Twisted rational zeros of linear recurrence sequences

Yuri Bilu
IMB, Université de Bordeaux & CNRS
E-mail: yuri@math.u-bordeaux.fr,

Florian Luca
School of Maths, Wits, South Africa
CCM, UNAM, Morelia, Mexico
E-mail: Florian.Luca@wits.ac.za,

Joris Nieuwveld and Joël Ouaknine
Max Planck Institute for Software Systems, Germany
E-mail: jnieuwve@mpi-sws.org; joel@mpi-sws.org,

James Worrell
Department of Computer Science, Oxford University, UK
Email: jbw@cs.ox.ac.uk

version of December 18, 2023

Abstract

We introduce the notion of a twisted rational zero of a non-degenerate linear recurrence sequence (LRS). We show that any non-degenerate LRS has only finitely many such twisted rational zeros. In the particular case of the Tribonacci sequence, we show that $1/3$ and $-5/3$ are the only twisted rational zeros which are not integral zeros.

Contents

1 Introduction

Let $\mathbb{K}$ be a field of characteristic 0. We fix an algebraic closure $\overline{\mathbb{K}}$. By a $\mathbb{K}$-*valued linear recurrence sequence* (LRS) of order m we mean a map $U : \mathbb{Z} \to \mathbb{K}$ such that for every $n \in \mathbb{Z}$ we have

$$U(n+m) = a_{m-1}U(n+m-1) + \cdots + a_0U(n), \tag{1.1}$$

where $a_0, \ldots, a_{m-1} \in \mathbb{K}$, with $a_0 \neq 0$. Sometimes instead of "$\mathbb{K}$-valued LRS" we will say "LRS over $\mathbb{K}$".

1.1 Twisted zeros and p-adic orders

Our initial motivation was the work of Marques and Lengyel [17], who computed the 2-adic order of the n^{th} Tribonacci number $T(n)$. The *Tribonacci numbers* is the $\mathbb{Q}$-valued LRS of order 3, defined by

$$T(0) = 0, \quad T(1) = T(2) = 1, \quad T(n+3) = T(n+2) + T(n+1) + T(n).$$

Marques and Lengyel proved that

$$\nu_2(T(n)) = \begin{cases} 0, & \text{if } n \equiv 1, 2 \pmod 4; \\ 1, & \text{if } n \equiv 3, 11 \pmod{16}; \\ 2, & \text{if } n \equiv 4, 8 \pmod{16}; \\ 3, & \text{if } n \equiv 7 \pmod{16}; \\ \nu_2(n) - 1, & \text{if } n \equiv 0 \pmod{16}; \\ \nu_2(n+4) - 1, & \text{if } n \equiv 12 \pmod{16}; \\ \nu_2(n+17) + 1, & \text{if } n \equiv 15 \pmod{32}; \\ \nu_2(n+1) + 1, & \text{if } n \equiv 31 \pmod{32}. \end{cases} \tag{1.2}$$

They conjectured that similar formulas must hold for other primes, not just for $p = 2$. This conjecture was refuted in [5], where it is shown that having formulas like (1.2) is exceptional rather than typical.

As one can see in (1.2), on certain residue classes one has formulas like $\nu_2(T(n)) = \nu_2(n-a) + \text{const}$, where a is one of the numbers $0, -1, -4, -17$. This not surprising, because these numbers are exactly the zeros of T: for $n \in \mathbb{Z}$ we have

$$T(n) = 0 \quad \text{if and only if} \quad n \in \{0, -1, -4, -17\}.$$

(For a proof see, for instance, [18], Example 2 on page 360; in that example u_n corresponds to our $T(-n)$.)

Let U be a $\mathbb{Q}$-valued LRS; in particular, the coefficients $a_0, \dots, a_{m-1}$ of the recurrence relation (1.1) belong to $\mathbb{Q}$. We call p a *regular prime* for U if it does not divide the denominators of the rational numbers $a_0, \dots, a_{m-1}$, and the numerator of a_0. In other words, $a_0, \dots, a_{m-1}$ are p-adic integers and a_0 is a p-adic unit.

The following theorem can be easily proved, using p-adic analysis, see Section 3.

Theorem 1.1. *Let a be a zero of a $\mathbb{Q}$-valued LRS U, and p a regular prime for U. Then there exist a positive integer Q, a positive integer κ and an integer τ such that*

$$\nu_p(U(n)) = \kappa\nu_p(n-a) + \tau \qquad \textit{when} \quad n \equiv a \pmod{Q} \tag{1.3}$$

Of course the converse also holds: if for some p there exist Q, κ, τ as above such that (1.3) holds, then a is a zero of U.

Now let us ask the following slightly more general question: what would happen if we take n in (1.3) not from the residue class of a modulo Q, but from a different residue class?

Question 1.2. *Let p be a prime number. Assume that there exist*

$$Q \in \mathbb{Z}_{>0}, \qquad a' \in \{0, 1, \dots, Q-1\}, \qquad \kappa \in \mathbb{Z}_{>0}, \qquad \tau \in \mathbb{Z}$$

such that

$$\nu_p(U(n)) = \kappa\nu_p(n-a) + \tau \qquad \textit{when} \quad n \equiv a' \pmod{Q}.$$

Assume further that $\nu_p(n-a)$ is not bounded on the residue class of a' modulo Q. Does it imply that $a' \equiv a \pmod{Q}$ and $U(a) = 0$?

As the result of Marques and Lengyel implies, it is indeed the case when $U = T$ and $p = 2$. But is it true in general?

The answer is "no", as the following example shows.

Example 1.3. *Consider $U(n) := 2^n + 1$ and let p be a prime number satisfying $p \equiv \pm 3 \pmod 8$. Then $2^{(p-1)/2} + 1 \equiv 0 \pmod p$. Define $\tau := \nu_p(2^{(p-1)/2} + 1)$. Then*

$$\nu_p(U(n)) = \nu_p(n) + \tau \quad \textit{when} \quad n \equiv \frac{p-1}{2} \pmod{p-1}.$$

However, $U(0) \neq 0$, and in fact $U(n)$ does not vanish at all.

The explanation is that 0 is, in fact, a kind of "hidden" zero of the LRS $2^n + 1$. To give an exact definition, recall that a $\mathbb{K}$-valued LRS U satisfying (1.1) admits the *Binet expansion*

$$U(n) = f_1(n)\lambda_1^n + \cdots + f_s(n)\lambda_s^n \qquad (n \in \mathbb{Z}), \tag{1.4}$$

where $\lambda_1, \ldots, \lambda_s$ are the distinct roots of the characteristic polynomial

$$X^m - a_{m-1}X^{m-1} - \cdots - a_0,$$

and $f_1, \ldots, f_s$ are polynomials with coefficients in the field $\mathbb{K}(\lambda_1, \ldots, \lambda_s)$. (Note that the roots λ_i are non-zero, because $a_0 \neq 0$.) We call $a \in \mathbb{Z}$ a *twisted zero* of the $\mathbb{K}$-valued LRS U if there exist roots of unity $\xi_1, \ldots, \xi_s \in \overline{\mathbb{K}}$ such that

$$\xi_1 f_1(a)\lambda_1^a + \cdots + \xi_s f_s(a)\lambda_s^a = 0.$$

For example, 0 is a twisted zero of the LRS with general term $2^n + 1^n$, because

$$1 \cdot 2^0 + (-1) \cdot 1^0 = 0.$$

In Section 3 we will prove the following theorem, which gives a partial positive answer to Question 1.2.

Theorem 1.4. *Let U be a $\mathbb{Q}$-valued LRS, $a \in \mathbb{Z}$ and p a regular prime number for U. Assume that there exists a sequence of integers (n_k) satisfying*

$$\nu_p(U(n_k)) \to +\infty, \qquad \nu_p(n_k - a) \to +\infty.$$

Then a is a twisted zero of U.

There is another phenomenon discovered in [5], again in the context of Tribonacci numbers. There exist infinitely many prime numbers p such that $\nu_p(T(n)) \geq \nu_p(n - 1/3)$ for $n \equiv 1/3 \pmod{p-1}$, and the same holds true with $1/3$ replaced by $-5/3$; see [5, Theorem 1.5]. The reason is that $1/3$ and $-5/3$ can be viewed as "rational zeros" of the LRS T, see [5, Section 2].

Let us give the general definition. We call $a \in \mathbb{Q}$ a *rational zero* of the $\mathbb{K}$-valued LRS U with Binet expansion (1.4) if, for some definition of the rational powers $\lambda_1^a, \ldots, \lambda_s^a \in \overline{\mathbb{K}}$, we have

$$f_1(a)\lambda_1^a + \cdots + f_s(a)\lambda_s^a = 0.$$

We call a a *twisted rational zero* (TRZ) of U if, for some definition of $\lambda_1^a, \ldots, \lambda_s^a$ and some roots of unity $\xi_1, \ldots, \xi_s$, we have

$$\xi_1 f_1(a)\lambda_1^a + \cdots + \xi_s f_s(a)\lambda_s^a = 0.$$

Theorem 1.4 remains true assuming that $a \in \mathbb{Q}$.

Theorem 1.5. *Let U be a $\mathbb{Q}$-valued LRS, $a \in \mathbb{Q}$ and p a regular prime number for U. Assume that there exists a sequence of integers (n_k) satisfying*

$$\nu_p(U(n_k)) \to +\infty, \qquad \nu_p(n_k - a) \to +\infty. \tag{1.5}$$

Then a is a TRZ of U.

This theorem is proved in Section 3 as well.

One may ask whether the converse is true; that is, if a is a TRZ, then there exists a sequence of integers (n_k) satisfying (1.5). Easy examples show that the answer is "no" in general.

Example 1.6. *If $p \equiv -1 \pmod 8$ then $\nu_p(2^n + 1) = 0$ for all n, though 0 is a twisted zero of the LRS $2^n + 1^n$.*

One may still hope that, when a is a TRZ, this holds for infinitely many primes.

Question 1.7. *Let a be a TRZ of a non-degenerate $\mathbb{Q}$-valued LRS U. Are there infinitely many prime numbers p with the following property: there exists a sequence of integers (n_k) satisfying (1.5)?*

We show that the answer is "yes" for twisted **integral** zeros of LRS of order 2; in fact, we will show that for them an analogue of Theorem 1.1 holds. However, we do not know the answer for rational zeros. As for LRS of higher order, the answer is, in general, "no" even for integral twisted zeros. See Section 6 for the details.

1.2 Finiteness

Call a non-zero LRS with roots $\lambda_1, \dots, \lambda_s$ *non-degenerate* if λ_k/λ_ℓ is not a root of unity for $k \neq \ell$. The following statement is the classical *Skolem-Mahler-Lech Theorem.*

Theorem 1.8 (Skolem-Mahler-Lech)**.** *A non-degenerate linear recurrence sequence U over a field of characteristic 0 has at most finitely many zeros:*

$$\#\{n \in \mathbb{Z} : U(n) = 0\} < \infty.$$

In Section 4 we prove that the same holds true for TRZs.

Theorem 1.9. *Let U be a non-degenerate linear recurrence sequence with values in a field of characteristic zero. Then U admits at most finitely many TRZs.*

The proof is a variation of the principal argument of Laurent's article [14]. The main step is bounding the denominators of the TRZs; moreover, the bound is effective if $\mathbb{K}$ is a number field. After the denominators are bounded, Theorem 1.9 can be reduced to the Skolem-Mahler-Lech theorem using the existing results about equations in roots of unity [10, 11, 16].

The Skolem-Mahler-Lech Theorem is, in general, non-effective, and so is our Theorem 1.9: while we bound effectively the denominators of the TRZs, we cannot do the same for their numerators. However, the Skolem-Mahler-Lech Theorem can be made effective in many special cases, and so can be Theorem 1.9. To illustrate this, we prove (see Section 5) the following.

Theorem 1.10. *The only TRZs of the Tribonacci sequence T are*

$$0, -1, -4, -17, \frac{1}{3}, -\frac{5}{3}.$$

2 Preliminaries

In this section we collect some basic facts and conventions that will be used throughout the article, usually without special reference.

2.1 Fields

The letter p denotes a prime number, and blackboard boldface letters $\mathbb{K}, \mathbb{L}, \mathbb{M}$ etc. denote (unless indicated otherwise) fields of characteristic 0. In particular, they can be number fields or local fields (finite extensions of $\mathbb{Q}_p$). If $\mathbb{K}$ is a number field and $\mathfrak{p}$ is a prime of $\mathbb{K}$ then $\mathbb{K}_\mathfrak{p}$ denotes the $\mathfrak{p}$-adic completion.

For every positive integer m we fix a primitive root of unity of order m and denote it ζ_m. We denote by μ_m the group of roots of unity of order m. Given a field $\mathbb{K}$, we denote by $\mu_\mathbb{K}$ the group of roots of unity belonging to $\mathbb{K}$.

The following lemma, which is Theorem 9.1 in [13, Chapter VI], will be used in the article on several occasions.

Lemma 2.1. *Let $\mathbb{K}$ be a field of characteristic 0 and $\alpha \in \mathbb{K}^\times$. Let m be a positive integer. Assume that*

$$\text{for all } p \mid m \text{ we have } \alpha \notin \mathbb{K}^p, \tag{2.1}$$

$$\text{when } 4 \mid m \text{ we have } \alpha \notin -4\mathbb{K}^4. \tag{2.2}$$

Then the polynomial $X^m - \alpha$ is irreducible in $\mathbb{K}[X]$.

Remark 2.2. *If $\sqrt{-1} \in \mathbb{K}$ then assumption (2.2) can be omitted, because in this case $-4 \in \mathbb{K}^4$ and (2.2) follows from (2.1).*

2.2 Linear recurrence sequences

Let U be an LRS with values in a field $\mathbb{K}$. We call m the *minimal order* of U if U admits a linear recurrence relation of order m, but not of order strictly smaller than m. By convention, the minimal order of the identically zero LRS is set to be 0.

Let m be the minimal order of a (non-zero) LRS U with values in $\mathbb{K}$. Then the coefficients $a_0, \dots, a_{m-1}$ of the recurrence relation

$$U(n+m) = a_{m-1}U(n+m-1) + \cdots + a_0 U(n)$$

are well-defined and belong to the field $\mathbb{K}$. Fix an algebraic closure $\overline{\mathbb{K}}$, and let $\lambda_1, \dots, \lambda_s \in \overline{\mathbb{K}}$ be the distinct roots of the characteristic polynomial

$$X^m - a_{m-1}X^{m-1} - \cdots - a_0. \tag{2.3}$$

Then U admits the Binet expansion

$$U(n) = f_1(n)\lambda_1^n + \cdots + f_s(n)\lambda_s^n,$$

where $f_1, \dots, f_s$ are polynomials with coefficients in the field $\mathbb{K}(\lambda_1, \dots, \lambda_s)$, such that the order of λ_i as a root of the characteristic polynomial (2.3) is equal to $\deg f_i + 1$. In particular, the polynomials f_i are all non-zero, and

$$\sum_{i=1}^{s} (\deg f_i + 1) = m.$$

Unless the contrary is stated explicitly, in this article, when referring to an LRS of order m, we will assume that m is the minimal order of this LRS.

It is important to note the following: if U is non-degenerate then it does not vanish identically on any residue class; that is, for any positive integer N and any $\ell \in \{0, \dots, N-1\}$, the function $n \mapsto U(\ell + Nn)$ is not identically zero. Indeed, assuming non-degeneracy of U, the numbers $\lambda_1^N, \dots, \lambda_s^N$ are all distinct. Hence

$$U(\ell + Nn) = \sum_{i=1}^{s} h_i(n)\theta_i^n, \quad \text{where} \quad h_i(T) := \lambda_i^\ell f_i(\ell + NT), \quad \theta_i := \lambda_i^N.$$

This implies that $U(\ell + Nn)$ is an LRS of the same minimal order as U; in particular, it is not identically zero.

3 Twisted rational zeros and the p-adic order

In this section we prove Theorems 1.1, 1.4 and 1.5 from the Introduction. The proofs rely on Skolem's p-adic interpolation of LRS, briefly recalled in Subsections 3.1 and 3.2.

3.1 p-adic analytic functions

In this subsection we recall some very basic facts about p-adic analytic functions. Most of them are quite standard. All missing proofs, unless indicated otherwise, can be found in any standard text like [12] or [19].

Let p be a prime number. We fix an algebraic closure $\overline{\mathbb{Q}_p}$, and extend the standard p-adic absolute value $|\cdot|_p$ to $\overline{\mathbb{Q}_p}$, so that $|p|_p = p^{-1}$. We will also use the additive valuation ν_p defined by $\nu_p(z) = -\log|z|_p/\log p$ for $z \in \overline{\mathbb{Q}_p}^\times$, with the convention $\nu_p(0) = +\infty$. All algebraic extensions of $\mathbb{Q}_p$ occurring below will be viewed as subfields of this fixed $\overline{\mathbb{Q}_p}$.

Let $\mathbb{K}$ be a finite extension of $\mathbb{Q}_p$. For $a \in \mathbb{K}$ and $r > 0$ we denote $\mathcal{D}(a, r)$ and $\overline{\mathcal{D}}(a, r)$ (or $\mathcal{D}_{\mathbb{K}}(a, r)$, $\overline{\mathcal{D}_{\mathbb{K}}}(a, r)$, if we want to indicate that the disk is in the field $\mathbb{K}$) the open and the closed disks with center a and radius r:

$$\mathcal{D}(a, r) = \{z \in \mathbb{K} : |z - a|_p < r\}, \qquad \overline{\mathcal{D}}(a, r) = \{z \in \mathbb{K} : |z - a|_p \le r\}.$$

It might be worth noting that every open disk in $\mathbb{K}$ is also closed, and any closed disk is open. That is, for every $r > 0$ there exist $r', r'' > 0$ such that

$$\mathcal{D}(a, r) = \overline{\mathcal{D}}(a, r'), \qquad \overline{\mathcal{D}}(a, r) = \mathcal{D}(a, r'').$$

Another useful observation is that every point of a disk serves as its center: if $b \in \mathcal{D}(a,r)$ then $\mathcal{D}(a,r) = \mathcal{D}(b,r)$, and similarly for the closed disks.

We denote by $\mathcal{O}_{\mathbb{K}}$, or simply by $\mathcal{O}$ if this does not lead to a confusion, the ring of integers of $\mathbb{K}$:

$$\mathcal{O} = \{z \in \mathbb{K} : |z|_p \leq 1\} = \overline{\mathcal{D}}(0,1).$$

Let D be a disk in $\mathbb{K}$ (open or closed), and $\mathbb{L}$ a finite extension of $\mathbb{K}$. We call $g : D \to \mathbb{L}$ an analytic function if for some $a \in D$ we have

$$g(z) = \sum_{n=0}^{\infty} \alpha_n (z-a)^n \qquad (z \in D), \tag{3.1}$$

where $\alpha_0, \alpha_1, \alpha_2, \ldots \in \mathbb{L}$. In particular, the infinite sum on the right converges for all $z \in D$.

Here are some simple properties of analytic functions, to be used below without special reference.

1. The coefficients $\alpha_0, \alpha_1, \alpha_2, \ldots$ are well-defined as soon as g and a are given. In particular, if the coefficients are not all 0, then g is a non-zero function.

2. The analytic function g admits a power series expansion around any other $b \in D$. Specifically, for any $b \in \mathcal{O}$ we have

$$g(z) = \sum_{k=0}^{\infty} \beta_k (z-b)^k, \tag{3.2}$$

where

$$\beta_k = \frac{g^{(k)}(b)}{k!} = \sum_{n=k}^{\infty} \binom{n}{k} \alpha_n (b-a)^{n-k}.$$

3. An analytic function on D is bounded. Indeed, set

$$r := \max\{|z-w|_p : z, w \in D\}.$$

Then $D = \overline{\mathcal{D}}(a,r)$, and convergence in (3.1) is equivalent to $|\alpha_n|_p r^n \to 0$. In particular, the sequence $|\alpha_n|_p r^n$ is bounded. Hence $\alpha_n (z-a)^n$ is bounded uniformly in $z \in D$. It follows that g is bounded.

4. A non-zero analytic function on a disk D may have at most finitely many zeros in D; this is because D is compact and the zeros are isolated. A quantitative version is given by the classical Theorem of Strassmann; see, for instance, [8, Theorem 4.1].

Theorem 3.1. *Let $\mathbb{K}$ be a finite extension of $\mathbb{Q}_p$ of ramification index e, and let $g : \mathbb{Z}_p \to \mathbb{K}$ be an analytic function, not identically 0. Denote by $\mathcal{A}$ the (finite) set of zeros of g. Then there exists a positive integer k such that for every $i \in \{0, 1, \ldots, p^k - 1\}$ we have one of the following two options.*

(C) There exists $\tau_i \in \mathbb{Z}$ such that for $z \in \mathbb{Z}_p$ satisfying $z \equiv i \pmod{p^k}$ we have $\nu_p(g(z)) = e^{-1}\tau_i$; in other words, $\nu_p(g(z))$ is constant on the residue class $z \equiv i \pmod{p^k}$.

(L) There exist

$$a_i \in \mathcal{A}, \qquad \tau_i \in \mathbb{Z}, \qquad \kappa_i \in \mathbb{Z}_{>0}$$

such that $a_i \equiv i \pmod{p^k}$, and for $z \in \mathbb{Z}_p$ satisfying $z \equiv i \pmod{p^k}$ we have

$$\nu_p(g(z)) = \kappa_i \nu_p(z - a_i) + e^{-1}\tau_i.$$

Proof. This is Theorem 3.2 from [5]. □

We denote

$$\rho := p^{-1/(p-1)}. \tag{3.3}$$

Let us recall the definition and the basic properties of the p-adic exponential and logarithmic function.

1. For $z \in \mathcal{D}(0, \rho)$ we define

$$\exp(z) = \sum_{n=0}^{\infty} \frac{z^n}{n!}.$$

For $z, w \in \mathcal{D}(0, \rho)$ we have

$$|\exp(z) - 1|_p = |z|_p, \quad \exp(z + w) = \exp(z)\exp(w), \quad \exp'(z) = \exp(z).$$

2. For $z \in \mathcal{D}(1, 1)$ we define

$$\log(z) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}(z-1)^n}{n}.$$

For $z, w \in \mathcal{D}(1, 1)$ we have

$$\log(zw) = \log(z) + \log(w), \quad \log'(z) = \frac{1}{z}.$$

3. For $z \in \mathcal{D}(1, \rho)$ we have

$$|\log(z)|_p = |z - 1|_p, \quad \exp(\log(z)) = z.$$

4. For $z \in \mathcal{D}(0, \rho)$ we have $\log(\exp(z)) = z$.

3.2 p-adic analytic interpolation of a linear recurrence sequence

The contents of this subsection is very classical and goes back to Skolem. Still, we prefer to include some proofs for the reader's convenience.

Let U be a non-zero LRS of (minimal) order m with values in a number field $\mathbb{K}$. We write its recurrence relation as

$$U(n+m) = a_{m-1}U(n+m-1) + \cdots + a_0 U(n),$$

where $a_0, \ldots, a_{m-1} \in \mathbb{K}$.

We call a prime $\mathfrak{p}$ of $\mathbb{K}$ *regular* for U if $a_1, \ldots, a_m$ are $\mathfrak{p}$-adic integers and a_0 is a $\mathfrak{p}$-adic unit.

Let $\mathfrak{p}$ be a regular prime for U, and $\mathbb{K}_\mathfrak{p}$ the $\mathfrak{p}$-adic completion of $\mathbb{K}$. It is a finite extension of $\mathbb{Q}_p$, where p is the rational prime number below $\mathfrak{p}$.

Proposition 3.2 (Skolem)**.** *There exists a positive integer N and analytic functions*

$$g_0, \ldots, g_{N-1} : \mathbb{Z}_p \to \mathcal{O}_{\mathbb{K}_\mathfrak{p}}$$

such that

$$u(\ell + Nn) = g_\ell(n) \qquad (\ell \in \{0, \ldots, N-1\}, \quad n \in \mathbb{Z}). \tag{3.4}$$

Moreover, if the LRS U is non-degenerate, then none of the functions g_ℓ vanishes identically.

Proof. Denote by $\mathbb{L}$ the splitting field over $\mathbb{K}_\mathfrak{p}$ of the characteristic polynomial $X^m - a_{m-1}X^{m-1} - \cdots - a_0$. Then U admits the Binet expansion

$$U(n) = f_1(n)\lambda_1^n + \cdots + f_s(n)\lambda_s^n,$$

where $\lambda_1, \ldots, \lambda_s$ are the distinct roots of the characteristic polynomial, and $f_1, \ldots, f_s$ are non-zero polynomials with coefficients in $\mathbb{L}$. Since p is a regular prime, $\lambda_1, \ldots, \lambda_s \in \mathcal{O}_\mathbb{L}^\times$.

Let ρ be defined as in (3.3). Since $\rho < 1$, the disk $\mathcal{D}_\mathbb{L}(1, \rho)$ is a multiplicative group. It is a finite index subgroup of $\mathcal{O}_\mathbb{L}^\times$, because $\mathcal{O}_\mathbb{L}^\times$ is compact and $\mathcal{D}_\mathbb{L}(1, \rho)$ is open. Hence there exists a positive integer N such that $x^N \in \mathcal{D}_\mathbb{L}(1, \rho)$ for every $x \in \mathcal{O}_\mathbb{L}^\times$. Note that we have

$$x^{Nn} = \exp(n \log(x^N)) \qquad (x \in \mathcal{O}_\mathbb{L}^\times, \quad n \in \mathbb{Z}). \tag{3.5}$$

Now define, for $\ell = 0, 1, \ldots, N-1$ and $z \in \mathbb{Z}_p$,

$$g_\ell(z) := \sum_{i=1}^{s} \lambda_i^\ell f_i(\ell + Nz) \exp(z \log(\lambda_i^N)).$$

Note that, *a priori*, $g_\ell(z) \in \mathbb{L}$, but we will see that $g_\ell(z) \in \mathbb{K}_\mathfrak{p}$ in a while.

From (3.5) we deduce that (3.4) holds. In particular, $g_\ell(z) \in \mathbb{K}$ when $z \in \mathbb{Z}$. Since $\mathbb{Z}$ is dense in $\mathbb{Z}_p$, we have $g_\ell(z) \in \mathbb{K}_\mathfrak{p}$ for all $z \in \mathbb{Z}_p$.

When U is non-degenerate, the function g_ℓ does not vanish identically, because the function $n \mapsto U(\ell + Nn)$ does not, see Subsection 2.2. □

As a by-product, we prove the Theorem of Skolem-Mahler-Lech (see Theorem 1.8 above) for $\overline{\mathbb{Q}}$-valued LRS.

Corollary 3.3 (Skolem-Mahler-Lech)**.** *Let U be a non-degenerate $\overline{\mathbb{Q}}$-valued LRS. Then the equation $U(n) = 0$ has at most finitely many solutions in $n \in \mathbb{Z}$.*

Proof. Pick some prime $\mathfrak{p}$ regular for U. Then each of the analytic functions g_ℓ has at most finitely many zeros on $\mathbb{Z}_p$, hence on $\mathbb{Z}$. □

Actually, the Skolem-Mahler-Lech Theorem, as stated in Theorem 1.8, applies to LRS over an arbitrary field of characteristic 0. To extend it to this generality, one more ingredient is needed, the *Lech-Cassels Specialization Theorem*, see [7].

3.3 Proof of Theorems 1.1, 1.4 and 1.5

Let U be an LRS taking values in a number field $\mathbb{K}$, and let $\mathfrak{p}$ be a prime of $\mathbb{K}$ regular for U, see Subsection 3.2. We denote by p the rational prime below $\mathfrak{p}$. In this section we prove the following two theorems, which generalize Theorems 1.1, 1.4 and 1.5 from the Introduction.

Theorem 3.4. *Let a be a zero of U. Then there exist a positive integer Q, a positive integer κ and an integer τ such that $\nu_\mathfrak{p}(U(n)) = \kappa\nu_p(n-a) + \tau$ for $n \equiv a \pmod{Q}$.*

Theorem 3.5. *Let $a \in \mathbb{Q}$ be such that there exists a sequence of integers (n_k) satisfying*

$$\nu_\mathfrak{p}(U(n_k)) \to +\infty, \qquad \nu_p(n_k - a) \to +\infty.$$

Then a is a TRZ of U.

Theorem 3.4 is more general than Theorem 1.1, while Theorem 3.5 is more general than Theorem 1.5 (and, *a fortiori*, than Theorem 1.4).

Proof of Theorem 3.4. Let the integer N and the functions $g_0, \dots, g_{N-1}$ be as in Proposition 3.2. Let $\ell \in \{0, \dots, N-1\}$ be such that $a \equiv \ell \pmod{N}$. Write $a = \ell + bN$ with $b \in \mathbb{Z}$. In the sequel, we denote $g := g_\ell$. We have $g(b) = 0$.

Theorem 3.1 implies that there exist positive integers k and τ', and an integer κ' such that for $z \equiv b \pmod{p^k}$ we have

$$\nu_p(g(z)) = \kappa'\nu_p(z-b) + e^{-1}\tau'. \tag{3.6}$$

Now set

$$Q := Np^k, \qquad \kappa := e\kappa', \qquad \tau := \tau' - \kappa\nu_p(N).$$

Let $n \equiv a \pmod{Q}$. Then $n \equiv \ell \pmod{N}$, and for $m := (n-\ell)/N$ we have

$$m \equiv b \pmod{p^k}, \qquad \nu_p(m-b) = \nu_p(n-a) - \nu_p(N), \qquad g(m) = U(n).$$

Applying (3.6) with $z = m$, we obtain

$$\nu_\mathfrak{p}(U(n)) = e\nu_p(g(m)) = e\kappa'\nu_p(m-b) + \tau' = \kappa\nu_p(n-a) + \tau.$$

The theorem is proved. □

Proof of Theorem 3.5. Once again, let N and $g_0, \dots, g_{N-1}$ be as in Proposition 3.2. Let $\ell \in \{0, \dots, N-1\}$ be such that $n_k \equiv \ell \pmod{N}$ holds for infinitely many k. By taking a subsequence, we may assume that this holds for all k. We denote $g := g_\ell$.

Set $b := (a-\ell)/N$ and $m_k := (n_k - \ell)/N$. Then, $m_k \to b$ and $g(m_k) \to 0$ in the p-adic topology. Hence $g(b) = 0$.

(Note that, unlike in the proof of Theorem 3.4, we do not, in general, have $g(b) = U(\ell + Nb) = U(a)$; this would only be true if $b \in \mathbb{Z}$. But this is not true in general: b is merely a rational number, not necessarily an integer.)

Recall that

$$g(z) = g_\ell(z) = \sum_{i=1}^{s} \lambda_i^\ell h_i(z), \quad \text{where} \quad h_i(z) := f_i(\ell + Nz) \exp(z \log(\lambda_i^N)).$$

Let A be the denominator of the rational number a. Then

$$(h_i(b))^{AN} = \left(\lambda_i^\ell f_i(a)\right)^{AN} \exp(ANb \log(\lambda_i^N)).$$

Since $ANb \in \mathbb{Z}$, we have $\exp(ANb \log(\lambda_i^N)) = \lambda_i^{AN^2 b}$. Hence

$$(h_i(b))^{AN} = \lambda_i^{AN\ell + AN^2 b} f_i(a)^{AN} = \left(\lambda_i^a f_i(a)\right)^{AN},$$

where we pick some definition for the rational power λ_i^a. Thus,

$$h_i(b) = \xi_i \lambda_i^a f(a),$$

where ξ_i is a root of unity.

We have proved that

$$0 = g(b) = \sum_{i=1}^{s} \xi_i \lambda_i^a f(a),$$

which exactly means that a is a TRZ of U. The theorem is proved. □

4 Finiteness of twisted rational zeros

In this section we prove Theorem 1.9. Throughout this section, unless the contrary is stated explicitly, $\mathbb{K}$ is a field of characteristic 0. We fix an algebraic closure $\overline{\mathbb{K}}$.

For a positive integer n we fix $\zeta_n \in \overline{\mathbb{K}}$, a primitive n^{th} root of unity. Recall that we denote by μ_n the group of n^{th} roots of unity, and by $\mu_{\mathbb{K}}$ the group of roots of unity in $\mathbb{K}$. We denote by $\mathbb{K}^n$ the set of n^{th} powers in $\mathbb{K}$:

$$\mathbb{K}^n := \{\alpha^n : \alpha \in \mathbb{K}\}.$$

We denote by $\mathbb{K}_{\text{ab}}$ the maximal abelian subfield of $\mathbb{K}$; that is, the maximal subfield of $\mathbb{K}$ which is an abelian extension of $\mathbb{Q}$.

4.1 Powers in fields

The following result is due to Chevalley [9] and Bass [1]. The proofs can be also found in [20] and [2].

Theorem 4.1. *[Chevalley, Bass] Let $\mathbb{K}$ be a finitely generated field of characteristic 0 (in particular, $\mathbb{K}_{\mathrm{ab}}$ is a finite extension of $\mathbb{Q}$). Then there exists a positive integer Λ, depending only on the degree $d := [\mathbb{K}_{\mathrm{ab}} : \mathbb{Q}]$, such that for every positive integer n the following holds: if $\alpha \in \mathbb{K}$ is a Λn^{th} power in $\mathbb{K}(\zeta_{\Lambda n})$, then α is an n^{th} power in $\mathbb{K}$. In symbols:*

$$\mathbb{K}(\zeta_{\Lambda n})^{\Lambda n} \cap \mathbb{K} \subset \mathbb{K}^n \qquad (n = 1, 2, 3, \ldots). \tag{4.1}$$

The smallest positive integer Λ satisfying (4.1) will be called the *Chevalley-Bass number* of the field $\mathbb{K}$; see [2, Section 6].

It might not be easy to determine the Chevalley-Bass number of a given field $\mathbb{K}$, but it is easy to estimate it in terms of $d := [\mathbb{K}_{\mathrm{ab}} : \mathbb{Q}]$. For instance, it is shown in [2, Section 6.1] that, when $d \geq 3$, the Chevalley-Bass number Λ satisfies $\Lambda \leq \exp(d^{2/\log\log d})$.

It will be convenient to introduce the following notion. For $\alpha \in \mathbb{K}^\times$ we define the *Kummer exponent* of α in $\mathbb{K}$ as the biggest positive integer n such that $\alpha\xi \in \mathbb{K}^n$ for some root of unity $\xi \in \mathbb{K}$. In symbols:

$$\varrho_{\mathbb{K}}(\alpha) := \max\{n : \alpha \in \mu_{\mathbb{K}}\mathbb{K}^n\}$$

(recall that $\mu_{\mathbb{K}}$ denotes the group of roots of unity in $\mathbb{K}$). Clearly, $\varrho_{\mathbb{K}}(\alpha) = \infty$ if α is a root of unity, and, when $\mathbb{K}$ is a finitely generated field, $\varrho_{\mathbb{K}}(\alpha)$ is finite if α is not a root of unity.

Proposition 4.2. *Let $\alpha \in \mathbb{K}$ be such that $\varrho_{\mathbb{K}}(\alpha)$ is finite, and n a positive integer.*

1. *We have $\alpha \in \mu_{\mathbb{K}}\mathbb{K}^n$ if and only if $n \mid \varrho_{\mathbb{K}}(\alpha)$.*
2. *Let $\alpha^{1/n} \in \overline{\mathbb{K}}$ be some determination of the n^{th} root, and $\xi \in \overline{\mathbb{K}}$ a root of unity. Then the degree $[\mathbb{K}(\alpha^{1/n}\xi) : \mathbb{K}]$ is a multiple of $n/\gcd(\varrho_{\mathbb{K}}(\alpha), n)$.*

Proof. Item 1 follows immediately from the definition. To prove item 2, define

$$\mathbb{L} := \mathbb{K}(\alpha^{1/n}\xi), \qquad m := [\mathbb{L} : \mathbb{K}], \qquad \rho := \varrho_{\mathbb{K}}(\alpha), \qquad d := \gcd(m, n).$$

All conjugates of $\alpha^{1/n}$ over $\mathbb{K}$ are equal to $\alpha^{1/n}$ times a root of unity. Hence $\beta := \mathcal{N}_{\mathbb{L}/\mathbb{K}}(\alpha^{1/n}\xi)$ is $\alpha^{m/n}$ times a root of unity. Let $r, s \in \mathbb{Z}$ be such that $mr + ns = d$. Then $\gamma := \alpha^s\beta^r$ is $\alpha^{d/n}$ times a root of unity. Since $\gamma^{n/d}$ is α times a root of unity, we have $n/d \mid \rho$. Hence $n/d \mid \gcd(\rho, n)$. It follows that $n/\gcd(\rho, n)$ divides d. Hence it divides m. □

4.2 Equations in roots of unity

The following result is due to Dvornicich and Zannier [11, 24], who improved on the previous work of Mann [16] and of Conway and Jones [10]. In this subsection $\mathbb{K}$ is a finitely generated field of characteristic 0.

Theorem 4.3. *[Dvornicich, Zannier] Let $\alpha_1, \dots, \alpha_s$ be non-zero elements of $\mathbb{K}$, and $\xi_1, \dots, \xi_s \in \overline{\mathbb{K}}$ roots of unity. Assume that*

$$\alpha_1\xi_1 + \cdots + \alpha_s\xi_s = 1,$$

and no proper sub-sum of the sum on the left vanishes: $\sum_{i\in I} \alpha_i\xi_i \neq 0$ when $\varnothing \subsetneq I \subsetneq \{1, \dots, s\}$. Then the order of the multiplicative group generated by $\xi_1, \dots, \xi_s$ is effectively bounded in terms of $d = [\mathbb{K}_{\mathrm{ab}} : \mathbb{Q}]$ and s.

In fact, Dvornicich and Zannier prove that, denoting by r the order of the group generated by $\xi_1, \dots, \xi_s$, we have the following properties:

- if $p^{a+1} \mid r$ for some positive integer a then $p^a \mid 2d$;
- $s + 1 \geq \dim_{\mathbb{K}}(\mathbb{K} + \mathbb{K}\xi_1 + \cdots + \mathbb{K}\xi_s) \geq 1 + \displaystyle\sum_{p\|r} \left(\frac{p-1}{\gcd(d, p-1)} - 1 \right)$.

Clearly, using these properties, it is easy to bound r explicitly in terms of d and s.

4.3 A Kummer property

As before, $\mathbb{K}$ is a finitely generated field of characteristic 0. Recall that we denote by $\mathbb{K}_{\mathrm{ab}}$ the maximal abelian subfield of $\mathbb{K}$. Let Γ be the division group of the multiplicative group $\mathbb{K}^\times$:

$$\Gamma := \{a \in \overline{\mathbb{K}}^\times : a^n \in \mathbb{K}^\times \text{ for some positive integer } n\}.$$

The following key proposition is, essentially, due to Laurent [14].

Proposition 4.4. *Let $\alpha_1, \dots, \alpha_s \in \Gamma$ be such that $\alpha_1 + \cdots + \alpha_s = 1$, and no proper sub-sum of the sum $\alpha_1 + \cdots + \alpha_s$ vanishes. Let Λ be the Chevalley-Bass number of $\mathbb{K}$ (see Section 4.1). Then there exist roots of unity $\xi_1, \dots, \xi_s \in \overline{\mathbb{K}}$ such that*

$$\alpha_i^\Lambda \xi_i \in \mathbb{K} \qquad (i = 1, \dots, m), \tag{4.2}$$

Proof. We follow Laurent [14, Section 2.2], but we replace the cohomological argument by a reference to Theorem 4.1.

Let n be a positive integer such that $\alpha_1^n, \dots, \alpha_s^n \in \mathbb{K}$. Denote by G the Galois group $\mathrm{Gal}(\overline{\mathbb{K}}/\mathbb{K}(\zeta_n))$. For $i \in \{1, \dots, s\}$ let $\chi_i : G \to \mathbb{K}(\zeta_n)$ be the character of G defined by $\sigma \mapsto \sigma(\alpha_i)/\alpha_i$. Since $\sigma(\alpha_1) + \cdots + \sigma(\alpha_s) = 1$ for every $\sigma \in G$, we have $\alpha_1\chi_1 + \cdots + \alpha_s\chi_s = 1$.

We claim that the characters $\chi_1, \ldots, \chi_s$ are all trivial:

$$\chi_1 = \cdots = \chi_s = 1. \tag{4.3}$$

Indeed, defining $\alpha_0 := -1$ and $\chi_0 := 1$, we have $\alpha_0\chi_0 + \cdots + \alpha_s\chi_s = 0$. After renumbering the characters $\chi_1, \ldots, \chi_s$, we may assume that for some $r \geq 0$ the characters $\chi_0, \ldots, \chi_r$ are distinct, and each of the remaining $\chi_{r+1}, \ldots, \chi_s$ is equal to one of $\chi_0, \ldots, \chi_r$. For $k = 0, \ldots, r$ define $I_k := \{i : \chi_i = \chi_k\}$. Then

$$\sum_{k=0}^{r} \chi_k \sum_{i \in I_k} \alpha_i = 0.$$

Artin's Theorem on Characters (see, for instance, Theorem 4.1 in [13, Chapter VI]) implies that $\sum_{i \in I_k} \alpha_i = 0$ for every k. Since no proper sub-sum of $\alpha_1 + \cdots + \alpha_s$ vanishes, this is possible only if $r = 0$, which proves (4.3).

It follows from (4.3) that $\alpha_1, \ldots, \alpha_s \in \mathbb{K}(\zeta_n)$. Hence each $\alpha_i^{\Lambda n}$ is an Λn^{th} power in $\mathbb{K}(\zeta_n)$. Theorem 4.1 implies that $\alpha_i^{\Lambda n}$ is an n^{th} power in $\mathbb{K}$. It follows that $\alpha_i^{\Lambda}\xi_i \in \mathbb{K}$ for some root of unity ξ_i, as wanted. □

4.4 Proof of Theorem 1.9

Let U be a non-degenerate LRS with values in a field of characteristic 0 and with Binet expansion

$$U(n) = f_1(n)\lambda_1^n + \cdots + f_s(n)\lambda_s^n. \tag{4.4}$$

Let $\mathbb{K}$ be a finitely generated field, containing $\lambda_1, \ldots, \lambda_s$ and the coefficient of the polynomials $f_1, \ldots, f_s$. Recall that we denote by $\mathbb{K}_{\text{ab}}$ the maximal abelian subfield of $\mathbb{K}$. Since $\mathbb{K}$ is finitely generated, $\mathbb{K}_{\text{ab}}$ is a finite extension of $\mathbb{Q}$, and we denote by d its degree over $\mathbb{Q}$.

Recall that we denote by $\varrho_{\mathbb{K}}(\alpha)$ the Kummer exponent of $\alpha \in \mathbb{K}$, see Subsection 4.1. Since the U is non-degenerate and the field $\mathbb{K}$ is finitely generated, we have $\varrho_{\mathbb{K}}(\lambda_i/\lambda_j) < \infty$ when $i \neq j$. We set

$$\rho := \gcd\{\varrho_{\mathbb{K}}(\lambda_i/\lambda_j) : 1 \leq i < j \leq s\}. \tag{4.5}$$

Let a be a TRZ of U. Recall that this means the following: there exist roots of unity $\xi_1, \ldots, \xi_s \in \overline{\mathbb{K}}$ such that for some determinations of $\lambda_1^a, \ldots, \lambda_s^a \in \overline{\mathbb{K}}$ we have

$$\xi_1 f_1(a)\lambda_1^a + \cdots + \xi_s f_s(a)\lambda_s^a = 0. \tag{4.6}$$

We call the TRZ *a primitive* if no proper sub-sum of the sum in (4.6) vanishes; that is, if $\varnothing \subsetneq I \subsetneq \{1, \ldots, s\}$ then $\sum_{i \in I} \xi_i f_i(a)\lambda_i^a \neq 0$.

Proposition 4.5. *Let $\mathbb{K}$ be as above (that is, a finitely generated field, containing $\lambda_1, \ldots, \lambda_s$ and the coefficient of the polynomials $f_1, \ldots, f_s$), and Λ the Chevalley-Bass number of $\mathbb{K}$. Let a be a primitive TRZ of U, and $\xi_1, \ldots, \xi_s$ roots of unity satisfying* (4.6)*. Assume that $s \geq 2$. Then the denominator of*

the rational number a divides $\Lambda\rho$, where ρ is defined in (4.5)*; in particular, the denominator is bounded effectively in terms of $d := [\mathbb{K}_{\mathrm{ab}} : \mathbb{Q}]$ and ρ. Moreover, the orders of the roots of unity ξ_i/ξ_j are effectively bounded in terms of d, ρ and s.*

Proof. Since $s \geq 2$ and no proper sub-sum of the sum in (4.6) vanishes, we have $f_i(a) \neq 0$ for $i = 1, \ldots, s$. There will be no loss of generality to assume that $\xi_s = 1$; so, instead of (4.6) we have

$$\xi_1 f_1(a)\lambda_1^a + \cdots + \xi_{s-1} f_{s-1}(a)\lambda_{s-1}^a + f_s(a)\lambda_s^a = 0. \tag{4.7}$$

Applying Proposition 4.4 to the relation

$$\sum_{i=1}^{s-1} -\xi_i \frac{f_i(a)}{f_s(a)} \left(\frac{\lambda_i}{\lambda_s}\right)^a = 1, \tag{4.8}$$

we obtain the following: there exist roots of unity $\eta_1, \ldots, \eta_{s-1}$ such that

$$(\lambda_i/\lambda_s)^{\Lambda a}\, \eta_i \in \mathbb{K} \qquad (i = 1, \ldots, s-1).$$

Write $a = k/\ell$, where k and ℓ are co-prime integers. We want to show that $\ell \mid \Lambda\rho$. We have $\varrho_{\mathbb{K}}\big((\lambda_i/\lambda_s)^{\Lambda k}\big) = \Lambda k \varrho_{\mathbb{K}}(\lambda_i/\lambda_s)$. Proposition 4.2 implies that the quotient $\ell/\gcd\big(\ell, \Lambda k \varrho_{\mathbb{K}}(\lambda_i/\lambda_s)\big)$ divides the degree $[\mathbb{K}((\lambda_i/\lambda_s)^{\Lambda a}\eta_i) : \mathbb{K}]$. But this degree is 1, which implies that $\ell \mid \Lambda k \varrho_{\mathbb{K}}(\lambda_i/\lambda_s)$. Since ℓ and k are coprime, this implies that $\ell \mid \Lambda \varrho_{\mathbb{K}}(\lambda_i/\lambda_s)$ for $i = 1, \ldots, s-1$.

We have clearly $\rho = \gcd\{\varrho_{\mathbb{K}}(\lambda_i/\lambda_s) : i = 1, \ldots, s-1\}$. It follows that $\ell \mid \Lambda\rho$, which proves the first statement of the proposition.

Now let us bound the orders of the roots of unity ξ_i. Let $\mathbb{L}$ be the field, generated over $\mathbb{K}$ by $(\lambda_1/\lambda_s)^a, \ldots, (\lambda_{s-1}/\lambda_s)^a$. Since the denominator of a divides $\Lambda\rho$, we have

$$[\mathbb{L}_{\mathrm{ab}} : \mathbb{K}_{\mathrm{ab}}] \leq [\mathbb{L} : \mathbb{K}] \leq (\Lambda\rho)^{s-1}.$$

Hence $[\mathbb{L}_{\mathrm{ab}} : \mathbb{Q}] \leq d(\Lambda\rho)^{s-1}$; in particular, $[\mathbb{L}_{\mathrm{ab}} : \mathbb{Q}]$ is effectively bounded in terms of d, s and ρ.

Applying Theorem 4.3 to relation (4.8), we bound the orders of the roots of unity ξ_i in terms of $[\mathbb{L}_{\mathrm{ab}} : \mathbb{Q}]$ and s. Hence it is bounded in terms of d, s and ρ, as wanted. The proposition is proved. □

Combining this proposition with the Skolem-Mahler-Lech Theorem, we obtain the following consequence.

Corollary 4.6. *Let U be a non-degenerate LRS over a field of characteristic* 0*. Then U admits at most finitely many primitive TRZs. More precisely, if* (4.4) *is the Binet expansion of U, then there exist at most finitely many s-tuples $(a, \xi_1, \ldots, \xi_{s-1})$ such that a is a rational number, $\xi_1, \ldots, \xi_{s-1}$ are roots of unity, and* (4.7) *holds.*

Proof. If $s = 1$ then $f_1(a) = 0$, which is possible only for finitely many a.

From now on we assume that $s \geq 2$. Proposition 4.5 implies that $a = n/\Lambda\rho$, where $n \in \mathbb{Z}$, and that there are at most finitely many choices for $(\xi_1, \ldots, \xi_{s-1})$ in (4.7). Pick some determinations $\theta_i := \lambda_i^{1/\Lambda\rho}$, so that $\lambda_i^a = \theta_i^n \eta_i$, where η_i are $\Lambda\rho^{\text{th}}$ roots of unity. Then

$$\xi_1\eta_1 g_1(n)\theta_1^n + \cdots + \xi_{s-1}\eta_{s-1}g_{s-1}(n)\theta_{s-1}^n + \eta_s g_s(n)\theta_s^n = 0, \tag{4.9}$$

where $g_i(t) := f_i(t/\Lambda\rho)$.

The left-hand side of (4.9) is a non-degenerate LRS, and the Skolem-Mahler-Lech Theorem implies that there can be at most finitely many n for every fixed choice of the roots of unity ξ_i and η_i. Since there are at most finitely many choices for $(\xi_1, \ldots, \xi_{s-1})$ and for $(\eta_1, \ldots, \eta_s)$, the result follows. □

Now we are ready to complete the proof of Theorem 1.9. Let a be a TRZ of U, so that (4.6) holds for some choice of roots of unity ξ_i. Let I be a minimal non-empty subset of $\{1, \ldots, s\}$ such that $\sum_{i\in I} \xi_i f_i(a)\lambda_i^a = 0$. Then a is a primitive TRZ of the LRS U_I, defined by

$$U_I(n) := \sum_{i\in I} f_i(n)\lambda_i^n. \tag{4.10}$$

Corollary 4.6 tells us that U_I may have at most finitely many primitive TRZs. Since there are finitely many possible I, Theorem 1.9 is proved.

4.5 An explicit result for $\mathbb{Q}$-valued linear recurrence sequences

Let U be an LRS over a field of characteristic 0 with Binet expansion (4.4), and let a be a rational number. If a is a common root of the polynomials $f_1, \ldots, f_s$, then it is, clearly, a rational zero of U. Such rational zeros will be called *trivial*; there are only finitely many of them, and in many interesting cases (for instance, if at least one of $f_1, \ldots, f_s$ is constant) there are none.

Arguing as at the end of Subsection 4.4, we obtain the following: the denominator of a non-trivial TRZ a of U is bounded in terms of d, ρ and s. Indeed, if $f_i(a) \neq 0$ for some i, then there exists a set $I \subset \{1, \ldots, s\}$ having at least 2 elements such that the LRS U_I, defined in (4.10), has a as a primitive TRZ. Now Proposition 4.5 implies that the denominator of a is bounded in terms of d, ρ and s.

Note that $s \leq m$, where m denoted the order of the LRS U. Hence the denominator of a is bounded in terms of d, ρ and m.

In the most interesting special case when U is a $\mathbb{Q}$-valued LRS of order m, we can take $\mathbb{K}$ in Proposition 4.5 as the splitting field of the characteristic polynomial of U. With this choice of $\mathbb{K}$, the degree d is bounded in terms of m. Hence the denominator of a is bounded in terms of m and ρ. We are going to make it totally explicit.

Proposition 4.7. *Let U be a $\mathbb{Q}$-valued LRS of order m with Binet expansion* (4.4)*, $\mathbb{K}$ the splitting field of the characteristic polynomial of U, and ρ as in* (4.5)*. Let a be a non-trivial TRZ of U. Then the denominator of a does not exceed $\rho \exp\exp(m/\log m)$.*

Proof. As we have just seen, if a is a non-trivial TRZ of U, then there exists $I \subset \{1, \dots, s\}$ with $\#I \geq 2$ such that a is a primitive TRZ of U_I. Proposition 4.5 implies that the denominator of a is bounded by $\rho\Lambda$. And we have $\Lambda \leq \exp\exp(m/\log m)$, see [2, Proposition 6.5]. This completes the proof. □

5 Twisted rational zeros of the Tribonacci sequence

In this section we prove Theorem 1.10. As in the proof of Theorem 1.9, the principal part is bounding the denominators of the TRZ, see Proposition 5.2. Instead of adapting the general argument of Section 4, using the Theorems of Chevalley-Bass and of Dvornicich-Zannier, we use an elementary ad hoc argument.

In this section we denote by $\overline{\mathbb{Q}} \subset \mathbb{C}$ the field of all complex algebraic numbers, and by $x \mapsto \overline{x}$ the complex conjugation.

5.1 The roots

Let $\lambda_1, \lambda_2, \lambda_3 \in \overline{\mathbb{Q}}$ be the complex roots of the characteristic polynomial

$$P(X) := X^3 - X^2 - X - 1.$$

Then

$$T(n) = \alpha_1\lambda_1^n + \alpha_2\lambda_2^n + \alpha_3\lambda_3^n, \qquad \alpha_i := P'(\lambda_i)^{-1}\lambda_i.$$

One of the roots $\lambda_1, \lambda_2, \lambda_3$ is real and the other two are complex conjugate. We will assume that $\lambda_1 \in \mathbb{R}$ and $\lambda_3 = \overline{\lambda_2}$.

We denote $\mathbb{K}_i := \mathbb{Q}(\lambda_i)$ and $\mathbb{L} := \mathbb{Q}(\lambda_1, \lambda_2)$, the splitting field of P. We have $[\mathbb{K}_i : \mathbb{Q}] = 3$ and $[\mathbb{L} : \mathbb{Q}] = 6$. The maximal abelian subfield $\mathbb{L}_{\mathrm{ab}}$ is $\mathbb{Q}(\sqrt{-11})$, because the discriminant of P is -44. The 6 numbers

$$\lambda_i/\lambda_j \qquad (1 \leq i \neq j \leq 3) \tag{5.1}$$

form a full Galois orbit over $\mathbb{Q}$; in particular, for $i \neq j$ we have $\mathbb{L} = \mathbb{Q}(\lambda_i/\lambda_j)$.

In the following proposition we collect some less obvious properties of the roots λ_i, to be used later.

Proposition 5.1. *1. For $i \neq j$, the quotient $P'(\lambda_i)/P'(\lambda_j)$ is not a Dirichlet unit.*

2. Let λ be one of $\lambda_1, \lambda_2, \lambda_3$ and $\mathbb{K} := \mathbb{Q}(\lambda)$. Then λ is not an m^{th} power in $\mathbb{K}$ for any integer $m > 1$, and neither is $-\lambda$. In terms of the Kummer exponent, defined in Subsection 4.1, this can be stated as $\varrho_{\mathbb{K}}(\lambda) = 1$.

3. *The quotients λ_i/λ_j are cubes in $\mathbb{L}$. More precisely, for $1 \le i, j \le 3$ there exists a unique $\theta_{ij} \in \mathbb{L}$ such that $\lambda_i/\lambda_j = \theta_{ij}^3$.*

Proof. If, say, $P'(\lambda_1)/P'(\lambda_2)$ is a unit, then so is every $P'(\lambda_i)/P'(\lambda_j)$. It follows that the 3 algebraic integers $P'(\lambda_i)$ generate the same principal ideal in $\mathcal{O}_{\mathbb{L}}$. This ideal must divide the sum $\sum_{i=1}^3 P'(\lambda_i) = 4$, which implies that the product $\prod_{i=1}^3 P'(\lambda_i)$ must be a power of 2. But

$$\prod_{i=1}^{3} P'(\lambda_i) = 44, \tag{5.2}$$

a contradiction. This proves item 1.

In the proof of item 2 we will use the notion of the *absolute logarithmic height* $\mathrm{h}(\cdot)$ of an algebraic number. The definition can be found in many sources, say, in [6, Section 1.5.7]. We will need only the following properties: if γ is an algebraic integer of degree d with conjugates $\gamma_1, \dots, \gamma_d \in \mathbb{C}$, and m is a positive integer, then $d\,\mathrm{h}(\gamma) = \sum_{i=1}^d \max\{\log|\gamma_i|, 0\}$, and $\mathrm{h}(\gamma^m) = m\,\mathrm{h}(\gamma)$. In particular,

$$3\,\mathrm{h}(\lambda) = \log\lambda_1 < 0.61,$$

because $\lambda_1 > 1$ and $|\lambda_2| = |\lambda_3| < 1$.

Now assume that $\lambda = \gamma^m$ for some $\gamma \in \mathbb{K}$ and $m > 1$. Then $\mathrm{h}(\lambda) = m\,\mathrm{h}(\gamma)$. On the other hand, the famous result of Smyth [21] implies that

$$3\,\mathrm{h}(\gamma) \ge \log\vartheta > 0.28.$$

where ϑ is the real root of the polynomial $X^3 - X - 1$. Hence

$$m \le \frac{\log\lambda}{\log\vartheta} < 2.2.$$

It follows that $m = 2$. Hence γ is a root of the polynomial $P(X^2)$. However, this polynomial is irreducible over $\mathbb{Q}$, which means that γ is of degree 6, a contradiction. In a similar fashion one shows that $-\lambda$ is not a proper power in $\mathbb{K}$. This proves item 2.

In item 3 uniqueness is clear, because $\zeta_3 \notin \mathbb{L}$, so we only have to prove existence. Using PARI [22] (or another similar tool), we calculate the X-resultant of the polynomials $P(X)$ and $P(XY)$. It is a polynomial in Y of degree 9, whose roots are exactly the 9 quotients λ_i/λ_j. It has a root 1 of multiplicity 3, which corresponds to the 3 quotients λ_i/λ_i, and it factors as $(Y-1)^3 R(Y)$, where

$$R(Y) := Y^6 + 4Y^5 + 11Y^4 + 12Y^3 + 11Y^2 + 4Y + 1$$

is the irreducible polynomial whose roots are the quotients (5.1).

Polynomial $R(Y^3)$ is reducible over $\mathbb{Q}$: it has an irreducible factor of degree 6

$$Q(Y) := Y^6 + Y^5 + 2Y^4 + 3Y^3 + 2Y^2 + Y + 1$$

and another irreducible factor of degree 12. Let θ be a root of Q. Then the field $\mathbb{Q}(\theta)$ is of degree 6, and θ^3 is one of the quotients (5.1); in particular, $\mathbb{Q}(\theta)$ contains $\mathbb{L}$. By equality of degrees we obtain $\mathbb{Q}(\theta) = \mathbb{L}$, which completes the proof of item 3. □

5.2 The denominator

In this subsection we prove that the denominator of a TRZ divides 3.

Proposition 5.2. *Let a be a TRZ of the Tribonacci LRS. Then $3a \in \mathbb{Z}$.*

We will use the following very simple lemma.

Lemma 5.3. *Let $\gamma \in \mathbb{C}$ be a complex number such that $\gamma/\overline{\gamma}$ is not a root of unity, and $\delta \in \mathbb{R}$ a real number. Then the equation $\gamma\eta + \overline{\gamma}\eta' = \delta$ may have at most one solution in roots of unity (η, η'). This solution satisfies $\eta \in \mathbb{Q}(\gamma, \overline{\gamma}, \delta)$ and $\eta' = \overline{\eta}$.*

Proof. If η, η' are roots of unity such that $\gamma\eta + \overline{\gamma}\eta' \in \mathbb{R}$, then the complex numbers $\overline{\gamma}\eta'$ and $\overline{\gamma\eta}$ have the same imaginary part: $\overline{\gamma}\eta' - \gamma\overline{\eta'} = \overline{\gamma\eta} - \gamma\eta$. If $\eta \neq \overline{\xi}$ then

$$\frac{\gamma}{\overline{\gamma}} = \frac{\eta' - \overline{\eta}}{\overline{\eta'} - \eta} = -\frac{\eta'}{\eta},$$

contradicting the hypothesis that $\gamma/\overline{\gamma}$ is not a root of unity. Hence $\eta' = \overline{\eta}$.

Thus, η is a root of the polynomial

$$F(X) := X^2 - (\delta/\gamma)X + \overline{\gamma}/\gamma \in \mathbb{Q}(\gamma, \overline{\gamma}, \delta)[X].$$

Since the free term $\overline{\gamma}/\gamma$ is not a root of unity, the other root of F cannot be a root of unity. This proves that there may exist only one possible η for given γ and δ.

Furthermore, if F is irreducible over $\mathbb{Q}(\gamma, \overline{\gamma}, \delta)$ then its other root is a root of unity as well, which is impossible, as we just saw. Hence F is reducible, which implies that $\eta \in \mathbb{Q}(\gamma, \overline{\gamma}, \delta)$. The lemma is proved. □

Proof of Proposition 5.2. Let m be the denominator of a; that is, $a = n/m$, where $m, n \in \mathbb{Z}$ are coprime and $m > 0$. Let $\lambda_1^{1/m}$ be the positive real m^{th} root, $\lambda_2^{1/m}$ some complex m^{th} root, and we define $\lambda_3^{1/m}$ as the complex conjugate of $\lambda_2^{1/m}$. With this choice of m^{th} roots we have

$$\lambda_1^{1/m}\lambda_2^{1/m}\lambda_3^{1/m} = 1. \tag{5.3}$$

Once the m^{th} roots are defined, the rational powers λ_i^a are well-defined as $(\lambda_i^{1/m})^n$. Note that $\lambda_3^a = \overline{\lambda_2^a}$.

Since a is a TRZ, we have $\alpha_1\lambda_1^a\eta_1 + \alpha_2\lambda_2^a\eta_2 + \alpha_2\lambda_3^a\eta_3 = 0$ for some roots of unity η_1, η_2, η_3. We may clearly assume that $\eta_1 = 1$, in which case Lemma 5.3 implies that $\eta_3 = \overline{\eta_2}$. In the sequel we write η_2 as η and η_3 as $\overline{\eta}$; that is, we have

$$\alpha_1\lambda_1^a + \alpha_2\lambda_2^a\eta + \alpha_3\lambda_3^a\overline{\eta} = 0. \tag{5.4}$$

Recall that we denote $\mathbb{K}_1 = \mathbb{Q}(\lambda_1)$. Fix an element σ in the absolute Galois group $G_1 := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{K}_1)$. Then $(\lambda_1^{1/m})^\sigma = \lambda_1^{1/m}\xi_1$ for some $\xi_1 \in \mu_m$. The group

$H := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{L})$ is an index 2 subgroup of G_1. If $\sigma \in H$ then $\lambda_2^\sigma = \lambda_2$ and $\lambda_3^\sigma = \lambda_3$, in which case there exist $\xi_2, \xi_3 \in \mu_m$ such that

$$(\lambda_2^{1/m})^\sigma = \lambda_2^{1/m}\xi_2, \qquad (\lambda_3^{1/m})^\sigma = \lambda_3^{1/m}\xi_3. \tag{5.5}$$

If $\sigma \notin H$ then $\lambda_2^\sigma = \lambda_3$ and $\lambda_3^\sigma = \lambda_2$; in this case there exist $\xi_2, \xi_3 \in \mu_m$ such that

$$(\lambda_2^{1/m})^\sigma = \lambda_3^{1/m}\xi_3, \qquad (\lambda_3^{1/m})^\sigma = \lambda_2^{1/m}\xi_2. \tag{5.6}$$

Let us apply σ to equalities (5.3) and (5.4). We obtain

$$1 = 1^\sigma = (\lambda_1^{1/m}\lambda_2^{1/m}\lambda_3^{1/m})^\sigma = \lambda_1^{1/m}\lambda_2^{1/m}\lambda_3^{1/m}\xi_1\xi_2\xi_3 = \xi_1\xi_2\xi_3, \tag{5.7}$$

$$\alpha_1^\sigma\lambda_1^a\xi_1^n + \alpha_2\lambda_2^a\xi_2^n\eta' + \alpha_3\lambda_3^a\xi_3^n\eta'' = 0, \qquad (\eta', \eta'') = \begin{cases} (\eta^\sigma, \overline{\eta}^\sigma), & \sigma \in H, \\ (\overline{\eta}^\sigma, \eta^\sigma), & \sigma \notin H. \end{cases} \tag{5.8}$$

Note that $\alpha_1^\sigma = \alpha_1$ because $\alpha_1 \in \mathbb{K}_1$, and that $\eta'\eta'' = (\eta\overline{\eta})^\sigma = 1$.

Rewrite (5.8) as

$$\alpha_1\lambda_1^a + \alpha_2\lambda_2^a\left(\frac{\xi_2}{\xi_1}\right)^n\eta' + \alpha_3\lambda_3^a\left(\frac{\xi_3}{\xi_1}\right)^n\eta'' = 0.$$

Comparing this to (5.4), the uniqueness statement in Lemma 5.3 implies that

$$\left(\frac{\xi_2}{\xi_1}\right)^n\eta' = \eta, \qquad \left(\frac{\xi_3}{\xi_1}\right)^n\eta'' = \overline{\eta}.$$

Multiplying these equalities, we obtain $(\xi_2\xi_3/\xi_1^2)^n = 1$. Since $\xi_1, \xi_2, \xi_3 \in \mu_m$ and m, n are coprime, this implies that $\xi_2\xi_3/\xi_1^2 = 1$, which, together with (5.7), implies that $\xi_1^3 = 1$.

We have proved the following: for any $\sigma \in G_1$ there exist $\xi_1 \in \mu_3$ such that $(\lambda_1^{1/m})^\sigma = \lambda_1^{1/m}\xi_1$. If $\xi_1 = 1$ for every $\sigma \in G_1$ then $\lambda_1^{1/m} \in \mathbb{K}_1$. Now assume that $\xi_1 = \zeta_3$ for some σ. Since $\mathbb{K}_1$ is a real field, any Galois orbit over $\mathbb{K}_1$ must be stable under the complex conjugation. Hence the Galois orbit of $\lambda_1^{1/m}$ over $\mathbb{K}_1$ is $\lambda_1^{1/m}, \lambda_1^{1/m}\zeta_3, \lambda_1^{1/m}\overline{\zeta_3}$.

Thus, $[\mathbb{K}_1(\lambda_1^{1/m}) : \mathbb{K}_1] \in \{1, 3\}$. On the other hand, item 2 of Proposition 5.1 implies that λ_1 is not a p^{th} power in $\mathbb{K}_1$ for any p, and $-\lambda_1$ is not a square in $\mathbb{K}_1$. Hence $[\mathbb{K}_1(\lambda_1^{1/m}) : \mathbb{K}_1] = m$ by Lemma 2.1. It follows that $m \in \{1, 3\}$, as wanted. □

We also need to take care of the roots of unity occurring in the definition of TRZ.

Proposition 5.4. *Let a be a TRZ of the Tribonacci LRS. Then, with suitable definitions of the rational powers λ_i^a we have*

$$\alpha_1\lambda_1^a + \alpha_2\lambda_2^a + \alpha_3\lambda_3^a = 0, \tag{5.9}$$

$$\lambda_1^a\lambda_2^a\lambda_3^a = 1 \tag{5.10}$$

Proof. We have $a = n/3$, with $n \in \mathbb{Z}$. We define $\lambda_1^{1/3}$ as the real cubic root of λ_1, and for $i = 2, 3$ we define $\lambda_i^{1/3} := \lambda_1^{1/3}\theta_{i1}$, where $\theta_{ij} \in \mathbb{L}$ are defined in item 3 of Proposition 5.1.

Note that $\theta_{31} = \overline{\theta_{21}}$. Indeed, $\overline{\theta_{21}}^3 = \overline{\lambda_2}/\overline{\lambda_1} = \lambda_3/\lambda_1$. Since λ_3/λ_1 has only one cubic root in $\mathbb{L}$, we must have $\theta_{31} = \overline{\theta_{21}}$.

From our definitions it follows that $\lambda_1^a\lambda_2^a\lambda_3^a$ is a positive real number. Since $(\lambda_1^a\lambda_2^a\lambda_3^a)^3 = (\lambda_1\lambda_2\lambda_3)^n = 1$, this proves (5.10), so we are only left with (5.9).

As we have seen in the proof of Proposition 5.2, there exists a root of unity η such that (5.4) holds. This can be rewritten as $\alpha_1 + \alpha_2\theta_{21}^n\eta + \alpha_3\theta_{31}^n\overline{\eta} = 0$. Lemma 5.3 implies that $\eta \in \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \theta_{21}, \theta_{31}) = \mathbb{L}$. Since $\mathbb{L}$ contains no roots of unity other than ± 1, we must have $\eta = 1$ or $\eta = -1$. In the former case we are done. Now let us assume that $\eta = -1$. In this case

$$\alpha_1 - \alpha_2\theta_{21}^n - \alpha_3\theta_{31}^n = 0. \tag{5.11}$$

Let $\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{Q})$ be such that

$$\lambda_1^\sigma = \lambda_2, \qquad \lambda_2^\sigma = \lambda_1, \qquad \lambda_3^\sigma = \lambda_3.$$

Then

$$\alpha_1^\sigma = \alpha_2, \quad \alpha_2^\sigma = \alpha_1, \quad \alpha_3^\sigma = \alpha_3, \quad \theta_{21}^\sigma = \theta_{12} = \theta_{21}^{-1}, \quad \theta_{31}^\sigma = \theta_{32} = \theta_{31}\theta_{21}^{-1}.$$

Applying σ to (5.11), we obtain $\alpha_2 - \alpha_1\theta_{21}^{-n} - \alpha_3\theta_{31}^n\theta_{21}^{-n} = 0$, which can be rewritten as $\alpha_1 - \alpha_2\theta_{21}^n + \alpha_3\theta_{31}^n = 0$. Comparing this with (5.11), we obtain $\alpha_3\theta_{31}^n = 0$, a contradiction. The proposition is proved. □

5.3 Proof of Theorem 1.10

Let W be the $\mathbb{Q}$-valued LRS with the general term given by

$$W(n) = 44\alpha_1^3\lambda_1^n + 44\alpha_2^3\lambda_2^n + 44\alpha_3^3\lambda_3^n - 3.$$

It is an LRS of order 4, defined by

$$W(0) = W(1) = 0, \quad W(2) = 2, \quad W(3) = 8, \qquad W(n+4) = 2W(n+3) - W(n).$$

Proposition 5.5. *Let $a \in \mathbb{Q}$ be a TRZ of the Tribonacci LRS. Then $3a$ is a zero of W.*

Proof. As we have seen in Proposition 5.2, if a is a TRZ of the Tribonacci LRS, then $n := 3a \in \mathbb{Z}$, so we only need to prove that $W(n) = 0$.

Define the rational powers λ_i^a as in Proposition 5.4, so that both (5.9) and (5.10) hold. Using (5.2), we also find

$$\alpha_1\alpha_2\alpha_3 = \frac{\lambda_1\lambda_2\lambda_3}{P'(\lambda_1)P'(\lambda_2)P'(\lambda_3)} = \frac{1}{44}. \tag{5.12}$$

Consider the polynomial

$$F(X_1, X_2, X_3) = X_1^3 + X_2^3 + X_3^3 - 3X_1X_2X_3 \in \mathbb{Z}[X_1, X_2, X_3].$$

Then $44F(\alpha_1\lambda_1^a, \alpha_2\lambda_2^a, \alpha_3\lambda_3^a) = W(n)$, because $\alpha_1\lambda_1^a\alpha_2\lambda_2^a\alpha_3\lambda_3^a = 1/44$, as follows from (5.10) and (5.12). The polynomial F factors as

$$F(X_1, X_2, X_3) = (X_1 + X_2 + X_3)(X_1 + \zeta_3 X_2 + \overline{\zeta_3} X_3)(X_1 + \overline{\zeta_3} X_2 + \zeta_3 X_3),$$

which implies that $F(\alpha_1\lambda_1^a, \alpha_2\lambda_2^a, \alpha_3\lambda_3^a) = 0$ by (5.9). This completes the proof. □

Proposition 5.6. *The only zeros of W are $-51, -12, -5, -3, 0, 1$.*

Proof. In [3] an algorithm is suggested which, when terminates, produces the full set of zeros of a given non-degenerate LRS, together with a mathematically rigorous proof that no other zeros exist. This algorithm is implemented, for simple[1] non-degenerate $\mathbb{Q}$-valued LRS, in the *Skolem Tool* [4]. Running the Skolem Tool for the LRS W, we obtain the result. □

We know (see [5, Section 2]) that $-17, -4, -5/3, -1, 0, 1/3$ are indeed TRZs of the Tribonacci LRS. Hence Theorem 1.10 is an immediate consequence of Propositions 5.5 and 5.6.

6 On Question 1.7

In this section we discuss Question 1.7. We will see that the answer is positive for twisted (integral) zeros of LRS of order 2, but (in general) not for higher order LRS. Unless the contrary is stated explicitly, the letter p in this section denotes a prime number.

For twisted (integral) zeros of LRS of order 2 we not only answer Question 1.7, but obtain a partial analog of Theorem 3.4.

Theorem 6.1. *Let U be a non-degenerate LRS of order 2 with values in a number field $\mathbb{K}$ and $a \in \mathbb{Z}$ a twisted zero of U. Then for infinitely many primes $\mathfrak{p}$ of $\mathbb{K}$ the following holds: there exist*

$$Q \in \mathbb{Z}_{>0}, \qquad a' \in \{0, 1, \ldots, Q-1\}, \qquad \tau \in \mathbb{Z} \tag{6.1}$$

such that for every $n \in \mathbb{Z}$ satisfying $n \equiv a' \pmod{Q}$ we have

$$\nu_{\mathfrak{p}}(U(n)) = \nu_p(n - a) + \tau,$$

where p is the rational prime below $\mathfrak{p}$. Moreover, $p \nmid Q$; in particular, $\nu_p(n-a)$ is unbounded on the set of n satisfying $n \equiv a' \pmod{Q}$.

In fact, we show that this holds true for primes $\mathfrak{p}$ from a set of positive lower density. Let us recall the definition of density. Denote by $\pi_{\mathbb{K}}(x)$ the counting function for primes of $\mathbb{K}$; that is, the number of primes $\mathfrak{p}$ of $\mathbb{K}$ such that $\mathcal{N}\mathfrak{p} \le x$; here $\mathcal{N}\mathfrak{p}$ denotes the absolute norm. Let $\mathcal{P}$ be a set of primes of $\mathbb{K}$. We denote its lower density as $\liminf_{x\to+\infty} \#\{\mathfrak{p} \in \mathcal{P} : \mathcal{N}\mathfrak{p} \le x\}/\pi_{\mathbb{K}}(x)$.

[1] An LRS is called *simple* if its characteristic polynomial has only simple roots.

6.1 A density result

The proof of Theorem 6.1 relies on a certain Chebotaryov[2]-style density result. To state it, let us introduce some more notation. In this subsection $\mathbb{K}$ is a number field, unless stated otherwise.

Let $\alpha \in \mathbb{K}^\times$ and a prime $\mathfrak{p}$ of $\mathbb{K}$ be such that $\nu_\mathfrak{p}(\alpha) = 0$. We denote by $\mathrm{ord}_\mathfrak{p}(\alpha)$ the multiplicative order of α modulo $\mathfrak{p}$. That is, let $\mathcal{O}_\mathfrak{p} := \{x \in \mathbb{K} : \nu_p(x) \geq 0\}$ be the local ring of $\mathfrak{p}$, and $\mathcal{O}_\mathfrak{p} \to \mathcal{O}_\mathfrak{p}/\mathfrak{p} : x \mapsto \overline{x}$ the reduction map[3] modulo $\mathfrak{p}$. Then $\overline{\alpha} \in (\mathcal{O}_\mathfrak{p}/\mathfrak{p})^\times$, and $\mathrm{ord}_\mathfrak{p}(\alpha)$ is the order of $\overline{\alpha}$ in the multiplicative group $(\mathcal{O}\mathfrak{p}/\mathfrak{p})^\times$.

For a positive integer r we denote by $\mathcal{P}_\mathbb{K}(\alpha, r)$ the set of $\mathbb{K}$-primes $\mathfrak{p}$ such that the multiplicative order $\mathrm{ord}_\mathfrak{p}(\alpha)$ is divisible by r. In symbols:

$$\mathcal{P}_\mathbb{K}(\alpha, r) := \{\mathfrak{p} : r \mid \mathrm{ord}_\mathfrak{p}(\alpha)\}.$$

Proposition 6.2. *Let r be a positive integer with the property*

$$\zeta_p \in \mathbb{K} \text{ for every } p \mid r. \tag{6.2}$$

Let $\alpha \in \mathbb{K}^\times$ be not a root of unity. Then the set $\mathcal{P}_\mathbb{K}(\alpha, r)$ is infinite, and, moreover, it is of positive lower density.

The proof of Proposition 6.2 depends on the following lemma.

Lemma 6.3. *Let p be a prime number and $\mathbb{K}$ a field of characteristic distinct from p. Define ℓ as the biggest integer such that $\zeta_{p^\ell} \in \mathbb{K}$. Assume that $\ell \geq 1$. Let $\alpha \in \mathbb{K}$ be such that $\alpha^{1/p} \in \mathbb{K}(\zeta_{p^{\ell+1}})$. Then $\alpha \in \mu_{p^\ell}\mathbb{K}^p$.*

Proof. We may assume that $\alpha \neq 0$, since there is nothing to prove otherwise. We use Kummer's Theory, as in Theorem 8.1 from [13, Chapter VI]. Let B be the subgroup of the multiplicative group $\mathbb{K}^\times$ generated by α, μ_{p^ℓ} and $(\mathbb{K}^\times)^p$. By the hypothesis, $\mathbb{K}(B^{1/p}) = \mathbb{K}(\zeta_{p^{\ell+1}})$. The above-mentioned theorem implies that

$$[B : (\mathbb{K}^\times)^p] = [\mathbb{K}(B^{1/p}) : \mathbb{K}] = [\mathbb{K}(\zeta_{p^{\ell+1}}) : \mathbb{K}] = p.$$

Since $[\mu_{p^\ell}(\mathbb{K}^\times)^p : (\mathbb{K}^\times)^p] = p$, this proves that $B = \mu_{p^\ell}(\mathbb{K}^\times)^p$, which exactly means that $\alpha \in \mu_{p^\ell}(\mathbb{K}^\times)^p$. □

Proof of Proposition 6.2. If the statement holds true with $\mathbb{K}$ replaced by a bigger field, then it is true for $\mathbb{K}$. Indeed, let $\mathbb{K}'$ be a finite extension of $\mathbb{K}$. If $\mathfrak{p}$ is a $\mathbb{K}$-prime, and $\mathfrak{p}'$ is a $\mathbb{K}'$-prime above $\mathfrak{p}$, then for any $\alpha \in \mathbb{K}^\times$ we have $\mathrm{ord}_{\mathfrak{p}'}(\alpha) = \mathrm{ord}_\mathfrak{p}(\alpha)$; so, it suffices to to show that the set $\mathcal{P}_{\mathbb{K}'}(\alpha, r)$ is of positive lower density. Thus, we may assume that $\sqrt{-1} \in \mathbb{K}$.

Let m be the order of the group of roots of unity $\mu_\mathbb{K}$. Condition (6.2) may be re-stated as $p \mid r \Rightarrow p \mid m$.

[2]We prefer the spelling *Chebotaryov*, as in [23], because it is more consistent with the original Russian and Ukrainian pronunciation.

[3]This is in conflict with the convention of Section 5, where $x \mapsto \overline{x}$ denotes the complex conjugation. However, in this section we never use complex conjugation, so there is no risk of confusion.

If the conclusion of the proposition holds true with r replaced a multiple of r, then it holds for r. Hence we may replace r by $\prod_{p|r} p^{\max\{\nu_p(r),\nu_p(m)+1\}}$ and assume in the sequel that

$$\nu_p(r) > \nu_p(m) \qquad (p \mid m); \tag{6.3}$$

in particular, $p \mid r \Leftrightarrow p \mid m$.

Next, we may replace α by $\alpha\xi$, where $\xi \in \mathbb{K}$ is a root of unity. Indeed, if $r \mid \mathrm{ord}_{\mathfrak{p}}(\alpha)$, then $\nu_p\big(\mathrm{ord}_{\mathfrak{p}}(\xi)\big) < \nu_p\big(\mathrm{ord}_{\mathfrak{p}}(\alpha)\big)$ for every $p \mid \mathrm{ord}_{\mathfrak{p}}(\xi)$, by (6.3). Hence $\mathrm{ord}_{\mathfrak{p}}(\alpha\xi) = \mathrm{ord}_{\mathfrak{p}}(\alpha)$.

Finally, we may assume that

$$\alpha \notin \mu_{\mathbb{K}}\mathbb{K}^p \qquad (p \mid r). \tag{6.4}$$

Indeed, call α with property (6.4) *r-reduced*. Since α is not a root of unity, we have $\alpha\xi = \beta^N$, where β is r-reduced, N is composed of primes dividing r and ξ is a root of unity. Now, if $Nr \mid \mathrm{ord}_{\mathfrak{p}}(\beta)$ then $r \mid \mathrm{ord}_{\mathfrak{p}}(\alpha\xi) = \mathrm{ord}_{\mathfrak{p}}(\alpha)$. Hence we may assume (6.4), replacing α by β and r by Nr.

Denote $\mathbb{L} := \mathbb{K}(\zeta_r)$. Properties (6.2) and (6.3) imply that

$$\mathrm{Gal}(\mathbb{L}/\mathbb{K}) \cong \prod_{p|m} \mathbb{Z}/p^{\nu_p(r/m)}\mathbb{Z}.$$

In particular, for every $p \mid r$, the extension $\mathbb{L}$ has exactly one subfield of degree p over $\mathbb{K}$; precisely, it is $\mathbb{K}(\zeta_{p^{\ell_p+1}})$, where $\ell_p := \nu_p(m)$.

Pick some value of the r^{th} root $\alpha^{1/r}$. This would define the roots $\alpha^{1/p}$ for every $p \mid r$. We claim that $\alpha^{1/p} \notin \mathbb{L}$ for any $p \mid r$. Indeed, in the opposite case, $\mathbb{K}(\alpha^{1/p})$ would be a subfield of $\mathbb{L}$ of degree p over $\mathbb{K}$. This would imply $\alpha^{1/p} \in \mathbb{K}(\zeta_{p^{\ell_p+1}})$, which, by Lemma 6.3, implies that $\alpha \in \mu_{p^{\ell_p}}\mathbb{K}^p$, contradicting (6.4).

Lemma 2.1, together with Remark 2.2, implies now that $\mathbb{M} := \mathbb{L}(\alpha^{1/r})$ is an extension of $\mathbb{L}$ of degree r. Moreover, since $\zeta_r \in \mathbb{L}$, extension $\mathbb{M}/\mathbb{L}$ is cyclic, and the map

$$\sigma \mapsto \xi_\sigma : \frac{(\alpha^{1/r})^\sigma}{\alpha^{1/r}} \tag{6.5}$$

defines an isomorphism of the groups $H := \mathrm{Gal}(\mathbb{M}/\mathbb{L})$ and μ_r.

Since $\mathbb{L} = \mathbb{K}(\zeta_r)$, extension $\mathbb{M}/\mathbb{K}$ is Galois, and we denote $G := \mathrm{Gal}(\mathbb{M}/\mathbb{K})$. Then H is the subgroup of G fixing ζ_r.

Let $\mathfrak{p}$ be a $\mathbb{K}$-prime not dividing r and satisfying $\nu_{\mathfrak{p}}(\alpha) = 0$. In particular, $\mathfrak{p}$ does not ramify in $\mathbb{M}$. For an $\mathbb{M}$-prime $\mathfrak{P}$ above $\mathfrak{p}$, we denote by $\phi_{\mathfrak{P}} \in G$ the Frobenius of $\mathfrak{P}$ above $\mathbb{K}$. Recall that $\phi_{\mathfrak{P}}$ is the element of G with the following property: let $\mathcal{O}_{\mathfrak{P}} := \{x \in \mathbb{M} : \nu_{\mathfrak{P}}(x) \geq 0\}$ be the local ring of $\mathfrak{P}$; then for every $x \in \mathcal{O}_{\mathfrak{P}}$ we have $x^{\mathcal{N}_{\mathfrak{p}}} \equiv x^{\phi_{\mathfrak{P}}} \pmod{\mathfrak{P}}$ (as before, $\mathcal{N}(\cdot)$ denotes the absolute norm).

Next, let $\big((\mathbb{M}/\mathbb{K})/\mathfrak{p}\big) := \{\phi_{\mathfrak{P}} : \mathfrak{P} \mid \mathfrak{p}\}$ be the Artin symbol of $\mathfrak{p}$. Note that it is a full conjugacy class in G. Denote by Σ the subset of H consisting of the

elements of exact order r. In symbols: $\Sigma := \{\sigma \in H : H = \langle\sigma\rangle\}$. Let $\mathfrak{p}$ be such that $\big((\mathbb{M}/\mathbb{K})/\mathfrak{p}\big) \subset \Sigma$. By the Theorem of Chebotaryov, the set of such $\mathfrak{p}$ is of positive density[4], so we only have to prove that $r \mid \mathrm{ord}_{\mathfrak{p}}(\alpha)$.

We are going to prove that $r \mid \mathcal{N}\mathfrak{p} - 1$, but $\overline{\alpha}$ is not a p^{th} power in $(\mathcal{O}_{\mathfrak{p}}/\mathfrak{p})^{\times}$ for any $p \mid r$. Since $\mathcal{N}\mathfrak{p} - 1$ is the order of the cyclic group $(\mathcal{O}_{\mathfrak{p}}/\mathfrak{p})^{\times}$, the order of $\overline{\alpha}$ in this group must be divisible by r, as wanted.

As before, let $\mathfrak{P}$ be an $\mathbb{M}$-prime above $\mathfrak{p}$. Since $\phi_{\mathfrak{P}} \in \Sigma \subset H$, we have $\phi_{\mathfrak{P}}(\zeta_r) = \zeta_r$, which means that $\zeta_r^{\mathcal{N}\mathfrak{p}} \equiv \zeta_r \pmod{\mathfrak{P}}$. Since $\mathfrak{P} \nmid r$, this implies that $\zeta_r^{\mathcal{N}\mathfrak{p}} = \zeta_r$, that is, $r \mid \mathcal{N}\mathfrak{p} - 1$.

We are left with proving that $\overline{\alpha}$ is not a p^{th} power in $(\mathcal{O}_{\mathfrak{p}}/\mathfrak{p})^{\times}$ for any prime p dividing r. Fix such p. Since $\phi_{\mathfrak{P}} \in \Sigma$, it is of exact order r in H. Hence $\xi := \xi_{\phi_{\mathfrak{P}}}$ (as defined in (6.5)) is a primitive r^{th} root of unity, and $\eta := \xi^{r/p}$ is a primitive p^{th} root of unity.

Applying (6.5) with $\sigma = \phi_{\mathfrak{P}}$, we obtain $\alpha^{(\mathcal{N}\mathfrak{p}-1)/r} \equiv \xi \pmod{\mathfrak{P}}$. Raising this congruence to the power r/p, we obtain $\alpha^{(\mathcal{N}\mathfrak{p}-1)/p} \equiv \eta \pmod{\mathfrak{P}}$. Since both sides of this congruence belong to $\mathbb{K}$, it is actually a congruence modulo $\mathfrak{p}$, and it implies the identity $\overline{\alpha}^{(\mathcal{N}\mathfrak{p}-1)/p} = \overline{\eta}$ in the group $(\mathcal{O}_{\mathfrak{p}}/\mathfrak{p})^{\times}$. If $\overline{\alpha}$ is a p^{th} power in $(\mathcal{O}_{\mathfrak{p}}/\mathfrak{p})^{\times}$ then $\overline{\alpha}^{(\mathcal{N}\mathfrak{p}-1)/p} = 1$, which is impossible because $\overline{\eta}$ is a primitive p^{th} root of unity. This completes the proof of the proposition. □

6.2 Proof of Theorem 6.1

Besides Proposition 6.2, the proof of Theorem 6.1 relies on the following lemma. It is very classical and goes back to the work of Lucas [15] or even earlier. Still, we give a proof for convenience.

Lemma 6.4. *Let $\mathbb{K}$ be a number field, $\mathfrak{p}$ a prime of $\mathbb{K}$ with underlying rational prime p and $e := \nu_{\mathfrak{p}}(p)$ the ramification index. Let $\theta \in \mathbb{K}$ be such that $\nu_{\mathfrak{p}}(\theta - 1) > 0$ and $n \in \mathbb{Z}$. Then we have the following.*

1. *If $p \nmid n$ then $\nu_{\mathfrak{p}}(\theta^n - 1) = \nu_{\mathfrak{p}}(\theta - 1)$.*
2. *In general, $\nu_{\mathfrak{p}}(\theta^n - 1) \geq \nu_{\mathfrak{p}}(\theta - 1) + \nu_p(n)\min\{e, (p-1)\nu_{\mathfrak{p}}(\theta - 1)\}$.*
3. *If $\nu_{\mathfrak{p}}(\theta - 1) > e/(p-1)$ then $\nu_{\mathfrak{p}}(\theta^n - 1) = \nu_{\mathfrak{p}}(\theta - 1) + e\nu_p(n)$.*

Proof. Item 1 must be proved only for $n > 0$ and $n = -1$. If $n > 0$ then

$$\theta^n - 1 = (\theta - 1)(\theta^{n-1} + \cdots + 1).$$

Since $\theta \equiv 1 \pmod{\mathfrak{p}}$ in the local ring $\mathcal{O}_{\mathfrak{p}}$, we have

$$\theta^{n-1} + \cdots + 1 \equiv n \pmod{\mathfrak{p}}.$$

In particular, $\nu_{\mathfrak{p}}(\theta^{n-1} + \cdots + 1) = 0$ if $p \nmid n$. This proves item 1 for $n > 0$. As for $n = -1$, it is obvious that $\nu_{\mathfrak{p}}(\theta^{-1} - 1) = \nu_{\mathfrak{p}}(\theta - 1)$.

[4] Actually, it is of density $\#\Sigma/\#G$, but the exact value of the density is not relevant to us.

Due to item 1, in items 2 and 3 we may assume that $n = p^k$. Moreover, using induction in k, we may assume that $n = p$. Write $\theta = 1 + \gamma$. Then

$$\theta^p - 1 = p\gamma + \sum_{\ell=2}^{p-1} \binom{p}{\ell} \gamma^\ell + \gamma^p.$$

Each of the terms inside the sum has $\mathfrak{p}$-adic valuation strictly bigger than $\nu_\mathfrak{p}(p\gamma) = \nu_\mathfrak{p}(\gamma) + e$. Hence

$$\nu_\mathfrak{p}(\theta^p - 1) \geq \nu_\mathfrak{p}(\gamma) + \min\{e, (p-1)\nu_\mathfrak{p}(\gamma)\} \tag{6.6}$$

which proves item 2. Finally, when $\nu_\mathfrak{p}(\gamma) > e/(p-1)$, inequality (6.6) becomes equality, and the minimum on the right is e, which proves item 3. □

Now we are ready to prove Theorem 6.1.

Proof of Theorem 6.1. By shifting, we may assume that $a = 0$. Thus, we have to prove that, for infinitely many $\mathbb{K}$-primes $\mathfrak{p}$ the following holds: there exist Q, a' and τ as in the statement of the theorem such that

$$\nu_\mathfrak{p}(U(n)) = \nu_\mathfrak{p}(n) + \tau \qquad \text{when} \quad n \equiv a' \pmod{Q}. \tag{6.7}$$

If the statement holds true with $\mathbb{K}$ replaced by a bigger number field, then it holds for $\mathbb{K}$. Hence we may assume that the roots of the characteristic polynomial of U belong to $\mathbb{K}$. Multiplying $U(n)$ by $\beta\theta^n$ with suitable $\beta, \theta \in \mathbb{K}^\times$, we may assume that either $U(n) = n - \beta$, where $\beta \in \mathbb{K}$, or $U(n) = \eta\lambda^n - 1$, where $\eta, \lambda \in K^\times$. If $U(n) = n - \beta$ and 0 is a twisted zero of U, then $\beta = 0$ and $U(n) = n$, so there is nothing to prove.

Now let us assume that $U(n) = \eta\lambda^n - 1$. Note that λ is not a root of unity, because U is non-degenerate. Since 0 is a twisted zero of U, we have $\eta\lambda^0 - \xi = 0$ for some root of unity ξ. Hence η is a root of unity. Denote by r its order.

Let $\mathcal{P}'_\mathbb{K}(\lambda, r)$ be the subset of $\mathcal{P}_\mathbb{K}(\lambda, r)$, consisting of $\mathfrak{p} \in \mathcal{P}_\mathbb{K}(\lambda, r)$, unramified and of degree 1 over $\mathbb{Q}$, and with underlying prime $\mathcal{N}\mathfrak{p} > 2$. Proposition 6.2 implies that the set $\mathcal{P}_\mathbb{K}(\lambda, r)$ is of positive lower density. Hence so is $\mathcal{P}'_\mathbb{K}(\lambda, r)$: this is because the set of unramified primes of degree 1 is of density 1. We claim that for every $\mathfrak{p} \in \mathcal{P}'_\mathbb{K}(\lambda, r)$, there exist Q, a' and τ as in (6.1) such that (6.7) holds, and $p \nmid Q$.

Thus, fix $\mathfrak{p} \in \mathcal{P}'_\mathbb{K}(\lambda, r)$. Since $\mathfrak{p}$ is of degree 1, the cyclic group $(\mathcal{O}_\mathfrak{p}/\mathfrak{p})^\times$ is of order $p - 1$, where $p := \mathcal{N}\mathfrak{p}$ is an odd prime number. Since $r \mid \mathrm{ord}_\mathfrak{p}(\lambda)$, the subgroup $\langle\overline{\lambda}\rangle$ of $(\mathcal{O}_\mathfrak{p}/\mathfrak{p})^\times$ contains $\overline{\eta}$. Hence there exists $s \in \{1, \ldots, p-1\}$ such that $\eta\lambda^s \equiv 1 \pmod{\mathfrak{p}}$. Lemma 6.4 implies that

$$\nu_\mathfrak{p}\big((\eta\lambda^s)^m - 1\big) = \nu_p(m) + \nu_\mathfrak{p}(\xi\lambda^s - 1) \qquad (m \in \mathbb{Z}).$$

Now note that, when $m \equiv 1 \pmod{r}$, we have $(\xi\lambda^s)^m - 1 = U(sm)$. Hence (6.7) holds with

$$Q := rs, \qquad a' := s, \qquad \tau := \nu_\mathfrak{p}(\xi\lambda^s - 1).$$

Note also that $p \nmid Q$ because $r \mid p - 1$ and $1 \leq s \leq p - 1$. The theorem is proved. □

Remark 6.5. *1. Our argument can be illustrated with the LRS from Example 1.3. In that case*

$$\mathbb{K} = \mathbb{Q}, \qquad \lambda = 2, \qquad \eta = -1, \qquad r = 2, \qquad s = \frac{p-1}{2},$$

and the set $\mathcal{P}'_{\mathbb{Q}}(2,2)$ contains all the primes satisfying $p \equiv \pm 3 \pmod 8$ (and some other primes as well).

2. This argument does not extend to rational a, because we can no longer do the shifting and assume that $a = 0$. We do not know whether Theorem 6.1 can be extended to twisted rational zeros.

3. The non-degeneracy hypothesis cannot be dropped. Indeed, consider

$$U(n) := \zeta_3^n + \overline{\zeta_3}^n = \begin{cases} 2, & \text{if } 3 \mid n, \\ -1, & \text{if } 3 \nmid n. \end{cases}$$

Then 0 is a twisted zero of U, but $\nu_p(U(n)) = 0$ for all n and all $p \neq 2$.

6.3 Concluding remarks

As we already indicated in the introduction, the answer to Question 1.7 is negative for LRS of order 3 or higher. Here is an example of order 3, but one can easily construct similar examples of any order.

Example 6.6. *Let p be a prime number. The LRS $U(n) := 8^n + 2^n + 1$ has a twisted zero at 0, because $1 + \zeta_3 + \overline{\zeta_3} = 0$. However, there does not exist a sequence (n_k) such that*

$$\nu_p(U(n_k)) \to +\infty, \qquad \nu_p(n_k) \to +\infty.$$

Indeed, let (n_k) be such a sequence. Let $\mathbb{K}$ be the splitting field of the polynomial $X^3 + X + 1$ and $\mathfrak{p}$ a prime of $\mathbb{K}$ above p. Then, replacing (n_k) by a subsequence, we have

$$\nu_{\mathfrak{p}}(2^{n_k} - \alpha) \to +\infty, \qquad \nu_{\mathfrak{p}}(n_k) \to +\infty$$

for some root α of this polynomial. Theorem 3.5 implies that 0 is a twisted zero of the LRS $2^n - \alpha$, a contradiction, because α is not a root of unity.

To conclude, let us ask one more question. Theorem 1.5 deals with just one individual prime number. What happens if a sequence (n_k) satisfying (1.5) can be found for all but finitely many primes? One may expect that in this case a is a genuine zero of U, not merely a TRZ.

Question 6.7. *Let U be an LRS with values in a number field $\mathbb{K}$, and $a \in \mathbb{Q}$. Assume that for every $\mathbb{K}$-prime $\mathfrak{p}$, with finitely many exceptions, there exist a sequence of integers (n_k) (depending on $\mathfrak{p}$) such that*

$$\nu_{\mathfrak{p}}(U(n_k)) \to +\infty, \qquad \nu_{\mathfrak{p}}(n_k - a) \to +\infty.$$

Does it imply that either a a trivial TRZ (as defined in Subsection 4.5) or $a \in \mathbb{Z}$ and $U(a) = 0$?

Probably, "all but finitely many primes" can be replaced by "primes from a set of density 1". But, as Example 1.3 shows, it is not enough to assume that this holds for infinitely many primes, or even for primes from a set of positive lower density.

Acknowledgments

Yuri Bilu and Florian Luca were supported by the ANR project JINVARIANT. James Worrell was supported by UKRI Fellowship EP/X033813/1.

While working on this project, Yuri Bilu enjoyed hospitality and support of MPIM Bonn, where he was visiting in June 2023.

Florian Luca worked on this paper in 2023 during research visits at the MPI-SWS, Saarbrücken, Germany and the Stellenbosch Institute for Advanced Studies, Stellenbosch, South Africa. He thanks these institutions for their hospitality and support.

Joël Ouaknine is also affiliated with Keble College, Oxford as `emmy.network` Fellow, and supported by DFG grant 389792660 as part of TRR 248 (see `https://perspicuous-computing.science`).

References

[1] H. Bass, *A remark on an arithmetic theorem of Chevalley*, Proc. Amer. Math. Soc. **16** (1965), 875–878. MR 184925

[2] Yuri Bilu, *The Chevalley-Bass Theorem*, Essays in Analytic Number Theory In Honor of Helmut Maier's 70th Birthday, to appear, arXiv:2305.05041 (2023).

[3] Yuri Bilu, Florian Luca, Joris Nieuwveld, Joël Ouaknine, David Purser, and James Worrell, *Skolem meets Schanuel*, 47th International Symposium on Mathematical Foundations of Computer Science, LIPIcs. Leibniz Int. Proc. Inform., vol. 241, Schloss Dagstuhl. Leibniz-Zent. Inform., Wadern, 2022, pp. Art. No. 20, 15. MR 4481938

[4] Yuri Bilu, Florian Luca, Joris Nieuwveld, Joël Ouaknine, David Purser, and James Worrell, *The Skolem Tool*, `\https://skolem.mpi-sws.org`, 2022, [Online; accessed 15-November-2023].

[5] Yuri Bilu, Florian Luca, Joris Nieuwveld, Jöel Ouaknine, and James Worrell, *On the p-adic zeros of the Tribonacci sequence*, Math. Comp. (2023).

[6] Enrico Bombieri and Walter Gubler, *Heights in Diophantine geometry*, New Mathematical Monographs, vol. 4, Cambridge University Press, Cambridge, 2006. MR 2216774

[7] J. W. S. Cassels, *An embedding theorem for fields*, Bull. Austral. Math. Soc. **14** (1976), 193–198, 479–480. MR 422221

[8] ———, *Local fields*, London Mathematical Society Student Texts, vol. 3, Cambridge University Press, Cambridge, 1986. MR 861410

[9] Claude Chevalley, *Deux théorèmes d'arithmétique*, J. Math. Soc. Japan **3** (1951), 36–44. MR 44570

[10] J. H. Conway and A. J. Jones, *Trigonometric Diophantine equations (On vanishing sums of roots of unity)*, Acta Arith. **30** (1976), no. 3, 229–240. MR 422149

[11] Roberto Dvornicich and Umberto Zannier, *On sums of roots of unity*, Monatsh. Math. **129** (2000), no. 2, 97–108. MR 1742911

[12] Fernando Q. Gouvêa, *p-adic numbers*, Universitext, Springer, Cham, 2020. MR 4175370

[13] Serge Lang, *Algebra*, third ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002. MR 1878556

[14] Michel Laurent, *Équations diophantiennes exponentielles*, Invent. Math. **78** (1984), no. 2, 299–327. MR 767195

[15] Edouard Lucas, *Theorie des Fonctions Numeriques Simplement Periodiques*, Amer. J. Math. **1** (1878), no. 4, 289–321. MR 1505176

[16] Henry B. Mann, *On linear relations between roots of unity*, Mathematika **12** (1965), 107–117. MR 191892

[17] Diego Marques and Tamás Lengyel, *The* 2*-adic order of the Tribonacci numbers and the equation* $T_n = m!$, J. Integer Seq. **17** (2014), no. 10, Article 14.10.1, 8. MR 3275869

[18] M. Mignotte and N. Tzanakis, *Arithmetical study of recurrence sequences*, Acta Arith. **57** (1991), no. 4, 357–364. MR 1109992

[19] W. H. Schikhof, *Ultrametric calculus*, Cambridge Studies in Advanced Mathematics, vol. 4, Cambridge University Press, Cambridge, 2006, An introduction to p-adic analysis, Reprint of the 1984 original [MR0791759]. MR 2444734

[20] John H. Smith, *A result of Bass on cyclotomic extension fields*, Proc. Amer. Math. Soc. **24** (1970), 394–395. MR 257049

[21] C. J. Smyth, *On the product of the conjugates outside the unit circle of an algebraic integer*, Bull. London Math. Soc. **3** (1971), 169–175. MR 289451

[22] The PARI Group, Univ. Bordeaux, *PARI/GP version 2.15.4*, 2023, available from `http://pari.math.u-bordeaux.fr/`.

[23] Wikipedia, *Nikolai Chebotaryov*, `https://en.wikipedia.org/wiki/Nikolai_Chebotaryov`, 2023, [Online; accessed 15-November-2023].

[24] U. Zannier, *Vanishing sums of roots of unity*, Rend. Sem. Mat. Univ. Politec. Torino **53** (1995), no. 4, 487–495, Number theory, II (Rome, 1995). MR 1452400