple is simply excluded. In case of $(a_0, a_1, a_2) = (1, 2, 3)$ the corresponding genus 2 curve is given by

$$3X^5 + 4 = Y^2,$$

which is of rank one. Then we use the procedure `Chabauty` of Magma (as well as in case of 12 alike curves) to get the rational points on the curve. We get that the above curve has the only rational points $(X, Y) = (-1, \pm 1), (0, \pm 2), (2, \pm 10)$. These points yield the only arithmetic progression given by

$$(x, d) = (1, 1).$$

(In the "symmetric" case $(a_0, a_1, a_2) = (3, 2, 1)$ we get the same curve, and the rational points yield the only arithmetic progression $(x, d) = (-3, 1)$.) Only in the cases $(a_0, a_1, a_2) = (1, 1, 3), (2, 9, 16)$ we get genus 2 curves of rank $>$ 1 (namely, of rank 2 in both cases). We handle these triples by the elliptic Chabauty method, and the procedure `Chabauty` of Magma. We give details only for the triple $(1, 1, 3)$, the other one can be handled similarly. In this case, using the identity $(x + d)^2 - x(x + 2d) = d^2$, we get the equation

$$X^5 - 3Y^5 = Z^2 \tag{5.6}$$

with $X = x_1^2$, $Y = x_0x_2$, $Z = d$. Further, the coprimality property yields $\gcd(X, Y, Z) = 1$. Finally, we may also assume that XY is odd. Indeed, $2 \mid Y$ would easily imply that both x_0 and x_2 are even, which would violate the coprimality property. Further, $2 \mid X$ would mean that $2 \mid x_1$. Then the identity $a_0x_0^5 + a_2x_2^5 = 2a_1x_1^5$ would give rise to

$$64(x_1/2)^5 - 3x_2^5 = x_0^5,$$

which is a contradiction by Lemma 5.4.2. Let K be the number field generated by $\alpha = \sqrt[5]{3}$ over $\mathbb{Q}$. Using the procedure `pSelmerGroup` of Magma, following the method of Bruin [24] we get that (5.6) can be factorized as

$$X^4 + \alpha XY^3 + \alpha^2X^2Y^2 + \alpha^3XY^3 + \alpha^4Y^4 = \delta U^2 \tag{5.7}$$

and

$$X - \alpha Y = \delta^{-1}V^2 \tag{5.8}$$

where U, V are some algebraic integers in K, and

$$\delta \in \{1, 7 + 6\alpha + 5\alpha^2 + 4\alpha^3 + 3\alpha^4, 1 + \alpha + \alpha^3, 4 + 2\alpha + \alpha^4\}.$$

Note that δ is a unit in K, so δ and δ^{-1} are algebraic integers in K. In case of $\delta = 1 + \alpha + \alpha^3$ or $4 + 2\alpha + \alpha^4$, write

$$V = b_0 + b_1\alpha + b_2\alpha^2 + b_3\alpha^3 + b_4\alpha^4$$

with some integers b_0, b_1, b_2, b_3, b_4 (using that $1, \alpha, \alpha^2, \alpha^3, \alpha^4$ is an integral basis for K). Expanding equation (5.8) in both choices for δ and using that XY is odd, we easily get a contradiction modulo 2 or 4, respectively. Assume next that $\delta = 1$. Then equation (5.7) yields the elliptic curve

$$E_1 : \ u^4 + \alpha u^3 + \alpha^2 u^2 + \alpha^3 u + \alpha^4 = v^2$$

over K, with $u = X/Y$ and $v = U/Y^2$. Using the point $(0, \alpha^2)$ of E_1, one can apply the elliptic Chabauty method and the procedure `Chabauty` of Magma to find the points of E_1 with $(u, v) \in \mathbb{Q} \times K$. In the present case the only such points are given by $(u, \pm v) = (0, \alpha^2)$. However, this point yields $x_1 = 0$ which is impossible. Finally, assume that $\delta = 7 + 6\alpha + 5\alpha^2 + 4\alpha^3 + 3\alpha^4$. Then (5.7) gives rise to the elliptic curve

$$E_2 : \ u^4 + \alpha u^3 + \alpha^2 u^2 + \alpha^3 u + \alpha^4 = (7 + 6\alpha + 5\alpha^2 + 4\alpha^3 + 3\alpha^4)v^2$$

over K, again with $u = X/Y$ and $v = U/Y^2$. Using the point $(-1, 1 + \alpha - \alpha^2 + \alpha^3 - \alpha^4)$ of E_2, by a similar procedure as in case of E_1 we get that the only points $(u, \pm v) \in \mathbb{Q} \times K$ of E_2 are $(-1, 1+\alpha-\alpha^2+\alpha^3-\alpha^4)$ and $(3, 3-3\alpha+7\alpha^2-3\alpha^3-\alpha^4)$. These points yield the only arithmetic progression given by $(x, d) = (-1, 2)$, and the triple $(1, 1, 3)$ is completely discussed. Note that obviously, in case of the coefficient triple $(3, 1, 1)$ we get the only progression $(x, d) = (-3, 2)$.

In case of the triple $(a_0, a_1, a_2) = (2, 9, 16)$ by a similar method we obtain that the only underlying arithmetic progression is $(x, d) = (2, 7)$ (and in case of $(a_0, a_1, a_2) = (16, 9, 2)$ it is $(x, d) = (-16, 7)$), and the proof of the case of $k = 3$ of Theorem 5.2.2 is complete. □

Proof of Theorem 5.2.3. We work inductively on t. Assume first that $t = 4$. Then the four terms $b_0 x_0^5, b_{i_1} x_{i_1}^5, b_{i_2} x_{i_2}^5, b_3 x_3^5$ in fact are consecutive ones of an arithmetic progression, that is, $i_1 = 1, i_2 = 2$. Then by case $k = 3$ of Theorem 5.2.2 (which has already been proved) we may assume that $5 \mid b_1 b_2$. Using symmetry (just as before) we may further suppose that $b_0 \leq b_3$. Now following the method explained in Subsection 5.3.2 we can list all such coefficient quadruples (b_0, b_1, b_2, b_3), which further have the properties as the coefficients in (5.2). Then we check the remaining quadruples modulo 11, modulo 25, then by Lemmas 5.4.1, 5.4.2. Since these checks go along the same lines as in the proof of the case of $k = 3$ of Theorem 5.2.2 above, we suppress the details.

Then in case of the quadruples still remain, we choose two arbitrary indices out of $\{0, 1, 2, 3\}$ as i, j (the remaining two indices will play the role of u, v), and apply Reduction method II as explained in Subsection 5.3.4 to construct

two genus 2 curves C_1 and C_2. If either of these curves happens to have rank ≤ 1, then by applying the Chabauty method (using Magma) its rational points can be determined. Then we get all arithmetic progressions corresponding to the actual coefficient quadruple. If the choice of i, j and u, v yields curves of ranks ≥ 2, then we make another choice for i, j and u, v, etc. Since we can construct $2 \cdot \binom{4}{2} = 12$ such curves (which apparently are "independent"), we have a good chance to handle all coefficient quadruples. In fact, this is just what happens indeed. For example, let $(b_0, b_1, b_2, b_3) = (3, 10, 1, 162)$. Then choosing $(i, j) = (0, 1)$ and $(u, v) = (2, 3)$ in Reduction method II, we have

$$-3x_0^5 + 20x_1^5 = x_2^5$$

and

$$-6x_0^5 + 30x_1^5 = 162x_3^5.$$

Multiplying these identities we get the equation

$$18x_0^{10} - 210(x_0x_1)^5 + 600x_1^{10} = 162(x_2x_3)^5.$$

Introducing the new variables $X = x_2x_3/x_1^2$ and $Y = 6x_0^5/x_1^5 - 35$, the previous equation yields

$$Y^2 = 324X^5 + 25.$$

This genus 2 equation is of rank 0. Using the procedure `Chabauty0` of Magma, we get that the only rational solutions of this equation are $(X, Y) = (0, \pm 5)$. Following the substitutions backwards, we obtain no solution for x_0, x_1, x_2, x_3.

We handled all the possible coefficient quadruples remaining after the above explained tests similarly. We get that the only non-trivial possibilities in case of $t = 4$ are those given in the theorem.

Now assume that the statement is proved for some $t \in \{4, 5, 6, 7\}$, and consider the value $t + 1$. The indices i_1, i_2 may take only $(t - 1)(t - 2)/2$ values altogether. From this point on we just repeat the same steps as with $t = 4$. For instance, suppose we have already finished with the case $t = 7$ and consider the case of $t + 1 = 8$ terms. Then we have 15 possibilities for the pair of indices (i_1, i_2), given by $0 < i_1 < i_2 < 7$. As an example, take $(i_1, i_2) = (2, 3)$ and consider the tuple $(b_0, b_2, b_3, b_7) = (24, 10, 3, 25)$. As it cannot be excluded neither modulo 11, modulo 25, nor by Lemmas 5.4.1, 5.4.2, we use Reduction method II, again. Choosing $(i, j) = (0, 7)$ and $(u, v) = (2, 3)$ we obtain

$$120x_0^5 + 50x_7^5 = 70x_2^5$$

and

$$96x_0^5 + 75x_7^5 = 21x_3^5.$$

Multiplying these identities we get

$$11520x_0^{10} + 13800x_0{x_7}^5 + 3750x_7^{10} = 1470(x_2x_3)^5.$$

After some calculations we are left with the equation

$$Y^2 = 3675X^5 + 30625,$$

where $X = 2x_2x_3/x_7^2$ and $Y = 960x_0^5/x_7^5 + 575$. This equation is of genus 2 and of rank 1. Using the procedure `Chabauty` of Magma again, we conclude that its rational solutions are $(X, Y) = (0, \pm 175), (2, \pm 385)$. Following the substitutions backwards, we find the only solution for the tuple $(x_0, x_2, x_3, x_7) = (-1, -1, -1, 1)$ and the arithmetic progression $(-24, -17, -10, -3, 4, 11, 18, 25)$.

Altogether we get the only possibilities listed in the statement, and the proof of the theorem is complete. □

Proof of the case $k \geq 4$ of Theorem 5.2.2. Clearly, the case $k = 4$ is an immediate consequence of Theorem 5.2.3. Further, observe that the cases $k = 8, 10, 11, 12, 14, 15, 17, 19, 20, 21, 22, 23$ trivially follow from the corresponding cases for $k-1$. Hence it is sufficient to consider the values $k = 5, 6, 7, 9, 13, 16, 18, 24$. In each case make the following steps. We list all the possible coefficient k-tuples $(a_0, a_1, \ldots, a_{k-1})$ by the method given in Subsection 5.3.2. As previously, by symmetry we may assume that $a_0 \leq a_{k-1}$. In the generation process we consider only those placements of primes which cannot be automatically excluded by induction. For example, let $k = 13$; then $P_k = 19$. If $19 \nmid a_4a_5a_6a_7a_8$ then by coprimality we have that either $P(a_0a_1 \ldots a_8) \leq 17$ or $P(a_4a_5 \ldots a_{12}) \leq 17$, and we can apply induction based upon the case $k = 9$. Further, if say $19 \mid a_8$ but $17 \nmid a_1a_2 \ldots a_6$ then one of $P(a_0a_1 \ldots a_6) \leq 13$, $P(a_1 \ldots a_7) \leq 13$ holds, and we can use the case $k = 7$, and so on. Then for the remaining tuples try to find indices $j_1, j_2, j_3, j_4 \in \{0, 1, \ldots, k-1\}$ which are (not necessarily consecutive) terms of an arithmetic progression of length t with $4 \leq t \leq 8$, such that $P(a_{j_1}a_{j_2}a_{j_3}a_{j_4}) \leq 5$. It turns out that it is possible to find such indices in case of all the remaining k-tuples. Having four such indices, we can simply apply Theorem 5.2.3 to handle the actual coefficient tuple. For example, let $k = 6$ and consider the tuple

$$(a_0, a_1, \ldots, a_5) = (20, 11, 2, 7, 16, 25).$$

Note that this tuple cannot be excluded by induction. Take $(j_1, j_2, j_3, j_4) = (0, 2, 4, 5)$, and observe that $P(a_0a_2a_4a_5) \leq 5$ holds. Applying Theorem 5.2.3 with $t = 6$, $b_0 = a_0, b_{i_1} = a_2, b_{i_2} = a_4, b_5 = a_5$, we find that the only nontrivial primitive increasing arithmetic progressions corresponding to this tuple are $-20, -11, -2, 7, 16, 25$ and its symmetric pair $-25, -16, -7, 2, 11, 20$. These progressions are listed in the statement.

Considering another example, let $k = 18$ and take the tuple

$$(a_0, a_1, \ldots, a_{17}) = (2, 125, 132, 13, 14, 57, 40, 29, 54, 1, 68, 105, 46, 11, 48, 1, 130, 9).$$

This tuple cannot be excluded using induction. However, we find four appropriate indices again, namely $(j_1, j_2, j_3, j_4) = (8, 9, 14, 15)$ for which $P(a_8a_9a_{14}a_{15}) \leq 5$ holds. Applying Theorem 5.2.3 with $t = 8$, $b_0 = a_8, b_{i_1} = a_9, b_{i_2} = a_{14}, b_{t-1} = a_{15}$, we find that the only possible underlying 8-tuple is $(a_8, a_9, \ldots, a_{15}) = (54, 1, 68, 105, 46, 11, 48, 1)$. However, there is no arithmetic progression having the appropriate property corresponding to this tuple. Therefore we have no solution with the original 18-tuple $(a_0, a_1, \ldots, a_{17})$.

By this process we have found all the nontrivial arithmetic progressions, which are just the ones listed in the statement. □

Proof of Corollary 5.2.1. Since the next prime after 31 is 37, the statement is an immediate consequence of Theorem 5.2.2. □

Proof of Theorem 5.2.1. For $k \leq 24$ the statement is a simple consequence of Theorem 5.2.3. In case of $25 \leq k \leq 54$, observe that in (5.2) the product $A := a_0a_1 \ldots a_{k-1}$ must be a full fifth power. Thus any prime $p \mid A$ must divide at least two coefficients a_i. Hence one can easily check that for these values of k there always exists an index i with $0 \leq i < k - 24$ such that $P(a_ia_{i+1} \ldots a_{i+23}) \leq 31$. So the statement follows from Theorem 5.2.3 also in this case. □

Summary

Our dissertation consists of five chapters each containing new results concerning Diophantine equations and Diophantine problems. Most problems have certain combinatorial background.

In the first chapter we presented the main method used in our studies namely the $\mathcal{E}llog$ method together with an improvement due to Hajdu and Kovács [50]. Mordell initiated the search for integral solutions of elliptic equations. By Siegel's famous theorem [100], at most finitely many integral solutions exist for any given elliptic equation. Since this result is ineffective, the determination of all such solutions remained a challenge. Baker's famous work on linear forms in logarithms of algebraic numbers made Siegel's theorem effective. Since then several improvements have been achieved, see e.g. [4], [19], [99], [102], [27], [49] and the references given there. Besides these results a great variety of methods and techniques have been successfully applied to solve individual equations, (see e.g. [71], [72], [2], [66], [3], [18], [119], [86] and the references given there) until a new method was developed simultaneously and independently by Stroeker, Tzanakis [103] and Gebel, Pethő, Zimmer [41]. This approach uses the arithmetic properties of elliptic curves and combines many deep ingredients, due to several authors. Later, the method of Stroeker and Tzanakis, the so-called $\mathcal{E}llog$ method has been developed further. The most recent version is already capable to find (at least in principle) all integral points on genus 1 curves (see [105], and also the references given there). In Chapter 1, we described in details the above mentioned $\mathcal{E}llog$ method and presented an improvement due to Hajdu and Kovács [50]. Stroeker and Tzanakis [104] gave convincing numerical and heuristic evidence for that in their $\mathcal{E}llog$ method a certain parameter λ plays a decisive role in the size of the final bound for the integral points on elliptic curves. Further, they provided an algorithm to determine that Mordell-Weil basis of the curve which corresponds to the optimal choice of λ. In the first chapter we showed that working with more Mordell-Weil bases simultaneously,

the final bound for the integral points can be further decreased.

In the second chapter some Diophantine equations concerning binomial coefficients, power sums and product of consecutive integers were solved. One of the first results giving all integer solutions of a combinatorial Diophantine equation is a theorem of Mordell [71], which provides all integer solutions of the equation $y(y+1) = x(x+1)(x+2)$. Other scattered equations have been investigated by several authors, see for example [2], [3], [18], [66], [86], [103], [118], [119], [122]. Hajdu and Pintér [52] systematically collected and solved those combinatorial equations that can be reduced to Mordell-type equations. Our purpose was to extend this result to more general combinatorial equations that can be reduced to general elliptic equations. Namely, we collected those equations that can be reduced to equations of genus 1. The equations were solved with the $\mathcal{E}llog$ method and with the Magma computational algebra system. We mention that beside a lot of sparse results (see e.g. [82], [83], [86], [106] and [121]), Stroeker and de Weger [107] solved all such equations involving binomial coefficients. The results of the second chapter are published in [58].

In the third chapter we gave several effective and explicit results concerning the values of some polynomials in binary recurrence sequences. There are many papers about values of a polynomial $p(x) \in \mathbb{Q}[x]$ (taken at integer values of x) in a binary linear recurrence sequence U. The first such results dealt with the case where U is a special sequence and $p(x) = x^m$ with some $m \geq 2$. Ogilvy [77] and later Moser and Carlitz [73], and Rollett [92] proposed the problem of determining all squares in the Fibonacci sequence F. The problem was solved by Cohn [29, 30] and Wyler [125] independently. Later, Alfred [1] and Cohn [31] determined the squares in the Lucas sequence L. Pethő [80] and Cohn [32] independently determined the perfect powers in the Pell sequence. Recently, Bugeaud, Mignotte and Siksek [28] computed all perfect powers in the Fibonacci and Lucas sequences. Another branch of problems is about triangular numbers in recurrence sequences. Hoggatt conjectured that there are only five triangular Fibonacci numbers. Ming [69] proved that this conjecture is true. Furthermore, Ming [70] and McDaniel [68] determined the triangular numbers in the Lucas and Pell sequences, respectively. In [108] Szalay described all values of the polynomials $S_2(x)$ and $S_3(x)$ in the Fibonacci, Lucas and Pell sequences, where $S_k(x)$ denotes the sum of the first $x-1$ kth powers($x \in \mathbb{N}$). Further, he listed all numbers of the form $\binom{x}{4}$ in the Fibonacci and Lucas sequences, as well. Beside the above mentioned results that give complete solutions of a given problem there are several results which provide effective upper bounds for the solutions under certain assumptions. The most extensively investigated situation is again the case of perfect powers. We mention that Szalay [108] provided

an algorithm for the complete description of the values of a polynomial $p(x)$ of degree 3 in a binary recurrence sequence U under some assumptions. In the third chapter we proved three theorems concerning the values of some polynomials in binary recurrence sequences. First we provided an effective finiteness theorem for certain combinatorial numbers, namely for binomial coefficients, products of consecutive integers, power sums and alternating power sums in binary recurrence sequences, under some assumptions. Our second theorem was an extension of the above mentioned result of Szalay. More precisely, it provided an efficient algorithm for determining the values of certain degree 4 polynomials in binary recurrence sequences, under some assumptions. We note that we implemented our algorithm in Magma [17] as well. Finally, partly by the help of this algorithm we gave all combinatorial numbers mentioned above for the small values of the parameter involved in the Fibonacci, Lucas, Pell and Associated Pell sequences. The results of the third chapter are published in [59].

In the fourth chapter we introduced the concept of balancing numbers in arithmetic progressions, and proved several effective finiteness and explicit results about them. The literature of balancing numbers is very rich. In [62] and [63] Liptai proved that there are no Fibonacci and Lucas balancing numbers, respectively. Later, Szalay [111] derived the same results by a different method. In [64] Liptai, Luca, Pintér and Szalay generalized the concept of balancing numbers to a (k, l)-power numerical center. In [64] several effective and ineffective finiteness results were proved for these numbers. Recently, the "balancing" property has been investigated in recurrence sequences (see [14]). In the fourth chapter we extended the concept of balancing numbers to arithmetic progressions. Let $a > 0$ and $b \geq 0$ be coprime integers. If for some positive integers n and r we have

$$(a + b) + \cdots + (a(n - 1) + b) = (a(n + 1) + b) + \cdots + (a(n + r) + b)$$

then we say that $an + b$ is an (a, b)-balancing number. The sequence of (a, b)-balancing numbers is denoted by $B_m^{(a,b)}$ $(m = 1, 2, \dots)$. We proved several effective finiteness and explicit results concerning polynomial values in the sequences $B_m^{(a,b)}$. That is, we considered the equation

$$B_m^{(a,b)} = f(x)$$

in integers m and x with $m \geq 1$, where f is some polynomial with rational coefficients, taking only integral values at integers. In the proofs of our results, among others, we combined Baker's method, the modular method developed by Wiles [124] and others, a result of Bennett [8] about the diophantine equation

$|ax^n - by^n| = 1$, the Chabauty method and the theory of elliptic curves. Our results from Chapter 4 are published in [60].

In the fifth chapter we proved that the product of k consecutive terms of a primitive arithmetic progression is never a perfect fifth power when $3 \leq k \leq 54$. We also provided a more precise statement, concerning the case where the product is an "almost" fifth power. Our theorems yield considerable improvements and extensions, in the fifth power case, of recent results due to Győry, Hajdu and Pintér [47].

A celebrated theorem of Erdős and Selfridge [38] states that the product of consecutive positive integers is never a perfect power. A natural generalization is the Diophantine equation

$$x(x+d)\dots(x+(k-1)d) = by^n \tag{2}$$

in non-zero integers x, d, k, b, y, n with $\gcd(x,d) = 1$, $d \geq 1$, $k \geq 3$, $n \geq 2$ and $P(b) \leq k$. Here $P(u)$ stands for the largest prime divisor of a non-zero integer u, with the convention $P(\pm 1) = 1$.

By a conjecture of Erdős, equation (2) has no solutions in positive integers when $k > 3$ and $b = 1$. In other words, the product of k consecutive terms of a primitive positive arithmetic progression with $k > 3$ is never a perfect power. The conjecture of Erdős has recently been verified for certain values of k in a more general form; see the papers [45], [46], [10], [47].

We explained why the case $n = 5$ is special and proved extensions of the previous results. Apparently, for $n = 5$ elliptic curves are not applicable. We showed that in this case the Chabauty method (both the classical and the elliptic versions) can be applied very efficiently. The results of Chapter 5 are published in [51].

Összefoglaló

Az értekezés öt fejezetből áll, melyek kombinatorikus háttérrel rendelkező diofantikus egyenletekkel, illetve diofantikus problémákkal kapcsolatos új eredményeket tartalmaznak.

Az **első fejezet**ben a vizsgálataink során használt legfontosabb módszert, az úgynevezett $\mathcal{E}llog$ módszert és annak egy tőlünk származó javítását mutatjuk be. Elliptikus egyenletek egész megoldásainak meghatározásával először Mordell foglalkozott. Siegel [100] egy klasszikus eredménye alapján ismert, hogy (bizonyos triviális feltételek mellett) egy ilyen egyenlet csak véges sok egész megoldással rendelkezik. Később Baker [4] az egyenlet paraméterei segítségével a megoldásokra effektív felső korlátot adott. Az utóbbi évtizedekben többen értek el további javításokat, lásd például [4], [19], [99], [102], [27], [49] és az ottani hivatkozásokat. Ezen eredmények mellett különböző módszerek használatával sikerült konkrét egyenletek összes egész megoldását meghatározni (lásd [71], [72], [2], [66], [3], [18], [119], [86] és az ottani hivatkozásokat). 1994-ben egymástól függetlenül Gebel, Pethő, Zimmer [41] és Stroeker, Tzanakis [103] kidolgozott egy általános módszert elliptikus görbék egész pontjainak meghatározására, mely a görbék algebrai és geometriai tulajdonságait használja. Az úgynevezett $\mathcal{E}llog$ módszer képes 1 génuszú görbék egész pontjainak meghatározására, legalábbis elvben. Az első fejezetben részletesen bemutatjuk a módszert és annak egy tőlünk származó javítását. A módszer három fő részre osztható. Elöljáróban az elliptikus görbe alapadatait határozzuk meg, például a torziócsoportot, az r rangot és egy $(P_1, \ldots, P_r)$ Mordell-Weil bázist. Tudjuk, hogy bármely $P \in E(\mathbb{Q})$ racionális pont egyértelműen felírható

$$P = P_0 + n_1 P_1 + \ldots + n_r P_r \tag{1}$$

alakban, ahol P_0 torziópont és $n_i \in \mathbb{Z}$ $(i = 1, \ldots, r)$. Legyen $N = \max_{1 \le i \le r}\{|n_i|\}$. A módszer első lépésében meghatározunk egy kezdeti felső korlátot N-re. Ezt

különböző magasságokra vonatkozó becslések és David [36] egy mély, elliptikus logaritmusok lineáris formáira vonatkozó eredménye segítségével tehetjük meg. Amennyiben rendelkezünk egy felső korláttal N-re, úgy minden az (1)-nek eleget tevő P pont meghatározható, legalábbis elvileg.

A kezdeti felső korlát N-re tipikusan nagyon nagy, így a gyakorlatban nem használható. Az *Ellog* módszer második lépésében ezt a kezdeti korlátot jelentős mértékben csökkentjük. Ennek eléréséhez kulcsfontosságú de Weger [120] egy az LLL-algoritmuson alapuló eredménye.

A módszer harmadik lépése triviálisnak tűnik: az N-re kapott végső korlátot felhasználva (ami tipikusan 10 körüli érték) leszámláljuk a kis megoldásokat. Azonban ez az ártalmatlannak tűnő rész akár a legproblémásabb is lehet. Ha a görbe rangja nagy, akkor a megoldásokat tartalmazó tartomány mérete hatalmas lehet. (Ezen a ponton érdemes megjegyezni, hogy egy sejtés szerint tetszőlegesen nagy rangú elliptikus görbe is létezik.) Tehát az N-re kapott „végső" korlát kis mértékű javítása vagy a megoldásokat tartalmazó tartomány méretének csökkentése rendkívül fontos lehet konkrét egyenletek megoldásánál. Emiatt érdemes külön figyelmet szentelni ennek a pontnak.

Stroeker és Tzanakis [104]-ben megmutatták, hogy az N_v végső korlát meghatározásánál döntő szerepe van egy bizonyos λ paraméternek, amely a Mordell-Weil bázishoz tartozó magasságmátrix legkisebb pozitív sajátértéke. Stroeker és Tzanakis kidolgoztak egy algoritmust, mely segítségével meghatározható egy optimális bázis, vagyis egy olyan bázis, melyhez tartozó λ érték a lehető legnagyobb. Egy ilyen bázisban dolgozva az N_v végső korlát minimális lesz. Egy ilyen bázist Stroeker-Tzanakis bázisnak, vagy röviden ST-bázisnak nevezünk. Stroeker és Tzanakis [104]-ben több példán keresztül illusztrálták, hogy egy ST-bázissal dolgozva kisebb végső korlát érhető el, mint bármely más bázisban. Ez különösen „nagy" rangú görbék esetén lényeges, amikor a végső korlát már egy kismértékű javítása is nagy mértékben redukálja a megoldásokat tartalmazó tartományt. Az első fejezetben megmutatjuk, hogy egy ST-bázis használata során adódó „legjobb" végső korlát is tovább javítható, ha több bázisban párhuzamosan dolgozunk, és kombináljuk az így adódó információkat. Az első fejezet eredményeit az [50] publikáció tartalmazza.

A **második fejezet**ben az *Ellog* módszert használva számos diofantikus egyenletet oldunk meg. A kombinatorikus hátterű, egymást követő számok szorzataival, hatványösszegekkel és binomiális együtthatókkal kapcsolatos diofantikus egyenletek irodalma rendkívül gazdag. Számos mély effektív és ineffektív eredmény ismert ilyen jellegű egyenletek megoldásaira vonatkozóan. Ezen a ponton csupán a [15], [16], [21], [88], [89] cikkekre és az ottani hivatkozásokra utalunk. Jelen keretek között csupán azon még mindig igen nagy

számú eredmény feltérképezésére vállalkozhatunk, melyek a vizsgált egyenletek *összes* megoldását meghatározzák. Az egyik első ilyen jellegű eredménynek Mordell [71] egy tétele tekinthető, mely az $y(y+1) = x(x+1)(x+2)$ egyenlet összes egész megoldását megadja. A későbbiekben számos olyan elszórt eredmény született, amely említett típusú egyenletek összes megoldását leírja, lásd például [2], [3], [18], [66], [86], [103], [118], [119], [122] és az ottani hivatkozásokat. Hajdu és Pintér [52] szisztematikusan összegyűjtötte azokat a kombinatorikus egyenleteket, melyek Mordell-típusú (azaz $f(x) = y^2$, $\deg f = 3$ alakú) elliptikus egyenletre redukálhatóak, és a korábban nem vizsgált egyenleteket megoldotta. A második fejezetben szisztematikusan összegyűjtjük és megoldjuk mindazon fenti típusú egyenletet, melyek 1 génuszú egyenletekre redukálhatóak. Megemlítjük, hogy az irodalomban ebben az esetben is számos elszórt eredmény ismert (lásd [82], [83], [86], [106], [107] és [121]). A második fejezet eredményeit az [58] dolgozat tartalmazza.

A **harmadik fejezet**ben másodrendű lineáris rekurzív sorozatok polinomértékeivel kapcsolatos effektív és explicit eredményeket mutatunk be. A másodrendű lineáris rekurzív sorozatokkal kapcsolatos diofantikus egyenletek irodalma rendkívül gazdag. 1962-ben Ogilvy [77], majd egy évvel később Moser és Carlitz [73], valamint Rollett [92] a következő problémát fogalmazták meg: határozzuk meg az F_n Fibonacci sorozatban található négyzetszámokat! A problémát egymástól függetlenül Cohn [29, 30] és Wyler [125] oldotta meg. Később, Alfred [1] és Cohn [31] megkeresték a négyzetszámokat az L_n Lucas sorozatban. Pethő [80], és később Cohn [32] egymástól függetlenül meghatározták a Pell sorozatban található teljes hatványokat. Újabban Bugeaud, Mignotte és Siksek [28] meghatározták a Fibonacci illetve Lucas sorozatban található teljes hatványokat.

Egy másik, az érdeklődés középpontjában álló probléma a tringuláris számok meghatározása adott másodrendű lineáris rekurzív sorozatokban. Hogatt sejtése szerint mindössze öt darab trianguláris Fibonacci szám létezik, ezt 1989-ben Ming [69] be is bizonyította. Később Ming [70] a Lucas sorozatban, majd McDaniel [68] a Pell sorozatban álló trianguláris számokat is megkereste. Az eredmények általánosításaként Tengely [114] meghatározta az úgynevezett g-szög számokat a Fibonacci, Lucas, Pell és asszociált Pell sorozatokban, a g paraméter több értékére. Tengely [115] a közelmúltban megmutatta, hogy az egyetlen $\binom{x}{5}$ alakú elem a Lucas sorozatban az $L_1 = 1$.

A fentiek mellett sok olyan eredmény is ismert, melyek különböző kombinatorikus hátterű számokat írnak le bizonyos másodrendű lineáris rekurzív sorozatokban. 2001-ben Szalay [108] a Fibonacci, Lucas és Pell sorozatban határozott meg egyes binomiális együtthatókat és hatványösszegeket. Szalay [108]-ban egy

algoritmust is megadott, mely segítségével bizonyos feltételek mellett meg lehet határozni egy harmadfokú polinom értékeit egy másodrendű lineáris rekurzív sorozatban.

A harmadik fejezetben először egy effektív végességi tételt bizonyítunk az $U_n = p(x)$ egyenlet egész megoldásaira vonatkozóan. Itt U_n egy nemdegenerált másodrendű lineáris rekurzív sorozat, $p(x)$ pedig egy legalább negyedfokú polinom, mely binomiális együtthatót, egymást követő számok szorzatait, hatványösszeget, vagy alternáló hatványösszeget jelöl. A bizonyítás a Baker-módszeren, valamint Brindza [19], Ping-Zhi [81], Pintér és Rakaczki [85] és Rakaczki [90] eredményein alapszik. Második tételünk Szalay fent említett algoritmusának kiterjesztése negyedfokú polinomok esetére. Megjegyezzük, hogy az algoritmusunkat implementáltuk a Magma [17] programcsomagban. Továbbá a fent említett három rekurzív sorozatban, illetve az asszociált Pell sorozatban egyes, a korábbi vizsgálatokból kimaradt binomiális együtthatókat, illetve a korábbi eredményekkel összhangban egymást követő számok szorzatait és alternáló hatványösszegeket keresünk, részben az algoritmusunk segítségével. A harmadik fejezet eredményeit az [59] cikk tartalmazza.

A **negyedik fejezet**ben balansz számok általánosításával foglalkozunk, konkrétan számtani sorozatok balansz számait definiáljuk és azokkal kapcsolatban bizonyítunk több tételt. Egy n pozitív egész számot balansz számnak nevezünk, ha

$$1 + \cdots + (n-1) = (n+1) + \cdots + (n+r)$$

teljesül valamely r pozitív egész számra (lásd [7] és [39]). A balansz számok sorozatát B_m-mel jelöljük ($m = 1, 2, \dots$). Könnyen ellenőrizhető, hogy $B_1 = 6$ és $B_2 = 35$. Behera és Panda [7] megmutatták, hogy a sorozatra a

$$B_{m+1} = 6B_m - B_{m-1} \qquad (m > 1).$$

rekurzió érvényes. Megjegyezzük, hogy végtelen sok balansz szám létezik.

A balansz számokkal kapcsolatos irodalom nagyon gazdag. Liptai [62]-ben és [63]-ban megmutatta, hogy nem létezik Fibonacci, illetve Lucas balansz szám. Később Szalay [111] más módszerrel belátta ugyanezt.

[64]-ben Liptai, Luca, Pintér és Szalay általánosították a balansz számok fogalmát a következőképpen. Legyen y, k, l rögzített pozitív egészek, $y \geq 4$. Egy x pozitív egészt, ahol $x \leq y - 2$, (k, l)-hatvány számtani középnek nevezünk, ha

$$1^k + \cdots + (x-1)^k = (x+1)^l + \cdots + (y-1)^l$$

teljesül. [64]-ben számos effektív és ineffektív végességi tételt bizonyítottak (k, l)-hatvány számtani közepekre.

Nemrégiben a „balansz” tulajdonságot rekurzív sorozatokban is vizsgálták (lásd [14]). A negyedik fejezetben kiterjesztjük a balansz számok fogalmát számtani sorozatokra. Legyen $a > 0$ és $b \geq 0$ relatív prím egészek. Ha valamely n és r pozitív egészekre

$$(a+b) + \cdots + (a(n-1)+b) = (a(n+1)+b) + \cdots + (a(n+r)+b)$$

teljesül, akkor azt mondjuk, hogy $an+b$ egy (a,b)-balansz szám. Jelölje $B_m^{(a,b)}$ $(m = 1, 2, \dots)$ az (a,b)-balansz számok sorozatát. Megjegyezzük, hogy mivel $B_m^{(1,0)} = B_m$ bármely m-re, így a balansz számok egy általánosítását kapjuk.

Vizsgálataink során több effektív végességi és explicit eredményt bizonyítunk a $B_m^{(a,b)}$ sorozatban található különböző polinomértékekkel kapcsolatban. Konkrétan, a

$$B_m^{(a,b)} = f(x)$$

egyenletet tekintjük, ahol m és x egészek, továbbá $m \geq 1$, f egy racionális együtthatós polinom, mely egész értékű helyeken egész értéket vesz fel. Bizonyításaink során Ping-Zhi [81], Pintér és Rakaczki [85] és Rakaczki [90] korábban említett eredményei mellett szükségünk van továbbá a Wiles [124] által kidolgozott moduláris módszerre, valamint Bennett [8] egy binom Thue egyenletekkel kapcsolatos mély eredményére. A negyedik fejezet eredményeit a [60] cikk tartalmazza.

Az **ötödik fejezet**ben bebizonyítjuk, hogy egy primitív számtani sorozat k darab egymást követő elemének szorzata nem lehet teljes ötödik hatvány $3 \leq k \leq 54$ esetén. Emellett megadunk egy pontosabb állítást abban az esetben, mikor a szorzat egy „majdnem” teljes ötödik hatvány. Erdős és Selfridge [38] egy ünnepelt tétele azt mondja ki, hogy egymást követő pozitív egészek szorzata nem lehet teljes hatvány. Az

$$x(x+d)\dots(x+(k-1)d) = by^n \tag{2}$$

egyenlet egy természetes általánosítása az előbbi problémának. Itt x, d, k, b, y, n nem-nulla egészek, $\gcd(x,d) = 1$, $d \geq 1$, $k \geq 3$, $n \geq 2$ és $P(b) \leq k$, ahol $P(u)$ az u nem-nulla egész legnagyobb prímosztóját jelöli és megállapodás szerint $P(\pm 1) = 1$.

A (2) egyenlet irodalma rendkívül gazdag. Az egyenletet $d = 1$-re teljesen megoldotta Saradha [94] ($k \geq 4$ esetén) illetve Győry [44] ($k < 4$ esetén). A $d > 1$ esetre vonatkozó igen nagy számú kapcsolódó eredmény áttekintése helyett ajánljuk az Olvasó figyelmébe Győry [45], Shorey [96], [97] és Tijdeman [116] összefoglaló cikkeit.

Erdős egy sejtése szerint a (2) egyenletnek nincs pozitív egész megoldása, ha $k > 3$ és $b = 1$; vagyis egy primitív, pozitív számtani sorozat k darab egymást követő elemének szorzata $k > 3$ esetén nem lehet teljes hatvány. Erdős sejtését bizonyos k értékekre egy általánosabb formában sikerült belátni; lásd [45], [46], [10], [47]. Mi az $n = 5$ esetre koncentrálunk. Az erre a kitevőre vonatkozó legjobb eredményt a következő tétel tartalmazza, mely [45] ($k = 3$ eset), [46] ($k = 4, 5$ esetek), [10] ($k = 6, 7$ esetek) és [47] ($8 \leq k \leq 34$ esetek) megfelelő eredményeinek ötvözete. (Megjegyezzük, hogy az említett eredmények bármely $n \geq 2$ esetén érvényesek.)

Tétel A. *A* (2) *egyenlet összes megoldása* $n = 5$, $3 \leq k \leq 34$ *és* $P(b) \leq P_k$ *esetén, ahol*

$$P_k = \begin{cases} 2, & \text{if } k = 3, 4, \\ 3, & \text{if } k = 5, \\ 5, & \text{if } k = 6, 7, \\ 7, & \text{if } 8 \leq k \leq 22, \\ \frac{k-1}{2}, & \text{if } 23 \leq k \leq 34 \end{cases}$$

az alábbiak:

$$(k, d) = (8, 1),\ x \in \{-10, -9, -8, 1, 2, 3\}; \quad (k, d) = (8, 2),\ x \in \{-9, -7, -5\};$$

$$(k, d) = (9, 1),\ x \in \{-10, -9, 1, 2\}; \quad (k, d) = (9, 2),\ x \in \{-9, -7\};$$

$$(k, d) = (10, 1),\ x \in \{-10, 1\}; \quad (k, d, x) = (10, 2, -9).$$

Az $n = 5$ kitevő esete speciális. Rögzített k és $n \geq 2$ esetén a legfontosabb eszköz a moduláris módszer, melyet Wiles [124] fejlesztett ki. Azonban ez a módszer csak „nagy" kitevők, tipikusan $n \geq 7$ esetén dolgozik eredményesen. Emiatt a „kis" kitevőket külön kell kezelni. Az $n = 2, 3$ kitevőket már több önálló cikkben vizsgálták. Az $n = 2$ és pozitív x esetén a (2) egyenletet teljesen megoldotta néhány kivételes esettől eltekintve Hirata-Kohno, Laishram, Shorey és Tijdeman [57] $k \leq 100$-ra, $b = 1$ esetén pedig $k \leq 109$-re. Legfontosabb eszközeik az elliptikus görbék és a kvadratikus maradékok voltak. Később a kimaradt kivételes eseteket Tengelynek [113] sikerült kezelnie a Chabauty módszer segítségével. Az $n = 3$ esetben főként köbmaradékok, illetve emellett az elliptikus görbék és a Chabauty módszer használatával Hajdu, Tengely és Tijdeman [54] teljesen megoldotta a (2) egyenletet $k < 32$-re, ahol $P(b) \leq k$, ha $4 \leq k \leq 12$ illetve $P(b) < k$, ha $k = 3$ vagy $k \geq 13$. Továbbá $b = 1$ esetén megoldották (2)-t $k < 39$-re. Az $n = 5$ esetet korábban nem vizsgálták meg közelebbről.

Az eddigi eredményekben főleg Dirichlet és Lebesgue klasszikus eredményeit használtak fel, lásd például [47]. Ennél a kitevőnél az elliptikus görbék nem használhatóak. Az ötödik fejezetben megmutatjuk, hogy a Chabauty módszer nagyon hatékonyan alkalmazható, eredményeinkben nagy számú 2 génuszú egyenletet oldunk meg a Chabauty módszerrel, majd egy ezeken alapuló szitarendszert dolgozunk ki. Az ötödik fejezet eredményeit az [51] dolgozat tartalmazza.

Bibliography

[1] B. U. Alfred, *On square Lucas numbers*, Fib. Quarterly **2** (1964), 11–12.

[2] E. T. Avanesov, *Solution of a problem on figurate numbers*, Acta Arith. **12** (1966/1967), 409–420.

[3] E. T. Avanesov, *The Diophantine equation* $3y(y+1) = x(x+1)(2x+1)$, Volz. Mat. Sb. Vyp. **8** (1971), 3–6.

[4] A. Baker, *The Diophantine equation* $y^2 = ax^3 + bx^2 + cx + d$, J. London Math. Soc. **43** (1968), 1–9.

[5] A. Baker, H. Davenport, *The equations* $3x^2 - 2 = y^2$ *and* $8x^2 - 7 = z^2$, Quart. J. Math. Oxford **20** (1969), 129–137.

[6] A. I. Barvinok, *A polynomial time algorithm for counting integral points in polyhedra when the dimension is fixed*, in 34th Annual Symposium of Foundations of Computer Science, pp. 566–572, IEEE, Nov. 1993.

[7] A. Behera, G. K. Panda, *On the square roots of triangular numbers*, Fibonacci Quart. **37** (1999), 98–105.

[8] M. A. Bennett, *Rational approximation to algebraic numbers of small height: the Diophantine equation* $|ax^n - by^n| = 1$, J. Reine Angew. Math. **535** (2001), 1–49.

[9] M. A. Bennett, *Products of consecutive integers*, Bull. London Math. Soc. **36** (2004), 683–694.

[10] M. A Bennett, N. Bruin, K. Győry and L. Hajdu, *Powers from products of consecutive terms in arithmetic progression*, Proc. London Math. Soc. **92** (2006), 273–306.

[11] M. A. Bennett, K. Győry, M. Mignotte, Á. Pintér, *Binomial Thue equations and polynomial powers*, Compositio Math. **142** (2006), 1103–1121.

[12] M. A. Bennett and C. Skinner, *Ternary Diophantine equations via Galois representations and modular forms*, Canad. J. Math. **56** (2004) 23-54.

[13] M. A. Bennett, V. Vatsal and S. Yazdani, *Ternary Diophantine equations of signature* $(p, p, 3)$, Compositio Math. **140** (2004), 1399–1416.

[14] A. Bérczes, K. Liptai, I. Pink, *On generalized balancing sequences*, Fibonacci Quart. **48** (2010), 121–128.

[15] F. Beukers, T. N. Shorey, R. Tijdeman, *Irreducibility of polynomials and arithmetic progressions with equal product of terms*, In: K. Győry, H. Iwaniec, J. Urbanowicz, eds., Number Theory in Progress: Proc. Int. Conf. in Number Theory in Honor of A. Schinzel, Zakopane, 1997, W. de Gruyter, 1999, pp. 11–26.

[16] Y. F. Bilu, B. Brindza, P. Kirschenhofer, Á. Pintér, R. F. Tichy, *Diophantine equations and Bernoulli ploynomials* Composotio Math. **131** (2002), 173–188.

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

[18] D. W. Boyd, H. H. Kisilevsky, *The diophantine equation* $u(u+1)(u+2)(u+3) = v(v+1)(v+2)$, Pacific J. Math. **40** (1972), 23–32.

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

[20] B. Brindza, Á. Pintér, *On equal values of power sums*, Acta Arith. **77** (1996), 97–101.

[21] B. Brindza, Á. Pintér, *On the irreducibility of some polynomials in two variables*, Acta Arith. **82** (1997), 303–307.

[22] N. Bruin, *Chabauty methods and covering techniques applied to generalized Fermat equations*, CWI Tract, Stichting Mathematisch Centrum, Centrum voor Wiskunde en Informatica, Amsterdam, 133, 2002.

[23] N. Bruin, *Chabauty methods using elliptic curves*, J. Reine Angew. Math. **562** (2003), 27–49.

[24] N. Bruin, *Some ternary Diophantine equations of signature* $(n, n, 2)$, In: Discovering mathematics with Magma, Algorithms Comput. Math. **19** (2006), 63–91.

[25] N. Bruin, K. Győry, L. Hajdu, Sz. Tengely, *Arithmetic progressions consisting of unlike powers*, Indag. Math. **17** (2006), 539–555.

[26] N. Bruin, M. Stoll *Two-cover descent on hyperelliptic curves*, Math. Comp. **78** (2009), 2347–2370.

[27] Y. Bugeaud, *Bounds for the solutions of superelliptic equations*, Compositio Math. **107** (1997), 187–219.

[28] Y. Bugeaud, M. Mignotte, S. Siksek, *Classical and modular approaches to exponential Diophantine equations. I. Fibonacci and Lucas perfect powers.*, Ann. Math. (2) **163** (2006), 969–1018.

[29] J. H. E. Cohn, *Square Fibonacci numbers, Etc.*, Fibonacci Quart. **2** (1964), 109–113.

[30] J. H. E. Cohn, *On square Fibonacci numbers*, J. London Math. Soc. **39** (1964), 537–540.

[31] J. H. E. Cohn, *Lucas and Fibonacci numbers and some Diophantine equations*, Proc. Glasgow Math. Assoc. **7** (1965), 24–28.

[32] J. H. E. Cohn, *Perfect Pell powers*, Glasgow Math. J. **38** (1996), 19–20.

[33] I. Connell, *Addendum to a paper of Harada and Lang*, J. Algebra **145** (1992), 463–467.

[34] J. E. Cremona, M. Prickett, S. Siksek, *Height Difference Bounds For Elliptic Curves over Number Fields*, J. Number Theory **116** (2006), 42–68.

[35] H. Darmon and L. Merel, *Winding quotients and some variants of Fermat's Last Theorem*, J. Reine Angew. Math. **490** (1997), 81–100.

[36] S. David, *Minorations de formes linéaires de logarithmes elliptiques*, Soc. Math. France, Mémoire 62 (Suppl. Bull. S. M. F.) 123, 1995, pp. 143.

[37] L. E. Dickson, *History of the theory of numbers. Vol. II: Diophantine analysis*, Chelsea Publishing Co., New York, 1966.

[38] P. Erdős and J. L. Selfridge, *The product of consecutive integers is never a power*, Illinois J. Math. **19** (1975), 292-301.

[39] R. P. Finkelstein, *The House Problem*, American Math. Monthly **72** (1965), 1082–1088.

[40] E. V. Flynn, *A flexible method for applying Chabauty's theorem*, Compositio Math. **105** (1997), 79–94.

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

[42] A. Grytczuk, A. Schinzel, *On Runge's theorem about Diophantine equations*, Sets, graphs and numbers, North Holland, 1992, Colloq. Math. Soc. János Bolyai **60** (1992), 329–356.

[43] R. K. Guy, *Unsolved Problems in Number Theory*, Springer, New York, 3rd edition, 2004, pp. XVIII+437.

[44] K. Győry, *On the diophantine equation* $n(n+1)\dots(n+k-1) = bx^l$, Acta Arith. **83** (1998), 87–92.

[45] K. Győry, *Power values of products of consecutive integers and binomial coefficients*, Number Theory and Its Applications, Kluwer Acad. Publ. 1999, 145–156.

[46] K. Győry, L. Hajdu and N. Saradha, *On the Diophantine equation* $n(n+d)\dots(n+(k-1)d) = by^l$, Canad. Math. Bull. **47** (2004), 373-388. Correction: Canad. Math. Bull. **48** (2005), 636.

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

[48] L. Hajdu, *Powerful arithmetic progressions*, Indag. Math. **19** (2008), 547–561.

[49] L. Hajdu, T. Herendi, *Explicit bounds for the solutions of elliptic equations with rational coefficients*, J. Symbolic Comput. **25** (1998), 361–366.

[50] L. Hajdu, T. Kovács, *Parallel LLL reduction for bounding the integral solutions of elliptic equations*, Math. Comp. **78** (2009), 1201–1210.

[51] L. Hajdu, T. Kovács, *Almost fifth powers in arithmetic progression*, J. Number Theory **131** (2011), 1912–1923.

[52] L. Hajdu, Á. Pintér, *Combinatorial diophantine equations*, Publ. Math. Debrecen **56** (2000), 391–403.

[53] L. Hajdu, Sz. Tengely, *Arithmetic progressions of squares, cubes and n-th powers*, J. Functiones et Approximatio **41** (2009), 129–138.

[54] L. Hajdu, Sz. Tengely and R. Tijdeman, *Cubes in products of terms in arithmetic progression*, Publ. Math. Debrecen **74** (2009), 215–232.

[55] K. Harada, M. L. Lang, *Some elliptic curves arising from the Leech lattice*, J. Algebra **125** (1989), 298–310.

[56] E. Herrmann, *Bestimmung aller ganzzahligen Lsungen quartischer elliptischer diophantischer Gleichungen unter Verwendung von Linearformen in elliptischen Logarithmen*, Diploma Thesis, 1998.

[57] N. Hirata-Kohno, S. Laishram, T. Shorey and R. Tijdeman, *An extension of a theorem of Euler*, Acta Arith. **129** (2007), 71–102.

[58] T. Kovács, *Combinatorial Diophantine equations - the genus 1 case*, Publ. Math. Debrecen **72** (2008) 243–255.

[59] T. Kovács, *Combinatorial numbers in binary recurrences*, Period. Math. Hungar. **58** (2009) 83–98.

[60] T. Kovács, K. Liptai, P. Olajos, *On $(a, b)-$balancing numbers*, Publ. Math. Debrecen **77** (2010) 485–498.

[61] S. Lang, *Diophantine Geometry*, Interscience, New York, 1962.

[62] K. Liptai, *Fibonacci balancing numbers*, Fibonacci Quart. **42** (2004), 330–340.

[63] K. Liptai, *Lucas balancing numbers*, Acta Math. Univ. Ostrav. **14** (2006), 43–47.

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

[65] J. A. De Loera, D. Haws, R. Hemmecke, P. Huggins, J. Tauzer, R. Yoshida, *A user's guide for LattE v1.1*, Nov. 2003.

[66] R. A. MacLeod, I. Barrodale, *On equal products of consecutive integers*, Canad. Math. Bulletin **13** (1970), 255–259.

[67] D. Masser, *Polynomial bound for Diophantine equations*, Amer. Math. Monthly **93** (1980), 486–488.

[68] W. L. McDaniel, *Triangular numbers in the Pell sequence*, Fibonacci Quart. **34** (1996), 105–107.

[69] L. Ming, *On triangular Fibonacci numbers*, Fibonacci Quart. **27** (1989), 98–108.

[70] L. Ming, *On triangular Lucas numbers*, Applications of Fibonacci numbers **4** (1991), 231–240.

[71] L. J. Mordell, *On the integer solutions of* $y(y+1) = x(x+1)(x+2)$, Pacific J. Math. **13** (1963), 1347–1351.

[72] L. J. Mordell, *Diophantine Equations*, Academic Press, London, 1969, pp. X+312.

[73] L. Moser, L. Carlitz, *Problem H-2*, Fibonacci Quart. **1** (1963), 46.

[74] I. Nemes, A. Pethő, *Polynomial values in linear recurrences II*, J. Number Theory **24** (1986), 47–53.

[75] R. Obláth, *Über das Produkt fünf aufeinander folgender Zahlen in einer arithmetischen Reiche*, Publ. Math. Debrecen **1** (1950), 222–226.

[76] R. Obláth, *Eine Bemerkung über Produkte aufeinander folgender Zahlen*, J. Indian Math. Soc. **15** (1951), 135–139.

[77] C. S. Ogilvy, *Tomorrow's math, unsolved problems for the amateur*, Oxford Univ. Press, 1962, p.100.

[78] A. Pethő, *On the Solution of the Equation* $G_n = P(x)$, in Fibonacci Numbers and Their Applications, D. Reidel Publ. Comp., 1986, 193–201.

[79] A. Pethő, *Diofantoszi egyenletek effektív és explicit megoldása* (in Hungarian), Academic doctoral dissertation, Hungarian Academy of Sciences, 1990, 114 pp.

[80] A. Pethő, *The Pell sequence contains only trivial perfect powers*, Sets, graphs and numbers, North Holland, 1992, Colloq. Math. Soc. János Bolyai **60** (1992), 561–568.

[81] Y. Ping-Zhi, *On a special diophantine equation* $a\binom{x}{n} = by^r + c$, Publ. Math. Debrecen **44** (1994), 137–143.

[82] Á. Pintér, *The diophantine equation* $\binom{x}{2} = y(y+1)(y+2)(y+3)$, unpublished manuscript.

[83] Á. Pintér, *A note on the Diophantine equation* $\binom{x}{4} = \binom{y}{2}$, Publ. Math. Debrecen **47** (1995), 411–415.

[84] Á. Pintér, *On the magnitude of integer points on elliptic curves*, Bull. Austral. Math. Soc. **52** (1995), 195–199.

[85] Á. Pintér, Cs. Rakaczki, *On the zeros of shifted Bernoulli polynomials*, Appl. Math. Comput. **187** (2007), 379–383.

[86] Á. Pintér, B. M. M. de Weger, $210 = 14 \times 15 = 5 \times 6 \times 7 = \binom{21}{2} = \binom{10}{4}$, Publ. Math. Debrecen **51** (1997), 175–189.

[87] H. Rademacher, *Topics in analytic number theory*, Die Grundlehren der math. Wissenschaften, Band 169, Springer-Verlag, Berlin, 1973, ix+320 pp.

[88] Cs. Rakaczki, *Binomial coefficients in arithmetic progressions*, Publ. Math. Debrecen **57** (2000), 547–558.

[89] Cs. Rakaczki, *On the Diophantine equation* $F(\binom{x}{n}) = b\binom{y}{m}$, Period. Math. Hungar. **49** (2004), 119–132.

[90] Cs. Rakaczki, *On some Diophantine results related to Euler polynomials*, Period. Math. Hungar. **56** (2008), 247–257.

[91] K. Ribet, *On the equation* $a^p + 2^\alpha b^p + c^p = 0$, Acta Arith. **79** (1997), 7–16.

[92] A. P. Rollett, *Problem 5080*, Amer. Math. Monthly, **70** (1963), 216.

[93] C. Runge, *Über ganzzalige Lösungen von Gleichungen zwischen zwei Veränderlichen*, J. Reine Angew. Math. **100** (1887), 425–435.

[94] N. Saradha, *On perfect powers in products with terms from arithmetic progressions*, Acta Arith. **82** (1997), 147–172.

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

[96] T. N. Shorey, *Powers in arithmetic progression*, in: A Panorama in Number Theory (G. Wüstholz, ed.), Cambridge University Press, Cambridge, 2002, 325-336.

[97] T. N. Shorey, *Powers in arithmetic progression (II)*, in: New Aspects of Analytic Number Theory, Kyoto 2002, 202–214.

[98] T. N. Shorey, S. Laishram, Sz. Tengely, *Squares in products in arithmetic progression with at most one term omitted and common difference a prime power*, Acta Arith. **135** (2008), 143–158.

[99] T. N. Shorey, R. Tijdeman, *Exponential diophantine equation*, Cambridge University Press, 1986, pp. X+280.

[100] C. L. Siegel, *Über einige Anwendungen Diophantischer Approximationen*, Abh. Preuss. Akad. Wiss. Phys. Math. Kl. (1929), 1–41. Reprinted as pp. 209-266 of his Gesammelte Abhandlungen I, Springer, Berlin, 1966.

[101] J. H. Silverman, J. Tate, *Rational Points on Elliptic Curves*, Springer-Verlag, New York, 1992, pp. X+281.

[102] V. G. Sprindžuk, *Classical Diophantine Equations*, Lecture Notes in Mathematics 1559, Springer-Verlag, Germany, 1993.

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

[104] R. J. Stroeker, N. Tzanakis, *On the Elliptic Logarithm Method for Elliptic Diophantine Equations: Reflections and an Improvement*, Experimental Math. **8** (1999), 135–149.

[105] R. J. Stroeker, N. Tzanakis, *Computing all integer solutions of a genus 1 equation*, Math. Comp. **72** (2003), 1935–1946.

[106] R. J. Stroeker, B. M. M. de Weger, *Solving elliptic diophantine equations: the general cubic case*, Acta Arith. **87** (1999), 339–365.

[107] R. J. Stroeker, B. M. M. de Weger, *Elliptic binomial diophantine equations*, Math. Comp. **68** (1999), 1257–1281.

[108] L. Szalay, *Some polynomial values in binary recurrences*, Revista Colombiana de Matemáticas **35** (2001), 99–106.

[109] L. Szalay, *On the resolution of the equation* $U_n = \binom{x}{3}$ *and* $V_n = \binom{x}{3}$, Fibonacci Quart. **40** (2002), 9–12.

[110] L. Szalay, *Superelliptic equations of the form* $y^p = x^{kp} + a_{kp-1}x^{kp-1} + \cdots + a_0$, Bull. Greek Math. Soc. **46** (2002), 23–33.

[111] L. Szalay, *On the resolution of simultaneous Pell equations*, Ann. Math. Info. **34** (2007), 77–87.

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

[113] Sz. Tengely, *Note on the paper "An extension of a theorem of Euler" by Hirata-Kohno et al.*, Acta Arith. **134** (2008), 329–335.

[114] Sz. Tengely, *Finding g-gonal numbers in recurrence sequences*, Fibonacci Quart. **46/47** (2009), 235–240.

[115] Sz. Tengely, *On the Diophantine equation* $L_n = \binom{x}{5}$, submitted.

[116] R. Tijdeman, *Diophantine equations and diophantine approximations*, in: Number Theory and Applications, Kluwer Acad. Press, 1989, 215-243.

[117] N. Tzanakis, *Solving Elliptic Diophantine Equations by estimating Linear Forms in Elliptic Logarithms. The case of Quartic Equations*, Acta Arith. **75** (1996), 165–190.

[118] N. Tzanakis, B. M. M. de Weger, *On the practical solution of the Thue equation*, J. Number Theory **31** (1989), 99–132.

[119] S. Uchiyama, *Solution of a Diophantine problem*, Tsukuba J. Math. **8** (1984), 131–157.

[120] B. M. M. de Weger, *Algorithms for diophantine equations*, CWI Tract 65, Stichting Mathematisch Centrum, Amsterdam, 1989.

[121] B. M. M. de Weger, *A binomial Diophantine equation*, Quart. J. Math. Oxford Ser. (2) **47** (1996), 221–231.

[122] B. M. M. de Weger, *Equal binomial coefficients: some elementary considerations*, J. Number Theory **63** (1997), 373–386.

[123] P. G. Walsh, *A quantitative version of Runge's theorem on Diophantine equations*, Acta Arith. **62** (1992), 157–172.

[124] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Ann. Math. **141** (1995), 443–551.

[125] O. Wyler, *In the Fibonacci series* $F_1 = 1, F_2 = 1, F_{n+1} = F_n + F_{n-1}$ *the first, second and twelfth terms are squares*, Amer. Math. Monthly **71** (1964), 221–222.

Appendix A

List of papers of the author

1. T. Kovács, *Combinatorial Diophantine equations - the genus 1 case*, Publ. Math. Debrecen **72** (2008), 243–255.

2. L. Hajdu, T. Kovács, *Parallel LLL-reduction for bounding the integral solutions of elliptic equations*, Math. Comp. **78** (2009), 1201–1210.

3. T. Kovács, *Combinatorial numbers in binary recurrences*, Periodica Mathematica Hungarica, **58** (2009), 83–98.

4. T. Kovács, K. Liptai, P. Olajos, *On (a,b)-balancing numbers*, Publ. Math. Debrecen **77** (2010), 485–498.

5. L. Hajdu, T. Kovács, *Almost fifth powers in arithmetic progression*, J. Number Theory **131** (2011), 1912–1923.

6. L. Aszalós, N. Bátfai, L. Csirmaz, J. Folláth, E. Hajdúné Pocsai, T. Herendi, T. Kovács, Z. Matolcsy, A. Pethő, P. Varga, *Secure utilization of local and regional data assets through mobile environments*, to appear in Conference Proceedings for ICAI 2010 - 8th International Conference on Applied Informatics.

Appendix B

List of conference talks of the author

1. *Kombinatorikus diofantikus egyenletek*, Berekfürdői Diofantikus és Kriptográfiai Napok, 22 April 2006, Berekfürdő.

2. *Combinatorial Diophantine equations - the genus 1 case*, 18th Czech and Slovak International Conference on Number Theory, 28 August 2007, Smolenice (Slovakia).

3. *Kombinatorikus számok rekurzív sorozatokban*, Soproni Diofantikus és Kriptográfiai Napok, 11 October 2008, Sopron.

4. *Parallel LLL-reduction for elliptic Diophantine equations*, Winter School on Explicit Methods in Number Theory, 28 Januar 2009, Debrecen.

5. *Combinatorial numbers in binary recurrences*, XXVImes Journées Arithmétiques, 7 July 2009, Saint-Étienne (France).

6. *Elliptikus, 1 és 2 génuszú görbék*, Számelméleti szeminárium, 18 March 2010, Eger.

7. *On (a, b)-balancing numbers*, ALANT Joint conferences on Algebra, Logic and Number Theory, 22 June 2010, Bukowina Tatrzańska (Poland).

8. *Almost fifth powers in arithmetic progression*, Number Theory and its Applications, An international conference dedicated to Kálmán Győry, Attila Pethő, János Pintz and András Sárközy, 5 October 2010, Debrecen.