1949

Diophantine problems related to linear recurrence sequences

Egyetemi doktori (PhD) értekezés

Szerző: Sebestyén Péter
Témavezető: Dr. Hajdu Lajos

DEBRECENI EGYETEM
Természettudományi és Informatikai Doktori Tanács
Matematika- és Számítástudományok Doktori Iskola
Debrecen, 2024

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, 2024. március ....　　　　..........................

A jelölt aláírása

Tanúsítom, hogy Sebestyén Péter doktorjelölt 2019-2023 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, 2024. március ....　　　　..........................

A témavezető aláírása

Diophantine problems related to linear recurrence sequences

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

Írta: Sebestyén Péter okleveles matematikus

Készült a Debreceni Egyetem Matematika- és Számítástudományok doktori iskolája (Diofantikus és Konstruktív Számelmélet programja) keretében

Témavezető: Dr. Hajdu Lajos

Az értekezés bírálói:

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

A bírálóbizottság:

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

Az értekezés védésének várható időpontja: 2024. ....

Köszönetnyilvánítás

Szeretném megköszönni a témavezetőmnek az éveken át tartó munkáját, amiért az egyetemi tanulmányaim során segítségemre volt, egyengette az utam, támogatott kutatásaimban.

Köszönetet mondok a Matematikai Intézet dolgozóinak, akikhez szintén fordulhattam, ha szakmai kérdésekben fennakadásaim voltak.

Contents

1 Introduction

Linear recurrence sequences form a classical field (among others) in Diophantine number theory. Their first appearance is linked to the famous book of Fibonacci [25]. Since then they have been studied from many aspects, in several books and papers, by many authors. We only mention a few directions where intensive and deep research has been made.

Concerning various divisibility properties of linear recurrence sequences one may discuss the paper of Bézivin, Pethő and van der Poorten [5], where a full characterisation of divisibility sequences is given. A more recent result, equally of great interest and importance is due to Bilu, Hanrot and Voutier [6] concerning primitive prime divisors of Lucas-sequences. Another direction concerns the existence of perfect powers among the terms of linear recurrence sequences. Here we may mention classical papers of Pethő [39] and Shorey and Stewart [42], who independently proved that (under general assumptions) there are only finitely many powers in binary linear recurrence sequences. As a particular, but interesting and deep related recent result we mention that Bugeaud, Mignotte and Siksek [11] found all perfect powers in the Fibonacci sequence and among Lucas numbers. For related results and general finiteness theorems, see e.g. the book of Shorey and Tijdeman [43]. Another important direction of research concerns the zero-multiplicity, or more generally the a-multiplicity of linear recurrence sequences: that is, we are interested in the number of terms being equal to 0 or to a of a fixed linear recurrence sequence. Here one can mention classical results of Skolem, Mahler and Lech (see for example Chapter C of [43] for an account), or e.g. the papers of Beukers and Tijdeman [4], Schmidt [44] and Brindza, Pintér and Schmidt [10], and the references therein. Finally, we mention that certainly there are many more directions one could discuss. As a particular, but interesting problem one may e.g. discuss the paper of Fuchs, Luca and Szalay [27] related to variants of so-called Diophantine sets. However, instead of trying to survey the enormous literature, we only refer the reader to the books of Everest, van der Poorten, Shparlinski and Ward [20] for generalities on recurrence sequences, the books of Shorey and Tijdeman [43] and of Evertse and Győry [21] for many effective and ineffective results and many applications related to them.

In this dissertation we discuss problems and prove various new results related to linear recurrence sequences. At this point we only sketch our results and their background. A detailed description of the studied problems will be given in the corresponding chapters, together with a thorough survey of the related literature.

First we consider the following question. Given a generalized Pell equation of the shape

$$x^2 - dy^2 = t$$

with non-zero integers d, t where $d > 1$ is square-free, how many of its integral solutions x, y can be represented as an arbitrary, but fixed term sum of integers with prime factors coming from some given finite set of primes? As we shall see, this problem leads to the investigation of the question that how many terms of a binary linear recurrence sequence can be obtained as the sum of a fixed number of so-called integral S-units. We prove that under some conditions, this number is finite. It is important to note that our conditions will be necessary, so in the qualitative sense our results are best possible.

Then we investigate the number of terms of linear recurrence sequences of arbitrary degree in the solution sets of generalized Pell-equations. We shall prove that under certain assumptions, the number of such terms is finite, and give effective upper bounds for the number of exceptional terms. We shall be able to describe all the degenerate cases (that is, cases where there are infinitely many solutions) completely. Thus our results are qualitatively precise in this case, as well.

Finally, we extend our results to the case of terms of recurrence sequences in the solution sets of norm form equations, i.e. equations of the form

$$\mathcal{N}(x_1\gamma_1 + \ldots + x_m\gamma_m) = t, \tag{1.1}$$

where $\mathcal{N}$ is the norm from an algebraic number field K to $\mathbb{Q}$, $\gamma_1, \ldots, \gamma_m$ are linearly independent elements of K over $\mathbb{Q}$, and t is a non-zero integer. We shall be able to give finiteness results for the number of such terms in this case, as well. Further, the conditions we impose will be necessary here, too.

To prove our results, we shall combine various deep tools, such as the theory of norm form equations, S-unit equations and polynomial-exponential equations.

The structure of the dissertation is the following. In the second chapter we summarize the most important notions and tools used. Namely, we introduce some notation and recall some important theorems and assertions related to recurrence sequences, algebraic number fields, S-units and S-unit equations and polynomial-exponential equations. The next three chapters contain our results, following the order indicated above.

2 Some important notions and tools

In this section, we collect those notions and tools which will be necessary for our purposes. They are in the background of the problems we study, and play important roles in our arguments and they (typically) appear at several points.

2.1 Recurrence sequences

Let r be a positive integer, $a_1, \ldots, a_r \in \mathbb{Z}$ such that $a_r \neq 0$ and $U_0, \ldots, U_{r-1} \in \mathbb{Z}$ not all zero. If

$$U_n = a_1 U_{n-1} + \cdots + a_r U_{n-r} \quad (n \geq r) \tag{2.1}$$

and r is minimal such that (U_n) satisfies a relation above, then we say that $U = (U_n) = (U_n)_{n\geq 0}$ is a linear recurrence sequence (of integers) of order r. Throughout this thesis, we always assume that a recurrence sequence is given by its minimal length relation (2.1). Importantly, we can do this without loss of generality. Indeed, by the Berlekamp-Massey algorithm [45], one can determine the order r and the minimal recursion as well. We shall also use the notation

$$U = U(a_1, \ldots, a_r, U_0, \ldots, U_{r-1}).$$

The characteristic polynomial of (U_n) is defined by

$$f(x) := x^r - a_1 x^{r-1} - \cdots - a_r = \prod_{i=1}^{q} (x - \alpha_i)^{m_i} \tag{2.2}$$

where $\alpha_1, \ldots, \alpha_q$ are distinct algebraic numbers and $m_1, \ldots, m_q$ are positive integers. Note that as $a_r \neq 0$, we have $\alpha_i \neq 0 \quad (i = 1, \ldots, q)$.

The sequence (U_n) is called degenerate if there are integers i, j with $1 \leq i < j \leq q$ such that α_i/α_j is a root of unity; otherwise it is non-degenerate. Note that in the literature one can find many different definitions for the non-degeneracy of a recurrence sequence, for example in many cases it is also required that some of the coefficients $a_1, \ldots, a_r$ are non-zero. However, the property that α_i/α_j is not a root of unity is always assumed. Here we only require this commonly used assumption. The non-degeneracy of the recurrence sequences will play an important role in our results. Namely, Theorem 4.1 and Theorem 5.1 are not valid for degenerate sequences (see the corresponding remarks after them).

We shall also need the following assertion for the explicit representation of the terms of recurrence sequences. In fact, it is a slightly extended version of Theorem C1 a.) in part C of [43]. The original theorem only claims that the polynomials g_j appearing in the statement are of degrees at most $m_j - 1$, but we shall also need that they are not identically zero. In fact, this is apparent from the proof of the theorem in [43]. However, to keep the presentation as much self-contained as possible, we give a full proof of this statement. For this, we follow the proof of Theorem C1 in part C of [43], with small modifications.

Lemma 2.1. Let U be a recurrence sequence given by (2.1). Then we have

$$U_n = \sum_{j=1}^{q} g_j(n)\alpha_j^n \quad \text{for all } n \geq 0, \tag{2.3}$$

where $g_j(x)$ is a not identically zero polynomial of degree at most $m_j - 1$ $(j = 1, \ldots, q)$ with coefficients in the number field $\mathbb{Q}(\alpha_1, \ldots, \alpha_q)$.

Proof. Let

$$E(x) = \sum_{n=0}^{\infty} U_n x^n$$

be the generating function of the recurrence sequence U and set

$$F(x) := x^r f\left(\frac{1}{x}\right) = 1 - \sum_{i=1}^{r} a_i x^i = \prod_{j=1}^{q} (1-\alpha_j x)^{m_j}.$$

Thus, introducing the notation

$$\phi_i = \begin{cases} -a_i, & \text{if } 0 < i \le r, \\ 1, & \text{if } i = 0, \end{cases}$$

we have

$$F(x) = \sum_{i=0}^{r} \phi_i x^i.$$

Then by (2.1),

$$G(x) := E(x)F(x) = \sum_{n=0}^{r-1}\sum_{j=0}^{n} \phi_j U_{n-j} x^n + \sum_{n=r}^{\infty}\sum_{j=0}^{r} \phi_j U_{n-j} x^n =$$

$$= \sum_{n=0}^{r-1}\sum_{j=0}^{n} \phi_j U_{n-j} x^n + \sum_{n=r}^{\infty} \left(U_n - \sum_{j=1}^{r} a_n U_{n-j} \right) x^n$$

$$= \sum_{n=0}^{r-1} x^n \sum_{j=0}^{n-1} \phi_j U_{n-j}.$$

Introduce the following notation:

$$\mathcal{H}_n := \sum_{j=0}^{n} \phi_j U_{n-j} \quad (n = 0, 1, \ldots, r-1).$$

Thus in view of

$$m_1 + \ldots + m_q = r,$$

splitting $G(x)/F(x)$ into partial fractions, we obtain

$$E(x) = \frac{G(x)}{F(x)} = \frac{\sum\limits_{n=0}^{r-1} \mathcal{H}_n x^n}{\prod\limits_{j=1}^{q} (1-\alpha_j x)^{m_j}} = \sum_{j=1}^{q}\sum_{i=1}^{m_j} \frac{\rho_{ij}}{(1-\alpha_j x)^i} \tag{2.4}$$

for certain numbers $\rho_{ij} \in \mathbb{Q}(\alpha_1, \dots, \alpha_q)$, which are uniquely determined. Recall that $\alpha_i \neq 0 \quad (i = 1, \dots, q)$.

Importantly, observe here that it is not possible that $\rho_{1j}, \dots, \rho_{m_j j}$ are all zero for any $j \in \{1, 2, \dots, q\}$. Indeed, otherwise (2.4) would yield a contradiction, since $1/\alpha_j$ would be a pole of the left hand side, but it would not be a pole of the right hand side.

For any x with

$$|x| < \min_{1 \leq j \leq q} |\alpha_j|^{-1},$$

we have

$$E(x) = \sum_{j=1}^{q} \sum_{i=1}^{m_j} \rho_{ij} \sum_{n=0}^{\infty} \binom{-i}{n} (-\alpha_j x)^n =$$
$$= \sum_{n=0}^{\infty} \left(\sum_{j=1}^{q} \sum_{i=1}^{m_j} \rho_{ij} \binom{n+i-1}{n} \alpha_j^n \right) x^n.$$

Note that the Taylor coefficients are uniquely determined. On comparing coefficients we find (2.3) with g_j defined by

$$g_j(x) = \sum_{i=1}^{m_j} \rho_{ij} \frac{(x+i-1)(x+i-2)\dots(x+1)}{(i-1)!} \quad (j = 1, \dots, q).$$

As for every j with $1 \leq j \leq q$ we have $\rho_{ij} \neq 0$ for some i with $1 \leq i \leq m_j$, our claim follows. $\square$

2.2 Basics from algebraic number theory

Let K be an algebraic number field of degree m. Let $\mathcal{O}_K$ denote the ring of integers of K. Write

$$m = s + 2l,$$

where s and l are the numbers of real and complex pairs of embeddings of K into $\mathbb{C}$, respectively. The following statement is the so-called Dirichlet unit theorem.

Theorem 2.1. *There exist units $\varepsilon_1, \ldots, \varepsilon_r$ with $r = s + l - 1$ in $\mathcal{O}_K$, such that every unit $\varepsilon \in \mathcal{O}_K$ has a unique representation in the form*

$$\varepsilon = \vartheta \varepsilon_1^{q_1} \ldots \varepsilon_r^{q_r},$$

where $q_1, \ldots, q_r \in \mathbb{Z}$ and $\vartheta \in \mathcal{O}_K$ is a root of unity.

Proof. See e.g. Theorem 5 of [7] on p. 112. □

Theorem 2.2. *The roots of unity in $\mathcal{O}_K$ form a finite cyclic group.*

Proof. The statement a is a simple consequence of Theorem 2 of [7] on p. 105. □

Let $\mathcal{N}$ be the norm from K to $\mathbb{Q}$. Let $\gamma_1, \ldots, \gamma_m$ be linearly independent elements of K over $\mathbb{Q}$, and t be a non-zero integer. Then the equation

$$\mathcal{N}(x_1\gamma_1 + \ldots + x_m\gamma_m) = t \tag{2.5}$$

is called a norm form equation.

For a ring R, a non-trivial ideal $P \subset R$ is a *prime ideal*, if for any ideals A, B of R

$$P|AB \text{ implies that } P|A \text{ or } P|B.$$

The following theorem is well-known.

Theorem 2.3. *$\mathcal{O}_K$ is a Dedekind domain, an integral domain where every ideal $I \neq (0)$ can be factorized into a product of prime ideals in a unique way.*

For a non-zero integer z, let $\omega(z)$ denote the number of distinct prime divisors of $|z|$. As it is well-known, any number field contains only finitely many pairwise non-associate algebraic integers of a given norm. That is, up to associates, equation (2.5) has only finitely many solutions. We shall use the following quantitative version of this assertion, due to Győry [31].

Theorem 2.4. *The number of pairwise non-associate solutions of* (2.5) *is at most*

$$m^{\omega(t)} \cdot \tau_m(t^{m-1}),$$

where $\tau_m(\alpha)$ *is the number of factorizations of the principal ideal* (α) *into* m *integral ideals in* $\mathcal{O}_K$.

Proof. The statement is a simple consequence of Lemma 5 of [31]. □

By the (naive) height $h(\gamma)$ of an element $\gamma \in K$ we mean the maximum of the absolute values of the coefficients of the defining primitive polynomial of γ in $\mathbb{Z}[x]$. Note that for $\gamma \in \mathbb{Q}$, $h(\gamma)$ is just the maximum of the absolute values of the numerator and the denominator of γ.

2.3 Pell equations

The equation

$$x^2 - dy^2 = t \tag{2.6}$$

is called a generalized Pell equation, where $d, t \in \mathbb{Z}$, $d > 1$ is square-free, and t is a non-zero integer. (Note that the name Pell equation usually refers to the cases $t = \pm 1, \pm 4$.) Observe that (2.6) is a norm form equation in $\mathbb{Q}(\sqrt{d})$. Indeed, in this case

$$m = 2,\ \gamma_1 = 1,\ \gamma_2 = \sqrt{d}.$$

If $t \in \{1, 4\}$, we call

$$x = \pm 1 \text{ or } \pm 2, y = 0$$

(respectively) the trivial solutions, the others (where $y \neq 0$) are the non-trivial solutions. It is well-known that if (2.6) has a solution, it has infinitely many solutions, and a Pell equation with $t = 1, 4$ always has infinitely many solutions. The following lemma tells us about the structure of solutions for $t = 1$.

Lemma 2.2. Let u_0 and v_0 be the smallest positive solutions (in x and y, respectively) of the equation

$$x^2 - dy^2 = 1. \tag{2.7}$$

Then all positive integer solutions u, v of (2.7) are given by

$$u + \sqrt{d}v = \left(u_0 + \sqrt{d}v_0\right)^m \quad (m \geq 1).$$

Proof. The statement is Theorem 7.26 of [38] on p. 354. □

Remark 2.1. The unit

$$\xi_0 := u_0 + \sqrt{d}v_0$$

is a fundamental unit with $\mathcal{N}(\xi_0) = 1$ in $\mathbb{Q}(\sqrt{d})$, in the sense that every unit ξ with $\mathcal{N}(\xi) = 1$ in $\mathbb{Q}(\sqrt{d})$ can be obtained as

$$\xi = \pm\xi_0^a \quad (a \in \mathbb{Z}).$$

2.4 S-units and S-unit equations

Let $p_1, \ldots, p_\ell$ be distinct primes and put

$$S = \{p_1, \ldots, p_\ell\}.$$

Then a rational number z is an S-unit, if z can be written as

$$z = \pm p_1^{b_1} \ldots p_\ell^{b_\ell}$$

with some $b_1, \ldots, b_\ell \in \mathbb{Z}$. Write U_S for the set of S-units.

We shall need a similiar concept in algebraic number fields as well.

Let

$$\mathcal{S} = \{P_1, \dots, P_\ell\}$$

be a finite set of prime ideals of K. Write $U_{\mathcal{S}}$ for the set of $\mathcal{S}$-units in K, that is, for the set of those $\chi \in K \neq 0$ for which the principal fractional ideal (χ) can be represented as

$$(\chi) = P_1^{b_1} \dots P_\ell^{b_\ell} \quad (b_1, \dots, b_\ell \in \mathbb{Z}).$$

Let K be an algebraic number field, and $e_1, \dots, e_k$ be non-zero elements of K. Then

$$e_1 x_1 + \ldots + e_k x_k = 1 \tag{2.8}$$

in unknown S-units $x_1, \dots, x_k$, is called an S-unit equation, given in inhomogeneous form. Note that by changing the notation, for example writing

$$e_{k+1} = -1, \ x_i = \frac{y_i}{y_{k+1}} \quad (i = 1, \dots, k)$$

where $y_i \in U_S$ $(i = 1, \dots, k+1)$, we can give (2.8) in homogeneous form, that is as

$$e_1 y_1 + \ldots + e_k y_k + e_{k+1} y_{k+1} = 0.$$

S-unit equations have a long history, a vast literature, and also many and many types of applications (see for example the book of Evertse and Győry [21]). We shall need results guaranteeing the finiteness of the number of solutions of S-unit equations. For this, we need to introduce the following notion.

If for a solution $x_1, \dots, x_k$ of (2.8) we have

$$e_{i_1} x_{i_1} + \cdots + e_{i_j} x_{i_j} = 0$$

for some $0 < j \leq k$ and $1 \leq i_1 < \cdots < i_j \leq k$, we say the solution has a vanishing subsum.

For example, let $S = \{2, 5\}$. Then for

$$x_1 + x_2 + x_3 + x_4 = 1$$

we can get an infinite number of solutions by the identity

$$2^a \cdot 5 - 2^{a+2} - 2^a + 1 = 1.$$

Observe that here we have

$$2^a(5 - 4 - 1) + 1 = 1,$$

where $5 - 4 - 1 = 0$ gives a vanishing subsum.

Lemma 2.3. Use the above notation, and let $e_1, \ldots, e_k$ be non-zero elements of K. Then the equation

$$e_1 x_1 + \ldots + e_k x_k = 1 \tag{2.9}$$

has at most c_0 solutions

$$(x_1, \ldots, x_k) \in U_{\mathcal{S}}^k$$

for which the left hand side of (2.9) has no vanishing subsums. Here c_0 is an effectively computable constant depending only on k, ℓ and $\deg K$.

Further, if $k = 2$ then we also have

$$\max(h(x_1), h(x_2)) < c_8,$$

where c_8 is an effectively computable constant depending only on the coefficients e_1, e_2 in (2.9), and on K and $\mathcal{S}$.

Proof. This statement follows from Theorem 6.1.3 on p. 132 and Corollary 4.1.5 on p. 65 of [21]. $\square$

2.5 Polynomial-exponential equations

Consider the equation

$$\sum_{\tau=1}^{k} P_\tau(\mathbf{x})\boldsymbol{\kappa}_\tau^{\mathbf{x}} = 0 \tag{2.10}$$

in variables

$$\mathbf{x} = (x_1, \ldots, x_s) \in \mathbb{Z}^s,$$

where the P_τ are polynomials with coefficients in an algebraic number field K, and

$$\boldsymbol{\kappa}_\tau^{\mathbf{x}} = \kappa_{\tau_1}^{x_1} \cdots \kappa_{\tau_s}^{x_s} \tag{2.11}$$

with given non-zero

$$\kappa_{\tau_1}, \ldots, \kappa_{\tau_s} \in K \quad (\tau = 1, \ldots, k).$$

Let $\mathcal{P}$ be a partition of the set

$$\Lambda = \{1, \ldots, k\}.$$

Then the system of equations

$$\sum_{\tau\in\lambda} P_\tau(\mathbf{x})\boldsymbol{\kappa}_\tau^{\mathbf{x}} = 0 \quad (\lambda \in \mathcal{P}) \tag{2.12}$$

yields a refinement of (2.10). Let $\mathcal{S}(\mathcal{P})$ be the set of solutions of (2.12) which are not solutions of

$$\sum_{\tau\in\lambda} P_\tau(\mathbf{x})\boldsymbol{\kappa}_\tau^{\mathbf{x}} = 0 \quad (\lambda \in \mathcal{Q})$$

with any proper refinement $\mathcal{Q}$ of $\mathcal{P}$. For two indices $\tau_1, \tau_2 \in \Lambda$, introduce the notation

$$\tau_1 \overset{\mathcal{P}}{\sim} \tau_2$$

if τ_1 and τ_2 lie in the same subset λ of $\mathcal{P}$. Let $G(\mathcal{P})$ be the subgroup of $\mathbb{Z}^s$ consisting of $\mathbf{z}$ with

$$\boldsymbol{\kappa}_{\tau_1}^{\mathbf{z}} = \boldsymbol{\kappa}_{\tau_2}^{\mathbf{z}} \quad \text{for any } \tau_1, \tau_2 \text{ with } \tau_1 \overset{\mathcal{P}}{\sim} \tau_2.$$

Now we can give a deep theorem of Schlickewei and Schmidt [41], yielding a strong finiteness result for such polynomial-exponential equations.

Lemma 2.4. Using the above notation, suppose that $G(\mathcal{P}) = \{\mathbf{0}\}$. Then we have

$$|\mathcal{S}(\mathcal{P})| < 2^{35A^3} D^{6A^2}$$

with $D = \deg(K)$ and

$$A = \max\left(s, \sum_{\tau\in\Lambda} \binom{s+\deg(\tau)}{s}\right),$$

where $\deg(\tau)$ is the total degree of the polynomial P_τ.

Proof. The statement is Theorem 1 in [41]. □

3 Sums of S-units in the solution sets of generalized Pell equations

3.1 Introduction

There are many papers about equations of the form

$$U_n = z_1 + \cdots + z_k, \tag{3.1}$$

where $(U_n)_{n=0}^{\infty}$ is a linear recurrence sequence, and $z_1, \ldots, z_k$ are integers with prime factors coming from a fixed finite set of primes. Here we only refer to the papers Guzman-Sanchez and Luca [30], Bertók, Hajdu, Pink and Rábai [2], Bérczes, Hajdu, Pink and Rout [3] and the (many) references there, where several and various related finiteness results have been proved. We mention that there are also many results in the literature where other similiar questions are discussed. For example, Bravo, Faye and Luca [9] considered a problem connected to sums of terms of a recurrence sequence yielding perfect powers (also see the references there).

In this section, we consider the problem of representability of solutions of generalized Pell equations as a fixed term sum of integers with prime factors coming from some finite set of primes. As we shall see, this problem is closely related to equation (3.1). In fact, the problem is more general: it turns out that we need to find sums of the form

$$z_1 + \cdots + z_k$$

in unions of recurrence sequences, rather than in only one fixed sequence. We note that there are some closely related results in the literature. We mention only two recent papers Luca and Togbé [37] and Ddamulira and Luca [14] about the x-coordinates of certain Pell-equations which are (generalized) Fibonacci numbers, and the references therein, and one by Erazo, Gómez and Luca [19] on linear combinations of prime powers in the x-coordinates of solutions of Pell equations.

3.2 New results

We recall from Section 2.3 of Chapter 2 that a generalized Pell equation is an equation of the shape

$$x^2 - dy^2 = t, \tag{3.2}$$

where $d, t \in \mathbb{Z}$, $d > 1$ is square-free, $t \neq 0$. We mention that in fact, such an equation can be considered to be a norm-form equation over a quadratic number field.

Let X and Y be the sets of solutions of equation (3.2) in $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$, respectively.

Now we can give our results about sums of S-units in the solution sets of generalized Pell equations. In the particular case of 'one-term' sums, our theorem is effective, that is, we are able to bound all the parameters involved. In the general case we can bound only the number of solutions.

Theorem 3.1 (Hajdu and Sebestyén [32]). *Use the above notation, and let $k \geq 1$. Then there are at most c_1 tuples*

$$(z_1, \ldots, z_k) \in U_S^k$$

such that

$$z_{i_1} + \cdots + z_{i_j} \neq 0 \tag{3.3}$$

for any $0 < j \leq k$ and $1 \leq i_1 < \cdots < i_j \leq k$, and

$$z_1 + \cdots + z_k \in X \cup Y, \tag{3.4}$$

where c_1 is an effectively computable constant depending only on $\omega(t)$, k and ℓ. Further, if $k = 1$ then we also have

$$h(z_1) < c_2,$$

where c_2 is an effectively computable constant depending only on d, t and S.

Remark. Schinzel [40] proved that the greatest prime divisor of $f(x)$ where f is a quadratic polynomial with integer coefficients having distinct roots effectively tends to infinity as $|x|$ tends to infinity. From this one can easily deduce the case $k = 1$ of the above theorem. However, as we would like to keep the presentation coherent, we shall give a general proof to Theorem 3.1, ultimately based upon the theory of S-unit equations.

We also note that the condition (3.3) related to vanishing subsums is not only natural, but it is necessary, as well. Indeed, if for some

$$z_1, \dots, z_k \in U_S$$

we have inclusion (3.4), but (3.3) does not hold for some indices with $0 < j \leq k$ and $1 \leq i_1 < \dots < i_j \leq k$, then the following sums

$$z_1 + \dots + z_k + (z_0 - 1)(z_{i_1} + \dots + z_{i_j}) \quad (z_0 \in U_S)$$

would yield infinitely many solutions for the inclusion (3.4).

3.3 The proof of Theorem 3.1

Before formulating our further lemmas, we need to introduce some notation concerning recurrence sequences. Let A, B be integers with $B \neq 0$, and let U_0, U_1 be integers such that at least one of them is non-zero. Then the sequence $U = (U_n)_{n\geq 0}$ satisfying a relation of the form

$$U_n = AU_{n-1} + BU_{n-2} \quad (n \geq 2) \tag{3.5}$$

is the special case $r = 2$ of (2.1), a binary linear recurrence sequence. We shall also use the notation

$$U = U(A, B, U_0, U_1)$$

for the sequence. Then by using (2.2), the characteristic polynomial of U is

$$f(x) := x^2 - Ax - B.$$

Write α and β for the roots of $f(x)$. It is known from (2.3) that if U is non-degenerate then we have

$$U_n = \frac{(U_1 - U_0\beta)\alpha^n - (U_1 - U_0\alpha)\beta^n}{\alpha - \beta} \quad (n \geq 0). \tag{3.6}$$

The following lemma shows that the sets of the coordinates of the solutions of equation (3.2) are unions of finitely many non-degenerate binary linear recurrence sequences. We note that this assertion is long and well-known qualitatively. However, we do not know any source where this statement is explicitly formulated (let alone the paper of Liptai [36] which is in Hungarian and which does not provide an upper bound for the number of the recurrence sequences involved). In fact, we shall need only the case concerning solutions with $\gcd(x, y) = 1$. However, we find the general case of possible independent interest. For a non-negative integer m, write $\tau(m)$ for the number of divisors of $|m|$.

Lemma 3.1. Let u_0 be as in Lemma 2.2. If equation (3.2) has a solution, then all its solutions are given by

$$(x, y) = \left(G_n^{(i)}, H_n^{(i)}\right) \quad (i = 1, \ldots, I)$$

with some binary recurrence sequences

$$G^{(i)} = G^{(i)}(2u_0, -1, G_0^{(i)}, G_1^{(i)}), \;\; H^{(i)} = H^{(i)}(2u_0, -1, H_0^{(i)}, H_1^{(i)}).$$

Here I and

$$G_0^{(i)}, G_1^{(i)}, H_0^{(i)}, H_1^{(i)} \quad (i = 1, \ldots, I)$$

are some positive integers with

$$I < c_3$$

and

$$|G_j^{(i)}|, |H_j^{(i)}| < c_4 \ (0 \leq j \leq 1, \ 1 \leq i \leq I), \tag{3.7}$$

where c_3 is an effectively computable constant depending only on $\tau(t)$, while c_4 is an effectively computable constant depending only on d and t. Further, for the solutions (x, y) of (3.2) with $\gcd(x, y) = 1$ the same conclusion holds, with

$$I < c_5$$

and (3.7), where c_5 is an effectively computable constant depending only on $\omega(t)$.

Proof. Obviously, we may restrict to positive integer solutions of (3.2). So let (ϵ, δ) be a positive solution of (3.2). Then the norm $\mathcal{N}(\epsilon + \sqrt{d}\delta)$ of the algebraic integer $\epsilon + \sqrt{d}\delta$ is t in the field $\mathbb{Q}(\sqrt{d})$. By Theorem 2.4 we know that there are only finitely many pairwise non-associate algebraic integers $U + \sqrt{d}V$ in $\mathbb{Q}(\sqrt{d})$ of norm t, and their number I can be bounded in terms of $\tau(t)$; further, under the assumption $\gcd(\epsilon, \delta) = 1$, even in terms of $\omega(t)$. It is well-known (see e.g. Chapter A of [43]) that we may assume here that

$$\max(|U|, |V|) < c_6,$$

where c_6 is an effectively computable constant depending only on d, t. Thus there exist algebraic integers $U_i + \sqrt{d}V_i$ with

$$N(U_i + \sqrt{d}V_i) = t$$

and

$$\max(|U_i|, |V_i|) < c_6 \quad (i = 1, \ldots, I)$$

such that

$$\epsilon + \sqrt{d}\delta = \nu(U_i + \sqrt{d}V_i)$$

for some $1 \le i \le I$, where ν is a unit in $\mathbb{Q}(\sqrt{d})$. We immediately get that $\mathcal{N}(\nu) = 1$. Thus Lemma 2.2 yields that

$$\nu = \pm(u_0 + \sqrt{d}v_0)^z \ \ (z \in \mathbb{Z}).$$

For simplicity, we assume that

$$\nu = (u_0 + \sqrt{d}v_0)^m$$

with some $m \ge 0$, since all the other cases are similar (or can be excluded by our assumption that ϵ and δ are positive). Then we have

$$\epsilon + \sqrt{d}\delta = (U_i + \sqrt{d}V_i)(u_0 + \sqrt{d}v_0)^m,$$

whence also

$$\epsilon - \sqrt{d}\delta = (U_i - \sqrt{d}V_i)(u_0 - \sqrt{d}v_0)^m.$$

Putting

$$\alpha := u_0 + \sqrt{d}v_0, \quad \beta := u_0 - \sqrt{d}v_0$$

from these assertions we obtain

$$\epsilon = \frac{U_i + \sqrt{d}V_i}{2}\alpha^m + \frac{U_i - \sqrt{d}V_i}{2}\beta^m$$

and

$$\delta = \frac{U_i + \sqrt{d}V_i}{2\sqrt{d}}\alpha^m - \frac{U_i - \sqrt{d}V_i}{2\sqrt{d}}\beta^m.$$

Hence as α, β are roots of the polynomial

$$x^2 - 2u_0x + 1$$

(also in view of (3.6)), we get that ϵ and δ are elements of the recurrence sequences

$$G = G(A, B, G_0^{(i)}, G_1^{(i)}) \quad \text{and} \quad H = H(A, B, H_0^{(i)}, H_1^{(i)}),$$

respectively, with

$$A = 2u_0, \quad B = -1$$

and

$$(G_0^{(i)}, G_1^{(i)}) = (U_i, u_0 U_i + d v_0 V_i), \quad (H_0^{(i)}, H_1^{(i)}) = (V_i, v_0 U_i + 2u_0 V_i).$$

Finally, note that it is obvious that the terms of these recurrence sequences are solutions of (3.2). Hence our claim follows. $\square$

We shall also need the following finiteness result of Bérczes, Hajdu, Pink and Rout [3] concerning the number of terms of recurrence sequences representable as k-term sums of S-units.

Lemma 3.2. Let U_n be a non-degenerate binary linear recurrence sequence as in (3.5), and suppose that the characteristic polynomial of U_n has non-rational roots. Then for any fixed $k \geq 1$, equation (3.1) is solvable in

$$z_1, \ldots, z_k \in U_S$$

at most for finitely many n. Further, the number of indices n for which (3.1) is solvable for this fixed k, can be bounded by an effectively computable constant depending only on ℓ and k.

Proof. The statement is a simple consequence of Theorem 1 of [3] and its proof. Note that the statement in [3] concerns only the case where

$$z_1, \ldots, z_k \in U_S \cap \mathbb{Z},$$

however, from the proof it is clear that this more general formulation is also valid. $\square$

Now we are ready to give the proof of Theorem 3.1.

Proof of Theorem 3.1. Let $z_1, \ldots, z_k \in U_S$ satisfying (3.4) and (3.3). Assume first that

$$z_1 + \cdots + z_k \in X.$$

Let (ϵ, δ) be a solution of (3.2) such that

$$z_1 + \cdots + z_k = \epsilon,$$

and write

$$z = \gcd(\epsilon, \delta).$$

Observe that

$$z \mid t.$$

By Lemma 3.1 we have that

$$z_1 + \cdots + z_k = zG_n^{(i)} \tag{3.8}$$

with some $i \in \{1, \ldots, I\}$ and $n \geq 0$, where I is bounded in terms of $\omega(t)$ and $G_n^{(i)}$ is a term of a non-degenerate binary recurrence sequence

$$G^{(i)} = G^{(i)}(2u_0, -1, G_0^{(i)}, G_1^{(i)}).$$

Note that as $v_0 > 0$ in Lemma 2.2, we have $u_0 > 1$. Thus the roots α and β of the characteristic polynomial

$$f(x) = x^2 - 2u_0 + 1$$

are (real) irrational numbers. (Observe that here $f(x)$, hence α and β are independent of i.) We can rewrite (3.8) as

$$z^{-1}z_1 + \cdots + z^{-1}z_k = G_n^{(i)},$$

and observe that here

$$w_j := z^{-1}z_j \quad (j = 1, \ldots, k)$$

are S^*-units, where

$$S^* = S \cup \{p \text{ prime} : p \mid t\}.$$

Thus by Lemma 3.2 we see that the number of possible indices n in (3.8) is bounded by a constant c_9 depending only on ℓ, $\omega(t)$ and k. Further, by (3.3),

$$G_n^{(i)} \neq 0$$

in (3.8). Thus setting

$$e_j = \frac{1}{G_n^{(i)}} \quad (j = 1, \dots, k),$$

equation (3.8) can be rewritten as

$$e_1 w_1 + \cdots + e_k w_k = 1.$$

Hence in view of (3.3), and as the number of the above type equations appearing is at most c_9, our statement concerning the number of solutions to (3.4) follows by Lemma 2.3. Further, in the particular case $k = 1$, equation (3.8) reduces to

$$w_1 = G_n^{(i)}, \tag{3.9}$$

which in view of Lemma 3.1 and (3.6) can be rewritten as

$$a_i \frac{\alpha^n}{w_1} + b_i \frac{\beta^n}{w_1} = 1$$

with some a_i, b_i depending only on d, t, where

$$\alpha = u_0 + \sqrt{d} v_0, \quad \beta = u_0 - \sqrt{d} v_0.$$

Let

$$\mathcal{S} = \bigcup_{p \in S^*} \{P : P \text{ is a prime ideal in } \mathbb{Q}(\sqrt{d}),\ P|(p)\}.$$

As α and β are roots of the polynomial

$$x^2 - 2u_0 x + 1,$$

they are units in $\mathbb{Q}(\sqrt{d})$, so

$$\alpha, \beta \in U_{\mathcal{S}}.$$

Thus by Lemma 2.3 we obtain that for some

$$(\gamma_1, \gamma_2) \in U_{\mathcal{S}} \times U_{\mathcal{S}}$$

with

$$\max(h(\gamma_1), h(\gamma_2)) < c_{10},$$

where c_{10} is a constant depending only on d, t and S, we have

$$\frac{\alpha^n}{w_1} = \gamma_1, \quad \frac{\beta^n}{w_1} = \gamma_2.$$

By multiplying these expressions, in view of

$$\alpha\beta = 1$$

we obtain

$$w_1^2 = \frac{1}{\gamma_1\gamma_2},$$

whence we can bound $h(z_1)$ in terms of d, t and S. Hence in this case our claim follows also for $k = 1$.

Let now

$$z_1 + \cdots + z_k \in Y.$$

In this case a similar argument applies, using the sequences $H^{(i)}$ in place of the sequences $G^{(i)}$. We can apply the same calculations once again, and the proof of the theorem is complete. $\square$

Remark. In case of

$$t \in \{\pm 1, \pm 4\},$$

one can easily check that the sequences

$$G^{(i)} \text{ and } H^{(i)} \quad (i = 1, \ldots, I)$$

are Lucas-sequences of the first and second kind, respectively. Hence, in this case for $k = 1$, in (3.9) (or in the equation

$$w_1 = H_n^{(i)}$$

when $z_1 \in Y$) one can get a very good bound for n, using the famous result of Bilu, Hanrot and Voutier [6] concerning the existence of primitive prime divisors of the terms of such sequences.

4 Terms of recurrence sequences in the solution sets of generalized Pell equations

4.1 Introduction

There are several papers in the literature concerning recurrence sequences with terms occurring in the solution sets of (generalized) Pell equations. We mention a few such recent results; the interested reader may consult their references. In the papers [8, 12, 13, 16, 14, 15, 18, 22, 28, 29, 35] the authors provide various finiteness results concerning the values (or sums or products of values) of certain concrete recurrence sequences (such as Fibonacci, Tribonacci, generalized Fibonacci, Lucas, Padovan, Pell, repdigits) in the x coordinate of equation (2.6), for the cases $t = \pm 1, \pm 4$. Concerning the y-coordinate, we are aware only of two related results. Faye and Luca [23] proved that for $t = 1$ and $d > d_0$ with some d_0, any fixed binary recurrence sequence has at most two terms among the y-coordinates of the solutions of (2.6), and the same authors [24] showed that again with $t = 1$, there are at most two solutions of (2.6) with y-coordinates of the form $2^n - 1$. For related results, for example concerning sums or linear combinations of integers with fixed prime factors in the solution sets of Pell equations, see e.g. the papers [17, 19, 32] and the references there.

In view of the above results, it seems to be interesting to consider the question under more general circumstances. In this section, we completely describe those recurrence sequences which have infinitely many terms in either of the x, y coordinates of the solution sets of generalized Pell equations, i.e. of (2.6) with arbitrary t. Furthermore, we establish an upper bound for the number of solutions in the case where there are only finitely many solutions. We note that equation (2.6) can be considered as a norm form equation of degree two. Recently, Fuchs and Heintze [26] obtained similar results concerning values of recurrence sequences in the coordinates of solutions of general norm form equations. However, their results concern only non-degenerate recurrences. Thus our results can also be considered as an extension of those in [26] in the case of norm form equations of degree two.

4.2 New results

In this section, we still examine the generalized Pell equation and its various properties. We recall that

$$x^2 - dy^2 = t$$

is a generalized Pell equation where $d, t \in \mathbb{Z}$, $d > 1$, square-free, $t \neq 0$. Let X and Y be sets of solutions in the first and second coordinates respectively.

Now we can give our main result about terms of recurrence sequences in the solution sets of generalized Pell equations.

Theorem 4.1 (Hajdu and Sebestyén [33]). *Let (U_n) be a non-degenerate linear recurrence sequence of integers of order $r \geq 2$, such that its characteristic polynomial is not of the form $x^2 + ax \pm 1$ with $(a^2 \mp 4)/d$ being a square in $\mathbb{Q}$. Then the inclusion*

$$U_n \in X \cup Y \tag{4.1}$$

holds only for finitely many indices n. Further, the number of such values n is bounded by $c_{10} = c_{10}(r, d, t)$, where c_{10} is an effectively computable constant depending only on r, d, t.

Remark. We note that the assumption that (U_n) is non-degenerate is necessary. Indeed, consider the sequence defined by $U_0 = 0$, $U_1 = 1$ and $U_{n+2} = U_{n+1} - U_n$ $(n \geq 0)$. Then the elements of the sequence

(U_n) are the following: $0, 1, 1, 0, -1, -1, 0, 1, \ldots$. Then taking $d = 7$ and $t = 1$ we have the equation

$$x^2 - 7y^2 = 1.$$

It is easy to see that $(x, y) = (\pm 1, 0)$ is a solution, so $U_n \in X \cup Y$ for infinitely many indices n. Here the characteristic polynomial of (U_n) is $f(x) = x^2 - x + 1$, so (U_n) is degenerate. Further, the exclusion of the specific binary recurrence sequences from Theorem 4.1 is also necessary. This is demonstrated by the following example. Take $d = 2$ and $t = 1$, that is consider the classical Pell equation

$$x^2 - 2y^2 = 1.$$

As it is well-known, its positive solutions are given by

$$x + \sqrt{2}y = (3 + 2\sqrt{2})^m \quad (m \geq 0). \tag{4.2}$$

Let $U_0 = 1$, $U_1 = 3$ and

$$U_{n+2} = 6U_{n+1} - U_n \quad (n \geq 0).$$

One can easily check that (U_n) is contained in X - this sequence comes from the formula (4.2). On the other hand, here $a = 6$, and $(a^2 - 4)/2 = 16$ is a full square, yielding that the roots of the characteristic polynomials $x^2 - 6x + 1$ are units of the ring of integers of $\mathbb{Q}(\sqrt{2})$.

4.3 The proof of Theorem 4.1

Proof of Theorem 4.1. Let (U_n) be a linear recurrence sequence of order r, satisfying the assumptions of the statement. In view of Lemma 3.1, $X \cup Y$ is the union of at most $2c_{11}$ binary recurrence sequences (V_m) satisfying

$$V_{m+2} = 2u_0 V_{m+1} - V_m \quad (m \geq 0)$$

with some V_0, V_1 obeying

$$|V_0|, |V_1| \leq c_{12}.$$

Here c_{11} and c_{12} are the constants c_3 and c_4 appearing in Lemma 3.1. Since $u_0 > 1$, by (2.3) we get that

$$V_m = Lv^m + M\omega^m \quad (m \geq 0),$$

where v, ω are the (real) roots of the polynomial

$$x^2 - 2u_0 x + 1$$

and L, M are non-zero conjugated elements of $\mathbb{Q}(\sqrt{d})$. In particular, v, ω are units and conjugates in $\mathbb{Q}(\sqrt{d})$.

Thus, writing U_n in the form (2.3), the inclusion $U_n \in X \cup Y$ is equivalent with

$$Lv^m + M\omega^m = \sum_{i=1}^{q} g_i(n)\alpha_i^n \tag{4.3}$$

for some $m \geq 0$. Note that by our convention on the minimality on r in (2.1), here none of g_i and α_i is zero; further, the degrees of the g_i are bounded by r. We shall show that (4.3) has only finitely many solutions in (n, m), whose number is effectively bounded in terms of r, d, t. This, in view of that L, M, v, ω are coming from a finite set of at most $2c_{11}$ elements, implies our theorem. Observe that as $\deg(g_i) \leq r$, the number of those values of n which are roots of one of these polynomials, is bounded by r^2. So in what follows we shall assume that n is not a root of g_i $(1 \leq i \leq q)$.

We shall handle equation (4.3) by Lemma 2.4. For this, introduce the following notation. Suppose that the positive integers n, m are solutions of (4.3). Write $\mathbf{N} = (n, m)$,

$$h_i(\mathbf{N}) = \begin{cases} g_i(n), & \text{if } i = 1, \dots, q, \\ -L, & \text{if } i = q+1, \\ -M, & \text{if } i = q+2, \end{cases}$$

and

$$\boldsymbol{\delta}_i = \begin{cases} (\alpha_i, 1), & \text{if } i = 1, \dots, q, \\ (1, \upsilon), & \text{if } i = q+1, \\ (1, \omega), & \text{if } i = q+2. \end{cases}$$

Let $\mathcal{P}$ be a partition of the set

$$\{1, \dots, q, q+1, q+2\}$$

such that we have

$$\sum_{i \in \lambda} h_i(\mathbf{N}) \boldsymbol{\delta}_i^{\mathbf{N}} = 0 \quad (\lambda \in \mathcal{P}), \tag{4.4}$$

but (4.4) does not hold for any proper refinement of $\mathcal{P}$. Observe that all solutions (n, m) of (4.3) are solutions of (4.4) with some $\mathcal{P}$. Now we distinguish subcases according to the structure of $\mathcal{P}$.

Assume first that there is a subset λ of $\mathcal{P}$ such that

$$\lambda \subseteq \{1, \dots, q\}.$$

Here $|\lambda| = 1$, as $\alpha_i \neq 0$ $(1 \leq i \leq q)$, is not possible. Thus $|\lambda| \geq 2$. We shall use Lemma 2.4 to prove our claim. For this, observe that by the non-degeneracy of (U_n) we have $G(\mathcal{P}) = \{(0,0)\}$. Hence by Lemma 2.4 we get an upper bound for the number of these values of n in terms of r.

Suppose next that there is a subset λ of $\mathcal{P}$ such that

$$q+1, q+2 \in \lambda.$$

Since υ/ω is not a root of unity, we see that $G(\mathcal{P}) = \{(0,0)\}$ again. So Lemma 2.4 yields an upper bound for the number of such values of n in terms of r also in this case.

Thus we are left with the case where $\mathcal{P}$ consists of precisely two sets, say λ_1 and λ_2 with

$$q+1 \in \lambda_1, \quad q+2 \in \lambda_2.$$

Obviously,

$$|\lambda_1|, |\lambda_2| \geq 2.$$

Assume that one of these sets, say λ_1, has more than two elements. Then there exist i, j with $1 \leq i < j \leq q$ with $i, j \in \lambda_1$. Since α_i/α_j is not a root of unity, we get that $G(\mathcal{P}) = \{(0,0)\}$. Thus Lemma 2.4 provides an upper bound in terms of r for the number of these values of n once again. That is, we may assume that

$$|\lambda_1| = |\lambda_2| = 2$$

and that (4.4) (switching back to the notation used in (4.3)) reads as

$$\begin{cases} L\upsilon^m = g_1(n)\alpha_1^n, \\ M\omega^m = g_2(n)\alpha_2^n. \end{cases} \tag{4.5}$$

Importantly, we also see that the characteristic polynomial of (V_n) has precisely two distinct roots. In particular, α_1, α_2 are either rational, or conjugated quadratic algebraic numbers. If in (4.5) we have $G(\mathcal{P}) = \{(0,0)\}$, then we can bound the number of solutions in the usual way. So we may assume that $G(\mathcal{P}) \neq \{(0,0)\}$. Thus there exist $t_1, t_2 \in \mathbb{Z}$ for which

$$\upsilon^{t_1} = \alpha_1^{t_2}, \quad \omega^{t_1} = \alpha_2^{t_2}.$$

If $\alpha_1, \alpha_2 \in \mathbb{Q}$, then taking conjugates in

$$K := \mathbb{Q}(\upsilon) = \mathbb{Q}(\omega),$$

we get that $\alpha_1 = \alpha_2$, a contradiction. So α_1, α_2 are conjugated quadratic integers. This easily implies that $\alpha_1, \alpha_2 \in K$, since υ and ω are units in $\mathbb{Z}[\sqrt{d}]$, α_1, α_2 are units in $\mathcal{O}_K$. Multiplying the left and right hand sides of (4.5), using that $\upsilon\omega = 1$ and that α_1, α_2 are conjugated units of $\mathcal{O}_K$, we obtain

$$LM = (\pm 1)^n g_1(n) g_2(n).$$

Hence, if any of g_1, g_2 is not a constant polynomial, we get at most $2r^2$ solutions for n in this case. Thus we may assume that g_1 and g_2 are constant, that is, the characteristic polynomial of (V_n) is

$$T(x) := (x - \alpha_1)(x - \alpha_2) \in \mathbb{Z}[x].$$

However, as the roots of $T(x)$ are units of $\mathcal{O}_K$, its constant term is ± 1 and the square-free part of its discriminant equals d. So we are just in the exceptional case excluded from the theorem, and the statement follows.

$\square$

5 Terms of recurrences in solutions of norm form equations

5.1 Introduction

Arithmetic properties of solutions of norm form equations have a considerable literature. Here we mention only one result (which is the most important from our viewpoint), and for generalities on norm form equations or other related result we refer the interested reader to the papers [1] or [26]. Fuchs and Heintze considered terms of so-called multi-recurrences (being natural generalizations of linear recurrence sequences) among the coordinates of solutions of norm form equations. They set the problem in the general case, however, their results concern the case of multi-recurrences which are simple. Simplifying their result to the case of linear recurrence sequences, this means that the characteristic polynomials of these sequences have simple zeroes. They could prove that a simple multi-recurrence, under certain necessary assumptions, can have only finitely many terms among the coordinates of solutions of a norm form equation.

In the special situation when the underlying field is quadratic, we in fact investigate terms of recurrence sequences among the solutions of generalized Pell equations. For an account on these results see the previous section (which is based on [32]). In particular, Theorem 4.1 states that under certain assumptions, a recurrence sequence has only finitely many terms among the coordinates of solutions of generalized Pell equations.

In this section, we provide a common extension of the main results of [26] (more precisely, its corollary to the case of linear recurrence sequences) and of Theorem 4.1. That is, we prove that under certain assumptions, an arbitrary linear recurrence sequence can have only finitely many terms in the coordinates of solutions of norm form equations. We show that the imposed assumptions are necessary. In our proof we shall combine the finiteness of solutions of polynomial-exponential equations proved by Schlickewei and Schmidt [41] with some other tools and ideas.

5.2 The main result

To formulate our main result, we need to introduce some notation. Let K be an algebraic number field of degree m, and write $\mathcal{N}(\gamma)$ for the norm of $\gamma \in K$ (over $\mathbb{Q}$). Let $\gamma_1, \ldots, \gamma_m \in K$ be linearly independent over $\mathbb{Q}$, and let t be a non-zero integer. Consider the norm form equation

$$\mathcal{N}(x_1\gamma_1 + \ldots + x_m\gamma_m) = t \tag{5.1}$$

in integers $x_1, \ldots, x_m$. Write X_i $(i = 1, \ldots, m)$ for the coordinate sets of solutions of (5.1).

Now we can formulate our main result.

Theorem 5.1 (Hajdu and Sebestyén [34]). *Let K be an algebraic number field of degree m, and (U_n) be a non-degenerate linear recurrence sequence of integers of order $r \geq 2$ given by* (2.1) *and* (2.3)*. If $\alpha_i \neq \pm 1$ for some $i = 1, \ldots, l$ and one of the conditions*

(i) $a_r \neq \pm 1$,

(ii) $K \cap \mathbb{Q}(\alpha_i) = \mathbb{Q}$ $(i = 1, \ldots, l)$

is satisfied, then

$$U_n \in X_1 \cup \ldots \cup X_m \tag{5.2}$$

holds only for finitely many indices n, where X_i $(i = 1, \ldots, m)$ are the sets of the coordinates of the solutions of (5.1)*. Further, the number of* *such indices is bounded by c_{13}, where $c_{13} = c_{13}(t, m, r)$ is an effectively computable constant depending only on t, m, r.*

Remarks. Clearly, the statement would remain valid also if we take only m' linearly independent algebraic integers

$$\gamma_i \in K \quad (i = 1, \ldots, m')$$

with $m' < m$ in (5.1). Indeed, in that case we could choose algebraic integers

$$\gamma_{m'+1}, \ldots, \gamma_m$$

from K such that $\gamma_1, \ldots, \gamma_m$ are linearly independent over $\mathbb{Q}$. As

$$X_1 \cup \ldots \cup X_{m'} \subseteq X_1 \cup \ldots \cup X_m,$$

the finiteness of the set of indices n with

$$U_n \in X_1 \cup \ldots \cup X_{m'}$$

immediately follows from Theorem 5.1.

We also note that the conditions in the theorem are all necessary. To show this, we exhibit some examples. However, we do so after the proof of Theorem 5.1, since then we shall have the required machinery and notation.

5.3 Lemmas and proofs

To prove our theorem we need an application of Lemma 2.4 with $s = 1$ to linear recurrence sequences. Note that it is closely related to the zero multiplicity of linear recurrence sequences, known to be finite and bounded due to a deep result of Schmidt [44].

Lemma 5.1. Let (U_n) be a non-degenerate linear recurrence sequence of integers of order $r \geq 2$. Using (2.3), let

$$I \subseteq \{1, \ldots, l\}.$$

Then there are only finitely many indices n for which

$$\sum_{i \in I} g_i(n)\alpha_i^n = 0 \tag{5.3}$$

holds. Further, the number of such indices n can be bounded by c_{14}, where $c_{14} = c_{14}(r)$ is an effectively computable constant depending only on r.

Proof. We apply Lemma 2.4 with $s = 1$. Let n be a solution of (5.3). First observe that if $g_i(n) = 0$ for some $i \in I$, then n comes from a finite set of cardinality bounded in terms of r. So we may assume that

$$g_i(n) \neq 0 \quad (i \in I).$$

Clearly, there is a partition $\mathcal{P}$ of I such that $n \in \mathcal{S}(\mathcal{P})$. If I has a class λ with $|\lambda| = 1$, then n is a root of one of the polynomials g_i $(i \in I)$, which is excluded. So we can suppose that $|\lambda| \geq 2$ for all $\lambda \in \mathcal{P}$. Clearly, since (U_n) is non-degenerate, we have $G(\mathcal{P}) = \{\mathbf{0}\}$. Thus by Lemma 2.4 n comes again from a finite set of cardinality bounded in terms of r, and our claim follows. □

Now we can prove our main result.

Proof of Theorem 5.1. By (2.4) we know that there are only finitely many pairwise non-associate algebraic integers μ in K of norm t, and their number can be bounded in terms of m, t. That is, if

$$(x_1, \ldots, x_m) \in \mathbb{Z}^m$$

is any solution of (5.1), then we have

$$x_1\gamma_1 + \ldots + x_m\gamma_m = \varepsilon\mu \tag{5.4}$$

with such a μ, where ε is a unit of K. As we need to bound the number of indices n for which $U_n = x_i$ for some solution $(x_1, \ldots, x_m)$ and i with $1 \leq i \leq m$, we may assume that μ is fixed. Let

$$\varepsilon_1, \ldots, \varepsilon_\ell$$

be a system of fundamental units in K. Then (5.4) yields

$$x_1\gamma_1 + \ldots + x_m\gamma_m = \zeta\varepsilon_1^{u_1}\ldots\varepsilon_\ell^{u_\ell}\mu, \tag{5.5}$$

where ζ is a root of unity in K. Since the number of roots of unity in K is bounded in terms of m, we may assume that here ζ is fixed. Taking the conjugates in (5.5) (following arguments from [1] and [26]) we get

$$\begin{pmatrix} \sigma_1(\gamma_1) & \cdots & \sigma_1(\gamma_m) \\ \vdots & \ddots & \vdots \\ \sigma_m(\gamma_1) & \cdots & \sigma_m(\gamma_m) \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = \begin{pmatrix} \sigma_1(\zeta\mu)\nu_{11}^{u_1}\cdots\nu_{1\ell}^{u_\ell} \\ \vdots \\ \sigma_m(\zeta\mu)\nu_{m1}^{u_1}\cdots\nu_{m\ell}^{u_\ell} \end{pmatrix}, \tag{5.6}$$

where $\sigma_1, \ldots, \sigma_m$ are the isomorphisms of K into $\mathbb{C}$ (in any order), and

$$\nu_{ij} = \sigma_i(\varepsilon_j) \quad (1 \leq i \leq m,\ 1 \leq j \leq \ell).$$

As the determinant of the matrix on the left hand side of (5.6) is known to be non-zero, we can write

$$x_i = b_{1i}\nu_{11}^{u_1}\cdots\nu_{1\ell}^{u_\ell} + \ldots + b_{mi}\nu_{m1}^{u_1}\cdots\nu_{m\ell}^{u_\ell} \quad (i = 1, \ldots, m) \tag{5.7}$$

with some algebraic numbers b_{ij} (belonging to the normal closure of K). Then, using the notation (2.11), by (2.3) and (5.7) relation (5.2) gives

$$b_{1i}\boldsymbol{\nu}_1^{\boldsymbol{u}} + \ldots + b_{mi}\boldsymbol{\nu}_m^{\boldsymbol{u}} = P_1(n)\alpha_1^n + \ldots + P_l(n)\alpha_l^n \tag{5.8}$$

with

$$\boldsymbol{u} = (u_1, \ldots, u_\ell)$$

for some i with $1 \le i \le m$. We may clearly assume that i is fixed. We shall apply Lemma 2.4 to handle the solutions $\boldsymbol{u}, n$ of (5.8). For this, we need to introduce some new notation. Define the $(m+1)$-tuples $\boldsymbol{\vartheta}_j$ $(1 \le j \le m+l)$ by

$$\boldsymbol{\vartheta}_j = \begin{cases} (\nu_{j1}, \ldots, \nu_{j\ell}, 1) & \text{for } 1 \le j \le m, \\ (1, \ldots, 1, \alpha_{j-m}) & \text{for } m+1 \le j \le m+l, \end{cases}$$

and the polynomials Q_j $(1 \le j \le m+l)$ in $\ell+1$ variables $\boldsymbol{z} = (z_1, \ldots, z_{\ell+1})$ by

$$Q_j(\boldsymbol{z}) = \begin{cases} b_{ji} & \text{for } 1 \le j \le m, \\ -P_j(z_{k+1}) & \text{for } m+1 \le i \le m+l. \end{cases}$$

Then we can rewrite (5.8) as

$$\sum_{j=1}^{m+l} Q_j(\boldsymbol{z}) \boldsymbol{\vartheta}_j^{\boldsymbol{z}} = 0. \tag{5.9}$$

Let $\mathcal{P}$ be any partition of the set $J = \{1, \ldots, m+l\}$. Observe that the number of such partitions is bounded in terms of m and r. Consider the refinement

$$\sum_{j \in \lambda} Q_j(\boldsymbol{z}) \boldsymbol{\vartheta}_j^{\boldsymbol{z}} = 0 \quad (\lambda \in \mathcal{P}). \tag{5.10}$$

of (5.9). We shall be concerned with the solutions of (5.10) which are not solutions of proper refinements of it; that is, with $\mathcal{S}(\mathcal{P})$. If there is a $\lambda \in \mathcal{P}$ such that

$$\lambda \subseteq \{m+1, \ldots, m+l\},$$

then any solution of (5.10) comes from a case where we have a vanishing subsum in the right hand side of (5.8). However, since by Lemma 5.1

the number of indices n which allow this is bounded in terms of r, we may assume that it is not the case. We study the set $G(\mathcal{P})$ - in fact, we show that $G(\mathcal{P}) = \{\mathbf{0}\}$ in any case. Take an index j_1 with $m+1 \leq j_1 \leq m+l$, such that $\alpha_{j_1} \neq \pm 1$. (By our assumptions, such an index exists.) Then $j_1 \in \lambda$ for some $\lambda \in \mathcal{P}$. By the above argument we see that there is a $j_2 \in \lambda$ with $1 \leq j_2 \leq m$ such that Q_{j_2} is not identically zero. If $\boldsymbol{z} \in G(\mathcal{P})$, then as $j_1 \overset{\mathcal{P}}{\sim} j_2$, we have

$$\nu_{j_2 1}^{z_1} \cdots \nu_{j_2 \ell}^{z_\ell} = \alpha_{j_1}^{z_{\ell+1}}. \tag{5.11}$$

If (i) holds, then since α_{j_1} is not a unit in $\sigma_{j_2}(K)$, we get $z_{\ell+1} = 0$. Then, as $\nu_{j_2 1}, \ldots, \nu_{j_2 \ell}$ is a system of fundamental units in $\sigma_{j_2}(K)$, we obtain $z_v = 0$ $(1 \leq v \leq \ell)$. Hence $\boldsymbol{z} = \mathbf{0}$, so $G(\mathcal{P}) = \{\mathbf{0}\}$, and our statement follows from Lemma 2.4 in this case. Assume that (ii) holds. Taking the inverse $\sigma_{j_2}^{-1}$ of σ_{j_2}, (5.11) yields

$$\varepsilon_1^{z_1} \cdots \varepsilon_\ell^{z_\ell} = \alpha_h^{z_{\ell+1}}, \tag{5.12}$$

where $\alpha_h = \sigma_{j_2}^{-1}(\alpha_{j_1})$. Clearly, α_h is an algebraic conjugate of α_{j_2}, so it is a root of $f(x)$ in (2.2). Thus (ii) gives that the unit $\alpha_h^{z_{\ell+1}}$ is rational - that is, it is ± 1. Since $\alpha_{j_1} \neq \pm 1$ and by the non-degenerate property of (U_n), α_h cannot be a root of unity, this gives $z_{\ell+1} = 0$. Then as $\varepsilon_1, \ldots, \varepsilon_\ell$ form a system of fundamental units in K, we also get $z_1 = \ldots = z_\ell = 0$. So $\boldsymbol{z} = \mathbf{0}$, and $G(\mathcal{P}) = \{\mathbf{0}\}$. Thus our statement follows from Lemma 2.4 also in this case. The proof of the theorem is complete. $\square$

As we mentioned earlier, the assumptions made in Theorem 5.1 are necessary. We conclude this section by some examples showing that this is the case indeed.

Examples. Let (U_n) be given by $U_0 = 0$, $U_1 = 1$ and $U_{n+2} = U_{n+1} - U_n$ $(n \geq 0)$. Then as one can easily check, (U_n) is given by $0, 1, 1, 0, -1, -1, 0, 1, \ldots$. That is, $U_n = 1$ for infinitely many indices n, and so it is easy to construct a norm form equation such that

$U_n \in X_1 \cup \ldots \cup X_m$ for infinitely many n. However, in this case the characteristic polynomial of (U_n) is $f(x) = x^2 - x + 1$, so the sequence is degenerate. Hence it is necessary to exclude this property.

Next, consider the sequence (U_n) defined by $U_0 = 0$, $U_1 = 1$ and $U_{n+2} = 2U_{n+1} - U_n$ $(n \geq 0)$. Then one readily gets that $U_n = n$ $(n \geq 0)$, so again, it is trivial to find a norm form equation such that $U_n \in X_1 \cup \ldots \cup X_m$ for infinitely many n. Now we have $f(x) = x^2 - 2x + 1 = (x-1)^2$, so the condition that one of the roots of f is different from ± 1 is violated.

Finally, assume that none of the conditions (i) and (ii) in Theorem 5.1 is satisfied. Let $\gamma = \sqrt[3]{2}$ and $K = \mathbb{Q}(\gamma)$. Then $1, \gamma, \gamma^2$ form an integral basis of K. Further, $\gamma - 1$ is a fundamental unit of K, and the only roots of unity in K are ± 1. Putting $(\gamma_1, \gamma_2, \gamma_3) = (1, \gamma, \gamma^2)$ and $t = 1$, the norm-form equation (5.1) is given by

$$\mathcal{N}(x_1 + x_2\gamma + x_3\gamma^2) = 1.$$

Since the norm of $\gamma - 1$ is 1, this equation is equivalent to

$$x_1 + x_2\gamma + x_3\gamma^2 = (\gamma - 1)^u \quad (u \in \mathbb{Z}).$$

Thus in this case (5.6) reads as

$$\begin{pmatrix} 1 & \gamma & \gamma^2 \\ 1 & \xi\gamma & \xi^2\gamma^2 \\ 1 & \xi^2\gamma & \xi\gamma^2 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} (\gamma - 1)^u \\ (\xi\gamma - 1)^u \\ (\xi^2\gamma - 1)^u \end{pmatrix},$$

where $\xi = (-1 + \sqrt{-3})/2$ (which is a primitive third root of unity). From this by a simple calculation we obtain that

$$x_1 = \frac{1}{3}(\gamma - 1)^u + \frac{1}{3}(\xi\gamma - 1)^u + \frac{1}{3}(\xi^2\gamma - 1)^u \quad (u \in \mathbb{Z}). \tag{5.13}$$

Set $U_0 = 1$, $U_1 = -1$, $U_2 = 1$ and $U_{n+3} = -3U_{n+2} - 3U_{n+1} + U_n$ $(n \geq 0)$. So (U_n) is a linear recurrence sequence of order $r = 3$, with characteristic polynomial $f(x) = x^3 + 3x^2 + 3x - 1$. As one can easily check, the roots of $f(x)$ are given by $\gamma - 1$, $\xi\gamma - 1$, $\xi^2\gamma - 1$, and also that in this case (2.3) is given by

$$U_n = \frac{1}{3}(\gamma - 1)^n + \frac{1}{3}(\xi\gamma - 1)^n + \frac{1}{3}(\xi^2\gamma - 1)^n \quad (n \geq 0). \tag{5.14}$$

Comparing (5.13) and (5.14) we see that $U_n \in X_1$ for every $n \geq 0$. Observe that now (i) does not hold as $a_3 = -1$, and (ii) does not hold since $K \cap \mathbb{Q}(\gamma - 1) = K$. So we need to require the validity of (i) or (ii), indeed.

References

[1] A. Bérczes, L. Hajdu, A. Pethő, *Arithmetic progressions in the solution sets of norm form equations*, Rocky Mountain J. Math. **40** (2010), 383–395.

[2] Cs. Bertók, L. Hajdu, I. Pink and Zs. Rábai, *Linear combinations of prime powers in binary recurrence sequences*, Int. J. Number Theory **13** (2017), 261–271.

[3] Cs. Bertók, L. Hajdu, I. Pink and S. S. Rout, *Sums of S-units in recurrence sequences*, J. Number Theory **196** (2019), 353–363.

[4] F. Beukers, R. Tijdeman, *On the multiplicities of binary complex recurrences*, Compositio Math. **51** (1984), 193–213.

[5] J.-P. Bézivin, A. Pethő and A. J. van der Poorten, American J. Math. **112**, (1990), 985–1001.

[6] Yu. Bilu, G. Hanrot and P. M. Voutier, *Existence of primitive divisors of Lucas and Lehmer numbers. With an appendix by M. Mignotte*, J. Reine Angew. Math. **539** (2001), 75–122.

[7] Z. I. Borevich, I. R. Shafarevich, *Number Theory*, Academic Press, New York, 1966.

[8] E. F. Bravo, C. A. Gómez and F. Luca, *X-coordinates of Pell equations as sums of two tribonacci numbers*, Period. Math. Hung. **77** (2018), 175–190.

[9] J. J. Bravo, B. Faye and F. Luca, *Powers of two as sums of three Pell numbers*, Taiwanese J. Math. **21** (2017), 739–751.

[10] B. Brindza, A. Pintér, W. M. Schmidt, *Multiplicities of Binary Recurrences*, Canad. Math. Bull. **44** 2001, 19–21.

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

[12] M. Ddamulira, *On the x-coordinates of Pell equations that are products of two Padovan numbers*, Integers **20** (2020), A70.

[13] M. Ddamulira, *On the x-coordinates of Pell equations that are products of two Lucas numbers*, Fibonacci Quart. **58** (2020), 18–34.

[14] M. Ddamulira and F. Luca, *On the x–coordinates of Pell equations which are k-generalized Fibonacci numbers*, J. Number Theory **207** (2020), 156–195.

[15] M. Ddamulira and F. Luca, *The x-coordinates of Pell equations and sums of two Fibonacci numbers II*, Proc. Indian Acad. Sci. (Math. Sci.) **130** (2020), art. no. 58.

[16] M. Ddamulira and F. Luca, *On the x-coordinates of Pell equations that are products of two Pell numbers*, (2020) Preprint, DOI: 10.33774/coe-2020-k4cc4

[17] H. Erazo and C. A. Gómez, *Linear combinations of prime powers in X-coordinates of Pell equations*, Ramanujan J. **53** (2020), 123–137.

[18] H. Erazo and C. A. Gómez, *An exponential Diophantine equation related to the sum of powers of two consecutive terms of a Lucas sequence and x-coordinates of Pell equations*, Period. Math. Hungar. **83** (2021), 165—184.

[19] H. Erazo, C. A. Gómez and F. Luca, *On Pillai's problem with X-coordinates of Pell equations and powers of* 2 *II*, Int. J. Number Theory **17** (2021), 2251–2277.

[20] G. Everest, A. van der Poorten, I. Shparlinski, T. Ward, *Recurrence Sequences*, Amer. Math. Soc., 2015, 318 pp.

[21] J.-H. Evertse and K. Győry, *Unit Equations in Diophantine Number Theory*, Cambridge University Press, 2015, pp. 378.

[22] B. Faye and F. Luca, *On the X-coordinates of Pell equations which are repdigits*, Fibonacci Quart. **56** (2018), 52–62.

[23] B. Faye and F. Luca, *On Y-coordinates of Pell equations which are members of a fixed binary recurrence*, New York J. Math. **26** (2020), 184–206.

[24] B. Faye and F. Luca, *On Y-coordinates of Pell equations which are base* 2 *repdigits*, Glas. Mat. Ser. III **55** (2020), 1–12.

[25] Fibonacci, *Liber Abaci*, 1202.

[26] C. Fuchs and S. Heintze, *Norm form equations with solutions taking values in a multi-recurrence*, Acta Arith. **198** (2021), 427–438.

[27] C. Fuchs, F. Luca, L. Szalay, *Diophantine triples with values in binary recurrences*, Ann. Sc. Norm. Sup. Pisa **7** (2008), 579–608.

[28] C. A. Gómez and F. Luca, *Zeckendorf representations with at most two terms to x-coordinates of Pell equations*, Sci. China Math. **63** (2018), 627–642.

[29] C. A. Gómez, F. Luca and F. S. Zottor, *On X-coordinates of Pell equations which are repdigits*, Res. Number Theory **6** (2020), paper no. 41.

[30] S. Guzman-Sanchez and F. Luca, *Linear combinations of factorials and S-units in a binary recurrence sequence*, Ann. Math. Qué. **38** (2014), 169–188.

[31] K. Győry, *On the numbers of families of solutions of systems of decomposable form equations*, Publ. Math. Debrecen **42** (1993), 65–101.

[32] L. Hajdu and P. Sebestyén, *Sums of S-units in the solution sets of generalized Pell equations*, Arch. Math. **115** (2020), 279–287.

[33] L. Hajdu, P. Sebestyén, *Terms of recurrence sequences in the solution sets of generalized Pell equations*, Int. J. Number Theory **18** (2022), 1605–1612.

[34] L. Hajdu, P. Sebestyén, *Terms of recurrence sequences in the solution sets of norm form equations*, Archiv der Math. (2023), https://doi.org/10.1007/s00013-023-01941-3

[35] B. Kafle, F. Luca, A. Montejano, L. Szalay and A. Togbé, *On the x-coordinates of Pell equations which are products of two Fibonacci numbers*, J. Number Theory **203** (2019), 310–333.

[36] K. Liptai, *Pell egyenletek megoldása lineáris rekurzív sorozatok segítségével*, Acta Acad. Paed. Agriensis, Sect. Mat. **21** (1993), 15–26.

[37] F. Luca and A. Togbé, *On the x–coordinates of Pell equations which are Fibonacci numbers*, Math. Scand. **122** (2018), 18–30.

[38] I. Niven, H. S. Zuckerman and H. L. Montgomery, *An Introduction to the Theory of Numbers*, Fifth Edition, John Wilea & Sons, Inc., 1991.

[39] A. Pethő, *Perfect powers in second order linear recurrences*, J. Number Theory **15** (1982), 5–13.

[40] A. Schinzel, On two theorems of Gelfond and some of their applications, Acta Arith. **13** (1967), 177–236. Corrigendum: Acta Arith. **16** (1969/1970), 101.

[41] H.-P. Schlickewei and W. Schmidt, *The Number of Solutions of Polynomial-Exponential Equations*, Compositio Math. **120** (2000), 193–225.

[42] 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.

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

[44] W. Schmidt, *The zero multiplicity of linear recurrence sequences*, Acta Math. **182** (1999), 243–282.

[45] Henk C.A. van Tilborg, *Encyclopedia of Cryptography and Security*, Springer, Boston, MA (2005), 29–30.

Magyar nyelvű összefoglaló (Summary in Hungarian)

A disszertációban lineáris rekurzív sorozatokra vonatkozó eredményeket tárgyalunk.

A lineáris rekurzív sorozatok irodalma rendkívül gazdag: számos klasszikus eredmény mellett rengeteg modern eredménnyel is találkozhatunk. Az ilyen típusú sorozatok tulajdonságait sok szerző több szempontból vizsgálta. Csupán néhány fő irányt említve: oszthatósági tulajdonságok vizsgálata (pl. Bézivin, Pethő és van der Poorten [5], vagy Bilu, Hanrot és Voutier [6]), teljes hatványok létezésének kérdése a sorozat tagjai között (pl. Pethő [39], Shorey és Stewart, vagy Bugeaud, Mignotte és Siksek [11]), a zéró-multiplicitás vagy általánosabban az a-multiplicitás kérdése (lásd pl. Beukers és Tijdeman [4], Schmidt [44] Brindza, Pintér és Schmidt [10], illetve az ezekben található hivatkozások). Egy további, speciális de érdekes problémát említve, Fuchs, Luca és Szalay [27] úgynevezett diofantoszi halmazok egy kiterjesztését vizsgálja lineáris rekurzív sorozatok esetére. További nyitott kérdéseket, illetve effektív és ineffektív végességi eredményeket és különböző alkalmazásokat például a Shorey és Tijdeman [43], Everest, van der Poorten, Shparlinski és Ward [20], illetve az Evertse és Győry [21] könyvekben találhatunk.

A jelen disszertációban különböző, lineáris rekurzív sorozatokhoz kapcsolódó problémákat és eredményeket tárgyalunk, illetve bizonyítunk.

Elsőként a következő kérdést vizsgáljuk. Adott d, t nem nulla egész számokat véve, ahol $d > 1$ négyzetmentes, tekintsük az

$$x^2 - dy^2 = t$$

alakú általánosított Pell egyenletet. A probléma: az egyenlet hány x, y egész megoldása állhat elő olyan számok rögzített tagszámú összegeiként, melyek prímfaktorai egy előre megadott véges prímhalmazhoz tartoznak? Amint a disszertációból kiderül, ez a kérdés másodrendű lineáris rekurzív sorozatok elemei között előforduló, úgynevezett S-egység összegek tanulmányozásához vezet. Bebizonyítjuk, hogy bizonyos feltételek mellett ez a szám véges. Fontos megjegyezni, hogy a végességet garantáló feltételünk szükséges, más szavakkal kvalitatív értelemben eredményünk nem javítható.

Ezután tetszőleges rendű lineáris rekurzív sorozatok elemeinek számát vizsgáljuk általánosított Pell egyenletek megoldáshalmazaiban. Bebizonyítjuk, hogy bizonyos megkötések mellett ez a szám is véges, valamint felső korlátot adunk a lehetséges előfordulások számára. Emellett teljes pontossággal meghatározzuk az összes elfajuló esetet (azaz azon eseteket, amikor végtelen sok megoldás létezik). Ily módon ezen eredményeink is kvalitatíve a lehető legpontosabbak.

Végül, eredményeinket kiterjesztjük rekurzív sorozatok elemeinek leírására norma forma egyenletek, azaz

$$\mathcal{N}(x_1\gamma_1 + \ldots + x_m\gamma_m) = t$$

alakú egyenletek megoldáshalmazaiban, ahol $\mathcal{N}$ egy adott K algebrai számtest normája $\mathbb{Q}$-ra nézve, $\gamma_1, \ldots, \gamma_m$ lineárisan független elemek K-ban $\mathbb{Q}$ felett, t pedig egy nem nulla egész. (Megjegyezzük, hogy az általánosított Pell egyenlet egy norma forma egyenlet egy másodfokú algebrai számtest felett.) Ebben az esetben is sikerül végességi eredményeket adnunk, oly módon, hogy az ebben az általánosságban megadott feltételeink is szükségesek lesznek.

Tételeink bizonyításához több különböző módszer és tétel kombinálására volt szükség: többek között felhasználtuk a a norma forma egyenletek, az S-egység egyenletek és a polinomiális-exponenciális egyenletek elméletét.

A disszertáció felépítése a következő. A második fejezetben összefoglaljuk a legfontosabb fogalmakat és eszközöket, amelyekre a disszertációban támaszkodunk. Nevezetesen, bevezetünk és összefoglalunk néhány, rekurzív sorozatokhoz, S-egységekhez, S-egység egyenletekhez és polinomiális-exponenciális egyenletekhez kapcsolódó jelölést és tételt. Az utána következő három fejezet tartalmazza új eredményeinket, a fent említett sorrendben. Az egyes fejezetekben az új eredmények és bizonyításaik bemutatása mellett a vizsgált problémák hátterét is felvázoljuk, illetve azok irodalmi beágyazását is elvégezzük.

Summary

The topic of this dissertation is the study of linear recurrence sequences.

Such sequences are of classical and recent interest, and have been investigated from many aspects: divisibility properties (see e.g. results of Bézivin, Pethő and van der Poorten [5], and Bilu, Hanrot and Voutier [6]), existence of perfect powers among the terms (cf. for example papers of Pethő [39], Shorey and Stewart [42], Bugeaud, Mignotte and Siksek [11]), zero-multiplicity or more generally, a-multiplicity (see for example Beukers and Tijdeman [4], Schmidt [44] and Brindza, Pintér and Schmidt [10], and the references therein). Certainly, there are many more directions one could mention. As a particular, but interesting problem one may e.g. discuss the paper of Fuchs, Luca and Szalay [27] related to variants of so-called Diophantine sets. For other problems, properties and various general effective and ineffective finiteness results and many applications, see e.g. the books of Shorey and Tijdeman [43], Everest, van der Poorten, Shparlinski and Ward [20], and Evertse and Győry [21].

In this dissertation we discuss problems and prove various new results related to linear recurrence sequences.

First we consider the following question. Given a generalized Pell equation of the shape

$$x^2 - dy^2 = t$$

with non-zero integers d, t where $d > 0$ is square-free, how many of its integral solutions x, y can be represented as an arbitrary, but fixed term sum of integers with prime factors coming from some given finite set of primes? As we see, this question leads to the investigation of the question that how many terms of a binary linear recurrence sequence can be obtained as the sum of a fixed number of so-called integral S-

units. We prove that under some conditions, this number is finite, and we give an effective upper bound for the number of such numbers. It is important to note that our conditions will be necessary, so in the qualitative sense our results are best possible.

Then, we investigate the number of terms of linear recurrence sequences of arbitrary degree in the solution sets of generalized Pell-equations. We prove that under certain assumptions, the number of such terms is finite, and give effective upper bounds for the number of exceptional terms. We are able to describe all the degenerate cases (that is, cases where there are infinitely many solutions) completely. Thus our results are qualitatively precise in this case, as well.

Finally, we extend our results to the case of terms of recurrence sequences in the solution sets of norm form equations, i.e. equations of the form

$$\mathcal{N}(x_1\gamma_1 + \ldots + x_m\gamma_m) = t,$$

where $\mathcal{N}$ is the norm from an algebraic number field K to $\mathbb{Q}$, $\gamma_1, \ldots, \gamma_m$ are linearly independent elements of K over $\mathbb{Q}$, and t is a non-zero integer. (We mention that the generalized Pell equation appearing in the previous paragraph, is in fact a norm form equation over an algebraic number field of degree two.) We are able to give finiteness results for the number of such terms in this case, as well. Further, the conditions we impose are necessary here, too.

To prove our results, we combine various deep tools, such as the theory of norm form equations, S-unit equations and polynomial-exponential equations.

The structure of the dissertation is the following. In the second chapter we summarize the most important notions and tools used. Namely, we introduce some notation and recall some important theorems and assertions related to recurrence sequences, algebraic number fields, S-units and S-unit equations and polynomial-exponential equations. The next three chapters contain our results, following the order indicated above. Beside our new results, in these chapters we give the background of the investigated problems, together with a thorough account of the related problems and literature as well.

Publications of Péter Sebestyén

- L. Hajdu and P. Sebestyén, *Sums of S-units in the solution sets of generalized Pell equations*, Archiv der Math. **115** (2020), 279–287.

- L. Hajdu and P. Sebestyén, *Terms of recurrence sequences in the solution sets of generalized Pell equations*, Int. J. Number Theory **18**, No. 07 (2022), 1605–1612.

- L. Hajdu and P. Sebestyén, *Terms of recurrence sequences in the solution sets of norm form equations*, Archiv der Math. (2023), published online, https://doi.org/10.1007/s00013-023-01941-3

Conference talks of Péter Sebestyén

- *S-egység összegek Pell egyenletek megoldáshalmazaiban*, Seminar of the Number Theory Research Group, 22 March 2019, Debrecen
- *Sums of S-units in the solution sets of generalized Pell equations*, Austrian-Hungarian Research Seminar, 7 May 2021, online talk
- *Terms of recurrence sequences in the solution sets of generalized Pell equations*, Number Theory Conference in honour of Professors Győry, Pintz and Sárközy, 4 July 2022, Debrecen