

# ON THE SKOLEM PROBLEM AND PRIME POWERS

GEORGE KENISON, RICHARD LIPTON, JOËL OUAKNINE, AND JAMES WORRELL

ABSTRACT. The Skolem Problem asks, given a linear recurrence sequence  $(u_n)$ , whether there exists  $n \in \mathbb{N}$  such that  $u_n = 0$ . In this paper we consider the following specialisation of the problem: given in addition  $c \in \mathbb{N}$ , determine whether there exists  $n \in \mathbb{N}$  of the form  $n = lp^k$ , with  $k, l \leq c$  and  $p$  any prime number, such that  $u_n = 0$ .

## 1. INTRODUCTION

A sequence  $(u_n)_{n=0}^{\infty}$  of real algebraic numbers is called a *linear recurrence sequence* if its terms satisfy a recurrence relation  $u_n = a_1u_{n-1} + a_2u_{n-2} + \dots + a_\ell u_{n-\ell}$ , with fixed real algebraic constants  $a_1, \dots, a_\ell$  such that  $a_\ell \neq 0$ . Such a recurrence is said to have order  $\ell$  and a sequence  $(u_n)$  satisfying the recurrence is wholly determined by the initial values  $u_0, \dots, u_{\ell-1}$ . The study of linear recurrence sequences is motivated by a wide range of phenomena, in areas such as analysis of algorithms, and biological and economic modelling. Natural decision problems for linear recurrence sequences include: whether all the terms in a sequence are positive, whether the terms of the sequence are eventually positive, and whether the sequence contains a zero. The latter, commonly known as the Skolem Problem [6, 7], is the main object of study in the current paper.

Let  $(u_n)$  be a linear recurrence sequence. A remarkable result of Skolem, Mahler, and Lech states that the set  $\{n \in \mathbb{N} : u_n = 0\}$  is the union of a finite set together with a finite number of (infinite) arithmetic progressions. The original result, proved by Skolem [14] for the field of rational numbers, was subsequently extended to the field of algebraic numbers by Mahler [9, 10], and then further extended to any field of characteristic 0 by Lech [8]. All known proofs of the Skolem-Mahler-Lech Theorem (as it is now known) employ techniques from  $p$ -adic analysis. These proofs are non-constructive and the decidability of the Skolem Problem remains open. Berstel and Mignotte, however, gave an effective method to obtain all of the arithmetic progressions in the statement of the theorem [2].

For fields of positive characteristic, the conclusion of the Skolem-Mahler-Lech Theorem does not hold. Indeed, Lech [8] gave the following illustrative example. Let  $K = \mathbb{F}_p(t)$  and consider the sequence with terms  $u_n = (1+t)^n - t^n - 1$ . Then  $(u_n)$  satisfies a linear recurrence over  $K$ , but  $u_n = 0$  if, and only if,  $n = p^k$ . Nevertheless, Derksen [5] established an analogue of the Skolem-Mahler-Lech Theorem for fields of positive characteristic, namely he proved that the set of zeroes in a field of characteristic  $p$  is a  $p$ -automatic set. The proof of Derksen was moreover effective,

---

*Key words and phrases.* Skolem Problem, Algebraic number theory, Recurrence sequences, Decidability.

The third author is supported by ERC grant AVS-ISS (648701) and DFG grant 389792660 as part of TRR 248 (see <https://perspicuous-computing.science>). Also affiliated to Department of Computer Science, Oxford University, Oxford, UK..

The fourth author is supported by EPSRC Fellowship EP/N008197/1.

Accepted for publication in the proceedings of the International Symposium on Symbolic and Algebraic Computation, ISSAC 2020.

allowing to construct for a given sequence the automaton representing the set of its zeros.

Returning to the characteristic-zero setting, progress on the decidability of the Skolem Problem has been made by restricting the problem to linear recurrence sequences of low order. Decidability of the Skolem Problem for sequences of order at most 2 is straightforward and the results are considered folklore. Breakthrough work by Mignotte, Shorey, and Tijdeman [11], and, independently, Vereshchagin [15], showed decidability of the Skolem Problem for linear recurrence sequences of order 3 and 4. Techniques from  $p$ -adic analysis and algebraic number theory are employed in both [11] and [15]. Both papers moreover make critical use of Baker's theorem for linear forms in logarithms of algebraic numbers. The approach via Baker's Theorem taken in the above papers does not appear to extend easily to recurrences of higher order. In particular, decidability of Skolem's Problem remains open for recurrences of order 5. However, the recent resurgence of research activity concerning the decidability of various sub-cases of the Skolem Problem and related questions (see the survey [13]) gives an indication of its fundamental importance to the field.

In this paper we pursue an alternative approach to restricting the order of the recurrence as a means of obtaining decidable specialisations of Skolem's Problem. We consider general recurrences, but ask to decide the existence of zeros of certain prescribed forms. For example, we ask whether one can show decidability of the Skolem Problem when we consider only those  $n \in \mathbb{N}$  that are prime powers. Our first basic result—which we will generalise in various ways in the rest of the paper—is the following, which applies to a class of *simple* linear recurrence sequences (i.e., those sequences without repeated characteristic roots):

**Theorem 1.1.** *Suppose that each term in a linear recurrence sequence  $(u_n)$  can be written as an algebraic exponential polynomial  $u_n = A_1\lambda_1^n + \cdots + A_m\lambda_m^n$  with  $A_1, \dots, A_m \in \mathbb{Z}$  and  $\lambda_1, \dots, \lambda_m$  distinct algebraic integers. Fix  $c \in \mathbb{N}$ . Then one can decide whether there exists  $n \in \{p^k : p \text{ prime}, k \leq c\}$  such that  $u_n = 0$ .*

In general, a simple linear recurrence sequence  $(u_n)$  has the property that each of its terms is given by an algebraic exponential polynomial  $u_n = A_1\lambda_1^n + \cdots + A_m\lambda_m^n$  with  $A_1, \dots, A_m \in \mathfrak{D}$  algebraic integers in a number field  $K$ . In Theorem 1.1 we assumed that  $A_1, \dots, A_m \in \mathbb{Z}$ . More generally, a linear recurrence sequence  $(u_n)$  can always be written in the form  $u_n = A_1(n)\lambda_1^n + \cdots + A_m(n)\lambda_m^n$ , where the  $A_i$  are univariate polynomials and the  $\lambda_i$  are characteristic roots of the recurrence relation. We establish decidability results for linear recurrence sequences  $(u_n)$  in this general setting. We consider the case of rational polynomial coefficients in Section 3; that is,  $A_1, \dots, A_m \in \mathbb{Z}[x]$  and, more generally, algebraic polynomial coefficients in Section 5. We outline two generalisations of Theorem 1.1 below.

First, assume that the linear recurrence sequence  $(u_n)$  satisfies  $u_n = A_1(n)\lambda_1^n + \cdots + A_m(n)\lambda_m^n$  such that  $A_1, \dots, A_m \in \mathbb{Z}[x]$ . The next result follows as a corollary to Theorem 3.3. In the proof of Theorem 3.3 we introduce and analyse an associated simple linear recurrence  $(v_n)$  with terms  $v_n = A_1(0)\lambda_1^n + \cdots + A_m(0)\lambda_m^n$ .

**Theorem 1.2.** *Let  $(u_n)$  be a recurrence sequence with rational polynomial coefficients and  $(v_n)$  the associated simple recurrence. Fix  $c \in \mathbb{N}$ . If  $v_1 \neq 0$  then one can decide whether there exists  $n \in \{p^k : p \text{ prime}, k \leq c\}$  such that  $u_n = 0$ .*

Now suppose that the terms of  $(u_n)$  are given by  $u_n = A_1(n)\lambda_1^n + \cdots + A_m(n)\lambda_m^n$  where the coefficients  $A_1, \dots, A_m \in \mathfrak{D}[x]$  are univariate polynomial with  $\mathfrak{D}$  the ring of integers of a finite Galois extension  $K$  over  $\mathbb{Q}$ . As before, let  $(v_n)$  be the associated simple recurrence. To each rational prime  $p$  we associate a constant  $f(p)$  (the *inertial degree* of  $p\mathbb{Z}$  in  $K$ ). The next result follows as a corollary to Theorem 4.1.

**Theorem 1.3.** *Suppose that  $(u_n)$  is a recurrence sequence with algebraic polynomial coefficients and  $(v_n)$  the associated linear recurrence as above. Fix  $c \in \mathbb{N}$ . If  $v_1 \neq 0$  then one can decide whether there exists  $n \in \{p^{kf(p)} : p \text{ prime}, k \leq c\}$  such that  $u_n = 0$ .*

We motivate our decidability results with a discussion of the decidability of the Skolem Problem for linear recurrence sequences of order 5. The authors of [7] claim to prove that the Skolem Problem is decidable for integer linear recurrence sequences of order 5; however, as pointed out in [12], there is a gap in the argument. The critical case for which the decidability of the Skolem Problem is open is that of a recurrence sequence of order 5 whose characteristic polynomial has five distinct roots: four distinct roots  $\lambda_1, \overline{\lambda_1}, \lambda_2, \overline{\lambda_2} \in \mathbb{C}$  such that  $|\lambda_1| = |\lambda_2|$ , and a fifth root  $\rho \in \mathbb{R}$  of strictly smaller magnitude. In this case the terms of such a recurrence sequence  $(u_n)$  are given by  $u_n = a(\lambda_1^n + \overline{\lambda_1}^n) + b(\lambda_2^n + \overline{\lambda_2}^n) + c\rho^n$ . Here  $a, b, c \in \mathbb{R}$  are algebraic numbers. If  $|a|$  and  $|b|$  are not equal then there is no known general procedure to determine  $\{n \in \mathbb{N} : u_n = 0\}$ .

Next we consider an example of a linear recurrence sequence from the aforementioned critical case. We motivate the results herein and also illustrate the techniques used in this paper by demonstrating that the sequence does not vanish at any prime index.

**Example 1.4.** For this example set  $\lambda_1 = 39 + 52i$ ,  $\lambda_2 = -60 + 25i$  and  $\rho = 1$ . (Our choices of Pythagorean triples  $(39, 52, 65)$  and  $(25, 60, 65)$  ensure that  $|\lambda_1| = |\lambda_2| = 65$ .) Let  $(v_n)$  be the linear recurrence sequence whose terms satisfy

$$v_n = \lambda_1^n + \overline{\lambda_1}^n + 3(\lambda_2^n + \overline{\lambda_2}^n) + \rho^n.$$

There are no rational primes  $p \in \mathbb{N}$  for which  $v_p = 0$ .

We omit many technical definitions and details in the following presentation (for such details we refer the reader to the preliminary material in the next section).

*Proof of Example 1.4.* Let  $K$  be the splitting field of the minimal polynomial (over  $\mathbb{Q}$ ) associated to  $(v_n)$ . We find that  $K = \mathbb{Q}(\lambda_1, \overline{\lambda_1}, \lambda_2, \overline{\lambda_2}, 1) \cong \mathbb{Q}(i)$ . The dimension  $d$  of the field  $K$  as a vector space over  $\mathbb{Q}$  is 2. There is a computable constant  $N \in \mathbb{N}$  depending only on  $v_1$  and the field  $K$  introduced in the preliminaries—the norm of the principal ideal generated by  $v_1$ —with the following property. Suppose that  $p \in \mathbb{N}$  is a rational prime. Then, by Corollary 3.1 and Lemma 3.2,  $v_p = 0$  only if  $p|N$ .

Assume that  $v_p = 0$  for some prime  $p \in \mathbb{N}$ . We calculate  $v_1 = -281$ , which we use to determine  $N$ . Here  $N = |v_1|^d = 281^2$ . Thus  $p|N = 281^2$  from our assumption. By happy coincidence, 281 is a rational prime and so it is sufficient to check whether  $v_p = 0$  for the only possible candidate  $p = 281$ . Using Mathematica we compute  $v_{281} \approx 3.7 \times 10^{509}$  (to two significant figures). We conclude that there does not exist a rational prime  $p \in \mathbb{N}$  such that  $v_p = 0$ .  $\square$

This paper is organised as follows. In Section 2, we recall preliminary terminology and background material from algebraic number theory and recurrence sequences. In Section 3, we prove decidability results locating zeroes of recurrence sequences of the form  $u_n = A_1(n)\lambda_1^n + \cdots + A_m(n)\lambda_m^n$  with polynomial coefficients  $A_1, \dots, A_m \in \mathbb{Z}[x]$  having integer coefficients. The main result in Section 3 is Theorem 3.3. In Section 4 we prove decidability results for linear recurrence sequences with polynomial coefficients  $A_1, \dots, A_m \in \mathfrak{D}[x]$ , where  $\mathfrak{D}$  is the ring of integers of a Galois number field. The main result in Section 4 is Theorem 4.1. In Section 5 we show that the problem of deciding whether a given linear recurrence sequence has

a prime zero is NP-hard. This matches the best known lower bound for the general Skolem Problem.

## 2. ALGEBRAIC NUMBER THEORY AND LINEAR RECURRENCE SEQUENCES

In this section we recall some basic notions concerning algebraic numbers and linear recurrences that will be used in the sequel.

A complex number  $\alpha$  is *algebraic* if there exists a polynomial  $P \in \mathbb{Q}[x]$  such that  $P(\alpha) = 0$ . The *minimal polynomial* of  $\alpha \in \mathbb{A}$  is the unique monic polynomial  $\mu_\alpha \in \mathbb{Q}[x]$  of least degree such that  $\mu_\alpha(\alpha) = 0$ . The *degree* of  $\alpha$ , written  $\deg(\alpha)$ , is the degree of its minimal polynomial. An *algebraic integer*  $\alpha$  is an algebraic number whose minimal polynomial has integer coefficients. The collection of all algebraic integers forms a ring  $\mathbb{B}$ .

A *number field*  $K$  is a field extension of  $\mathbb{Q}$  whose dimension as a vector space over  $\mathbb{Q}$  is finite. We call the dimension of this vector space the *degree* of the number field and use the notation  $[K : \mathbb{Q}]$  for the degree of  $K$ . Call a number field  $K$  *Galois* if it is the splitting field of some separable polynomial over  $\mathbb{Q}$ . Let  $\mathfrak{D} = \mathbb{B} \cap K$  be the ring of algebraic integers in  $K$ . Because  $\mathbb{B} \cap \mathbb{Q} = \mathbb{Z}$ , we refer to the elements of  $\mathfrak{D}$  as *rational integers*. For each  $\alpha \in K$  there exists a non-zero  $q \in \mathbb{Z}$  such that  $q\alpha \in \mathfrak{D}$ .

Given a number field  $K$  of degree  $d$  over  $\mathbb{Q}$ , there are exactly  $d$  distinct monomorphisms  $\sigma_i : K \rightarrow \mathbb{C}$ . We define the *norm*  $N_K(\alpha)$  of  $\alpha \in K$  by

$$N_K(\alpha) = \prod_{\ell=1}^d \sigma_\ell(\alpha).$$

Then  $N_K(\alpha) \in \mathbb{Q}$  and furthermore  $N_K(\alpha) \in \mathbb{Z}$  if  $\alpha \in \mathfrak{D}$ .

Suppose that  $P \in \mathbb{Z}[x]$  is a polynomial with integer coefficients. The *height* of  $P$  is the maximum of the absolute values of its coefficients and write  $\|P\|$  for the bit length of the list of its coefficients encoded in binary. It is clear that the degree of  $P$  is at most  $\|P\|$ , and the height of  $P$  is at most  $2^{\|P\|}$ .

There is a standard representation of an algebraic number  $\alpha$  as a tuple  $(\mu_\alpha, a, b, \varepsilon)$  where  $\mu_\alpha$  is the minimal polynomial of  $\alpha$  and  $a, b, \varepsilon \in \mathbb{Q}$  with  $\varepsilon > 0$  sufficiently small so that  $\alpha$  is the unique root of  $\mu_\alpha$  inside the ball of radius  $\varepsilon$  centred at  $a + bi \in \mathbb{C}$ . Given a polynomial  $P \in \mathbb{Z}[x]$ , we can compute a standard representation for each of its roots in time polynomial in  $\|P\|$ .

We recall some standard terminology and basic results about ideals in  $\mathfrak{D}$ . The ideal  $\mathfrak{a} = a\mathfrak{D}$  generated by a single element  $a \in \mathfrak{D}$  is called *principal*. For two ideals  $\mathfrak{a}$  and  $\mathfrak{b}$  of  $\mathfrak{D}$ , define the sum and product by

$$\mathfrak{a} + \mathfrak{b} := \{a + b : a \in \mathfrak{a}, b \in \mathfrak{b}\}, \quad \text{and}$$

$$\mathfrak{a}\mathfrak{b} := \left\{ \sum_{j=1}^k a_j b_j : a_j \in \mathfrak{a}, b_j \in \mathfrak{b} \right\}.$$

Two ideals  $\mathfrak{a}$  and  $\mathfrak{b}$  are said to be *coprime* if  $\mathfrak{a} + \mathfrak{b} = \mathfrak{D}$ . In this case we have  $\mathfrak{a}\mathfrak{b} = \mathfrak{a} \cap \mathfrak{b}$ .

For ideals  $\mathfrak{a}, \mathfrak{b}$  of  $\mathfrak{D}$  we say  $\mathfrak{a}$  *divides*  $\mathfrak{b}$ , and write  $\mathfrak{a} | \mathfrak{b}$ , if there exists an ideal  $\mathfrak{c}$  such that  $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$ . In addition,  $\mathfrak{a} | \mathfrak{b}$  if, and only if,  $\mathfrak{b} \subseteq \mathfrak{a}$ . An ideal  $\mathfrak{p}$  of  $\mathfrak{D}$  is called *prime* if  $\mathfrak{p} | \mathfrak{a}\mathfrak{b}$  implies  $\mathfrak{p} | \mathfrak{a}$  or  $\mathfrak{p} | \mathfrak{b}$ . Recall that the ring of integers  $\mathfrak{D}$  of a number field does not necessarily have unique factorisation. However every non-zero ideal of  $\mathfrak{D}$  can be written as a product of prime ideals and, in addition, this factorisation is unique up to the order of the factors.

Let  $\mathfrak{a}$  be a non-zero ideal of  $\mathfrak{D}$  then the quotient ring  $\mathfrak{D}/\mathfrak{a}$  is finite, which leads us to define the *norm* of  $\mathfrak{a}$  by  $N(\mathfrak{a}) = |\mathfrak{D}/\mathfrak{a}|$ . This norm has a multiplicative property:  $N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$  for every pair of non-zero ideals  $\mathfrak{a}, \mathfrak{b}$  of  $\mathfrak{D}$ . We can connect

norms of elements and ideals as follows. Suppose that  $a \in \mathfrak{D}$  is non-zero then  $N(a\mathfrak{D}) = |N_K(a)|$  and, in addition, if  $a \in \mathbb{Q}$  then  $N(a\mathfrak{D}) = |a^d|$  where  $d = [K: \mathbb{Q}]$ .

Suppose that  $\mathfrak{p}$  is a prime ideal. Since the quotient ring  $\mathfrak{D}/\mathfrak{p}$  is a finite field and, by definition,  $N(\mathfrak{p}) = |\mathfrak{D}/\mathfrak{p}|$ , we conclude that  $N(\mathfrak{p}) = p^f$  where  $f \leq [K: \mathbb{Q}]$  and  $p$  is a rational prime. Indeed,  $p \in \mathfrak{p}$  and, further, it is the only rational prime in  $\mathfrak{p}$ . Thus, we say that the prime ideal  $\mathfrak{p}$  *lies above* the prime ideal  $p\mathbb{Z}$ . We will frequently use the following version of Fermat's Little Theorem:

**Theorem 2.1.** *For any prime ideal  $\mathfrak{p}$  and algebraic integer  $\lambda \in \mathfrak{D}$ ,  $\lambda^{N(\mathfrak{p})} - \lambda \in \mathfrak{p}$ .*

We now recall some of the terminology connecting linear recurrence sequences and exponential polynomials. For further details on this correspondence we refer the reader to [6].

We call a sequence of algebraic numbers  $(u_n)_{n=0}^{\infty}$  satisfying a recurrence relation  $u_n = a_1 u_{n-1} + a_2 u_{n-2} + \cdots + a_\ell u_{n-\ell}$  with fixed real algebraic constants  $a_1, \dots, a_\ell$  such that  $a_\ell \neq 0$  a *linear recurrence sequence*. Together with the recurrence relation, the sequence is wholly determined by the initial values  $u_0, \dots, u_{\ell-1}$ . The polynomial  $f(x) = x^\ell - a_1 x^{\ell-1} - \cdots - a_{\ell-1} x - a_\ell$  is called the *characteristic polynomial* associated to the relation. Associated to each linear recurrence sequence  $(u_n)$  is a recurrence relation of minimal length. We call the characteristic polynomial of this minimal length relation the *minimal polynomial* of the sequence. Moreover, given a recurrence relation the minimal polynomial divides any characteristic polynomial. The *order* of a linear recurrence sequence is the degree of its minimal polynomial.

Let  $\mu$  be the minimal polynomial of a linear recurrence sequence  $(u_n)$  and  $K$  the splitting field of  $\mu$ . Over  $K$  the polynomial factorises as a product of powers of distinct linear factors  $\mu(x) = \prod_{i=1}^m (x - \lambda_i)^{n_i}$ . Here the constants  $\lambda_1, \dots, \lambda_m \in K$  are the *characteristic roots* of  $(u_n)$  with multiplicities  $n_1, \dots, n_m$ . The terms of a linear recurrence sequence can be realised as an *exponential polynomial* such that  $u_n = \sum_{i=1}^m A_i(n) \lambda_i^n$ . Here the  $\lambda_i$  are the distinct characteristic roots of the recurrence  $(u_n)$  alongside polynomial coefficients  $A_i \in K[x]$ . If the characteristic polynomial of a sequence has no repeated roots, the terms in the sequence are each given by an exponential polynomial  $u_n = \sum_{i=1}^m A_i(0) \lambda_i^n$  with constant coefficients. A linear recurrence sequence that satisfies this condition is called *simple*.

Suppose that  $(u_n)_{n=0}^{\infty}$  is a linear recurrence sequence with characteristic roots  $\lambda_1, \dots, \lambda_m \in K$ . For each  $i \in \{1, \dots, m\}$  there exist non-zero  $q_i \in \mathbb{Z}$  such that  $q_i \lambda_i \in \mathfrak{D}$ . Consider the linear recurrence sequence  $(w_n)_{n=0}^{\infty}$  with terms given by  $w_n = q_1^n \cdots q_m^n u_n$ . By construction,  $w_n = 0$  if and only if  $u_n = 0$  and, further, the characteristic roots of  $(w_n)$  are algebraic integers in  $\mathfrak{D}$ . Thus, without loss of generality, we assume that each  $\lambda_i \in \mathfrak{D}$  and, in addition, that  $A_1, \dots, A_m \in \mathfrak{D}[x]$ .

Let  $(u_n)$  be a linear recurrence sequence with terms  $u_n = A_1(n) \lambda_1^n + \cdots + A_m(n) \lambda_m^n$  where  $\lambda_1, \dots, \lambda_m \in \mathfrak{D}$  and  $A_1, \dots, A_m \in \mathfrak{D}[x]$ . We associate to  $(u_n)$  a simple linear recurrence  $(v_n)$  given by an exponential polynomial  $v_n = A_1(0) \lambda_1^n + \cdots + A_m(0) \lambda_m^n$ .

We are interested in determining whether  $u_n = 0$  for  $n = \ell p^k$  with  $k, \ell \in \mathbb{N}$  bounded and  $p$  any rational prime. In particular, our method is limited to those coefficients  $\ell \in \{0, 1, \dots, c\}$  for which  $v_\ell \neq 0$ . We introduce the set  $\mathcal{L}_c = \{\ell \in \mathbb{N} : \ell \leq c, v_\ell \neq 0\}$  consisting of such coefficients. In the case that  $(u_n)_{n=0}^{\infty}$  is simple we have that  $u_n = v_n$  for each  $n \in \mathbb{N}$ , and so we need only consider the  $\ell \leq c$  such that  $v_\ell \neq 0$ . In the case that  $(u_n)_{n=0}^{\infty}$  is not simple it is possible that  $(v_n)$  is identically zero; for example,  $u_n = n \lambda^n$ . If  $v_0 \neq 0$  then  $(v_n)$  is not identically zero. Otherwise  $v_0 = u_0 = 0$  and we have identified a zero term at an index of the desired form.

3. COEFFICIENTS IN  $\mathbb{Z}[x]$ 

**3.1. Decidability results.** Given a positive rational integer  $n$ , recall the multinomial expansion with exponent  $n$  is given by the identity

$$(A_1x_1 + \cdots + A_mx_m)^n = \sum_{b_1+\cdots+b_m=n} \binom{n}{b_1, b_2, b_3, \dots, b_m} \prod_{t=1}^m A_t^{b_t} x_t^{b_t}$$

with the combinatorial coefficient representing the quotient

$$\binom{n}{b_1, b_2, b_3, \dots, b_m} = \frac{n!}{b_1!b_2!\cdots b_m!}.$$

We shall make use of the following result, commonly called the *freshman's dream*.

**Corollary 3.1.** *Suppose that  $A_1, \dots, A_m \in \mathbb{Z}$  and  $\lambda_1, \dots, \lambda_m$  lie in the ring  $\mathfrak{D}$  of integers of some number field  $k$ . Then for any prime  $p$  and  $k \in \mathbb{N}$  we have the following congruence:*

$$(A_1\lambda_1 + \cdots + A_m\lambda_m)^{p^k} \equiv A_1\lambda_1^{p^k} + \cdots + A_m\lambda_m^{p^k} \pmod{p\mathfrak{D}}.$$

*Proof.* Let us expand the left-hand side using the aforementioned multinomial identity. Now consider each of the combinatorial coefficients in this expansion. If exactly one of the choices  $b_1, \dots, b_i$  is equal to  $p^k$  then the corresponding coefficient is equal to 1, and otherwise it is an integer multiple of  $p$ . Hence

$$(A_1\lambda_1 + \cdots + A_m\lambda_m)^{p^k} \equiv A_1^{p^k}\lambda_1^{p^k} + \cdots + A_m^{p^k}\lambda_m^{p^k} \pmod{p\mathfrak{D}}.$$

The result follows by repeated application of Fermat's Little Theorem,  $A_i^{p^k} \equiv A_i \pmod{p\mathbb{Z}}$ .  $\square$

In combination with Corollary 3.1, we use the following technical lemma in the proof of Theorem 1.1.

**Lemma 3.2.** *Suppose that  $b \in \mathfrak{D}$  is non-zero. There are only finitely many rational primes  $p$  such that  $p\mathfrak{D} \mid b\mathfrak{D}$  and, in addition,  $N(b\mathfrak{D})$  is an effective bound on such primes.*

*Proof.* Since the ideal norm is multiplicative we have  $p^d = N(p\mathfrak{D}) \mid N(b\mathfrak{D})$  where  $d = [K: \mathbb{Q}]$ . We can calculate  $N(b\mathfrak{D}) \in \mathbb{Z}$  and so obtain an effective bound on any rational prime  $p$  such that  $p\mathfrak{D} \mid b\mathfrak{D}$ .  $\square$

*Proof of Theorem 1.1.* Let us assume that the algebraic integers  $\lambda_1, \dots, \lambda_m$  all lie in a given number field  $K$ , and let us denote by  $\mathfrak{D}$  the ring of algebraic integers in  $K$ . We note that it is decidable whether  $u_{p^0} = u_1 = A_1 + \cdots + A_m = 0$ . Thus we can assume, without loss of generality, that  $u_1 \neq 0$ . We shall prove the case  $k = 1$ . The proof for higher powers follows with only minor changes to the argument below.

By Corollary 3.1, the following congruence holds modulo  $p\mathfrak{D}$ ,

$$u_1^p = (A_1\lambda_1 + \cdots + A_m\lambda_m)^p \equiv A_1\lambda_1^p + \cdots + A_m\lambda_m^p = u_p.$$

Thus  $u_1^p$  and  $u_p$  lie in the same coset of  $p\mathfrak{D}$ . It follows that  $u_p = 0$  only if  $u_1^p \in p\mathfrak{D}$ . Since  $p\mathfrak{D} \mid u_1^p\mathfrak{D}$  and  $u_1 \neq 0$  (by assumption), we can apply Lemma 3.2. As  $N(u_1^p\mathfrak{D})$  has only finitely many prime divisors, we obtain an effective bound on the rational primes  $p$  such that  $u_p = 0$ . We have the desired result: given  $c \in \mathbb{N}$ , it is decidable whether there exists an  $n \in \{p : p \text{ prime}\}$  such that  $u_n = 0$ .  $\square$

We now turn our attention to decidability results for linear recurrence sequences whose terms are given by an exponential polynomial with polynomial coefficients in  $\mathbb{Z}[x]$ .

Let  $(u_n)$  be a linear recurrence sequence whose terms are given by  $u_n = A_1(n)\lambda_1^n + \cdots + A_m(n)\lambda_m^n$  with  $A_1, \dots, A_m \in \mathbb{Z}[x]$  and  $\lambda_1, \dots, \lambda_m \in \mathfrak{D}$  for some ring of integers in a number field  $K$ . We associate a simple sequence  $(v_n)$  with terms given by  $v_n = A_1(0)\lambda_1^n + \cdots + A_m(0)\lambda_m^n$  to each such sequence  $(u_n)$ . Given  $c \in \mathbb{N}$ , we define the set  $\mathcal{N}_c \subset \mathbb{N}$  as follows:

$$\mathcal{N}_c := \bigcup_{\ell \in \mathcal{L}_c} \{\ell p^k : p \text{ prime}, k \leq c\}.$$

We recall the set  $\mathcal{L}_c = \{\ell \in \mathbb{N} : \ell \leq c, v_\ell \neq 0\}$  defined in the previous section. Hence  $\mathcal{N}_c$  implicitly depends on the sequence  $(u_n)$ . If  $u_0 = 0$  then we have identified a zero term at a desired index. Otherwise  $u_0 \neq 0$  and so, for  $c$  sufficiently large,  $\mathcal{N}_c$  is infinite. The goal of this section is to prove the following theorem.

**Theorem 3.3.** *Let  $(u_n)$  be a linear recurrence sequence whose terms are given by an exponential polynomial with rational polynomial coefficients as above. Fix  $c \in \mathbb{N}$ . Then one can decide whether there is an  $n \in \mathcal{N}_c$  such that  $u_n = 0$ .*

Lemma 3.4 below is a generalisation of Corollary 3.1 in two senses: the lemma considers sequences that are not necessarily simple and indices of the form  $\ell p^k \in \mathbb{N}$ .

**Lemma 3.4.** *Let  $(u_n)$  be a recurrence sequence as above and  $(v_n)$  the associated simple recurrence sequence. Let  $p \in \mathbb{N}$  be prime and  $k, \ell \in \mathbb{N}$ . Then  $v_\ell^{p^k} - u_{\ell p^k} \in p\mathfrak{D}$ .*

*Proof.* We prove the case when  $k = 1$ . The general case, dealing with higher powers  $p^k$ , follows with only minor changes.

First, we have the congruence  $v_\ell^p \equiv v_{\ell p} \pmod{p\mathfrak{D}}$  by Corollary 3.1 since

$$\left(A_1(0)\lambda_1^\ell + \cdots + A_m(0)\lambda_m^\ell\right)^p \equiv A_1(0)\lambda_1^{\ell p} + \cdots + A_m(0)\lambda_m^{\ell p}.$$

Recall that for  $A \in \mathbb{Z}[x]$  we have  $(x - y)|(A(x) - A(y))$ . By induction, one can show that  $p|(A(\ell p) - A(0))$  and so  $A(0) \equiv A(\ell p) \pmod{p\mathbb{Z}}$  for each  $A \in \mathbb{Z}[x]$ . This is sufficient to deduce a second congruence

$$v_{\ell p} \equiv A_1(\ell p)\lambda_1^{\ell p} + \cdots + A_m(\ell p)\lambda_m^{\ell p} = u_{\ell p} \pmod{p\mathfrak{D}}.$$

Together these two congruences give  $v_\ell^p - u_{\ell p} \in p\mathfrak{D}$ , the desired result.  $\square$

*Proof of Theorem 3.3.* Let us consider the case that  $k = 1$ . As previously noted, we can assume there is an  $\ell \leq c$  and  $v_\ell \neq 0$  (otherwise  $u_0 = 0$ ). Suppose that  $u_{\ell p} = 0$ . Then, by Lemma 3.4,  $v_\ell^p \in p\mathfrak{D}$  and so  $p\mathfrak{D} | v_\ell^p \mathfrak{D}$ . Thus  $p | N(v_\ell^p \mathfrak{D})$ . Since  $\mathfrak{D}$  is a commutative ring and the ideal norm is multiplicative, we have that  $p | N(v_\ell \mathfrak{D})$ . By Lemma 3.2, we obtain an effective bound on the divisors of  $v_\ell \mathfrak{D}$  of the form  $p\mathfrak{D}$  and hence a bound on the rational primes for which  $u_{\ell p} = 0$  is possible. Mutatis mutandis the proof holds for prime powers  $p^k$  with  $k > 1$ . Clearly the case  $k = 0$  is decided by determining whether  $u_\ell = 0$ .  $\square$

**3.2. Complexity upper bound.** Given a simple linear recurrence sequence  $(u_n)$ , we establish a quantitative bound on the magnitude of any prime  $p$  such that  $u_p = 0$ . The bound is in terms of the size of the problem instance. In the case that  $(u_n)$  is a simple linear recurrence sequence, we know that  $u_n = A_1\lambda_1^n + \cdots + A_m\lambda_m^n$  and so the size of the problem instance is the bit length  $S = \|\langle \lambda_1, \lambda_2, \dots, \lambda_m, A_1, A_2, \dots, A_m \rangle\|$ .

We give the following rudimentary bounds in terms of  $S$ . First, we bound  $\log_2 |A_i| + 1$ , bit length of the integer  $A_i$ , from above by  $2^S$ . Second,  $|\lambda_i|$  is bounded from above by  $H(\lambda_i) \leq 2^S$  where the height  $H(\lambda_i)$  is the maximum absolute value of the coefficients in  $\mu_{\lambda_i}$ . Finally, we have  $\deg(\lambda_i) \leq S$ , from which it follows that

$[K: \mathbb{Q}] = [\mathbb{Q}(\lambda_1, \dots, \lambda_m): \mathbb{Q}] \leq m^S \leq S^S$ . Because  $u_1 = A_1\lambda_1 + \dots + A_m\lambda_m$  we have the following elementary bound

$$N(u_1\mathfrak{D}) \leq \prod_{\ell=1}^{[K: \mathbb{Q}]} \sum_{k=1}^m |\sigma_\ell(A_k)\sigma_\ell(\lambda_k)| \leq \prod_{\ell=1}^{[K: \mathbb{Q}]} S2^{3S} \leq (S2^{3S})^{S^S}.$$

From the above calculations it follows that if  $u_p = 0$  for some prime  $p$  then  $p$  is at most  $(S2^{3S})^{S^S}$ , i.e., double exponential in  $S$ , the size of the problem instance.

#### 4. COEFFICIENTS IN $\mathfrak{D}[x]$

Let us first recall some background material on the decomposition of prime ideals in the ring of integers  $\mathfrak{D}$  of a Galois number field  $K$ . Such decompositions (as products of powers of prime ideals) are particularly well-behaved in this setting—a comprehensive presentation of this material can be found in [4]. Let  $p \in \mathbb{N}$  be prime. Then  $p\mathfrak{D} = \prod_{i=1}^g \mathfrak{p}_i^e$  where the  $\mathfrak{p}_i$  are the prime ideals lying above  $p\mathbb{Z}$ . Here the integer  $e(p) \geq 1$  is the *ramification index* of  $p$ . The degree of the field extension  $f(p) = [\mathfrak{D}/\mathfrak{p}_i : \mathbb{Z}/p\mathbb{Z}]$ , the *inertial degree* of  $\mathfrak{p}_i$  over  $p\mathbb{Z}$ , is independent of the prime ideal  $\mathfrak{p}_i$ . Suppose that  $\mathfrak{p}$  lies above  $p\mathbb{Z}$ . We have  $N(\mathfrak{p}) = N(p\mathbb{Z})^{f(p)} = p^{f(p)}$ . A prime  $p\mathbb{Z}$  is *ramified* in  $\mathfrak{D}$  if  $e > 1$  and *unramified* otherwise. In particular, only finitely many primes ramify in  $\mathfrak{D}$  since  $p\mathbb{Z}$  ramifies in  $\mathfrak{D}$  if, and only if,  $p$  divides the discriminant of  $K$  (see e.g. [4]).

Suppose that  $K$  is Galois over  $\mathbb{Q}$  and let  $\mathfrak{D}$  be the algebraic integers in  $K$ . In this section we shall prove decidability results locating the zeroes of sequences  $(u_n)$  whose terms are given by an exponential polynomial of the form  $u_n = A_1(n)\lambda_1^n + \dots + A_m(n)\lambda_m^n$  with coefficients  $A_1, \dots, A_m \in \mathfrak{D}[x]$  and  $\lambda_1, \dots, \lambda_m \in \mathfrak{D}$ . For such a sequence, fix  $c \in \mathbb{N}$  and let  $\mathcal{L}_c = \{\ell \in \mathbb{N} : \ell \leq c, v_\ell \neq 0\}$  where  $(v_n)$  is the simple recurrence sequence with terms given by  $v_n = A_1(0)\lambda_1^n + \dots + A_m(0)\lambda_m^n$ . Let  $f(p)$  be the inertial degree of  $p\mathbb{Z}$  in  $\mathfrak{D}$ . Then define the set  $\mathcal{N}_c(K)$  as the union

$$\mathcal{N}_c(K) = \bigcup_{\ell \in \mathcal{L}_c} \{\ell p^{k f(p)} : p \text{ prime}, k \leq c\}.$$

Here our choice of notation is meant to draw comparison with our previous definition for the set  $\mathcal{N}_c$ . Without loss of generality we assume that given  $c \in \mathbb{N}$  there is an  $l \leq c$  such that  $v_\ell \neq 0$  for otherwise the sequence  $(u_n)$  vanishes at  $u_0 = v_0 = 0$ . We denote by  $\mathcal{Q}_c(K)$  the subset

$$\mathcal{Q}_c(K) = \bigcup_{\ell \in \mathcal{L}_c} \{\ell p^{k f(p)} : p\mathbb{Z} \text{ unramified}, k \leq c\}.$$

Similarly, let  $\mathcal{R}_c(K) \subset \mathcal{N}_c(K)$  be the corresponding set of elements where  $p\mathbb{Z}$  is ramified in  $\mathfrak{D}$ . Since there are only finitely many prime ideals  $p\mathbb{Z}$  that are ramified in  $\mathfrak{D}$ , the cardinality of the set  $\mathcal{R}_c(K)$  is finite. By definition,  $\mathcal{N}_c(K) = \mathcal{Q}_c(K) \cup \mathcal{R}_c(K)$ .

Our main result is the following theorem.

**Theorem 4.1.** *Fix  $c \in \mathbb{N}$ . Given  $(u_n)$  as above, one can decide whether there is an  $n \in \mathcal{N}_c(K)$  such that  $u_n = 0$ .*

Since the set  $\mathcal{R}_c(K)$  is finite, locating zero terms  $u_n = 0$  for  $n \in \mathcal{R}_c(K)$  is clearly decidable. So to prove Theorem 4.1 it is sufficient to prove the next theorem.

**Theorem 4.2.** *Fix  $c \in \mathbb{N}$ . Given  $(u_n)$  as above, one can decide whether there is an  $n \in \mathcal{Q}_c(K)$  such that  $u_n = 0$ .*

In order to prove Theorem 4.2, we first prove two technical results. The first, Lemma 4.3, concerns elements of cosets of  $p\mathfrak{D}$  in  $\mathfrak{D}$ . The second, Lemma 4.4, plays an analogous rôle to that of Lemma 3.4 in Section 3.



**Lemma 4.3.** *Suppose that  $\varphi \in \mathfrak{D}$  and  $p\mathbb{Z}$  is non-zero prime ideal. If  $p\mathbb{Z}$  is unramified with inertial degree  $f(p)$  then  $\varphi^{p^{f(p)}} - \varphi \in p\mathfrak{D}$ .*

*Proof.* Write  $p\mathfrak{D} = \mathfrak{p}_1 \cdots \mathfrak{p}_g$  for the unique factorisation of  $p\mathfrak{D}$  as a product of the distinct prime ideals  $\mathfrak{p}_i$  lying above  $p\mathbb{Z}$ . Here the ramification index is unity because  $p\mathbb{Z}$  is unramified. By Theorem 2.1, for each  $i \in \{1, \dots, g\}$  and  $\varphi \in \mathfrak{D}$  we have  $\varphi^{N(\mathfrak{p}_i)} - \varphi \in \mathfrak{p}_i$ . Since each of the exponents satisfy  $N(\mathfrak{p}_i) = p^{f(p)}$ , we deduce that  $\varphi^{p^{f(p)}} - \varphi \in \cap_i \mathfrak{p}_i$ . Because the distinct prime ideals  $\mathfrak{p}_i$  are pairwise co-prime, we have  $\cap_i \mathfrak{p}_i = \mathfrak{p}_1 \cdots \mathfrak{p}_g = p\mathfrak{D}$  and hence we have the desired result.  $\square$

**Lemma 4.4.** *Let  $(u_n)$  be a recurrence sequence and  $(v_n)$  the associated simple recurrence sequence as above. Let  $p \in \mathbb{N}$  be a rational prime and  $k, \ell \in \mathbb{N}$ . If  $p\mathbb{Z} \subset \mathfrak{D}$  is unramified with inertial degree  $f(p)$  then  $v_\ell - u_{\ell p^{kf(p)}} \in p\mathfrak{D}$ .*

*Proof.* The result is a consequence of the next congruences

$$v_\ell \equiv v_{\ell p^{kf(p)}} \equiv u_{\ell p^{kf(p)}} \pmod{p\mathfrak{D}}.$$

The congruences hold trivially when  $k = 0$ . We shall prove the case  $k = 1$  below and omit the case  $k > 1$  as it follows similarly. The first congruence is a simple application of Lemma 4.3:

$$v_\ell = \sum_{j=1}^m A_j(0) \lambda_j^\ell \equiv \sum_{j=1}^m A_j(0) \lambda_j^{\ell p^{f(p)}} = v_{\ell p^{f(p)}} \pmod{p\mathfrak{D}}.$$

Recall that for  $A \in \mathfrak{D}[x]$  we have  $(x-y)|(A(x)-A(y))$ . The second congruence holds since  $p\mathfrak{D} \ni \ell p^{f(p)}|(A(\ell p^{f(p)}) - A(0))$  or equivalently  $A(0) \equiv A(\ell p^{f(p)}) \pmod{p\mathfrak{D}}$  for each  $A \in \mathfrak{D}[x]$ . Thus

$$v_{\ell p^{f(p)}} \equiv \sum_{j=1}^m A_j(\ell p^{f(p)}) \lambda_j^{\ell p^{f(p)}} = u_{\ell p^{f(p)}} \pmod{p\mathfrak{D}}.$$

Hence  $v_\ell - u_{\ell p^{f(p)}} \in p\mathfrak{D}$  as desired.  $\square$

*Proof of Theorem 4.2.* Fix  $c \in \mathbb{N}$  and assume that  $n \in \mathcal{Q}_c(K)$  such that  $u_n = 0$ . Then  $n$  is of the form  $\ell p^{kf(p)}$  where  $p$  is a prime and  $p\mathbb{Z} \subset \mathfrak{D}$  is unramified. By Lemma 4.4,  $v_\ell - u_{\ell p^{kf(p)}} \in p\mathfrak{D}$ . Thus  $v_\ell \in p\mathfrak{D}$  and therefore  $p\mathfrak{D} | v_\ell \mathfrak{D}$ . We then apply Lemma 3.2 to give an effective bound on the primes by a divisibility argument for  $N(v_\ell \mathfrak{D})$ . Hence the result.  $\square$

Our approach in the proof of Theorem 4.1 extends in the following way: we can decide whether there exists there is an  $n = \sum_{j=1}^t l_j p^{k_j f(p)}$  such that  $u_n = 0$ . Here the constants  $k_j, l_j \in \mathbb{N}$  are bounded independently of the rational prime  $p$ , and  $f(p)$  is the inertial degree of  $p\mathbb{Z} \subset \mathfrak{D}$ . For  $l_1, \dots, l_t, k_1, \dots, k_t \in \mathbb{N}$ , we define

$$S_m = S_m(l_j; k_j) := \begin{cases} \sum_{j=1}^t l_j m^{k_j f(p)} & \text{if } m \text{ is prime,} \\ \sum_{j=1}^t l_j & \text{if } m = 1. \end{cases}$$

Fix  $c \in \mathbb{N}$  and, as before, let  $\mathcal{L}_c = \{\ell \in \mathbb{N} : \ell \leq c, v_\ell \neq 0\}$ . Define the set  $\mathcal{N}'_c(K)$  as follows

$$\mathcal{N}'_c(K) = \bigcup_{S_1 \in \mathcal{L}_c} \{S_p(l_j; k_j) : p \text{ prime, } k_j \leq c\}.$$

We define the sets  $\mathcal{Q}'_c(K)$ , for unramified  $p\mathbb{Z}$  in  $K$ , and  $\mathcal{R}'_c(K)$ , for ramified  $p\mathbb{Z}$  in  $K$ , in an analogous manner to the sets  $\mathcal{Q}_c(K)$  and  $\mathcal{R}_c(K)$  associated to  $\mathcal{N}_c(K)$ . Then, like before,  $\mathcal{N}'_c(K) = \mathcal{Q}'_c(K) \cup \mathcal{R}'_c(K)$  and  $\mathcal{R}'_c(K)$  has finite cardinality.

We have the next decidability result.

**Theorem 4.5.** Fix  $c \in \mathbb{N}$ . Then, given  $(u_n)$  as above, one can decide whether there is an  $n \in \mathcal{N}'_c(K)$  such that  $u_n = 0$ .

The proof of Theorem 4.5 follows the approach in the proof of Theorem 4.1. Since the cardinality of  $\mathcal{R}'_c(K)$  is finite, we need only prove the next theorem in order to prove Theorem 4.5.

**Theorem 4.6.** Fix  $c \in \mathbb{N}$ . Then, given  $(u_n)$  as above, one can decide whether there is an  $n \in \mathcal{Q}'_c(K)$  such that  $u_n = 0$ .

Given its similarities to the proof of Theorem 4.2, we omit a formal proof of Theorem 4.6; instead, we outline the key steps in the proof. We require the following technical lemma; Lemma 4.7 generalises the result in Lemma 4.4.

**Lemma 4.7.** Let  $(u_n)$  be a recurrence sequence and  $(v_n)$  the associated simple recurrence sequence as above. Let  $p \in \mathbb{N}$  be a rational prime and  $S_p(l_j; k_j)$  be defined as above. If  $p\mathbb{Z} \subset \mathfrak{D}$  is unramified then  $u_{S_p} - v_{S_1} \in p\mathfrak{D}$ .

*Proof.* We avoid repeating the proof of Lemma 4.4 by limiting our presentation to the next two observations. First, for each polynomial  $A \in \mathfrak{D}[x]$  we have  $A(S_p) - A(0) \in p\mathfrak{D}$  since  $p\mathfrak{D} \ni S_p$  divides  $A(S_p) - A(0)$ . Second, by repeated application of Lemma 4.3, we have  $\lambda^{S_p} - \lambda^{S_1} \in p\mathfrak{D}$  for  $\lambda \in \mathfrak{D}$ . From these observations, one can obtain the congruences  $v_{S_1} \equiv v_{S_p} \equiv u_{S_p} \pmod{p\mathfrak{D}}$  and hence the desired result.  $\square$

We sketch the key steps in the proof of Theorem 4.6.

*Proof of Theorem 4.6.* Fix  $c \in \mathbb{N}$ . Assume that  $u_{S_p} = 0$  for some  $S_p(l_j; k_j) \in \mathcal{N}'_c(K)$  where  $p\mathbb{Z} \subset \mathfrak{D}$  is an unramified prime. Note that  $v_{S_1} \neq 0$  since  $S_p(l_j; k_j) \in \mathcal{N}'_c(K)$ . Then, by Lemma 4.7,  $v_{S_1} \in p\mathfrak{D}$  and so  $p\mathfrak{D} | v_{S_1}\mathfrak{D}$ . By Lemma 3.2,  $p$  necessarily divides  $N(v_{S_1}\mathfrak{D})$ . Since  $N(v_{S_1}\mathfrak{D})$  is computable, one can derive an effective bound on the rational primes  $p$  such that  $u_{S_p} = 0$ .  $\square$

## 5. HARDNESS RESULT

In [3], Blondel and Portier proved that the Skolem Problem is NP-hard (see also [1]). In this section we show that the prime variant of the Skolem Problem is likewise NP-hard. Following [1], our proof is by reduction from the *Subset Sum Problem*: given a finite set of integer  $A = \{a_1, \dots, a_m\}$  and  $b \in \mathbb{Z}$  a target, written in binary, decide whether there is a subset  $S \subseteq \{1, \dots, m\}$  such that  $\sum_{k \in S} a_k = b$ .

Let us state two well-known theorems in number theory in order to derive a simple corollary that is fundamental to our proof of Theorem 5.6.

**Theorem 5.1** (Chinese remainder theorem). Let  $n_1, \dots, n_m$  be positive integers that are pairwise co-prime. Then the system of  $m$  equations  $r \equiv a_k \pmod{n_k}$  with each  $a_k \in \mathbb{Z}$  has a unique solution modulo  $N$  where  $N = n_1 n_2 \cdots n_m$ .

Dirichlet proved the following theorem on primes in arithmetic progressions. We use the notation  $(m, n)$  to indicate the greatest common divisor of  $m, n \in \mathbb{Z}$ .

**Theorem 5.2.** Suppose that  $q$  and  $r$  are co-prime positive integers. Then there are infinitely many primes of the form  $\ell q + r$  with  $\ell \in \mathbb{N}$ .

The next corollary is immediate.

**Corollary 5.3.** Let  $p_1, \dots, p_m$  be a finite set of distinct primes. Then the system of  $m$  equations  $r \equiv a_k \pmod{p_k}$  with each  $a_k \in \mathbb{Z}$  has a unique solution  $r \in \{0, 1, \dots, P-1\}$  where  $P = p_1 p_2 \cdots p_m$ . Additionally, if  $(r, P) = 1$  then there are infinitely many  $\ell \in \mathbb{N}$  for which  $\ell P + r$  is prime.

Recall that the  $n$ th cyclotomic polynomial given by

$$\Phi_n(x) = \prod_{\substack{k \in \{1, \dots, n\} \\ (k, n) = 1}} (x - e^{2\pi i k/n})$$

is the minimal polynomial over  $\mathbb{Q}$  of a primitive  $n$ th root of unity.

We call an integer linear recurrence sequence *cyclotomic* if its characteristic roots are all roots of unity. The next theorem, concerning Skolem's Problem in the restricted setting of cyclotomic sequences, follows from work in [1]. We reproduce the proof as a lead into our original work on the Skolem Problem restricted to prime numbers.

**Theorem 5.4.** *The cyclotomic Skolem Problem is NP-hard.*

The proof of Theorem 5.4 is by reduction from the Subset Sum Problem and follows directly from the technical lemma, Lemma 5.5, below. Before we present the proof, we introduce some notation.

Let  $\{p_1, \dots, p_m\}$  be the set of the first  $m$  prime numbers. We define the linear recurrence sequence  $(s_k(n))_{n=0}^{\infty}$  with  $k \in \{1, \dots, m\}$  as follows. Let  $s_k(n) = s_k(n - p_k)$  for  $n \geq p_k$  with initial conditions  $s_k(0) = 1$ ,  $s_k(1) = \dots = s_k(p_k - 1) = 0$ . Then each sequence  $(s_k(n))$  is periodic with period  $p_k$ . The characteristic polynomial associated to  $(s_k(n))$  is given by

$$x^{p_k} - 1 = \prod_{\ell=0}^{p_k-1} (x - e^{2\pi i \ell/p_k}).$$

Thus  $(s_k(n))$  is a cyclotomic sequence.

In order to reduce the Subset Sum Problem to the cyclotomic Skolem Problem, we consider the inhomogeneous linear recurrence sequence  $(t(n))_{n=0}^{\infty}$  with terms given by  $t(n) = b - \sum_{k=1}^m a_k s_k(n)$ . The characteristic polynomial associated to  $(t(n))$  is given by the least common multiple of

$$(x^{p_1} - 1)(x - 1), x^{p_2} - 1, \dots, x^{p_m} - 1$$

(see [6]), from which it follows that each of the characteristic roots of  $(t(n))$  are themselves roots of unity, i.e.,  $(t(n))$  is a cyclotomic sequence.

**Lemma 5.5.** *For  $(t(n))$  given as above, there exists  $N \in \mathbb{N}$  such that  $t(N) = 0$  if and only if the Subset Sum Problem with inputs  $\{a_1, \dots, a_m; b\}$  has a solution.*

*Proof.* Suppose that there exists an  $N \in \mathbb{N}$  such that  $t(N) = 0$ , then the Subset Sum Problem has a solution because the selectors  $s_k(n)$  are  $\{0, 1\}$ -valued. Conversely, suppose that there is a subset  $S \subseteq \{1, \dots, m\}$  such that  $\sum_{k \in S} a_k = b$  and define  $N = \prod_{k \in S} p_k$ . We have  $s_k(N) = 1$  for each  $k \in S$  since  $p_k \mid N$ , and  $s_k(N) = 0$  otherwise. Thus

$$t(N) = b - \sum_{k=1}^m a_k s_k(N) = b - \sum_{k \in S} a_k = 0,$$

as required.  $\square$

We prove the following complexity result for the Skolem Problem for primes.

**Theorem 5.6.** *Suppose that  $(u_n)$  is a cyclotomic integer linear recurrence sequence. The problem of deciding whether there is a prime  $p \in \mathbb{N}$  such that  $u_p = 0$  is NP-hard.*

The proof of Theorem 5.6 involves an analysis of the NP-hardness proof for Skolem's Problem. Technically we will derive the result from Lemma 5.7, below.

Let  $p_1, \dots, p_m$  be the first  $m$  odd primes. We define selector sequences  $(\sigma_k(n))$  with  $k \in \{1, \dots, m\}$  as follows. Let  $\sigma_k(n) = \sigma_k(n - p_k)$  for  $n \geq p_k$  with initial

conditions  $\sigma_k(1) = 1, \sigma_k(0) = \sigma_k(2) = \dots = \sigma_k(p_k - 1) = 0$ . Then each sequence  $(\sigma_k(n))$  is periodic with period  $p_k$ . Let  $\tau(n) = b - \sum_{k=1}^m a_k \sigma_k(n)$ . It is easily shown that  $(\sigma_k(n))$  and  $(\tau(n))$  are cyclotomic recurrence sequences.

**Lemma 5.7.** *There exists an odd prime  $p \in \mathbb{N}$  such that  $\tau(p) = 0$  if and only if there exists a subset  $S \subseteq \{1, \dots, m\}$  that is a solution to the Subset Sum Problem with inputs  $\{a_1, \dots, a_m; b\}$ .*

*Proof.* Suppose that there is an odd prime  $p \in \mathbb{N}$  such that  $\tau(p) = 0$ . Then there is a solution to the Subset Sum Problem as  $\sigma_k(p) \in \{0, 1\}$  for each  $k$ .

Conversely, suppose that there a subset  $S \subseteq \{1, \dots, m\}$  such that  $\sum_{k \in S} a_k = b$ . Consider the set  $Q(S) \subseteq \mathbb{Z}$  of integer solutions to the set of  $m$  equations

$$\begin{cases} r \equiv 1 \pmod{p_k} & \text{if } k \in S, \text{ and} \\ r \equiv 2 \pmod{p_k} & \text{if } k \in \{1, \dots, m\} \setminus S. \end{cases}$$

The choice of residue ensures that  $r$  is not divisible by any of the primes  $p_1, p_2, \dots, p_m$ . By the Chinese Remainder Theorem,  $Q(S)$  is an infinite arithmetic progression. Suppose that  $q \in Q(S)$ . Then, by definition of the selector sequences,  $\sigma_k(q) = 1$  if and only if  $q \equiv 1 \pmod{p_k}$  if and only if  $k \in S$ . Then

$$\tau(q) = b - \sum_{k=1}^m a_k \sigma_k(q) = b - \sum_{k \in S} a_k = 0.$$

It remains to show that there is a prime number in  $Q(S)$ . This result follows easily from Corollary 5.3, which completes the proof.  $\square$

## 6. SUMMARY

In this paper we have given decision procedures for finding zeroes of certain prescribed linear recurrence sequences. Our main result shows how to decide the existence of a prime  $p$  such that  $u_p = 0$  for a simple linear recurrence sequence  $(u_n)$ . We have noted that this decision problem is NP-hard and, implicitly, that the magnitude of the smallest prime  $p$  such that  $u_p = 0$  is at least exponential in the size of the problem instance. On the other hand, our decision procedure yields a double exponential bound on the magnitude of the prime  $p$ . Closing this exponential gap would be an interesting direction for further work. Another direction for research would be to locate zeroes  $u_n = 0$  where the index  $n \in \mathbb{N}$  has two prime factors.

## REFERENCES

- [1] S. Akshay, Nikhil Balaji, and Nikhil Vyas. Complexity of Restricted Variants of Skolem and Related Problems. In K. Larsen, H. Bodlaender, and J-F. Raskin, editors, *42nd International Symposium on Mathematical Foundations of Computer Science (MFCS 2017)*, volume 83 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 78:1–78:14, Dagstuhl, Germany, 2017. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik. doi:10.4230/LIPIcs.MFCS.2017.78.
- [2] Jean Berstel and Maurice Mignotte. Deux propriétés décidables des suites récurrentes linéaires. *Bulletin de la Société Mathématique de France*, 104(2):175–184, 1976.
- [3] Vincent D. Blondel and Natacha Portier. The presence of a zero in an integer linear recurrent sequence is NP-hard to decide. *Linear Algebra Appl.*, 351/352:91–98, 2002. Fourth special issue on linear systems and control. doi:10.1016/S0024-3795(01)00466-9.
- [4] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.
- [5] Harm Derksen. A Skolem-Mahler-Lech theorem in positive characteristic and finite automata. *Inventiones Mathematicae*, 168(1):175–224, 2007.
- [6] Graham Everest, Alf van der Poorten, Igor Shparlinski, and Thomas Ward. *Recurrence sequences*, volume 104 of *Mathematical Surveys and Monographs*. Amer. Math. Soc., Providence, RI, 2003.
- [7] Vesa Halava, Tero Harju, Mika Hirvensalo, and Juhani Karhumäki. Skolem’s problem—on the border between decidability and undecidability. Technical report, Turku Centre for Computer Science, 2005.

- [8] Christer Lech. A note on recurring series. *Arkiv för Matematik*, 2:417–421, 1953.
- [9] K. Mahler. Eine arithmetische Eigenschaft der Taylor-koeffizienten rationaler Funktionen. *Proc. Akad. Wet. Amst.*, 38:50–69, 1935.
- [10] K. Mahler and J. Cassels. On the Taylor coefficients of rational functions. *Mathematical Proceedings of the Cambridge Philosophical Society*, 52(1):39–48, 1956.
- [11] Maurice Mignotte, Tarlok Shorey, and Robert Tijdeman. The distance between terms of an algebraic recurrence sequence. *Journal für die Reine und Angewandte Mathematik*, pages 63–76, 1984.
- [12] Joël Ouaknine and James Worrell. Decision problems for linear recurrence sequences. In *Reachability problems*, volume 7550 of *Lecture Notes in Computer Science*, pages 21–28. Springer, Heidelberg, 2012.
- [13] Joël Ouaknine and James Worrell. On linear recurrence sequences and loop termination. *ACM SIGLOG News*, 2(2):4–13, April 2015.
- [14] Thoralf Skolem. Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen und diophantischer Gleichungen. *8de Skand. Mat. Kongress, Stockholm (1934)*, pages 163–188, 1934.
- [15] Nikolai Vereshchagin. Occurrence of zero in a linear recursive sequence. *Mathematical notes of the Academy of Sciences of the USSR*, 38(2):609–615, Aug 1985.

GEORGE KENISON, DEPARTMENT OF COMPUTER SCIENCE, UNIVERSITY OF OXFORD, OXFORD, UK.  
E-mail address: `george.kenison@cs.ox.ac.uk`

RICHARD LIPTON, GEORGIA INSTITUTE OF TECHNOLOGY, ATLANTA, USA.  
E-mail address: `richard.lipton@cc.gatech.edu`

JOËL OUAKNINE, MAX PLANCK INSTITUTE FOR SOFTWARE SYSTEMS, SAARBRÜCKEN, GERMANY.  
E-mail address: `joel@mpi-sws.org`

JAMES WORRELL, DEPARTMENT OF COMPUTER SCIENCE, UNIVERSITY OF OXFORD, OXFORD, UK.  
E-mail address: `jbw@cs.ox.ac.uk`