# Coprimality in consecutive terms of integer sequences

Doktori (PhD) értekezés

**Szikszai Márton**

Témavezető: Dr. Hajdu Lajos
egyetemi tanár

DEBRECENI EGYETEM
Természettudományi Doktori Tanács
Matematika-és Számítástudományok Doktori Iskola
Debrecen, 2018.

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

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

Debrecen, 2018. ..........................

A jelölt aláírása

Tanúsítom, hogy Szikszai Márton doktorjelölt 2013-2016 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, 2018. ..........................

A témavezető aláírása

# Coprimality in consecutive terms of integer sequences

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

Írta: Szikszai Márton okleveles alkalmazott 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. .................... ...........................
tagok: Dr. .................... ...........................
Dr. .................... ...........................

A doktori szigorlat időpontja: 2017.01.30.

Az értekezés bírálói:

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

A bírálóbizottság:

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

Az értekezés védésének várható időpontja: 2018.

# Acknowledgements

The completion of my doctoral thesis would not have been possible without the personal and professional support of many people.

I am most grateful to my supervisor Professor Lajos Hajdu for bringing me into mathematical research early and encouraging me to pursue a scientific career throughout my university years. I could always rely on his advice and help in the challenges of my career.

Special thanks are due to my family, my wife Bettina, my mother Enikő, my sister Nóra, and my brother Balázs. They provided a calm and relaxing environment whenever I had to take my mind off work.

I would also like to express my gratitude toward my colleagues at the Department of Algebra and Number Theory, especially to Professor Kálmán Győry, Attila Bérczes, Szabolcs Tengely, and István Pink.

Finally, I thank all the people, friends, colleagues, former classmates, and other persons whose help I may not aware of, who contributed in some way to my career and its most recent cornerstone.

*Édesapám emlékére, aki nem tudott tovább maradni...*

*To the memory of my Father, who could not stay longer...*

# Contents

# 1 Introduction

Let us begin by considering a problem which, to the author's knowledge, was first studied by Szekeres [20] in an unpublished communication[1] and independently in a paper of Pillai [62]. We present it as follows, albeit the formulations were different.

**Problem 1.** Let $k \geq 2$ be an integer. Is it true that in every set of $k$ consecutive integers there exists one which is coprime to all the others?

One may immediately answer the question if $k$ is reasonably small. For instance, each of two consecutive integers is always coprime to the other. Same holds for the one in the middle of a block of three consecutive integers. Similarly straightforward and easy considerations can settle the cases of $k = 4$, 5, or 6. Obviously, the larger $k$ becomes, the harder it is to directly check the possible common divisors.

The earliest documented result traces back to Erdős [19], who proved that if $k$ is larger than some positive constant $k_0$, then the answer should be false. However, his method is ineffective and does not give a way to compute $k_0$. The first effective statement was made by Pillai[2] [62] half a decade later. Indeed, he showed that there always exists an element coprime to all the others if $k \leq 16$, but the contrary holds whenever $17 \leq k \leq 430$. The latter result was extended to every $k \geq 17$ in a work of Brauer[3] [11], resolving Problem 1 completely. Since then, various proofs of these bounds appeared in the literature, notably by Pillai [64, 65], Evans [22], Harborth [44, 45], Eggleton [18], and Gassko [30].

[1] Erdős [20] mentioned it, but no accessible publication of Szekeres discusses it, see [33] for a complete list of them.

[2] In [20], this was independently attributed to Szekeres as well.

[3] Pillai [64] noted that between the papers of his and Brauer's, he received a letter from Scott, in which the constant 430 was improved to a number slightly less than $2.5 \cdot 10^9$.

Note that the interest in the study of Problem 1 is many-folded. Here, we briefly mention two important directions that stimulated the early progress of the topic.

Pillai was motivated by the long standing folklore conjecture which states that the product of $k \geq 2$ consecutive integers can never be a perfect power. Combining his result with further elementary methods he verified it for $k \leq 16$, see [63]. It is well-known that a complete solution was given by the famous theorem of Erdős and Selfridge [21].

Another closely related research area is that of prime gaps. Originally, Erdős [19] worked on lower bounds concerning the difference of consecutive primes, but he did not discuss the consequences regarding Problem 1. On the other hand, Brauer [11] definitely related his interest in the topic to an earlier result he obtained with Zeitz [12, 5]. There, they considered an old problem of Legendre [53] on the maximum number of consecutive integers which are divisible by at least one of the first $m$ primes.

Gradually, Problem 1 itself began to attract increased attention and was extended in many directions. There are two natural ways to take if we intend to generalize the original question: one is to relax the coprimality condition, the other is to replace consecutive integers with consecutive terms of some sequence of integers. Since the related literature is very rich in each case, we give a detailed exposition of the results.

Before starting the discussion, it is time to introduce some parts of the terminology. This includes a more general notion of coprimality and two strongly connected quantities, simplifying the description of results related to Problem 1.

Let $T$ be an arbitrary set of positive integers such that $1 \in T$. The integers $x$ and $y$ are said to be *$T$-coprime* if $\gcd(x, y) \in T$. Now take any sequence of integers $s = (s_n)_{n=0}^{\infty}$ and define two numbers, $g_s(T)$ and $G_s(T)$, as follows. Let $g_s(T)$ be the smallest positive integer such that there exist $g_s(T)$ consecutive terms of $s$ with the property[4] that none of them is $T$-coprime to all the others. Similarly, let $G_s(T)$ stand for the smallest positive integer such that for each $k \geq G_s(T)$ one can find $k$ consecutive terms so that the latter property holds. Both quantities may or may not exist, we will see examples of every possibility later. Note that whenever $s$ is the sequence of consecutive non-negative integers or if $T = \{1\}$, we suppress the dependence both on $s$ and $T$, respectively. For instance, we write that the combined efforts of Pillai [62] and Brauer [11] gave $g = G = 17$.

We start with the first type of generalizations, the relaxation of the coprimality condition. Let $d$ be a fixed positive integer. Caro [15] proved the existence of $g(d) = g(\{1, 2, \ldots, d\})$ and $G(d) = G(\{1, 2, \ldots, d\})$ for arbitrary $d$ and established the upper bounds

$$g(d) \leq 45d \log d \qquad \text{and} \qquad G(d) \leq 54d \log d.$$

Both were slightly improved in a joint work of Saradha and Thangadurai [72], in case $d \geq 11$ and $d \geq 20$, respectively. Interestingly, neither paper contains any exact values of $g(d)$ or $G(d)$ for some value of $d$, let it be very small[5].

In a recent work, Hajdu and Saradha [37] made significant progress on the previous results. Let $T$ be a non-empty set of positive integers. Provided that $T$ does not have "too many" elements, they obtained effective upper bounds on both $g(T)$ and $G(T)$. More precisely, if there exists some constant $c_0$ such that for every $c > c_0$ the number of elements in $T$ does not exceed $c/(10 \log c)$, then

$$G(T) \leq \max(425, 2c_0 + 1).$$

They derived a similar upper bound under the assumption that the set of all primes dividing some element in $T$ satisfies analogous restric-

[4] In a number of papers, this property has its own notation $P(T)$.

[5] For instance, $g(2) \leq 63$ and $G(2) \leq 75$ and the exact value can be checked by straightforward computation using a rather modest capacity.

tions on its natural density[6]. On the other hand, they also invented a heuristic algorithm for the exact computation of $g(T)$ and $G(T)$, in case $T$ is given explicitly. It was used, for instance, to show that $g(2) = G(2) = 25$ and that $g(\{2^\alpha : \alpha \geq 0\}) = G(\{2^\alpha : \alpha \geq 0\}) = 86$. For a comprehensive list of their calculations, see [38].

One may replace consecutive integers by consecutive terms of some sequence of integers as well. Evans [23] was the first to study arithmetic progressions $s = (a + nd)_{n=0}^{\infty}$ and he proved the analogue of Erdős's result by showing the existence of $G_s$. As in the paper of Erdős [19], the means of effectively computing it, or at least $g_s$, are not discussed. Ohtomo and Tamari [60] derived the same result, but also obtained $g_s \leq 385$ for the sequence of odd numbers. Hajdu and Saradha [37] noted that if one aims to find effective upper bounds, then either the problem is trivial[7] or there is a set $T$ such that $g_s = g(T)$ and $G_s = G(T)$ hold. Unsurprisingly, the set $T$ is the set of all integers composed of primes dividing $d$. We mention that arithmetic progressions over unique factorization domains were also considered, see the paper of Ghorpade and Ram [32] on this particular case.

An arithmetic progression $(a + nd)_{n=0}^{\infty}$ is essentially the evaluation of the linear polynomial $a + dx \in \mathbb{Z}[x]$ over non-negative integers. In this spirit, Harrington and Jones [46] extended the scope of Problem 1 to quadratic sequences[8], that is, to sequences defined by polynomials of degree 2 with integer coefficients. Using direct computation they gave all the possible values of $g_s$ for every monic and a specific family of non-monic quadratic polynomials. They also conjectured that $g_s$ exists for any quadratic sequence and is uniformly bounded. On the other hand, they did not study $G_s$ to any extent.

[6] A set of positive integers $T$ has natural density $\alpha$ if $\lim\limits_{n\to\infty} \frac{|T(n)|}{n} = \alpha$, where $T(n)$ consists of elements in $T$ not exceeding $n$.

[7] In case the initial term $a$ and the difference $d$ satisfy $\gcd(a, d) > 1$, no two terms can be coprime.

[8] In certain pieces of literature, these sequences appear as second-order arithmetic progressions.

Present thesis connects to the previous investigations and considers Problem 1 in important sequences of integers under varying coprimality conditions. Our new results and contributions to the theory are summarized in the remaining part of the section.

To follow in the footsteps of Evans [23], we begin the discussion with sequences of the form

$$s = (f(n))_{n=0}^{\infty} \qquad f \in \mathbb{Z}[x].$$

Our main concern is the conjecture made by Harrington and Jones. Indeed, we prove the existence of $G_s$ provided that the degree of the corresponding polynomial is at most 3. As a corollary, the existence of $g_s$ for quadratic sequences immediately follows, providing a qualitative answer to the conjecture. The backbone of our proof is formed by a simple, but fruitful relationship between $f$ and an auxiliary polynomial arising from the resultant of $f$ and its shifts. Based on this connection, we explain a "greedy" approach to finding a constant $k_0$ such that for every $k \geq k_0$ one can construct infinitely many sets of $k$ consecutive terms

$$f(n+1), f(n+2), \ldots, f(n+k)$$

so that none of them is coprime to all the others. In particular, this proves the existence of $G_s$. The success of our idea relies on estimates concerning primes satisfying desirable properties on both their size and their relation to congruences involving $f$ and the corresponding auxiliary polynomial. Note that our construction of $k_0$ is ineffective, but in principle, it can be made effective. On the reasons why we do not make it so and for remarks on both the relaxation of the coprimality condition and the uniform upper bound in the conjecture of Harrington and Jones, see the end of Section 2.

In the second part of the thesis, we turn our attention to recurrence sequences. Section 3 deals with sequences $s = (s_n)_{n=0}^{\infty}$ which obey a linear recurrence relation of the form

$$s_{n+r} = a_1 s_{n+r-1} + a_2 s_{n+r-2} + \cdots + a_r s_n \qquad (n \geq 0)$$

for some fixed integers $r \geq 1$ and $a_1, a_2, \ldots, a_r$ and satisfy, in most cases, the additional divisibility property that $m \mid n$ implies $s_m \mid s_n$. Let $S$ be a finite set of primes and $T$ be some subset of $\mathbb{Z}_S$, the set of all integers having no prime factors outside $S$, with $1 \in T$. Under the natural assumption of non-degeneracy, we prove that both $g_s(T)$ and $G_s(T)$ exist and are effectively bounded in terms of $r$ and $|S|$. In our reasoning, we rely on the divisibility property to construct a set $T'$ such that $G_s(T) \leq G(T')$ holds. A key element here is a deep theorem of Schlickewei and Schmidt [74], concerning the number of solutions to polynomial-exponential equations. With its help, we are able to apply results of Hajdu and Saradha [37] and verify the existence and effective boundedness of $G(T')$.

Restricting ourselves to binary recurrences only, that is, to $r = 2$, we obtain much stronger statements. A simple characterization result identifies linear divisibility sequences of order 2 as Lucas sequences of the first kind[9]. As a superior alternative to the estimates of Schlickewei and Schmidt, we can apply the celebrated theorem of Bilu, Hanrot, and Voutier [8] on the existence of primitive prime divisors. Lucas sequences of the first kind also satisfy the strong divisibility, meaning $\gcd(s_m, s_n) = s_{\gcd(m,n)}$. This way, we can write $g_s(T) = g(T')$ and $G_s(T) = G(T')$ in place of the inequalities. The considerably stronger construction has its benefits, in the sense that we are able to compute every possible values of $g_s$ and $G_s$. Let us briefly mention that as an intermediate step we solve a problem of Beukers [7] concerning ±1 elements among terms of Lucas sequences of the first kind.

Our results raise the natural question on the necessity of the divisibility property assumed. A promising study of this problem is induced by Lucas sequences of the second kind[10]. Here, the strong restrictions

[9] Lucas sequences of the first kind are binary recurrences with initial terms $s_0 = 0$ and $s_1 = 1$ satisfying the recurrence $s_{n+2} = Ps_{n+1} - Qs_n$ for some nonzero integers $P$ and $Q$.

[10] Lucas sequences of the second kind are binary recurrences with initial terms $s_0 = 2$ and $s_1 = P$ satisfying the same recurrence as Lucas sequences of the first

on the arithmetic of the recurrences are only slightly weakened, yet our corresponding theorem shows that already the existence of $G_s$ becomes “rare” and that frequently, not even $g_s$ exists. Nevertheless, the behavior is by no means chaotic, as we are able to completely classify each phenomenon and provide strong quantitative results. In the final part of the section, we briefly discuss linear recurrences devoid of any specific divisibility property.

One may also wonder what happens if we drop the linearity in the recursive definition, but keep the strong arithmetic intact. We study this situation in Section 4. The subject of our experiment is a family of bilinear recurrences known as elliptic divisibility sequences. Let $E$ be an elliptic curve over $\mathbb{Q}$ given by a generalized Weierstrass equation of the form

$$E: \qquad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

and let $P$ be an affine rational point of infinite order. Write the coordinates of the multiples $nP$ in the form

$$nP = \left(\frac{A_n}{B_n^2}, \frac{C_n}{B_n^3}\right) \qquad (n \geq 1)$$

with $A_n, B_n, C_n \in \mathbb{Z}$ and $\gcd(A_nC_n, B_n) = 1$. Putting $B_0 = 0$, the resulting sequence $B = (B_n)_{n=0}^{\infty}$ is said to be anelliptic divisibility sequence. Ward [83] was the first to define such sequences using the bilinear recurrence relation

$$B_{m+n}B_{m-n} = B_{m+1}B_{m-1}B_n^2 - B_{n+1}B_{n-1}B_m^2 \qquad (m \geq n \geq 0),$$

but the definition[11] we use has become more standard over time. We prove that in this specific family of bilinear recurrences, one can obtain the analogues of our theorems on linear divisibility sequences. Indeed,

kind.

[11] This is often attributed to Silverman [76], but the construction was essentially known to Ward [83] already.

let $S$ be a finite set of primes and $T$ be some subset of $\mathbb{Z}_S$. Once more, $g_B(T)$ and $G_B(T)$ exist and can be effectively bounded in terms of the equation $E$ and the set $S$. The main steps of the proof are identical to those we make for linear divisibility sequences. The only change is the application of a result concerning integral and $S$-integral points on elliptic curves due to Hajdu and Herendi [35] in place of the theorem of Schlickewei and Schmidt [74].

Note that elliptic divisibility sequences are also strong divisibility sequences. One may be optimistic about the complete resolution of the related version of Problem 1, as it is the case with Lucas sequences of the first kind. However, a similar approach would fail for various reasons. We discuss these briefly.

Finally, in Section 4, we consider Diophantine applications. Recall that Pillai [63] studied whether the Diophantine equation

$$x(x+1)\dots(x+k-1)=y^\ell$$

can have a solution in unknown positive integers $x, y, k$, and $\ell$, where $k, \ell \geq 2$. The folklore conjecture stated that it does not have any. To verify it for $k < g = 17$, Pillai used the fact that one of

$$x, x+1, \dots, x+k-1$$

has to be an $\ell$th power itself, since it is coprime to all the others. The idea naturally translates to similar equations consisting of consecutive terms of some sequence of integers.

As an illustration, we consider a problem involving terms of an elliptic divisibility sequence $B = (B_n)_{n=0}^{\infty}$. More precisely, we show that if $\ell \geq 2$ is fixed and $B_1 = 1$, then the equation

$$B_n B_{n+d} \dots B_{n+(k-1)d} = y^\ell$$

can admit only finitely many solutions in unknown integers $m, d, k$, and $y$, where $m, d \geq 1$, $k \geq 2$ and $\gcd(m, d) = 1$. Note that $B_1$

depends on both the curve and the point chosen. This makes the assumption $B_1 = 1$ seem to be a serious restriction. We discuss why it is merely a technical condition and how one can eliminate it, at least in principle. Our proof relies on the arithmetic of elliptic divisibility sequences, explicit computations made by Hajdu and Saradha [38], estimates on the number of primes in certain intervals, and a finiteness result on perfect powers in $B$ by Everest, Reynolds, and Stevens [27]. While our result is not effective, an additional condition makes it so. We also explain how our proof turns into an algorithm which can be applied to solve a given specific case efficiently.

As a closure to the introduction, let us mention that most of the content can be found scattered across the papers [39, 40, 41, 36, 71]. Compared to these our discussion is slow-paced, but more uniform and detailed. While some of the results are left out to keep integrity, in certain cases, we improve the earlier ones and refine the proofs as well. We also put emphasis on a considerably exhaustive presentation of the history of Problem 1 and related results.

Finally, we note that the author was involved in other scientific activities during his doctoral scholarship period. Since these results are only loosely connected to the content of the present thesis, we do not include them here and for details we refer to the papers [29, 17, 66, 42, 81]

# 2 Quadratic and cubic sequences

This section is devoted entirely to the study of sequences of the form $s = (f(n))_{n=0}^{\infty}$, where $f \in \mathbb{Z}[x]$. We do not give them any specific name, although for the sake of clarification, and non the less of aesthetics, we use expressions like the *sequence corresponding to $f$*, and *quadratic* or *cubic sequence*. In any case, we make sure that $s$ is clearly identified from the context. Our main concern is an extension of Problem 1 to such sequences and, in particular, a conjecture of Harrington and Jones [46] on the existence of $g_s$ when $f$ is quadratic. Note that the results of this section can be found in a joint paper of Sanna and the author [71].

## 2.1 Brief overview of related results

We begin with a summary of what is already known on the topic. The case when $f$ is constant is not much of interest. Indeed, if $f = \pm 1$, then neither $g_s$ nor $G_s$ exist, otherwise both of them do and $g_s = G_s = 2$. For linear polynomials $f(x) = a + dx$ the situation is more complex, but, in principle, it is also solved. Recall that Evans [23] proved the existence of $G_s$ in arithmetic progressions and, in turn, that of $g_s$ as well. Further, Hajdu and Saradha [37] explained how to obtain effective upper bounds for both quantities depending on $d$ only[12]. Exact computation is also possible using their heuristic algorithm, for instance, it is known that if $d = 2^{\alpha}$ for some positive integer $\alpha$, then $g_s = G_s = 86$.

The next reasonable step is to consider polynomials of degree 2 and their corresponding sequences. The only known result in this direction, that appears in the literature, is due to Harrington and Jones [46]

[12] For each $d$ they construct a set $T$ such the $G_s \leq G(T)$. It is very straightforward how the bound can be made dependent on $d$ only following their explanation.

concerning $g_s$.

**Theorem 2.1** (Harrington and Jones [46]). *Let $f(x) = ax^2 + bx + c \in \mathbb{Z}[x]$ be an irreducible polynomial of degree 2 and let $s = (f(n))_{n=0}^{\infty}$. Suppose that one of the following holds:*

*i)* $a = 1$;

*ii)* $(a, b) = (2^k, 0)$ *for some positive integer $k$;*

*iii)* $\Delta_f = b^2 - 4ac \in \{a^2, -q^k\}$, *for some positive integer $k$, where $q$ is an odd prime.*

*Then $g_s$ exists and $g_s \leq 35$. In particular, $g_s \leq 18$ provided that $f(x) \neq 4x^2 - 17$.*

Note that Theorem 2.1 is a combination of Theorems 5.1 and 6.1 in [46] restricted to irreducible polynomials. For reducible quadratics Harrington and Jones claimed $g_s = 17$ which can be easily disproved as the following example shows.

**Example 2.1.** Let $f_k = h_k^2$, where $h_k(x) = a + d_k x$ with $a$ being a non-zero integer coprime to $d_k$, the product of the first $k$ primes. A simple argument shows that if $s = (f_k(n))_{n=0}^{\infty}$ and $u = (h_k(n))_{n=0}^{\infty}$, then $g_s = g_u > p_k$, where $p_k$ is the $k$th prime number. As a consequence, $g_s$ is unbounded.

Similar counterexamples are easy to construct. The confusion seems to come from a wrong reference to the early work of Pillai [62] instead of that of Evans [22].

Harrington and Jones also made a conjecture on a uniform bound for every quadratic sequence. Once again, they did not exclude the reducible case, and hence we reformulate it accordingly.

**Conjecture 2.1** (Harrington and Jones [46]). *Let $f \in \mathbb{Z}[x]$ be an irreducible polynomial of degree 2 and let $s = (f(n))_{n=0}^{\infty}$. Then $g_s$ exists and $g_s \leq 35$.*

A natural question to ask is that how well-supported, either theoretically or computationally, the conjecture is. We provide more related information as the section progresses.

## 2.2 A qualitative answer to Conjecture 2.1

Now we begin to explain how we connect to, and extend, the previous results. Our aim is to prove the following statement.

**Theorem 2.2** (Sanna and Szikszai [71], 2017). *Let $f \in \mathbb{Z}[x]$ and let $s = (f(n))_{n=0}^{\infty}$. If $\deg f \leq 3$, then there exists a positive constant $k_0$ such that for every integer $k \geq k_0$ there are infinitely many non-negative integers $n$ with the property that none of*

$$f(n+1), f(n+2), \ldots, f(n+k)$$

*is coprime to all the others. In particular, both $G_s$ and $g_s$ exist.*

Note that Theorem 2.2 verifies the existence part of Conjecture 2.1 immediately. On the other hand, the result is ineffective and we do not get any upper bound, let alone a uniform one, for $G_s$. This still leaves the problem of $g_s \leq 35$ wide open.

In what follows, we give a series of preliminary results which are used in our proof of Theorem 2.2. First, we fix some notations. If not stated otherwise, we always take $p$ to a be a prime number. Further, for any $x \geq 1$ and for any set of positive integers $S$ we put

$$S(x) = S \cap [1, x].$$

We also use the Landau-Bachmann $O$ and the associated Vinogradov symbols $\ll$ and $\gg$. The dependence of the implied constants is either indicated by subscripts or explicitly stated. For instance, we write $O_f$, $\ll_f$, and $\gg_f$. Finally, the function $\nu_p(z)$ denotes the standard $p$-adic valuation of the integer $z$.

Note that our scope is not restricted to quadratic and cubic polynomials only. Whenever a result holds in generality, we state it that way.

Let

$$f(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_0$$

be a polynomial of degree $d \geq 1$ with integer coefficients $a_0, a_1, \ldots, a_d$ and define

$$\tilde{f}(x) = a_d^{2d-2} \prod_{1\leq i,j\leq d, i\neq j} (x - (\alpha_i - \alpha_j)), \tag{2.1}$$

where $\alpha_1, \alpha_2, \ldots, \alpha_d$ are all the roots of $f$ in $\mathbb{C}$. Observe that the polynomial $\tilde{f}$ is related to the resultant. Indeed, denoting by $\mathrm{Res}_x$ the resultant of polynomials with respect to $x$, one can compute it from the relation

$$\mathrm{Res}_x(f(x), f(x+y)) = a_d^2 y^k \tilde{f}(y).$$

The most important cases for our purpose correspond to degree 2 and 3 given by

$$\tilde{f}(x) = a_2^2 x^2 - \Delta_f$$

and

$$\tilde{f}(x) = (a_3^2 x^2 + 3a_1 a_3 - a_2^2)^2 x^2 - \Delta_f,$$

respectively. Here, $\Delta_f$ stands for the discriminant of $f$.

The following lemma shows that the auxiliary polynomial $\tilde{f}$ is not a random construction, it is related to the solvability of certain systems of congruences involving $f$.

**Lemma 2.1.** *Let $f \in \mathbb{Z}[x]$ be a quadratic or cubic polynomial. If there is a prime $p \nmid 6a_d$ such that $p \mid \tilde{f}(r)$ for some positive integer $r$, then the system of congruences*

$$\begin{cases} f(n) & \equiv 0 \pmod{p} \\ f(n+r) & \equiv 0 \pmod{p} \end{cases}$$

*has a positive integer solution $n$.*

*Proof.* Let $\alpha_1, \alpha_2, \ldots, \alpha_d$ be the roots of $f$ in the algebraic closure of the finite field $\mathbb{F}_p$. In view of (2.1), we can assume that $\alpha_1 - \alpha_2 = r$, where $r$ is considered as an element of $\mathbb{F}_p$. We distinguish between the cases of degree 2 and 3.

If $d = 2$, then by the Viéte's formulas we have $\alpha_1 + \alpha_2 \in \mathbb{F}_p$. Since $p > 2$, the roots $\alpha_1$ and $\alpha_2$ are in $\mathbb{F}_p$ and our claim follows.

In case $d = 3$, we split the proof. If $f$ has a root in $\mathbb{F}_p$, then it is either one of $\alpha_1$ or $\alpha_2$, and hence $\alpha_1, \alpha_2 \in \mathbb{F}_p$, or it is $\alpha_3$, in which case $\alpha_1$ and $\alpha_2$ are the roots of a quadratic polynomial in $\mathbb{F}_p$. Proceeding as in the case $d = 2$, we get $\alpha_1, \alpha_2 \in \mathbb{F}_p$. On the other hand, if $f$ is irreducible, then any Galois automorphism of $f$ over $\mathbb{F}_p$ which sends $\alpha_1$ to $\alpha_2$ also sends $\alpha_2$ to $\alpha_3$. Thus

$$r = \alpha_1 - \alpha_2 = \alpha_2 - \alpha_3$$

and

$$3\alpha_2 = (\alpha_1 + \alpha_2 + \alpha_3) - (\alpha_1 - \alpha_2) + (\alpha_2 - \alpha_3).$$

By $p > 3$, this implies $\alpha_1, \alpha_2 \in \mathbb{F}_p$ which, in turn, concludes the proof. □

A natural question to ask would be that why we cannot draw the same conclusion for polynomials of higher order. As the following example shows, the statement of Lemma 2.1 is no longer true for quartics already.

**Example 2.2.** Consider the polynomials $f_a(x) = (x-a)^4 + 1$, where $a \in \mathbb{Z}$. Since $f_0(x) = x^4 + 1$ is irreducible so are all $f_a$ in $\mathbb{Z}[x]$. Further,

$$\tilde{f}_a(x) = x^{12} + 8x^8 - 112x^4 + 256$$

for every $a$ and we have $7 \mid \tilde{f}_a(3)$. However, the congruence

$$f_a(n) \equiv 0 \pmod 7$$

does not have a solution at all. Note that similar infinite families are easy to construct.

We take a short detour to explain how we aim to apply Lemma 2.1. Suppose that there is an abundance of primes $p$ dividing some $\tilde{f}(r)$. For each $r$, we can find an $n$ so that $f(n)$ and $f(n+r)$ are both divisible by $p$. Provided that $k$ is large enough one can expect to construct sets of consecutive integers

$$n+1, n+2, \ldots, n+k$$

with the property that only a few terms among the corresponding evaluations

$$f(n+1), f(n+2), \ldots, f(n+k)$$

can be coprime to all the others. The problem lies with these exceptional terms. However, we may not actually need every $p$ and if there were really enough of them, we can hope to spare some. Thus handling the outlying terms should not cause any trouble.

The following results aim to give our idea a sufficient support and, in turn, to prove Theorem 2.2. First, we mention the strong connection between the Galois groups of $f$ and $\tilde{f}$ over $\mathbb{Q}$, since it is fundamental to some intermediate estimates.

**Lemma 2.2.** *Let $f \in \mathbb{Z}[x]$ be a non-constant polynomial. Then $f$ and $\tilde{f}$ have the same Galois group over $\mathbb{Q}$.*

*Proof.* The identity

$$\alpha_i = \frac{1}{d}\left(\sum_{j=1}^{d}(\alpha_i - \alpha_j) - \frac{a_{d-1}}{a_d}\right) \qquad (i = 1, 2, \ldots, d)$$

implies that $f$ and $\tilde{f}$ have the same splitting field over $\mathbb{Q}$, and hence the same Galois group. □

For any non-constant polynomial $f \in \mathbb{Z}[x]$ we define

$$\mathcal{P}_f = \{p : p \mid f(n) \text{ for some } n \in \mathbb{N}\}.$$

It is well-known that $\mathcal{P}_f$ has a positive relative density[13] $\delta_f$ in the set of prime numbers. More precisely, the Frobenius density theorem [79] says that

$$\delta_f = \frac{\mathrm{Fix}(G)}{|G|},$$

where $G$ is the Galois group of $f$ over $\mathbb{Q}$ and $\mathrm{Fix}(G)$ is the number of elements of $G$ which have at least one fixed point when regarded as permutations on the roots of $f$. The next lemma establishes an asymptotic formula for the number of elements of $\mathcal{P}_f(x)$ in terms of the logarithmic integral function

$$\mathrm{Li}(x) = \int\limits_2^x \frac{dt}{\log t}.$$

**Lemma 2.3.** *Let $f \in \mathbb{Z}[x]$ be a non-constant polynomial. Then,*

$$|\mathcal{P}_f(x)| = \delta_f \mathrm{Li}(x) + O_f\left(\frac{x}{\exp\left(C(f)\sqrt{\log x}\right)}\right),$$

*for all $x \geq 2$, where $C(f) > 0$ is a constant depending on $f$ only.*

*Proof.* The formula is a direct consequence of the effective version of the Chebotarev density theorem, see Theorem 3.4 in [75]. □

We also need information on the $p$-adic valuation of products consisting of consecutive values of a polynomial. We set

$$Q_k = \prod_{i=1}^{k} f(i)$$

for later use.

[13] Let $A \subset B$ be sets of positive integers. The set $A$ has relative density $\alpha$ in the set $B$, if $\lim\limits_{n\to\infty} \frac{|A(n)|}{|B(n)|} = \alpha$.

**Lemma 2.4.** *Let $f \in \mathbb{Z}[x]$ be a polynomial without a positive integer root. For any prime number $p$ and for all integers $k \geq 2$ we have*

$$\nu_p(Q_k) = \frac{t_f k}{p-1} + O_f\left(\frac{\log k}{\log p}\right),$$

*where $t_f$ is the number of roots of $f$ in $\mathbb{Q}_p$.*

*Proof.* The statement is almost identical to Theorem 1.2 in [2]. The only difference is that the error term is written as $O(\log k)$, but one can easily check that it is indeed $O_f(\log k/\log p)$. □

Now we apply both Lemma 2.3 and 2.4 to obtain a lower bound on the density of the set

$$S_k = \{p : p > k \text{ and } p \mid f(n) \text{ for some positive integer } n \leq k\}.$$

**Lemma 2.5.** *Let $f \in \mathbb{Z}[x]$ be a non-constant polynomial. Then*

$$|S_k| \gg_f (1 - \delta_f)k$$

*for all sufficiently large integers $k$.*

*Proof.* We proceed similarly to the first part of the proof of Theorem 5.1 in [28].

Observe that if $f$ has a positive integer root, then $\delta_f = 1$ and our claim follows. Hence we assume that it is not the case. In particular, $Q_k \neq 0$ for any positive integer $k$. Clearly, we may write

$$S_k = \{p : p \mid Q_k \text{ and } p > k\}.$$

Put

$$S'_k = \{p : p \mid Q_k \text{ and } p \leq k\}.$$

Taking the logarithm of $Q_k$, for every positive integer $k$ we have

$$\log |Q_k| = \sum_{p \in S_k} \nu_p(Q_k) \log p + \sum_{p \in S'_k} \nu_p(Q_k) \log p. \tag{2.2}$$

Now assume that $k \geq 2$ and apply Lemma 2.4 to obtain

$$\nu_p(Q_k) = \frac{t_f k}{p-1} + O_f\left(\frac{\log k}{\log p}\right)$$

and, as a consequence, get

$$\sum_{p \in S_k} \nu_p(Q_k) \log p \ll_f \sum_{p \in S_k} \log p \ll_f \sum_{p \in S_k} \log |f(k)| \ll_f |S_k| \log k. \quad (2.3)$$

Since $S_k'$ is a subset of the set of all prime numbers up to $k$, we can use the Prime Number Theorem, or even Chebyshev's estimates, to deduce that

$$|S_k'| \ll_f \frac{k}{\log k}.$$

Further, $S_k' \subset \mathcal{P}_f$. Thus, by Lemma 2.4 and partial summation, we get

$$\sum_{p \in S_k'} \frac{\log p}{p-1} \leq \sum_{p \in \mathcal{P}_f(k)} \frac{\log p}{p-1} = \delta_f \log k + O_f(1).$$

Therefore,

$$\sum_{p \in S_k'} \nu_p(Q_k) \log p \leq \sum_{p \in S_k'} \left(\frac{dk \log p}{p-1} + O_f(\log k)\right) \leq \delta_f dk \log k + O_f(k). \quad (2.4)$$

Applying Stirling's formula for factorials, that is

$$\ln n! = n \ln n - n + O(\ln n),$$

we obtain

$$\log |Q_k| = dk \log k + O_f(k), \quad (2.5)$$

since we may write $f(n) = O_f(n^d)$. Now putting together (2.2), (2.3), (2.4), and (2.5) culminates in

$$|S_k| \gg_f (1 - \delta_f) dk + O_f\left(\frac{k}{\log k}\right)$$

which finishes the proof. □

After this series of preliminary results we have everything at hand to give the proof of Theorem 2.2.

*Proof of Theorem 2.2.* Let $f \in \mathbb{Z}[x]$ be a polynomial of degree 2 or 3. If $f$ is reducible in $\mathbb{Z}[x]$, then there exists a linear polynomial $h \in \mathbb{Z}[x]$ such that $h(n) \mid f(n)$ for all integers $n$. With the notations $s = (f(n))_{n=0}^{\infty}$ and $u = (h(n))_{n=0}^{\infty}$, the existence of $G_s$ follows from the existence of $G_u$.

Hence we can assume that $f$ is irreducible in $\mathbb{Z}[x]$. The Galois group of $f$ over $\mathbb{Q}$ is precisely one of $S_2$, $S_3$, or $A_3$, where $S_n$ and $A_n$ stand for the symmetric and alternating groups, respectively. The Frobenius density theorem says that $\delta_f$ is 1/2, 2/3, or 1/3, accordingly. By Lemma 2.2 we know that $f$ and $\widetilde{f}$ have the same Galois group over $\mathbb{Q}$, and thus $\delta_{\tilde{f}} = \delta_f$.

In what follows, $k$ is always assumed to be sufficiently large. Define $\tilde{S}_k$ as

$$\tilde{S}_k = \{p : p > k/2 \text{ and } p \mid \tilde{f}(r) \text{ for some positive integer } r \leq k/2\}.$$

From the previous considerations, and by Lemma 2.5, we have that

$$|\tilde{S}_k| \geq c_1 k, \tag{2.6}$$

where $c_1 > 0$ is a constant depending only on $f$. Lemma 2.1 tells us that for each $p \in \tilde{S}_k$ there exist two integers $z_p^-$ and $z_p^+$ such that

$$f(z_p^-) \equiv f(z_p^+) \equiv 0 \pmod{p}$$

and $0 < z_p^+ - z_p^- \leq k/2 < p$. Since

$$\sum_{p \in \mathcal{P}_f} \frac{1}{p} = +\infty,$$

we may fix $s \geq 1$ elements $p_1 < \cdots < p_s$ of $\mathcal{P}_f$ such that

$$\prod_{i=1}^{s} \left(1 - \frac{1}{p_i}\right) < \frac{c_1}{3}. \tag{2.7}$$

By the definition of $\mathcal{P}_f$, for each $p \in \mathcal{P}_f$ we can pick an integer $z_p$ such that $f(z_p) \equiv 0 \pmod{p}$.

Let $a_1 < a_2 < \ldots < a_{k_1}$ be all the elements of $\{1, 2, \ldots, k\}$ which are not divisible by any of the primes $p_1, p_2, \ldots, p_s$, and let $b_1 < \cdots < b_{k_2}$ be all the remaining elements, so that $k = k_1 + k_2$. Applying the sieve of Erasthotenes and (2.7), we obtain

$$k_1 \leq k \prod_{i=1}^{s} \left(1 - \frac{1}{p_i}\right) + 2^s < \frac{c_1}{2} k. \tag{2.8}$$

Let $q_1 < q_2 < \cdots < q_t$ be all the elements of $\tilde{S}_k \setminus \{p_1, p_2 \ldots, p_s\}$. From (2.6) and (2.8) we get

$$t \geq c_1 k - s > \frac{c_1}{2} k > k_1.$$

As a consequence, for any $j = 1, 2, \ldots, k_1$, we can define $r_j = z_{q_j}^-$ if $a_j \leq k/2$, and $r_j = z_{q_j}^+$ if $a_j > k/2$. Finally, we assume that $k \geq 2p_s$.

At this point $p_1, p_2, \ldots, p_s$ and $q_1, q_2, \ldots, q_{k_1}$ are all pairwise distinct. Thus, by the Chinese Remainder Theorem, the system of congruences

$$\begin{cases} n \equiv z_{p_i} \pmod{p_i} & (i = 1, 2, \ldots, s) \\ n \equiv r_j - a_j \pmod{q_j} & (j = 1, 2, \ldots, k_1) \end{cases}$$

has infinitely many positive integer solutions $n$. For each $n$, none of

$$f(n+1), f(n+2), \ldots, f(n+k)$$

is relatively prime to all the others.

Indeed, take any $h \in \{1, 2, \ldots, k\}$. On one hand, if $h$ is divisible by some $p_i$, then

$$f(n+h) \equiv f(n+h \pm p_i) \equiv f(z_{p_i}) \equiv 0 \pmod{p_i}.$$

Hence

$$\gcd(f(n+h), f(n+h \pm p_i)) > 1,$$

since $h \pm p_i \in \{1, 2, \dots, k\}$ for the right choice of the sign by the assumption $k \geq 2p_s$.

On the other hand, if $h$ is not divisible by any of $p_1, p_2, \dots, p_s$, then $h = a_j$ for some $j \in \{1, 2, \dots, k_1\}$. If $a_j \leq k/2$, then

$$f(n+h) \equiv f(z_{q_j}^-) \equiv 0 \pmod{q_j},$$

and

$$f(n+h+z_{q_j}^+ - z_{q_j}^-) \equiv f(z_{q_j}^+) \equiv 0 \pmod{q_j}.$$

Thus

$$\gcd(f(n+h), f(n+h+z_{q_j}^+ - z_{q_j}^-)) > 1,$$

as $h + z_{q_j}^+ - z_{q_j}^- \in \{1, 2, \dots, k\}$. Similarly, if $a_j > k/2$, then

$$\gcd(f(n+h+z_{q_j}^- - z_{q_j}^+), f(n+h)) > 1,$$

since $h + z_{q_j}^- - z_{q_j}^+ \in \{1, 2, \dots, k\}$. This finishes the proof. □

## 2.3 Remarks and generalizations

Theorem 2.2 raises a few natural questions. While it does prove the existence of $G_s$ for every quadratic and cubic sequence it fails to address the uniform boundedness of $g_s$ in Conjecture 2.1. Further, one may ask why we limit the scope to polynomials of degree at most 3. Finally, the investigation of the more general $T$-coprimality property is missing. We briefly discuss each topic.

### Uniform boundedness of $g_s$.

In principle, the dependence of the constants on the polynomial can be made effective. Here, we avoid this for two reasons. On one hand, Conjecture 2.1 claims the existence of a uniform bound, not only an effective one. On the other hand, already a rough estimate on what we can expect seems to be far from optimal in view Theorem 2.1.

In spite of what we have just written, one can be optimistic that $g_s$ is uniformly bounded. Observe that to obtain $g_s$, we aim to find the first $k$ such that our construction in the proof of Theorem 2.2 works and we do not care whether we can continue with $k+1, k+2, \dots$ or not. The problem is closely related to the number of primitive divisors of $\tilde{f}$. A prime $p$ is said to be a *primitive divisor* of $s_n$, where $s = (s_n)_{n=0}^{\infty}$ is a sequence of integers, if $p \mid s_n$ for some positive $n$, but $p \nmid s_m$ for every positive $m < n$.

By Lemma 2.1, whenever $\tilde{f}(r)$ has a primitive prime divisor $p$, the system of congruences

$$\begin{cases} f(n) & \equiv & 0 \pmod p \\ f(n+r) & \equiv & 0 \pmod p \end{cases}$$

has a solution in $n$. If for small values of $r$ we find primitive divisors for the majority of the numbers $\tilde{f}(r)$, then the Chinese Remainder Theorem can be applied to find infinitely many $n$ and some "small" $k$ so that

$$f(n+1), f(n+2), \dots, f(n+k)$$

is "densely" covered. With some further computation we can be hopeful to find $g_s$ easily.

Recall that $\tilde{f}(x) = a^2x^2 - \Delta_f$ if $f$ is quadratic. The author is not aware of any piece of literature which addresses primitive divisors of quadratics in general. Everest and Harman [24] proved that certain infinite families of simple quadratic polynomials $f \in \mathbb{Z}[x]$ fail to have a primitive divisor infinitely often. We do not go deeper, but mention that there is an interesting connection with generalized Ramanujan-Nagell equations as well. For further content, we only refer to the papers [46, 24] and the references given therein.

### Limitations on the degree.

Observe that Lemma 2.1 is fundamental to our proof of Theorem 2.2 and its conclusion already fails in the case $f$ is quartic, see Example 2.2. However, by no means we suggest that this is the only promising approach. Indeed, one can expect the following. If $f$ is a polynomial of degree $d$, then there will be a positive density of primes $p$ for which $f$ has exactly $0, 1, \ldots,$ or $d$ roots in $\mathbb{F}_p$. In case $f$ is cubic, we were satisfied with systems of the form

$$\begin{cases} f(n) & \equiv & 0 \pmod{p} \\ f(n+r) & \equiv & 0 \pmod{p}. \end{cases}$$

This construction does not exploit when we have a third root. More precisely, we do not study the phenomenon when

$$\begin{cases} f(n) & \equiv & 0 \pmod{p} \\ f(n+r_1) & \equiv & 0 \pmod{p} \\ f(n+r_2) & \equiv & 0 \pmod{p} \end{cases}$$

has a solution $n$ for some $0 < r_1 < r_2 < p$.

It would be interesting to see how one can extend the idea of Lemma 2.1 in a way that a similar approach can work for some infinite family of irreducible quartics. One may also try to replace the lemma entirely and obtain a different proof of Theorem 2.2 that can be generalized for some higher degree polynomials as well.

### $T$-coprimality.

One may be curious not just about the limitations of Theorem 2.2, but the absence of the more general $T$-coprimality property. The proof of Theorem 2.2 is definitely not sensitive to the exclusion of divisors from a set of positive integers $T$ provided that the set of primes dividing some term in $T$ has relative density 0 in the set of prime numbers. Thus we can formulate the following result.

**Corollary 2.1** (Sanna and Szikszai, 2017). *Let $f \in \mathbb{Z}[x]$, $s = (f(n))_{n=0}^{\infty}$, and let $T$ be a subset of $\mathbb{Z}_S$, where $S$ is a set of primes having relative density $0$ in the set of prime numbers. If $\deg f \leq 3$, then $G_s(T)$, and hence $g_s(T)$, exist.*

*Proof.* Since $S$ has relative density 0 in the set of prime numbers, we can simply repeat the proof of Theorem 2.2. □

Here, we do not discuss this matter further, but suggest that a more interesting problem would be to consider what happens when the set $S$ has a positive relative density. Note that the corresponding question has been put forward in the case of consecutive integers and arithmetic progressions as well, see [37], and are yet to be answered in any measure.

# 3 Linear recurrences

In this section, we work exclusively with linear recurrences. We begin with a moderately paced introduction to the basic theory and certain arithmetic properties. After that, we proceed with the statement of our theorems and their proofs. The content there is split into several parts as each requires a somewhat different approach. Note that the results of this section can be found in the joint papers of Hajdu and the author [39, 40]. However, present formulations contain a number of improvements.

## 3.1 Basic theory and arithmetic properties

First and foremost, note that linear recurrences arise as solutions to homogeneous linear difference equations and the reader with background may find most of what we discuss here familiar. We also emphasize that every definition and result here lies at the very base of the theory and, as such, can be found in many lecture notes and books. To avoid breaking the flow of content with various references, we mention the book of Everest, van der Poorten, Shparlinski, and Ward [26] as a potential source, although our formulation does not necessarily follow any specific piece of literature.

Let $r$ be a positive integer. A sequence of integers $u = (u_n)_{n=0}^{\infty}$ is called a *linear recurrence of order $r$* if

$$u_{n+r} = a_1 u_{n+r-1} + a_2 u_{n+r-2} + \cdots + a_r u_n \tag{3.1}$$

holds for every $n \geq 0$ and with some integers $a_1, a_2, \ldots, a_r$ such that $a_r \neq 0$. Note that $r$ is minimal by the assumption $a_r \neq 0$. Otherwise, the recurrence would be of order at most $r - 1$ and our definition would not make much sense in general. The numbers $u_0, u_1, \ldots, u_{r-1}$ and $a_1, a_2, \ldots, a_r$ are said to be the *initial terms* and the *coefficients* of the sequence, respectively. Frequently, we write $u = u(a_1, a_2, \dots, a_r)$ to signal both the order and the coefficients of the relation (3.1).

There are a number of basic examples of linear recurrences of low order. For instance, $r = 1$ leads to the consideration of geometric progressions. Of course, there are less trivial ones. We mention two of the most common, and perhaps the most popular recurrences.

**Example 3.1.** The sequence of Fibonacci numbers $F = (F_n)_{n=0}^{\infty}$ has initial values $F_0 = 0$ and $F_1 = 1$ and obeys the linear recurrence relation

$$F_{n+2} = F_{n+1} + F_n \qquad (n \geq 0)$$

of order 2. The sequence of Lucas numbers $L = (L_n)_{n=0}^{\infty}$ also satisfies the above relation, but with initial terms $L_0 = 2$ and $L_1 = 1$.

Indeed, if $r = 2$, then we have a lot of noteworthy examples, like those of Mersenne, Pell, Jacobsthal, and balancing numbers.

To a linear recurrence $u = u(a_1, a_2, \dots, a_r)$ we associate the polynomial

$$x^r - a_1 x^{r-1} - \cdots - a_r. \tag{3.2}$$

Let $\alpha_1, \alpha_2, \dots, \alpha_k$ be the distinct roots of (3.2) over $\mathbb{C}$. We call (3.2) the *companion* or *characteristic polynomial* of $u$, while $\alpha_1, \alpha_2, \dots, \alpha_k$ are said to be the *characteristic roots*, or simply *roots*, of the sequence. These objects play crucial roles in the theory of linear recurrences. Let the multiplicity of $\alpha_i$ be $e_i$ $(i = 1, 2, \dots, k)$. A fundamental result states that any term of the sequence can be obtained in a closed form, namely as

$$u_n = f_1(n)\alpha_1^n + f_2(n)\alpha_2^n + \cdots + f_k(n)\alpha_k^n \qquad (n \geq 0), \tag{3.3}$$

where $f_1, f_2, \dots, f_k \in \mathbb{K}[x]$ with $\mathbb{K} = \mathbb{Q}[\alpha_1, \alpha_2, \dots, \alpha_k]$ and $\deg f_i \leq e_i - 1$ $(i = 1, 2, \dots, k)$. Here, the polynomials $f_1, f_2, \dots, f_k$ are uniquely determined by the initial terms. Technically, one may consider linear recurrences as generalized power sums of order $r$.

**Example 3.2.** The companion polynomial of the Fibonacci sequence $F = (F_n)_{n=0}^{\infty}$ is $x^2 - x - 1$ and its distinct roots are

$$\alpha = \frac{1+\sqrt{5}}{2} \qquad \text{and} \qquad \beta = \frac{1-\sqrt{5}}{2}.$$

The corresponding representation is the well-known Binet's formula

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \qquad (n \geq 0).$$

We can use the roots to describe another important property. If for some distinct $i$ and $j$ the quotient $\alpha_i/\alpha_j$ is a root of unity, then we call the sequence *degenerate*, otherwise we say that it is *non-degenerate*. Note that the case $r = 1$ is always considered as degenerate in our context. It turns out that the study of arbitrary linear recurrences reduces, in some sense, to the study of non-degenerate sequences. Namely, for any linear recurrence of order $r$, each subsequence of the form $(u_{a+nd})_{n=0}^{\infty}$ is either identically zero or non-degenerate, where $a$ is a non-negative integer and $d$ is a positive integer effectively bounded in terms of the order $r$ only. Subsequences of the above form are called *arithmetic sub-sequences* and are linear recurrences of order at most $r$ themselves.

The arithmetic of linear recurrences also attracted a vast amount of interest. Since the properties are not specific for them, our definitions concern integer sequences in general. A sequence of integers $s = (s_n)_{n=0}^{\infty}$ is said to be a *divisibility sequence*, if for any non-negative integers $m$ and $n$ with $m \mid n$ we have $s_m \mid s_n$. Whenever the more restrictive relation $\gcd(s_m, s_n) = s_{\gcd(m,n)}$ holds, we call $s$ a *strong divisibility sequence*[14]. It is obvious that the latter property implies the former. While the divisibility property is far from being automatic, it is clearly not artificial, as the following example suggests.

**Example 3.3.** Let $u = u(a_1)$ be a linear recurrence of order 1 with $u_0 \neq 0$ and $a_1 \neq 0, \pm 1$. Then $u$ is a divisibility sequence, but not

[14] This property is also known as *exact divisibility.*

a strong divisibility sequence. The sequence of Fibonacci numbers is both a divisibility and a strong divisibility sequence.

Usually, there are two natural assumptions to be taken if one works with divisibility sequences. On one hand, we take $s_1 = 1$, otherwise we may study the normalized sequence $s' = (s_n/s_1)_{n=0}^{\infty}$ instead. On the other hand, we assume that $s_0 = 0$. This probably needs a bit more explanation. Observe that $s_n \mid s_0$ for every positive integer $n$. If $s_0 \neq 0$, then all the primes dividing some term of the sequence $s$ are contained in the finite set consisting of prime factors of $s_0$. Since linear recurrences modulo a prime $p$ are ultimately periodic, this would make the arithmetic of the sequence somewhat simple, but at least, not much of interest. Further, an early result of Pólya [67] implies that if $s$ is a linear divisibility sequence of order at least 2, then $s_0 \neq 0$ can only happen if $s$ is degenerate[15].

Let us note that the problem of characterizing all linear divisibility sequences traces back to Hall and Ward [43] and has attracted a vast amount of interest. As the theorem of Bézivin, Pethő, and van der Poorten [4] suggests, such a sequence is essentially a divisor of a product of linear divisibility sequences of order 2. For more details we refer to the works [4, 61, 3] and the references given therein.

## 3.2 Results on linear divisibility sequences

After the brief overview of the basic theory, we begin the exposition of our results. We divide those concerning divisibility sequences into three parts depending on whether the order is $r = 1$, $r = 2$, or $r \geq 3$.

Note that if $u = u(a_1, a_2, \ldots, a_r)$ is a linear recurrence, then $d = \gcd(a_1, a_2, \ldots, a_r) \mid u_n$ for every $n \geq r$. Now $d \geq 2$ would imply the existence of both $g_u$ and $G_u$ and also $g_u = G_u = 2$. In view of this, we can assume that $d = 1$. While this seems to be a natural restriction

[15] Note that this is not the case if we omit the divisibility property.

when studying the standard coprimality, the case $d \geq 2$ could still prove to be an interesting one when we consider the more general $T$-coprimality. However, as the section progresses it becomes more and more evident that the consideration of such recurrences would not yield stronger results, but would involve more technicalities. Hence we avoid $d \geq 2$ under any circumstances.

**The case $r = 1$.**

Observe that if $u = u(a_1)$ is a linear recurrence of order 1, then its general term is given by $u_n = u_0 a_1^{n-1}$. Technically, we have to work with geometric progressions, a very specific situation. Recall that such sequences are considered as degenerate in our discussion. They also satisfy the divisibility property, although not necessarily the natural assumptions $u_0 = 0$ and $u_1 = 1$. We state the following simple result for sake of completeness.

**Proposition 3.1.** *Let $u = u(a_1)$ be a linear recurrence and let $T$ be a subset of $\mathbb{Z}_S$, where $S$ is any set of primes. If either $|u_0| \notin T \cup \{0\}$, or $|u_0| \in T$ and there is a prime $p \mid a_1$ such that $\nu_p(x)$ is bounded for every $x \in T$ holds, then both $g_u(T)$ and $G_u(T)$ exist and $g_u(T) = G_u(T) = 2$. In particular, $g_u$ and $G_u$ exist if and only if either $|u_0| \geq 2$, or $|u_0| = 1$ and $|a_1| \geq 2$ holds.*

*Proof.* If $|u_0| \notin T \cup \{0\}$, then $u_0$ is neither zero nor it has all of its divisors in $T$. Since the general term is $u_n = u_0 a_1^{n-1}$, we see that $u_0 \mid u_n$ for every $n \geq 0$ and the claim follows. Otherwise, all the divisors of $u_0$ are contained in $T$, but there exists a prime $p \mid a_1$ such that $\nu_p$ is bounded over the elements of $T$. Since $p^{n-1} \mid u_n$, there is a positive index $n_0$ with the property that for every $n \geq n_0$ the prime power $p^n$ does not divide any element of $T$. Putting these observations together this part of the theorem follows as well.

The specific case of $T = \{1\}$ is completely trivial. □

It is easy to see that the assumptions in Proposition 3.1 concerning the $T$-coprimality are not necessary, except $u_0 \neq 0$. However, the set $T$ would be very unnatural if it does not satisfy them. We do not explore this in more detail as there would be more pain than gain.

**The case $r = 2$.**

Specializing (3.1) for $r = 2$ and replacing the coefficients in it, we can write

$$u_{n+2} = Pu_{n+1} - Qu_n \qquad (n \geq 0)$$

for every linear recurrence $u = (u_n)_{n=0}^{\infty}$ of order 2 with some nonzero integers $P$ and $Q$. We slightly modify our notation for the dependence on $P$ and $Q$ and write $u = u(P, Q)$ instead of $u(P, -Q)$. By assumption, $P$ and $Q$ are coprime. Further, by the divisibility property, we can require that the initial terms are $u_0 = 0$ and $u_1 = 1$, otherwise the sequence would be either degenerate or it would have a fixed divisor $d \geq 2$. These together leads to a famous family of binary recurrences, the *Lucas sequences of the first kind.* If $\alpha$ and $\beta$ are the roots of the corresponding companion polynomial $x^2 - Px + Q$, then it is easy to check that the power sum representation is similar to that of the Fibonacci sequence in Example 3.2. Indeed, we have

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \tag{3.4}$$

for every $n \geq 0$, where $\alpha$ and $\beta$ are the roots of $x^2 - Px + Q$. These sequences were introduced by Lucas [56] and were studied extensively in a series of his papers [56, 57, 58]. The most important fact for us is that they satisfy more than the divisibility property, namely.

**Proposition 3.2.** *Every Lucas sequence of the first kind is a strong divisibility sequence.*

*Proof.* This fundamental result was already shown to be true by Lucas

[56]. A more recent proof can be found in the book of Ribenboim [69]. □

The arithmetic of Lucas sequences is a topic with rich literature and the corresponding results found many applications in other areas of number theory. Here, we restrict ourselves to the parts which are needed to prove the results of the section. For a comprehensive introduction to the general theory we refer to the book of Ribenboim [69].

Our first result on Lucas sequences concerns the $T$-coprimality property, in case the set $T$ has a nice structure.

**Theorem 3.1** (Hajdu and Szikszai [39], 2012). *Let $u$ be a non-degenerate Lucas sequence of the first kind and let $T$ be a subset of $\mathbb{Z}_S$, where $S$ is a finite set of primes. Then, both $g_u(T)$ and $G_u(T)$ exist and we have*

$$g_u(T) \leq G_u(T) \leq 20(2|S|+30)\log(2|S|+30).$$

In the proof, we construct a set $T'$ such that the existence of $G(T')$ can be proven and $G_u(T) \leq G(T')$. To do so we need the following result of Hajdu and Saradha [37].

**Lemma 3.1.** *Let $T$ be a set of positive integers with $1 \in T$. If there exists a constant $c_0$ such that for every $c \geq c_0$ the number of elements in $T$ not exceeding $c$ is at most $c/(10\log c)$, then $G(T)$ exists and*

$$G(T) \leq \max(425, 2c_0+1).$$

*In particular, if $T$ is finite, then $G(T)$ exists and is effectively bounded.*

*Proof.* This is a reformulation of Theorem 2.1 from [37]. Since the bound on the number of terms in $T$ is monotone increasing from some point on, the specific case of finite sets easily follows. □

The applicability of Lemma 3.1 relies on a powerful theorem of Bilu, Hanrot and Voutier [8] which gives a strong uniform bound in every non-degenerate Lucas sequence for the index of a term without a primitive divisor. The problem of completely describing terms without primitive divisors has a long history and the following result can be thought of as the coronation of the classical works on the topic by Zsigmondy [85], Carmichael [14], and later by Schinzel [73] and Stewart [80].

**Lemma 3.2.** *Let $u = u(P, Q)$ be a non-degenerate Lucas sequence of the first kind. Then $u_n$ has a primitive prime divisor if $n > 30$. Further, $u_n$ has a primitive prime divisor for every $n > 4$, $n \neq 6$, except finitely many possibilities, listed in Table 1. In particular, the number of terms without a primitive divisor is at most 10 in a single sequence.*

| $(P, Q)$ | $n$ |
|---|---|
| $(\pm 1, 1), (\pm 1, 3), (\pm 1, 4)$ | $5, 12$ |
| $(\pm 2, 11), (\pm 12, 55), (\pm 12, 377)$ | $5$ |
| $(\pm 1, 2)$ | $5, 7, 8, 12, 13, 18, 30$ |
| $(\pm 1, 5)$ | $7, 12$ |
| $(\pm 2, 7)$ | $8$ |
| $(\pm 2, 3), (\pm 5, 7)$ | $10$ |
| $(\pm 2, 15)$ | $12$ |

Table 1: Lucas sequences with terms $u_n$ without primitive divisor for $n = 5$ or some $n \geq 7$.

*Proof.* The statement is a reformulation of Theorem C from [8]. The upper bound on the number of terms without primitive prime divisors is a simple consequence in all but one case, when $(P, Q) = (\pm 1, 2)$. We check it directly. □

Now we are ready to prove our theorem.

*Proof of Theorem 3.1.* Put

$$T' = \{n : u_n \in T\}.$$

Since $u$ is non-degenerate and $S$ is finite, we can apply Lemma 3.2 and obtain that

$$|T'| \leq 10 + |S|.$$

Observe that the requirements of Lemma 3.1 are satisfied and a simple calculation leads to the upper bound

$$G(T') \leq 20(2|S| + 30)\log(2|S| + 30).$$

Now take any integer $k \geq G(T')$. Then there exist $k$ consecutive indices

$$n + 1, n + 2, \ldots, n + k$$

with the property that for every $i \in \{1, 2, \ldots, k\}$ there is an $i \neq j \in \{0, 1 \ldots, k - 1\}$ such that $\gcd(n + i, n + j) \notin T'$. By Proposition 3.2 we have that $\gcd(u_{n+i}, u_{n+j}) = u_{\gcd(n+i,n+j)}$ and the construction of $T'$ implies that $u_{\gcd(n+i,n+j)} \notin T$. This proves the existence of $G_u(T)$ and, since $G_u(T) = G(T')$, we obtain the upper bound as well. □

Note that if the size of the primes in $S$ is reasonably small, then for a given sequence we can easily construct $T'$ and improve the bound. The background is provided by the following classical result on the rank of apparition of primes dividing some term. For a prime $p$ we call the positive integer $r_p$ its *rank of apparition*, if $p$ is a primitive divisor of $u_{r_p}$.

**Proposition 3.3.** *Let $u = u(P, Q)$ be a non-degenerate Lucas sequence of the first kind and let $p$ be an odd prime. Then one of the following holds.*

*i) If $p \mid Q$, then $p \nmid u_n$ for every positive integer $n$.*

*ii) If $p \mid (P^2 + 4Q)$, then $r_p = p$.*

*iii) Otherwise, $r_p \mid p - \epsilon$ with $\epsilon = \left(\dfrac{P^2 + 4Q}{p}\right)$, where $\left(\dfrac{x}{p}\right)$ stands for the Legendre-symbol.*

*Further, if $p = 2$, then either $Q$ is even and $p$ does not divide any term, or $r_p \leq 3$.*

*Proof.* This is a well-known and fundamental property of Lucas sequences of the first kind and can be found in many works, for instance, in the book of Ribenboim [69]. □

We can use Proposition 3.3 in the following way. For every $p \in S$ we check if $p$ divides any term at all. If it does, then we bound $r_p$ with one of $p-1, p$, or $p+1$, according to how $p$ is related to the discriminant $P^2+4Q$. Listing the divisors of this possible maximal value of $r_p$ we can check the corresponding terms of $u$ one after another and find the exact value of $r_p$. In the end, we construct $T'$ explicitly, replace the estimate $|S|+10$ with the exact number of elements, and apply Lemma 3.1 to obtain a better bound on $G_u(T)$.

In Theorem 3.1, we could only bound $G_u(T)$, since there we have no specific information on $S$ except that it is finite. On the other hand, our construction made sure that $G_u(T) = G(T')$. One may expect that if $S$ is "simple", then, depending on $(P,Q)$, we do not have too many possibilities for $T'$. Choosing $S = \emptyset$, and hence $T = \{1\}$, our next theorem replaces the estimates of $g_u$ and $G_u$ with their exact values.

**Theorem 3.2** (Hajdu and Szikszai [39], 2012). *Let $u = u(P,Q)$ be a Lucas sequence of the first kind. Then $g_u$ and $G_u$ exist if and only if $(P,Q)$ is not one of $(0,\pm1)$ or $(\pm1,1)$. In case $g_u$ and $G_u$ exist, we have $g_u = G_u = 17$, except the sequences listed in Table 2.*

Note that we left the non-degeneracy assumption and this way the resulting theorem completely settles the corresponding form of Problem 1 in Lucas sequences of the first kind.

We base the proof on three lemmas. The first one shows that allowing degenerate sequences only leads to the consideration of six concrete, and in fact very simple, sequences.

| $(P,Q)$ | $g_u$ | $G_u$ |
|---|---|---|
| $(\pm 1, Q), Q \neq 1,2,3,5$ | 25 | 25 |
| $(P, P^2-1), \vert P\vert > 1$ | 43 | 43 |
| $(\pm 12, 55), (\pm 12, 377)$ | 31 | 31 |
| $(\pm 1, 3)$ | 45 | 45 |
| $(\pm 1, 5)$ | 49 | 51 |
| $(\pm 1, 2)$ | 107 | 107 |

Table 2: Values of $g_u$ and $G_u$ for exceptional Lucas sequences.

**Lemma 3.3.** *Let $u = u(P,Q)$ be a Lucas sequence of the first kind. Then $u$ is degenerate if and only if $(P,Q)$ is one of $(0,\pm 1), (\pm 1, 1)$, or $(\pm 2, 1)$.*

*Proof.* Let $\alpha$ and $\beta$ be the two roots of the companion polynomial $x^2 - Px + Q$. The sequence $u$ is degenerate precisely when the quotient $\alpha/\beta$ is a root of unity. Since $\alpha/\beta$ is either rational or a quadratic algebraic integer, it is one of $\pm 1, \pm i, \pm\epsilon$ or $\pm\epsilon^2$, where $\epsilon = (1 + i\sqrt{3})/2$. We pick up a single possibility to illustrate how to check each.

Suppose that $\alpha/\beta = -\epsilon$. Then $P = (1-\epsilon)\beta$ and $Q = -\epsilon\beta$, and hence $P^2 = Q$. By the coprimality of $P$ and $Q$, the only possibility we get is $(1,1)$, since $(-1,1)$ would give $\alpha/\beta \neq -\epsilon$. Proceeding similarly in every other case, we obtain the result. □

The second lemma lists all possible ±1 elements in Lucas sequences. In other words, with the notation of the proof of Theorem 3.1, we determine the set $T'$ under every circumstance. We do not consider degenerate sequences, since they may have infinitely many ±1 terms.

**Lemma 3.4.** *Let $u = u(P,Q)$ be a non-degenerate Lucas sequence of the first kind. The only solutions $n$ to the equation $|u_n| = 1$ are listed in Table 3, except when $n = 1$ is the only solution.*

*Proof.* By definition $u_1 = 1$ always and there is nothing to discuss.

| $(P, Q)$ | Indices $n$ with $\lvert u_n \rvert = 1$ |
|---|---|
| $(\pm 1, Q), Q \neq 1, 2, 3, 5$ | $1, 2$ |
| $(P, P^2 \pm 1), \lvert P \rvert \geq 2$ | $1, 3$ |
| $(\pm 12, 55), (\pm 12, 377)$ | $1, 5$ |
| $(\pm 1, 3)$ | $1, 2, 5$ |
| $(\pm 1, 5)$ | $1, 2, 7$ |
| $(\pm 1, 2)$ | $1, 2, 3, 5, 13$ |

Table 3: Lucas sequences of the first kind with more than one term satisfying $|u_n| = 1$.

Observe now that if $n \geq 2$ and the equation $|u_n| = 1$ has a solution, then $u_n$ cannot admit a primitive divisor. Since $u$ is non-degenerate, we can apply Lemma 3.2 and obtain $n \leq 6$, $n \neq 5$ for all, but the finitely many pairs $(P, Q)$ listed in Table 1. We can check these exceptional cases one by one and list all the solutions by direct computation of $u_n$ up to $n = 30$.

Now suppose that $n$ is one of $n = 2, 3, 4$ or 6. Writing $u_n$ in terms of $P$ and $Q$ we get $P, P^2 - Q, P^3 - 2PQ$, and $P^5 - 4P^3Q + 3PQ^2$, respectively. We are left to check finitely many equations and systems of equations, depending on whether one or more of these terms are $\pm 1$. As in the proof of Lemma 3.3, we illustrate how to proceed in one case. Since the systems are just as easy to solve as single equations, we consider the solution of $u_6 = 1$. This is equivalent to solving

$$P^5 - 4P^3Q + 3PQ^2 = 1.$$

Note that $P \mid 1$ instantly follows and necessarily we have $P = \pm 1$. But then $Q = 0$, a contradiction. We may proceed by similarly simple arguments in each case. □

Note that the description of all ±1 elements among terms of non-degenerate Lucas sequences of the first kind was a problem of Beukers [7]. In possession of the primitive prime divisor theorem, it reduces to the consideration of rather simple polynomial equations, yet we may say that Lemma 3.4 settles the problem completely.

Now we are just one step from the proof of Theorem 3.2, as we only need to compute $g(T')$ and $G(T')$ in every case.

**Lemma 3.5.** *For every set $T$ listed in the first column of Table 4, the exact values of $g(T)$ and $G(T)$ are given in the second and third columns.*

| $T$ | $g(T)$ | $G(T)$ |
|---|---|---|
| $\{1\}$ | 17 | 17 |
| $\{1,2\}$ | 25 | 25 |
| $\{1,3\}$ | 43 | 43 |
| $\{1,5\}$ | 31 | 31 |
| $\{1,2,5\}$ | 45 | 45 |
| $\{1,2,7\}$ | 49 | 51 |
| $\{1,2,3,5,13\}$ | 107 | 107 |

Table 4: The values of $g(T)$ and $G(T)$ for some particular sets $T$.

*Proof.* The cases $T = \{1\}, \{1,2\}$, and $\{1,2,3\}$ are already known, see [38]. For the remaining ones we use the algorithm invented by Hajdu and Saradha [37]. □

The proof of Theorem 3.2 becomes a simple combination of the preceding results.

*Proof of Theorem 3.2.* Suppose first that $u$ is non-degenerate. With the same notations and following the proof of Theorem 3.1 we find that $g_u(T) = g(T')$ and $G_u(T) = G_u(T')$. Applying Lemma 3.4 we can give all possible $T'$ exactly and then we use Lemma 3.5 to get $g(T')$ and $G(T')$ in each case. If $u$ is degenerate, we simply check all of the six sequences and find that these are either just sequences of zeros and

$\pm 1$ elements or the sequence of consecutive non-negative integers up to sign. □

**The case $r \geq 3$.**

So far we have worked with very specific linear divisibility sequences. In order $r = 1$, we identified them with geometric progressions and obtained simple results. In order $r = 2$, we had to deal with Lucas sequences of the first kind which satisfied considerably stronger properties than divisibility only. As we mentioned at the end of our overview on the basic theory, the characterization of linear divisibility sequences by Bézivin, Pethő, and van der Poorten [4] implies that any such a recurrence must be a termwise divisor of a product of Lucas sequences of the first kind. This alone is not enough to deduce that every divisibility sequence of order $r \geq 3$ is also a strong divisibility sequence, albeit they can be, see, for instance, [61]. On the other hand, the construction in the proof of Theorem 3.1 does not change considerably if we only work with the weaker divisibility property. Indeed, we have the following result.

**Theorem 3.3** (Hajdu and Szikszai [39], 2012)**.** *Let $u$ be a non-degenerate linear divisibility sequence of order $r \geq 3$ and let $T$ be a subset of $\mathbb{Z}_S$, where $S$ is a finite set of primes. Then $G_u(T)$, and hence $g_u(T)$, exist and*

$$g_u(T) \leq G_u(T) \leq r^{2^{8(|S|+r)}}.$$

The only auxiliary result we give is a consequence of a deep theorem of Schlickewei and Schmidt [74] concerning the number of solutions to polynomial-exponential equations. It serves as our alternative to the primitive prime divisor theorem of Bilu, Hanrot and Voutier.

**Lemma 3.6.** *Let $u = (u_n)_{n=0}^{\infty}$ be a non-degenerate linear recurrence of order $r \geq 2$ and let $p_1, p_2, \ldots, p_k$ be distinct primes. Then, the equation*

$$u_n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$$

*has at most* $r^{2^{7(k+r)}}$ *solutions in non-negative integers* $n, \alpha_1, \alpha_2, \dots, \alpha_k$.

*Proof.* Let $k$ be the number of distinct roots of the companion polynomial of $u$ in $\mathbb{C}$. Using (3.3) we can rewrite the equation as

$$\sum_{i=1}^{k} P_i(n)\alpha_i^n - p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s} = 0.$$

This way, the statement follows from Theorem 1 in [74] by a simple calculation, similarly to the proof of Theorem 2.1 in [74]. □

The proof of Theorem 3.3 is now very straightforward.

*Proof of Theorem 3.3.* Put

$$T' = \{n : u_n \in T\}.$$

From Lemma 3.6 it follows that $T'$ is finite. Indeed,

$$|T'| \leq r^{2^{7(|S|+r)}}.$$

By Lemma 3.1 we know that $G(T')$ exists and a simple calculation shows that

$$G(T') \leq r^{2^{8(|S|+r)}}.$$

Note that by the divisibility property $u_{\gcd(m,n)} \mid u_m$ and $u_{\gcd(m,n)} \mid u_n$, and hence $u_{\gcd(m,n)} \mid \gcd(u_m, u_n)$ and as in the proof of Theorem 3.1, the existence of $G(T')$ implies that of $G_u(T)$ and we have $G_u(T) \leq G(T')$. This finishes the proof. □

Observe that the main difference between Theorems 3.1 and 3.3 is that in the former, one may write $g_u(T) = g(T')$ and $G_u(T) = G(T')$, but in the latter, we only get inequality. Further, one cannot be too optimistic about the explicit construction of $T'$. We do not discuss this matter in detail.

## 3.3 Relaxation of the divisibility

In view of the previous results, it seems that for linear divisibility sequences the existence of both $g_s$ and $G_s$ is somewhat automatic, except certain degenerate cases. However, our proofs of the corresponding results relied on the divisibility property. It is natural to ask what happens if we leave this condition. In this part of the section, we show that even a very modest weakening of the arithmetic properties can cause a dramatic change in the behavior. A promising study of such a phenomenon is induced by Lucas sequences of the second kind.

A *Lucas sequence of the second kind* is a linear recurrence $v = (v_n)_{n=0}^{\infty}$ of order 2 with initial terms $v_0 = 2$ and $v_1 = P$ satisfying the relation

$$v_{n+2} = Pv_{n+1} - Qv_n \qquad (n \geq 0).$$

As in the case of Lucas sequences of the first kind, we slightly modify the notation and write $v = v(P, Q)$ instead of $v = v(P, -Q)$. Note that $P$ and $Q$ are once again assumed to be coprime. If $\alpha$ and $\beta$ are the roots of the recurrence, then

$$v_n = \alpha^n + \beta^n \tag{3.5}$$

for every $n \geq 0$. The main reason for choosing Lucas sequences of the second kind for our experiments is the following theorem of McDaniel [59]. It shows that while Lucas sequences of the second kind are not divisibility sequences, they still satisfy strong arithmetic properties.

**Proposition 3.4.** *Let $v = v(P, Q)$ be a Lucas sequence of the second kind. Then, for any $m, n \geq 1$, we have*

$$\gcd(v_m, v_n) = \begin{cases} v_{\gcd(m,n)}, & \text{if } \nu_2(m) = \nu_2(n), \\ 1 \text{ or } 2, & \text{otherwise.} \end{cases}$$

*Proof.* This is just the main result in the paper of McDaniel [59] □

Observe that, in some sense, a Lucas sequence of the second kind is "almost" a strong divisibility sequence. More precisely, Proposition 3.4 says that the subsequence of terms with odd indices behaves as a strong divisibility sequence, otherwise the common divisor is controlled by the 2-adic valuation of the terms. As our next theorem shows this somewhat slight difference, compared to strong divisibility, leads to all the possible situations regarding the existence of $g_v$ and $G_v$.

**Theorem 3.4** (Hajdu and Szikszai [41], 2015)**.** *Let $v = v(P, Q)$ be a non-degenerate Lucas sequence of the second kind.*

*i) If $P$ is even and $Q$ is odd, then both $g_v$ and $G_v$ exist and $g_v = G_v = 2$.*

*ii) If both $P$ and $Q$ are odd and coprime, then $G_v$ does not exist, but $g_v$ does and*

$$g_v = \begin{cases} 171, & \textit{if } P = \pm 1, \\ 341, & \text{if } Q = (P^2+1)/2, \\ 6, & \textit{otherwise.} \end{cases}$$

*iii) If $P$ is odd and $Q$ is even, then neither $g_v$ nor $G_v$ exists.*

We mention that the part ii) in Theorem 3.4 is not present in the paper of Hajdu and the author [41] and hence it can be considered as a new result of the thesis.

Besides Proposition 3.4 we need the following two preliminary results to prove Theorem 3.4.

**Lemma 3.7.** *Let $T = \{2^\alpha : \alpha \geq 0\}$. Then $g(T) = 86$. In particular, the following holds.*

*i) For the sequence $s = (2n+1)_{n=0}^{\infty}$ we have $g_s = 86$.*

*ii) For the sequence $s = (4n+2)_{n=0}^{\infty}$ we have $g_s(\{1, 2\}) = g_s(T) = 86$.*

*Proof.* The results on $g(T)$ follows immediately from the tables of Hajdu and Saradha [38]. Case i) is a straightforward consequence, while in case ii), we reduce to the sequence $s = (2n+1)_{n=0}^{\infty}$ first. It takes an easy argument to see how our claim follows. □

**Lemma 3.8.** *Let $v = v(P, Q)$ be a non-degenerate Lucas sequence of the second kind such that $P$ and $Q$ are odd. Then the only solutions to the equation $|v_n| = 1$ are $n = 1$, if $P = \pm 1$, and $n = 2$, if $Q = (P^2 + 1)/2$.*

*Proof.* Combining (3.4) and (3.5) we can write

$$v_n = \frac{u_{2n}}{u_n} \qquad (n \geq 1),$$

where $v$ and $u$ are Lucas sequences of the first and the second kind given by the same pair $(P, Q)$, respectively. Thus the equation $|v_n| = 1$ can be translated into the pair of equations $u_{2n} = \pm u_n$. We apply Lemma 3.2 to bound $n$ in the following way. Since $u_{2n} = \pm u_n$ is not possible whenever $u_{2n}$ admits a primitive divisor, and since both $P$ and $Q$ are odd, we are left to deal with $n \leq 5$. Now write $v_1, v_2, \ldots, v_5$ in terms of $P$ and $Q$ and proceed similarly to the proof of Lemma 3.4. □

*Proof of Theorem 3.4.* Case i) is trivial, since every term is divisible by 2.

Case iii) is also evident. Indeed, if we take any $k \geq 2$ consecutive indices

$$n+1, n+2, \ldots, n+k,$$

then there always exists one, let say $n+i$, such that $\nu_2(n+i) > \nu_2(n+j)$ for every $i \neq j \in \{1, 2, \ldots, k\}$. Further, 2 does not divide any term. By Proposition 3.4, $\gcd(v_{n+i}, v_{n+j}) = 1$ for every $i \neq j \in \{1, 2, \ldots, k\}$, and hence neither $G_v$ nor $g_v$ exists.

Finally, we consider case ii). For later use it is important to note that $2 \mid v_n$ if and only if $3 \mid n$. Also, by Proposition 3.4, $v_1 \mid v_{2n+1}$ for every $n \geq 0$.

We prove first that $G_v$ does not exist. Let $k = 2^\alpha$ for some positive integer $\alpha$ and take $k$ consecutive indices

$$n+1, n+2, \ldots, n+k.$$

Then there are two indices, say $n+i_1$ and $n+i_2$, such that $\nu_2(n+i_1) > \nu_2(n+i_2) > \nu_2(n+j)$ for every $j \in \{1,2,\ldots,k\} \setminus \{i_1,i_2\}$. By Proposition 3.4, $\gcd(v_{n+i_1}, v_{n+j}), \gcd(v_{n+i_2}, v_{n+j}) \in \{1,2\}$ for every $j \in \{1,2,\ldots,k\} \setminus \{i_1,i_2\}$ depending on whether 2 is a divisor of the terms in question. However, $|n+i_1-(n+i_2)|$ is a power of 2 and hence it is not possible that both $v_{n+i_1}$ and $v_{n+i_2}$ are divisible by 2. Thus one of them is coprime to all the others which, in turn, proves that $G_v$ does not exist.

We split the proof on $g_v$ into three parts according to the conditions listed in Theorem 3.4.

First, let $P = \pm 1$. From Lemma 3.8 it follows that the equation $|v_n| = 1$ has the single solution $n = 1$. By Lemma 3.7, we may find 86 consecutive odd indices

$$n+1, n+3, \ldots, n+171$$

so that none of them is coprime to all the others. By Proposition 3.4, the corresponding terms

$$v_{n+1}, v_{n+3}, \ldots, v_{171}$$

also satisfy this. According to the tables in [38], we may also choose $n$ in a way that among

$$n+1, n+2, \ldots, n+171$$

we have $3 \mid n+84$ and $\nu_2(n+84) > \nu_2(n+i)$ for every $i \in \{1,2,\ldots,171\} \setminus \{84\}$. Observe that for every even index $n+2i$ we can find another even index $n+2j$, where $i,j \in \{1,2,\ldots,85\} \setminus \{42\}$ and $i \neq j$, with the property that $\nu_2(n+2i) = \nu_2(n+2j) \geq 1$. Further, $3 \mid n+84$

implies $2 \mid v_{n+84}$. Hence none of the terms $v_{n+2i}$ can be coprime to all the others, if $i \in \{1, 2, \ldots, 85\}$. This shows that $g_v \leq 171$.

Now take $k \leq 170$ consecutive terms, let say

$$v_{n+1}, v_{n+2}, \ldots, v_{n+k}.$$

In particular, we only have at most 85 among them with odd indices. We may use Lemma 3.7 once more and find that one of the odd indices, let say $n + i$, is coprime to all the others. Hence, by Proposition 3.4, the corresponding term $v_{n+i}$ is coprime to all the other terms with odd indices. Suppose now that $v_{n+i}$ is not coprime to some term with an even index. It is possible if $v_{n+i}$ is even, that is, $3 \mid n + i$. This means that there can be no other odd index which is divisible by 3, otherwise $k \geq 171$, a contradiction. Thus $k$ is at most 11. Checking every $2 \leq k \leq 11$ by direct computation we find that one of the terms is always coprime to the others. Hence $g_v = 171$.

Consider now the case $Q = (P^2 + 1)/2$. From Lemma 3.8 it follows that the equation $|v_n| = 1$ has the single solution $n = 2$. In particular, $v_1 = P \neq \pm 1$ divides every term with an odd index. Now take 86 indices

$$n + 2, n + 6, \ldots, n + 342$$

so that each of them is divisible by 2, but none of them by 4. By Lemma 3.7, for each $n + (4i - 2)$ we can find an $n + (4j - 2)$ , where $i, j \in \{1, 2, \ldots, 86\}$ and $i \neq j$, with the property that $\gcd(n + (4i - 2), n + (4j - 2))$ is divisible by an odd prime $p$. As a consequence, $1 \neq v_p \mid \gcd(v_{n+(4i-2)}, v_{n+(4j-2)}) = v_{\gcd(n+(4i-2),n+(4j-2))}$. Once again, by the tables in [38], we may choose $n$ so that $\nu_2(n + 174) > \nu_2(n + s)$, where $s \in \{2, 3, \ldots, 342\} \setminus \{174\}$ and $3 \mid n + 174$. It is now straightforward why none of

$$v_{n+2}, v_{n+3}, \ldots, v_{n+342}$$

can be coprime to all the others. Indeed, $3 \mid n + 174$ so $v_{n+174}$ is divisible by 2. Further, every $v_{n+i}$ with an odd index is divisible by

$P \neq \pm 1$. Finally, by construction, for every even index $n+i$ there is a distinct even index $n+j$ such that either $\nu_2(n+i) = \nu_2(n+j) > 1$ or $\nu_2(n+i) = \nu_2(n+j) = 1$, but both $n+i$ and $n+j$ are divisible by the same odd prime $p \neq 3$. Hence $g_v \leq 341$.

The proof of $g_v \geq 341$ goes the same way as in the previous case. Namely, take at most 340 consecutive indices. Then there can be at most 85 among them of the form $4t+2$. By Lemma 3.7, one of them, say $n$, does not have any odd common factor with the others. Thus if $v_n$ is not coprime to all the others, then $2 \mid v_n$ and hence $3 \mid n$. But then there can be at most 24 consecutive terms, otherwise it would contradict the choice of $n$. We can check each case by direct computation and find that in every set of at most 24 consecutive terms one is always coprime to the others. Hence $g_v = 341$.

If neither $P \pm 1$ nor $Q = (P^2+1)/2$, then from Lemma 3.8 we get that there are no solutions to the equation $|v_n| = 1$. In particular, $v_1 = P \neq \pm 1$ and by Proposition 3.4, $P \mid v_{2n+1}$ for every $n \geq 0$. Without losing generality we may choose $n$ so that among

$$n+1, n+2, \ldots, n+6$$

both $3 \mid n+4$ and $\nu_2(n+4) > \nu_2(n+i)$ are satisfied for every $i \in \{1,2,3,5,6\}$. Since $3 \mid n+1$ and $\nu_2(n+2) = \nu_2(n+6) = 1$. we find that $\gcd(v_{n+4}, v_{n+1}) = 2$ and $\gcd(v_{n+2}, v_{n+6}) = v_2 \geq 2$. Finally, every term of odd index is divisible by $P$, and hence none of

$$v_{n+1}, v_{n+2}, \ldots, v_{n+6}$$

is coprime to all the others. This proves that $g_v \leq 6$. The fact that $g_v \geq 6$ follows from a simple computation for the cases of $k = 2, 3, 4,$ and 5. □

## 3.4 Further results and open problems

As the final thoughts in the section, we briefly discuss some connected results and problems arising from further relaxations of the divisibility property.

**Lehmer sequences.**

A sequence of integers $\tilde{u} = (\tilde{u}_n)_{n=0}^{\infty}$ is said to be a *Lehmer sequence of the first kind*, if it satisfies the fourth-order linear recurrence relation

$$\tilde{u}_{n+4} = (P - 2Q)\tilde{u}_{n+2} - Q^2\tilde{u}_n \qquad (n \geq 0)$$

with initial terms $\tilde{u}_0 = 0, \tilde{u}_1 = \tilde{u}_2 = 1$ and $\tilde{u}_3 = P - Q$. These sequences were introduced by Lehmer [54] and are intimately related to Lucas sequences of the first kind. Indeed, if we write its terms in the form (3.3), then we obtain

$$\tilde{u}_n = \begin{cases} \dfrac{\alpha^n - \beta^n}{\alpha - \beta} & \text{if } n \text{ is odd,} \\ \dfrac{\alpha^n - \beta^n}{\alpha^2 - \beta^2} & \text{otherwise.} \end{cases}$$

Here, $\alpha$ and $\beta$ are the distinct roots of the companion polynomial of the recurrence, but, since both are double roots, we can think of them as roots of the polynomial

$$x^2 - \sqrt{P}x + Q.$$

Two important facts about non-degenerate Lehmer sequences of the first kind are that they satisfy both the strong divisibility property and the primitive prime divisor theorem of Bilu, Hanrot, and Voutier [8], albeit the latter holds with slightly more restrictions on the indices and the exceptional sequences. In view of this, one would expect that the analogues of Theorem 3.1 and 3.2 can be replicated for them. Here, we only emphasize that this is the case indeed and do not state the results explicitly. Instead, we refer to the joint paper of Hajdu and the author [39], where such sequences are addressed in detail.

We note that there are also *Lehmer sequences of the second kind.* These are also fourth-order linear recurrences and share a similarly close bond with Lucas sequences of the second kind as it is between Lucas and Lehmer sequences of the first kind. Now it is no surprise that the statement of Proposition 3.4 extends to them without major changes. Once again, we do not go into details and for the related results, we refer to another work of Hajdu and the author [41].

**Open problems.**

Suppose that $u$ is a linear recurrence of order 2. From the results of the section it is clear what happens if $u$ is a Lucas sequence. The same can be said about any shifts[16] of such sequences. However, for other binary recurrences we did not study either of $g_u$ or $G_u$. Indeed, we are not aware of any example for which the questions of existence or boundedness were addressed to any extent. Hence for future work we pose two problems. In what follows, we may exclude degenerate sequences.

**Problem 2.** Find a non-trivial example of a linear recurrence $u$ of order 2 such that it is not a Lucas sequence, nor its shift, for which the existence of $g_u$ and $G_u$ can be proved or disproved.

By non-trivial we mean a sequence without an eventual fixed divisor. For instance, we exclude the recurrence $u = (u_n)_{n=0}^{\infty}$ given initial terms $u_0 = 5$, $u_1 = 1$ and the relation

$$u_{n+2} = 5u_{n+1} + u_n \qquad (n \geq 0).$$

It is easy to check that apart from $u_1$ every term of $u$ is divisible by 5 and the study of $g_u$ and $G_u$ is rather pointless.

We also pose a more serious problem.

**Problem 3.** For linear recurrences of order 2 find necessary and sufficient conditions on the existence of $g_u$ and $G_u$.

[16] By shift we mean that for some fixed positive integer $k$ and some Lucas sequence of either kind $\hat{u} = (\hat{u}_n)_{n=0}^{\infty}$, we have $u = (\hat{u}_{n+k})_{n=0}^{\infty}$.

Note that from the previous example it is clear for linear recurrences of order 2, the divisibility property is not necessary, even if that sequence is very specific. Except this observation we do not get into details concerning the problem, but mention that for linear recurrences without strong arithmetic properties, like the divisibility, similar questions can be asked.

# 4 Elliptic divisibility sequences

We can draw the following picture from the preceding section. If $u$ is a non-degenerate linear divisibility sequence, then both $g_u$ and $G_u$ exist and are effectively bounded. On the other hand, if the divisibility property is weakened, then we may lose the existence of not only $G_u$ but also that of $g_u$. A reasonable next step would be to drop the linearity of the recurrence and keep the strong arithmetic intact. For this end, we consider the important family of elliptic divisibility sequences. The results of this section can be found in a paper of Hajdu and the author [40].

## 4.1 Elliptic curves and a related recurrence

The definition of elliptic divisibility sequences assumes familiarity with the basic theory of elliptic curves over $\mathbb{Q}$. A nice introduction can be found, for instance, in the book of Washington [84]. Once again, we do not refer to various pieces of literature, but instead point the reader toward this book.

By an *elliptic curve* over $\mathbb{Q}$, we understand an equation of the form

$$E: \qquad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{4.1}$$

where $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Q}$. The set of rational solutions to (4.1), together with a symbol $\infty$, that is,

$$E(\mathbb{Q}) = \{(x, y) \in \mathbb{Q}^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\infty\}$$

is called the *set of rational points* on $E$. The symbol $\infty$ is said to be the *point at infinity*. Note that we consider the points in the affine space $\mathbb{Q}^2$ instead of the two-dimensional projective space $\mathbb{P}^2(\mathbb{Q})$, where the point at infinity would make sense immediately. The reason is that the affine representation is sufficient for our discussion. Hence we treat $\infty$ as a symbol devoid of any representation as some element of $\mathbb{Q}^2$ and clarify its relation to other rational points whenever it becomes necessary.

It is well-known that there is a standard additive operation on the points which turns $E(\mathbb{Q})$ into an Abelian group. Let us call it simply the *addition of points*. The famous theorem of Mordell states that $E(\mathbb{Q})$ is finitely generated, that is, has the representation

$$E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus T$$

for some non-negative integer $r$ and a finite group $T$. The number $r$ is said to be the *rank* of the curve. The group $T$ is isomorphic to the group of *torsion points*, points of finite order with respect to the addition in $E(\mathbb{Q})$.

Now let $P \in E(\mathbb{Q})$ be any rational point. By the $n$ times *multiple* $nP$ we understand the $n$th-fold addition of $P$. We may write these in the form

$$nP = \left(\frac{A_n}{B_n^2}, \frac{C_n}{B_n^3}\right) \qquad (n \geq 1),$$

where $A_n, B_n, C_n \in \mathbb{Z}$ and $\gcd(A_nC_n, B_n) = 1$. Taking $B_0$ to be 0, the sequence $B = (B_n)_{n=0}^{\infty}$ is said to be an *elliptic divisibility sequence.* The choice $B_0 = 0$ is natural, since $0P$ is understood as $\infty$ and in the affine representation $\infty$ can be thought of as division by zero. Note that $B$ depends both on the point and the equation chosen for the elliptic curve. For this reason we usually signal the dependence by writing $B = B(E, P)$.

Throughout the section we assume that $P$ is a point of infinite order in $E(\mathbb{Q})$. Otherwise, $P$ would belong to the torsion group and the multiples of $P$ would form a periodic sequence. The famous theorem of Mazur restricts the length of the period to at most 12. Such sequences have a very simple arithmetic and we do not concern ourselves with their study[17].

[17] One may think of this phenomenon as the analogue of degeneracy in case of

The most important property of elliptic divisibility sequences for our purposes is given in the following proposition. This also justifies us choosing them for study.

**Proposition 4.1.** *Every elliptic divisibility sequence is a strong divisibility sequence.*

*Proof.* This is a fundamental result which, for instance, is direct consequence of formula (13) on the $p$-adic valuation of multiples of points in [76]. □

As a closure to the introductory part, we note that the original definition of elliptic divisibility sequences calls upon a bilinear recurrence relation of the form

$$B_{m+n}B_{m-n} = B_{m+1}B_{m-1}B_n^2 - B_{n+1}B_{n-1}B_m^2 \qquad (m \geq n \geq 0).$$

This formulation goes back to Ward [83] who was the first to study such recurrences extensively. In fact, he already showed the connection with elliptic curves. Here, we emphasize that our definition of elliptic divisibility sequences coincide with that of Ward's up to sign and has become more standard during the past decades. Finally, we note that a comprehensive study of elliptic divisibility sequences, both as bilinear recurrences and multiples of points on elliptic curves, can be found in the theses of Shipsey [77] and Swart [82].

## 4.2 An "expected" result

Our one and only result in this section shows that replacing linear recurrences with elliptic divisibility sequences in Theorem 3.3 does not change the conclusion.

linear recurrences.

**Theorem 4.1** (Hajdu and Szikszai [40], 2014)**.** *Let $B = B(E, P)$ be an elliptic divisibility sequence and let $T$ be a subset of $\mathbb{Z}_S$, where $S$ is a finite set of primes. Then both $g_B(T)$ and $G_B(T)$ exist and*

$$g_B(T) \leq G_B(T) \leq C(E, |S|, \max S),$$

*where $C(E, |S|, \max S)$ is an effective constant depending on $E$, $|S|$ and $\max S$ only. In particular, $g_u$ and $G_u$ exist and are effectively bounded in terms of $E$ only.*

Note that the divisibility property itself was not enough to obtain either Theorem 3.1 or Theorem 3.3 as we also needed control over the number of terms falling into $\mathbb{Z}_S$. For this end, we use the following result.

**Lemma 4.1.** *Let $S$ be a finite set of primes. Then the number of elements of $\mathbb{Z}_S$ in the elliptic divisibility sequence $B = B(E, P)$ is finite and effectively bounded in terms of $E$, $|S|$ and $\max S$ only. In particular, the number of $\pm 1$ terms in $B$ is effectively bounded in terms of $E$ only.*

*Proof.* The lemma is a simple consequence of Theorems 1 and 2 in [35]. □

Observe that, like in Theorem 4.1, the upper bound is not given explicitly despite its effective nature. We already indicate that the reasons are closely related, but we only discuss this matter after the proof.

*Proof of Theorem 4.1.* Put

$$T' = \{n : B_n \in T\}.$$

By Lemma 4.1, $T'$ is finite and the number of terms is effectively bounded. Indeed, we have

$$|T'| \leq C_1(E, |S|, \max S).$$

Lemma 3.1 tells us that both $G(T')$ and $g(T')$ exists and can be effectively bounded as

$$g(T') \leq G(T') \leq C(E, |S|, \max S).$$

The existence and effective boundedness of $g_B(T)$ and $G_B(T)$ are verified by the same argument as in the proof of Theorem 3.1, the only difference is that we refer to Proposition 4.1 instead of 3.2 regarding the strong divisibility property. □

Note that in the paper of Hajdu and Herendi [35], the bounds concern the size of the solutions to elliptic equations of the form (4.1) rather than the number of solutions. Neverthless, they do give an upper bound on the latter. Since these bounds are complex, we chose to omit them. The main point is that an effective upper bound can be obtained. Let us mention that the study of the number of integral and $S$-integral points on elliptic curves is a very active field of arithmetic geometry and opening up on the connection between our bounds and the related results would divert from the content considerably. For recent research we refer to the yet unpublished paper of Alpoge [1] and the references given therein.

Now another important point is that whether we can find better, or at least alternative, estimates on the size of $T'$ or not. In the case of Lucas sequences of the first kind, this was obtained with the help of the theorem of Bilu, Hanrot and Voutier. Indeed, a deep theorem of Silverman [76] states that in a single elliptic divisibility sequence, only finitely many terms can fail to have a primitive prime divisor. However, this result is ineffective and cannot be applied in place of Lemma 4.1. Neverthless, if we restrict ourselves to curves having integral $j$-invariant or we specify (4.1) and, more importantly, the point, then we can certainly do better. For further information we refer to the papers [25, 48, 49, 50].

# 5 Diophantine applications

Now we arrive at the final section of the thesis. The topic we discuss here can be considered as a standalone, since it concerns the solution of a Diophantine equation. However, it shares a close bond with the previous three. In what follows, we make this connection clear.

## 5.1 Powers in products and $g_s$

Recall that there is a deep Diophantine interest in Problem 1. Namely, Pillai himself was motivated by the famous folklore conjecture that the product of at least two consecutive positive integers is never a perfect power. This translates to the consideration of the equation

$$n(n+1)\dots(n+k-1) = y^{\ell} \tag{5.1}$$

in unknown positive integers $n, y, k$, and $\ell$ with $k, l \geq 2$. Pillai [63] was able to prove that there is no solution if $k \leq 16$. Observe that the limitation on $k$ is not a random choice. Indeed, $k < g = 17$ and as a consequence, one of

$$n+1, n+2, \dots, n+k$$

has to be coprime to all the others. Hence it is a perfect power itself which is, in some sense, a serious restriction and something which one can make use of. Of course, this observation alone is not enough to settle the problem.

The idea naturally extends to products of consecutive terms of a sequence of integers $s = (s_n)_{n=0}^{\infty}$. Consider the equation

$$s_{n+1}s_{n+2}\dots s_{n+k} = y^{\ell} \tag{5.2}$$

with the same conditions as (5.1). Recall that the specific case (5.1) of (5.2) was completely solved by Erdős and Selfridge [21]. However, besides the case of consecutive positive integers, other variants of (5.2) have also been studied in detail.

A long-standing conjecture[18] that if $s$ is an arithmetic progression with coprime initial term and difference, then there exists a constant $k_0$ such that (5.2) has no solutions provided that $k \geq k_0$. In a recent publication, Bennett and Siksek [6] proved a weaker version of this conjecture. For a nice and comprehensive survey of the history of the problem and related results we refer to the introduction of their paper as well as to that of Győry, Hajdu, and Pintér [34]. On the other hand, for sequences corresponding to higher order polynomials, the equation has not yet been studied extensively, see Cilleruelo [16] and He, Togbé, and Yang [47] for partial results.

Variants of (5.2) for linear recurrences have also been considered. Luca and Shorey [55] chose $s$ to be a Lucas sequence of the first or second kind and obtained effective finiteness result on the size of the solutions. They also gave complete solution in case $s$ is the sequence of Fibonacci numbers. For related progress in this direction we refer to the recent paper of Bravo, Das, Guzmán, and Laishram [13] and the references given therein.

In the above mentioned works, the arithmetic of the sequences usually plays an important role. However, it is a rather common phenomenon that the authors only partially exploit the connection with $g_s$ or do not at all. We have seen that $g_s$ may or may not exist. In any case, one is able to derive simple, yet important consequences under certain conditions. We given an example of this phenomenon.

Suppose that the set

$$\mathcal{P}(s) = \{n : s_n \text{ is a perfect power}\}$$

is finite. If $g_s$ exists, then it is clear that there can be only finitely many solutions with $k < g_s$. Otherwise, if $g_s$ does not exist, this claim

[18] This conjecture is widely attributed to Erdős, see, for instance, [78].

extends to any $k$. Indeed, if $\mathcal{P}(s)$ is given explicitly, then we may turn this knowledge into an effective method to solve the corresponding variant of (5.2) completely.

The second part of the section picks up a concrete example of (5.2) for which the ideas we just briefly discussed find applications.

## 5.2 A finiteness result

Let $B = B(E, P) = (B_n)_{n=0}^{\infty}$ be an elliptic divisibility sequence and consider the equation

$$B_n B_{n+d} \dots B_{n+(k-1)d} = y^{\ell} \tag{5.3}$$

in unknown positive integers $n, d, k, y$, and $\ell$ with $\gcd(m, d) = 1$, where $k, \ell \geq 2$. Note that the indices in (5.3) come from an arithmetic progression and in this sense the equation is more general than (5.2).

Now assume that $B_1 = 1$. Since $B$ is dependent on both the equation of the curve $E$ and the generator point $P$, this seems a serious limitation. However, as the section progresses, we discuss why it is merely a technical condition. For later use we set

$$\mathcal{P}_{\ell}(B) = \{n : B_n \text{ is an } \ell\text{th power}\}.$$

By a theorem of Everest, Reynolds, and Stevens [27], we know that $\mathcal{P}_{\ell}(B)$ is finite for every $\ell \geq 2$. Indeed, Reynolds [68] explained how to effectively determine it if either $E$ or $P$ satisfies some additional conditions.

Let us also put

$$N_{\ell} = |\mathcal{P}_{\ell}(B)| \qquad \text{and} \qquad M_{\ell} = \max_{n \in \mathcal{P}_{\ell}(B)} n$$

for easier reference. The aim of this section is to prove the following result.

**Theorem 5.1** (Hajdu, Laishram, and Szikszai [36], 2016)**.** *Let $\ell \geq 2$ be fixed. Then* (5.3) *has only finitely many solutions. Further, if $(n, d, k, y)$ is a solution, then*

$$\max(n, d, k, y) \leq C_2(N_\ell, M_\ell),$$

*where $C_2$ is an effectively computable constant depending on $N_\ell$ and $M_\ell$ only. In particular, if $\mathcal{P}_\ell(B)$ is given explicitly, then all the solutions to* (5.3) *can be effectively determined.*

What follows is devoted entirely to the proof of Theorem 5.1. Like in the preceding sections, we break it down to a series of auxiliary results.

Recall some of the notations we already used. For instance, $p$ is a prime if not stated otherwise, $\nu_p(z)$ is the standard $p$-adic valuation of the integer $z$, and $r_p$ is the rank of apparition of the prime $p$ in $B$ if it exists. In addition, we let $P(z)$ denote the greatest prime factor of the non-zero integer $z$ with the convention that $P(1) = 1$.

According to Proposition 4.1, every elliptic divisibility sequence has the strong divisibility property. Our first lemma gives further insight into the arithmetic properties.

**Lemma 5.1.** *Let $B = (B_n)_{n=0}^{\infty}$ be an elliptic divisibility sequence. Then we have the following properties.*

*i) If $p \mid B_n$, then $\nu_p(B_n) = \nu_p\left(\dfrac{n}{r_p}\right) + \nu_p(B_{r_p})$ for every $n \geq 1$.*

*ii) For every prime $p$ we have $r_p \leq p + 1 + 2\sqrt{p}$.*

*iii) If $m \mid n$, then $\gcd\left(B_m, \dfrac{B_n}{B_m}\right) \Big| \dfrac{n}{m}$ for every $n \geq m > 0$.*

*Proof.* Case i) is a reformulation of (13) in [76] and ii) is a simple consequence of Hasse's theorem on the number of points on elliptic curves over finite fields, see, for instance, [77]. In case iii), we can apply i) to get

$$\nu_p\left(\frac{B_n}{B_m}\right) = \nu_p\left(\frac{n}{r_p}\right) + \nu_p(B_{r_p}) - \nu_p\left(\frac{m}{r_p}\right) - \nu_p(B_{r_p}) = \nu_p\left(\frac{n}{m}\right).$$

Hence

$$\min\left(\nu_p(B_m), \nu_p\left(\frac{B_n}{B_m}\right)\right) \leq \nu_p\left(\frac{n}{m}\right)$$

and our claim follows. □

With the help of Lemma 5.1 we can obtain further information on the arithmetic relations among the terms

$$B_n, B_{n+d}, \ldots, B_{n+(k-1)d}.$$

Write $n + id = a_i x_i$ for every $0 \leq i \leq k-1$ such that $P(a_i) \leq k$ and

$$\gcd\left(x_i, \prod_{p\leq k} p\right) = 1.$$

Note that $B_{x_i} \mid B_{n+id}$ by the divisibility property. The following result explains how one can "control" the common divisor of $B_{x_i}$ and the other terms of the product.

**Lemma 5.2.** *Let* $0 \leq i < k$. *Then*

$$\gcd\left(B_{x_i}, \prod_{j\neq i} B_{n+jd}\right) = 1 \quad \text{and} \quad \gcd\left(B_{x_i}, \frac{B_{n+id}}{B_{x_i}}\right)\Big| \, a_i.$$

*Proof.* If $x_i = 1$, then the assertion follows from $B_1 = 1$. Hence assume that $x_i \neq 1$. For for every $p \mid x_i$ we have $p > k$. Since a prime greater than $k$ can divide at most one of

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

for every $j \neq i$ we get $\gcd(x_i, n+jd) = 1$. By property i) in Lemma 5.1, the first formula follows. The second part of the statement is an immediate consequence of iii) in Lemma 5.1. □

We stop for a moment and prove Theorem 5.1 for small values of $k$. Indeed, the following proposition explains how one can relate the quantity $g$ to the solution of (5.3).

**Proposition 5.1.** *Let $(n, d, k, y)$ be a solution to (5.3) with $k \leq 48$. Then we have $\max(n, d) \leq cM_\ell$, where $c = 1$ for $k \leq 16$, $c = 2$ for $17 \leq k \leq 24$, and $c = 3$ for $25 \leq k \leq 48$.*

*Proof.* Recall that $g = 17$ and, by the tables in [38], $g(T) = 25$ or 49 depending on whether $T = \{1, 2\}$ or $T = \{1, 2, 3\}$, respectively. Further, note that if $s$ is an arithmetic progression, then $g_s \geq g$ provided that the initial term and the difference are coprime. In what follows, $i$ and $j$ are always elements of the set $\{0, 1, \ldots, k-1\}$.

We consider first the case $k < g = 17$. Among the indices

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

we can find one, let say $n+id$, which is coprime to all the others. From Proposition 4.1 it follows that $\gcd(B_{n+id}, B_{n+jd}) = B_1 = 1$ for every $i \neq j$. Hence $n + id \in \mathcal{P}_\ell(B)$. If $i > 0$, then $n + d \leq n + id \leq M_\ell$ and the claim follows. Otherwise, we can repeat the same argument for the other $k - 1$ consecutive indices.

In the second case, we let $k < g(\{1, 2\}) = 25$. Thus one of

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

let say $n + id$ as before, satisfies that $\gcd(n + id, n + jd) \leq 2$ for every $i \neq j$. Once more we can assume $i > 0$. The case when $\gcd(n+id, n+jd) = 1$ goes the same way as the previous one. Hence suppose that $\gcd(n+id, n+jd) = 2$ and put $a_i = 2t$. Observe that $\gcd(t, n+jd) = 1$ for all $i \neq j$. We can rewrite (5.3) as

$$B_{tx_i} \frac{B_{n+id}}{B_{tx_i}} \prod_{j \neq i} B_{n+jd} = y^\ell. \tag{5.4}$$

On one hand, $\gcd(tx_i, n+jd) = 1$ and $\gcd(B_{tx_i}, B_{n+jd}) = B_1 = 1$ follows. On the other hand, by part iii) of Lemma 5.1, we have

$$\gcd\left(B_{tx_i}, \frac{B_{n+id}}{B_{tx_i}}\right)\Bigg| \, 2.$$

If $2 \mid B_{tx_i}$, then $r_2 \mid tx_i$. According to ii) of Lemma 5.1, $r_2 \leq 5$ and this implies that $r_2 \mid t$. However, this would contradict the choice of $n+id$. Thus $B_{tx_i}$ is odd, and hence coprime to $B_{n+id}/B_{tx_i}$. By (5.4), $tx_i \in \mathcal{P}_\ell(B)$ and we get $\max(m,d) \leq m+id = 2tx_i \leq 2M_\ell$, proving our claim also in this case.

Finally, let $k < g(\{1,2,3\}) = 49$. As before, we can find an $n+id$ such that $\gcd(n+id, n+jd) \leq 3$ for every $j \neq i$. Obviously, the only interesting case is when $\gcd(n+id, n+jd) = 3$. In particular, $3 \mid a_i$, and we can write $a_i = 3t$. Following the argument of the previous case, we finish the proof. □

Based on the proof of Proposition 5.1 one may expect that if $g(D) = g(\{1,2,\ldots,D\})$ is given, then for any solution $(n,d,k,y)$ of (5.3) with $k < g(D)$ we get $\max(n,d) \leq DM_\ell$. This idea would rely on a strong enough lower bound on $g(D)$ so that we can really get contradiction by looking at upper bound on the rank of apparition. The author is not aware of any such result in the literature, however it seems rather feasible to obtain one. Nevertheless, this approach only works for fixed $k$ and we still need other means of proving Theorem 5.1.

For later use, we set $k' = k + 1 + 2\sqrt{k}$ and put

$$\begin{aligned} W_1 &= \{i \,:\, \exists p \mid (m+id) \text{ with } p > k\}, \\ W_2 &= \{i \in W_1 \,:\, \exists p \mid (m+id) \text{ with } k < p \leq k'\}, \\ W_0 &= W_1 \setminus W_2. \end{aligned}$$

Further, we write $w_i = |W_i|$ for $i = 0,1,2$. It is obvious that $w_0 = w_1 - w_2$ and we also have

$$w_2 \leq \pi_d(k') - \pi_d(k) \leq \pi(k') - \pi(k),$$

where $\pi_d(x)$ stands for the number of primes up to $x$ which does not divide $d$. Note that $W_0$ can be thought of as the set of all primes divisors of indices which have "considerably large" prime factors. This way, the set $W_0$ is closely related to $\mathcal{P}_\ell(B)$ as the next lemma shows.

**Lemma 5.3.** *Let $(n, d, k, y)$ be a solution to* (5.3)*. Then $x_i \in \mathcal{P}_\ell(B)$ for each $i \in W_0$. In particular, we have $w_0 \leq N_\ell$ and also $k < M_\ell$ if $w_0 > 0$.*

*Proof.* Observe that for $i \in W_0$ the numbers $x_i$ are distinct and for every prime divisor $q \mid x_i$ we have $q > k'$. Let $i \in W_0$ and let $p$ be a prime divisor of $a_i$. Then, by ii) of Lemma 5.1, $r_p \leq p + 1 + 2\sqrt{p} \leq k'$. Thus $r_p \nmid x_i$, and hence $p \nmid B_{x_i}$ as well. From Lemma 5.2 we get $\gcd(B_{x_i}, B_{m+id}/B_{x_i}) = 1$ and it follows that $x_i \in \mathcal{P}_\ell(B)$. Since the $x_i$-s are distinct, we obtain $w_0 \leq N_\ell$ proving the first part of the statement. The second part follows simply from the inequality $k < x_i \leq M_\ell$, finishing the proof. □

In what follows, we establish lower bounds for $w_0$ in terms of $k$. Our aim is to get an upper bound on the size of $k$, since in view of the previous lemma we have $w_0 \leq N_\ell$. First, we need some intermediate results concerning the number of terms $W(\Delta)$ in the product

$$\Delta = m(m + d) \ldots (m + (k - 1))d$$

having a prime factor larger than $k$.

**Lemma 5.4.** *Let $k \geq 31$. Then we have the following.*

*i)* $W(\Delta) \geq \min\left(\left\lfloor \frac{3}{4}\pi(k) \right\rfloor - 1, \pi(2k) - \pi(k) - 1\right)$ *if $d = 1$ and $m > k$.*

*ii)* $W(\Delta) > \pi(2k) - \pi_d(k) - \rho$ *if $d > 1$, where $\rho = 1$ for $d = 2$ and $\rho = 0$ otherwise.*

*Proof.* Part i) immediately follows from Corollary 1 in [52]. Although the assertion was stated for the number of distinct prime factors of $\Delta$, it is valid for $W(\Delta)$ as well. Part ii) is a simple consequence of Theorem 1 in [51]. □

We also use estimates for $\pi(x)$, due to Rosser and Schoenfeld [70].

**Lemma 5.5.** *For every $x \geq 17$ we have*

$$\frac{x}{\log x} < \pi(x) < \frac{x}{\log x}\left(1 + \frac{3}{2\log x}\right).$$

*Proof.* The upper and lower bounds are part of Theorem 1 and Corollary 1 in [70], respectively. □

The previous two lemmas can be combined to get a trivial lower bound on $w_0$.

**Lemma 5.6.** *Let $k \geq 2$ and assume that $n > k$ if $d = 1$. Then there exists an absolute constant $c > 0$ such that*

$$w_0 > \frac{ck}{\log k}.$$

*Proof.* Recall that $w_0 = w_1 - w_2$ and $w_2 \leq \pi_d(k+1+2\sqrt{k}) - \pi_d(k) \leq \pi(k+1+2\sqrt{k}) - \pi(k)$. Since $w_1 \geq W(\Delta)$, the assertion follows from Lemmas 5.4 and 5.5 by a simple calculation. □

If we put further restrictions on $n$, $d$, and $k$, we can considerably improve Lemma 5.6.

**Lemma 5.7.** *Let $k \geq 48$, and assume that $n + d \geq (k-1)^4$. Then we have*

$$w_0 \geq \frac{3(k-1)}{4} - \pi_d(k+1+2\sqrt{k}).$$

*Proof.* We follow standard arguments going back to Erdős. For each prime $p \leq k$ and $p \nmid d$, we can choose an index $i_p$ with $0 \leq i_p < k$ such that $\nu_p(n + i_p d) \geq \nu_p(n + id)$ for every $i \in \{0, 1, \ldots, k-1\}$. Put

$$I = \{i_p \ : \ p \leq k, \ p \nmid d\}$$

and write $J$ for the complement of $I \cup W_0 \cup \{0\}$ in $\{0, 1, \ldots, k-1\}$. Clearly, $|J| \geq k - w_1 - \pi_d(k) - 1$. Let

$$\Delta' = \prod_{i \in J} (n + id),$$

and observe that all prime divisors of $\Delta'$ are at most $k$ and also that $\gcd(\Delta', d) = 1$. For any $i = 0, 1, \ldots, k-1$ we have

$$\nu_p(n + id) \leq \nu_p(n + id - (n + i_p d)) \leq \nu_p(i - i_p).$$

Thus $\nu_p(\Delta') \leq \nu_p((k-1)!)$, and it follows that $\Delta' \mid (k-1)!$. Hence we get

$$(n + d)^{k - w_1 - \pi_d(k) - 1} \leq (k-1)!.$$

Using our assumption $n + d \geq (k-1)^4$, we obtain

$$w_1 \geq \frac{3(k-1)}{4} - \pi_d(k).$$

Since $w_0 = w_1 - w_2$ and $w_2 \leq \pi_d(k + 1 + 2\sqrt{k}) - \pi_d(k)$, the assertion follows. □

*Proof of Theorem 5.1.* In view of Proposition 5.1, we may assume that $k \geq 49$. We split the proof into two parts.

Suppose first that $d > 1$, or $d = 1$ and $n > k$. By Lemmas 5.3 and 5.6, $k$ is bounded in terms of $N_\ell$. In case $n + d \leq (k-1)^4$, we are done. Otherwise, Lemma 5.7 gives

$$w_0 \geq \frac{3(k-1)}{4} - \pi_d(k + 1 + 2\sqrt{k}).$$

Now apart from at most $\pi_d(k)$ indices $i$, we have that $\nu_p(a_i) \leq \nu_p((k-1)!)$. With the notation of Lemma 5.7, the exceptions are those indices $i_p$ for which $\nu_p(a_{i_p})$ is maximal. This implies that if

$$\frac{3(k-1)}{4} - \pi_d(k+1+2\sqrt{k}) - \pi_d(k) > 1, \tag{5.5}$$

then there are at least two indices $i \neq j$ such that all $a_i, a_j, x_i, x_j$ are bounded in terms of $N_\ell$ and $M_\ell$. As one of these indices, say $i$, is positive, and by $n + d \leq n + id = a_i x_i$, we obtain that $n$ and $d$ are also bounded in terms of $N_\ell$ and $M_\ell$. A simple calculation based upon Lemma 5.5 shows that (5.5) holds whenever $k \geq 62$. In fact, working with the concrete values of $\pi(x)$ function, we can get down to $k \geq 42$. Hence the theorem follows in this case.

In the second part, assume that $d = 1$ and $m \leq k$. There exists an effectively computable constant $c_3 = c_3(N_\ell) > 0$, depending only on $N_\ell$, such that if $n + k - 1 > c_3(N_\ell)$, then the open interval $\left(\frac{2}{3}(n+k-1), n+k-1\right)$ contains more than $N_\ell$ primes. Observe that, by $n \leq k$, such primes are among

$$n, n+1, \ldots, n+k-1$$

and each of them divides exactly one of these numbers. Let $q$ be any of these primes, and write $q = n+i$. By Proposition 4.1, $\gcd(B_{n+i}, B_{n+j}) = B_1 = 1$ for any $j \neq i$ with $0 \leq j < k$. Hence $n + i \in \mathcal{P}_\ell(B)$. However, since we have more than $N_\ell$ primes among $n, \ldots, n+k-1$, this yields a contradiction. Thus $n + k - 1 \leq c_3(N_\ell)$, finishing the proof. □

Recall that we assumed from the beginning that $B_1 = 1$. Now we address how one eliminates this condition. Assume that $B_1 \neq 1$ and consider the normalized sequence $B' = (B_n/B_1)_{n=0}^{\infty}$. A simple argument shows that property i) of Lemma 5.1 remains intact for $B'$. Property ii) holds for elliptic curves in general, and hence it is also valid. Now iii) follows from i) as well, and hence we can also prove Lemma 5.2. Since these are the only auxiliary results which concern the arithmetic of elliptic divisibility sequences, one may hope that the proof of Theorem 5.1 can be pulled through the same way. The only issue we left to address is the change in $\mathcal{P}_\ell(B)$. Note that $\mathcal{P}_\ell(B')$ consists essentially of terms in $B$ which are $B_1$ times multiples of an $\ell$th power. Everest, Reynolds and Stevens [27] mentions that the proof on the finiteness of $\mathcal{P}_\ell(B)$ can be modified to obtain the same conclusion for $S$-unit multiples of $\ell$th powers. This is exactly what we need in order to drop the condition $B_1 = 1$ entirely.

## 5.3 Effective enumeration: an example

Following the proof of Theorem 5.1 it is clear that both the finiteness of the solutions and the existence of an effectively computable upper bound, depending on $N_\ell$ and $M_\ell$, have been proven. In fact, if $P_\ell(B)$ is given explicitly, then with a finite, trial and error, computation we can enumerate each solution to (5.3). However, this is certainly the most undesirable way to follow. In the next example, we explain on how to proceed in a specific case and close the discussion of our results.

**Example 5.1.** Consider the elliptic curve

$$E:\ y^2 + xy = x^3 + x^2 - 7x + 5$$

and the elliptic divisibility sequence $B = (B_n)_{n=1}^{\infty}$ generated by the point $P = (2, -3)$. Reynolds [68] found that

$$B_1 = B_2 = B_3 = B_4 = B_7 = 1,\ B_{12} = 2^7$$

are perfect powers in $B$. For the sake of simplicity, assume that there are no other perfect power besides these. Then

$$\mathcal{P}_\ell(B) = \begin{cases} \{1,2,3,4,7,12\}, & \text{if } \ell = 7; \\ \{1,2,3,4,7\}, & \text{otherwise,} \end{cases}$$

and hence

$$N_\ell = \begin{cases} 6, & \text{if } \ell = 7; \\ 5, & \text{otherwise;} \end{cases} \qquad \text{and} \qquad M_\ell = \begin{cases} 12, & \text{if } \ell = 7; \\ 7, & \text{otherwise.} \end{cases}$$

Following the proof of Lemma 5.6, by a simple calculation, we get $w_0 \geq 1$ for $k \geq 49$. However, in view of Lemma 5.3, we find that $k < M_\ell \leq 12$, a contradiction.

Hence we conclude that $k \leq 48$. By Proposition 5.1, we get $m + d \leq 3M_\ell \leq 36$. As $m, d$ and $k$ are reasonably small, we can easily check all possibilities. We find that the only solutions $(m, d, k, y)$ of (5.3) for arbitrary $\ell$ are given by

$$(1,1,2,1),\ (1,1,3,1),\ (1,1,4,1),\ (1,2,2,1),\ (1,3,2,1),\ (1,3,3,1),$$

$$(1,6,2,1),\ (2,1,2,1),\ (2,1,3,1),\ (2,5,2,1),\ (3,1,2,1),\ (3,4,2,1)$$

$$(4,3,2,1)$$

and further, for $\ell = 7$, we also find the solutions

$$(1,11,2,2),\ (2,5,3,2),\ (7,5,2,2).$$

# References

[1] L. Alpoge, *The average number of integral points on elliptic curves is bounded*, arXiv:1412.1047 [math.NT].

[2] T. Amdeberhan, L. A. Medina and V. H. Moll, *Asymptotic valuations of sequences satisfying first order recurrences*, Proc. Amer. Math. Soc. **137** (2009), no. 3, 885-890.

[3] S. Barbero, *Generalized Vandermonde determinants and characterization of divisibility sequences*, J. Number Theory **173** (2017), 371–377.

[4] J. P. Bézivin, A. Pethő and A. J. van der Poorten, *A full characterisation of divisibility sequences*, Amer. J. Math. **112** (1990), 985–1001.

[5] A. A. Bennett and A. Brauer, *Questions, Discussions, and Notes: Question Concerning the Maximum Term in the Diatomic Series*, Amer. Math. Monthly **40** (1933), no. 7, 409–410.

[6] M. A. Bennett and S. Siksek, *A conjecture of Erdős, supersingular primes and short character sums*, arXiv:1709.01022 [math.NT].

[7] F. Beukers, *The multiplicity of binary recurrences*, Compos. Math. **40** (1980), no. 2, 251–267.

[8] Y. 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. **593** (2001), 75-122.

[9] O. Bizim and B. Gezer, *Squares in elliptic divisibility sequences*, Acta Arith. **144** (2010), no. 2, 125–134.

[10] O. Bizim and B. Gezer, *Cubes in elliptic divisibility sequences*, Math. Rep. (Bucur.) **14**(64) (2012), no. 1, 21-29.

[11] A. Brauer, *On a property of $k$ consecutive integers*, Bull. Amer. Math. Soc. **47** (1941), 328-331.

[12] A. Brauer and H. Zeitz, *Über eine zahlentheoretische Behauptung von Legendre*, Sitz. Berliner Math. Ges. **29** (1930), 116-125.

[13] J. J. Bravo, P. Das, S. Guzmán and S. Laishram, *Powers in products of terms of Pell's and Pell-Lucas Sequences*, Int. J. Number Theory **11** (2015), 1259-1274.

[14] R. D. Carmichael, *On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$*, Ann. of Math. (2) **(**15) (1913), no. 1-4, 49-70.

[15] Y. Caro, *On a division property of consecutive integers*, Israel J. Math. **33** (1979), no. 1, 32-36.

[16] J. Cilleruelo, *Square in* $(1^2+1)\ldots(n^2+1)$, J. Number Theory **128** (2008), no. 8, 2488-2491.

[17] A. Dujella, M. Kazalicki, M. Mikić and M. Szikszai, *There are infinitely many rational Diophantine sextuples*, Int. Math. Res. Not. IMRN (2017), no. 2, 490-508.

[18] R. B. Eggleton, *Common factors of integers: a graphic view*, Discrete Math. **65** (1987), no. 2, 141-147.

[19] P. Erdős, *On the difference of consecutive primes*, Q. J. Math. **6** (1935), 124-128.

[20] P. Erdős, *Some remarks on number theory*, Israel J. Math. **3** (1965), 6-12.

[21] P. Erdős and J. L. Selfridge, *The product of consecutive integers is never a power*, Illinois J. Math. **19** (1975), 292-301.

[22] R. J. Evans, *Mathematical Notes: On Blocks of $N$ Consecutive Integers*, Amer. Math. Monthly **76** (1969), no. 1, 48-49.

[23] R. J. Evans, *On $N$ consecutive integers in an arithmetic progression*, Acta Sci. Math. (Szeged) **33** (1972), 295-296.

[24] G. Everest and G. Harman, *On primitive divisors of* $n^2+b$, Number theory and polynomials, 142–154, London Math. Soc. Lecture Note Ser. **352**, Cambridge Univ. Press, Cambridge, 2008.

[25] G. Everest, G. Mclaren and T. Ward, *Primitive divisors of elliptic divisibility sequences*, J. Number Theory **118** (2006), no. 1, 71-89.

[26] G. Everest, A. van der Poorten, I. Shparlinski, T. Ward, *Recurrence Sequences*, Math. Surveys Monogr., vol. 104, Amer. Math. Soc., Providence, RI, 2003.

[27] G. Everest, J. Reynolds and S. Stevens, *On the denominators of rational points on elliptic curves*, Bull. Lond. Math. Soc. **39** (2007), no. 5, 762-770.

[28] G. Everest, S. Stevens, D. Tamsett, and T. Ward, *Primes generated by recurrence sequences*, Amer. Math. Monthly **114** (2007), no. 5, 417-431.

[29] Z. Gál, Á. Nagy, M. Szikszai, and Gy. Terdik, *Stochastic modeling of Wireless Networks: a case study in time domain*, Proceedings of the 9th International Conference on Applied Informatics, Eger, Hungary, January 29-February 1, 2014. Vol. 2., 195-201.

[30] I. Gassko, *Stapled sequences and stapling coverings of natural numbers*, Electron. J. Combin. **3** (1996), no. 1, #R 33, 20 pp.

[31] J. Gebel, H. Emanuel, A. Pethő and H. G. Zimmer, *Computing all $S$-integral points on elliptic curves*, Math. Proc. Cambridge Philos. Soc. **127** (1999), no. 3, 383-402.

[32] S. Ghorpade and S. Ram, *Arithmetic progressions in a unique factorization domain*, Acta Arith. **154** (2012), no. 2, 161-171.

[33] J. R. Giles and J. Seberry Wallis, *George Szekeres: With affection and respect*, J. Austral. Math. Soc. Ser. A **21** (1976), no. 4, 385-392.

[34] K. Győry, L. Hajdu, and Á. Pintér, *Perfect powers from products of consecutive terms from arithmetic progressions*, Compos. Math. **145** (2009), 845-864.

[35] L. Hajdu and T. Herendi, *Explicit bounds for the solutions of elliptic equations with rational coefficients*, J. Symbolic Comput. **25** (1998), no. 3, 361-366.

[36] L. Hajdu, S. Laishram and M. Szikszai, *Perfect powers in products of terms of elliptic divisibility sequences*, Bull. Aust. Math. Soc. **94** (2016), no. 3, 395-404.

[37] L. Hajdu and N. Saradha, *On a problem of Pillai and its generalizations*, Acta Arith. **144** (2010), no. 4, 323-347.

[38] L. Hajdu and N. Saradha, *Examples for sets $S_m$ not having property $P(T)$*, neumann.math.unideb.hu/∼hajdul/Tables.pdf.

[39] L. Hajdu and M. Szikszai, *On the GCD-s of $k$ consecutive terms of Lucas sequences*, J. Number Theory **132** (2012), no. 12, 3056-3069.

[40] L. Hajdu and M. Szikszai, *On common factors within a series of consecutive terms of an elliptic divisibility sequence*, Publ. Math. Debrecen **84** (2014), no. 1-2, 291-301.

[41] L. Hajdu and M. Szikszai, *Common factors in series of consecutive terms of associated Lucas and Lehmer sequences*, Fibonacci Quart. **53** (2015), no. 3, 221-229.

[42] L. Hajdu, M. Szikszai and V. Ziegler, *On arithmetic progressions in Lucas sequences*, J. Integer Seq. **20** (2017), no. 8, Art. 17.8.6, 18 pp.

[43] M. Hall, *Divisibility sequences of Third Order*, Amer. J. Math. **58** (1936), no. 3, 577-584.

[44] H. Harborth, *Eine Eigenschaft aufeinanderfolgender Zahlen*, Arch. Math. (Basel) **21** (1970), 50-51.

[45] H. Harborth, *Sequenzer ganzer Zahlen*, Zahlentheorie (Tagung, Math. Forschungsinst. Oberwolfach, 1970), pp. 59–66. Ber. Math. Forschungsinst., Oberwolfach, Heft 5, Bibliographisches Inst., Mannheim, 1971.

[46] J. Harrington and L. Jones, *Extending a theorem of Pillai to quadratic sequences*, Integers **15A** (2015), Paper No. A7, 22 pp.

[47] B. He, A. Togbé, and S. Yang, *Diophantine equations with products of consecutive values of a quadratic polynomial*, J. Number Theory **131** (2011), 1840-1851.

[48] P. Ingram, *Elliptic divisibility sequences over certain curves*, J. Number Theory **123** (2007), no. 2, 473-486.

[49] P. Ingram, *A quantitative primitive divisor result for points on elliptic curves*, J. Théor. Nombres Bordeaux **21** (2009), no. 3, 609-634.

[50] P. Ingram and J. H. Silverman, *Uniform estimates for primitive divisors in elliptic divisibility sequences*, Number theory, analysis and geometry, 243–271, Springer, New York, 2012.

[51] S. Laishram and T. N. Shorey, *Number of prime divisors in a product of consecutive integers*, Acta Arith. **113** (2004), no. 4, 327-341.

[52] S. Laishram and T. N. Shorey, *Number of prime divisors in a product of terms of an arithmetic progression*, Indag. Math. (N. S.) **17** (2006), no. 3, 425-436.

[53] A. M. Legendre, *Théorie des nombres, Tome II*, Paris, 1830.

[54] D. H. Lehmer, *An extended theory of Lucas' functions*, Ann. of Math. (2) **31** (1930), no. 3, 419-448.

[55] F. Luca and T. N. Shorey, *Diophantine equations with products of consecutive terms in Lucas sequences*, J. Number Theory **114** (2005), 298-311.

[56] E. Lucas, *Théorie des Fonctions Numériques Simplement Périodiques*, Amer. J. Math. **1** (1878), no. 2, 184-196.

[57] E. Lucas, *Théorie des Fonctions Numériques Simplement Périodiques*, Amer. J. Math. **1** (1878), no. 3, 197-240.

[58] E. Lucas, *Théorie des Fonctions Numériques Simplement Périodiques*, Amer. J. Math. **1** (1878), no. 4, 289-321.

[59] L. W. McDaniel, *The g.c.d. in Lucas sequences and Lehmer number sequences*, Fibonacci Quart. **29** (1991), no. 1, 24-29.

[60] M. Ohtomo and F. Tamari, *On relative prime number in a sequence of positive integers*, J. Statist. Plann. Inference **106** (2002), no. 1-2, 509-515.

[61] A. Oosterhout, *Characterisation of Divisibility Sequences*, Master's thesis, Utrecht Univ., 2011.

[62] S. S. Pillai, *On $m$ consecutive integers. I.*, Proc. Indian Acad. Sci., Sect. A. **11** (1940), 6-12.

[63] S. S. Pillai, *On $m$ consecutive integers. II.*, Proc. Indian Acad. Sci., Sect. A. **11** (1940), 73-80.

[64] S. S. Pillai, *On $m$ consecutive integers. III.*, Proc. Indian Acad. Sci., Sect. A. **13** (1940), 530-533.

[65] S. S. Pillai, *On $m$ consecutive integers. IV.*, Bull. Calcutta Math. Soc. **36** (1944), 99-101.

[66] I. Pink and M. Szikszai, *A Brocarcd-Ramanujan-type equation with Lucas and associated Lucas sequences*, Glas. Mat. Ser. III **52(72)** (2017), no. 1, 11-21.

[67] G. Pólya, *Arithmetische Eigenschaften der Reihenentwicklungen rationaler Funktionen*, J. Reine Angew. Math. **151** (1921), 1-31.

[68] J. Reynolds, *Perfect powers in elliptic divisibility sequences*, J. Number Theory **132** (2012), no. 5, 998-1015.

[69] P. Ribenboim, *Little book of bigger primes*, Second edition, Springer-Verlag, New York, 2004.

[70] J. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. **6** (1962), 64-94.

[71] C. Sanna and M. Szikszai, *On a coprimality condition for consecutive values of polynomials*, Bull. Lond. Math. Soc., accepted.

[72] N. Saradha and R. Thangadurai, *Pillai's problem on consecutive integers*, Number theory and applications, 175–188, Hindustan Book Agency, New Delhi, 2009.

[73] A. Schinzel, *Primitive divisors of the expression $A^n - B^n$ in algebraic number fields*, J. Reine Angew. Math. **269/269** (1974), 27-33.

[74] H. P. Schlickewei and W. M. Schmidt, *The number of solutions of polynomial-exponential equations*, Compos. Math. **120** (2000), no. 2, 193-225.

[75] J.-P. Serre, *Lectures on $N_x(p)$*, Chapman & Hall/CRC Research Notes in Mathematics, vol. 11, CRC Press, Boca Raton, FL, 2012.

[76] J. H. Silverman, *Wieferich's criterion and the abc-conjecture*, J. Number Theory **30** (1988), no. 2, 226-237.

[77] R. Shipsey, *Elliptic Divisibility Sequences*, PhD thesis, Goldsmiths, University of London, 2001.

[78] T. N. Shorey and R. Tijdeman, *Perfect powers in products of terms in an arithmetic progression*, Compos. Math. **75** (1990), 307-344.

[79] P. Stevenhagen and H. W. Lenstra, *Chebotarëv and his density theorem*, Math. Intelligencer **18** (1996), no. 2, 26-37.

[80] C. Stewart, *Primitive divisors of Lucas and Lehmer numbers* in A. Baker and D. W. Masser (eds.), Transcendence Theory: Advances and Applications, Academic Press, 1977, 79-92.

[81] M. Szikszai, *Distinct products in Lucas sequences - On a problem of Kimberling*, Fibonacci Quart., accepted.

[82] C. Swart, *Sequences related to elliptic curves*, PhD thesis, Royal Holloway, University of London, 2003.

[83] M. Ward, *Memoir on elliptic divisibility sequences*, Amer. J. Math. **70**, (1948), 31-74.

[84] L. C. Washington, *Elliptic curves. Number theory and cryptography. Second edition.* Discrete Mathematics and its Applications (Boca Raton), xviii+513 pp., Chapman & Hall/CRC, Boca Raton, FL, 2008.

[85] K. Zsigmondy, *Zur Theorie der Potenzreste*, Monatsh. Math. Phys. **3** (1892), no. 1, 265-284.

# Szikszai Márton publikációs jegyzéke

[1] L. Hajdu and M. Szikszai, *On the GCD-s of k consecutive terms of Lucas sequences*, J. Number Theory **132** (2012), no. 12, 3056-3069.

[2] L. Hajdu and M. Szikszai, *On common factors within a series of consecutive terms of an elliptic divisibility sequence*, Publ. Math. Debrecen **84** (2014), no. 1-2, 291-301.

[3] Z. Gál, Á. Nagy, M. Szikszai, and Gy. Terdik, *Stochastic modeling of Wireless Networks: a case study in time domain*, Proceedings of the 9th International Conference on Applied Informatics, Eger, Hungary, January 29-February 1, 2014. Vol. 2., 195-201.

[4] L. Hajdu and M. Szikszai, *Common factors in series of consecutive terms of associated Lucas and Lehmer sequences*, Fibonacci Quart. **53** (2015), no. 3, 221-229.

[5] L. Hajdu, S. Laishram and M. Szikszai, *Perfect powers in products of terms of elliptic divisibility sequences*, Bull. Aust. Math. Soc. **94** (2016), no. 3, 395-404.

[6] A. Dujella, M. Kazalicki, M. Mikić and M. Szikszai, *There are infinitely many rational Diophantine sextuples*, Int. Math. Res. Not. IMRN (2017), no. 2, 490-508.

[7] I. Pink and M. Szikszai, *A Brocarcd-Ramanujan-type equation with Lucas and associated Lucas sequences*, Glas. Mat. Ser. III **52(72)** (2017), no. 1, 11-21.

[8] L. Hajdu, M. Szikszai and V. Ziegler, *On arithmetic progressions in Lucas sequences*, J. Integer Seq. **20** (2017), no. 8, Art. 17.8.6, 18 pp.

[9] C. Sanna and M. Szikszai, *On a coprimality condition for consecutive values of polynomials*, Bull. Lond. Math. Soc. **49** (2017), 908-915.

[10] M. Szikszai, *Distinct products in Lucas sequences - On a problem of Kimberling*, Fibonacci Quart. **55** (2017), no. 4, 291-296.

# 6. Összefoglaló

Jelen dolgozatban a következő, gyakran Pillainak [62] tulajdonított, klasszikus számelméleti probléma általánosításait tekintettük.

**1. Probléma.** Legyen $k \geq 2$ egész szám. Igaz-e, hogy bármely $k$ egymást követő egész szám között létezik olyan, mely az összes többihez relatív prím?

A fenti kérdést mind a hosszú prímhézagok tanulmányozása, mind a Diofantikus alkalmazások lehetőségei motiválják, lásd a [19, 12, 5, 64] cikkeket. Következésképpen a probléma több irányban is kiterjesztésre került, egyrészt a relatív prím feltétel gyengítése, másrészt az egymást követő egészek valamely egész számokból álló sorozattal való helyettesítése révén. Itt a [22, 15, 37, 46] művekre hivatkozunk.

A témában elért új eredményeinket négy fejezetre osztottuk. Az első három tartalma közvetlenül kapcsolódik az 1. Probléma különféle változataihoz, míg a negyedik egy Diofantikus egyenlet megoldását részletezi. Tételeink összefoglalása előtt felidézzük az azok egyszerű megfogalmazásához szükséges terminológia fontosabb elemeit.

Pozitív egészek egy $T$ halmazát megadva, melyre $1 \in T$, az $x$ és $y$ egészeket $T$-relatív prímnek nevezzük, ha $\text{lnko}(x, y) \in T$. Vegyük egészek egy tetszőleges $s = (s_n)_{n=0}^{\infty}$ sorozatát. Legyen $g_s(T)$ az a legkisebb pozitív egész, hogy létezik a sorozatnak $g_s(T)$ darab egymást követő eleme azzal a tulajdonsággal, hogy egyikük sem $T$-relatív prím az összes többihez. Hasonlóan, legyen $G_s(T)$ az a legkisebb pozitív egész, hogy minden egyes $k \geq G_s(T)$ esetén található $k$ egymást követő tagja a sorozatnak az utóbbi követelménynek megfelelően. Amennyiben $T = \{1\}$ vagy pedig $s$ az egymást követő nem-negatív egészek sorozata, úgy a jelölésből elhagyjuk mind a $T$ halmazt, mind a sorozatot.

Elsőként, a 2. Fejezetben,

$$s = (f(n))_{n=0}^{\infty} \qquad (f \in \mathbb{Z}[x])$$

alakú sorozatokat tanulmányoztunk. Az $f$ lineáritása okán valójában számtani sorozatokkal kell dolgozzunk. Ebben az esetben az 1. Probléma kapcsolódó változata lényegében megoldott Evans [22], illetve Hajdu és Saradha [37] eredményeinek köszönhetően. Ugyanakkor, ha $f$ kvadratikus, az egyetlen korábbi eredmény a szakirodalomban Harrington és Jones [46] nevéhez fűződik, akik $g_s$ értékét explicit módon meghatározták kvadratikus polinomok egyes családjaira. Ezen túlmenően sejtésként fogalmazták meg, hogy $g_s$ minden kvadratikus sorozat esetén létezik, illetve uniform módon korlátos. A disszertációban kvalitatív választ adtunk erre a sejtésre, kiterjesztve azt harmadfokú sorozatokra is.

**6.1. Tétel** (Sanna and Szikszai [71], 2017)**.** *Legyen $f \in \mathbb{Z}[x]$ és legyen $s = (f(n))_{n=0}^{\infty}$. Ha $\deg f \leq 3$, akkor létezik olyan $k_0$ pozitív konstans, hogy bármely pozitív $k \geq k_0$ egész esetén végtelen sok $n$ nem-negatív egész található azzal a tulajdonsággal, hogy*

$$f(n+1), f(n+2), \ldots, f(n+k)$$

*egyike sem relatív prím az összes többihez. Speciálisan, mind $g_s$, mind pedig $G_s$ létezik.*

A 3. Fejezetben lineáris rekurzív sorozatokkal foglalkoztunk. Ezek egészek olyan $u = u(a_1, a_2, \ldots, a_r) = (u_n)_{n=0}^{\infty}$ sorozatai, melyek eleget tesznek egy

$$u_{n+r} = a_1 u_{n+r-1} + a_2 u_{n+r-2} + \cdots + a_r u_n \qquad (n \geq 0)$$

alakú rekurzív relációnak valamely $a_1, a_2, \ldots, a_r$ egész számok esetén, ahol $a_r \neq 0$. Feltettük, hogy a kérdéses sorozatok tagjaira fennáll az oszthatósági tulajdonság, azaz bármely $m \mid n$ indexek esetén $u_m \mid u_n$ következik. Az általánosságot nem megszorítva, a rekurzív reláció

$a_1, a_2, \ldots, a_r$ együtthatóit relatív prímnek tekintettük, a sorozat első két tagját pedig $u_0 = 0$ és $u_1 = 1$ módon választottuk. Megjegyezzük továbbá, hogy az $u$ sorozatot degeneráltnak nevezzük, amennyiben az

$$x^r - a_1 x^{r-1} - \cdots - a_r$$

polinom valamely két külöböző gyökének hányadosa egységgyök.

Eredményeinket a sorozat rendje, azaz $r$ szerint három részre osztottuk. Amennyiben $r = 1$, az alábbi egyszerű állítás adódik.

**6.1. Állítás.** *Legyen $u = u(a_1)$ egy lineáris rekurzió és legyen $T \subset \mathbb{Z}_S$, ahol $S$ prímek egy tetszőleges halmaza. Ha $|u_0| \notin T \cup \{0\}$ vagy $|u_0| \in T$ és létezik olyan $p \mid a_1$ prím, hogy $\nu_p(x)$ korlátos minden $x \in T$ esetén, akkor mind $g_u(T)$, mind $G_u(T)$ létezik és $g_u(T) = G_u(T) = 2$. Speciálisan, $g_u$ és $G_u$ pontosan akkor létezik, ha vagy $|u_0| \geq 2$, vagy $|u_0| = 1$ és $|a_1| \geq 2$ áll fenn.*

A lineáris rekurziók tagjait általánosított hatványösszegként előállítva következik, hogy ha a $r = 2$, akkor éppen az úgynevezett elsőfajú Lucas-sorozatok családját kapjuk. Ezek több olyan erős aritmetikai tulajdonságot teljesítenek, melyek számottevően megkülönböztetik őket más lineáris oszthatósági sorozatoktól. Lucas-sorozatokkal kapcsolatban elsőként az alábbi általános eredményt igazoltuk.

**6.2. Tétel** (Hajdu és Szikszai [39], 2012)**.** *Legyen $u$ egy nem-degenerált elsőfajú Lucas-sorozat és legyen $T \subset \mathbb{Z}_S$ egy részhalmaza, ahol $S$ prímeknek egy véges halmaza. Ekkor mind $g_u(T)$, mind $G_u(T)$ létezik, továbbá*

$$g_u(T) \leq G_u(T) \leq 20(2|S| + 30)\log(2|S| + 30)$$

*teljesül.*

A $T$ halmazt a $T = \{1\}$ esetre megszorítva egy sokkal erősebb állítást fogalmaztunk meg.

**6.3. Tétel** (Hajdu és Szikszai [39], 2012). *Legyen $u = u(a_1, a_2)$ egy elsőfajú Lucas-sorozat. Ekkor $g_u$ és $G_u$ pontosan akkor létezik, ha $(a_1, a_2)$ nem a $(0, \pm 1)$ vagy $(\pm 1, -1)$ párok valamelyike. Amennyiben $g_u$ és $G_u$ létezik, úgy $g_u = G_u = 17$, kivéve az 5. Táblázatban található sorozatokat.*

| $(a_1, a_2)$ | $g_u$ | $G_u$ |
|---|---|---|
| $(\pm 1, a_2), a_2 \neq -1, -2, -3, -5$ | 25 | 25 |
| $(a_1, -a_1^2 + 1), \lvert a_1 \rvert > 1$ | 43 | 43 |
| $(\pm 12, -55), (\pm 12, -377)$ | 31 | 31 |
| $(\pm 1, -3)$ | 45 | 45 |
| $(\pm 1, -5)$ | 49 | 51 |
| $(\pm 1, -2)$ | 107 | 107 |

5. táblázat. A $g_u$ és $G_u$ értékei a kivételes Lucas sorozatok esetén.

Vegyük észre, hogy 6.3. Tétel teljességgel megoldja az 1. Probléma Lucas-sorozatokra vonatkozó formáját. Megjegyezzük továbbá, hogy a 6.3. Tétel bizonyításának egyik lépéseként megválaszoltuk Beukers [7] egy kérdését elsőfajú nem-degenerált Lucas sorozatok ±1 értékű elemeinek jellemzésére vonatkozóan.

Lineáris oszthatósági sorozatokkal kapcsolatos utolsó eredményünk minden legalább harmadrendű nem-degenerált sorozatot magába foglalt, így téve teljessé vizsgálatainkat.

**6.4. Tétel** (Hajdu és Szikszai [39], 2012). *Legyen $u$ egy $r \geq 3$ rendű nem-degenerált lineáris oszthatósági sorozat és legyen $T \subset \mathbb{Z}_S$, ahol $S$ prímek egy véges halmaza. Ekkor $G_u(T)$, és így $g_u(T)$ is létezik, továbbá*

$$g_u(T) \leq G_u(T) \leq r^{2^{8(|S|+r)}}$$

*teljesül.*

A lineáris rekurzív sorozatokra vonatkozó eredmények alapján úgy tűnhet, hogy a $g$ és $G$ mennyiségek létezése szinte automatikus. Ugyanakkor a bizonyításokban központi szerepet játszik a sorozatok által teljesített oszthatósági tulajdonság. Annak tanulmányozása végett, hogy mi történik, ha elhagyjuk ezt a feltételt, úgynevezett másodfajú Lucas-sorozatokat tekintettünk. Ezek olyan másodrendű $v = (v_n)_{n=0}^{\infty}$ lineáris rekurziók, melyek kezdőtagjai $v_0 = 2$ és $v_1 = a_1$, továbbá az oszthatóságnál csak ,,árnyalatnyival" gyengébb tulajdonságokat teljesítenek. A következő tételből láthatjuk, hogy ez önmagában is elegendő a $g$ és $G$ mennyiségek viselkedésének jelentős megváltozásához.

**6.5. Tétel** (Hajdu és Szikszai [41], 2015)**.** *Legyen $v = v(a_1, a_2)$ egy nem-degenerált másodfajú Lucas sorozat. Ekkor a következők teljesülnek.*

*i) Ha $a_1$ páros és $a_2$ páratlan, akkor mind $g_v$, mind $G_v$ létezik, továbbá $g_v = G_v = 2$.*

*ii) Ha mind $a_1$, mind $a_2$ páratlan, akkor $G_v$ nem létezik, azonban $g_v$ igen és ekkor teljesül, hogy*

$$g_v = \begin{cases} 171, & \textit{ha } a_1 = \pm 1, \\ 341, & \text{ha } a_2 = -(a_1^2 + 1)/2, \\ 6, & \textit{egyébként.} \end{cases}$$

*iii) Ha $a_1$ páratlan és $a_2$ páros, akkor $g_v$ és $G_v$ egyike sem létezik.*

Láthattuk tehát, hogy lineáris rekurzív sorozatok vizsgálata során az oszthatósági tulajdonság szoros összefüggésben áll a $g$ és $G$ mennyiségek viselkedésével. Felvetődött a kérdés, hogy az erős aritmetika érvényben maradása esetén, a linearitás elhagyásával, milyen eredmények nyerhetők.

Az elliptikus oszthatósági sorozatok olyan bilineáris rekurziók, melyek egy racionális számtest feletti

$$E: \qquad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

általános Weierstrass-egyenlettel adott görbe pontjaiból állíthatók elő a következő módon. Legyen $P$ az $E$ egy racionális affin pontja. Ekkor

$$nP = \left( \frac{A_n}{B_n^2}, \frac{C_n}{B_n^3} \right) \qquad (n \geq 1)$$

írható, ahol $A_n, B_n, C_n \in \mathbb{Z}$ és $\mathrm{lnko}(A_nC_n, B_n) = 1$. A $B_0 = 0$ választással, a $B = B(E,P) = (B_n)_{n=0}^{\infty}$ sorozatot elliptikus oszthatósági sorozatnak nevezzük. Ezek lényegében a Lucas sorozatokkal azonos oszthatósági tulajdonságokat teljesítenek. A 4. Fejezetben a következő kapcsolódó, és nem meglepő, eredményt nyertük.

**6.6. Tétel** (Hajdu és Szikszai [40], 2014). *Legyen $B = B(E,P)$ egy elliptikus oszthatósági sorozat és legyen $T \subset \mathbb{Z}_S$, ahol $S$ prímek egy véges halmaza. Ekkor mind $g_B(T)$, mind $G_B(T)$ létezik és*

$$g_B(T) \leq G_B(T) \leq C(E, |S|, \max S),$$

*teljesül, ahol $C(E, |S|, \max S)$ egy effektív konstans, mely kizárólag az $E$, $|S|$ and $\max S$ paraméterektől függ. Speciálisan, $g_u$ és $G_u$ létezik és effektív módon korlátozható kizárólag $E$ függvényében.*

Az utolsó, azaz 5. Fejezetben, a $g$ értékére vonatkozó effektív eredmények egy diofantikus alkalmazását tanulmányoztuk. Legyen $B = (B_n)_{n=0}^{\infty}$ egy elliptikus oszthatósági sorozat és tekintsük a

$$B_nB_{n+d}\dots B_{n+(k-1)d} = y^{\ell} \tag{6.1}$$

egyenletet, ahol $n, d, k, y, \ell$ olyan ismeretlen pozitív egészek, melyekre $\mathrm{lnko}(m,d) = 1$ és $k, \ell \geq 2$ teljesül. Megjegyezzük, hogy a (6.1)-hez hasonló egyenleteknek igen kiterjedt az irodalma. Kapcsolódó eredményekért a [21, 34, 6, 16, 47, 13] tudományos munkákat említjük meg.

Egyszerűbb hivatkozás kedvéért vezessük be a

$$\mathcal{P}_{\ell}(B) = \{i : B_i \ \ell\text{-edik hatvány}\}$$

és

$$N_\ell = |\mathcal{P}_\ell(B)| \qquad \text{és} \qquad M_\ell = \max_{n \in \mathcal{P}_\ell(B)} n$$

jelöléseket. A disszertáció utolsó állítása az (6.1) megoldásaira fogalmaz meg ineffektív végességet, míg további feltételek esetén egy explicit leszámlálást és effektív korlátosságot adó eljárást létezését mondja ki.

**6.7. Tétel** (Hajdu, Laishram és Szikszai [36], 2016)**.** *Legyen $\ell \geq 2$ rögzített. Ekkor az* (6.1) *egyenletnek csak véges sok megoldása lehet. Továbbá, ha $(n, d, k, y)$ egy megoldás, akkor*

$$\max(n, d, k, y) \leq C(N_\ell, M_\ell)$$

*teljesül, ahol $C$ egy effektív módon kiszámítható konstans, mely kizárólag az $N_\ell$ és $M_\ell$ értékétől függ. Speciálisan, ha $\mathcal{P}_\ell(B)$ explicit adott, akkor a* (6.1) *egyenlet összes megoldása effektív módon meghatározható.*

# 7 Summary

In the present thesis, we studied the following classical number-theoretical problem, often attributed to Pillai [62].

**Problem 1.** Let $k \geq 2$ be an integer. Is it true that in every set of $k$ consecutive integers there exists one which is coprime to all the others?

The above question is motivated by both the study of long prime gaps and Diophantine applications, see the papers [19, 11, 5, 64]. Gradually, the problem was extended in many directions on one hand by the relaxation of the coprimality conditon, and on the other by replacing consecutive integers with some sequence of integers. Here, we refer to the works [22, 15, 37, 46].

We split our new results on the topic into four sections. The content of the first three is directly connected to variants of Problem 1 while the fourth concerns the solution of a Diophantine equation. Before summarizing our theorems, we recall the most important parts of the terminology needed to formulate them.

Given a set of positive integers $T$, such that $1 \in T$, the integers $x$ and $y$ are said to be $T$-coprime if $\gcd(x, y) \in T$. Now take an arbitrary sequence of integers $s = (s_n)_{n=0}^{\infty}$. Let $g_s(T)$ be the smallest positive integer such that there exist $g_s(T)$ consecutive terms of the sequence such that none of them is $T$-coprime to all the others. Similarly, let $G_s(T)$ stand for the smallest positive integers so that for each $k \geq G_s(T)$ we can find $k$ consecutive terms of the sequence with the latter property. Whenever $T = \{1\}$ or $s$ is the sequence of consecutive nonnegative integers, we suppress the dependence on $T$ and $s$, respectively.

First, in Section 2, we studied sequences of the form

$$s = (f(n))_{n=0}^{\infty} \qquad (f \in \mathbb{Z}[x]).$$

Observe that when $f$ is linear we have to work with arithmetic progressions. In this case, the corresponding version of Problem 1 is essentially solved thanks to results of Evans [22] and Hajdu and Saradha [37]. However, if $f$ is quadratic, the only result appearing in the literature is due to Harrington and Jones [46] who determined the value of $g_s$ explicitly for certain families of quadratic polynomials. Further, they conjectured that $g_s$ exists for every quadratic sequences and that it is uniformly bounded. In the dissertation, we gave a qualitative answer to this conjecture, extending its scope to cubic sequences as well.

**Theorem 7.1** (Sanna and Szikszai [71], 2017)**.** *Let $f \in \mathbb{Z}[x]$ and let $s = (f(n))_{n=0}^{\infty}$. If $\deg f \leq 3$, then there exists a positive constant $k_0$ such that for every integer $k \geq k_0$ there are infinitely many non-negative integers $n$ with the property that none of*

$$f(n+1), f(n+2), \ldots, f(n+k)$$

*is coprime to all the others. In particular, both $G_s$ and $g_s$ exist.*

In Section 3, we dealt with linear recurrences. These are sequences of integers $u = u(a_1, a_2, \ldots, a_r) = (u_n)_{n=0}^{\infty}$ that satisfy a recurrence relation of the form

$$u_{n+r} = a_1 u_{n+r-1} + a_2 u_{n+r-2} + \cdots + a_r u_n \qquad (n \geq 0)$$

for some integers $a_1, a_2, \ldots, a_r$, where $a_r \neq 0$. We assumed that the terms of such a sequence satisfy the divisibility property, that is for every pair of indices $m \mid n$ we have $u_m \mid u_n$. Without losing generality, we considered $a_1, a_2, \ldots, a_r$ to be coprime and chose the initial terms as $u_0 = 0$ and $u_1 = 1$. Further, we note that $u$ is called non-degenerate whenever the quotient of any two distinct roots of the polynomial

$$x^r - a_1 x^{r-1} - \cdots - a_r$$

is not a root of unity.

We split our results into three cases depending on the order $r$. When $r = 1$, we have the following simple statement.

**Proposition 7.1** (Szikszai, 2017). *Let $u = u(a_1)$ be a linear recurrence and let $T$ be a subset of $\mathbb{Z}_S$, where $S$ is any set of primes. If either $|u_0| \notin T \cup \{0\}$, or $|u_0| \in T$ and there is a prime $p \mid a_1$ such that $\nu_p(x)$ is bounded for every $x \in T$ holds, then both $g_u(T)$ and $G_u(T)$ exist and $g_u(T) = G_u(T) = 2$. In particular, $g_u$ and $G_u$ exist if and only if either $|u_0| \geq 2$, or $|u_0| = 1$ and $|a_1| \geq 2$ holds.*

From the representation of terms of linear recurrences as generalized power sums it follows that if $r = 2$, then we work with so-called Lucas sequences of the first kind. These are sequences with strong arithmetic properties that distinguish them from other linear divisibility sequences. First, we proved the following general result.

**Theorem 7.2** (Hajdu and Szikszai [39], 2012). *Let $u$ be a non-degenerate Lucas sequence of the first kind and let $T$ be a subset of $\mathbb{Z}_S$, where $S$ is a finite set of primes. Then, both $g_u(T)$ and $G_u(T)$ exist and we have*

$$g_u(T) \leq G_u(T) \leq 20(2|S| + 30)\log(2|S| + 30).$$

Restricting $T$ to $T = \{1\}$ we made a much stronger statement.

**Theorem 7.3** (Hajdu and Szikszai [39], 2012). *Let $u = u(a_1, a_2)$ be a Lucas sequence of the first kind. Then $g_u$ and $G_u$ exist if and only if $(a_1, a_2)$ is not one of $(0, \pm 1)$ or $(\pm 1, 1)$. In case $g_u$ and $G_u$ exist, we have $g_u = G_u = 17$, except the sequences listed in Table 6.*

Observe that Theorem 7.3 completely solves the corresponding form of Problem 1 in Lucas sequences. We also note that our proof of said result answers a problem of Beukers [7] concerning terms of Lucas sequences of the first kind with ±1 values.

Our last result concerning linear divisibility sequences includes every non-degenerate sequence of order at least 3, thus completing the picture.

| $(a_1, a_2)$ | $g_u$ | $G_u$ |
|---|---|---|
| $(\pm 1, a_2), a_2 \neq -1, -2, -3, -5$ | 25 | 25 |
| $(a_1, -a_1^2 + 1), \lvert a_1 \rvert > 1$ | 43 | 43 |
| $(\pm 12, -55), (\pm 12, -377)$ | 31 | 31 |
| $(\pm 1, -3)$ | 45 | 45 |
| $(\pm 1, -5)$ | 49 | 51 |
| $(\pm 1, -2)$ | 107 | 107 |

Table 6: Values of $g_u$ and $G_u$ for exceptional Lucas sequences.

**Theorem 7.4** (Hajdu and Szikszai [39], 2012)**.** *Let $u$ be a non-degenerate linear divisibility sequence of order $r \geq 3$ and let $T$ be a subet of $\mathbb{Z}_S$, where $S$ is a finite set of primes. Then $G_u(T)$, and hence $g_u(T)$, exist and*

$$g_u(T) \leq G_u(T) \leq r^{2^{8(|S|+r)}}.$$

Based on our results related to linear recurrences it may seem that the existence of $g$ and $G$ are almost automatic. However, the divisibility property plays a central role in the proofs. To study what happens if we drop these assumptions, we considered so-called Lucas sequences of the second-kind. These are second-order linear recurrences $v = (v_n)_{n=0}^{\infty}$ with initial terms $v_0 = 2$ and $v_1 = a_1$ and they satisfy only slightly weaker properties than divisibility. However, we showed that this minor difference already leads to a major changes in the existence of $g_s$ and $G_s$.

**Theorem 7.5** (Hajdu and Szikszai [41], 2015)**.** *Let $v = v(a_1, a_2)$ be a non-degenerate Lucas sequence of the second kind.*

*i) If $a_1$ is even and $a_2$ is odd, then both $g_v$ and $G_v$ exist and $g_v = G_v = 2$.*

*ii) If both $a_1$ and $a_2$ are odd and coprime, then $G_v$ does not exist,* *but $g_v$ does and*

$$g_v = \begin{cases} 171, & \textit{if } a_1 = \pm 1, \\ 341, & \text{if } a_2 = (P^2+1)/2, \\ 6, & \textit{otherwise.} \end{cases}$$

*iii) If $a_1$ is odd and $a_2$ is even, then neither $g_v$ nor $G_v$ exists.*

We have seen that in the investigation of linear recurrences, the presence or absence of the divisibility property considerably impacts the behavior of the quantities $g$ and $G$. Question arose what results can be obtained if the strong arithmetic remains intact but we drop the linearity. Elliptic divisibility sequences are bilinear recurrences which can be constructed from the points of a curve given by a generalized Weierstrass equation over $\mathbb{Q}$

$$E: \qquad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Let $P$ be a rational affine point. Then we can write

$$nP = \left(\frac{A_n}{B_n^2}, \frac{C_n}{B_n^3}\right) \qquad (n \geq 1),$$

where $A_n, B_n, C_n \in \mathbb{Z}$ and $\gcd(A_nC_n, B_n) = 1$. Choosing $B_0 = 0$ we call the sequence $B = (B(E,P) = (B_n)_{n=0}^{\infty}$ an elliptic divisibility sequence. These have essentially the same divisibility properties as the Lucas sequences of the first kind. In Section 4, we obtained the following related result.

**Theorem 7.6** (Hajdu and Szikszai [40], 2014). *Let $B = B(E,P)$ be an elliptic divisibility sequence and let $T$ be a subset of $\mathbb{Z}_S$, where $S$ is a finite set of primes. Then both $g_B(T)$ and $G_B(T)$ exist and*

$$g_B(T) \leq G_B(T) \leq C(E, |S|, \max S),$$

*where $C(E, |S|, \max S)$ is an effective constant depending on $E$, $|S|$ and $\max S$ only. In particular, $g_u$ and $G_u$ exist and are effectively bounded in terms of $E$ only.*

In the last section, that is, in Section 5, we considered a Diophantine application concerning effective results using $g$. Let $B = (B_n)_{n=0}^{\infty}$ be an elliptic divisibility sequence and consider the equation

$$B_n B_{n+d} \dots B_{n+(k-1)d} = y^{\ell} \tag{7.1}$$

in unknown positive integers $n, d, k, y$, and $\ell$ with $\gcd(m, d) = 1$, where $k, \ell \geq 2$. Note that the study of related equations has a wide literature. Here, we refer to the works [21, 34, 6, 16, 47, 13].

Let us introduce the notations

$$\mathcal{P}_{\ell}(B) = \{n : B_n \text{ is an } \ell\text{th power}\}$$

and

$$N_{\ell} = |\mathcal{P}_{\ell}(B)| \qquad \text{and} \qquad M_{\ell} = \max_{n \in \mathcal{P}_{\ell}(B)} n.$$

The last result of the thesis established ineffective finiteness of the solutions to equation (7.1). Further, with additional conditions, we obtained both a computational effective upper bound and and efficient algorithm for explicit enumeration of the solutions.

**Theorem 7.7** (Hajdu, Laishram, and Szikszai [36], 2016)**.** *Let $\ell \geq 2$ be fixed. Then* (7.1) *has only finitely many solutions. Further, if* $(n, d, k, y)$ *is a solution, then*

$$\max(n, d, k, y) \leq C(N_{\ell}, M_{\ell}),$$

*where $C$ is an effectively computable constant depending on $N_{\ell}$ and $M_{\ell}$ only. In particular, if $\mathcal{P}_{\ell}(B)$ is given explicitly, then all the solutions to* (7.1) *can be effectively determined.*