1949

EXPONENTIAL DIOPHANTINE EQUATIONS AND REPRESENTATION PROBLEMS

Egyetemi doktori (PhD) értekezés

Bertók Csanád

Témavezető: Dr. Hajdu Lajos
egyetemi tanár

DEBRECENI EGYETEM
Természettudományi és Informatikai Doktori Tanács
Matematika– és Számítástudományok Doktori Iskola
Debrecen, 2019.

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

Nyilatkozom arról, hogy a tézisekben leírt eredmények nem képezik más PhD disszertáció részét.

Debrecen, 2019. február 26. .....

A jelölt aláírása

Tanúsítom, hogy Bertók Csanád doktorjelölt 2014–2017 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.

Nyilatkozom továbbá arról, hogy a tézisekben leírt eredmények nem képezik más PhD disszertáció részét.

Az értekezés elfogadását javasolom.

Debrecen, 2019. február 26. .....

A témavezető aláírása

EXPONENTIAL DIOPHANTINE EQUATIONS AND REPRESENTATION PROBLEMS

Értekezés a doktori (Ph.D.) fokozat megszerzése érdekében a
Matematika– és Számítástudományok tudományágban

Írta: Bertók Csanád okleveles matematikus

Készült a Debreceni Egyetem Matematika– és Számítástudományok
Doktori Iskolája Diofantikus és Konstruktív Számelmélet
programjának keretében

Témavezető: Dr. Hajdu Lajos

A doktori szigorlati bizottság:

elnök:	Dr. Páles Zsolt
tagok:	Dr. Gyarmati Katalin
	Dr. Bérczes Attila

A doktori szigorlat időpontja: 2017.10.16.

Az értekezés bírálói:

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

A bírálóbizottság:

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

Az értekezés védésének várható időpontja: 2019.

Acknowledgements

The completion of this dissertation would not have been possible without the support of my family and colleagues.

First of all I am exceedingly grateful to my supervisor Professor Lajos Hajdu for introducing me to the "world of mathematicians". His enthusiasm towards mathematical research really inspired me.

I am also indebted to my mother Katalin and to my bride Tünde who supported and encouraged me during this stressful, but also wonderful period of my life.

I would also like to express my gratitude towards everybody at the Department of Algebra and Number Theory, especially to Professor Kálmán Győry for helping me during this long journey.

Last but not least I am grateful to my new colleagues at the Department of Computer Science, especially to Professor Attila Pethő whom I owe a lot.

Nagyapám emlékére, akit soha nem feledek.

In loving memory of my grandfather, whom I will never forget.

Tartalomjegyzék

1. Introduction **1**

2 Representation problems **8**

2.1 Representing integers as sums of general power products . . . 8

2.1.1 New results . . . 9

2.1.2 Lemmas . . . 11

2.1.3 Proofs . . . 15

2.2 Multi-base representations . . . 21

2.2.1 New results . . . 22

2.2.2 Lemmas . . . 24

2.2.3 Proofs . . . 25

2.3 Representation of terms of binary recurrence sequences as linear combinations of prime powers . . . 35

2.3.1 New results . . . 36

2.3.2 Proofs . . . 39

3 Exponential Diophantine equations **43**

3.1 Exponential Diophantine equations over $\mathbb{Z}$ . . . 43

3.1.1 New results . . . 45

3.1.2 An algorithm for solving exponential Diophantine equations . . . 46

3.1.3 Proofs . . . 51

3.2 Exponential Diophantine equations over number fields . . . 65

3.2.1 New results . . . 68

3.2.2 Lemmas . . . 69

3.2.3 Proofs . . . 72

3.2.4 An algorithm for solving exponential Diophantine equations over number fields 73

4 Applications **78**

4.1 A complete solution of a conjecture of Terai 78

4.2 Representing terms of binary recurrence sequences as sums of powers 84

4.3 A problem concerning balancing numbers 92

4.4 Multi-base representations 95

References **99**

Bertók Csanád publikációs jegyzéke **108**

5 Összefoglaló **110**

6. Summary **117**

1. Introduction

In this dissertation, we consider representation problems of integers as expressions involving exponential terms. We also give algorithms which can be used to solve exponential Diophantine equations over $\mathbb{Z}$ and rings of integers of number fields. As applications, by using our method we solve some Diophantine problems, too.

First, we consider representation problems. Let $a_1, \ldots, a_l$ be distinct positive integers and put $A = \{a_1, \ldots, a_l\}$. Consider the set

$$A' := \{a_1^{x_1} \cdot \ldots \cdot a_l^{x_l} | x_1, \ldots, x_l \text{ are non-negative integers}\}.$$

A natural question to ask is that at least how many elements do we need from A' to represent a given positive integer as their sum? If A consists of only one number b then the question basically asks about the representation of positive integers in the base b number system. If A consists of two primes, then we have a so-called "double base" representation problem (as a related paper, see e.g. the work of Dimitrov and Howe [25]). If we define the function $F(k)$ $(k \in \mathbb{N})$ to be the smallest natural number which cannot be represented as the sum of less than k terms from A', and $F_{\pm}(k)$ to be the function defined similarly, except that A' is replaced by $A'_{\pm} = A' \cup (-A')$ and ask about the properties of $F(k)$ and $F_{\pm}(k)$, then we get a similar problem proposed by Nathanson [56]. If for example $A = \{2\}$, then $F(4) = 15$, since $15 = 2^3 + 2^2 + 2^1 + 2^0$, thus we need at least 4 elements from A' to represent 15. The problem however is not trivial if A consists of more than one number. In the case when A consists of primes, Hajdu and Tijdeman [38, 39] gave upper bounds for the function $F(k)$ and $F_{\pm}(k)$.

In this dissertation, we give a lower and upper bound for $F(k)$ and $F_{\pm}(k)$

in the case, where A consists of arbitrary integers. These results answer a question of Nathanson [56] in the above setting, and extend the mentioned results of Hajdu and Tijdeman. These bounds are relatively sharp, as well. The corresponding results are given in Section 2.1.

Another related topic is the analysis of integers which have only "few" non-zero digits in a special number system (see e.g. papers by Erdős, Mauduit, Pomerance, Sárközy [26, 27, 52, 53, 54] and the references there). On the other hand, if a number n has to hold certain other arithmetical property, it may happen that it must have "many" digits. This is the case when n belongs to some recurrence sequence; see e.g. Bugeaud, Cipu and Mignotte [21], Luca [48] and Stewart [78] for effective results in this direction. In Section 2.2 we consider multi-base representations. Senge and Straus [71] proved that the number of those integers, whose number of non-zero digits in two different bases b_1 and b_2 with $\log b_1 / \log b_2 \notin \mathbb{Q}$ remains under some fixed bound, is finite. Later, Stewart [78] gave a more precise, effective version of this result (for an extension to the case of several number systems, see Schlikewei [69], and for number systems based on recurrence sequences see the papers of Pethő and Tichy [61, 62]). In this subsection we go one step further and study representations of integers which have only a "few" non-zero digits in different multi-base representations simultaneously. For this, let S be a finite set of primes, and write $\mathbb{Z}_S$ (resp. $\mathbb{Z}_S^+$) for the set of integers (resp. positive integers) having no prime divisors outside S. We consider the representations of integers n of the form

$$n = u_1 + \cdots + u_t$$

with $u_1, \dots u_t \in \mathbb{Z}_S$. We write $w_S(n)$ for the minimal t for which the above equation holds. If n is positive and the numbers on the right hand side are elements of $\mathbb{Z}_S^+$, we write $w_S^+(n)$ instead. In Section 2.2 we prove effective and

ineffective results regarding $w_S(n)$ and $w_S^+(n)$. To prove those theorems, we need deep tools, including Baker's method and the quantitative subspace theorem.

In Section 2.3 we consider the problem of representation of terms of binary recurrence sequences as linear combinations of powers. Marques and Togbé [50] determined all Fibonacci and Lucas numbers which can be written as the sum of powers of $2, 3, 5$ under certain assumptions. Pethő and de Weger [59] gave an algorithm which can be used to solve the Diophantine equation $U_n = wp_1^{x_1} \cdot \ldots \cdot p_m^{x_m}$, where U_n is a binary recurrence sequence with positive discriminant. Pethő [58] and Shorey and Stewart [72] independently proved that under certain natural assumptions, a linear recurrence sequence may contain only finitely many perfect powers. In the case of some special, famous sequences all perfect powers have been determined. In the case of the Pell sequence P_n, Pethő [60] proved that it does not contain non-trivial powers. Bugeaud, Mignotte and Siksek [22] proved that the Fibonacci-sequence F_n contains only the powers $0, 1, 8, 144$, and the only powers in the sequence of Lucas numbers L_n are $1, 4$. Results of Pethő and Tichy [62] imply that there are only finitely many Fibonacci numbers of the form $p^x + p^y + p^z$, where p is a fixed prime. Kovács [42] found all combinatorial numbers of certain shapes among the terms of F_n, L_n, P_n and Q_n (the associated Pell-sequence). We give a general finiteness result for the solutions of the equation

$$U_n = b_1 p_1^{x_1} + \cdots + b_s p_s^{x_s}$$

in non-negative integers $x_1, \ldots, x_s$. In our proofs we use Baker's method (more precisely we use a theorem due to Matveev [51]).

In Chapter 3 we consider exponential Diophantine equations of the form

$$a_1 b_{11}^{x_{11}} \dots b_{1\ell}^{x_{1\ell}} + \dots + a_k b_{k1}^{x_{k1}} \dots b_{k\ell}^{x_{k\ell}} = c \qquad \text{(A)}$$

in non-negative integers $x_{11}, \dots, x_{1\ell}, \dots, x_{k1}, \dots, x_{k\ell}$, where the coefficients, bases and the right hand side are given non-negative integers. This equation has a very rich literature. If $k = 2$ then using Baker's method one can give explicit upper bounds for the exponents. (This follows from results of Győry [35, 36]. This result has lots of extensions, see e.g. the books [73] and [32], and the references given there.) If $k = 3, 4$ then under some restrictive assumptions, the solutions can still be determined (see results of Vojta [86] and Bennett [8]). However, in general, for $k \geq 3$, the problem becomes significantly more difficult. In this case the method of Baker fails and we need to use the subspace theorem, which is ineffective, and is capable only to provide a bound for the number of non-degenerate solutions. Here we refer to Evertse [29], and again to the book of Evertse and Győry [32] and the references given there. It is important to note that there is no known algorithm in the literature, which would be capable to produce all the solutions of such an equation. In Chapter 3 we give a heuristic algorithm, based upon exponential congruences for the solutions of such equations. As a starting point, we consider the congruences

$$a_1 b_{11}^{x_{11}} \dots b_{1\ell}^{x_{1\ell}} + \dots + a_k b_{k1}^{x_{k1}} \dots b_{k\ell}^{x_{k\ell}} \equiv c \pmod{m} \qquad \text{(B)}$$

with some $m \in \mathbb{Z}$. It is easy to see that if for some m we have no solutions, then we can immediately say that (A) also has no solutions. However, the reverse statement is not at all obvious. Namely, what happens if we know that congruence (B) has a solution for every possible moduli? If we consider

a polynomial Diophantine equation, then it is possible to have no solutions despite of the fact that the corresponding congruence has solutions for every modulus m. The most famous example is due to Selmer [70]. Consider the equation

$$3X^3 + 4Y^3 + 5Z^3 = 0$$

in $X, Y, Z \in \mathbb{Z}$. Selmer proved that although this equation has non-trivial solutions modulo m for all $m \geq 2$, it has no non-trivial solutions in $\mathbb{Z}$.

This problem is related to the so-called Hasse-principle, which states that if a Diophantine equation has no solutions at all then there exists a modulus m such that the corresponding congruence has no solutions modulo m. As one can see from the example above, this principle is false if we consider polynomial Diophantine equations. However, for equations of the type (A) it is believed that the Hasse-principle is true; it is sufficient to think of a famous conjecture of Skolem [75]. There are several results in the literature regarding this conjecture. One of the most important is due to Schinzel [66], who proved that if $k = 1$ then this conjecture is true.

In Section 3.1 we prove a slightly modified version of this conjecture, and provide some support that it should hold. We prove that if we fix the bases and coefficients in (A) and

$$H = \{c \in \mathbb{Z} \ : \ \text{(A) is not solvable, but (B) is solvable for all } m\},$$

then H has density zero inside the set

$$H_0 = \{c \in \mathbb{Z} \ : \ \text{(A) is not solvable}\}.$$

Moreover, based upon this conjecture, we present an algorithm which can be

used to find every solution of a given exponential Diophantine equation, provided it has only finitely many solutions. We give several concrete examples, as well.

In Section 3.2 we consider a similar problem as in Section 3.1 with the difference that instead of working in $\mathbb{Z}$, now we work in the ring of integers of an arbitrary algebraic number field. We present several theorems considering the exponential Hasse-principle in this number field case and provide an extended algorithm which can be used to find the solutions of these types of equations. Finally, we also give some numerical examples which demonstrate the usability of our algorithm.

In Chapter 4 we present some applications of the theorems and methods from the previous chapters. In Section 4.1 we prove a classical conjecture of Terai regarding the solutions of the equation

$$(4t^2+1)^x + (5t^2-1)^y = (3t)^z,$$

where t is an arbitrary but fixed positive integer and x, y, z are unknown positive integers. In Section 4.2 we concentrate on the equations

$$U_n = 2^x + 3^y \quad \text{and} \quad U_n = 2^x + 3^y + 5^z,$$

where U_n is the n-th term of one of the Fibonacci-, Lucas-, Pell- or associated Pell-sequence and x, y, z are unknown non-negative integers. In particular, we extend a result of Marques and Togbé [50], and solve a problem of Sanches amd Luca [65]. In Section 4.3 we turn to a related problem, namely we solve the equation

$$B_u + B_v + B_w = b^z$$

in non-negative integers u, v, w, z where B_i is the i-th balancing number and

$b \in \{2, 3, 5, 7\}$.

Finally in Section 4.4 we discuss applications regarding multi-base representations. Namely, let S_1 and S_2 be disjoint non-empty sets of primes with $S_1 \cup S_2 = \{2, 3, 5\}$ and let $w_S^+(n)$ be defined as before. In this section we give all solutions to the inequality

$$w_{S_1}^+(n) + w_{S_2}^+(n) \leq 4.$$

The results of this dissertation are published in the papers [9, 10, 12, 13, 14, 16]. As one can see, the main theme of our theorems is exponential equations and representation problems related to exponential expressions. We note that we have several other results: in [17] we obtain van der Waerden type theorems for linear recurrence sequences; in [18] we consider the problem of simultaneous approximation of linear forms in number fields by using the LLL algorithm; in [15] we provide results concerning the distribution of polynomials with bounded height; in [11] we prove theorems regarding exceptional units in number fields. However, to keep the presentation coherent, these results are not included in this dissertation.

2 Representation problems

In this chapter of the dissertation we prove some theoretical results regarding various representation problems, including problems concerning the representation of integers as power products, multi-base representations and representation of terms of recurrence sequences as linear combinations of pure powers.

2.1 Representing integers as sums of general power products

Let $a_1, \ldots, a_l$ be distinct positive integers and put $A = \{a_1, \ldots, a_l\}$. Let A' be the set of products of powers of elements from A, that is

$$A' := \{a_1^{m_1} \cdot \ldots \cdot a_l^{m_l} \mid m_1, \ldots, m_l \text{ are non-negative integers}\}$$

and let $A'_{\pm} = A' \cup (-A')$. Let $F(k)$ $(k \in \mathbb{N})$ be defined as the smallest natural number which cannot be represented as the sum of less than k terms from A'. We define $F_{\pm}(k)$ similarly as $F(k)$ except that we replace the set A' with $A'_{\pm}$.

Nathanson in Problem 2 of [56] asked for the growth properties of $F_{\pm}(k)$, in the particular case when the elements a_i $(i = 1, \ldots, l)$ of A are primes. Hajdu and Tijdeman [38, 39] proved several related theorems, both for $F(k)$ and $F_{\pm}(k)$. More precisely , they proved that for all $k > 1$

$$k^{C_0^* k} < F(k) < C_1^* (kl)^{(1+\varepsilon^*)kl} \text{ and } k^{C_0^* k} < F_{\pm}(k) < \exp((kl)^{C_2^*}) \quad (2.1)$$

hold, where C_0^* and C_2^* are positive absolute constants, $\varepsilon^* > 0$ is arbitrary, and C_1^* is a positive constant depending only on ε^*.

In this section we consider the general case, where the elements a_i $(i = 1, \ldots, l)$ of A are arbitrary positive integers. It is important to note that it seems

to be more natural to consider the problem under this condition. On the one hand, this is the case e.g. in [1] and [37]. On the other hand, since a part of the argument goes modulo m (with some appropriate m), the extra assumption that the numbers a_i $(i = 1, \ldots, l)$ should be primes is irrelevant at many points. To prove our results, among other things we need to extend classical results of Tijdeman [84, 85] concerning the gaps in A' where the a_i are primes, to the case of arbitrary positive integers a_i $(i = 1, \ldots, l)$.

Now we state the main results of this section. Since we use a handful of lemmas, we give them in a separate subsection (with the exception of Lemma 2.1 since this result is connected to Theorem 2.3). Then we present the proofs of these theorems.

2.1.1 New results

As usual, we call the positive integers $n_1, n_2, \ldots, n_t$ multiplicatively independent, if

$$n_1^{\alpha_1} \cdot n_2^{\alpha_2} \cdot \ldots \cdot n_t^{\alpha_t} = 1 \ \ (\alpha_1, \ldots, \alpha_t \in \mathbb{Z})$$

occurs only when $\alpha_1 = \alpha_2 = \ldots = \alpha_t = 0$.

The first result concerns the non-degenerate case, where A contains a pair of multiplicatively independent elements. This is Theorem 2.1 in Bertók [9].

Theorem 2.1. *Let $A, A', A'_{\pm}, F(k)$ and $F_{\pm}(k)$ be as above and suppose that A has two multiplicatively independent elements. Then for every $k > 1$ we have:*

i) $F(k) > k^{C_1 k}$*, where C_1 is a constant depending only on A,*

ii) $F(k) < C_2(kl)^{(1+\varepsilon)kl}$ *for every $\varepsilon > 0$, where C_2 is a constant depending only on ε,*

iii) $F_{\pm}(k) < \exp((kl)^{C_3})$, *where* C_3 *is an absolute constant.*

Noting that $F_{\pm}(k) \geq F(k)$ holds for all $k \geq 1$, one can observe that part i) of the above theorem yields a lower estimate for $F_{\pm}(k)$ as well. Comparing Theorem 2.1 with (2.1), we see that our result provides similar bounds for $F(k)$ and $F_{\pm}(k)$ as [39] but under more general circumstances.

The next result (Proposition 2.1 from our paper [9]) describes the degenerate situation, where the elements of A are pairwise multiplicatively dependent. Comparing this result with Theorem 2.1, one can see that the behaviour of $F(k)$ and $F_{\pm}(k)$ are completely different in these cases.

Theorem 2.2. *If all pairs of elements of* A *are multiplicatively dependent, then there exist constants* $1 < C_4 < C_5$ *depending only on* A *such that*

$$C_4^k < F(k) \leq F_{\pm}(k) < C_5^k \quad \textit{for all } k > 1.$$

The next theorem plays a key role in the proof of Theorem 2.1. This result extends classical theorems of Tijdeman [84, 85] concerning the gaps in A' in the case where the elements of A are primes, to the case where the elements of A are arbitrary positive integers. This is Theorem 2.2 in Bertók [9].

Theorem 2.3. *Suppose that* A *has at least two multiplicatively independent elements and write* $1 = a'_0 < a'_1 < \ldots$ *for the sequence of the elements of* A'. *Then there exist a positive integer* N *and positive constants* C_6, C_7 *depending only on* A *such that:*

i) $a'_{n+1} - a'_n > \frac{a'_n}{(\log a'_n)^{C_6}}$ *for* $a'_n \geq 3$,

ii) $a'_{n+1} - a'_n < \frac{a'_n}{(\log a'_n)^{C_7}}$ *for* $a'_n \geq N$.

The following lemma (Lemma 3.5 in Bertók [9]) considers the case where all pairs of elements in A are pairwise multiplicatively dependent.

Lemma 2.1. *If the elements of A are pairwise multiplicatively dependent, then there exists a positive integer b such that A' contains only non-negative powers of b. Furthermore, there exist non-negative integers C_8, C_9 depending only on A, such that for any non-negative integer β with $\beta \geq C_9$ we have $b^\beta \in A'$. In particular, if $a'_n > b^{C_9}$ then*

$$a'_{n+1} - a'_n = (b-1)b^{n+C_8}.$$

Proof. If the elements of A are pairwise multiplicatively dependent, then we can find non-negative integers γ_i, γ_j such that $a_i^{\gamma_i} = a_j^{\gamma_j}$ holds for any $i, j \leq l$. One can easily see that this means that there exists a positive integer b for which $a_i = b^{\beta_i}$ holds for every $i = 1, \ldots, l$. If this number is not uniquely determined then let b be the largest number for which the previous equality holds.

To prove the second part of the lemma, observe that gcd$(\beta_1, \beta_2, \ldots, \beta_l) = 1$ holds. Consider the Diophantine equation

$$\beta_1 x_1 + \beta_2 x_2 + \ldots + \beta_l x_l = \beta$$

in positive integers $x_1, \ldots, x_l$, where β is a fixed positive integer. It is well-known (see e.g. [64]) that there exists a constant $c_1 \in \mathbb{N}$ depending only on $\beta_1, \ldots, \beta_l$, such that for every $\beta \geq c_1$ the above equation is solvable. Thus every number of the form b^β with $\beta \geq c_1$ belongs to A'. By choosing $C_9 = c_1$ the statement immediately follows. □

2.1.2 Lemmas

To prove the theorems we need several lemmas. The first one (Lemma 3.1 in Bertók [9]) is a simple equivalent condition for multiplicative dependence of

two integers. Since its proof is obvious, we omit it completely.

Lemma 2.2. *Let u and $v \neq 1$ be positive integers. Then $\frac{\log u}{\log v}$ is rational if and only if u and v are multiplicatively dependent.*

The next lemma (Lemma 3.2 in Bertók [9]) concerns the convergents of numbers $\frac{\log u}{\log v}$. Note that a similar statement is proved in [84], in the special case where u and v are primes. In fact the proof of this lemma is rather similar to that from [84]. However, for the convenience of the reader, and to keep the presentation self-contained, we give the proof here, too.

Lemma 2.3. *Let $u, v \neq 1$ be multiplicatively independent positive integers. Write $\frac{p_0}{q_0}, \frac{p_1}{q_1} \ldots$ for the sequence of convergents of $\frac{\log u}{\log v}$. There exists a constant C_{10}, depending only on u and v such that for any $i \geq 2$ we have*

$$q_{i+1} < q_i^{C_8} \log v.$$

Proof. If $i \geq 2$ then $q_i \geq 2$. It is well-known that

$$\left| \frac{p_i}{q_i} - \frac{\log u}{\log v} \right| < \frac{1}{q_i q_{i+1}}.$$

Thus we have

$$|p_i \log v - q_i \log u| < \frac{\log v}{q_{i+1}}. \tag{2.2}$$

Note that by Lemma 2.2 we have $|p_i \log v - q_i \log u| \neq 0$. Thus by a classical result of Baker [5] we get

$$|p_i \log v - q_i \log u| > \exp\{-c_2(\log H)\},$$

where $H = \max(p_i, q_i)$ and c_2 is a constant depending only on u and v. Since $\frac{p_i}{q_i} < 1 + \frac{\log u}{\log v}$, we get $\log H \leq c_3 \log q_i$ $(i \geq 2)$, where c_3 is a constant depending only on u and v. Thus we obtain

$$|p_i \log v - q_i \log u| > q_i^{-c_4} \quad (i \geq 2), \tag{2.3}$$

where c_4 is a constant depending only on u and v. With $C_{10} = c_4$, the lemma now follows from (2.2) and (2.3). □

For the next lemma, let $\lambda(m)$ denote the Carmichael function of an integer $m > 1$. This is the smallest positive integer b such that for any integer a for which $(a, m) = 1$ we have $a^b \equiv 1 \pmod{m}$. The following lemma is a generalization of Theorem 1 from [38] (and also an explicit version of a theorem of Erdős, Pomerance and Schmutz [28]). This lemma is Theorem 2.2 in Bertók and Hajdu [12].

Lemma 2.4. *There exist positive constants $C_{11} > 1$ and C_{12} such that for any positive integer r and for every large integer i there is an integer m with $r \mid m$, such that*

$$\log m \in [\log i + \log r, (\log i)^{C_{11}} + \log r]$$

and

$$\lambda(m) < r(\log m/r)^{C_{12} \log\log\log m/r}.$$

Proof. Let r be an arbitrary positive integer, and let i be sufficiently large. By Theorem 1 of [38] there exists an n such that

$$\log n \in [\log i, (\log i)^{C_{11}}] \text{ and } \lambda(n) < (\log n)^{C_{12} \log\log\log n},$$

where C_{11}, C_{12} are positive constants with $C_{11} > 1$. Put $m := rn$. Then

obviously, $r \mid m$. Furthermore, we immediately obtain

$$\log m \in [\log i + \log r, (\log i)^{C_{11}} + \log r].$$

Finally, as it is well-known, for any positive integers a, b we have $\lambda(ab) \leq a\lambda(b)$. Hence

$$\lambda(m) \leq r\lambda(n) < r(\log n)^{C_{12} \log\log\log n} = r(\log m/r)^{C_{12} \log\log\log m/r},$$

and the lemma follows. □

Remark 1. In fact, in the proofs of the theorems in this section we will use Lemma 2.4 only with $r = 1$. However, later in Section 3, we will need this result in its full generality.

Let now k be a positive integer and let $H_{A,k}$ be the set of those integers n which can be represented as the sum of at most k elements from A'. That is, put

$$H_{A,k} = \{n \in \mathbb{Z} \mid n = \sum_{i=1}^{I} a_i' \text{ with } I \leq k \text{ and } a_i' \in A' \ (i = 1, \ldots, I)\}.$$

Moreover, for any $H \subseteq \mathbb{Z}$ and $m \in \mathbb{Z}, m \geq 2$ let $H \pmod m$ be the set of the residues of the elements of H modulo m, i.e.

$$H \pmod m = \{i \mid 0 \leq i < m, h \equiv i \pmod m \text{ for some } h \in H\}.$$

The following lemma is Theorem 1 from [39]. This result tells us that there exists a modulus m such that the elements of $H_{A,k}$ cover only a "few" residues modulo m.

Lemma 2.5. *Let C_{11}, A and k be as above. There is a constant C_{13} such that for every sufficiently large integer i there exists an integer m with $\log m \in [\log i, (\log i)^{C_{11}}]$ and*

$$|H_{A,k} \pmod m| < (\log m)^{C_{13}kl \log\log\log m}.$$

2.1.3 Proofs

Because in the proof of Theorem 2.1 we use Theorem 2.3, we prove the latter result first.

Proof of Theorem 2.3. First we prove part i) of the statement. In case where the elements of A are primes, it is a result of Tijdeman [84]. If the elements of A are not primes, then let $P = \{p_1, \ldots, p_m\}$ be the set of the prime factors of the elements of A and put

$$P' = \{p_1^{\alpha_1} \ldots p_m^{\alpha_m} \mid \alpha_1, \ldots, \alpha_m \text{ are non-negative integers}\}.$$

It can be easily seen that $A' \subseteq P'$. Thus part i) follows from the result of Tijdeman [84].

To prove part ii) of the theorem, we follow the method of Tijdeman [85]. Let u and v be multiplicatively independent elements of A, and write $1 = x_0 < x_1 < \ldots$ for the elements of the set $\{u^r v^s | r, s \geq 0\}$. For the rest of the proof we note that from now on all constants depend only on u and v. Let $x = x_n = u^r v^s \geq N$, where N is chosen later. We may assume that $u^r \geq \sqrt{x}$. Thus we have

$$r \geq \frac{\log x}{2 \log u}. \tag{2.4}$$

Let $\frac{p_0}{q_0}, \frac{p_1}{q_1}, \ldots$ be the convergents of $\frac{\log u}{\log v}$. As it is well-known, $q_0, q_1, \ldots$ is a monotone increasing sequence. Choose i such that $q_i \leq r < q_{i+1}$ and suppose that N is so large that both $n \geq 3$ and $i \geq 2$. We distinguish two cases.

a) Assume first that

$$\frac{p_i}{q_i} > \frac{\log u}{\log v}.$$

Putting $x' = u^{r-q_i} v^{s+p_i}$, we have $x' > x$. Hence using well-known properties of the convergents, we get

$$\frac{p_i}{q_i} - \frac{\log u}{\log v} < \frac{p_i}{q_i} - \frac{p_{i+1}}{q_{i+1}} = \frac{1}{q_i q_{i+1}}.$$

Thus

$$\log \frac{x'}{x} = \log \frac{v^{p_i}}{u^{q_i}} = p_i \log v - q_i \log u < \frac{\log v}{q_{i+1}}.$$

Using $r < q_{i+1}$ and (2.4) we obtain

$$\log \frac{x'}{x} < \frac{\log v}{q_{i+1}} < \frac{\log v}{r} \leq \frac{2 \log u \log v}{\log x}.$$

Hence we see that $\frac{x'}{x}$ has an upper bound depending only on u and v. Using that $x' > x$, and by the elementary properties of the function $f(y) = \frac{\log y}{y-1}$ (where $y = \frac{x'}{x}$) one can easily prove that

$$\log \frac{x'}{x} > c_5 \left(\frac{x'}{x} - 1 \right).$$

It follows from the inequalities above, that

$$\frac{x'}{x} - 1 < \frac{c_6}{\log x}.$$

Thus

$$x_{n+1} \leq x' < x + c_6 \frac{x}{\log x} = x_n + c_6 \frac{x_n}{\log x_n}. \tag{2.5}$$

b) Now suppose that

$$\frac{p_i}{q_i} < \frac{\log u}{\log v}.$$

Then as it is well-known, $\frac{p_{i-1}}{q_{i-1}} > \frac{\log u}{\log v}$. Letting $x' = u^{r-q_{i-1}} v^{s+p_{i-1}}$, we have $x' > x$. Hence

$$\frac{p_{i-1}}{q_{i-1}} - \frac{\log u}{\log v} < \frac{p_{i-1}}{q_{i-1}} - \frac{p_i}{q_i} = \frac{1}{q_{i-1} q_i}.$$

It follows that

$$\log \frac{x'}{x} = \log \frac{v^{p_{i-1}}}{u^{q_{i-1}}} = p_{i-1} \log v - q_{i-1} \log u < \frac{\log v}{q_i}.$$

By Lemma 2.3 we obtain

$$q_i > \left(\frac{q_{i+1}}{\log v} \right)^{c_7}.$$

Using the above inequalities, (2.4) and $r < q_{i+1}$, we get

$$\log \frac{x'}{x} < \frac{\log v}{q_i} < \frac{(\log v)^{1+c_7}}{q_{i+1}^{c_7}} < \frac{(2 \log u)^{c_7} (\log v)^{1+c_7}}{(\log x)^{c_7}}.$$

Thus similarly as in case a) there exists a constant c_8 such that

$$\log \frac{x'}{x} > c_8 \left(\frac{x'}{x} - 1 \right).$$

This yields

$$x_{n+1} \le x' < x + c_9 \frac{x}{(\log x)^{c_7}} = x_n + c_9 \frac{x_n}{(\log x_n)^{c_7}}. \tag{2.6}$$

Thus by (2.5) and (2.6), we have in both cases a) and b) that

$$x_{n+1} \le x_n + c_{10} \frac{x_n}{(\log x_n)^{c_{11}}}, \quad \text{for } x_n \ge N.$$

For N sufficiently large this implies

$$x_{n+1} < x_n + \frac{x_n}{(\log x_n)^{c_{12}}}, \quad \text{for } x_n \ge N,$$

which proves the statement with $C_7 = c_{12}$. □

Proof of Theorem 2.2. First note that $F(k) \le F_{\pm}(k)$ obviously holds for all $k \ge 1$. To prove the lower estimate $C_4^k < F(k)$, observe that by Lemma 2.1 in this case A' contains only powers of b, further, A' contains all powers of b from some point on. Hence this part of the statement follows by a simple calculation.

To prove the upper estimate $F_{\pm}(k) < C_5^k$, without loss of generality we may clearly assume that by the above notation $A' = \{b^i | i = 0, 1, 2, \ldots\}$. Let $k > 1$ and if $b \ge 3$ then let $n = b^{k-1} + b^{k-2} + \ldots + b + 1$. We show that for any representation of n of the form $n = a'_1 + \ldots + a'_t$ ($a'_i \in A'_{\pm}$, $i = 1, 2, \ldots, t$) we have $t \ge k$. Let t be minimal with this property and assume that $|a'_1| \ge |a'_2| \ge \ldots \ge |a'_t|$. Because of the minimality of t one can easily

check that $a'_1 = b^{k-1}$ must hold. Now let $n' = n - b^{k-1}$ and apply the same argument for n' to determine a'_2. By induction we get that $a'_1 = b^{k-1}, a'_2 = b^{k-2}, \ldots, a'_{t-1} = b, a'_t = 1$. Thus we get that $F_{\pm}(k) \leq n < b^k$ so $C_5 = b$ is an appropriate choice. If $b = 2$ then we can use a similar argument with $n = 2^{2k-2} + 2^{2k-4} + \ldots + 1$. In this case we have $n < 4^k$ and the statement follows. □

Proof of Theorem 2.1. We follow the argument of Theorem 3 of Hajdu and Tijdeman [39]. The important difference is that by using Theorem 2.3, we can prove a more general statement.

To prove part i) of Theorem 2.1 we use the greedy algorithm. Suppose that we want to express the positive integer n as a sum of elements of A'. Let a'_1, a'_2 be successive elements of A' such that $a'_1 \leq n < a'_2$, and let $n_1 := n - a'_1$. Then by Theorem 2.3 we have $n_1 \leq a'_2 - a'_1 < \frac{a'_1}{(\log a'_1)^{c_{13}}} < \frac{n}{(\log n)^{c_{13}}}$ with some number $c_{13} > 0$ depending only on A. Then we repeat this step for n_1, to get n_2 with $n_2 < \frac{n_1}{(\log n_1)^{c_{14}}}$. We can iterate this method and reduce the "rest" each time by a factor at least $(\log n)^{c_{15}}$ until n_i exceeds $\exp(\sqrt{\log n})$. If n_i is smaller than $\exp(\sqrt{\log n})$ we can reduce n_i, n_{i+1}, and so on, in each step by a factor larger than some constant $c_{16} > 1$ with c_{16} depending only on the smallest element of A. We can repeat it as long as $(\log n_{i+j})^{c_{16}} > c_{17}$ where c_{17} is a constant depending only on A. After the procedure, we find that

$$k \leq i + j + c_{17} < \frac{\log n}{c_{15} \log\log n} + \frac{\sqrt{\log n}}{\log c_{16}} + c_{17}$$

elements of A' suffices to represent n, which implies $F(k) > k^{C_1 k}$.

To prove part ii) of Theorem 2.1 and give an upper bound for $F(k)$ we study the number of representations of postive integers up to n as $\sum_{j=1}^{k} a'_j$ with

$a'_j \in A' \cup \{0\}$. Since the number of elements of $A' \cup \{0\}$ not exceeding n is at most $(c_{18} \log n)^l$, the number of represented integers is at most $(c_{18} \log n)^{kl}$. If this number is less than n, then we are sure that some positive integer $\leq n$ is not represented. This is the case if

$$kl < \frac{\log n}{\log\log n + \log c_{18}}.$$

Suppose $n > (kl)^{(1+\varepsilon)kl}$. Then it follows from the monotonicity of the function $\frac{\log x}{\log\log x + c_{18}}$ for large x that

$$\frac{\log n}{\log\log n + c_{18}} > \frac{(1+\varepsilon)kl\log(kl)}{\log(kl) + \log((1+\varepsilon)\log(kl)) + c_{18}} > kl$$

for kl sufficiently large. By choosing C_2 suitably for the smaller values of kl, it suffices for all values of kl that $n \geq C_2(kl)^{(1+\varepsilon)kl}$. Thus

$$F(k) \leq C_2(kl)^{(1+\varepsilon)kl}$$

which proves part ii) of Theorem 2.1.

To prove part iii) of Theorem 2.1 we consider representations by sums of elements from $A'_{\pm}$. Let $H^*_{A,k}$ be the same set as $H_{A,k}$, with the only difference that instead of working with elements of A' we are now using the elements of $A'_{\pm}$. Choose the smallest positive integer $i > 10$ such that $j > (\log j)^{C_{13}kl\log\log\log j}$ for $j \geq i$. Then $i < 2(\log i)^{C_{13}kl\log\log\log i}$, where C_{13} is the same as in Lemma 2.5. It follows that

$$\log i < c_{19}kl(\log\log i)(\log\log\log i),$$

whence $\log i < c_{20}kl(\log(kl))(\log\log(kl))$ for some constants c_{19} and c_{20}. By

Lemma 2.4 there exists an integer m with $\log i \leq \log m \leq (\log i)^{C_{11}}$ such that all representations in $H^*_{A,k}$ are covered by at most $(\log m)^{C_{11}kl \log\log\log m}$ residues modulo m. By the definition of i and the inequality $i \leq m$, we see that this number of residues is less than m, therefore at least one positive integer $n \leq m$ has no representation of the form $\sum_{j=1}^{k} a'_j$, with $a'_j \in A'_{\pm}$. Hence

$$\log n \leq \log m \leq (\log i)^{C_{11}} < (c_{20}kl(\log(kl))(\log\log(kl)))^{C_{11}} < (kl)^{c_{21}}$$

for some constant c_{21}. Thus $F_{\pm}(k) < \exp((kl)^{c_{21}})$ and part iii) of Theorem 2.1 is proved with $C_3 = c_{21}$. □

2.2 Multi-base representations

It is an old problem to study integers having only a "few" non-zero digits in some classical base b representation. A generalization of this problem is the analysis of the so-called multi-base representations, when instead of linear combinations of powers of a fixed number b, one can combine products of powers of fixed primes. For some related results see the papers of Ádám, Hajdu and Luca [1], Dimitrov and Howe [25], Hajdu and Luca [37], Hajdu and Tijdeman [38, 39] and Nathanson [56], and the references given there.

It is also an interesting question to study integers having only "few" non-zero digits in different bases simultaneously. Senge and Straus [71] proved that the number of those integers, whose number of non-zero digits in two different bases b_1 and b_2 with $\log b_1 / \log b_2 \notin \mathbb{Q}$ remains under some fixed bound, is finite. Later, Stewart [78] gave a more precise, effective version of this result (for an extension to the case of several number systems, see Schlikewei [69], and for number systems based on recurrence sequences see the papers of Pethő and Tichy [61, 62]).

In this section we consider the following problem. Let S be a finite set of primes, and write $\mathbb{Z}_S$ (resp. $\mathbb{Z}_S^+$) for the set of integers (resp. positive integers) having no prime divisors outside S. We consider the representations of integers n of the form

$$n = u_1 + \cdots + u_t \tag{2.7}$$

with $u_1, \ldots, u_t \in \mathbb{Z}_S$. Such a representation of n is often called a multi-base representation. We write $w_S(n)$ for the minimal t for which (2.7) holds with some $u_1, \ldots, u_t \in \mathbb{Z}_S$. If $n > 0$ and we also require that $u_1, \ldots, u_t \in \mathbb{Z}_S^+$, we then write $w_S^+(n)$ instead.

In this section we prove finiteness theorems for integers n with "small" values of $w_S^+(n)$ with respect to different sets S simultaneously. For the theoretical results we use Baker's method concerning linear forms in logarithm and a deep theorem of Evertse [30] bounding the number of non-degenerate solutions of S-unit equations.

Similarly to Section 2.1 we first state the theorems, then in a later subsection we prove these results.

2.2.1 New results

The first part of the following theorem (which is Theorem 2.1 in Bertók, Hajdu, Luca, Sharma [14]) shows that for fixed disjoint sets of primes $S_1, \ldots, S_k$, and a fixed T, there can only be finitely many integers n such that the sum of the $w_{S_i}^+(n)$ $(i = 1, \ldots, k)$ is lower than T. In the second part of the theorem we give an effective upper bound for the number of such numbers. We note that this result is an extension of the above mentioned result of Stewart [78] to the multi-base situation.

Theorem 2.4. *Let k be a positive integer, $S_1, \ldots, S_k$ be finite sets of primes*

such that $S_1 \cap \cdots \cap S_k = \emptyset$. *Then for any* T *the inequality*

$$w_{S_1}^+(n) + \cdots + w_{S_k}^+(n) \le T$$

is valid only for finitely many integers n. *Furthermore, the number of such integers* n *is at most* $C_{14} = C_{14}(T,\ k,\ s)$, *where* C_{14} *is an effectively computable constant depending only on* $T,\ k$ *and* $s := |S_1 \cup \cdots \cup S_k|$.

Remark 2. It is important to note that the condition $S_1 \cap \cdots \cap S_k = \emptyset$ in the above theorem is necessary. Indeed, if $p \in S_1 \cap \cdots \cap S_k$ would hold with some prime p, then for $T := k \ge 1$ we would have

$$w_{S_1}^+(n) + \cdots + w_{S_k}^+(n) \le T$$

for all $n = p^\alpha$ $(\alpha \ge 0)$, since in this case $w_{S_i}^+(n) = 1$ for all $1 \le i \le k$.

The second result (Theorem 2.2 in our paper [14]) gives an effective lower bound for $w_S^+(n)$ in a special case.

Theorem 2.5. *Let* ℓ *be a positive integer,* $S_1 = \{p_1, \ldots, p_\ell\}$ *and* $S_2 = \{q\}$, *where* $p_1, \ldots, p_\ell,\ q$ *are distinct primes. If* n *is a positive integer with* $n > e^{e^e}$ *such that* $w_{S_1}^+(n) = 1$, *then we have*

$$w_{S_2}^+(n) > \frac{C_{15} \log\log n}{\log\log\log n},$$

where $C_{15} = C_{15}(\ell,\ p_1, \ldots, p_\ell,\ q)$ *is an effectively computable positive constant depending only on* $\ell,\ p_1, \ldots, p_\ell,\ q$.

Remark 3. The condition $q \notin S_1$ is necessary. This can be easily checked by a similar example as in Remark 2. Furthermore, we note that if the sets S_i

consists of multiplicatively independent elements instead of primes, then after the necessary modifications Theorems 2.4 and 2.5 still hold.

2.2.2 Lemmas

For the proofs of the theorems we need several lemmas and some notations. Let $a_1, \dots, a_\ell \in \mathbb{Q}^*$. Consider the equation

$$a_1 x_1 + \cdots + a_\ell x_\ell = 0 \tag{2.8}$$

in $x_1, \dots, x_\ell \in \mathbb{Z}_S$. A solution $(x_1, \dots, x_\ell)$ of the above equation is said to be *non-degenerate* if

$$\sum_{i \in I} a_i x_i \neq 0 \text{ for each non-empty } I \subset \{1, \dots, \ell\}$$

and *degenerate* otherwise. Furthermore, two solutions $(x_1, \dots, x_\ell)$ and $(y_1, \dots, y_\ell)$ of (2.8) are called *proportional* if for some $z \in \mathbb{Q}^*$, we have

$$x_i = z y_i \text{ for } i = 1, \dots, \ell.$$

Now we are ready to state the required lemmas and propositions. The first lemma gives an upper bound for the number of non-degenerate solutions of (2.8). This lemma is Theorem 3 of Evertse [30].

Lemma 2.6. *Let $s = |S|$. Then equation* (2.8) *has at most*

$$(2^{35}(\ell - 1)^2)^{(\ell-1)^3 s}$$

non-degenerate solutions $(x_1, \dots, x_\ell) \in \mathbb{Z}_S^\ell$, no two of them are proportional.

2.2.3 Proofs

Now we give the proof of Theorem 2.4. In fact, we prove a more general result, which implies Theorem 2.4. Namely, we prove the following statement (which is Proposition 3.1 in our paper [14]).

Proposition 2.1. *Let $k \geq 2$ and let $t_1, \ldots, t_k \in \mathbb{N}$. For $i = 1, \ldots, k$, let*

$$A_i = \{a_{i,1}, \ldots, a_{i,t_i}\}$$

be a set of t_i positive integers. Then the number of positive integers n such that for each i, there exist $u_{i,1}, \ldots, u_{i,t_i} \in \mathbb{Z}^+_{S_i}$ such that

$$n = a_{i,1}u_{i,1} + \cdots + a_{i,t_i}u_{i,t_i},$$

is at most

$$(2^{35}(t-1)^2)^{(k-1)(t-1)^4 s},$$

where $t = t_1 + \cdots + t_k$ and $s = |S_1 \cup S_2 \cup \cdots \cup S_k|$.

Proof. Let $S = S_1 \cup S_2 \cup \cdots \cup S_k$. We prove the statement by induction on k.

Suppose that $k = 2$. We will prove that the result holds in this case using induction on $t = t_1 + t_2$. Suppose that $t = 2$. Then $t_1 = t_2 = 1$. We now show that the equation

$$a_{1,1}u_{1,1} = a_{2,1}u_{2,1} \tag{2.9}$$

in $(u_{1,1}, u_{2,1}) \in \mathbb{Z}^+_{S_1} \times \mathbb{Z}^+_{S_2}$ has at most one solution. Indeed, equation (2.9) implies that

$$\frac{u_{1,1}}{u_{2,1}} = \frac{a_{2,1}}{a_{1,1}}.$$

Hence the claim follows by the coprimality of $u_{1,1}$ and $u_{2,1}$. Therefore, the result holds when $k = t = 2$. Let $t \geq 3$ and assume that the result holds

whenever $t_1 + t_2 \leq t - 1$. We now consider the case $t_1 + t_2 = t$. We have to count the number of solutions of the S-unit equation

$$a_{1,1}u_{1,1} + \cdots + a_{1,t_1}u_{1,t_1} = a_{2,1}u_{2,1} + \cdots + a_{2,t_2}u_{2,t_2}, \tag{2.10}$$

where $u_{1,j} \in \mathbb{Z}_{S_1}^+$ and $u_{2,j} \in \mathbb{Z}_{S_2}^+$. By Lemma 2.6, this equation has at most

$$(2^{35}(t-1)^2)^{(t-1)^3 s}$$

non-degenerate solutions. Next, we count the number of classes of degenerate solutions. (Observe that if $t = 3$, then $(t_1, t_2) = (1, 2)$ or $(2, 1)$ and hence all the solutions are non-degenerate. Therefore, while counting degenerate solutions, it is understood that $t \geq 4$.) For a degenerate solution, there exists a non-empty subset I of $\{1, \ldots, t_1\}$ and a non-empty subset J of $\{1, \ldots, t_2\}$ such that

$$\sum_{i \in I} a_{1,i}u_{1,i} - \sum_{j \in J} a_{2,j}u_{2,j} = 0, \tag{2.11}$$

but no proper subsum in this equation vanishes. Fix I, J. We count the number of solutions of (2.10) satisfying (2.11). Since $|I| + |J| \leq t - 2$, it follows from Lemma 2.6 that the S-unit equation (2.11) has at most

$$(2^{35}(t-3)^2)^{(t-3)^3 s}$$

classes of non-degenerate solutions. Furthermore, by the induction hypothesis, the equation

$$\sum_{i \notin I} a_{1,i}u_{1,i} - \sum_{j \notin J} a_{2,j}u_{2,j} = 0$$

has at most

$$(2^{35}(t-3)^2)^{(t-3)^4 s}$$

solutions. Hence, given I, J, we obtain that there are at most

$$(2^{35}(t-3)^2)^{s(t-3)^3(t-2)}$$

solutions. Varying I and J, we obtain that the total number of degenerate solutions is at most

$$2^t(2^{35}(t-3)^2)^{s(t-3)^3(t-2)} \ \leq \ \frac{1}{2}(2^{35}(t-1)^2)^{(t-1)^4 s}.$$

Thus, (2.10) has at most

$$(2^{35}(t-1)^2)^{(t-1)^3 s} + \frac{1}{2}(2^{35}(t-1)^2)^{(t-1)^4 s} \ \leq \ (2^{35}(t-1)^2)^{(t-1)^4 s}$$

solutions. This completes the induction on t. Hence, the result holds for $k = 2$.

Now let $k \geq 3$. Suppose that the result holds for every k' with $2 \leq k' < k$. That is, given k' in the above range, we assume that the result is valid for all t and for all choices of the sets A_i and S_i. Note that $t = t_1 + \cdots + t_k \geq k \geq 3$. We have to bound the number of solutions of the following system of S-unit equations:

$$\begin{aligned} a_{1,1}u_{1,1} + \cdots + a_{1,t_1}u_{1,t_1} &= a_{2,1}u_{2,1} + \cdots + a_{2,t_2}u_{2,t_2} \\ &\vdots \\ &= a_{k,1}u_{k,1} + \cdots + a_{k,t_k}u_{k,t_k}, \end{aligned} \tag{2.12}$$

where $u_{i,j} \in \mathbb{Z}_{S_i}^+$. We mention that similar systems of S-unit equations have been studied by Evertse and Győry [31]. However, their theorems cannot be

used directly here, so we apply some other results. Namely, by Lemma 2.6, the first equation in (2.12) has at most

$$(2^{35}(t-2)^2)^{(t-2)^3 s} \tag{2.13}$$

non-degenerate solutions. For a degenerate solution, there exists a positive integer $l \leq t-2$ and distinct non-empty subsets $I_1, \ldots, I_l \subseteq \{1, \ldots, t_1\}$, $J_1, \ldots, J_l \subseteq \{1, \ldots, t_2\}$ such that for $m = 1, \ldots, l$,

$$\sum_{i \in I_m} a_{1,i} u_{1,i} = \sum_{i \in J_m} a_{2,i} u_{2,i}, \tag{2.14}$$

but no proper subsum vanishes. Fix $I_1, \ldots, I_l, J_1, \ldots, J_l$. We count the number of solutions of the system (2.12) satisfying the additional equations (2.14). By Lemma 2.6, for each $m = 1, \ldots, l$, equation (2.14) has, up to proportionality, at most

$$(2^{35}(t-3)^2)^{(t-3)^3 s}$$

non-degenerate solutions. Let $((u_{1,i})_{i \in I_m}, (u_{2,i})_{i \in J_m})$ be a solution of (2.14) with $\gcd((u_{1,i})_{i \in I_m}, (u_{2,i})_{i \in J_m}) = 1$. Set

$$a'_m = \sum_{i \in I_m} a_{1,i} u_{1,i} \left(= \sum_{i \in J_m} a_{2,i} u_{2,i} \right).$$

Then

$$\{((U_m u_{1,i})_{i \in I_m}, (U_m u_{2,i})_{i \in J_m}) : U_m \in \mathbb{Z}^+_{S_1 \cap S_2}\}$$

is precisely the set of solutions of (2.14) which are proportional to $((u_{1,i})_{i \in I_m}, (u_{2,i})_{i \in J_m})$. The problem is thus reduced to considering the fol-

lowing system of equations in the variables $U_1, \ldots, U_l$, $u_{3,1} \ldots, u_{k,t_k}$:

$$\begin{aligned} a'_1 U_1 + \cdots + a'_l U_l &= a_{3,1} u_{3,1} + \cdots + a_{3,t_3} u_{3,t_3} \\ &\vdots \\ &= a_{k,1} u_{k,1} + \cdots + a_{k,t_k} u_{k,t_k}. \end{aligned}$$

Since $(S_1 \cap S_2) \cap S_3 \cap \cdots \cap S_k = \emptyset$, we apply the induction hypothesis for $k' = k - 1$ to conclude that the above system of equations has at most

$$(2^{35}(t-2)^2)^{(k-2)(t-2)^4 s}$$

solutions. Hence, given $I_1, \ldots, I_l, J_1, \ldots, J_l$, we get at most

$$(2^{35}(t-3)^2)^{(t-3)^3 s(t-2)} \cdot (2^{35}(t-2)^2)^{(k-2)(t-2)^4 s}$$

solutions. Therefore the number of classes of degenerate solutions is bounded by

$$t^t (2^{35}(t-2)^2)^{(k-1)(t-2)^4 s} \leq \frac{1}{2} (2^{35}(t-1)^2)^{(k-1)(t-1)^4 s}. \tag{2.15}$$

Combining the above bound (2.15) with (2.13), we obtain that the total number of solutions is at most

$$(2^{35}(t-1)^2)^{(k-1)(t-1)^4 s}.$$

This completes the induction and the proof of the proposition. □

As we mentioned before, Theorem 2.4 is an easy consequence of Proposiiton 2.1.

Proof of Theorem 2.4. Taking $t_i = w_{S_i}^+(n)$ and $A_i = \{1\}$ for all $i = 1, \dots, k$ in Proposition 2.1, the statement immediately follows. □

Now we prove Theorem 2.5. For the proof we use a Baker type estimate of Matveev [51]. For its formulation we need to introduce some notations.

For an algebraic number α of degree D over $\mathbb{Q}$, the absolute logarithmic height of α is defined by

$$h(\alpha) = \frac{1}{D}\left(\log a_0 + \sum_{i=1}^{D} \log \max(1, |\alpha^{(i)}|)\right),$$

where $a_0 > 0$ is the leading coefficient of the minimal polynomial of α over $\mathbb{Z}$ and $\alpha^{(i)}$ $(i = 1, \dots, D)$ are the conjugates of α. Note that in the special case when $\alpha = p/q$ is a non-zero rational number with $\gcd(p, q) = 1$, then $h(\alpha) = h(1/\alpha) = \log \max\{|p|, |q|\}$.

The following result is due to Matveev [51].

Lemma 2.7. *Assume that $\alpha_1, \dots, \alpha_r$ are positive real algebraic numbers in a real algebraic number field of degree D, $d_1, \dots, d_r$ are rational integers, and*

$$\Lambda := \alpha_1^{d_1} \dots \alpha_r^{d_r} - 1$$

is not zero. Set

$$B \geq \max\{|d_1|, \dots, |d_r|\},$$

and

$$A_i \geq \max\{Dh(\alpha_i), |\log \alpha_i|, 0.16\}, \text{ for all } i = 1, \dots, r.$$

Then we have

$$|\Lambda| > \exp(-1.4 \cdot 30^{r+3} r^{4.5} D^2 (1 + \log D)(1 + \log B) A_1 \cdots A_r). \quad (2.16)$$

Now we are ready to give the proof of Theorem 2.5.

Proof of Theorem 2.5. We combine arguments of Luca [48] and Stewart [78] with some other considerations.

Let n be a positive integer with $w^+_{S_1}(n) = 1$ and $w^+_{S_2}(n) = t$, and write

$$u_1 = n = v_1 + \cdots + v_t \tag{2.17}$$

with $u_1 \in \mathbb{Z}^+_{S_1}$ and $v_1, \ldots, v_t \in \mathbb{Z}^+_{S_2}$. Without loss of generality we may assume that $v_1 \geq \cdots \geq v_t$.

We write

$$u_1 = p_1^{\alpha_1} \ldots p_\ell^{\alpha_\ell}, \quad v_i = q^{\beta_i} \qquad (i = 1, \ldots, t). \tag{2.18}$$

Let B be the maximum of the exponents appearing in (2.18).

Equation (2.17) can be rewritten as

$$u_1 - v_1 = v_2 + \cdots + v_t. \tag{2.19}$$

Since $u_1 \neq v_1$ and $v_1 \neq 1$ (otherwise $n = 1$ or $t = n$ and the statement is trivial), Lemma 2.7 yields

$$v_1 \exp(-c_{22}(1 + \log B)) < v_1(u_1 v_1^{-1} - 1), \tag{2.20}$$

with $c_{22} := c_{23} h(p_1) \cdots h(p_\ell) h(q)^2$, where

$$c_{23} := 1.4 \cdot 30^{\ell+5}(\ell + 2)^{4.5}$$

is the constant appearing in the conclusion of Matveev's theorem (2.16) when Λ involves $r = \ell + 2$ rational numbers. (Note that $D = 1$.)

Now we show that

$$\frac{v_1}{v_j} < \exp(2j \log t (c_{22}(1 + \log B))^{j-1}) \qquad (j = 2, \ldots, t). \tag{2.21}$$

We prove it by induction. Combining inequality (2.20) with

$$v_1(u_1 v_1^{-1} - 1) = u_1 - v_1 < t v_2$$

implied by (2.19), we get

$$\frac{v_1}{v_2} < \exp\left(\log t + c_{22}(1 + \log B)\right) \leq \exp\left(2(\log t) c_{22}(1 + \log B)\right).$$

Let now i be arbitrary with $2 \leq i < t$, and assume by induction that

$$\frac{v_1}{v_j} < \exp\left(2j \log t (c_{22}(1 + \log B)^{j-1})\right) \quad \text{for all } j = 2, \ldots, i. \tag{2.22}$$

Rewrite (2.17) as

$$u_1 - v_1 - \cdots - v_i = v_{i+1} + \cdots + v_t. \tag{2.23}$$

Observe that by (2.18) and (2.22) (used with $j = i$), we have

$$\begin{aligned} h\left(1 + \frac{v_2}{v_1} + \cdots + \frac{v_i}{v_1}\right) &= h\left(\frac{q^{\beta_1 - \beta_i} + \cdots + q^{\beta_{i-1} - \beta_i} + 1}{q^{\beta_1 - \beta_i}}\right) = \\ &= \log(q^{\beta_1 - \beta_i} + \cdots + q^{\beta_{i-1} - \beta_i} + 1) \leq \log(t q^{\beta_1 - \beta_i}) = \\ &= \log t + \log\left(\frac{v_1}{v_i}\right) < (2i + 1)(\log t)(c_{22}(1 + \log B))^{i-1}. \end{aligned}$$

Hence, Lemma 2.7 yields

$$v_1 \exp(-(2i+1)(c_{22}(1+\log B))^i) <$$

$$< v_1 \left(u_1 v_1^{-1} \left(1 + \frac{v_2}{v_1} + \cdots + \frac{v_i}{v_1} \right)^{-1} - 1 \right) <$$

$$< v_1 \left(1 + \frac{v_2}{v_1} + \cdots + \frac{v_i}{v_1} \right) \left(u_1 v_1^{-1} \left(1 + \frac{v_2}{v_1} + \cdots + \frac{v_i}{v_1} \right)^{-1} - 1 \right).$$

The above inequality together with

$$v_1 \left(1 + \frac{v_2}{v_1} + \cdots + \frac{v_i}{v_1} \right) \left(u_1 v_1^{-1} \left(1 + \frac{v_2}{v_1} + \cdots + \frac{v_i}{v_1} \right)^{-1} - 1 \right) =$$

$$= u_1 - v_1 - \cdots - v_i < t v_{i+1}$$

obtained from (2.23), implies the inequality

$$\begin{aligned} \frac{v_1}{v_{i+1}} &< \exp\left(\log t + (2i+1)(\log t)(c_{22}(1+\log B))^i \right) \\ &< \exp\left((2i+2)(\log t)(c_{22}(1+\log B))^i \right), \end{aligned}$$

which completes the induction step. Hence, our claim (2.21) follows. Now note that either $B = \beta_1$ or $B \in \{\alpha_1, \ldots, \alpha_\ell\}$. In the latter case we have $2^B \leq n \leq t q^{\beta_1}$, so $\beta_1 \geq c_{24} B - c_{25} \log t$, where $c_{24} := \log 2 / \log q$ and $c_{25} := 1/\log q$. Since $q \geq 2$, it follows that the inequality

$$\beta_1 \geq c_{24} B - c_{25} \log t$$

holds both when $B = \beta_1$ and when $B \in \{\alpha_1, \ldots, \alpha_\ell\}$.

Furthermore, $\log n/\log(p_1 \cdots p_\ell) \le B \le \log n/\log 2$ showing that

$$\log\log n - c_{26} \le \log B \le \log\log n + c_{27}, \tag{2.24}$$

where $c_{26} := \log\log\max\{3, p_1 \dots p_\ell\}$ and $c_{27} := -\log\log 2$. Note that since $q \notin \{p_1, \dots, p_\ell\}$, it follows that $v_t = 1$. Setting $j = t$ in (2.21) and taking logarithms we get

$$c_{24}B - c_{25}\log t \le \beta_1 \le c_{28} t \log t (c_{22}(1 + \log B))^{t-1}, \tag{2.25}$$

where we can take $c_{28} := \max\{1, 2(\log q)^{-1}\}$. If the left-hand side of (2.25) is smaller than $c_{24}B/2$, we get that

$$\log t > c_{29}B,$$

where $c_{29} := c_{24}/(2c_{25})$, therefore

$$t > e^{c_{29}B} > n^{c_{30}},$$

where $c_{30} := c_{29}/\log(p_1 \cdots p_\ell)$, which for large n is better than the inequality we are after. If the left-hand side of (2.25) is at least $c_{24}B/2$, then by taking logarithms we get

$$\log B - c_{31} < (t-1)\log(c_{22}(1 + \log B)) + \log t + \log\log t,$$

where $c_{31} := -\log(c_{24}/2) + \log c_{28}$. From here, we immediately get

$$t > (1 + o(1))\frac{\log B}{\log\log B}$$

as $B \to \infty$. Combining this with (2.24), we get that for every $\varepsilon > 0$, taking $c_{32} := 1 - \varepsilon$, the inequality

$$t > c_{32} \frac{\log \log n}{\log \log \log n}$$

holds for all $n > n_0(\varepsilon)$, where $n_0(\varepsilon)$ is effectively computable in terms of ε and $p_1, \ldots, p_\ell, q$. Hence, the statement follows. □

2.3 Representation of terms of binary recurrence sequences as linear combinations of prime powers

In this section we consider the problem of representation of terms of binary recurrence sequences as linear combinations of prime powers. We present some theoretical results and in a different section we will give numerical examples as well. To start off we need to introduce some notations. The sequence $U_n = U_n(A, B, U_0, U_1)$ is called a binary linear recurrence sequence if the relation

$$U_n = AU_{n-1} + BU_{n-2} \ (n \geq 2) \tag{2.26}$$

holds, where A, B, U_0, U_1 are fixed integers with $AB \neq 0$ and $|U_0| + |U_1| > 0$. The polynomial $f(x) = x^2 - Ax - B$ is called the companion polynomial of the sequence U_n. Let $D = A^2 + 4B$ be the discriminant of f. We call D the discriminant of the sequence U_n. The roots of the companion polynomial are denoted by α and β. From now on we shall always assume that $|\alpha| \geq |\beta|$. Using this notation, if $D \neq 0$ then as it is well known, we can write

$$U_n = \frac{a\alpha^n - b\beta^n}{\alpha - \beta} \tag{2.27}$$

for $n \geq 0$, where $a = U_1 - U_0\beta$ and $b = U_1 - U_0\alpha$. Note that $\alpha - \beta = \sqrt{D}$. The sequence U_n is called *non-degenerate*, if $ab\alpha\beta \neq 0$ and α/β is not a root of unity.

Let $b_1, \ldots, b_s$ be fixed integers, and $p_1, \ldots, p_s$ be given primes. In this section, under certain assumptions, we give a general finiteness result for the solutions of the equation

$$U_n = b_1 p_1^{x_1} + \cdots + b_s p_s^{x_s} \tag{2.28}$$

in non-negative integers $n, x_1, \ldots, x_s$. It is important to note that in our results we do not require the primes to be distinct; in particular it is possible that $p_i = p_j$ for all $1 \leq i, j \leq s$.

Marques and Togbé [50] gave all solutions of equation (2.28) with U_n being the Fibonacci or Lucas sequence, $s = 3$ and $b_1 = b_2 = b_3 = 1$ and $p_1 = 2, p_2 = 3, p_3 = 5$. In their proof they used Baker's method and a further restriction, namely $\max(x_1, x_2, x_3) = x_3$. In their approach, this restriction is unavoidable. Pethő and de Weger [59] gave an algorithm on how to solve explicitly the Diophantine equation $U_n = w p_1^{x_1} \cdot \ldots \cdot p_m^{x_m}$, where U_n is a binary recurrence sequence with positive discriminant.

2.3.1 New results

The first theorem gives an effective upper bound for the number of solutions of (2.28) under certain assumptions. This result (which is Theorem 2.1 in [16]) extends the result of Marques and Togbé [50] in a sense that in our theorem U_n can be an arbitrary non-degenerate binary recurrence sequence and the number of primes on the right hand side of (2.28) can be arbitrary as well. However, this result cannot be used to find all solutions of given equations directly.

Theorem 2.6. *Let U_n be a non-degenerate binary recurrence sequence with a positive discriminant, $p_1 \le p_2 \le \cdots \le p_s$ be given, not necessarily distinct prime numbers and $b_1, \ldots, b_s$ be nonzero integers. Put $T = \max_{1 \le i \le s} |b_i|$. Using the notations from before, assume further that $\log(|a/b_s\sqrt{D}|)$, $\log|\alpha|$ and $\log p_s$ are linearly independent over the rationals.*

Consider the equation

$$U_n = b_1 p_1^{x_1} + b_2 p_2^{x_2} \cdots + b_s p_s^{x_s} \tag{2.29}$$

in non-negative integers $n, x_1, \ldots, x_s$. Let $0 < \varepsilon < 1$, and write H_ε for the set of those solutions $(n, x_1, \ldots, x_s)$, for which $x_s = \max_{1 \le i \le s} x_i$, and $x_i < (1-\varepsilon)x_s$ for those $i = 1, \ldots, s-1$ for which $p_i = p_s$. Then H_ε is finite, and for all $(n, x_1, \ldots, x_s)$ in H_ε we have

$$\max\{n, x_1, \ldots, x_s\} < C_{16},$$

where C_{16} is an effectively computable constant depending only on ε, A, B, U_0, U_1, T, s, p_s.

Remark 4. Obviously, if p_s is greater than all the other primes $p_1, \ldots, p_{s-1}$, then H_ε is independent of ε. Indeed, in this case for any $1 \le i \le s-1$ we have $p_i \ne p_s$, thus the inequality $x_i < (1-\varepsilon)x_s$ is not required.

Remark 5. The condition that $\log(|a/b_s\sqrt{D}|)$, $\log|\alpha|$ and $\log p_s$ are linearly independent over the rationals is necessary. (Though it possibly could be weakened.) This is shown by the following example. Put $A = 5$, $B = -6$, $U_0 = 0$ and $U_1 = 1$. Then $\alpha = 3$, $\beta = 2$, $a = b = \sqrt{D} = 1$ and we have

$$U_n = 3^n - 2^n \quad (n \ge 0).$$

Take $s = 2$, $p_1 = 2$, $p_2 = 3$, $b_1 = -1$ and $b_2 = 1$. Then the equation

$$U_n = b_1 p_1^{x_1} + b_2 p_2^{x_2}$$

has infinitely many solutions given by $(n, x_1, x_2) = (n, n, n)$ $(n \geq 0)$, which belong to H_ε for any ε. Observe that now $\log(|a/b_s\sqrt{D}|)$, $\log|\alpha|$ and $\log p_s$ are linearly dependent over $\mathbb{Q}$, however, all the other conditions of Theorem 2.6 are satisfied.

Furthermore, we would like to point out that the condition that U_n is non-degenerate is also necessary. This is related to the Skolem–Mahler–Lech theorem. Skolem [74] proved that the indices of the zero terms of U_n is the union of a finite set and finitely many arithmetic progressions. (Later, this result has been extended to algebraic number fields by Mahler [49] and to fields of zero characteristic by Lech [46].) In particular, if U_n is non-degenerate, then it contains only finitely many zero terms. So this condition is rather important for our present purposes. Indeed, consider the equation

$$U_n = 5^{x_3} - 3^{x_2} - 2^{x_1}, \tag{2.30}$$

in non-negative integers n, x_1, x_2, x_3 where $U_0 = 0,\ U_1 = 1$ and

$$U_n = U_{n-1} - U_{n-2} \quad (n \geq 2).$$

In this case $A = 1,\ B = -1$. The characteristic roots of U_n are $\alpha = \frac{1-\sqrt{-3}}{2}$ and $\beta = \frac{1+\sqrt{-3}}{2}$, which are roots of unity, hence the sequence is degenerate. In fact, U_n is given by:

$$0,\ 1,\ 1,\ 0,\ -1,\ -1,\ 0,\ 1, \ldots$$

In particular, $U_n = 0$ if $4 \mid n$, so equation (2.30) has infinitely many solutions of the form $(n, x_1, x_2, x_3) = (4t, 1, 1, 1)$. This shows that the criterion that U_n is non-degenerate is necessary, indeed.

2.3.2 Proofs

The main tool to prove Theorem 2.6, is Baker's method. In particular, we shall use Lemma 2.7, due to Matveev [51].

Proof of Theorem 2.6. First, for later use observe that the assumptions imply that

$$|b_1 p_1^{x_1} + \cdots + b_{s-1} p_{s-1}^{x_{s-1}}| = p_s^{x_s} \left| b_1 \frac{p_1^{x_1}}{p_s^{x_s}} + \cdots + b_{s-1} \frac{p_{s-1}^{x_{s-1}}}{p_s^{x_s}} \right| \leq (s-1) T p_s^{(1-\delta_1)x_s}, \tag{2.31}$$

where $T = \max_{1 \leq i \leq s} |b_i|$ and

$$\delta_1 = \min(\varepsilon, 1 - \max_{p_i < p_s} (\log(p_i)/\log(p_s))).$$

If $p_1 = \cdots = p_s$ then we take $\delta_1 = \varepsilon$. Since $D > 0$ and U_n is assumed to be non-degenerate, we have

$$|\alpha| > |\beta|. \tag{2.32}$$

Note that by our assumptions we also have $|\alpha| > 1$. A simple calculation shows that if

$$\left| 1 - \frac{b\beta^n}{a\alpha^n} \right| \leq \frac{1}{2}$$

then n is bounded by a constant depending only on A, B, U_0, U_1. Then since by (2.31) we get that the right hand side of (2.29) tends to infinity as x_s tends to infinity, we obtain that x_s is bounded by a constant depending only on

A, B, U_0, U_1, s, p_s. Hence the statement follows in this case. So we may assume that

$$\left|1 - \frac{b\beta^n}{a\alpha^n}\right| > \frac{1}{2}.$$

Then (2.29) implies that

$$\left|\frac{a\alpha^n}{2\sqrt{D}}\right| < \left|\frac{a\alpha^n}{\sqrt{D}}\right| \left|1 - \frac{b\beta^n}{a\alpha^n}\right| = |U_n| \le sTp_s^{x_s}. \tag{2.33}$$

This gives

$$n \le \frac{\log \frac{2\sqrt{D}sT}{|a|} + x_s \log p_s}{\log |\alpha|}. \tag{2.34}$$

If

$$\log \frac{2\sqrt{D}sT}{|a|} > x_s \log p_s,$$

then the theorem trivially follows. So we may assume the contrary. Then by (2.34) we obtain

$$n \le \frac{2x_s \log p_s}{\log |\alpha|}. \tag{2.35}$$

If $|\beta| > 1$ we need more. In this case, if

$$\log \frac{2\sqrt{D}sT}{|a|} > \frac{x_s \log p_s (\log |\alpha| - \log |\beta|)}{2 \log |\beta|}$$

then the theorem easily follows. So we may assume the opposite. Then by

(2.34) we get

$$n \leq \frac{x_s \log p_s (\log |\alpha| + \log |\beta|)}{2 \log |\alpha| \log |\beta|}. \tag{2.36}$$

Now we rewrite (2.29) as

$$\frac{a}{b_s \sqrt{D}} \alpha^n p_s^{-x_s} - 1 = \frac{b_1 p_1^{x_1} + \cdots + b_{s-1} p_{s-1}^{x_{s-1}} + \frac{b\beta^n}{\sqrt{D}}}{b_s p_s^{x_s}}. \tag{2.37}$$

In the case of $|\beta| \leq 1$ we obviously have

$$\frac{|\beta|^n}{p_s^{x_s}} \leq p_s^{-x_s}.$$

If $|\beta| > 1$, then (2.36) implies

$$\frac{|\beta|^n}{p_s^{x_s}} \leq p_s^{-\delta_2 x_s},$$

where

$$\delta_2 = 1 - \frac{\log |\alpha| + \log |\beta|}{2 \log |\alpha|}.$$

Note that $1 > \delta_2 > 0$. Using the above inequalities together with (2.31), from (2.37) we get

$$|\Lambda| \leq c_{33} p_s^{-\delta x_s},$$

where $\Lambda = \frac{a}{b_s \sqrt{D}} \alpha^n p_s^{-x_s} - 1$, $\delta = \min\{\delta_1, \delta_2\}$ and $c_{33} = (s-1)T + |b|/\sqrt{D}$.

On the other hand, since by the assumption

$$\log \frac{|a|}{|b_s| \sqrt{D}}, \quad \log |\alpha|, \quad \log p_s$$

are linearly independent over the rationals, we have $\Lambda \neq 0$. Hence, in view of (2.35) Lemma 2.7 gives that

$$|\Lambda| > \exp(-c_{34} \log x_s)$$

holds with some constant c_{34} depending only on A, B, U_0, U_1 and p_s.

Combining the upper and lower estimates for $|\Lambda|$, we get an upper bound for x_s in terms of ε, A, B, U_0, U_1, T, s and p_s. Thus by using (2.35) the statement clearly follows. □

3 Exponential Diophantine equations

3.1 Exponential Diophantine equations over $\mathbb{Z}$

Let $a_1, \dots, a_k, b_{11}, \dots, b_{1\ell}, \dots, b_{k1}, \dots, b_{k\ell}$ be fixed non-zero integers and c be a fixed integer. In this section we consider the exponential Diophantine equation

$$a_1 b_{11}^{x_{11}} \dots b_{1\ell}^{x_{1\ell}} + \dots + a_k b_{k1}^{x_{k1}} \dots b_{k\ell}^{x_{k\ell}} = c \tag{3.1}$$

in non-negative integer unknowns $x_{11}, \dots, x_{1\ell}, \dots, x_{k1}, \dots, x_{k\ell}$. This equation has a very rich literature. If $k = 2$, then by using Baker's method we can give an explicit upper bound for the exponents. (This follows from results of Győry [35, 36]; for extensions see e.g. the books [73] and [32], and the references given there.) Thus, in principle, we have an algorithm to find all solutions in this case. This algorithm however usually yields very large bounds for the exponents, thus to be able to actually determine all solutions one needs to use other results (e.g. the Baker–Davenport lemma in [6]) to reduce the size of these bounds. However, if k is at least 3, then this method fails and we have only results which if effective, then require additional restrictions. See for example Vojta [86] who gave an effective method to determine all non-degenerate solutions of S-unit equations in 3 unknown variables if the cardinality of the set S is at most 3. Later Bennett [8] extended this result to the case $k = 4$, but still requiring the necessary condition that $|S| \leq 3$. By using the p-adic subspace theorem of Schmidt and Schlikewei it is possible to determine an upper bound for the number of solutions of S-unit equations in $k \geq 3$ unknowns, but this result does not yield any information regarding the size of these solutions. Our goal in this section is to prove theoretical and nu-

merical results concerning equation (3.1). First we propose a conjecture which is a variant of a classical conjecture of Skolem [75].

Conjecture 1. Suppose that equation (3.1) has no solutions. Then there exists an integer m with $m \geq 2$ such that the congruence

$$a_1 b_{11}^{x_{11}} \dots b_{1\ell}^{x_{1\ell}} + \dots + a_k b_{k1}^{x_{k1}} \dots b_{k\ell}^{x_{k\ell}} \equiv c \pmod{m} \tag{3.2}$$

has no solutions in non-negative integers $x_{11}, \dots, x_{1\ell}, \dots, x_{k1}, \dots, x_{k\ell}$.

The classical conjecture of Skolem (see Schinzel [66]) concerns the equation

$$a_1 b_{11}^{x_1} \dots b_{1\ell}^{x_\ell} + \dots + a_k b_{k1}^{x_1} \dots b_{k\ell}^{x_\ell} = 0$$

thus our conjecture can be considered as a generalization of that one.

In this subsection we show that for any fixed $a_1, \dots, a_k$, $b_{11}, \dots, b_{1\ell}$, $\dots, b_{k1}, \dots, b_{k\ell}$, the set of integers c for which the above conjecture fails, has density zero inside the set of those values c for which equation (3.1) is not solvable. Moreover, the appropriate moduli m can be chosen to have the extra property that they are all divisible by r, for any preliminary chosen non-zero integer r. The main tools in the proof are a variant of a classical result of Erdős, Pomerance and Schmutz [28] concerning small values of Carmichael's λ-function, and a result of Ádám, Hajdu and Luca [1] about the number of values c up to any x, for which equation (3.1) is solvable. Later on, we also give some "numerical evidence" for the conjecture, by checking its validity for a relatively large set of the parameters involved.

At the second part of the subsection we present a method which can be used to solve these types of equations under some assumptions. Namely if we assume that (3.1) has only finitely many solutions then first we find all "small" solutions, then based on this list we transform the initial equation into

a new one which (presumably) has no solutions. After this step if we take this new equation and suppose that Conjecture 1 is true then our method makes it possible to find a modulus m such that the congruence (3.2) has no solutions modulo m. If we succeed, then we get an upper bound for at least one of the variables in our original equation. It is important to note that this method works if the left hand side of (3.1) has no vanishing subsums (since in this case we may have infinitely many solutions). At the end of this section we give some concrete examples as well to demonstrate our method. Later on, in Section 4 we give some applications, as well.

3.1.1 New results

First we show that Conjecture 1 is true for "almost all" cases. The next theorem is Theorem 2.1 in Bertók and Hajdu [12].

Theorem 3.1. *Let $a_1, \dots, a_k, b_{11}, \dots, b_{1\ell}, \dots, b_{k1}, \dots, b_{k\ell}$ be fixed, and let H be the set of right hand sides in* (3.1) *for which Conjecture 1 is violated, that is*

$$H = \{c \in \mathbb{Z} \ : \ \text{(3.1) } \textit{is not solvable, but} \text{ (3.2) } \textit{is solvable for all } m\}.$$

Then H has density zero inside the set

$$H_0 = \{c \in \mathbb{Z} \ : \ \text{(3.1) } \textit{is not solvable}\}.$$

We also give some numerical evidence (which is Theorem 2.3 in Bertók and Hajdu [12]) which strengthens Conjecture 1.

Theorem 3.2. *Let c be an integer with $0 \leq c \leq 1000$. Then Conjecture 1 is valid for the following cases of equation* (3.1)*:*

(1) $p_1^{x_1} - p_2^{x_2} = c$ *and* $p_1^{x_1} + p_2^{x_2} - p_3^{x_3} = c$ *where* p_1, p_2, p_3 *are distinct primes less than* 100*,*

(2) $p_1^{x_1} + \cdots + p_{t-1}^{x_{t-1}} - p_t^{x_t} = c$ *where* $p_1 < \cdots < p_t$ *are primes less than* 30 *with* $4 \leq t \leq 8$*,*

(3) $p_1^{x_1} p_2^{x_2} + p_3^{x_3} p_4^{x_4} - p_5^{x_5} p_6^{x_6} = c$ *where* $p_1, p_2, p_3, p_4, p_5, p_6$ *is a permutation of the primes* $2, 3, 5, 7, 11, 13$*,*

(4) $2^{x_1} + 3^{x_2} + 5^{x_3} + 7^{x_4} + 11^{x_5} + 13^{x_6} + 17^{x_7} + 19^{x_8} - 23^{x_9} = 55191.$

Remark 6. The number 55191 in the last equation of Theorem 3.2 is special, since for every number which is smaller than 55191 the equation has at least one solution, so in fact 55191 is the first number for which the equation has no solutions.

3.1.2 An algorithm for solving exponential Diophantine equations

In this section we present a heuristic algorithm which can be used to solve equations of type (3.1). This algorithm allows us to find all solutions of exponential Diophantine equations regardless of the number of terms. As it was mentioned before, we have an algorithm (based upon Baker's method) to find all solutions only when the number of the terms on the left hand side of equation (3.1) is 2 (or under some further restrictrictions 3 or 4, see Vojta [86] and Bennett [8]). Thus our algorithm is much more general than these methods.

Suppose that in equation (3.1) both the coefficients a_i $(1 \leq i \leq k)$, the bases b_{ij} $(1 \leq i \leq k, 1 \leq j \leq \ell)$ and the constant c on the right hand side are all fixed. We also suppose that the equation has only finitely many solutions. This is the case when the equation has no solutions with vanishing subsums.

Otherwise (since we work locally) it is not possible to find all solutions in general by using this method.

The algorithm consists of four steps, namely:

(I) Find all solutions to equation (3.1) by an exhaustive search. [Note: Of course, the search can provide only a suspected list of solutions. However, heuristically we can be "sure" that we have found all solutions.]

(II) Choose any of the unknowns, x_{11} say, and based upon the suspected list of solutions find an integer x_0 such that this number is larger than any of the solutions for x_{11}. [Note: by choosing more than one unknowns we can speed up the calculations, but this modification has no theoretical significance.]

(III) Instead of equation (3.1) consider the equation obtained from (3.1) by replacing the coefficient a_1 by $a_1 b_{11}^{x_0}$. [Note: by the choice of x_0, we expect that the new equation has no solutions.]

(IV) Find an m such that the new equation has no solution already modulo m. [Note: If Conjecture 1 is true, such a modulus exists. One can try to find an appropriate m by the help of Lemma 2.4. Observe that for the unsolvability of the congruence modulo m the relation $b_{11}^{x_0} \mid m$ should hold, hence the importance of the divisibility property comes from.]

Later in this section we will provide some numerical results which demonstrates the efficiency of our algorithm. For now we only give a very simple example which helps to understand how this method works.

Suppose that we want to solve the equation

$$5^x - 2^y - 3^z = 23,$$

in $x, y, z \in \mathbb{N} \cup \{0\}$. Based on a simple search, say we try every integer between 0 and 100 for x, y and z, we find that the only solution in this range is $(x, y, z) = (2, 0, 0)$. Heuristically we are "sure" that no other solutions exist and by using our method we try to prove this. Since in the solution we found the exponent of 2 is 0, instead of the original equation, consider the modified equation

$$5^x - 2 \cdot 2^{y_0} - 3^z = 23,$$

where x, y_0, z are in $\mathbb{N} \cup \{0\}$. If the assumptions are correct then this new equation has no solutions. By choosing m to be 2 we can immediately see that the modified equation has no solutions modulo m, which means that the exponent of 2 is 0 indeed. By using this new information we can get rid of one of the unknowns and get the equation

$$5^x - 3^z = 24.$$

By a similar argument as before we can write

$$5^x - 3 \cdot 3^{z_0} = 24,$$

where x and z_0 are non-negative integers, suspecting that this equation has no solutions. If we take m to be 3 we can immediately see that this equation has no solutions modulo m (since the left hand side cannot be 0 modulo 3). This means we were able to show that $z = 0$, thus we got rid of one more variable. The remaining equation is $5^x = 25$ which gives $x = 2$.

As we mentioned before, this example is a very easy one, but it was perfect to demonstrate the steps of our algorithm.

An interesting and important question may occur though: how did we find the moduli $m = 2$ and $m = 3$? In this specific case it was quite easy, since the

exercise was "made to be nice", but for harder equations guessing the moduli will not work. One possible way to find the modulus is to use Lemma 2.4. Later on we will discuss this problem in more details.

It is of utmost importance to emphasize that although at the start of the procedure we could not be sure that the solution(s) what we found are the only solution(s), but during the process we were able to fix the unknown variables one by one. Thus if somehow we can find an appropriate modulus m then we can be sure that we found every solution.

This strategy works, at least in principle, if there exists a constant A, such that for all solutions of (3.1) we have $\min_{1\le i\le k, 1\le j\le \ell} x_{ij} < A$. This is the case, for example, if (3.1) has no solutions with vanishing subsum.

At this point we mention that one can find in the literature several sparse results of this type; see e.g. the papers [20, 2, 3] and the references there. However, in these papers the appropriate moduli are found in a rather ad-hoc way (just how we did in the example above), at least no clear strategy is explained to choose them. In our results we could use the moduli provided by Lemma 2.4. We give an explanation in the proofs of the forthcoming theorems.

Now we give some theorems which show how the algorithm works. The first result (which is Theorem 3.1 in our paper [12]) concerns the representation of zero as the sum and difference of powers of several distinct primes. Note that this result is closely related to a question of Brenner and Foster [20].

Theorem 3.3.

1. *Let* $2 \le t \le 5$ *and let* $p_1, \dots, p_{t+1}$ *be distinct primes, with* $p_i \le 19$ $(i = 1, \dots, t+1)$. *Consider the Diophantine equations*

$$\sum_{i=1}^{t} p_i^{x_i} = p_{t+1}^{x_{t+1}}.$$

For all the solutions of these equations we have $\min_{1\le i\le t+1}(x_i) \le 15$.

2. *The Diophantine equation*

$$3^{x_1} + 5^{x_2} + 11^{x_3} + 13^{x_4} + 17^{x_5} = 19^y$$

has only two solutions in $(x_1, x_2, x_3, x_4, x_5, y)$*, given by*

$$(x_1, x_2, x_3, x_4, x_5, y) = (0, 1, 1, 0, 0, 1), (1, 0, 0, 1, 0, 1).$$

The next theorem (Theorem 3.2 in Bertók and Hajdu [12]) concerns the case where the primes on the left hand side are the same.

Theorem 3.4.

1. *Let* $2 \le t \le 8$ *and let* p, q *be distinct primes with* $p, q \le 19$ *and consider the Diophantine equations*

$$\sum_{i=1}^{t} p^{x_i} = q^y - 1.$$

For all the solutions of these equations we have $\min_{1\le i\le t}(x_i, y) \le 6$.

2. *The Diophantine equation*

$$5^{x_1} + 5^{x_2} + 5^{x_3} + 5^{x_4} + 5^{x_5} + 5^{x_6} + 5^{x_7} + 5^{x_8} + 5^{x_9} = 17^y$$

has only two solutions with $x_i \le x_{i+1}$ $(i = 1, \ldots, 8)$*, namely*

$$\begin{aligned}(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, y) =& (0, 0, 0, 0, 0, 0, 0, 1, 1, 1),\\ & (0, 0, 0, 0, 1, 1, 2, 3, 3, 2).\end{aligned}$$

The final result in connection with (3.1) concerns the case where $l = 2$. This is Theorem 3.3 in our paper [12].

Theorem 3.5.

1. *Let $p_1, \ldots, p_6$ be distinct primes with $p_i \leq 19$ $(i = 1, \ldots, 6)$ and consider the Diophantine equations*

$$p_1^{x_1} p_2^{x_2} + p_3^{x_3} p_4^{x_4} - p_5^{x_5} p_6^{x_6} = 1.$$

   For all the solutions of these equations we have $\min_{1 \leq i \leq 6}(x_i) \leq 5$.

2. *The Diophantine equation*

$$2^{x_1} 3^{x_2} + 5^{x_3} 7^{x_4} - 11^{x_5} 13^{x_6} = 1$$

   has only two solutions in $(x_1, x_2, x_3, x_4, x_5, x_6)$, namely

$$(x_1, x_2, x_3, x_4, x_5, x_6) = (0, 0, 0, 0, 0, 0), (0, 2, 1, 0, 0, 1).$$

3.1.3 Proofs

We start with the proof of Theorem 3.1. For this, beside Lemma 2.4 we need the following two results of Ádám, Hajdu and Luca [1].

Lemma 3.1. *Using the notation of Theorem 3.1, write $H_0(x)$ for the elements h of H_0 with $|h| \leq x$ where x is a positive real number. Then for all large x we have*

$$\#H_0(x) > 2x - C_{17}(\log x)^{C_{18}}$$

where C_{17} and C_{18} are constants depending only on the parameters k, a_i and b_{ij} occurring in (3.1).

Proof. The statement is a simple consequence of Theorem 1 of [1]. □

Lemma 3.2. *Let $m = q_1^{x_1} \cdots q_z^{x_z}$ where $q_1, \ldots, q_z$ are distinct primes, and let $b \in \mathbb{Z}$. Then we have*

$$\#\{b^u \pmod m : u \geq 0\} \leq \lambda(m) + \max_{1 \leq i \leq z} x_i.$$

Proof. The statement is Lemma 1 in [1]. □

We are now ready to prove the theorems.

Proof of Theorem 3.1. For a positive real number x set

$$H(x) := \{h \in H : |h| \leq x\} \quad \text{and} \quad H_0(x) := \{h \in H_0 : |h| \leq x\}.$$

We apply Lemma 3.2 and Lemma 2.4 with $r = 1$ to prove our statement. Partly we follow the argument of Theorem 1 of [39]; see also the proof of Theorem 3 in [1].

By Lemma 2.4 we can choose an integer m, satisfying

$$\lambda(m) < (\log m)^{C_{10} \log\log\log m}.$$

We may assume that m is the largest integer below $\sqrt{x}$ with this property. Then by Lemma 2.4 we have that $m > f(x)$, with some strictly monotone increasing function f of x, tending to infinity as x goes to infinity.

Let $m = q_1^{x_1} \cdots q_z^{x_z}$ be the prime factorization of m, where $q_1, \ldots, q_z$ are distinct primes and $x_1, \ldots, x_z$ are positive integers. Write $C(m)$ for the residue classes of those integers c modulo m for which the congruence (3.2) is solv-

able. Lemma 3.2 implies that we have

$$\#C(m) \leq (\lambda(m) + \max_{1\leq i\leq z} x_i)^{k\ell}. \tag{3.3}$$

On the other hand, we easily obtain that

$$\lambda(m) + \max_{1\leq i\leq z} x_i \leq \frac{\log m}{\log 2} + (\log m)^{c_{35}\log\log\log m}. \tag{3.4}$$

Now by inequalities (3.3) and (3.4) we get that

$$\#C(m) < (\log m)^{c_{36}\log\log\log m}, \tag{3.5}$$

where c_{36} is a constant depending only on k and ℓ.

Write now $x = um + v$ where u is a positive integer and v is a positive real number with $v < m$. Observe that by the choice of m, u and v here we have that

$$\log u \geq (\log(u+1))/2 \geq (\log x - \log m)/2 \geq (\log x)/4.$$

Assuming that x is large enough, we further have

$$x > 1.5c_{37}(\log x)^{c_{38}}$$

where c_{37} and c_{38} are respectively C_{17} and C_{18} in Lemma 3.1. Let now ε be an arbitrary positive real number. Then, assuming that x is large enough, the above inequalities imply

$$\varepsilon x/3 > c_{37}(\log x)^{c_{38}}/2,$$

and

$$\varepsilon x/3 \geq \varepsilon um/3 > m > v.$$

Finally, the lower bound $m > f(x)$ also gives

$$\varepsilon x/3 \geq \varepsilon um/3 > u(\log m)^{c_{36} \log\log\log m}$$

provided that x is large enough. Thus, since by (3.5) we have that

$$\#H(x) \leq 2(u(\log m)^{c_{36} \log\log\log m} + v),$$

the statement immediately follows by comparing $\#H_0(x)$ and $\#H(x)$. □

Proof of Theorem 3.2. Since the proofs of the parts (1) to (4) are similar, we only give details in case of (3). Also, here we consider only the equations

$$2^{x_1}3^{x_2} + 5^{x_3}7^{x_4} - 11^{x_5}13^{x_6} = c \tag{3.6}$$

with $0 \leq c \leq 1000$. First, letting the exponents x_i $(i = 1, \ldots, 6)$ vary between 0 and 100, we find a list L (with $\#L = 224$) of c values for which we expect equation (3.6) not to have solutions. (Note that in this case we could not find solutions already with $0 \leq x_i \leq 10$ $(i = 1, \ldots, 6)$, however, some other equations in (3) do have solutions with $\max_{1 \leq i \leq 6} x_i = 12$.) At this stage, at least we are certain that for integers c with $0 \leq c \leq 1000$ not in the list L, equation (3.6) is solvable. Now we investigate the values $c \in L$ one by one. The smallest such value is $c = 11$, we shall work only with this, the others can be handled similarly. Take the modulus

$$m := 7031324575728 = 2^4 \cdot 3^2 \cdot 17 \cdot 19 \cdot 37 \cdot 73 \cdot 97 \cdot 577.$$

Now we could simply say that as one can easily check, equation (3.6) has no solutions modulo m. However, as this check is not that easy for some of the

instances in (1) to (4), it is worth to do it in a sophisticated way. (In particular, since the appropriate modulus m in some other cases can be much larger than the one given above.)

First observe that all the factors of m have λ values composed exclusively of 2-s and 3-s. (This is the choice indicated by the proof of Erdős, Pomerance and Schmutz [28].) This makes it possible to combine the information obtained for the exponents $x_1, \dots, x_6$ modulo the separate factors. (It is highly not economic to work with m as a modulus directly.) For example, modulo 16 we immediately get that $x_1 = 0$ must hold, and we also get some congruence conditions for the other exponents, modulo a power of 2 (since the orders of all the factors modulo 16 are certainly powers of 2). Finally, using all the factors as modulus, the resulting system of congruences proves to be non-solvable, which shows that equation (3.6) has no solutions indeed modulo m.

In all the other cases the proof goes along the same lines. As we mentioned, in some cases one really needs to work with huge moduli. However, in all cases we encountered the modulus

$$m = 2^4 \cdot 3^2 \cdot \prod_{\substack{p-1=2^u 3^v 5^w \\ 3<p<20000}} p$$

proved to be appropriate. The calculations have been performed by the program package Magma [19]. □

Now we turn to the proofs of Theorems 3.3, 3.4, 3.5. These statements have similar structures: they contain a "general" statement, and a "particular" one. As we shall see, the proofs will deal only with the second parts of these statements. The reason is twofold. On the one hand, the proofs of the "general" statements would be rather similar to the those of the "particular" ones. On

the other hand, giving the proofs of the first parts as well, would considerably increase the length of the dissertation. (Indeed, already the proofs of the second parts are rather detailed and lengthy.)

Proof of Theorem 3.3. To prove the theorem we use a program written in Sage [77]. We only prove the second statement, the first part can be proved similarly. First we find all solutions of the equation

$$3^{x_1} + 5^{x_2} + 11^{x_3} + 13^{x_4} + 17^{x_5} = 19^{y} \tag{3.7}$$

with $x_1, \dots, x_5, y < 15$. By doing this we get two solutions, namely $(0, 1, 1, 0, 0, 1)$ and $(1, 0, 0, 1, 0, 1)$. Let us assume that there are no more solutions and instead of (3.7) consider the equation

$$3^2 \cdot 3^{x_{1,0}} + 5 \cdot 5^{x_{2,0}} + 11^{x_3} + 13 \cdot 13^{x_{4,0}} + 17 \cdot 17^{x_{5,0}} = 19 \cdot 19^{y_0}. \tag{3.8}$$

Before we move on to the next step, we comment a few words about the above equation. In our algorithm we mentioned that after we find "all" small solutions we choose one of the exponents and try to give an upper bound for it. However, in this equation we chose multiple exponents at the same time. This step has no theoretical significance, however in most cases it can speed up the computations. After concluding that the new equation has no solutions for some modulus m we get multiple restrictions for the exponents which yields us many sets of equations which need to be considered in a similar way. Another important note is that we found out that the exponent of 19 can be 1, however we only used $19 \cdot 19^{y_0}$ instead of $19^2 \cdot 19^{y_0}$ in the above equation (and similarly we used $5 \cdot 5^{x_{2,0}}$ instead of $5^2 \cdot 5^{x_{2,0}}$, 11^{x_3} instead of $11^2 \cdot 11^{x_{3,0}}$ and $13 \cdot 13^{x_{4,0}}$ instead of $13^2 \cdot 13^{x_{4,0}}$). We did this because the λ values of $5, 13$ and 19 are "small", thus they can rule out quite a few equations. However, we found that

11 is not a good modulus, thus we tried to avoid using that number. So in the first step we were not trying to bound the exponents of $5, 13$ and 19, instead we were focusing on 3 and 17 and we just simply used the other numbers as part of our moduli. This may lead us to some extra equations without solutions (see the last equation below), but since this step speeds up the computations, it is worth to have a few extra equations which can be handled quite easily.

If we determined all solutions of (3.7) correctly, then (3.8) has no solutions. To prove it we have to find a modulus m such that the congruence

$$3^2 \cdot 3^{x_{1,0}} + 5 \cdot 5^{x_{2,0}} + 11^{x_3} + 13 \cdot 13^{x_{4,0}} + 17 \cdot 17^{x_{5,0}} \equiv 19 \cdot 19^{y_0} \pmod{m}$$

has no solutions. By using Lemma 2.4 we are able to find such modulus. Let

$$A = \{2, 5, 7, 9, 13, 17, 19, 37, 73, 97, 109, 163, 193, 257, 769\}.$$

By examining the congruence mod m^* for all $m^* \in A$ and comparing the results we find that it has no solutions, thus $m = \prod_{m^* \in A} m^* = 469692490871958086293470$ is an appropriate modulus. This means that (3.7) has no such solutions where $x_1 > 1$ and $x_2 > 0$ and $x_4 > 0$ and $x_5 > 0$ and $y > 0$ simultaneously. This yields us six new equations, namely

$$\begin{aligned}
5^{x_2} + 11^{x_3} + 13^{x_4} + 17^{x_5} &= 19^y - 1 \\
5^{x_2} + 11^{x_3} + 13^{x_4} + 17^{x_5} &= 19^y - 3 \\
3^{x_1} + 11^{x_3} + 13^{x_4} + 17^{x_5} &= 19^y - 1 \\
3^{x_1} + 5^{x_2} + 11^{x_3} + 17^{x_5} &= 19^y - 1 \\
3^{x_1} + 5^{x_2} + 11^{x_3} + 13^{x_4} &= 19^y - 1 \\
3^{x_1} + 5^{x_2} + 11^{x_3} + 13^{x_4} + 17^{x_5} &= 1.
\end{aligned}$$

We only solve the first one, because the next four can be solved similarly and the last one is trivial. The mentioned equation has only one "small" solution, which is $(1, 1, 0, 0, 1)$, thus we suspect that if the conjecture is true then there exists a modulus m such that the congruence

$$5 \cdot 5^{x_{2,0}} + 11^{x_3} + 13 \cdot 13^{x_{4,0}} + 17^{x_5} \equiv 19^y - 1 \pmod{m}$$

has no solutions modulo m. Similarly as before, the reason for using $5 \cdot 5^{x_{2,0}}$ instead of $5^2 \cdot 5^{x_{2,0}}$ is that we used 5 as part of our modulus because of its good λ value and not because we tried to bound the exponent for x_2. Let now

$$A = \{2, 3, 5, 7, 13, 37, 73, 97, 109, 163, 193, 257, 769\}$$

and examine this congruence for every modulus m^*, where $m^* \in A$. By doing that we find that the congruence has no solutions with $m = \prod_{m^* \in A} m^* = 484718772829678107630$. So we conclude that there are no solutions with $x_2 > 0$ and $x_4 > 0$ simultaneously, which means that we were able to reduce the number of unknowns by one. The remaining cases are

$$11^{x_3} + 13^{x_4} + 17^{x_5} = 19^y - 2$$
$$5^{x_2} + 11^{x_3} + 17^{x_5} = 19^y - 2.$$

The first equation has no solutions modulo

$$m = 2 \cdot 3 \cdot 7 \cdot 37 \cdot 73 \cdot 97 \cdot 109 \cdot 163 \cdot 193 \cdot 257 \cdot 433 = 4198924249980006414,$$

and because $\gcd(m, 11, 13, 17, 19) = 1$ this branch will not give us new equations. The second one however has one "small" solution, which is $(1, 1, 0, 1)$.

If we consider the congruence

$$5^{x_2} + 11^{x_3} + 17 \cdot 17^{x_{5,0}} \equiv 19^y - 2 \pmod{m}$$

with $m = 2 \cdot 3 \cdot 7 \cdot 17 \cdot 37 \cdot 73 \cdot 97 \cdot 109 \cdot 163$ then we find that it has no solutions, so $x_5 = 0$ and the remaining equation is

$$5^{x_2} + 11^{x_3} = 19^y - 3$$

which still has one "small" solution, which is $(1, 1, 1)$. If our assumptions are correct, then the congruence

$$5^2 \cdot 5^{x_{2,0}} + 11^{x_3} \equiv 19^y - 3 \pmod{m}$$

has no solutions with some m. By choosing $m = 2^5 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 31$ this is true, thus $x_2 < 2$ which yields two new equations

$$11^{x_3} = 19^y - 4$$
$$11^{x_3} = 19^y - 8.$$

The first one does not have any solutions modulo 3, and by choosing $m = 2^6 \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 11^2 \cdot 17 \cdot 23 \cdot 31 \cdot 37 \cdot 43 \cdot 61$, the congruence

$$11^2 \cdot 11^{x_{3,0}} = 19^y - 8 \pmod{m}$$

has no solutions either. This means that $x_3 = 0$ or $x_3 = 1$. If $x_3 = 0$ then the resulting Diophantine equation is not solvable, but if $x_3 = 1$ then we get one of the solutions, which is $(x_1, x_2, x_3, x_4, x_5, y) = (0, 1, 1, 0, 0, 1)$. By following the same argument we can solve the remaining four non-trivial equations and

get all the solutions. □

Proof of Theorem 3.4. We only prove the second part, since the first statement of the theorem can be handled similarly. First observe that if all x_i are greater than 0, then the equation does not have any solutions modulo 5. So we have a new equation:

$$5^{x_1} + 5^{x_2} + 5^{x_3} + 5^{x_4} + 5^{x_5} + 5^{x_6} + 5^{x_7} + 5^{x_8} = 17^y - 1.$$

After finding the "small" solutions (which are the suspected solutions) choose $m = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 19 \cdot 37 \cdot 109 \cdot 163$ and consider the congruence

$$5 \cdot (5^{x_1'} + 5^{x_2'} + 5^{x_3'} + 5^{x_4'} + 5^{x_5'} + 5^{x_6'} + 5^{x_7'} + 5^{x_8'}) \equiv 17^y - 1 \pmod{m}.$$

This congruence has no solutions, which means that at least x_1 has to be 0, so the new equation is

$$5^{x_2} + 5^{x_3} + 5^{x_4} + 5^{x_5} + 5^{x_6} + 5^{x_7} + 5^{x_8} = 17^y - 2.$$

If our assumption is correct, then in this equation $x_8 \leq 3$ and $x_2 = 0$. If we choose $m = 2 \cdot 3 \cdot 5^3 \cdot 7 \cdot 13 \cdot 19 \cdot 37 \cdot 109$ then the congruence

$$5^3 \cdot (5^{x_2'} + 5^{x_3'} + 5^{x_4'} + 5^{x_5'} + 5^{x_6'} + 5^{x_7'} + 5^{x_8'}) \equiv 17^y - 2 \pmod{m}.$$

has no solutions, so at least x_2 has to be smaller than 3. Thus we have three

new equations, namely

$$5^{x_3} + 5^{x_4} + 5^{x_5} + 5^{x_6} + 5^{x_7} + 5^{x_8} = 17^y - 3,$$
$$5^{x_3} + 5^{x_4} + 5^{x_5} + 5^{x_6} + 5^{x_7} + 5^{x_8} = 17^y - 7,$$
$$5^{x_3} + 5^{x_4} + 5^{x_5} + 5^{x_6} + 5^{x_7} + 5^{x_8} = 17^y - 27.$$

We only solve the first one, the method for the other two is similar. This equation has one "small" solution, which is $(0, 0, 0, 0, 1, 1, 1)$. Let $m = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 19 \cdot 37 \cdot 109$ and consider the congruence

$$5 \cdot (5^{x_3'} + 5^{x_4'} + 5^{x_5'} + 5^{x_6'} + 5^{x_7'} + 5^{x_8'}) \equiv 17^y - 3 \pmod{m}.$$

Since this does not have any solutions, we can take $x_3 = 0$. By using the same steps as above and the same m we get that $x_4 = 0$ too, thus the equation simplifies to

$$5^{x_5} + 5^{x_6} + 5^{x_7} + 5^{x_8} = 17^y - 5.$$

Of course it can be seen modulo 5 that in this case x_5 has to be 0 too, so the remaining equation is

$$5^{x_6} + 5^{x_7} + 5^{x_8} = 17^y - 6$$

which has only one small solution, given by $(0, 1, 1, 1)$. If $m = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 19 \cdot 37 \cdot 109$ then the congruence

$$5 \cdot (5^{x_6'} + 5^{x_7'} + 5^{x_8'}) \equiv 17^y - 6 \pmod{m}$$

does not have any solutions. So $x_6 = 0$ and the implied equation is

$$5^{x_7} + 5^{x_8} = 17^y - 7.$$

Similarly, if we let m to be $2 \cdot 3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 19 \cdot 41$ then

$$5^2 \cdot (5^{x'_7} + 5^{x'_8}) \equiv 17^y - 7 \pmod{m}$$

is not solvable, so we have two new equations:

$$5^{x_8} = 17^y - 8$$
$$5^{x_8} = 17^y - 12.$$

The first one does not have any solutions at all, which can be seen modulo $2 \cdot 3 \cdot 7 \cdot 13$. Let $m = 2 \cdot 3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$. Then the congruence

$$5^2 \cdot 5^{x'_8} \equiv 17^y - 12 \pmod{m}$$

has no solutions, which means that either $x_8 = 0$ or $x_8 = 1$. If $x_8 = 0$ then there are no solutions and if $x_8 = 1$ then we get the only solution $(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, y) = (0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$. By solving the remaining equations similarly, the proof is complete. □

Proof of Theorem 3.5. Again, we deal only with the second statement. Since its proof is very similar to the previous ones, we only give the list of moduli and the appropriate bounds obtained from the congruences. The base equation is

$$2^{x_1}3^{x_2} + 5^{x_3}7^{x_4} - 11^{x_5}13^{x_6} = 1.$$

1. modulo 2: $x_1 = 0$.

2. modulo $5 \cdot 7 \cdot 13 \cdot 17 \cdot 19 \cdot 37 \cdot 41 \cdot 73 \cdot 97 \cdot 109 \cdot 193$: $x_3 = 0$ or $x_4 = 0$ or $x_6 = 0$. From now on we only consider the case $x_3 = 0$, because the other two can be handled similarly.

3. modulo $13 \cdot 17 \cdot 19 \cdot 37 \cdot 41 \cdot 73 \cdot 97 \cdot 109 \cdot 193$: $x_6 = 0$.

4. modulo 3: $x_2 = 0$.

5. The remaining equation is $7^{x_4} - 11^{x_5} = 0$ which is only solvable, if $x_4 = x_5 = 0$.

The acquired solution in this case is $(x_1, x_2, x_3, x_4, x_5, x_6) = (0, 0, 0, 0, 0, 0)$. Using the same method we can give a bound for the exponents in the first part of the theorem and solve the remaining equations in the second part, thus the proof is complete. □

Remark 7. In the above theorems we used Lemma 2.4 (based upon other results from the literature) to find an appropriate modulus m. We now describe some strategies about how to find an appropriate modulus.

1. If we choose a positive integer m such that for every prime factor p_i of m the number $p_i - 1$ has only "small" prime divisors then $\lambda(m)$ will be "small". A very nice example for this is the number $m = 7031324575728 = 2^4 \cdot 3^2 \cdot 17 \cdot 19 \cdot 37 \cdot 73 \cdot 97 \cdot 577$. It can be seen that for all prime divisors p_i of m, $p_i - 1$ is divisible by at most the primes 2 and 3. For this m the value $\lambda(m)$ is 576 which is quite low compared to the size of m. (This idea is based upon Lemma 2.4 and its predecessors. Note that the modulus m obtained in this way, can be efficient for general bases.)

2. For equations where we have only a few different bases which are fixed (e.g. the second equation from Theorem 3.4) we can use an elementary method to find a good modulus. For the sake of better understanding suppose that in the equation we have lots of v's and w's as bases, thus we want to find a modulus m such that the order of v and w is small modulo m. In this case we can proceed as follows. Take a positive integer A and calculate $m = \gcd(v^A - 1, w^A - 1)$. This number m is a modulus for which the order of v and w are at most A. Of course, in general we need to do this with more than two numbers to get an upper bound for the orders, but the more numbers we involve, the harder it becomes to find a non-trivial m in this way. (Note that in contrast with the above point 1, the modulus m obtained this way is "good" only for specifically v and w.)

We close this subsection with two remarks.

Remark 8. For the actual computations we start with a set consisting of numbers with "small" λ-values. In our applications this set has more than 100 numbers. Then after finding the "small" solutions of the equation in question, we expand this set based on this computation. For example if we find that in every solution of an equation the largest power of say 2 is 17, then we put 2^{18} into this set (sometimes we even use smaller powers of 2 as well, but this only speeds up the computations, it has no theoretical value). Then we find the "best" number m_1 from this set, by which we mean the modulus for which the product of the orders of the bases is the smallest. We then find all solutions of the equation modulo m_1. Based on the solutions we modify the equation and find the next "best" modulus from the list. We continue this method until we either prove that we have no solutions or we have used up all the numbers from the set. In the latter case we were not able to give a bound for any exponent.

This means that either the set of moduli was too small or that we were not able to find all "small" solutions at the beginning (possibly because there is a solution with vanishing subsums).

Remark 9. Another important thing to mention is that based on our theorems and algorithm we are able to find all solutions of a wide variety of exponential Diophantine equations if the equations have only finitely many solutions. Based on results of e.g. Győry and Evertse [32] we know that this is the case if the equation has no solutions with vanishing subsums. If this is not the case then the equation has infinitely many solutions. Thus our method does not work for such equations. However, in some special cases the algorithm can be used to bound the other variables. An easy example for this is the equation

$$2^x - 3^y + 7^z - 7^w = 0$$

in non-negative integers x, y, z, w. It can be seen that we have infinitely many solutions of the shape $(x, y, z, w) = (0, 0, a, a)$, where a is an arbitrary non-negative integer. However, it can also be seen that if $x \geq 1$ then the left side is odd, thus modulo 2 we can conclude that x must be 0. Now if we try to solve the congruence

$$1 \equiv 3^y - 7^z + 7^w \pmod 3,$$

we notice that it has no solutions if $y \geq 1$, which means that $y = 0$, too. So we are left with $7^z = 7^w$ from which we get that $z = w$.

3.2 Exponential Diophantine equations over number fields

In this subsection, we handle a similar problem as in Section 3.1, but instead of working over $\mathbb{Z}$, we now consider exponential Diophantine equations over the ring of integers of an algebraic number field $\mathbb{K}$. From now on let $\mathcal{O}_{\mathbb{K}}$ denote

the ring of integers of $\mathbb{K}$ and let $\alpha_1, \ldots, \alpha_k$, $\beta_{11}, \ldots, \beta_{1\ell}, \ldots, \beta_{k1}, \ldots, \beta_{k\ell}$ be non-zero elements of $\mathbb{K}$ and $\gamma \in \mathbb{K}$. Consider the equation

$$\alpha_1 \beta_{11}^{x_{11}} \ldots \beta_{1\ell}^{x_{1\ell}} + \cdots + \alpha_k \beta_{k1}^{x_{k1}} \ldots \beta_{k\ell}^{x_{k\ell}} = \gamma \tag{3.9}$$

in unknown integers $x_{11}, \ldots, x_{1\ell}, \ldots, x_{k1}, \ldots, x_{k\ell}$. This equation is the analogue of equation (3.1) over number fields. The main difference (apart from not working above $\mathbb{Z}$) is that in (3.9) we do not restrict the exponents to be non-negative integers. However, we can assume this, since we may split (3.9) into several cases, replacing some of the β_{ij} by $1/\beta_{ij}$ to achieve this property. Furthermore, if some β_{ij} is not in $\mathcal{O}_{\mathbb{K}}$, then we can write $\beta_{ij} = \beta'_{ij}/\beta''_{ij}$ with $\beta'_{ij}, \beta''_{ij} \in \mathcal{O}_{\mathbb{K}}$. Then clearing the denominators, we obtain an equation of the form (3.9) again, where the β_{ij} are algebraic integers. Hence, from this point on we shall always assume that all the β_{ij} are in $\mathcal{O}_{\mathbb{K}}$, and that the unknown exponents x_{ij} are all non-negative integers.

Regarding the solutions of equation (3.9) for $k = 2, 3, 4$ one may use similar methods which were mentioned in Section 3.1 (see e.g. results of Győry [35, 36] for $k = 2$ or Vojta [86] and Bennett [8] for $k = 3, 4$; or the book of Evertse and Győry [32]). Also, it is long known that (3.9) has only finitely many solutions for any k for which the left hand side has no vanishing subsum. Furthermore, the number of such solutions can be explicitly bounded in terms of k and ℓ (see e.g. [34], [4] and for several related results [33], [32], and the references given there).

We propose the following conjecture which is the analogue of Conjecture 1 in Section 3.1.

Conjecture 2. Suppose that one of the following two properties hold:

(i) equation (3.9) has no solution in **integers** x_{ij} $(1 \leq i \leq k, 1 \leq j \leq \ell)$,

(ii) none of the β_{ij} $(1 \leq i \leq k, 1 \leq j \leq \ell)$ is a proper unit (i.e. a unit different from roots of unity) in $\mathcal{O}_{\mathbb{K}}$, and equation (3.9) has no solution in non-negative integers x_{ij} $(1 \leq i \leq k, 1 \leq j \leq \ell)$.

Then there exists an ideal $\mathfrak{M}$ in $\mathcal{O}_{\mathbb{K}}$ such that the congruence

$$\alpha_1 \beta_{11}^{x_{11}} \dots \beta_{1\ell}^{x_{1\ell}} + \dots + \alpha_k \beta_{k1}^{x_{k1}} \dots \beta_{k\ell}^{x_{k\ell}} \equiv \gamma \pmod{\mathfrak{M}} \tag{3.10}$$

has no solutions in non-negative integers x_{ij} $(1 \leq i \leq k, 1 \leq j \leq \ell)$.

This conjecture is a variant of a classical conjecture of Skolem [75], but the original formulation of Skolem is not completely precise. For an exact formulation we refer to [66], pp. 398–399. The conjecture predicts a Hasse-type principle for exponential Diophantine equations. Skolem's conjecture has been considered in several papers. Here we only mention those of Schinzel [66, 67, 68], and Bartolome, Bilu and Luca [7] (see also the references therein). Importantly, Theorem 2 of Schinzel [66] also implies that in case of $k = 1$ the conjecture is true.

This conjecture can be considered as an extension of Conjecture 1 from Section 3.1 to the algebraic case. The main difference apart from working over $\mathbb{Z}$ is that in Conjecture 1 it is enough to consider the case when the exponents are non-negative integers. Unfortunately, in the extended conjecture this is not sufficient. To understand the necessity of the extra requirement, let $\mathbb{K} = \mathbb{Q}(\sqrt{2})$, and consider the equation

$$(1 + \sqrt{2})^x + (1 + \sqrt{2})^y = 2\sqrt{2}.$$

As one can easily check, this equation has no solution in non-negative integers x, y. However, the corresponding congruence does have a solution modulo $\mathfrak{M}$, for any ideal $\mathfrak{M}$ in $\mathcal{O}_{\mathbb{K}}$. The reason is that the above equation has

solutions in **integers**, e.g. $(x, y) = (1, -1)$. Since $1 + \sqrt{2}$ is a unit in $\mathcal{O}_{\mathbb{K}}$, we can find a positive integer t such that $(1 + \sqrt{2})^t \equiv 1 \pmod{\mathfrak{M}}$ for any $\mathfrak{M}$. Hence we get

$$(1 + \sqrt{2}) + (1 + \sqrt{2})^{t-1} \equiv 2\sqrt{2} \pmod{\mathfrak{M}}.$$

However, this phenomenon clearly occurs only if one of the numbers β_{ij} is a unit in $\mathcal{O}_{\mathbb{K}}$ - otherwise we may find some modulus $\mathfrak{M}$ such that none of the β_{ij} is invertible modulo $\mathfrak{M}$. Furthermore, if β_{ij} is a root of unity, and its exponent x_{ij} is negative in some solution, then we may clearly replace x_{ij} by a positive integer, to obtain another solution. Thus altogether it seems that the conditions (i) and (ii) may be sufficient to guarantee Conjecture 2 to hold.

In this section we prove similar theorems as in Section 3.1, but for the more general case. We prove among others that for any fixed α_i and β_{ij} $(1 \leq i \leq k, 1 \leq j \leq \ell)$, the set of $\gamma \in \mathcal{O}_{\mathbb{K}}$ for which Conjecture 2 might fail, is "very small". We extend our previous algorithm for solving exponential Diophantine equations over number fields and show how it works by some numerical examples. An interesting property of this algorithm is that under some circumstances we are able to solve equations where neither of the conditions (i) and (ii) in Conjecture 2 is satisfied.

3.2.1 New results

We start with a theorem (which is Theorem 1 from our paper [13]) which yields a good support for Conjecture 2. For any subset L of $\mathcal{O}_{\mathbb{K}}$ and any ideal $\mathfrak{M}$ of $\mathcal{O}_{\mathbb{K}}$, write $L \pmod{\mathfrak{M}}$ for the natural embedding of the set L into $\mathcal{O}_{\mathbb{K}}/\mathfrak{M}\mathcal{O}_{\mathbb{K}}$. Finally, write $N(\mathfrak{M})$ for the norm of the ideal $\mathfrak{M}$ in $\mathcal{O}_{\mathbb{K}}$.

Theorem 3.6. *Let $\alpha_1, \ldots, \alpha_k$, $\beta_{11}, \ldots, \beta_{1\ell}, \ldots, \beta_{k1}, \ldots, \beta_{k\ell}$ be non-zero ele-*

ments of $\mathcal{O}_{\mathbb{K}}$, and put

$$H = \{\alpha_1\beta_{11}^{x_{11}}\dots\beta_{1\ell}^{x_{1\ell}}+\dots+\alpha_k\beta_{k1}^{x_{k1}}\dots\beta_{k\ell}^{x_{k\ell}} : x_{ij} \geq 0\,(1 \leq i \leq k, 1 \leq j \leq \ell)\}.$$

Then for any ideal $\mathfrak{A}$ of $\mathcal{O}_{\mathbb{K}}$ and any $\varepsilon > 0$ there exists an ideal $\mathfrak{M}$ such that $\mathfrak{A} \mid \mathfrak{M}$, and $|H \pmod{\mathfrak{M}}| < N(\mathfrak{M})^{\varepsilon}$.

Remark 10. Choosing ε "very small", the above theorem shows that it is "very unlikely" that (3.9) is not solvable, but the corresponding congruence modulo $\mathfrak{M}$ is solvable. Since for any ε we can choose infinitely many $\mathfrak{M}$, this assertion seems to give a strong support for Conjecture 2 indeed.

Remark 11. The presence of $\mathfrak{A}$ is important to guarantee that some of the β_{ij} will not be invertible modulo $\mathfrak{M}$ (or even, we can make some β_{ij} be zero modulo $\mathfrak{M}$). This will be important later on, in applying the conjecture to find all solutions of (3.9) in the case where it does have solutions.

3.2.2 Lemmas

To give the proof of Theorem 3.6, we need some preparation. For an ideal $\mathfrak{I}$ in $\mathcal{O}_{\mathbb{K}}$, denote by $\varphi(\mathfrak{I})$ the number of invertible elements in $\mathcal{O}_{\mathbb{K}}/\mathfrak{I}$. Note that if $\mathbb{K} = \mathbb{Q}$, then the φ function is Euler's totient function. The following lemma is a well-known property of the φ function; see e.g. Theorem 1.19 on p.23 of Narkiewicz [55].

Lemma 3.3. *Suppose that $\mathfrak{I}$ is an ideal in $\mathcal{O}_{\mathbb{K}}$ with $\mathfrak{I} = \mathfrak{p}_1^{n_1}\dots\mathfrak{p}_k^{n_k}$, where $\mathfrak{p}_1, \dots, \mathfrak{p}_k$ are distinct prime ideals in $\mathcal{O}_{\mathbb{K}}$. Then we have*

$$\varphi(\mathfrak{I}) = N(\mathfrak{p}_1)^{n_1-1}\cdots N(\mathfrak{p}_k)^{n_k-1}(N(\mathfrak{p}_1)-1)\cdots(N(\mathfrak{p}_k)-1),$$

where $N(\mathfrak{I})$ is the norm of $\mathfrak{I}$.

For any ideal $\mathfrak{I}$ in $\mathcal{O}_{\mathbb{K}}$, write

$$\lambda(\mathfrak{I}) := \mathrm{lcm}\{\mathrm{ord}_{\mathfrak{I}}(\alpha) \mid \alpha \in \mathcal{O}_{\mathbb{K}}\,, \alpha \text{ is invertible in } \mathcal{O}_{\mathbb{K}}/\mathfrak{I}\},$$

where $\mathrm{ord}_{\mathfrak{I}}(\alpha)$ is the smallest positive integer t with $\alpha^t \equiv 1 \pmod{\mathfrak{I}}$. Note that if $\mathbb{K} = \mathbb{Q}$, then the λ function coincides with Carmichael's function. Obviously, for any ideal $\mathfrak{I}$, we have $\lambda(\mathfrak{I}) \mid \varphi(\mathfrak{I})$. Furthermore, as it is well-known, see e.g. Laššák and Porubský [45], we have the following assertion.

Lemma 3.4. *Suppose that $\mathfrak{I}$ is an ideal in $\mathcal{O}_{\mathbb{K}}$ with $\mathfrak{I} = \mathfrak{p}_1^{n_1} \dots \mathfrak{p}_k^{n_k}$, where $\mathfrak{p}_1, \dots, \mathfrak{p}_k$ are distinct prime ideals in $\mathcal{O}_{\mathbb{K}}$. Then we have*

$$\lambda(\mathfrak{I}) = \mathrm{lcm}(\lambda(\mathfrak{p}_1^{n_1}), \dots, \lambda(\mathfrak{p}_k^{n_k})).$$

We shall also need the following variant of a result of Erdős, Pomerance and Schmutz [28] concerning small values of Carmichael's function due to Pollack [63]. (For other variants see e.g. [1], [38] and Lemma 2.4.)

Lemma 3.5. *Let $\mathbb{K} = \mathbb{Q}$, and P be a set of primes of positive upper relative density. For each $\kappa > 0$, there are infinitely many square-free natural numbers n which are divisible only by primes in P and which satisfy $\lambda(n) < n^{\kappa}$.*

Combining the above lemmas with certain other assertions, we obtain the following property of the λ function defined over $\mathbb{K}$. Note that this result (Lemma 4 from Bertók and Hajdu [13]) is a kind of extension of the above mentioned results concerning Carmichael's function over algebraic number fields.

Lemma 3.6. *For any $\delta > 0$ and ideal $\mathfrak{A}$ in $\mathcal{O}_{\mathbb{K}}$ there exists an ideal $\mathfrak{M}$ in $\mathcal{O}_{\mathbb{K}}$ such that $\mathfrak{A} \mid \mathfrak{M}$ and $\lambda(\mathfrak{M}) < N(\mathfrak{M})^{\delta}$.*

Proof. To prove the statement, we closely follow arguments of Pollack [63], with small modifications. Let P be the set of those primes p which split completely in $\mathbb{K}$, such that (p) and $\mathfrak{A}$ are coprime ideals in $\mathcal{O}_{\mathbb{K}}$. It follows from Landau's prime ideal theorem [44] that P has positive upper density. Thus applying Lemma 3.5 with this set and some $\kappa > 0$, such that $\kappa < \delta d$, where d is the degree of $\mathbb{K}$, we obtain that there exists a positive integer n of the form $n = p_1 \dots p_k$ where $p_1, \dots, p_k$ are distinct primes from P, such that $\lambda(n) < n^{\kappa}$ and $N(\mathfrak{A})^{1-\delta} < n^{\delta d - \kappa}$. (Here and later on, $\lambda(n)$ is to be understood over $\mathbb{Q}$.) Write $\mathfrak{M} = (n)\mathfrak{A}$ with this n, and let $p_i = \mathfrak{p}_{i1} \dots \mathfrak{p}_{id}$ $(i = 1, \dots, k)$, where the $\mathfrak{p}_{ij}$ are prime ideals in $\mathbb{K}$. Then using Lemmas 3.3 and 3.4 we have

$$\lambda(\mathfrak{M}) \leq \lambda(\mathfrak{A})\mathrm{lcm}(\lambda(\mathfrak{p}_{11}), \dots, \lambda(\mathfrak{p}_{1d}), \dots, \lambda(\mathfrak{p}_{k1}), \dots, \lambda(\mathfrak{p}_{kd})) \leq$$

$$\leq \lambda(\mathfrak{A})\mathrm{lcm}(\varphi(\mathfrak{p}_{11}), \dots, \varphi(\mathfrak{p}_{1d}), \dots, \varphi(\mathfrak{p}_{k1}), \dots, \varphi(\mathfrak{p}_{kd})) =$$

$$= \lambda(\mathfrak{A})\mathrm{lcm}(p_1 - 1, \dots, p_k - 1) = \lambda(\mathfrak{A})\lambda(n) < N(\mathfrak{A})n^{\kappa} < N(\mathfrak{A})^{\delta} n^{\delta d} = N(\mathfrak{M})^{\delta}.$$

This proves the statement. □

In fact, we shall need a statement which shows that for all $\alpha \in \mathcal{O}_{\mathbb{K}}$, the powers of α form a "small" set modulo some $\mathfrak{M}$, and Lemma 3.6 guarantees this only for α with $\gcd((\alpha), \mathfrak{M}) = 1$. To get such a statement, observe that for any ideal $\mathfrak{I}$ in $\mathcal{O}_{\mathbb{K}}$ and $\alpha \in \mathcal{O}_{\mathbb{K}}$ with $\gcd((\alpha), \mathfrak{M}) = 1$, we have

$$\mathrm{ord}_{\mathfrak{I}}(\alpha) = \#\{\alpha^k \pmod{\mathfrak{I}} : k \in \mathbb{Z}\}.$$

We shall use the above notation for any $\alpha \in \mathcal{O}_{\mathbb{K}}$, and further write

$$L(\mathfrak{I}) = \max\{\mathrm{ord}_{\mathfrak{I}}(\alpha) \mid \alpha \in \mathcal{O}_{\mathbb{K}}\}.$$

The next lemma (Lemma 5 from Bertók and Hajdu [13]) provides the necessary extension. Note that similar statements can be found in [37] and in Section 3.1 (over $\mathbb{Z}$).

Lemma 3.7. *Let $\mathfrak{I} = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_\ell^{n_\ell}$ be the prime ideal factorization of an ideal $\mathfrak{I}$ of $\mathcal{O}_\mathbb{K}$, and write $t = \max\{n_1, \ldots, n_\ell\}$. Then for all $\alpha \in \mathcal{O}_\mathbb{K}$ we have $ord_\mathfrak{I}(\alpha) \leq \lambda(\mathfrak{I}) + t$.*

Proof. Write $(\alpha) = \mathfrak{q}_1^{u_1} \cdots \mathfrak{q}_r^{u_r} \cdot \mathfrak{p}_1^{v_1} \cdots \mathfrak{p}_\ell^{v_\ell}$, where the $\mathfrak{q}_i$ are prime ideals with $\mathfrak{q}_i \neq \mathfrak{p}_j$, and the exponents u_i, v_j are non-negative integers. We show that for any $x > \lambda(\mathfrak{I})$ there exists a y with $1 \leq y \leq \lambda(\mathfrak{I})$ such that $\alpha^{x+t} \equiv \alpha^{y+t} \pmod{\mathfrak{I}}$. Given x, choose a y with $1 \leq y \leq \lambda(\mathfrak{I})$ such that $\alpha^{x+t} \equiv \alpha^{y+t} \pmod{\mathfrak{I}'}$, where $\mathfrak{I}' = \prod_{v_i=0} \mathfrak{p}_i^{n_i}$. Since $\gcd(\alpha, \mathfrak{I}') = 1$ and $\lambda(\mathfrak{I}') \leq \lambda(\mathfrak{I})$, such a y exists. Thus it remains only to prove that $\alpha^{x+t} \equiv \alpha^{y+t} \pmod{\mathfrak{I}''}$, where $\mathfrak{I}'' = \prod_{v_i \neq 0} \mathfrak{p}_i^{n_i}$. Since $x, y \geq 0$, this statement is trivial. □

3.2.3 Proofs

In this section we present the proof of Theorem 3.6.

Proof of Theorem 3.6. Take a $\delta > 0$, and using Lemma 3.6, choose an ideal $\mathfrak{M}$ such that $\mathfrak{A} \mid \mathfrak{M}$ and $\lambda(\mathfrak{M}) < N(\mathfrak{M})^\delta$. Here (by choosing some appropriate ideal divisor $\mathfrak{B}$ of $\mathfrak{M}$) we may further assume that $N(\mathfrak{M})$ is so large that $N(\mathfrak{M})^\delta \geq \log(N(\mathfrak{M}))$. Then, using Lemma 3.7, we get that

$$\mathrm{ord}_\mathfrak{M}(\alpha) \leq N(\mathfrak{M})^\delta + \log(N(\mathfrak{M}))/\log 2$$

for any $\alpha \in \mathcal{O}_\mathbb{K}$. Thus

$$|H \pmod{\mathfrak{M}}| \leq (N(\mathfrak{M})^\delta + \log(N(\mathfrak{M}))/\log 2)^{k\ell}.$$

Hence choosing δ appropriately, the theorem follows. □

3.2.4 An algorithm for solving exponential Diophantine equations over number fields

Our algorithm for solving exponential Diophantine equations over number fields is very similar to what we have seen in Section 3.1.2. So without any further explanation we simply give the steps needed to handle equation (3.9).

(I) We find the "small" solutions of equation (3.9). [Note: since the exponents x_{ij}, $1 \leq i \leq k$, $1 \leq j \leq \ell$ can be negative numbers, we need to check for the "small" solutions $x_{ij} \in \mathbb{Z}$.]

(II) We choose one of the unknowns, x_{ij} say, belonging to some β_{ij} which is **not a unit**. Using the list of solutions from step (I) we take an integer x_0 with $x_{ij} < x_0$ in all known solutions. [Note: as a variant of the method, at this point we could choose more exponents to speed up the calculations.]

(III) In place of equation (3.9), we consider the equation obtained by replacing the coefficient α_i with $\alpha_i \beta_{ij}^{x_0}$. [Note: if the list of solutions is indeed complete, then the new equation has no solutions in non-negative integer exponents.]

(IV) We search for an $\mathfrak{M}$ such that the new equation has no solution modulo $\mathfrak{M}$. Having such an $\mathfrak{M}$, we can conclude that $x_{ij} < x_0$ holds for all solutions of (3.9). [Note: if Conjecture 2 is true, then such a modulus exists. In the examples we shall show strategies how we try to find such an $\mathfrak{M}$. One method is based upon the proof of Theorem 3.6. As an important point, observe that for the unsolvability of the congruence modulo $\mathfrak{M}$

the relation we need to have $\mathfrak{A} := (\beta_{ij}^{x_0}) \mid \mathfrak{M}$ should hold, showing the importance of the divisibility property.]

Remark 12. If we iterate this method, then after some steps we are left with equations where all the remaining β_{ij} are units. Since our algorithm cannot be used in this case we need to use another method to handle these equations (e.g. if we only have two units remaining then we may apply Baker's method to find all solutions).

Remark 13. Note that the method might also work if there are solutions with vanishing subsums: if there are terms which are not involved in such subsums, then the corresponding exponents may be bounded as above, and the final equation obtained can be solvable (e.g. by Baker's method, if the number of remaining terms is sufficiently reduced).

The rest of this section is devoted to numerical examples, and we also analyze our method from certain aspects. At the end of the section, we formulate a theorem based upon these results and computations.

Let $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, where d is one of $2, 3, 5$ and consider the equations

$$\beta_1^{x_1} + 2\beta_2^{x_2} - 3\beta_3^{x_3} = 1, \tag{3.11}$$

where $\beta_i = a_i + b_i\sqrt{d}$ such that a_i and b_i are integers with $\max\{|a_i|, |b_i|\} \leq 3$ and x_i is a non-zero integer for every $i = 1, 2, 3$. (We decided to exclude the case when one or more exponents are zero, since in those cases we can use e.g. Baker's method to handle the equations.) Taking everything into account we have $7^6 = 117649$ equations for every d.

Our goal is that for any equations (3.11) which is not solvable, give an ideal $\mathfrak{M}$ such that the equation has no solutions modulo $\mathfrak{M}$. Thus first we need to exclude all equations (3.11) which has a solution. For this, we do an exhaustive

search for the exponent triple (x_1, x_2, x_3) in some large domain. Namely, we check the domain with $\max_{i=1,2,3} |x_i| \leq 100$. Note that if some β_i is a unit in $\mathcal{O}_{\mathbb{K}}$, then we have to check the negative values of x_i indeed. After this search we are rather sure that we have found all equations (3.11) which are solvable. (Note that obviously, at this point we cannot be sure that this is really the case - however, as we shall see later, this expectation is proved to be valid.) After this step, we use three ideals for $d = 2, 3, 5$ ($\mathfrak{M}_2, \mathfrak{M}_{2,3}, \mathfrak{M}_{2,3,5}$). These ideals are defined in the following way. Fixing d (and hence $\mathbb{K}$), $\mathfrak{M}_2$ is generated by those ideals $\mathfrak{M}$ in $\mathcal{O}_{\mathbb{K}}$ which are prime ideals with norm less than 50 and $\varphi(\mathfrak{M})$ has only 2 as a prime divisor. We define the ideals $\mathfrak{M}_{2,3}$ and $\mathfrak{M}_{2,3,5}$ similarly by simply expanding the list of possible prime divisors to $2, 3$ and to $2, 3, 5$, respectively. The use of these ideals is motivated by the following approach: by collecting the mentioned generators, we get an ideal with "small" λ-value.

We get that after using $\mathfrak{M}_2$, $\mathfrak{M}_{2,3}$ and $\mathfrak{M}_{2,3,5}$ most of the equations for which we did not find solutions at the first stage, are not solvable. To handle the remaining equations we extended the ideals $\mathfrak{M}_2$, $\mathfrak{M}_{2,3}$ and $\mathfrak{M}_{2,3,5}$ to be generated by primes in $\mathcal{O}_{\mathbb{K}}$ with the same property as before, but norm at most 150. By using these new ideals we were able to prove that none of the remaining equations have solutions.

We summarize our results in the Tables 1,2 and 3. We only work with the cases where we have not found solutions at the first stage. Since for all $\beta_i = a_i + b_i\sqrt{d}$ we have $\max\{|a_i|, |b_i|\} \leq 3$ then we need to work with $7^6 = 117649$ possible equations. First we rule out those equations which have solutions with $\max_{i=1,2,3} |x_i| \leq 100$, and only keep the others. For example for $d = 2$ after this step we get that 113361 equations have no solutions if the exponents are "small". After this step we first consider these equations modulo $\mathfrak{M}_2$ where the primes generating $\mathfrak{M}_2$ have norms $N \leq 50$. The algorithm proved that 92636 equations are unsolvable modulo $\mathfrak{M}_2$. Still using $N \leq 50$

as a bound for the norms of the primes generating $\mathfrak{M}_2, \mathfrak{M}_{2,3}$ and $\mathfrak{M}_{2,3,5}$, we get that out of the remaining 20725 equations 20173 are not solvable modulo $\mathfrak{M}_{2,3}$. By using $\mathfrak{M}_{2,3,5}$ we were not able to rule out all remaining equations, the algorithm was unable to decide if 22 of them are solvable or not. Thus we increased the bound for N to 150 and started over. For $\mathfrak{M}_2$ we did not get any new information, but using $\mathfrak{M}_{2,3}$ was enough to prove that all remaining equations are unsolvable, thus in this case we were not required to use $\mathfrak{M}_{2,3,5}$.

		Solved	Remaining
$\mathfrak{M}_2$	$N \leq 50$	92636	20725
	$N \leq 150$	92636	20725
$\mathfrak{M}_{2,3}$	$N \leq 50$	20173	552
	$N \leq 150$	20725	0
$\mathfrak{M}_{2,3,5}$	$N \leq 50$	530	22
	$N \leq 150$	–	–

Table 1. The results for $d = 2$.

		Solved	Remaining
$\mathfrak{M}_2$	$N \leq 50$	55223	58305
	$N \leq 150$	55223	58305
$\mathfrak{M}_{2,3}$	$N \leq 50$	57622	583
	$N \leq 150$	57801	504
$\mathfrak{M}_{2,3,5}$	$N \leq 50$	380	203
	$N \leq 150$	504	0

Table 2. The results for $d = 3$.

		Solved	Remaining
$\mathfrak{M}_2$	$N \leq 50$	44184	72165
	$N \leq 150$	44184	72165
$\mathfrak{M}_{2,3}$	$N \leq 50$	56815	15350
	$N \leq 150$	71407	758
$\mathfrak{M}_{2,3,5}$	$N \leq 50$	15326	24
	$N \leq 150$	758	0

Table 3. The results for $d = 5$.

Summarizing our results, we obtain the following theorem.

Theorem 3.7. *Let $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, where d is one of $2, 3, 5$ and consider the equation*

$$\beta_1^{x_1} + 2\beta_2^{x_2} - 3\beta_3^{x_3} = 1, \tag{3.10}$$

in integers x_1, x_2, x_3, where $\beta_i = a_i + b_i\sqrt{d}$ such that a_i and b_i are integers with $\max\{|a_i|, |b_i|\} \leq 3$ $(i = 1, 2, 3)$. If equation (3.11) *has no solutions then there exists an ideal $\mathfrak{M}$ such that the equation has no solutions modulo $\mathfrak{M}$.*

4 Applications

In this section we give some applications of the methods from Sections 3.1 and 3.2 to Diophantine problems which can be reduced to the solution of exponential Diophantine equations. These problems are proposed by Terai [83, 80, 81, 82], Marques, Togbé [50], Luca [48] and others.

4.1 A complete solution of a conjecture of Terai

The first problem is related to a famous conjecture of Terai. Namely, let a, b, c be positive integers with $\gcd(a, b, c) = 1$ and consider the Diophantine equation

$$a^x + b^y = c^z \tag{4.1}$$

where x, y, z are unknown positive integers. This equation has been investigated by several authors. In particular, Terai [80] conjectured that if $a, b, c \geq 2$ then equation (4.1) has at most one solution in (x, y, z) with $x, y, z \geq 2$ (see also [81, 82, 83]). This conjecture implies the classical conjecture of Jeśmanowicz [41], saying that

$$(m^2 - n^2)^x + (2mn)^y = (m^2 + n^2)^z$$

has no solutions other than $(x, y, z) = (2, 2, 2)$, where m, n are positive integers with $m > n$, $\gcd(m, n) = 1$ and $m \not\equiv n \pmod 2$. Note that in this case $a = m^2 - n^2$, $b = 2mn$, $c = m^2 + n^2$ form a reduced Diophantine triple, thus $(x, y, z) = (2, 2, 2)$ is always a solution.

As a related problem, Terai [83] investigated the equation

$$(4t^2 + 1)^x + (5t^2 - 1)^y = (3t)^z, \tag{4.2}$$

where t is an arbitrary but fixed positive integer, and x, y, z are unknown positive integers. He proved the following.

Theorem A (Terai [83]). *If* $0 < t \leq 20$ *or* $t \not\equiv 3 \pmod 6$ *then equation* (4.2) *has the only solution* $(x, y, z) = (1, 1, 2)$.

Recently, Su and Li [76] investigated the cases where $3 \mid t$. They obtained the following result.

Theorem B (Su and Li [76]). *If* $t \geq 90$ *and* $3 \mid t$ *then the only solution to the Diophantine equation* (4.2) *is* $(x, y, z) = (1, 1, 2)$.

As one can see, combining Theorems A and B, we get the complete solution of equation (4.2) for $t \leq 20$ and $90 \leq t$.

Here we complete the solution of (4.2). Solving the remaining cases and putting it together with Theorem A and B we obtain the following theorem (Theorem 1 from Bertók [10])

Theorem 4.1. *For any positive integer* t*, the Diophantine equation* (4.2) *has only one solution in* x, y *and* z*, namely* $(x, y, z) = (1, 1, 2)$.

The proof uses the method from Section 3.1. We note that in these specific equations one could use Baker's method to get bounds for the solutions, and then by some reduction method all solutions could be obtained. However, our approach is more elementary.

Proof of Theorem 4.1. In view of Theorem A and B, we only have to solve (4.2) for $20 < t < 90$ and $t \equiv 3 \pmod 6$, namely for

$$t = 21, 27, 33, 39, 45, 51, 57, 63, 69, 75, 81, 87.$$

Letting $a = 4t^2 + 1$, $b = 5t^2 - 1$, $c = 3t$ for these t's, the equation can be written as

$$a^x + b^y = c^z. \tag{4.3}$$

Altogether we have twelve equations of type (4.3) to solve. We solve these equations by using the algorithm presented in Section 3.1.

To prove Theorem 4.1, we show that (4.3) has no solution with $z > 2$. For this purpose, instead of (4.3), we consider the equation

$$a^x + b^y = c^2 \cdot c^{z_0} \tag{4.4}$$

in positive integers x, y, z_0. Our strategy is the following. We find an appropriate modulus m such that (4.4) has no solutions modulo m. Then we conclude that (4.3) has no solutions with $z = z_0 + 2 \geq 3$. Since a, b and c are all fixed positive integers, the remaining cases where $z < 3$ can be checked easily.

To find appropriate moduli m, one can use primes p such that $p - 1$ are composed only of "small" primes. As we described the construction of such moduli at Section 3.1 we do not give details here.

Since every equation can be handled similarly, we only demonstrate the solution for $t = 21$. However, in this case we provide extensive data. We use the program package Sage [77] to perform the necessary calculations.

If $t = 21$ then the equation is

$$1765^x + 2204^y = 63^z.$$

Following the strategy we consider instead the equation

$$1765^x + 2204^y = 63^2 \cdot 63^{z_0}. \tag{4.5}$$

First consider this equation modulo 37. For the orders of the bases $1765, 2204, 63$ modulo 37 we get

$$\text{ord}_{37}(1765) = 3, \quad \text{ord}_{37}(2204) = 18, \quad \text{ord}_{37}(63) = 3.$$

Hence the exponents x, y, z_0 are determinded modulo $3, 18, 3$, respectively. It can be checked that we have six solutions, namely

i) $x \equiv 1 \pmod 3$, $y \equiv 16 \pmod{18}$, $z_0 \equiv 1 \pmod 3$,

ii) $x \equiv 2 \pmod 3$, $y \equiv 13 \pmod{18}$, $z_0 \equiv 1 \pmod 3$,

iii) $x \equiv 0 \pmod 3$, $y \equiv 7 \pmod{18}$, $z_0 \equiv 2 \pmod 3$,

iv) $x \equiv 2 \pmod 3$, $y \equiv 10 \pmod{18}$, $z_0 \equiv 2 \pmod 3$,

v) $x \equiv 0 \pmod 3$, $y \equiv 4 \pmod{18}$, $z_0 \equiv 0 \pmod 3$,

vi) $x \equiv 1 \pmod 3$, $y \equiv 1 \pmod{18}$, $z_0 \equiv 0 \pmod 3$.

After some calculations we get six new equations

i) $1765 \cdot (1765^3)^{x_1} + 2204^{16} \cdot (2204^{18})^{y_1} = 63^3 \cdot (63^3)^{z_1}$,

ii) $1765^2 \cdot (1765^3)^{x_1} + 2204^{13} \cdot (2204^{18})^{y_1} = 63^3 \cdot (63^3)^{z_1}$,

iii) $(1765^3)^{x_1} + 2204^7 \cdot (2204^{18})^{y_1} = 63^4 \cdot (63^3)^{z_1}$,

iv) $1765^2 \cdot (1765^3)^{x_1} + 2204^{10} \cdot (2204^{18})^{y_1} = 63^4 \cdot (63^3)^{z_1}$,

v) $(1765^3)^{x_1} + 2204^4 \cdot (2204^{18})^{y_1} = 63^2 \cdot (63^3)^{z_1}$,

vi) $1765 \cdot (1765^3)^{x_1} + 2204 \cdot (2204^{18})^{y_1} = 63^2 \cdot (63^3)^{z_1}$,

where x_1, y_1 and z_1 are positive integers.

We consider these equations modulo 193. We have

$$\text{ord}_{193}(1765^3) = 16, \quad \text{ord}_{193}(2204^{18}) = 2, \quad \text{ord}_{193}(63^3) = 4.$$

It can be seen that the first two equations have no solutions modulo 193, and the other four has two solutions each, where the exponents x_1, y_1, z_1 are considered modulo $16, 2, 4$, respectively. We only take the fourth equation, the other ones can be handled similarly. In this case we get that the two solutions of the equation are

i') $x_1 \equiv 15 \pmod{16}$, $y_1 \equiv 0 \pmod{2}$, $z_1 \equiv 1 \pmod{4}$,

ii') $x_1 \equiv 7 \pmod{16}$, $y_1 \equiv 1 \pmod{2}$, $z_1 \equiv 3 \pmod{4}$.

This leads us to the following two new equations:

i') $1765^{47} \cdot (1765^{48})^{x_2} + 2204^{10} \cdot (2204^{36})^{y_2} = 63^7 \cdot (63^{12})^{z_2}$,

ii') $1765^{23} \cdot (1765^{48})^{x_2} + 2204^{28} \cdot (2204^{36})^{y_2} = 63^{13} \cdot (63^{12})^{z_2}$,

where x_2, y_2 and z_2 are positive integers.

Now we work modulo 109. We have

$$\text{ord}_{109}(1765^{48}) = 9, \quad \text{ord}_{109}(2204^{36}) = 3, \quad \text{ord}_{109}(63^{12}) = 1.$$

We obtain that the second equation has no solutions while the solutions of the first eqation satisfiy

$$x_2 \equiv 7 \pmod{9}, \quad y_2 \equiv 0 \pmod{3}, \quad z_2 \geq 0.$$

The corresponding equation is

$$1765^{383} \cdot (1765^{432})^{x_3} + 2204^{10} \cdot (2204^{108})^{y_3} = 63^7 \cdot (63^{12})^{z_3}.$$

Now modulo 3^6 we get that this equation has no solutions. We used the number 3^6 because we want to prove that equation (4.2) has no solutions with $z > 2$. Since the equation has a solution with $z = 2$ and $3t = 3^2 \cdot 7$ we need to put 3^6 in m, otherwise we are not able to rule out the possible solutions with $z \leq 2$. We note that the modulus $m = 3^6 \cdot 37 \cdot 109 \cdot 193$ works for the other arising equations as well.

Hence we obtain that equation (4.5) has no solutions modulo m, which means that in the original equation $z < 3$ holds. This easily implies $(x, y, z) = (1, 1, 2)$.

For the remaining cases we only list the used moduli in Table 4. □

t	m
27	$3^{12} \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 19 \cdot 37 \cdot 41 \cdot 73 \cdot 97 \cdot 109 \cdot 163 \cdot 193 \cdot 257 \cdot 577$
33	$3^6 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 19 \cdot 37 \cdot 41 \cdot 73 \cdot 97 \cdot 163 \cdot 433$
39	$3^6 \cdot 7 \cdot 13 \cdot 17 \cdot 19 \cdot 37 \cdot 41 \cdot 73 \cdot 97 \cdot 109 \cdot 43$
45	$5^3 \cdot 7 \cdot 13 \cdot 17 \cdot 19 \cdot 41 \cdot 97$
51	$3^6 \cdot 7 \cdot 13 \cdot 17 \cdot 19 \cdot 37 \cdot 41 \cdot 73 \cdot 97 \cdot 109 \cdot 163$
57	$3^6 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 19 \cdot 37 \cdot 73 \cdot 97 \cdot 109 \cdot 163 \cdot 193 \cdot 433 \cdot 577 \cdot 769$
63	$3^9 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 19 \cdot 37 \cdot 73 \cdot 109 \cdot 433$
69	$3^6 \cdot 7 \cdot 17 \cdot 19 \cdot 37 \cdot 73 \cdot 97 \cdot 109 \cdot 163 \cdot 193$
75	$3^6 \cdot 7 \cdot 17 \cdot 19 \cdot 37 \cdot 73 \cdot 97 \cdot 109 \cdot 163 \cdot 257$
81	$3^{15} \cdot 7 \cdot 17 \cdot 19 \cdot 37 \cdot 41 \cdot 73 \cdot 97 \cdot 109 \cdot 163 \cdot 193 \cdot 257 \cdot 433 \cdot 577$
87	$3^6 \cdot 7 \cdot 19 \cdot 37 \cdot 41 \cdot 73 \cdot 109$

Table 4. The used moduli for equation (4.2).

4.2 Representing terms of binary recurrence sequences as sums of powers

As our second application we give some results for binary recurrence sequences.

Searching for specific terms of linear recurrence sequences has a long history and a rich literature. A famous book addressing these kinds of problems is [73] or the reader may consult the papers [42, 50, 65] and the references given there. Pethő [58] and Shorey and Stewart [72] independently proved that under certain natural assumptions, a linear recurrence sequence may contain only finitely many perfect powers. In the case of some special, famous sequences all perfect powers have been determined. In the case of the Pell sequence P_n, Pethő [60] proved that it does not contain non-trivial powers. Bugeaud, Mignotte and Siksek [22] proved that the Fibonacci-sequence F_n contains only the powers $0, 1, 8, 144$, and the only powers in the sequence of Lucas numbers L_n are $1, 4$. Results of Pethő and Tichy [62] imply that there are only finitely many Fibonacci numbers of the form $p^x + p^y + p^z$, where p is a fixed prime. Kovács [42] found all combinatorial numbers of certain shapes among the terms of F_n, L_n, P_n and Q_n (the associated Pell-sequence). Sanchez and Luca [65], among others showed that the only Fibonacci number of the shape $\pm m! \pm 2^x 3^y 5^z 7^v$ is $F_{24} = 8! + 2^5 3^3 5^0 7^1$. Sanchez and Luca noted that by their method they cannot solve the equation $F_n = 2^x + 3^y$.

Finally we mention a result of Irmak and Szalay [40] who determined all Tribonacci numbers which are close to the sum of powers of $2, 3$ and 5. For other related results, see the references e.g. in our paper [16].

In this section first we concentrate on the equations $U_n = 2^x + 3^y$ and $U_n = 2^x + 3^y + 5^z$ in non-negative integers x, y, z where U_n is one of the Fibonacci-sequence F_n, the Lucas-sequence L_n, the Pell-sequence P_n or the

associated Pell-sequence Q_n.

The second part of the first theorem extends the above mentioned result of Marques and Togbé [50]. Namely, we get rid of the condition $z \geq \max(x, y)$ in the equation

$$U_n = 2^x + 3^y + 5^z$$

with $U_n = F_n, L_n$, and we consider the cases $U_n = P_n, Q_n$, as well. The first part of the first theorem with $U_n = F_n$ solves the previously mentioned problem of Sanchez and Luca [65]. This result is Theorem 2.2 in [16].

Theorem 4.2. *Let U_n be one of F_n, L_n, P_n, Q_n. Then the solutions of the equation*

$$U_n = 2^x + 3^y \tag{4.6}$$

in non-negative integers n, x, y are given by Table 5.

	(n, x, y)
F_n	$(3,0,0), (4,1,0), (5,1,1), (5,2,0), (7,2,2), (11,3,4)$
L_n	$(0,0,0), (3,0,1), (2,1,0), (5,1,2),$ $(7,1,3), (4,2,1), (13,9,2), (5,3,1)$
P_n	$(2,0,0), (3,1,1), (5,1,3), (3,2,0), (9,8,6)$
Q_n	$(2,1,0), (3,2,1), (4,3,2), (4,4,0), (5,5,2)$

Table 5. Solutions of equation (4.6).

Furthermore, still with U_n being one of F_n, L_n, P_n, Q_n, the solutions of the equation

$$U_n = 2^x + 3^y + 5^z \tag{4.7}$$

in non-negative integers n, x, y, z are those occurring in Table 6.

	(n, x, y, z)
F_n	$(4,0,0,0), (5,0,1,0), (6,1,0,1), (9,1,3,1),$ $(6,2,1,0), (9,3,0,2), (12,4,1,3), (9,5,0,0)$
L_n	$(2,0,0,0), (4,0,0,1), (7,0,1,2), (5,0,2,0), (7,0,3,0),$ $(3,1,0,0), (6,2,2,1), (6,3,2,0), (6,4,0,0)$
P_n	$(3,0,1,0), (5,0,3,0), (4,1,2,0), (5,0,1,2), (4,2,1,1),$ $(4,3,1,0), (6,6,0,1), (8,8,3,3), (10,10,6,4)$
Q_n	$(2,0,0,0), (3,0,0,1)$

Table 6. Solutions of equation (4.7).

Remark 14. Note that the solutions of the equation $U_n = 2^x$ are also known for these sequences: for $U_n = F_n, L_n$ they can be obtained from the already mentioned results of Bugeaud, Mignotte and Siksek [22] (the solutions are $(n, x) = (1, 0), (2, 0), (5, 3)$ and $(n, x) = (0, 2), (1, 0)$, respectively), for $U_n = P_n$ the only solution $(n, x) = (1, 0)$ is given by the result of Pethő [60], while for $U_n = Q_n$ the only solutions are $(n, x) = (0, 0)$ and $(1, 0)$, since all the terms of Q_n with $n > 0$ are odd and greater than one.

Proof of Theorem 4.2. Since we apply the method from Section 3.2 for every equation, we only demonstrate our approach for the case of $F_n = 2^x + 3^y$. For the remaining equations we only list the moduli used.

We rewrite the equation $F_n = 2^x + 3^y$ as

$$\alpha^n - \beta^n - \sqrt{5} \cdot 2^x - \sqrt{5} \cdot 3^y = 0, \tag{4.8}$$

where $\alpha = \frac{1+\sqrt{5}}{2}$ and $\beta = \frac{1-\sqrt{5}}{2}$. First we list all "small" solutions of this equation, i.e. the solutions with $n, a, b \leq 100$. (Note that it is not necessary to check for negative values of n, since $\alpha^{-1} = -\beta$. Thus we cannot have negative

even solutions in n and if n is a negative odd number then we can simply take its absolute value since equation (4.8) remains the same.) In fact, we just find the solutions given in Table 5. We observe that in every "small" solution the exponent of 2 is at most 3, and instead of (4.8) we consider the equation

$$\alpha^n - \beta^n - \sqrt{5} \cdot 2^4 \cdot 2^{x_0} - \sqrt{5} \cdot 3^y = 0. \tag{4.9}$$

We suspect that equation (4.9) has no solutions in non-negative integers n, x_0, y. To show this, we work in the ring of integers $\mathcal{O}_{\mathbb{K}}$ of the number field $\mathbb{K} = \mathbb{Q}(\sqrt{5})$. We exhibit a modulus $\mathfrak{M} \in \mathcal{O}_{\mathbb{K}}$ such that (4.9) has no solutions already modulo $\mathfrak{M}$. (Here, and elsewhere from this point on, all congruences are to be taken in $\mathcal{O}_{\mathbb{K}}$.) As we shall see,

$$\mathfrak{M} = 2^4 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 19 \cdot 29 \cdot 31 \cdot 37 \cdot 43 \cdot 73$$

is an appropriate choice. For this, consider equation (4.9) modulo $\mathfrak{M}_1 = 2^4$. One can easily check that $\mathrm{ord}_{2^4}(\alpha) = \mathrm{ord}_{2^4}(\beta) = 24$, $\mathrm{ord}_{2^4}(3) = 4$. Since $\sqrt{5} \cdot 2^4 \cdot 2^{x_0} \equiv 0 \pmod{2^4}$, we only need to consider $24 \cdot 4 = 96$ possibilities. By checking all these cases, we get that there are only eight solutions modulo 2^4. These solutions are given by

$$(n, y) \equiv (1, 0), (2, 0), (4, 1), (11, 2), (13, 2),$$

$$(14, 2), (16, 3), (23, 0) \pmod{(24, 4)},$$

where here and later on by

$$(u_1, \ldots, u_k) \equiv (v_1, \ldots, v_k) \pmod{(q_1, \ldots, q_k)}$$

we mean that $u_i \equiv v_i \pmod{q_i}$ for every $i = 1, \dots, k$. We consider only the case $n \equiv 4 \pmod{24}$ and $y \equiv 1 \pmod{4}$, the other cases can be handled similarly. Now putting $n = 24n_0 + 4$ and $y = 4y_0 + 1$, from (4.9) we get

$$\alpha^4 \cdot (\alpha^{24})^{n_0} - \beta^4 \cdot (\beta^{24})^{n_0} - \sqrt{5} \cdot 2^4 \cdot 2^{x_0} - \sqrt{5} \cdot 3 \cdot (3^4)^{y_0} = 0. \quad (4.10)$$

Take $\mathfrak{M}_2 = 5$. As we have $\mathrm{ord}_5(\alpha^{24}) = \mathrm{ord}_5(\beta^{24}) = 5$, $\mathrm{ord}_5(2) = 4$ and $\mathrm{ord}_5(3^4) = 1$, we need to consider $5 \cdot 4 = 20$ cases. By a simple computation we get that

$$(n_0, x_0) \equiv (1,3), (2,0), (3,2), (4,1) \pmod{(5,4)}.$$

We pick up the case $n_0 \equiv 3 \pmod{5}$ and $x_0 \equiv 2 \pmod{4}$, the other cases can be treated similarly. Now letting $n_0 = 5n_1 + 3$ and $x_0 = 4x_1 + 2$, (4.10) yields

$$\alpha^{76} \cdot (\alpha^{120})^{n_1} - \beta^{76} \cdot (\beta^{120})^{n_1} - \sqrt{5} \cdot 2^6 \cdot (2^4)^{x_1} - \sqrt{5} \cdot 3 \cdot (3^4)^{y_0} = 0. \quad (4.11)$$

We take $\mathfrak{M}_3 = 7$. As one can easily check, we have $\mathrm{ord}_7(\alpha^{120}) = \mathrm{ord}_7(\beta^{120}) = 2$ and $\mathrm{ord}_7(2^4) = \mathrm{ord}_7(3^4) = 3$. That is, we have to consider $2 \cdot 3 \cdot 3 = 18$ cases. By doing this we get two solutions, namely

$$(n_1, x_1, y_0) \equiv (0,0,0), (1,2,2) \pmod{(2,3,3)}.$$

Taking the first triplet (the other one can be handled similarly), putting $n_1 = 2n_2$, $x_1 = 3x_2$ and $y_0 = 3y_1$, we obtain

$$\alpha^{76} \cdot (\alpha^{240})^{n_2} - \beta^{76} \cdot (\beta^{240})^{n_2} - \sqrt{5} \cdot 2^6 \cdot (2^{12})^{x_2} - \sqrt{5} \cdot 3 \cdot (3^{12})^{y_1} = 0. \quad (4.12)$$

Now choose $\mathfrak{M}_4 = 13$. Then $\mathrm{ord}_{13}(\alpha^{240}) = \mathrm{ord}_{13}(\beta^{240}) = 7$, and $\mathrm{ord}_{13}(2^{12}) = \mathrm{ord}_{13}(3^{12}) = 1$. If we check all seven possibilities modulo $\mathfrak{M}_4 = 13$, we get that there are no solutions.

By following the same argument as above for the occurring possibilities, using the factors of $\mathfrak{M}$, we conclude that (4.9) has no solutions modulo m. This implies that in (4.8) we must have $x \leq 3$. From this point on one can use the same method again to solve the four new equations (with $x = 0, 1, 2, 3$).

In Table 7 we give the moduli used for the equations. Furthermore, we also indicate what is the conclusion we can draw by the help of that modulus. In the table we use the notation

$$\mathfrak{M}_1 = 7 \cdot 13 \cdot 17 \cdot 19 \cdot 29 \cdot 31 \cdot 37 \cdot 73,$$

$$\mathfrak{M}_2 = \mathfrak{M} \cdot 3^7 \cdot 5 \cdot 11 \cdot 41 \cdot 12289 \cdot 17497 \cdot 18433 \cdot 65537,$$

$$\mathfrak{M}_3 = \mathfrak{M} \cdot 2^{11} \cdot 3^7 \cdot 12289 \cdot 17497 \cdot 18433,$$

$$\mathfrak{M}_4 = \mathfrak{M} \cdot 2 \cdot 3^7 \cdot 11 \cdot 41 \cdot 12289 \cdot 17497,$$

$$\mathfrak{M}_5 = \mathfrak{M} \cdot 2^{12} \cdot 3 \cdot 11 \cdot 41 \cdot 39367 \cdot 65537,$$

where

$$\mathfrak{M} = 7 \cdot 13 \cdot 17 \cdot 19 \cdot 29 \cdot 31 \cdot 37 \cdot 43 \cdot 73 \cdot 97 \cdot 109 \cdot 163 \cdot 193 \cdot 257 \cdot 433 \cdot 487 \cdot 577 \cdot$$

$$\cdot 769 \cdot 1153 \cdot 1297 \cdot 1459 \cdot 2593 \cdot 2917 \cdot 3137 \cdot 3457 \cdot 3889 \cdot 10369.$$

seq.	representation	modulus	conclusion	modulus	conclusion
F_n	$2^x + 3^y$	$\mathfrak{M}_1 \cdot 2^4 \cdot 5 \cdot 43$	$x \leq 3$	-	-
	$2^x + 3^y + 5^z$	$\mathfrak{M}_1 \cdot 2^6 \cdot 97 \cdot$ $\cdot 109 \cdot 193 \cdot 769$	$x \leq 5$	$\mathfrak{M}_1 \cdot 2 \cdot 3^4 \cdot$ $\cdot 97 \cdot 109 \cdot 769$	$y \leq 3$
L_n	$2^x + 3^y$	$\mathfrak{M}_1 \cdot 3^4 \cdot 5 \cdot 43 \cdot$ $\cdot 97 \cdot 109 \cdot 163 \cdot$ $\cdot 193 \cdot 257 \cdot 433 \cdot$ $\cdot 487 \cdot 577 \cdot 769 \cdot 3889$	$y \leq 3$	-	-
	$2^x + 3^y + 5^z$	$\mathfrak{M}_1 \cdot 2^5 \cdot$ $\cdot 97 \cdot 109 \cdot 193$	$x \leq 4$	$\mathfrak{M}_1 \cdot 2^5 \cdot 3^4 \cdot 11^2 \cdot$ $\cdot 41 \cdot 61 \cdot 67 \cdot$ $\cdot 71 \cdot 109 \cdot 271$	$y \leq 3$
P_n	$2^x + 3^y$	$\mathfrak{M}_2$	$y \leq 6$	-	-
	$2^x + 3^y + 5^z$	$\mathfrak{M}_3$	$x \leq 10$ or $y \leq 6$	$\mathfrak{M}_4$ resp. $\mathfrak{M}_5$	$y \leq 6$ resp. $x \leq 11$
Q_n	$2^x + 3^y$	$3^3 \cdot 5 \cdot 7 \cdot 13 \cdot$ $\cdot 97 \cdot 109 \cdot 193$	$y \leq 2$	-	-
	$2^x + 3^y + 5^z$	2^2	$x \leq 1$	$3 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot$ $\cdot 19 \cdot 31 \cdot 37 \cdot 73$	$y = 0$

Table 7. Used moduli and the conclusion drawn for the equations considered.

In the above table it can be seen that we only used our method to reduce the number of unknown variables to two (n and either x or y for $2^x + 3^y$ or n and z for $2^x + 3^y + 5^z$). As it was mentioned before, it would be possible to use the algorithm again and solve the equations completely. However, instead of doing so we used a different approach, since in these special cases it was much faster than our method. Namely, we used elliptic curves. This approach, as we shall see, always becomes available whenever we can restrict two variables from x, y, z. Then by the help of the identities

$$L_n^2 - 5F_n^2 = \pm 4 \quad \text{and} \quad 2P_n^2 - Q_n^2 = \pm 1 \tag{4.13}$$

one can reduce the problem to finding integral points on elliptic curves. We demonstrate this method by exhibiting a particular case. Recall that in the case of the equation $F_n = 2^x + 3^y$ the local arguments implied $x = 0, 1, 2, 3$. As an example, we take $x = 3$, the other cases can be handled similarly. In this case we need to solve the equation

$$F_n = 3^y + 8. \tag{4.14}$$

We can write $y = 2k$ or $y = 2k + 1$ with some integer k. Put $Y = L_n$ and $X = 3^k$. Then from the first identity in (4.13) in the case of $y = 2k$ we get

$$Y^2 = 5X^4 + 80X^2 + 320 \pm 4,$$

while for $y = 2k + 1$ we obtain

$$Y^2 = 45X^4 + 240X^2 + 320 \pm 4.$$

Using the Magma [19] procedure `IntegralQuarticPoints`, we get the integer solutions X, Y of these equations. Namely, if (X, Y) is a solution to any of the above equations in non-negative integers, then it is one of

$$(X, Y) = (0, 18), (9, 199), (15, 521).$$

Among these solutions we select those where X is a non-negative power of 3. In this case the only such solution is $(X, Y) = (9, 199)$. We conclude that equation (4.14) has the only solution $y = 4$ (with $n = 11$).

In the case of all the other equations (4.6) and (4.7), after reducing the number of variables on the right hand sides to one, the above method worked and provided the solutions in Tables 5 and 6. □

4.3 A problem concerning balancing numbers

Now we turn to a problem related to balancing numbers. Namely we discuss equations consisting of balancing numbers. The sequence of balancing numbers B_n is defined by $B_0 = 0$, $B_1 = 1$ and $B_{n+2} = 6B_{n+1} - B_n$ $(n \geq 0)$. That is, the sequence is a special Lucas-sequence. Problems related to balancing numbers have a vast literature; see e.g. the papers [43, 47, 57, 79] and the references given there. We can write

$$B_n = \frac{\beta_1^n - \beta_2^n}{\beta_1 - \beta_2} \quad (n \geq 0),$$

where $\beta_1 = 3 + 2\sqrt{2}$ and $\beta_2 = 3 - 2\sqrt{2}$. Consider the following equation

$$B_u + B_v + B_w = b^z \tag{4.15}$$

in non-negative integers u, v, w, z, where $b \in \{2, 3, 5, 7\}$. Such equations (that is, representing powers as sums of terms of certain linear recurrence sequences) is of large recent interest, many papers deal with such questions. We refer e.g. to the articles [16, 23, 24] and the references given there. In these papers typically deep methods (such as Baker's method) are combined with certain reduction techniques. For finding all solutions of (4.15) we shall apply the method from Section 3.2.

For this, let $\mathbb{K} = \mathbb{Q}(\sqrt{2})$, and rewrite (4.15) as

$$\beta_1^u - \beta_2^u + \beta_1^v - \beta_2^v + \beta_1^w - \beta_2^w = 4\sqrt{2}b^z. \tag{4.16}$$

To find all solutions, first we perform an exhaustive search on the domain $\max(|u|, |v|, |w|, |z|) \leq 100$ to get all "small" solutions. (Since both β_1 and β_2 are units in $\mathcal{O}_{\mathbb{K}}$, it is possible that (4.16) has solutions with negative values of

u, v, w, as well.) We obtained that in all solutions we got, we have

$$z \leq \begin{cases} 6, & \text{if } b = 2, \\ 1, & \text{if } b = 3, \\ 1, & \text{if } b = 5, \\ 1, & \text{if } b = 7. \end{cases} \tag{4.17}$$

We suspect that we have found all solutions - we only need to show this. For this, we construct moduli (separately for the values $b = 2, 3, 5, 7$) which show that (4.17) in fact holds for all solutions to (4.16) (and (4.15)). Since the process is similar in all cases, we explain it in detail only for $b = 2$.

Since we can write $2 = (\sqrt{2})^2$ in $\mathbb{K}$, (4.16) can be reformulated as

$$\beta_1^u - \beta_2^u + \beta_1^v - \beta_2^v + \beta_1^w - \beta_2^w = (\sqrt{2})^{2z+5}.$$

Based upon (4.17) we suspect that here $z \leq 6$. If this is true, then the equation

$$\beta_1^u - \beta_2^u + \beta_1^v - \beta_2^v + \beta_1^w - \beta_2^w = 2^9(\sqrt{2})^{z'} \tag{4.18}$$

has no solution in integers u, v, w, z'. However, then by Conjecture 2 we should be able to find a modulus $\mathfrak{M}$ to show this. It turns out that the modulus appearing in Table 8 is appropriate for this purpose. Hence we have that $z \leq 6$ for all solutions to (4.15). The solutions with $z \leq 6$ can be easily listed. Following the same argument, we got that (4.17) is valid in each case $b = 2, 3, 5, 7$, for all solutions. The moduli used are given in Table 8.

We got the moduli in Table 8 in the following way. First we put b^k in the moduli, where k is the bound for z appearing in (4.17). This is an inevitable step, since we want to prove that the modified equation (see equation (4.18))

b	Modulus
2	$2^9 \cdot 3 \cdot 17 \cdot 257 \cdot 7681$
3	$3^2 \cdot 5 \cdot 11 \cdot 13 \cdot 19 \cdot 29 \cdot \sqrt{2} \cdot (1+3\sqrt{2}) \cdot$ $(7+2\sqrt{2}) \cdot (1+2\sqrt{2}) \cdot (1+4\sqrt{2})$
5	$5^2 \cdot 3 \cdot 11 \cdot 25 \cdot (1+4\sqrt{2}) \cdot \sqrt{2} \cdot (7+2\sqrt{2}) \cdot (1+2\sqrt{2})$
7	$7^2 \cdot (1+2\sqrt{2}) \cdot 3 \cdot 5 \cdot 11 \cdot 13 \cdot 19 \cdot 29 \cdot 251 \cdot \sqrt{2}$ $\cdot(1+8\sqrt{2}) \cdot (1+3\sqrt{2}) \cdot (7+2\sqrt{2}) \cdot (1+7\sqrt{2}) \cdot$ $(1+4\sqrt{2})$

Table 8. The moduli used for $b = 2, 3, 5, 7$.

has no so solutions. After this step we tried to find a modulus with "small" λ value. For this we searched for prime ideals $\mathfrak{M}_\mathfrak{i}$ (either generated by a rational prime, or by a prime in $\mathcal{O}_\mathbb{K}$) such that $\varphi(\mathfrak{M}_\mathfrak{i})$ is divisible by "small" rational primes only for all i. After building a list of such ideals we used our algorithm described in 3.2 to prove that the equations have no solutions modulo $\mathfrak{M} = \prod_i \mathfrak{M}_i$. We summarize the results of the calculations in the following theorem, which is Theorem 2 in Bertók and Hajdu [13].

Theorem 4.3. *All solutions to equation* (4.15) *are given in the following table*

b	u	v	w	z
2	0	1	1	1
2	1	1	2	3
3	1	1	1	1
7	0	1	2	1

Table 9. The solutions for equation (4.15).

Remark 15. Inequalities (4.17) provide different bounds for the results of (4.16) than what can be seen in the theorem above. The reason for this is that

since α and β are units in $\mathcal{O}_{\mathbb{K}}$ we may have solutions (and in most cases we actually have) with negative exponents. But in Theorem 4.3 we only list the solutions for (4.15), hence we only need those solutions of (4.16) where u, v and w are non-negative integers.

4.4 Multi-base representations

Our last application is related to multi-base representations. It is a very old problem to study integers which have only a "few" non-zero digits in some kind of a number system. This problem becomes much more interesting and harder if instead of using only one number as the base of the number system we use a so-called multi-base representation, e.g. we want to express the number c by using sums of powers of for example 2 and 3. For details and related results, see Section 2.2.

Let S be a finite set of primes, and write $\mathbb{Z}_S$ (resp. $\mathbb{Z}_S^+$) for the set of integers (resp. positive integers) having no prime divisors outside S. A multi-base representation of an integer n is an expression of the form

$$n = u_1 + \cdots + u_t \tag{4.19}$$

with $u_1, \ldots, u_t \in \mathbb{Z}_S$. If $S = \{p\}$ and we require that $u_1, \ldots, u_t \in \mathbb{Z}_S^+$, we can express n as sums of powers of p in multiple ways, with the shortest one (namely, the one with fewest terms) being the usual expansion of n in base p. As in Section 2.2, for an integer n, we write $w_S(n)$ for the minimal t for which (4.19) holds with some $u_1, \ldots, u_t \in \mathbb{Z}_S$. If $n > 0$ and we also require that $u_1, \ldots, u_t \in \mathbb{Z}_S^+$, we then write $w_S^+(n)$ instead.

In Section 2.2 we gave some theoretical theorems regarding $w_S(n)$ and $w_S^+(n)$. Here we concentrate on numerical results. Using the method from

Section 3.1, we prove the following theorem (Theorem 2.3 from our paper [14]).

Theorem 4.4. *Let $S_1,\ S_2$ be disjoint non-empty sets with $S_1 \cup S_2 = \{2,\ 3,\ 5\}$. Then*

$$w^+_{S_1}(n) + w^+_{S_2}(n) \leq 4$$

implies that

1. *if $S_1 = \{2\}$ and $S_2 = \{3,\ 5\}$ then $n \in \{1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 8,\ 9,\ 10,\ 12,\ 16,\ 18,\ 20,\ 24,\ 25,\ 32,\ 34,\ 36,\ 40,\ 48,\ 72,\ 80,\ 81,\ 96,\ 128,\ 130,\ 136,\ 144,\ 160,\ 258,\ 260,\ 288,\ 384,\ 640,\ 1152,\ 2050,\ 2052,\ 4104,\ 32832\}$;*

2. *if $S_1 = \{3\}$ and $S_2 = \{2,\ 5\}$ then $n \in \{1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 9,\ 10,\ 12,\ 18,\ 27,\ 28,\ 30,\ 36,\ 54,\ 81,\ 82,\ 84,\ 90,\ 108,\ 162,\ 252,\ 270,\ 324,\ 729,\ 756,\ 810,\ 6561,\ 6570\}$;*

3. *if $S_1 = \{5\}$ and $S_2 = \{2,\ 3\}$ then $n \in \{1,\ 2,\ 3,\ 5,\ 6,\ 10,\ 25,\ 26,\ 27,\ 30,\ 50,\ 125,\ 126,\ 130,\ 150,\ 625,\ 630,\ 650,\ 3125,\ 3126,\ 15625,\ 78750\}$.*

Proof of Theorem 4.4. If $w^+_{S_1}(n) + w^+_{S_2}(n) = 2$, then it is clear that the only solution is $n = 1$, so we suppose that $w^+_{S_1}(n) + w^+_{S_2}(n) \geq 3$. We describe the method in detail only in the case when $S_1 = \{3\}$, $S_2 = \{2, 5\}$, the other cases can be handled similarly. In this case we have five equations to solve, namely:

$$\begin{aligned}
3^{x_1} &= 2^{y_1} \cdot 5^{z_1} + 2^{y_2} \cdot 5^{z_2}, \\
3^{x_1} &= 2^{y_1} \cdot 5^{z_1} + 2^{y_2} \cdot 5^{z_2} + 2^{y_3} \cdot 5^{z_3}, \\
3^{x_1} + 3^{x_2} &= 2^{y_1} \cdot 5^{z_1}, \\
3^{x_1} + 3^{x_2} &= 2^{y_1} \cdot 5^{z_1} + 2^{y_2} \cdot 5^{z_2}, \\
3^{x_1} + 3^{x_2} + 3^{x_3} &= 2^{y_1} \cdot 5^{z_1}.
\end{aligned}$$

To find all solutions of the above equations we apply the algorithm from Section 3. We only concentrate on how to use it for the present equations. First

by an exhaustive search we find all "small" solutions of the equations in non-negative integers x_i, y_i, z_i, $(i = 1, 2, 3)$. Then after modifying the equations appropriately we try to find a modulus m such that the modified equation has no solutions modulo m. Consider the equation

$$3^{x_1} = 2^{y_1} \cdot 5^{z_1} + 2^{y_2} \cdot 5^{z_2}$$

in non-negative integers x_1, y_1, z_1, y_2, z_2. We may clearly assume that here $y_1 \leq y_2$, and $z_1 \leq z_2$ if $y_1 = y_2$. By an exhaustive search we get that under this assumption the equation has only five solutions with $x_1,\ y_1,\ z_1,\ y_2,\ z_2 \leq 100$, namely

$$\begin{aligned}(x_1,\ y_1,\ z_1,\ y_2,\ z_2) = &(1,\ 0,\ 0,\ 1,\ 0),\ (2,\ 0,\ 0,\ 3,\ 0),\ (4,\ 0,\ 0,\ 4,\ 1),\\ &(2,\ 0,\ 1,\ 2,\ 0),\ (3,\ 0,\ 2,\ 1,\ 0),\end{aligned}$$

yielding $n = 3,\ 9,\ 27,\ 81$. Note that $9 = 3^2$ appears in two different solutions, since $9 = 1 + 8 = 5 + 4$. We suspect that the equation has no other solutions. First it can be seen that if both y_1 and y_2 are greater than zero then this equation has no solutions modulo 2. The same argument applies for z_1, z_2 modulo 5, thus we conclude that we have to solve the following two equations:

$$3^{x_1} = 1 + 2^{y_2} \cdot 5^{z_2}, \tag{4.20}$$

$$3^{x_1} = 5^{z_1} + 2^{y_2}. \tag{4.21}$$

Since in every "small" solution the exponent of 3 is at most 4, then instead of

the equations above, we consider

$$3^5 \cdot 3^{x_{1,0}} = 1 + 2^{y_2} \cdot 5^{z_2}, \tag{4.22}$$

$$3^5 \cdot 3^{x_{1,0}} = 5^{z_1} + 2^{y_2}, \tag{4.23}$$

respectively, where every exponent is a non-negative integer. If our expectation is true, then these equations have no solutions. To prove this, we show that these equations are already not solvable locally, modulo an appropriately chosen modulus. About how to find such a modulus, we refer once again to Section 3. Now we only state that if we choose m to be $3^5 \cdot 7 \cdot 13 \cdot 17 \cdot 19 \cdot 37 \cdot 73 \cdot 97 \cdot 109 \cdot 163 \cdot 193 \cdot 257 \cdot 433 \cdot 487 \cdot 577 \cdot 769 \cdot 1153 \cdot 1297 \cdot 2593 \cdot 3457 \cdot 10369$, then as one can check, equation (4.22) has no solutions modulo m. Thus, in (4.20), x_1 has to be less than or equal to 4. By checking every possibility we get that this equation has three solutions, namely

$$(x_1,\, y_2,\, z_2) = (1,\, 1,\, 0),\, (2,\, 3,\, 0),\, (4,\, 4,\, 1).$$

Similarly, if $m = 3^5 \cdot 7 \cdot 13 \cdot 17 \cdot 19 \cdot 37 \cdot 73 \cdot 97 \cdot 109 \cdot 163 \cdot 193 \cdot 433 \cdot 577 \cdot 769$, then equation (4.23) has no solutions modulo m, thus we only have to check (4.21) with $x_1 \leq 4$. In this case we get the remaining two "small" solutions. The other equations can be handled similarly. Finally, we mention that an appropriately chosen divisor of $M = 2^{16} \cdot 3^{10} \cdot 5^8 \cdot 7 \cdot 13 \cdot 17 \cdot 19 \cdot 163 \cdot 37 \cdot 433 \cdot 193 \cdot 97 \cdot 73 \cdot 257 \cdot 109 \cdot 577 \cdot 769 \cdot 487 \cdot 1153 \cdot 1297 \cdot 1459 \cdot 2593 \cdot 2917 \cdot 3457 \cdot 3889 \cdot 10369 \cdot 1373 \cdot 3137 \cdot 12289 \cdot 17497 \cdot 18433 \cdot 39367 \cdot 52489 \cdot 65537 \cdot 50177 \cdot 139969 \cdot 147457 \cdot 209953 \cdot 331777 \cdot 472393 \cdot 114689 \cdot 268913 \cdot 470597 \cdot 629857 \cdot 746497 \cdot 786433 \cdot 839809 \cdot 995329 \cdot 614657$ is sufficient for every equation under investigation. □

References

[1] Zs. Ádám, L. Hajdu, F. Luca, *Representing primes as linear combinations of pure powers*, Acta Arith. **138** (2009), 101–107.

[2] L. J. Alex, L. L. Foster, *On the diophantine equation* $1 + x + y = z$, Rocky Mountain J. Math. **22** (1992), 11–62.

[3] L. J. Alex, L. L. Foster, *On the diophantine equation* $w+x+y = z$*, with* $wxyz = 2^r 3^s 5^t$, Revista Mat. Univ. Comp. Madrid **8** (1995), 13–48.

[4] F. Amoroso, E. Viada, *Small points on subvariaties of a torus*, Duke Math. J. **150** (2009), 407–442.

[5] A. Baker, *Linear forms in the logarithms of algebraic numbers*, Mathematika, **13** (1966), 204–216.

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

[7] B. Bartolome, Y. Bilu, F. Luca, *On the exponential local-global principle*, Acta Arith. **159** (2013), 101–111.

[8] M. Bennett, *Effective* S*-unit equations and a conjecture of Newman*, unpublished conference talk, Marseille-Luminy, 2010.

[9] Cs. Bertók, *Representing integers as sums or differences of general power products*, Acta Mathematica Hungarica **141** (2013), 291–300.

[10] Cs. Bertók, *The complete solution of the Diophantine equation* $(4m^2 + 1)^x + (5m^2 - 1)^y = (3m)^z$, Periodica Mathematica Hungarica **72** (2016), 37–42.

[11] Cs. Bertók, K. Győry, L. Hajdu, A. Schinzel, *On the smallest number of terms of vanishing sums of units in number fields*, Journal of Number Theory **192** (2018), 328–347.

[12] Cs. Bertók, L. Hajdu, *On a Hasse-type principle for exponential diophantine equations and its applications*, Mathematics of Computations **85** (2016), 849–860.

[13] Cs. Bertók, L. Hajdu, *A Hasse-type principle for exponential Diophantine equations over number fields and its applications*, Monatshefte für Mathematik **187** (2018), 425–436.

[14] Cs. Bertók, L. Hajdu, F. Luca, D. Sharma, *On the number of non-zero digits of integers in multi-base representations*, Publicationes Mathematicae Debrecen, **90** (2017), 181-194.

[15] Cs. Bertók, L. Hajdu, A. Pethő, *On the distribution of polynomials with bounded height*, Journal of Number Theory **179** (2017), 172–184.

[16] Cs. Bertók, L. Hajdu, I. Pink, Zs. Rábai, *Linear combinations of prime powers in binary recurrence sequences*, International Journal of Number Theory, **13** (2017), 261–271.

[17] Cs. Bertók, G. Nyul, *On monochromatic linear recurrence sequences*, Contributions to Discrete Mathematics, **11** (2016), 58–62.

[18] Cs. Bertók, A. Pethő, M. Pohst, *On multidimensional Diophantine approximation of algebraic numbers*, Journal of Number Theory, **171** (2017), 422–448.

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

[20] J. L. Brenner, L. L. Foster, *Exponential diophantine equations*, Pacific J. Math. **101** (1982), 263–301.

[21] Y. Bugeaud, M. Cipu, M. Mignotte, *On the representation of Fibonacci and Lucas numbers in an integer base*, Ann. Math. Québec **37** (2013), 31–43.

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

[23] K. C. Chim, I. Pink, V. Ziegler, *On a variant of Pillai's problem*, International Journal of Number Theory, **13** (2017), 1711–1727.

[24] M. Ddamulira, F. Luca, M. Rakotomalala, *On a Problem of Pillai with Fibonacci Numbers and Powers of* 2, Proc. Indian Acad. Sci. (Math. Sci.), **127** (2017), 411–421.

[25] V. S. Dimitrov, E. W. Howe, Lower bounds on the lengths of double-base representations, *Proc. Amer. Math. Soc.*, **139** (2011), 3423–3430.

[26] P. Erdős, C. Mauduit, A. Sárközy, *On arithmetic properties of integers with missing digits. I. Distribution in residue classes*, Journal of Number Theory **70** (1998), 99–120.

[27] P. Erdős, C. Mauduit, A. Sárközy, *On arithmetic properties of integers with missing digits. II. Prime factors*, Discrete Math. **200** (1999), 149–164. Paul Erdős memorial collection.

[28] P. Erdős, C. Pomerance, E. Schmutz, *Carmichael's lambda function*, Acta Arith. **58** (1991), 365–385.

[29] J.-H. Evertse, *On sums of S-units and linear recurrences*, Compositio Math. **53** (1984), 225–244.

[30] J.-H. Evertse, *The number of solutions of decomposable form equations*, Invent. Math. **122** (1995), 559–601.

[31] J.-H. Evertse, K. Győry, *On the number of solutions of weighted unit equations*, Compositio Math. **66** (1988), 329–354.

[32] J.-H. Evertse, K. Győry, *Unit Equations in Diophantine Number Theory*, pp. 378, Cambridge University Press, Cambridge (2015).

[33] J.-H. Evertse, K. Győry, C. Stewart, R. Tijdeman, *S-unit equations and their applications*, New Advances in Transcendence Theory (A. Baker, ed.), 110–174, Cambridge University Press, Cambridge (1988).

[34] J. H. Evertse, H. P. Schlickewei and W. M Schmidt, *Linear equations in variables which lie in a multiplicative group*, Annals of Math. **155** (2002), 807–836.

[35] K. Győry, *On the number of solutions of linear equations in units of an algebraic number field*, Comment. Math. Helv. **54** (1979), 583–600.

[36] K. Győry, *Résultats effectifs sur la représentation des entiers par des formes décomposables*, Queen's Papers in Pure and Appl. Math. **56** (1980).

[37] L. Hajdu, F. Luca, *On the length of arithmetic progressions in linear combinations of S-units*, Arch. Math. **94** (2010), 357–363.

[38] L. Hajdu, R. Tijdeman, *Representing integers as linear combinations of powers*, Publ. Math. Debrecen **79** (2011), 461–468.

[39] L. Hajdu, R. Tijdeman, *Representing integers as linear combinations of power products*, Arch. Math. **98** (2012), 527–533.

[40] N. Irmak, L. Szalay, *Tribonacci Numbers Close to the Sum* $2^a + 3^b + 5^c$, Math. Scand. **118** (2016), 27–32.

[41] L. Jeśmanowicz, *Some remarks on Pythagorean numbers*, Wiadom. Mat. **1** (1955/1956), 196–202.

[42] T. Kovács, *Combinatorial numbers in binary recurrences*, Period. Math. Hungar. **58** (2009), 83–98.

[43] T. Kovács, K. Liptai, P. Olajos, *On* (a, b)*-balancing numbers*, Publ. Math. Debrecen **77** (2010), 485–498.

[44] E. Landau, *Neuer Beweis des Primzahlsatzes und Beweis des Primidealsatzes*, Math. Ann. **56** (1903), 645–670.

[45] M. Laššák, Š. Porubský, *Fermat-Euler theorem in algebraic number fields*, J. Number Theory **60** (1996), 254–290.

[46] C. Lech, *A Note on Recurring Series*, Arkiv för Matematik **2** (1953), 417–421.

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

[48] F. Luca, *Distinct digits in base* b *expansions of linear recurrence sequences*, Quaest. Math. **23** (2000), 389–404.

[49] K. Mahler, *"Eine arithmetisehe Eigenschaft der Taylor-koeffizienten ralionaler Funktionen"*, Akad. Wetensch. Amsterdam, Proc. **38** (1935), 50–60

[50] D. Marques, A. Togbé, Fibonacci and Lucas numbers of the form $2^a + 3^b + 5^c$, *Proc. Japan Acad. Ser. A Math Sci.* **89** (2013), 47–50.

[51] E. M. Matveev, *An explicit lower bound for a homogeneous rational linear form in the logarithms of algebraic numbers II*, Izv. Ross. Akad. Nauk Ser. Mat. **64** (2000), 125–180; translation in Izv. Math. **64** (2000) 1217–1269.

[52] C. Mauduit, C. Pomerance, A. Sárközy, *On the distribution in residue classes of integers with a fixed sum of digits*, Ramanujan J. **9** (2005), 45–62.

[53] C. Mauduit, A. Sárközy, *On the arithmetic structure of sets characterized by sum of digits properties*, Journal of Number Theory **61** (1996), 25–38.

[54] C. Mauduit, A. Sárközy, *On the arithmetic structure of the integers whose sum of digits is fixed*, Acta Arith. **81** (1997), 145–173.

[55] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, pp. 712, Springer-Verlag Berlin Heidelberg (2004).

[56] M. B. Nathanson, *Geometric group theory and arithmetic diameter*, Publ. Math. Debrecen **79** (2011), 563–572.

[57] G. K. Panda, *Sequence balancing and cobalancing numbers*, Fibonacci Quart. **45**, 265–271 (2008).

[58] A. Pethő, *Perfect powers in second order linear recurrences*, J. Number Theory **15** (1982) 5–13.

[59] A. Pethő, B. M. M. de Weger, *Products of Prime Powers in Binary Recurrence Sequences, Part I: The Hyperbolic Case, with an Application to the Generalized Ramanujan-Nagell Equation*, Math. Comp. **47** (1986), 714–727.

[60] A. Pethő, *The Pell sequence contains only trivial perfect powers*, Proc. Sets Graphs and Numbers. Coll. Math. Soc. János Bolyai Vol. **60** (1992), 561–568.

[61] A. Pethő, R. F. Tichy, *On digit expansions with respect to linear recurrences*, J. Number Theory **33** (1989), 243–256.

[62] A. Pethő, R. F. Tichy, *S-unit equations, linear recurrences and digit expansions*, Publ. Math. Debrecen **42** (1993), 145–154.

[63] P. Pollack, *A simple proof of a theorem of Hajdu–Jarden–Narkiewicz*, Colloq. Math. **147** (2017), 217–220.

[64] J. L. Ramírez Alfonsín, *The Diophantine Frobenius Problem*, Oxford Univ. Press (2005).

[65] S. G. Sanchez, F. Luca, *Linear combinations of factorials and S-units in a binary recurrence sequence*, Ann. Math. Qué. **38** (2014), 169–188.

[66] A. Schinzel, *On power residues and exponential congruences*, Acta Arith. **27** (1975), 397–420.

[67] A. Schinzel, *Abelian binomials, power residues and exponential congruences*, Acta Arith. **32** (1977), 245–274.

[68] A. Schinzel, *Addendum and corrigendum to the paper "Abelian binomials, power residues and exponential congruences", Acta Arith. 32(1977), pp. 245-274*, Acta Arith. **36** (1980), 101–104.

[69] H. P. Schlikewei, *Linear equations in integers with bounded sum of digits*, J. Number Theory **35** (1990), 335–344.

[70] E. Selmer, *The diophantine equation* $ax^3 + by^3 + cz^3 = 0$, Acta Math. **85** (1951), 203–362.

[71] H. G. Senge, E. G. Straus, *PV-numbers and sets of multiplicity*, Period. Math. Hungar. **3** (1973), 93–100.

[72] T. N. Shorey, C. L. Stewart, *On the Diophantine equation* $ax^{2t} + bx^t y + cy^2 = d$ *and pure powers in recurrence sequences*, Math. Scand. **52** (1983), 24–36.

[73] T. N. Shorey, R. Tijdeman, *Exponential Diophantine Equations*, Cambridge University Press, Cambridge, 1986.

[74] T. Skolem, *Einige Sätze über gewisse Reihenentwicklungen und exponentiale Beziehungen mit Anwendung auf diophantische Gleichungen*, Oslo Vid. akad. Skrifter, I (6) (1933).

[75] T. Skolem, *Anwendung exponentieller Kongruenzen zum Beweis der Unlsbarkeit gewisser diophantischer Gleichungen*, Vid. akad. Avh. Oslo I 1937 nr 12.

[76] J. Su, X. Li, *The Exponential Diophantine Equation* $(4m^2+1)^x+(5m^2-1)^y = (3m)^z$, Abstr. Appl. Anal. **2014** (2014), Article ID 670175.

[77] W. A. Stein et al., *Sage Mathematics Software (Version 6.1.1)*, The Sage Development Team, 2014, http://www.sagemath.org.

[78] C. L. Stewart, *On the representation of an integer in two different bases*, J. Reine Angew. Math. **319** (1980), 63–72.

[79] Sz. Tengely, *Balancing numbers which are products of consecutive integers*, Publ. Math. Debrecen **83** (2013), 197–205.

[80] N. Terai, *The Diophantine Equation* $a^x + b^y = c^z$, Proc. Japan Acad. Ser. A Math. Sci. **70** (1994), 22–26.

[81] N. Terai, *The Diophantine Equation* $a^x + b^y = c^z$*, II.*, Proc. Japan Acad. Ser. A Math. Sci. **71** (1995), 109–110.

[82] N. Terai, *The Diophantine Equation* $a^x + b^y = c^z$*, III.*, Proc. Japan Acad. Ser. A Math. Sci. **72** (1996), 20–22.

[83] N. Terai, *On the Exponential Diophantine Equation* $(4m^2+1)^x+(5m^2-1)^y = (3m)^z$, Internat. J. Algebra **6** (2012), 1135–1146.

[84] R. Tijdeman, *On integers with many small prime factors*, Compos. Math., **26** (1973), 319–330.

[85] R. Tijdeman, *On the maximal distance of integers composed of small primes*, Compos. Math., **28** (1974), 159–162.

[86] P. Vojta, *Integral Points on Varieties*, Dissertation, Harvard University, 1983.

Bertók Csanád publikációs jegyzéke

[i] Cs. Bertók, *Representing integers as sums or differences of general power products*, Acta Mathematica Hungarica **141** (2013), 291–300.

[ii] Cs. Bertók, *The complete solution of the Diophantine equation* $(4m^2 + 1)^x + (5m^2 - 1)^y = (3m)^z$, Periodica Mathematica Hungarica **72** (2016), 37–42.

[iii] Cs. Bertók, K. Győry, L. Hajdu, A. Schinzel, *On the smallest number of terms of vanishing sums of units in number fields*, Journal of Number Theory **192** (2018), 328–347.

[iv] Cs. Bertók, L. Hajdu, *On a Hasse-type principle for exponential diophantine equations and its applications*, Mathematics of Computations **85** (2016), 849–860.

[v] Cs. Bertók, L. Hajdu, *A Hasse-type principle for exponential Diophantine equations over number fields and its applications*, Monatshefte für Mathematik **187** (2018), 425–436.

[vi] Cs. Bertók, L. Hajdu, F. Luca, D. Sharma, *On the number of non-zero digits of integers in multi-base representations*, Publicationes Mathematicae Debrecen, **90** (2017), 181-194.

[vii] Cs. Bertók, L. Hajdu, A. Pethő, *On the distribution of polynomials with bounded height*, Journal of Number Theory **179** (2017), 172–184.

[viii] Cs. Bertók, L. Hajdu, I. Pink, Zs. Rábai, *Linear combinations of prime powers in binary recurrence sequences*, International Journal of Number Theory, **13** (2017), 261–271.

[ix] Cs. Bertók, G. Nyul, *On monochromatic linear recurrence sequences*, Contributions to Discrete Mathematics, **11** (2016), 58–62.

[x] Cs. Bertók, A. Pethő, M. Pohst, *On multidimensional Diophantine approximation of algebraic numbers*, Journal of Number Theory, **171** (2017), 422–448.

5 Összefoglaló

A disszertáció fő témaköre az egész számok exponenciális kifejezésekkel történő reprezentációs problémáinak vizsgálata. Az elméleti eredmények mellett bemutatunk egy algoritmust melynek segítségével meghatározhatjuk exponenciális Diofantikus egyenletek összes megoldását mind $\mathbb{Z}$, mind pedig számtestek egészeinek gyűrűje felett. Ezen eljárást alkalmazva pedig megoldunk több Diofantikus problémát is.

Elsőként tekintsük a reprezentációs problémákat. Legyenek $a_1, \ldots, a_l$ különböző pozitív egészek és legyen $A = \{a_1, \ldots, a_l\}$. Tekintsük az alábbi halmazt

$$A' := \{a_1^{x_1} \cdot \ldots \cdot a_l^{x_l} | x_1, \ldots, x_l \text{ nemnegatív egészek}\}.$$

Természetes problémaként merül fel a kérdés, miszerint legkevesebb hány elemre van szükségünk A'-ből ahhoz, hogy egy adott pozitív egészet kifejezhessünk ezen elemek összegeként? Amennyiben A csupán egyetlen b számból áll, úgy a kérdés lényegében a pozitív egészek felírására korlátozódik a b alapú számrendszerben. Amennyiben A mindössze két prímet tartalmaz, úgy úgynevezett "két alapú" reprezentációs problémáról beszélhetünk (kapcsolódó irodalomként ld. például Dimitrov és Howe [25] eredményeit). Definiáljuk az $F(k)$ $(k \in \mathbb{N})$ függvényt úgy, hogy jelentse a legkisebb olyan természetes számot, melyet nem tudunk előállítani k-nál kevesebb A'-beli elem összegeként. Legyen továbbá $F_{\pm}(k)$ hasonlóan definiálva, azzal az eltéréssel, hogy A' helyett az $A'_{\pm} = A' \cup (-A')$ halmazt használjuk. Amennyiben $F(k)$ és $F_{\pm}(k)$ tulajdonságaira vagyunk kíváncsiak, úgy eljutunk egy Nathanson [56] által vizsgált problémakörhöz.

A 2.1-es fejezetben alsó korlátot adunk mind $F(k)$-ra, mind pedig $F_{\pm}(k)$-

ra abban az általános esetben amikor A tetszőleges egészekből áll. Az alábbi tételeket látjuk be.

2.1. Tétel (2.1-es Tétel [9]-ben)**.** *Legyenek $A, A', A'_{\pm}, F(k)$ és $F_{\pm}(k)$ a fentiek szerint definiálva és tegyük fel, hogy A tartalmaz két multiplikatíve független elemet. Ekkor minden $k > 1$ esetén:*

i) $F(k) > k^{C_1 k}$*, ahol C_1 egy csak A-tól függő konstans.*

ii) $F(k) < C_2(kl)^{(1+\varepsilon)kl}$ *minden $\varepsilon > 0$ esetén, ahol C_2 egy csak ε-tól függő konstans,*

iii) $F_{\pm}(k) < \exp((kl)^{C_3})$*, ahol C_3 egy abszolút konstans.*

2.2. Tétel (2.1-es Állítás [9]-ben)**.** *Amennyiben A elemei páronként multiplikatíve függőek, úgy léteznek olyan, csak A-tól függő $1 < C_4 < C_5$ konstansok, hogy*

$$C_4^k < F(k) \leq F_{\pm}(k) < C_5^k \quad \textit{minden } k > 1 \textit{ esetén.}$$

Ezen eredmények megválaszolják Nathanson [56] egy kérdését és kiterjesztik Hajdu és Tijdeman [38, 39] eredményeit. Az így nyert korlátok továbbá igen élesek.

A fentiekhez kapcsolódó problémakör azon egészek vizsgálata, melyek valamely speciális számrendszerbeli előállításában csupán "néhány" nem-nulla számjegy szerepel (kapcsolódó eredményekért ld. többek között Erdős, Mauduit, Pomerance, Sárközy [26, 27, 52, 53, 54] munkáit, illetve az ott szereplő hivatkozásokat). A 2.2-es fejezetben ún. "többalapú" reprezentációs problémákkal foglalkozunk. Ezen alfejezetben egész számok olyan "többalapú" számrendszerbeli előállításait vizsgáljuk, mely előállításoknak csupán "néhány" nem-nulla számjegyük van egyszerre több ilyen számrendszerben. Eh-

hez legyen S prímeknek egy véges halmaza és jelölje $\mathbb{Z}_S$ (hasonlóan $\mathbb{Z}_S^+$) egészek (hasonlóan pozitív egészek) azon halmazát, melyeknek nincs S-en kívüli prímosztójuk. A fejezetben az egész n-ek

$$n = u_1 + \cdots + u_t$$

alakú reprezentációival foglalkozunk, ahol $u_1, \ldots u_t \in \mathbb{Z}_S$. Jelölje továbbá $w_S(n)$ azt a legkisebb t számot, melyre a fenti egyenletnek van megoldása. Amennyiben n pozitív és az egyenlet jobb oldalán szereplő számok a $\mathbb{Z}_S^+$ halmaz elemei, úgy a fenti jelölés helyett $w_S^+(n)$-t írunk. Az alfejezetben az alábbi tételeket bizonyítjuk.

2.4. Tétel (2.1-es Tétel [14]-ben)**.** *Legyen k egy pozitív egész, $S_1, \ldots, S_k$ pedig prímeket tartalmazó olyan véges halmazok, melyekre $S_1 \cap \cdots \cap S_k = \emptyset$. Ekkor bármely T-re a*

$$w_{S_1}^+(n) + \cdots + w_{S_k}^+(n) \leq T$$

egyenlőtlenség csupán véges sok egész n esetén áll fent. Továbbá ezen egész n-ek száma legfeljebb $C_{14} = C_{14}(T,\, k,\, s)$, ahol C_{14} egy effektíven meghatározható konstans, mely csupán T-től, k-tól és $s := |S_1 \cup \cdots \cup S_k|$-tól függ.

2.5. Tétel (2.2-es Tétel [14]-ben)**.** *Legyen ℓ egy pozitív egész és legyenek $p_1, \ldots, p_\ell,\, q$ különböző prímek. Legyen továbbá $S_1 = \{p_1, \ldots, p_\ell\}$ és $S_2 = \{q\}$. Ha n egy olyan pozitív egész, melyre $n > e^{e^e}$ és $w_{S_1}^+(n) = 1$, úgy*

$$w_{S_2}^+(n) > \frac{C_{15} \log\log n}{\log\log\log n},$$

ahol $C_{15} = C_{15}(\ell,\, p_1, \ldots, p_\ell,\, q)$ egy effektíven meghatározható, csak $\ell,\, p_1, \ldots, p_\ell,\, q$ értékétől függő pozitív konstans.

A 2.3-as fejezetben binér rekurzív sorozatok előállításával foglalkozunk

hatványok lineáris kombinációjaként. Marques és Togbé [50] bizonyos megkötések mellett meghatározták az összes olyan Fibonacci és Lucas számot, melyek előállnak, a $2, 3, 5$ számok hatványainak összegeként. Pethő és de Weger [59] kifejlesztettek egy algoritmust az $U_n = wp_1^{x_1} \cdot \ldots \cdot p_m^{x_m}$ Diofantikus egyenlet megoldására, ahol U_n egy pozitív diszkriminánsú binér rekurzív sorozat. Pethő [58], illetve Shorey és Stewart [72] egymástól függetlenül belátták, hogy bizonyos feltételek teljesülése mellett egy lineáris rekurzív sorozat csupán véges sok teljes hatványt tartalmazhat. Néhány speciális rekurzív sorozat esetén lehetőség van meghatározni a sorozatban előforduló összes teljes hatványt is. A Pell sorozat esetén Pethő [60] belátta, hogy a sorozat nem tartalmaz nem-triviális hatványokat. Bugeaud, Mignotte és Siksek [22] bizonyította, hogy a Fibonacci sorozatban csupán a $0, 1, 8$, illetve a 144 fordulnak elő mint teljes hatványok, míg a Lucas sorozatban csupán az 1 és a 4 jelennek meg. Pethő és Tichy [62] eredményei alapján ismert, hogy csupán véges sok olyan Fibonacci szám létezik, mely előáll $p^x + p^y + p^z$ alakban, ahol p egy rögzített prím. Kovács [42] megtalálta a Fibonacci, Lucas, Pell és asszociált Pell sorozatokban szereplő összes, bizonyos tulajdonságokkal rendelkező kombinatorikus számot. Ezen fejezetben az alábbi tételt látjuk be.

2.6. Tétel (2.1-es Tétel [16]-ban)**.** *Legyen U_n egy nem-degenerált, pozitív diszkriminánsú binér rekurzió, $p_1 \leq p_2 \leq \cdots \leq p_s$ pedig adott, nem szükségszerűen különböző prímek. Legyenek továbbá $b_1, \ldots, b_s$ nem-nulla egészek. Legyen végül $T = \max_{1 \leq i \leq s} |b_i|$. A fejezetben felhasznált jelölések mellett tegyük fel továbbá, hogy $\log(|a/b_s\sqrt{D}|)$, $\log|\alpha|$ és $\log p_s$ lineárisan függetlenek a racionális számok felett.*

Tekintsük az

$$U_n = b_1 p_1^{x_1} + b_2 p_2^{x_2} \cdots + b_s p_s^{x_s} \tag{2.29}$$

egyenletet, ahol $n, x_1, \dots, x_s$ *nemnegatív egész ismeretlenek. Legyen* $0 < \varepsilon < 1$*, és jelölje* H_ε *azon* $(n, x_1, \dots, x_s)$ *megoldások halmazát, melyekre egyrészt* $x_s = \max_{1 \le i \le s} x_i$ *teljesül, másrészt pedig azon* $i = 1, \dots, s-1$ *indexek esetén, melyekre* $p_i = p_s$*, az* $x_i < (1-\varepsilon)x_s$ *egyenlőtlenség is fennáll. Ekkor* H_ε *véges, és minden* $(n, x_1, \dots, x_s) \in H_\varepsilon$ *esetén*

$$\max\{n, x_1, \dots, x_s\} < C_{16}$$

teljesül, ahol C_{16} *egy effektíven meghatározható konstans, mely csupán az* $\varepsilon, A, B, U_0, U_1, T, s, p_s$ *paraméterektől függ.*

A harmadik fejezetben olyan

$$a_1 b_{11}^{x_{11}} \dots b_{1\ell}^{x_{1\ell}} + \dots + a_k b_{k1}^{x_{k1}} \dots b_{k\ell}^{x_{k\ell}} = c \qquad \text{(A)}$$

alakú exponenciális Diofantikus egyenletekkel foglalkozunk, ahol az $x_{11}, \dots, x_{1\ell}, \dots, x_{k1}, \dots, x_{k\ell}$ kitevők ismeretlen nemnegatív egészek, míg az együtthatók, alapok, illetve az egyenlet jobb oldala előre megadott egészek. A disszertációban fontos szerepet játszik a fenti egyenletből kapható kongruencia (valamilyen $m \ge 2$ modulus szerint), így ezt a későbbiekben (A')-vel jelöljük. Ha $k = 2$ (vagy bizonyos megszorítások mellett ha $k = 3, 4$), akkor a Baker módszer segítségével lehetőségünk van meghatározni egy felső korlátot a fenti egyenlet megoldásainak nagyságára. Ehhez kapcsolódó eredményekért ld. többek között Győry [35] munkáját, vagy Evertse és Győry [32] könyvét. Azonban teljes általánosságban amennyiben $k \ge 3$, úgy ez a probléma lényegesen nehezebbé válik. Ebben az esetben a Baker módszer nem használható, a rendelkezésünkre álló altér tétel pedig egyrészt ineffektív, másrészt csupán a nem-degenerált megoldások számára ad felső korlátot, azok nagyságára nem. Ehhez kapcsolódó irodalomért ld. Evertse [29] munkáját, Evertse és Győry

[32] könyvét, illetve az ott található hivatkozásokat. Igen fontos megjegyezni, hogy a szakirodalomban nincs olyan ismert algoritmus, melynek segítségével lehetséges lenne a fenti típusú egyenletek összes megoldásának meghatározása. Ebben a fejezetben bemutatunk egy heurisztikus algoritmust ezen egyenletcsalád megoldásainak megkeresésére. Algoritmusunk Skolem exponenciális kongruenciákra kimondott sejtésén alapul. A 3.1-es fejezetben több numerikus eredmény mellett az alábbi tételt bizonyítjuk.

3.1. Tétel (2.1-es Tétel [12]-ben)**.** *Legyenek az* $a_1, \ldots, a_k$ *együtthatók és* $b_{11}, \ldots, b_{1\ell}, \ldots, b_{k1}, \ldots, b_{k\ell}$ *alapok rögzítettek és definiáljuk* H*-t a következőképp:*

$$H = \{c \in \mathbb{Z} \ : \ \text{(A) } \textit{nem megoldható, de } \text{(A') } \textit{megoldható minden } m \textit{ esetén}\}.$$

Ekkor H *sűrűsége* 0 *a*

$$H_0 = \{c \in \mathbb{Z} \ : \ \text{(A) } \textit{nem megoldható}\}$$

halmazban.

A 3.2-es fejezetben egy, a 3.1-es fejezetben bemutatott problémához hasonlóval foglalkozunk, azzal a különbséggel, hogy ahelyett, hogy az egyenletünket és a hozzá kapcsolódó kongruenciát $\mathbb{Z}$ felett vizsgálnánk, most az együtthatók, alapok és a jobb oldal is egy tetszőleges algebrai számtest egészeinek gyűrűjéből kerülnek ki. Több tételt bizonyítunk, mely Skolem sejtésének számtestekre való kiterjesztéséhez kapcsolódik, illetve bemutatjuk az algoritmusunk kiterjesztett változatát, mellyel lehetővé válik az (A) alakú egyenletek megoldásainak meghatározása algebrai számtestek egészeiben. Végezetül több numerikus eredménnyel demonstráljuk ezen algoritmus hatékonyságát. A fejezetben szereplő eredmények a [13] cikkben kerültek közlésre.

A negyedik fejezetben bemutatunk néhány – az előző fejezetekben felmerült problémákhoz kapcsolódó – alkalmazást. Ezen tételek és alkalmazások a [10, 13, 14, 16] cikkeinkben szerepelnek. A 4.1-es fejezetben Terai egy klasszikus sejtését bizonyítjuk. Legyen t egy tetszőleges, de rögzített pozitív egész, x, y, illetve z pedig ismeretlen pozitív egészek. A fejezetben meghatározzuk a

$$(4t^2+1)^x + (5t^2-1)^y = (3t)^z$$

egyenlet megoldásait. A 4.2-es fejezetben rekurzív sorozatok hatványösszegekként történő előállításával foglalkozunk. Ehhez legyen U_n a Fibonacci, Lucas, Pell, vagy asszociált Pell sorozat n-edik tagja, x, y, z pedig ismeretlen nemnegatív egészek. Ezen fejezetben megadjuk az

$$U_n = 2^x + 3^y \quad \text{és} \quad U_n = 2^x + 3^y + 5^z$$

egyenletek összes megoldását. A 4.3-as fejezetben egy ehhez kapcsolódó problémát vizsgálunk. Jelentse B_i az i-edik balansz számot. A fejezetben meghatározzuk a

$$B_u + B_v + B_w = b^z$$

egyenlet összes u, v, w, z nemnegatív egész megoldását a $b \in \{2, 3, 5, 7\}$ feltétel mellett. Végül a 4.4-es fejezetben a többalapú reprezentációkhoz kapcsolódó alkalmazásokkal foglalkozunk. Ehhez legyenek S_1 és S_2 diszjunkt, nemüres halmazok, melyekre $S_1 \cup S_2 = \{2, 3, 5\}$ teljesül. Legyen továbbá $w_S^+(n)$ a jelen bevezető elején megadott módon definiálva. Ebben a fejezetben meghatározzuk a

$$w_{S_1}^+(n) + w_{S_2}^+(n) \leq 4$$

egyenlőtlenség összes megoldását.

6. Summary

In this dissertation, we consider representation problems of integers as expressions involving exponential terms. We also give algorithms which can be used to solve exponential Diophantine equations over $\mathbb{Z}$ and rings of integers of number fields. As applications, by using our method we solve some Diophantine problems, too.

First, we consider representation problems. Let $a_1, \ldots, a_l$ be distinct positive integers and put $A = \{a_1, \ldots, a_l\}$. Consider the set

$$A' := \{a_1^{x_1} \cdot \ldots \cdot a_l^{x_l} | x_1, \ldots, x_l \text{ are non-negative integers}\}.$$

A natural question to ask is that at least how many elements do we need from A' to represent a given positive integer as their sum? If A consists of only one number b then the question basically asks about the representation of positive integers in the base b number system. If A consists of two primes, then we have a so-called "double base" representation problem (as a related paper, see e.g. the work of Dimitrov and Howe [25]). If we define the function $F(k)$ $(k \in \mathbb{N})$ to be the smallest natural number which cannot be represented as the sum of less than k terms from A', and $F_{\pm}(k)$ to be the function defined similarly, except that A' is replaced by $A'_{\pm} = A' \cup (-A')$ and ask about the properties of $F(k)$ and $F_{\pm}(k)$, then we get a similar problem proposed by Nathanson [56].

In Section 2.1, we give a lower and upper bound for $F(k)$ and $F_{\pm}(k)$ in the case, where A consists of arbitrary integers. We prove the following theorems.

Theorem 2.1 (Theorem 2.1 in [9])**.** *Let $A, A', A'_{\pm}, F(k)$ and $F_{\pm}(k)$ be as above and suppose that A has two multiplicatively independent elements. Then for every $k > 1$ we have:*

i) $F(k) > k^{C_1 k}$, where C_1 is a constant depending only on A,

ii) $F(k) < C_2(kl)^{(1+\varepsilon)kl}$ *for every* $\varepsilon > 0$*, where* C_2 *is a constant depending only on* ε*,*

iii) $F_{\pm}(k) < \exp((kl)^{C_3})$*, where* C_3 *is an absolute constant.*

Theorem 2.2 (Proposition 2.1 in [9])**.** *If all pairs of elements of* A *are multiplicatively dependent, then there exist constants* $1 < C_4 < C_5$ *depending only on* A *such that*

$$C_4^k < F(k) \leq F_{\pm}(k) < C_5^k \quad \textit{for all } k > 1.$$

These results answer a question of Nathanson [56] in the above setting, and extend results of Hajdu and Tijdeman [38, 39]. These bounds are relatively sharp, as well.

Another related topic is the analysis of integers which have only "few" non-zero digits in a special number system (see e.g. papers by Erdős, Mauduit, Pomerance, Sárközy [26, 27, 52, 53, 54] and the references there). In Section 2.2 we consider multi-base representations. In this subsection we study representations of integers which have only a "few" non-zero digits in different multi-base representations simultaneously. For this, let S be a finite set of primes, and write $\mathbb{Z}_S$ (resp. $\mathbb{Z}_S^+$) for the set of integers (resp. positive integers) having no prime divisors outside S. We consider the representations of integers n of the form

$$n = u_1 + \cdots + u_t$$

with $u_1, \ldots u_t \in \mathbb{Z}_S$. We write $w_S(n)$ for the minimal t for which the above equation holds. If n is positive and the numbers on the right hand side are elements of $\mathbb{Z}_S^+$, we write $w_S^+(n)$ instead. In this subsection we prove the following theorems

Theorem 2.4 (Theorem 2.1 in [14]). *Let k be a positive integer, $S_1, \ldots, S_k$ be finite sets of primes such that $S_1 \cap \cdots \cap S_k = \emptyset$. Then for any T the inequality*

$$w^+_{S_1}(n) + \cdots + w^+_{S_k}(n) \leq T$$

is valid only for finitely many integers n. Furthermore, the number of such integers n is at most $C_{14} = C_{14}(T,\ k,\ s)$, where C_{14} is an effectively computable constant depending only on $T,\ k$ and $s := |S_1 \cup \cdots \cup S_k|$.

Theorem 2.5 (Theorem 2.2 in [14]). *Let ℓ be a positive integer, $S_1 = \{p_1, \ldots, p_\ell\}$ and*
$S_2 = \{q\}$, where $p_1, \ldots, p_\ell,\ q$ are distinct primes. If n is a positive integer with $n > e^{e^e}$ such that $w^+_{S_1}(n) = 1$, then we have

$$w^+_{S_2}(n) > \frac{C_{15} \log\log n}{\log\log\log n},$$

where $C_{15} = C_{15}(\ell,\ p_1, \ldots, p_\ell,\ q)$ is an effectively computable positive constant depending only on $\ell,\ p_1, \ldots, p_\ell,\ q$.

In Section 2.3 we consider the problem of representation of terms of binary recurrence sequences as linear combinations of powers. Marques and Togbé [50] determined all Fibonacci and Lucas numbers which can be written as the sum of powers of $2, 3, 5$ under certain assumptions. Pethő and de Weger [59] gave an algorithm which can be used to solve the Diophantine equation $U_n = wp_1^{x_1} \cdot \ldots \cdot p_m^{x_m}$, where U_n is a binary recurrence sequence with positive discriminant. Pethő [58] and Shorey and Stewart [72] independently proved that under certain natural assumptions, a linear recurrence sequence may contain only finitely many perfect powers. In the case of some special, famous sequences all perfect powers have been determined. In the case of the Pell

sequence P_n, Pethő [60] proved that it does not contain non-trivial powers. Bugeaud, Mignotte and Siksek [22] proved that the Fibonacci-sequence F_n contains only the powers $0, 1, 8, 144$, and the only powers in the sequence of Lucas numbers L_n are $1, 4$. Results of Pethő and Tichy [62] imply that there are only finitely many Fibonacci numbers of the form $p^x + p^y + p^z$, where p is a fixed prime. Kovács [42] found all combinatorial numbers of certain shapes among the terms of F_n, L_n, P_n and Q_n (the associated Pell-sequence). We prove the following theorem.

Theorem 2.6 (Theorem 2.1 in [16])**.** *Let U_n be a non-degenerate binary recurrence sequence with a positive discriminant, $p_1 \leq p_2 \leq \cdots \leq p_s$ be given, not necessarily distinct prime numbers and $b_1, \ldots, b_s$ be nonzero integers. Put $T = \max_{1 \leq i \leq s} |b_i|$. Using the notations from the corresponding section, assume further that $\log(|a/b_s\sqrt{D}|)$, $\log|\alpha|$ and $\log p_s$ are linearly independent over the rationals.*

Consider the equation

$$U_n = b_1 p_1^{x_1} + b_2 p_2^{x_2} \cdots + b_s p_s^{x_s} \tag{2.29}$$

in non-negative integers $n, x_1, \ldots, x_s$. Let $0 < \varepsilon < 1$, and write H_ε for the set of those solutions $(n, x_1, \ldots, x_s)$, for which $x_s = \max_{1 \leq i \leq s} x_i$, and $x_i < (1-\varepsilon)x_s$ for those $i = 1, \ldots, s-1$ for which $p_i = p_s$. Then H_ε is finite, and for all $(n, x_1, \ldots, x_s)$ in H_ε we have

$$\max\{n, x_1, \ldots, x_s\} < C_{16},$$

where C_{16} is an effectively computable constant depending only on ε, A, B, U_0, U_1, T, s, p_s.

In Chapter 3 we consider exponential Diophantine equations of the form

$$a_1 b_{11}^{x_{11}} \dots b_{1\ell}^{x_{1\ell}} + \dots + a_k b_{k1}^{x_{k1}} \dots b_{k\ell}^{x_{k\ell}} = c \tag{A}$$

in non-negative integers $x_{11}, \dots, x_{1\ell}, \dots, x_{k1}, \dots, x_{k\ell}$, where the coefficients, bases and the right hand side are given integers. Denote by (A') the "congruence version" of (A) modulo $m \geq 2$. If $k = 2$ (under some restrictive assumptions if $k = 3, 4$), then by Baker's method it is possible to give an upper bound for the size of the solutions. For related results see e.g. Győry [35] or the book of Evertse and Győry [32]. However in general if $k \geq 3$ then this problem becomes significantly more difficult. In this case we cannot use Baker's method and we need to use the subspace theorem, which is ineffective, and is capable only to provide a bound for the number of non-degenerate solutions. Here we refer to Evertse [29], and again to the book of Evertse and Győry [32] and the references given there. It is important to note that there is no known algorithm in the literature, which would be capable to produce all the solutions of such an equation. In this chapter we give a heuristic algorithm for the solutions of exponential Diophantine equations based upon an extension of Skolem's conjecture involving exponential congruences. In Section 3.1 among some numerical results we prove the following theorem.

Theorem 3.1 (Theorem 2.1 in [12]). *Let $a_1, \dots, a_k, b_{11}, \dots, b_{1\ell}, \dots, b_{k1}, \dots, b_{k\ell}$ be fixed, and let H be defined by*

$$H = \{c \in \mathbb{Z} \ : \ \text{(A) } \textit{is not solvable, but } \text{(A') } \textit{is solvable for all } m\}.$$

Then H has density zero inside the set

$$H_0 = \{c \in \mathbb{Z} \ : \ \text{(A) } \textit{is not solvable}\}.$$

In Section 3.2 we consider a similar problem as in Section 3.1 with the difference that instead of working in $\mathbb{Z}$, now we work in the ring of integers of an arbitrary algebraic number field. We present several theorems related to an extension of Skolem's conjecture over number fields, and provide an extended algorithm which can be used to find the solutions of equations of type (A). Finally, we also give some numerical examples which demonstrate the usability of our algorithm. The results from this section are published in [13].

In Chapter 4 we present some applications of the theorems and methods from the previous chapters. These applications and theorems appear in our papers [10, 13, 14, 16]. In Section 4.1 we prove a classical conjecture of Terai regarding the solutions of the equation

$$(4t^2+1)^x + (5t^2-1)^y = (3t)^z,$$

where t is an arbitrary but fixed positive integer and x, y, z are unknown positive integers. In Section 4.2 we give all solutions of the equations

$$U_n = 2^x + 3^y \quad \text{and} \quad U_n = 2^x + 3^y + 5^z,$$

where U_n is the n-th term of one of the Fibonacci-, Lucas-, Pell- or associated Pell-sequence and x, y, z are unknown non-negative integers. In Section 4.3 we turn to a related problem, namely we solve the equation

$$B_u + B_v + B_w = b^z$$

in non-negative integers u, v, w, z where B_i is the i-th balancing number and $b \in \{2, 3, 5, 7\}$. Finally, in Section 4.4 we discuss applications regarding multi-base representations. Namely, let S_1 and S_2 be disjoint non-empty sets

with $S_1 \cup S_2 = \{2, 3, 5\}$ and let $w_S^+(n)$ be defined as before. In this section we give all solutions of the inequality

$$w_{S_1}^+(n) + w_{S_2}^+(n) \leq 4.$$