On the $p$-adic zeros of the Tribonacci sequence

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

Florian Luca  
School of Maths, Wits, South Africa  
Research Group in Algebraic Structures and Applications,  
King Abdulaziz University, Saudi Arabia  
CCM, UNAM, Morelia, Mexico  
E-mail: Florian.Luca@wits.ac.za,

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

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

November 1, 2022

Contents

1 Introduction 2  
2 Rational zeros of the Tribonacci sequence 6  
3 $p$-adic analytic functions 8  
3.1 $p$-adic order of values of an analytic function 5  
3.2 Vanishing of power series 10  
3.3 Functions exp and log in the $p$-adic domain 11  
4 $p$-adic analytic interpolation of the Tribonacci sequence 11  
5 Proof of Theorem 1.5 12  
6 Analytic form of Conjectures 1.2 and 1.6 14  
7 Detecting zeros of $f_\ell(z)$ 16  
7.1 A non-vanishing condition 16  
7.2 The first vanishing condition 16  
7.3 The second vanishing condition 17  
8 Sufficient conditions for validity and for failure of Conjectures 1.2 and 1.6 18  
9 The proofs of Theorems 1.4, 1.7, and 1.8 19  
10 Conjectures and Heuristics 23
1 Introduction

Let $\Lambda = \{\lambda_1, \lambda_2, \lambda_3\} \subset \mathbb{Q}$ be the set of roots of the polynomial

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

For $\lambda \in \Lambda$ define $c_\lambda = \lambda P'(\lambda)^{-1}$. For $n \in \mathbb{Z}$, the Tribonacci number $T(n) \in \mathbb{Z}$ is defined by

$$T(n) = \sum_{\lambda \in \Lambda} c_\lambda \lambda^n.$$

More famously, $T : \mathbb{Z} \to \mathbb{Z}$ is defined by the recurrence relation

$$T(0) = 0, \quad T(1) = T(2) = 1, \quad T(n + 3) = T(n + 2) + T(n + 1) + T(n) \quad (n \in \mathbb{Z}).$$

Attention: $u(n)$ in [8] corresponds to our $T(n + 1)$.

It is known that $T(n) = 0$ if and only if $n \in \mathbb{Z}_T := \{0, -1, -4, -17\}$. For a proof see, for instance, [10], Example 2 on page 360; in that example $u_n$ corresponds to our $T(n + 1)$. In [9], Marques and Lengyel determined the exponent of 2 in $T_n$. Denoting for a prime $p$ and an nonzero integer $m$ by $\nu_p(m)$ the exact exponent of $p$ in the factorization of $m$, and setting $\nu_p(0) = \infty$, they proved the following theorem.

**Theorem 1.1.** For $n \geq 1$, we have

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

Encouraged by their result for the prime $p = 2$, they conjectured that such formulas should hold for $\nu_p(T_n)$ for every prime $p$. More precisely, here is their conjecture.

**Conjecture 1.2 (Conjecture 8 from [9]).** Let $p$ be a prime number. There exists a positive integer $Q$ such that for every $i \in \{0, 1, \ldots, Q - 1\}$ we have one of the following two options.

(C) There exists $\kappa_i \in \mathbb{Z}_{\geq 0}$ such that for all but finitely many $n \in \mathbb{Z}$ satisfying $n \equiv i \pmod{Q}$ we have $\nu_p(T(n)) = \kappa_i$.

(L) There exist $a_i \in \mathbb{Z}$, $\kappa_i \in \mathbb{Z}$, $\mu_i \in \mathbb{Z}_{>0}$.
satisfying

\[ \nu_p(a_i - i) \geq \nu_p(Q), \]  

(1.1)

such that for all but finitely many \( n \in \mathbb{Z} \) satisfying \( n \equiv i \pmod{Q} \) we have

\[ \nu_p(T(n)) = \kappa_i + \mu_i \nu_p(n - a_i). \]  

(1.2)

Note that our statement looks different from Conjecture 8 from [9], but, in fact, it is equivalent to it.

Informally, in the case (C) (that is, “constant”) \( \nu_p(T(n)) \) is a constant function on the entire residue class \( n \equiv i \pmod{Q} \) with finitely many \( n \) removed, while in the case (L) (“linear”) it is a linear function of \( \nu_p(n - a_i) \).

**Remark 1.3.** Let us comment on condition (1.1), which does not appear in [9]. This condition is needed to ensure that the right-hand side of (1.2) is not constant (in which case option (C) would hold for the class \( n \equiv i \pmod{Q} \)). To be precise, the following three statements are equivalent:

1. (1.1) holds;
2. \( \nu_p(n - a_i) \) is not constant on the residue class \( n \equiv i \pmod{Q} \);
3. \( \nu_p(n - a_i) \) is not bounded on the residue class \( n \equiv i \pmod{Q} \).

Indeed, if \( \nu_p(a_i - i) < \nu_p(Q) \) then \( \nu_p(n - a_i) = \nu_p(i - a_i) \) for \( n \equiv i \pmod{Q} \), which proves the implication 2 \( \Rightarrow \) 3. The implication 3 \( \Rightarrow \) 2 is obvious. Finally, assume that (1.1) holds. Denoting \( \nu := \nu_p(Q) \), for every \( k \geq \nu \) the Chinese remainder theorem provides \( m_k \in \mathbb{Z} \) satisfying

\[ m_k \equiv \frac{a_i - i}{p^\nu} \pmod{p^{k-\nu}}, \quad m_k \equiv 0 \pmod{Q p^{-\nu}}. \]

Then \( n_k := i + m_k p^\nu \) satisfies \( n_k \equiv a_i \pmod{p^k} \) and \( n_k \equiv i \pmod{Q} \), which proves the implication 3 \( \Rightarrow \) 2.

Already the case \( p = 3 \) looks encouraging.

**Theorem 1.4.** For \( n \geq 1 \), we have

\[
\nu_3(T_n) = \begin{cases} 
0, & \text{if } n \equiv 1, 2, 3, 4, 5, 6, 8, 10, 11 \pmod{13}; \\
1, & \text{if } n \equiv 7 \pmod{13}; \\
\nu_3(n) + 2, & \text{if } n \equiv 0 \pmod{13}; \\
\nu_3(n + 1) + 2, & \text{if } n \equiv 12 \pmod{13}; \\
4, & \text{if } n \equiv 9 \pmod{39}; \\
\nu_3(n + 17) + 4, & \text{if } n \equiv 22 \pmod{39}; \\
\nu_3(n + 4) + 4, & \text{if } n \equiv 35 \pmod{39}.
\end{cases}
\]

However, the following theorem shows that Conjecture 1.2 fails for infinitely many primes.
Theorem 1.5. There is an infinite set of prime numbers congruent to 2 (mod 3) such that for every prime $p$ from this set the following holds.

1. For each $n \in \mathbb{Z}$ satisfying $n \equiv 1/3 \pmod{p-1}$ we have
$$\nu_p(T(n)) \geq \nu_p(n - 1/3).$$

2. For each $n \in \mathbb{Z}$ with $n \equiv -5/3 \pmod{p-1}$ we have
$$\nu_p(T(n)) \geq \nu_p(n + 5/3).$$

Clearly, Theorem 1.5 contradicts Conjecture 1.2. Indeed, let $p$ be as in the theorem, and let $(n_k)$ be a sequence of integers satisfying $n_k \equiv 1/3 \pmod{(p-1)p^k}$. If Conjecture 1.2 is true for this $p$ then for some $i \in \{0, \ldots, Q-1\}$ the residue class $i$ (mod $Q$) contains infinitely many $n_k$. Since $\nu_p(n_k - 1/3) \to \infty$, we have $\nu_p(T(n)) \to \infty$. Hence for this $i$ we must have option (L) of Conjecture 1.2:
$$\nu_p(T(n_k)) = \kappa_i + \mu_i \nu_p(n_k - a_i).$$

Moreover, we must have $\nu_p(n_k - a_i) \to \infty$ as well. But, since $a_i \in \mathbb{Z}$, we have $a_i \neq 1/3$, and hence $\nu_p(n_k - 1/3)$ and $\nu_p(n_k - a_i)$ cannot both tend to infinity.

One may hope to rescue Conjecture 1.2 by allowing $a_i$ to be rational numbers, as below:

Conjecture 1.6. Let $p$ be a prime number. There exists a positive integer $Q$ such that for every $i \in \{0, 1, \ldots, Q-1\}$ we have one of the following two options.

(C) There exists $\kappa_i \in \mathbb{Z}_{\geq 0}$ such that for all but finitely many $n \in \mathbb{Z}$ satisfying $n \equiv i \pmod{Q}$ we have $\nu_p(T(n)) = \kappa_i$.

(L) There exist $a_i \in \mathbb{Q}$, $\kappa_i \in \mathbb{Z}$, $\mu_i \in \mathbb{Z}_{>0}$ satisfying $\nu_p(a_i - i) \geq \nu_p(Q)$, such that for all but finitely many $n \in \mathbb{Z}$ satisfying $n \equiv i \pmod{Q}$ we have $\nu_p(T(n)) = \kappa_i + \mu_i \nu_p(n - a_i)$.

However we show that even this weaker conjecture fails for many primes. In fact we provide a method to decide for which primes $p$ Conjectures 1.2 and 1.6 hold and for which they fail. In some cases our method is unable to make the desired decision. When the method works and decides that the conjecture holds, it also determines the parameters $Q$ and $(a_i, \mu_i)$ for those $i = \{0, \ldots, Q-1\}$ for which option (L) takes place.

Concerning Conjecture 1.2 we have:

1We will see that this set of primes is not only infinite, but is of relative density $1/12$ in the set of all primes.
Theorem 1.7. (i) Conjecture 1.2 fails for $p \in [5, 599] \setminus \{11, 83, 103, 163, 397\}$.

(ii) Conjecture 1.2 holds for $p \in \{83, 397\}$ in the form

$$\nu_p(T_n) = \begin{cases} 
\nu_p(n + c) + 1, & \text{if } n \equiv -c \pmod{Q_p}, -c \in \mathbb{Z}_T; \\
0, & \text{otherwise},
\end{cases}$$

with $Q_{83} = 287$ and $Q_{397} = 132$.

Note that our method does not handle the prime $p = 11$. As for $p \in \{103, 163\}$, our method failed to decide whether Conjecture 1.2 holds.

Concerning Conjecture 1.6, we have:

Theorem 1.8. (i) Conjecture 1.6 fails for $p \in [5, 599] \setminus \{11, 47, 53, 83, 103, 163, 269, 397, 401, 419, 499, 587\}$.

(ii) Conjecture 1.6 holds for $p \in \{269, 401, 419, 499, 587\}$ in the form

$$\nu_p(T_n) = \begin{cases} 
\nu_p(n + c) + 1, & \text{if } n \equiv c \pmod{Q_p}, c \in \{0, -1, -4, -17, 1/3, -5/3\}; \\
0, & \text{otherwise},
\end{cases}$$

with $Q_{269} = 268$, $Q_{401} = 400$, $Q_{419} = 418$, $Q_{499} = 166$ and $Q_{587} = 293$.

Note here that (again) our method does not apply to the prime $p = 11$. As for $p \in \{47, 53, 103, 163\}$, our method failed to decide whether Conjecture 1.6 holds.

Plan of the article In Section 2 we introduce the basic notions of this article, those of twisted zeros and of rational zeros of the Tribonacci sequence.

In Section 3 we recall the necessary tools from $p$-adic analysis. In Sections 4–8 we apply these tools to study the Tribonacci sequence. In particular, Theorem 1.5 is proved in Section 5. In Section 6 we give a $p$-adic analytic interpretation of Conjectures 1.2 and 1.6. Using it, we produce in Section 8 easily verifiable sufficient conditions for both conjectures to hold and to fail.

Theorems 1.4 and 1.7 are proved in Section 9 as application of the previous results together with some computations.

The final Section 10 contains heuristics which suggest that if $\mathcal{ML}$ and $\mathcal{NMLR}$ are the sets of all primes such that Conjecture 1.2 holds and Conjecture 1.6 and fails, respectively, then both $\mathcal{ML}$ and $\mathcal{NMLR}$ are infinite and maybe even of positive relative densities as subsets of all primes.

A convention Unless otherwise stated, all congruences such as $x \equiv y \pmod{N}$ and divisibility relations such as $x \mid y$ refer to the ring of rational integers $\mathbb{Z}$.

We slightly abuse notation by writing $x \equiv y \pmod{N}$ with $x, y \in \mathbb{Q}$ if there exists $m \in \mathbb{Z}$ with $\gcd(m, N) = 1$ such that $mx, my \in \mathbb{Z}$ and $mx \equiv my \pmod{N}$.
2 Rational zeros of the Tribonacci sequence

As we mentioned in the introduction, \( T(n) = 0 \) if and only if \( n \) belongs to the set \( \mathcal{Z}_T = \{0, -1, -4, -17\} \). It turns out that, in a sense, the Tribonacci sequence also “vanishes” at some non-integral rational numbers.

**Proposition 2.1.** For some definition of the cubic roots

\[
\lambda^{1/3} \quad (\lambda \in \Lambda)
\]

we have

\[
\sum_{\lambda \in \Lambda} c_{\lambda} \lambda^{1/3} = 0.
\]

Similarly, for some definition of the cubic roots \((2.1)\) we have \( \sum_{\lambda \in \Lambda} c_{\lambda} \lambda^{-5/3} = 0 \).

**Proof.** Consider the polynomial

\[
F(X_1, X_2, X_3) = X^3_1 + X^3_2 + X^3_3 - 3X_1X_2X_3 \in \mathbb{Z}[X_1, X_2, X_3].
\]

Write again \( \Lambda = \{\lambda_1, \lambda_2, \lambda_3\} \). Define somehow the cubic roots \( \lambda_1^{1/3}, \lambda_2^{1/3} \) and set \( \lambda_3^{1/3} = (\lambda_1^{1/3} \lambda_2^{1/3})^{-1} \). Now define

\[
\alpha_i = c_{\lambda_i} \lambda_i^{1/3}, \quad \beta_i = c_{\lambda_i} \lambda_i^{-5/3} \quad (i = 1, 2, 3).
\]

A direct verification shows that

\[
F(\alpha_1, \alpha_2, \alpha_3) = \sum_{\lambda \in \Lambda} c_{\lambda} \lambda - 3 \prod_{\lambda \in \Lambda} c_{\lambda} = 0,
\]

and, similarly, \( F(\beta_1, \beta_2, \beta_3) = 0 \). Since \( F(X_1, X_2, X_3) \) factors as

\[
F(X_1, X_2, X_3) = (X_1 + X_2 + X_3)(X_1 + \zeta X_2 + \overline{\zeta} X_3)(X_1 + \overline{\zeta} X_2 + \zeta X_3),
\]

where \( \zeta, \overline{\zeta} \) are the primitive cubic roots of unity, the result follows. \( \square \)

Call \( r \in \mathbb{Q} \) a rational zero of \( T \) if for some definition of the rational powers \( \lambda_1^r, \lambda_2^r, \lambda_3^r \) we have \( \sum_{i=1}^{3} c_{\lambda_i} \lambda_i^r = 0 \).

More generally, call \( r \in \mathbb{Q} \) a twisted rational zero of \( T \) if for some definition of the rational powers \( \lambda_1^r, \lambda_2^r, \lambda_3^r \) and for some roots of unity \( \xi_1, \xi_2, \xi_3 \), we have

\[
\sum_{i=1}^{3} \xi_i c_{\lambda_i} \lambda_i^r = 0.
\]

We denote \( \mathcal{Q}_T \) the set of twisted rational zeros of \( T \). Clearly, \( \mathcal{Z}_T \subset \mathcal{Q}_T \) and \( 1/3, -5/3 \in \mathcal{Q}_T \). It turns out that \( T \) has no other twisted rational zeros.

**Theorem 2.2.** We have

\[
\mathcal{Q}_T = \mathcal{Z}_T \cup \{1/3, -5/3\} = \{0, -1, -4, -17, 1/3, -5/3\}.
\]

Moreover, if \( r \in \mathcal{Q}_T \) and the powers \( \lambda_1^r, \lambda_2^r, \lambda_3^r \) are suitably defined, then for the roots of unity \( \xi_1, \xi_2, \xi_3 \) satisfying \( \sum_{i=1}^{3} \xi_i c_{\lambda_i} \lambda_i^r = 0 \) we have \( \xi_1 = \xi_2 = \xi_3 \).
The full proof of this theorem will appear in [4]. Now we will prove only a weaker version of this theorem, addressing twisted integral zeros.

**Theorem 2.3.** Let \( n \in \mathbb{Z} \) and \( \xi_1, \xi_2, \xi_3 \) roots of unity such that \( \sum_{i=1}^3 \xi_i c_\lambda \lambda_i^n = 0 \). Then \( n \in \mathbb{Z}_T \) and \( \xi_1 = \xi_2 = \xi_3 = 1 \). In particular, the only twisted integral zeros of the Tribonacci sequence are its actual zeros \( 0, -1, -4, -17 \).

**Remark 2.4.** Of course, twisted zeros can be defined for any linear recurrent sequence, not just of the Tribonacci sequence: if \( U(n) \) is a linear recurrence with Binet expansion

\[
U(n) = P_1(n)\gamma_1^n + \cdots + P_s(n)\gamma_s^n
\]

(where \( \gamma_1, \ldots, \gamma_s \) are non-zero algebraic numbers and \( P_1, \ldots, P_s \) are polynomials with algebraic coefficients), then we call \( r \in \mathbb{Q} \) a twisted rational zero of \( U \) if for some definition of the powers \( \gamma_1^n, \ldots, \gamma_s^n \) and some roots of unity \( \xi_1, \ldots, \xi_s \) we have \( \xi_i P_i(r)\gamma_i^n + \cdots + \xi_s P_s(r)\gamma_s^n = 0 \). Note that the analogue of Theorem 2.3 does not hold for any linear recurrent sequence. For instance, the binary sequence \( U(n) = 2^n + 1^n \) has no integral zeros, but it has a twisted zero at \( n = 0 \), the relevant roots of unity being 1 and \(-1\):

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

For the proof of Theorem 2.3 we need some lemmas.

**Lemma 2.5.** Let \( \alpha \) be an algebraic number of degree 3. Assume that \( \mathbb{Q}(\alpha) \) is not a Galois extension of \( \mathbb{Q} \). Let \( \alpha_1 = \alpha, \alpha_2, \alpha_3 \) be the conjugates of \( \alpha \) over \( \mathbb{Q} \). Assume further that the field \( \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) \) does not contain primitive cubic roots of unity.

Let \( \xi_1, \xi_2, \xi_3 \) be roots of unity such that

\[
\alpha_1 \xi_1 + \alpha_2 \xi_2 + \alpha_3 \xi_3 = 0.
\]

Then \( \xi_1 = \xi_2 = \xi_3 \) and hence \( \alpha_1 + \alpha_2 + \alpha_3 = 0 \).

**Proof.** We may assume that \( \xi_3 = 1 \), so that \( \alpha_1 \xi_1 + \alpha_2 \xi_2 + \alpha_3 = 0 \). We want to prove that \( \xi_1 = \xi_2 = 1 \).

Denote \( \mathbb{K} = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) \) and let \( \mathbb{K}_0 \) be the unique quadratic subfield of \( \mathbb{K} \); note that \( \mathbb{K}_0 \) is the maximal abelian subfield of \( \mathbb{K} \).

Assume for a contradiction that \( \{ \xi_1, \xi_2 \} \not\subset \mathbb{K} \). Then there is a non-trivial element \( \sigma \in \text{Gal}(\mathbb{K}(\xi_1, \xi_2)/\mathbb{K}) \). We have \( \alpha_1 \xi_1^\sigma + \alpha_2 \xi_2^\sigma + \alpha_3 = 0 \) and, without loss of generality, \( \xi_3^\sigma \neq \xi_1 \). It follows that \( \eta := \alpha_1/\alpha_2 = -(\xi_2 - \xi_3^\sigma)/(\xi_1 - \xi_3^\sigma) \). In particular, \( \eta \) belongs to an abelian field and so \( \eta \in \mathbb{K}_0 \). But the elements of \( \mathbb{K}_0 \) are fixed by a cyclic permutation of \( \alpha_1, \alpha_2, \alpha_3 \). Hence \( \eta = \alpha_1/\alpha_2 = \alpha_2/\alpha_3 = \alpha_3/\alpha_1 \). It follows that \( \eta^3 = (\alpha_1/\alpha_2)(\alpha_2/\alpha_3)(\alpha_3/\alpha_1) = 1 \), contradicting the hypothesis that \( \mathbb{K} \) contain no primitive cubic roots of unity. We conclude that \( \xi_1 \) and \( \xi_2 \) belong to \( \mathbb{K} \) and hence also to \( \mathbb{K}_0 \).

Observe that any element of \( \text{Gal}(\mathbb{K}/\mathbb{Q}) \) of order 2 restricts to the non-trivial element \( \iota \) of \( \text{Gal}(\mathbb{K}_0/\mathbb{Q}) \). Consider first the element of \( \text{Gal}(\mathbb{K}/\mathbb{Q}) \) that switches \( \alpha_1, \alpha_2 \) and fixes \( \alpha_3 \). Now we have \( \alpha_1 \xi_1^\iota + \alpha_2 \xi_1^\iota + \alpha_3 = 0 \). If \( \xi_2 \neq \xi_1 \) then...
If $\alpha_1/\alpha_2 = (\xi_1 - \xi_2)/(\xi_1 - \xi_2) \in K_0$, and we finish as before. Thus, $\xi_2 = \xi_1$ (and $\xi_1 = \xi_2$). Applying next the element that switches $\alpha_1, \alpha_3$ and fixes $\alpha_2$, we obtain $\alpha_1 + \alpha_2 \xi_1 + \alpha_3 \xi_2 = 0$. Multiplying by $\xi_1 = \xi_2^{-1}$, we get $\alpha_1 \xi_1 + \alpha_2 \xi_1^2 + \alpha_3 = 0$. Hence $\alpha_2(\xi_1^2 - \xi_2) = 0$, which shows that $\xi_1 = \xi_2 = \xi_1^{-1}$. Thus, $\xi_1 = 1$, which implies that $\xi_1 = 1$ by our hypothesis. Hence $\xi_2 = \xi_1 = 1$ as well, and we are done.

**Lemma 2.6.** Let $\lambda$ be a root of $P(X) = X^3 - X^2 - X - 1$, and $n \in \mathbb{Z}$. Then $\alpha = \lambda^n/P'(\lambda)$ satisfies the hypothesis of Lemma 2.5.

**Proof.** Clearly, $\alpha \in \mathbb{Q}(\lambda)$, which is field of degree 3. If $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\lambda)$ then $\alpha \in \mathbb{Q}$. Hence, denoting $\lambda_1, \lambda_2, \lambda_3$ the roots of $P(X)$, the three numbers $\lambda_3^n/P'(\lambda_1)$ must be equal. In particular, if $\lambda_2$ is the real root, and $\lambda_2, \lambda_3$ are the complex conjugate roots, then $\lambda_3^n/P'(\lambda_1) = \lambda_2^n/P'(\lambda_2)$, which implies that

$$n = \frac{\log |P'(\lambda_2)/P'(\lambda_1)|}{\log |\lambda_1/\lambda_2|} = -0.718 \ldots \not\in \mathbb{Z},$$

a contradiction.

Thus, $\mathbb{Q}(\alpha) = \mathbb{Q}(\lambda)$ is not a Galois extension of $\mathbb{Q}$. It remains to note that its Galois closure $\mathbb{Q}(\lambda_1, \lambda_2, \lambda_3)$ may not contain primitive cubic roots of unity, because prime 3 is not ramified therein.

**Proof of Theorem 2.2.** If $\sum_{i=1}^{3} \xi_i c_i \lambda_i^n = 0$ then the above lemmas imply that $\xi_1 = \xi_2 = \xi_3$. Hence $T(n) = 0$, and we are done.

Theorem 2.2 is proved in two steps. Using a Galois-theoretic argument similar to that of Lemma 2.6, but more involved, one reduces the problem to finding actual integral zeros of another linear recurrence, of order 4. Those are determined using standard technique, with logarithmic forms and Baker-Davenport reduction. See [4] for the details.

### 3 \( p \)-adic analytic functions

In this section 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 [7].

Let $p$ be a prime number and let $K$ be a finite extension of $\mathbb{Q}_p$. We extend the standard $p$-adic absolute value $| \cdot |$ from $\mathbb{Q}_p$ to $K$, so that $|p|_p = p^{-1}$. We will also use the additive valuation $\nu_p$ defined by $\nu_p(z) = -\log |z|_p/\log p$ for $z \in K^\times$, with the convention $\nu_p(0) = +\infty$.

For $a \in K$ and $r > 0$ we denote $D(a, r)$ and $\overline{D}(a, r)$ the open and the closed disk with center $a$ and radius $r$:

$$D(a, r) = \{ z \in K : |z - a|_p < r \}, \quad \overline{D}(a, r) = \{ z \in K : |z - a|_p \leq r \}.$$

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

$$\mathcal{O} = \{ z \in K : |z|_p \leq 1 \} = \overline{D}(0, 1).$$
We call \( f : \mathcal{O} \to \mathcal{O} \) an analytic function if there is a sequence \( \alpha_0, \alpha_1, \alpha_2, \ldots \in \mathcal{O} \) with \( \lim_{n \to \infty} |\alpha_n|_p = 0 \) such that
\[
f(z) = \sum_{n=0}^{\infty} \alpha_n z^n \quad (z \in \mathcal{O}).
\]

Note that for any \( b \in \mathcal{O} \) we have
\[
f(z) = \sum_{k=0}^{\infty} \beta_k (z - b)^k,
\]
where
\[
\beta_k = \frac{f^{(k)}(b)}{k!} = \sum_{n=k}^{\infty} \binom{n}{k} \alpha_n b^{n-k}.
\]

### 3.1 \( p \)-adic order of values of an analytic function

We start from the following trivial, but useful observation.

**Proposition 3.1.** Let \( f(z) \) be an analytic function. Then for any \( a, b \in \mathcal{O} \) we have \( |f(a) - f(b)|_p \leq |a - b|_p \).

**Proof.** Substituting \( z = a \) into (3.1) and noting that \( \beta_0 = f(b) \), we obtain
\[
|f(a) - f(b)|_p = |b - a|_p \sum_{k=1}^{\infty} \beta_k |a - b|^{k-1}.
\]
All terms in the sum on the right belong to \( \mathcal{O} \), whence the result. \qed

Assume now that \( f \) is not identically 0. Then the set of zeros of \( f \) is finite, because it is a discrete subset of the compact set \( \mathcal{O} \); we denote this set \( A \).

**Theorem 3.2.** Let \( e \) be the ramification index of \( \mathbb{K} / \mathbb{Q}_p \). 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 \( \kappa_i \in e^{-1} \mathbb{Z} \) such that for \( z \in \mathcal{O} \) satisfying \( z \equiv i \pmod{p^k} \) we have \( \nu_p(f(z)) = \kappa_i \); in other words, \( \nu_p(f(z)) \) is constant on the residue class \( z \equiv i \pmod{p^k} \).

(L) There exist
\[
a_i \in A, \quad \kappa_i \in e^{-1} \mathbb{Z}, \quad \mu_i \in \mathbb{Z}_{>0}
\]
such that for \( z \in \mathcal{O} \) satisfying \( z \equiv i \pmod{p^k} \) we have
\[
\nu_p(f(z)) = \kappa_i + \mu_i \nu_p(z - a_i).
\]
Proof. Let $m$ be a positive integer, and for every $j \in \{0, 1, \ldots, p^m - 1\}$ define $f_j(z) = f(j + p^mz)$. Clearly, if the statement holds true for every $f_j$ then it holds for $f$ as well. Taking $m$ so large that every residue class $z \equiv j \pmod{p^m}$ contains at most one element from $A$, we reduce the theorem to the case when $f$ has at most one zero. If $f$ does have a zero, say $a$, then, expanding

$$f(z) = \alpha_\mu(z-a)^\mu + \alpha_{\mu+1}(z-a)^{\mu+1} + \cdots,$$

with $\mu \geq 1$ and $\alpha_\mu \neq 0$, we note that the statement holds for $f$ as soon as it holds for the analytic function $\alpha_\mu + \alpha_{\mu+1}(z-a) + \cdots$, which has no zero at all.

Thus, it suffices to consider the case $A = \emptyset$. We need to show that the $p$-adic order $\nu_p(f(z))$ is constant on every residue class modulo a suitable power of $p$.

Since $f$ does not vanish on $O$, then, by compactness, $|f(z)|_p$ must be bounded from below by some strictly positive number. It follows that $f(z)$ belongs to one of the finitely many sets

$$O^\times, \pi O^\times, \ldots, \pi^n O^\times,$$

where $\pi$ is a primitive element of $K$ and $n$ is some positive integer. Note that $\nu_p(\pi) = e^{-1}$.

Since these sets are open, their inverse images by $f$ are open as well. Hence each of these inverse images is a union of finitely many residue classes modulo some power of $p$. This completes the proof. \qed

3.2 Vanishing of power series

In this subsection we recall two fundamental results about vanishing of a power series on $O$: Hensel’s Lemma and Strassman’s Theorem.

Hensel’s Lemma is the principal technical tool of $p$-adic analysis. It is usually stated for polynomials, but in this article we need a slightly more general version, for power series.

**Proposition 3.3** (Hensel’s Lemma for power series). Let $b_0 \in O$ be such that $|f(b_0)|_p < 1$ and $|f'(b_0)|_p = 1$. Then there exists a unique $b \in O$ such that $f(b) = 0$ and $|b - b_0|_p < |f(b_0)|_p$.

The proof can be found, for instance, in [2], see Theorems 8.2 and 9.4 therein, or in [11], see Theorem 27.6 therein.

The number of zeros can be estimated using Strassman’s Theorem.

**Theorem 3.4** (Strassman). Assume that $f(z)$ does not vanish identically on $O$; equivalently, the coefficients $\alpha_0, \alpha_1, \ldots$ are not all 0. Define $\mu$ as the largest $m$ with the property

$$|\alpha_m|_p = \max\{|\alpha_n|_p : n = 0, 1, \ldots\}.$$

(Since $|\alpha_n|_p \to 0$, such $\mu$ must exist.) Then $f(z)$ has at most $\mu$ zeros on $O$.

The proof can be found in many sources; see, for instance, [1] Theorem 4.1].
3.3 Functions $\exp$ and $\log$ in the $p$-adic domain

We denote $\rho = p^{-1/(p-1)}$. 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 $\log(\exp(z)) = z$.

**Remark 3.5.** Note that, when $p > 2$ and $p$ is unramified in $\mathbb{K}$, we have
\[
\mathcal{D}(0, \rho) = \mathcal{D}(0, 1), \quad \mathcal{D}(1, \rho) = \mathcal{D}(1, 1), \quad \mathcal{D}(0, 1) = \mathcal{D}(0, p^{-1}).
\]
This will always be the case starting from Section 4. This excludes the primes $p \in \{2, 11\}$ from our analysis.

4 $p$-adic analytic interpolation of the Tribonacci sequence

Recall that we denote $\Lambda = \{\lambda_1, \lambda_2, \lambda_3\}$ the set of roots of the polynomial
\[
P(X) = X^3 - X^2 - X - 1.
\]

Let $p$ be a prime number and let $\mathbb{K} = \mathbb{Q}_p(\lambda_1, \lambda_2, \lambda_3)$ be the splitting field of $P(X)$ over $\mathbb{Q}_p$. As before, we denote $\mathcal{O}$ its ring of integers. The discriminant
of \( P(X) \) is \(-44\). Hence, assuming in the sequel that \( p \neq 2, 11 \), the field \( K \) is unramified over \( \mathbb{Q}_p \).

We denote \( d = [K : \mathbb{Q}_p] \). There are three possibilities. If all the roots of \( P(X) \) are in \( \mathbb{Q}_p \) then \( K = \mathbb{Q}_p \) and \( d = 1 \). If \( P(X) \) has exactly one root in \( \mathbb{Q}_p \) then \( d = 2 \). Finally, if \( P(X) \) is irreducible in \( \mathbb{Q}_p \) then \( d = 3 \).

Recall that
\[
T(n) = \sum_{\lambda \in \Lambda} c_\lambda \lambda^n, \quad c_\lambda = \lambda P'(\lambda)^{-1}
\]
Note that, since \( p \neq 2, 11 \), we have \( c_\lambda \in \mathcal{O}_p^\times \) for \( \lambda \in \Lambda \). Recall also that \( T(n) = 0 \) if and only if \( n \in \mathbb{Z}_T \). Note that \( \Lambda \subset \mathcal{O}_p^\times \). Let \( N = N_p \) be the order of the subgroup of the multiplicative group \( (\mathcal{O}_p/p)^\times \) generated by \( \Lambda \). In [9] this quantity is denoted \( \pi(p) \). Note that \( N \mid p^d - 1 \). When \( d = 3 \), we have the more precise divisibility relation \( N \mid p^2 + p + 1 \).

For \( \ell \in \{0, 1, \ldots, N - 1\} \) we consider the analytic function \( f_\ell : \mathbb{Z}_p \to \mathbb{Z}_p \) defined by
\[
f_\ell(z) = \sum_{\lambda \in \Lambda} c_\lambda \lambda^\ell \exp(z \log(\lambda^N)). \tag{4.1}
\]
Note that by the definition of \( N \) we have
\[
\lambda^N \in \mathcal{D}(1, 1) = \mathcal{D}(1, \rho)
\]
(see Remark 3.5), so \( f_\ell(z) \) is indeed well-defined for \( z \in \mathbb{Z}_p \). Furthermore, for \( m \in \mathbb{Z} \) we have
\[
f_\ell(m) = T(\ell + mN) \in \mathbb{Z}. \tag{4.2}
\]
Since \( \mathbb{Z} \) is dense in \( \mathbb{Z}_p \) and \( f_\ell \) is continuous, we indeed have \( f_\ell(z) \in \mathbb{Z}_p \) for \( z \in \mathbb{Z}_p \).

Note also that \( f_\ell(z) \) does not vanish identically on \( \mathbb{Z}_p \): this also follows from equation (4.2).

5 Proof of Theorem 1.5

We use the terminology and the notation of Section 4. In this section \( p \) is a prime number, distinct from 2 and 11, and satisfying the following two conditions:
\( p \equiv 2 \pmod{3} \) and \( \Lambda \subset \mathbb{Q}_p \). The last condition means that \( K = \mathbb{Q}_p \) and \( d = 1 \).

By the Chebotarev Density Theorem, the set of such \( p \) is infinite and, moreover, it is of density \( 1/12 \) in the set of all primes.

We are going to show that for every such \( p \) both statements of Theorem 1.5 hold true. Actually, we will prove only the former statement:
\[
n \equiv 1/3 \pmod{p - 1} \implies \nu_p(T(n)) \geq \nu_p(n - 1/3), \tag{5.1}
\]
because the second statement, with \( 1/3 \) replaced by \(-5/3\), is proved absolutely similarly.

To start with, let us make the following observation: since \( p \equiv 2 \pmod{3} \), every element of \( \mathbb{Z}_p^\times \) has a single cubic root in \( \mathbb{Z}_p \). In particular, for every \( \lambda \in \Lambda \) there is a well-defined cubic root \( \lambda^{1/3} \in \mathbb{Z}_p \).

It turns out that these cubic roots are exactly those for which we have (4.2).
Proposition 5.1. With our choice of the cubic roots $\lambda^{1/3}$ we have

$$\sum_{\lambda \in \Lambda} c_{\lambda} \lambda^{1/3} = 0.$$

Proof. Assuming the contrary, we must have one of the options

\begin{align*}
c_{\lambda_1} \lambda_1^{1/3} + c_{\lambda_2} \lambda_2^{1/3} + c_{\lambda_3} \lambda_3^{1/3} &= 0, \quad (5.2) \\
c_{\lambda_1} \lambda_1^{1/3} + \zeta c_{\lambda_2} \lambda_2^{1/3} + c_{\lambda_3} \lambda_3^{1/3} &= 0, \quad (5.3) \\
c_{\lambda_1} \lambda_1^{1/3} + \overline{\zeta} c_{\lambda_2} \lambda_2^{1/3} + c_{\lambda_3} \lambda_3^{1/3} &= 0, \quad (5.4)
\end{align*}

where $\zeta$ and $\overline{\zeta}$ are the primitive cubic roots of unity. Option (5.3) reduces to (5.2), so we only need to rule out (5.2) and (5.4).

Note that $\zeta / \in \mathbb{Q}_p$ because $p \equiv 2 \mod 3$. Therefore, by Galois conjugation, in the case (5.2) we also have

$$c_{\lambda_1} \lambda_1^{1/3} + \overline{\zeta} c_{\lambda_2} \lambda_2^{1/3} + c_{\lambda_3} \lambda_3^{1/3} = 0.$$

It follows that $(\zeta - \overline{\zeta})(c_{\lambda_2} \lambda_2^{1/3} - c_{\lambda_3} \lambda_3^{1/3}) = 0$, again a contradiction.

Similarly, in the case (5.4) we also have

$$c_{\lambda_1} \lambda_1^{1/3} + \zeta c_{\lambda_2} \lambda_2^{1/3} + c_{\lambda_3} \lambda_3^{1/3} = 0.$$

It follows that $(\zeta - \overline{\zeta})(c_{\lambda_2} \lambda_2^{1/3} - c_{\lambda_3} \lambda_3^{1/3}) = 0$, again a contradiction. □

Now we are in a position to prove (5.1). We define $N = N_p$ as in Section 4; note that in our special case $d = 1$ and so $N | p - 1$. In particular, the residue class $1/3 \pmod{N}$ is well-defined.

Let $n \in \mathbb{Z}$ and $\ell \in \{0, \ldots, N - 1\}$ satisfy

$$n \equiv \ell \equiv 1/3 \pmod{N}.$$

We define $f_{\ell}(z)$ as in (4.1). Write $n = \ell + Nm$ and $1/3 = \ell + Nb$ with $m \in \mathbb{Z}$ and $b \in \mathbb{Z}_p \cap \mathbb{Q}$. We have clearly $T(n) = f_{\ell}(m)$. We claim that $f_{\ell}(b) = 0$. Indeed, for $\lambda \in \Lambda$ we have

$$(\lambda^{\ell} \exp(b \log(\lambda^N)))^3 = \lambda^{3(\ell + Nb)} = \lambda.$$

Since $\lambda^{\ell} \exp(b \log(\lambda^N)) \in \mathbb{Z}_p$, it must be equal to the cubic root $\lambda^{1/3}$ specified above. Hence

$$f_{\ell}(b) = \sum_{\lambda \in \Lambda} c_{\lambda} \lambda^{\ell} \exp(b \log(\lambda^N)) = \sum_{\lambda \in \Lambda} c_{\lambda} \lambda^{1/3} = 0. \quad (5.5)$$

by Proposition 5.1.

Now we are done: Proposition 3.1 implies that

$$\nu_p(T(n)) = \nu_p(f_{\ell}(m) - f_{\ell}(b)) \geq \nu_p(m - b) = \nu_p(n - 1/3),$$

as wanted. Note that $p \equiv 2 \mod 3$ was only required to ensure that $3 \nmid N$. The argument above can be generalized for all $p$ such that $3 \nmid N$ and $\Lambda \subset \mathbb{Q}_p$.  

13
6 Analytic form of Conjectures 1.2 and 1.6

In this section \( p \) is a prime number distinct from 2, 3, 11. We continue using the notation of Section 4.

We are going to show that Conjectures 1.2 and 1.6 have very natural interpretations in terms of the zeros of the functions \( f_\ell(z) \).

Theorem 6.1. 1. The following three statements are equivalent.

(a) Conjecture 1.2 holds for the given \( p \).
(b) For every \( \ell \in \{0, \ldots, N-1\} \), the zeros of the function \( f_\ell(z) \) belong to \( N^{-1}\mathbb{Z} \).
(c) For every \( \ell \) the following holds: if \( b \in \mathbb{Z}_p \) is a zero of \( f_\ell(z) \) then \( \ell + Nb \in \mathbb{Z}_T \).

2. The following three statements are equivalent.

(d) Conjecture 1.6 holds for the given \( p \).
(e) For every \( \ell \in \{0, \ldots, N-1\} \), the zeros of the function \( f_\ell(z) \) belong to \( \mathbb{Q} \cap \mathbb{Z}_p \).
(f) For every \( \ell \) the following holds: if \( b \in \mathbb{Z}_p \) is a zero of \( f_\ell(z) \) then \( \ell + Nb \in \mathbb{Q}_T \).

This theorem is very useful for producing counter-examples to both conjectures, see Section 8. More importantly, it provides a clear motivation why the conjectures can only be expected to hold for relatively few primes. Indeed, there is absolutely no reason to expect that every \( f_\ell(z) \) would have only zeros in \( \mathbb{Q} \), and it is even less of a reason to expect that it would not vanish outside a fixed set of six elements.

Let us start with some lemmas.

Lemma 6.2. If \( b \in \mathbb{Q} \cap \mathbb{Z}_p \) is a zero of \( f_\ell(z) \) then \( \ell + Nb \) is a twisted rational zero of \( T \), as defined in Section 2.

Proof. Denote \( a = \ell + Nb \) and for every \( \lambda \in \Lambda \) choose some determination for \( \lambda^a \).

Let \( m \) be a non-zero integer such that \( mb \in \mathbb{Z} \). Then

\[
\left( \lambda^\ell \exp(b \log(\lambda^N)) \right)^m = \lambda^{m\ell} \exp(mb \log(\lambda^N)) = \lambda^{ma}.
\]

Hence \( \lambda^\ell \exp(b \log(\lambda^N)) = \xi_\lambda \lambda^a \), where \( \xi_\lambda \) is a root of unity. It follows that

\[
0 = f_\ell(b) = \sum_{\lambda \in \Lambda} \xi_\lambda c_\lambda \lambda^a,
\]

as wanted.

Lemma 6.3. Assume that Conjecture 1.6 holds for a given \( p \).
1. Let $\ell \in \{0, 1, \ldots, N-1\}$ and let $b \in \mathbb{Z}_p$ be a zero of $f_\ell(z)$. Then there exists $i \in \{0, 1, \ldots, Q-1\}$ such that option (L) holds for the residue class of $i$, and such that $a_i = \ell + Nb$. In particular, $b \in \mathbb{Q}$, and if $a_i \in \mathbb{Z}$ then $b \in N^{-1}\mathbb{Z}$.

2. Conversely, let $i \in \{0, 1, \ldots, Q-1\}$ be such that option (L) holds for the residue class of $i$. Then there exists $\ell \in \{0, 1, \ldots, N-1\}$ such that

$$f_\ell\left(\frac{a_i - \ell}{N}\right) = 0.$$ 

Only item (1) will be used, but we include the converse statement for completeness.

Proof of item (1). This is the argument that already appeared in the introduction. Let $(m_k)$ be a sequence of rational integers satisfying $m_k \equiv b \pmod{p^k}$, and set $n_k = \ell + Nm_k$. Then

$$\nu_p(T(n_k)) = \nu_p(f_\ell(m_k)) \geq \nu_p(n_k - b) \geq k,$$

and, in particular, $\nu_p(T(n_k)) \to \infty$ as $k \to \infty$. Infinitely many of the numbers $n_k$ belong to the same residue class $i \pmod{Q}$, and we will assume in the sequel that all $n_k$ do, by taking a subsequence. Since $\nu_p(T(n_k)) \to \infty$, we must have option (L) for this residue class, and moreover, we must have $\nu_p(n_k - a_i) \to \infty$. Since we also have $\nu_p(n_k - (\ell + Nb)) \to \infty$, we obtain $a_i = \ell + Nb$. \hfill $\Box$

Proof of item (2). It is similar, but other way round. As in Remark 1.3, we find a sequence of integers $(n_k)$ such that $n_k \equiv i \pmod{Q}$ and $n_k \equiv a_i \pmod{p^k}$. By choosing a subsequence, we find $\ell \in \{0, 1, \ldots, N-1\}$ that $n_k \equiv \ell \pmod{N}$ for all $k$.

Define $m_k = (n_k - \ell)/N$. Then the sequence $(m_k)$ converges $p$-adically to $(a_i - \ell)/N$. Since $\nu_p(f_\ell(m_k)) = \nu_p(T(n_k)) \geq k$, the sequence $(f_\ell(m_k))$ converges $p$-adically to 0. Hence $f_\ell((a_i - \ell)/N) = 0$. \hfill $\Box$

Proof of Theorem 6.1. The implications (a)$\Rightarrow$(b) and (d)$\Rightarrow$(e) follow from item (1) of Lemma 6.3. The converse implications (b)$\Rightarrow$(a) and (e)$\Rightarrow$(d) follow from Theorem 3.2 applied to the functions $f_\ell(z)$. Implications (b)$\Rightarrow$(e) and (e)$\Rightarrow$(f) follow by combining Lemma 6.2 with Theorems 2.3 and 2.2 respectively. Finally, the converse implications (e)$\Rightarrow$(b) and (f)$\Rightarrow$(e) are trivial. \hfill $\Box$

As a byproduct, we also established the following.

Corollary 6.4. If Conjecture 1.2 holds for the given $p$, then the numbers $a_i$ emerging in the residue classes with option (L) belong to the set $\mathbb{Z}_T$. If Conjecture 1.6 holds, then $a_i$ belong to $\mathbb{Q}_T$. 

15
7 Detecting zeros of $f_\ell(z)$

To make use of Theorem 6.1, we must develop a practical method for locating zeros of $f_\ell(z)$. As in the previous sections, $p$ is a prime number distinct from 2 and 11, and $\ell \in \{0, 1, \ldots, N - 1\}$.

7.1 A non-vanishing condition

To start with, let us give a simple sufficient condition for $f_\ell$ be non-vanishing on $\mathbb{Z}_p$.

**Proposition 7.1.** If $p \nmid T(\ell)$ then $f_\ell(z) \neq 0$ for $z \in \mathbb{Z}_p$.

*Proof.* By the definition of $N$ we have $f(n) \equiv f(\ell) \pmod{p}$ when $n \equiv \ell \pmod{N}$. In particular, for such $n$ we have $|T(n)|_p = |T(\ell)|_p = 1$. In other words, for $m \in \mathbb{Z}$ we have $|f_\ell(m)|_p = 1$. By continuity, $|f_\ell(z)|_p = 1$ for $z \in \mathbb{Z}_p$. This completes the proof. \qed

7.2 The first vanishing condition

Now let study sufficient conditions for $f_\ell(z)$ to have a zero $\mathbb{Z}_p$. As follows from above, the first condition must be

\[ p \mid T(\ell). \] (7.1)

This will be assumed for the rest of the section.

It will be more convenient to work with the function

\[ g(z) = \frac{f_\ell(z)}{p} \]

instead of $f_\ell(z)$ itself. For further use, note that $g(z)$ has the expansion

\[ g(z) = \sum_{k=0}^{\infty} \beta_k z^k \] (7.2)

with the following properties:

\begin{align*}
\beta_k &\in \mathbb{Z}_p & (k = 0, 1, 2 \ldots); \\
\beta_k &\in p\mathbb{Z}_p & (k = 2, 3, \ldots); \\
|\beta_k|_p &\to 0 & (k \to \infty). \quad (7.3) \quad (7.4) \quad (7.5)
\end{align*}

Indeed,

\[ \beta_0 = g(0) = \frac{f_\ell(0)}{p} = \frac{T(\ell)}{p} \in \mathbb{Z} \] (7.6)

by our choice of $\ell$. Furthermore, we have

\[ \beta_k = \frac{p^{k-1}}{k!} \sum_{\lambda \in \Lambda} c_\lambda \lambda^\ell \left(\frac{\log(\lambda^N)}{p}\right)^k. \] (7.7)
Since $\lambda^N \equiv 1 \pmod{p}$, we have $\log(\lambda^N) \equiv 0 \pmod{p}$, which shows that the sum in (7.7) belongs to $\mathbb{Z}_p$. We also have $p^{k-1}/k! \in \mathbb{Z}_p$ when $p \geq 3$ and $k \geq 1$. Hence $\beta_k \in \mathbb{Z}_p$ for $k \geq 1$ as well. This proves (7.3).

Next, since the sum in (7.7) belongs to $\mathbb{Z}_p$, we have $\nu_p(\beta_k) \geq k - 1 - \nu_p(k!)$.

It is known that $\nu_p(k!) < k/(p-1)$ for $k \geq 1$. In particular, $\nu_p(k!) < k/2$ for $p \geq 3$. It follows that $\nu_p(\beta_k) > 0$ for $k \geq 2$ and $\nu_p(\beta_k) \to +\infty$ as $k \to \infty$. This proves (7.4) and (7.5).

Note the following consequence of (7.4): for $z \in \mathbb{Z}_p$ we have

$$g'(z) \equiv g'(0) \pmod{p}.$$  (7.8)

Indeed,

$$g'(z) = \beta_1 + \sum_{k=2}^{\infty} k\beta_k z^{k-1}.$$  

Here $\beta_1 = g'(0)$ and each term in the sum is divisible by $p$ by (7.4).

7.3 The second vanishing condition

The second condition that we impose is

$$g'(0) \not\equiv 0 \pmod{p}.$$  (7.9)

This condition means that $\beta_1 = g'(0) \in \mathbb{Z}_p^\times$. Hence there exists $b_0 \in \mathbb{Z}$ such that

$$b_0 \equiv -\beta_0 \beta_1^{-1} \pmod{p}.$$  (7.10)

Substituting $z = b_0$ into expansion (7.2), and using (7.4), we obtain

$$p \mid g(b_0).$$  (7.11)

On the other hand, (7.8) and (7.9) imply that $g'(b_0) \equiv g'(0) \not\equiv 0 \pmod{p}$. Together with (7.11) this can be expressed as

$$|g(b_0)|_p < 1, \quad |g'(b_0)|_p = 1.$$

Now using Hensel’s Lemma as given in Proposition 3.3, we find $b \in \mathbb{Z}_p$ such that $g(b) = 0$. Then we also have $f_\ell(b) = 0$.

Actually, we have even more.

**Proposition 7.2.** Assume that (7.1) and (7.9) hold. Then $f_\ell(z)$ has exactly one zero on $\mathbb{Z}_p$.

**Proof.** Existence of a zero is already proved above. To show uniqueness, we invoke Strassman’s Theorem 3.4. Since $|\beta_1|_p = 1$ by (7.9), the quantity $\mu$ from Theorem 3.4 must be 1 by (7.4). Whence the result.  \[\Box\]
Sufficient conditions for validity and for failure of Conjectures 1.2 and 1.6

To implement this in practice, we need to express condition (7.9) in terms of the Tribonacci numbers $T(n)$ rather than the function $g(z)$. This is not hard. For $z \in p\mathcal{O}$ we have
\[
\log z \equiv z - 1 \pmod{p^2}.
\]
In particular, for $\lambda \in \Lambda$ we have
\[
\log(\lambda N) \equiv \lambda N - 1 \pmod{p}.
\]
Hence,
\[
g'(0) = \beta_1 = \sum_{\lambda \in \Lambda} c_\lambda N \log(\lambda N) \equiv \sum_{\lambda \in \Lambda} c_\lambda N \lambda N - 1 \pmod{p} \equiv T(\ell + N) - T(\ell) \pmod{p}.
\]
Therefore condition (7.9) is equivalent to
\[
T(\ell + N) \not\equiv T(\ell) \pmod{p^2}.
\]

Now, to disprove Conjecture 1.2 for some prime number $p$, we must find $\ell$ such that both (7.1) and (8.2) are satisfied, and such that the resulting zero $b$ of $f_\ell(z)$ satisfies
\[
\ell + bN \not\in \mathbb{Z}_T.
\]
It suffices to show that
\[
\ell + bN \not\equiv 0, -1, -4, -17 \pmod{p}.
\]
Moreover, since $b \equiv b_0 \pmod{p}$, this can be re-written as
\[
\ell + b_0 N \not\equiv 0, -1, -4, -17 \pmod{p}.
\]
Using (7.10) and (8.1), this translates into
\[
u := \ell - \frac{T(\ell)}{p} \left(\frac{T(\ell + N) - T(\ell)}{p}\right)^{-1} N \not\equiv 0, -1, -4, -17 \pmod{p}.
\]
Similarly, when $p \neq 3$, then Conjecture 1.6 would fail if
\[
u \not\equiv 0, -1, -4, -17, 1/3, -5/3 \pmod{p}.
\]
Let us summarize what we proved.

**Theorem 8.1.** Let $p \neq 2, 11$ be a prime number, and let $\ell \in \{0, 1, \ldots, N_p - 1\}$ be such that (7.1), (8.2) and (8.3) hold true. Then Conjecture 1.2 fails for this $p$. Similarly, if $p \neq 3$ and (7.1), (8.2) and (8.4) hold true then Conjecture 1.6 fails for this $p$. 

18
Now let us give sufficient conditions of validity of each conjecture. For Conjecture \ref{conjecture1.6} we will restrict to the primes congruent to 2 modulo 3.

**Theorem 8.2.** Let \( p \) be a prime number distinct from 2 and 11. Assume that for every \( \ell \) satisfying (7.1), condition (8.2) holds true as well, and the following also holds: \( \ell \equiv a \pmod{N} \) for some \( a \in \mathbb{Z}_T \). Then Conjecture \ref{conjecture1.6} holds for this \( p \).

For Conjecture \ref{conjecture1.6} we will restrict to the primes congruent to 2 modulo 3.

**Theorem 8.3.** Let \( p \) be a prime number satisfying \( \Lambda \subset \mathbb{Q}_p \) and \( 3 \nmid N \). Assume that for every \( \ell \) satisfying (7.1), condition (8.2) holds true as well, and the following also holds: \( \ell \equiv a \pmod{N} \) for some \( a \in \mathbb{Q}_T \). Then Conjecture \ref{conjecture1.6} holds for this \( p \).

**Proof of Theorem 8.3.** Fix \( \ell \in \{0, 1, \ldots, N-1\} \). If \( p \nmid T(\ell) \) then \( f_\ell(z) \) has no zeros on \( \mathbb{Z}_p \), see Proposition 7.1. Now assume that \( p \mid T(\ell) \). Proposition 7.2 implies that \( f_\ell(z) \) has a single zero on \( \mathbb{Z}_p \).

Now let \( a \in \mathbb{Z}_T \) be such that \( \ell \equiv a \pmod{N} \). Write \( a = \ell + Nb \) with \( b \in \mathbb{Z} \). Then \( f_\ell(b) = T(\ell + Nb) = 0 \). Thus, the single zero of \( f_\ell(z) \) is \( b \).

We have just showed that condition (c) of Theorem 6.1 holds true for this \( p \). The theorem is proved. \( \square \)

The proof of Theorem 8.3 is the same, with the exception that this time we may have \( b \notin \mathbb{Z} \). However, when \( \Lambda \subset \mathbb{Q}_p \), \( p \neq 2, 11 \) and due to \( 3 \nmid N \), we still have \( f_\ell(b) = 0 \), see (5.3).

**9 The proofs of Theorems 1.4, 1.7, and 1.8**

We start with the negative part (part (i)) of Theorem 1.7. We implemented the algorithms implied by Theorem 8.1 in Mathematica for all primes \( p \leq 600 \). There are 109 primes \( p \leq 600 \). For each prime \( p \), we first computed \( N := N_p \), the period of \((T_n)_{n \in \mathbb{Z}} \) modulo \( p \). Then for each \( p \) we searched \( \ell \) such that (7.1), (8.2) and (8.3) all hold true. This calculation took a few minutes and found such an example \( \ell \) for all \( p \leq 600 \) except for \( p \in \{2, 3, 11, 83, 103, 163, 397\} \). See Table 1 for the actual data. This proves the negative part of Theorem 1.7.

As for part (ii) of Theorem 1.7 when \( p \in \{83, 397\} \), we have that \( N = N_p \) is 287 and 132, respectively. In both cases, the only \( \ell \in \{0, 1, \ldots, N-1\} \) such that \( T(\ell) \equiv 0 \pmod{p} \) are \( \ell \equiv -17, -4, -1, 0 \pmod{N} \). Furthermore for \( \ell \in \mathbb{Z}_T \), we have \((T(N + \ell) - T(\ell))/p = T(N + \ell)/p \not\equiv 0 \pmod{p} \). Thus, taking \( \ell \in \mathbb{Z}_T \) and writing for positive integers \( n \equiv \ell \pmod{N} \), \( z = (n - \ell)/N \), we have that

\[
T(n) = f_\ell(z) = pg(z) = p \sum_{k \geq 0} \beta_k z^k.
\]

Note that \( \beta_0 = g(0) = T(\ell)/p = 0 \), and \( \beta_1 = g'(0) \equiv T(N + \ell)/p \pmod{p} \), so \( |\beta_1|_p = |g'(0)|_p = 1 \). Further, since \( \nu_p(p^{k-1}/(k-1)!) \geq 1 \) for all \( k \geq 2 \), it follows
Table 1: Data for the proofs of Theorems 1.7 and 1.8. A * means that for this prime, Theorem 1.8 does not conclude.

| p  | N   | ℓ   | u   | p  | N   | ℓ   | u   | p  | N   | ℓ   | u   |
|----|-----|-----|-----|----|-----|-----|-----|----|-----|-----|-----|
| 5  | 34  | 21  | 2   | 179| 32221| 100 | 114 | 379| 48007| 309 | 76  |
| 7  | 48  | 5   | 1   | 181| 10981| 26  | 66  | 383| 147073| 219 | 338 |
| 11 | 68  | 6   | 4   | 191| 3663| 72  | 22  | 409| 151711| 1709| 664 |
| 17 | 96  | 28  | 7   | 193| 4666| 174 | 76  | 401| 400  | 205 | 152 |
| 19 | 360 | 18  | 12  | 197| 3234 | 382 | 84  | 409| 41820 | 365 | 310 |
| 23 | 553 | 29  | 15  | 199| 198  | 26  | 40  | 419*| 418  | 277 | 138 |
| 29 | 140 | 77  | 24  | 211| 5365 | 83  | 203 | 421| 420  | 118 | 214 |
| 31 | 331 | 14  | 22  | 223| 16651| 301 | 35  | 431| 61920 | 466 | 31  |
| 37 | 469 | 19  | 17  | 227| 17176| 34  | 57  | 433| 62007 | 385 | 344 |
| 41 | 500 | 35  | 15  | 229| 17557| 249 | 61  | 439| 6424 | 781 | 160 |
| 43 | 308 | 82  | 11  | 233| 9048  | 36  | 126 | 443| 196693| 516 | 21  |
| 47 | 46  | 46  | 16  | 239| 4790  | 28  | 55  | 449| 202051| 107 | 229 |
| 53 | 52  | 33  | 10  | 241| 29040| 506 | 57  | 457| 14888 | 858 | 30  |
| 59 | 3541| 64  | 34  | 251| 63253| 304 | 218 | 461| 35420 | 192 | 9   |
| 61 | 1800| 68  | 34  | 257| 2560 | 54  | 34  | 463| 71611 | 624 | 199 |
| 67 | 1519| 100 | 43  | 263| 23056| 37  | 214 | 467| 218557| 1269 | 70  |
| 71 | 5113 | 132 | 62  | 269*| 268  | 177 | 88  | 479| 76480 | 56  | 8   |
| 73 | 5328 | 31  | 30  | 271 | 73440| 331 | 165 | 487| 79219 | 131 | 85  |
| 79 | 3120 | 18  | 76  | 277 | 12788| 61  | 191 | 491| 10045 | 802 | 289 |
| 83 | 3169| 19  | 51  | 283 | 13348| 777 | 193 | 503| 421008| 102 | 497 |
| 89 | 689 | 186 | 23  | 289 | 28616| 458 | 200 | 509| 250591| 1228 | 433 |
| 97 | 1272 | 184 | 52  | 307 | 31416| 30  | 163 | 521| 271963 | 2058 | 220 |
| 101| 990 | 105 | 62  | 311 | 310  | 123 | 58  | 523| 273528 | 237 | 16  |
| 107| 12883| 172 | 15  | 313 | 32761| 29  | 184 | 541| 58536 | 633 | 200 |
| 109| 5376 | 488 | 30  | 317 | 108000| 36  | 186 | 547| 149094 | 104 | 42  |
| 113| 5720 | 79  | 101 | 331 | 36631| 188 | 2   | 557| 103416 | 509 | 424 |
| 117| 18907| 11  | 5   | 337 | 16224| 320 | 103 | 563| 52828 | 87  | 232 |
| 127| 3864 | 34  | 49  | 347 | 49136| 156 | 244 | 569| 53900 | 322 | 49  |
| 131| 1400 | 40  | 38  | 349 | 17400| 1428 | 33  | 571| 10755 | 527 | 155 |
| 137| 2890 | 423 | 145 | 353 | 122963| 95  | 38  | 597| 111199 | 341 | 85  |
| 149| 8269 | 71  | 107 | 359 | 12960| 1204 | 115 | 587| 283  | 96  | 194 |
| 167| 9296 | 41  | 68  | 367 | 45019| 692 | 99  | 593| 3256  | 849 | 422 |
| 173| 2494 | 314 | 25  | 373 | 130128| 279 | 188 | 599| 598  | 257 | 485 |
that $|\beta_k|_p < 1$ for $k \geq 2$. This shows that

$$\nu_p(T(n)) = 1 + \nu_p(g(z)) = 1 + \nu_p \left( \sum_{k \geq 1} \beta_k z^k \right) = 1 + \nu_p(z) = 1 + \nu_p(n - \ell),$$

which proves Item (ii) of Theorem 1.7.

Theorem 1.8 is proved similarly. Only (8.3) is exchanged for (8.4) and $Z_T$ for $Q_T$.

Proof of Theorem 1.4. For $p = 3$, we have $N = 13$. The only $\ell \in \{0, \ldots, 12\}$ such that $T(\ell) \equiv 0 \pmod{3}$ are $\ell \in \{0, 7, 9, 12\}$. When $\ell = 7$, the subsequence $T(13n + \ell)$ is constant 6 modulo 9, and so $v_3(T(n)) = 1$ if $n \equiv 7 \pmod{13}$.

Next assume that $\ell = 0, -1$. Then $g(0)$ is congruent modulo 3 to one of $T(13)/3$, $T(12)/3$ and they are both 0, so we need additional terms. We have

$$\beta_1 = \sum_{\lambda \in A} c_\lambda \lambda^\ell \left( \log \frac{\lambda^N}{3} \right),$$

$$\equiv \sum_{\lambda \in A} c_\lambda \lambda^\ell \left( \frac{\lambda^N - 1}{3} - \frac{(\lambda^N - 1)^2}{2 \cdot 3} \right) \pmod{3^2}$$

$$\equiv \frac{T(N + \ell) - T(\ell)}{3} - \frac{T(2N + \ell) - 2T(N + \ell) + T(\ell)}{2 \cdot 3} \pmod{3^2}.$$

For both $\ell = 0, -1$, we have $v_3((T(N + \ell) - T(\ell))) = 2$ and

$$v_3(T(2N + \ell) - 2T(N + \ell) + T(\ell)) = 3.$$

Thus, $v_3(\beta_1) = 1$. For $j \geq 4$, we get that $v_3(\beta_j) \geq v_3(3^{j-1}/j!) \geq 2$. It remains to study $v_3(\beta_j)$ for $j = 2, 3$. But we have

$$\beta_j = \frac{3^{j-1}}{j!} \sum_{\lambda \in A} c_\lambda \lambda^\ell \left( \frac{\log \lambda^N}{3} \right)^j$$

$$\equiv \frac{3^{j-1}}{j!} \sum_{\lambda \in A} c_\lambda \lambda^\ell \left( \frac{\lambda^N - 1}{3} \right)^j \pmod{3^j}$$

$$\equiv \frac{3^{j-1}}{j!} \left( \sum_{i=0}^{j} (-1)^{j-i} \binom{j}{i} T((j - i)N + \ell) \right) \frac{3^i}{3^j} \pmod{3^j},$$

and computations show that for $j = 2, 3$, we have

$$v_3(T(2N + \ell) - 2T(N + \ell) + T(\ell)) = 3;$$

$$v_3(T(3N + \ell) - 3T(2N + \ell) + 3T(N + \ell) - T(\ell)) = 5.$$

Since also $v_3(3^{j-1}/j!) = 1$ for $j = 2, 3$, we get that $v_3(\beta_2) \geq 2$, $v_3(\beta_3) \geq 2$.

Thus, for $n \equiv \ell \pmod{13}$, we have

$$v_3(T(n)) = v_3 \left( \beta_1 z + \sum_{k \geq 2} \beta_k z^k \right) = v_3(\beta_1 z) = 2 + v_3(n - \ell).$$
It remains to study the case $\ell = 9$. For this, we take $N_1 = 3N = 39$. This case then becomes $\ell \equiv -4, -17, 9 \pmod{39}$. For $\ell = 9$, the subsequence $T(3Nn + \ell)$ is constantly $3^4 \pmod{3^5}$, and so $\nu_3(T(n)) = 4$ for all $n \equiv 9 \pmod{3N}$. So let $\ell = -4, -17$. Then, if $n \equiv \ell \pmod{3N}$, putting $z = (n - \ell)/3N$, we get

$$T(n) = 3^2 g(z),$$

where now

$$g(z) = \sum_{\lambda \in \Lambda} c_\lambda \lambda^\ell \left( \frac{\exp(\log \lambda^{3Nz})}{3^2} \right) = \sum_{k \geq 0} \beta_k z^k.$$

For both possibilities of $\ell$, $\beta_0 = 0$. However, modulo $3^4$ we have

$$\beta_1 = \sum_{\lambda \in \Lambda} c_\lambda \lambda^\ell \left( \frac{\log \lambda^{3N}}{3^2} \right) \equiv \frac{1}{3^2} \sum_{\lambda \in \Lambda} c_\lambda \lambda^\ell \left( \lambda^{3N} - 1 - \frac{(\lambda^{3N} - 1)^2}{2} \right) \equiv \frac{1}{3^2} \left( T(3N + \ell) - T(\ell) - \frac{T(2 \cdot 3N + \ell) - 2T(3N + \ell) + T(\ell)}{2} \right).$$

In both cases, $\nu_3(T(3N+\ell) - T(\ell)) = 5$ but $\nu_3(T(2 \cdot 3N + \ell) - 2T(3N + \ell) + T(\ell)) = 6$. Thus, $\nu_3(\beta_1) = 3$. Since $\nu_3(\beta_j) \geq \nu_3(3^{2j-1}/j!)$ for $j \geq 4$, we only need to calculate $\beta_2$ and $\beta_3$. We find that

$$\beta_2 \equiv \frac{3^2}{2!} \left( \frac{T(2 \cdot 3N + \ell) - 2T(3N + \ell) + T(\ell)}{3^4} \right) \equiv 0 \pmod{3^4}$$

and

$$\beta_3 \equiv \frac{3^4}{3!} \left( \frac{T(3 \cdot 3N + \ell) - 3T(2 \cdot 3N + \ell) + 3T(3N + \ell) - T(\ell)}{3^6} \right) \equiv 0 \pmod{3^6}.$$

We conclude that

$$\nu_3(T(n)) = \nu_3 \left( 3^2 \left( \sum_{k \geq 0} \beta_k z^k \right) \right) = \nu_3(3^2 \beta_0 z^k) = 5 + \nu_3((n + \ell)/39) = 4 + \nu_3(n + \ell),$$

which completes the proof of this theorem.

For the primes $p \in \{11, 103, 163\}$ not covered by Theorem 1.7 as we previously said, our method does not handle 11. As for $p \in \{103, 163\}$, a computer calculation found that for such primes whenever $\ell \in \{0, 1,\ldots, N - 1\}$ is such that condition (7.1) is satisfied, then (8.2) holds but (8.3) fails, so our method
could not conclude. Similarly, for the primes $p \in \{11, 47, 53, 103, 163\}$ which are not covered by Theorem 1.8 our methods fail. Again, 11 is excluded and for $p \in \{103, 163\}$ we cannot conclude for the same reason. Moreover, $p \in \{47, 53\}$ suffer the problem that modulo $N$, $-17$ is congruent to either $1/3$ or $-5/3$, and so congruences modulo $p$ are too weak to conclude.

### 10 Conjectures and Heuristics

Let $\mathcal{ML}$ and $\mathcal{NMLR}$ be the subsets of primes $p$ such that Conjecture 1.2 holds and Conjecture 1.3 fails, respectively. We propose the following conjecture.

**Conjecture 10.1.** Both subsets $\mathcal{ML}$ and $\mathcal{NMLR}$ are infinite. In fact, they are both of positive lower density as subsets of the set of all primes.

We conclude by offering some heuristics to support our conjecture. Let $k$ be a large positive integer. The splitting field of the polynomial

$$g(X) = f(X^k) = X^{3k} - X^{2k} - X^k - 1$$

is $L_k = \mathbb{Q}(\sqrt[k]{\alpha}, \sqrt[k]{\beta}, \zeta_k)$, where $\zeta_k$ is some primitive root of unity of order $k$. The degree of $L_k$ is at most $k^2 \phi(k)$, where $\phi(k)$ is the Euler function of $k$. By the Chebotarev Density Theorem, the primes such that $p \equiv 1 (mod k)$ and also $\alpha^{(p-1)/k} \equiv \beta^{(p-1)/k} \equiv 1 (mod p)$ form a set of density which is at least $1/(k^2 \phi(k))$. For such primes, $N | (p-1)/k$, so $N$ is small. Since $N \leq (p-1)/k$ a proportion of only about $1/k$ residues modulo $p$ (at most) are in the image of $\{T \ell (mod p) : 0 \leq \ell \leq N - 1\}$ which suggests that the probability of having an additional zero modulo $p$; i.e., a positive integer $\ell$ such that $T \ell \equiv 0 (mod p)$ and $\ell \not\equiv 17, -4, -1, 0 (mod p)$ should be at most $1/k$. Thus, for a positive proportion of such primes, maybe at least $(k-1)/(k^2 \phi(k))$ of them, have the property that $T \ell \equiv 0 (mod p)$ implies $\ell \equiv -17, -4, -1, 0 (mod p)$. For such primes, $f_\ell(0) = 0$, so

$$f_\ell(z) = p \sum_{k=1}^{\infty} \beta_k z^k.$$ 

If additionally (8.2) is satisfied, so $\beta_1 \not\equiv 0 (mod p)$, which we conjecture it happens for most such primes, then we would get that $\nu_p(T_n) = 0$ provided $n \not\equiv -17, -4, -1, 0 (mod p)$ and $\nu_p(T_n) = 1 + \nu_p(n-c)$ for $n \equiv c (mod p)$, with $c \in \{-17, -4, -1, 0\}$. This heuristic suggests that $\mathcal{ML}$ is infinite and of positive lower density.

For $\mathcal{NMLR}$ let $p$ be a prime such that $p \equiv 2 (mod 3)$ and $f(X) (mod p)$ is irreducible. By the Chebotarev Density Theorem the set of such primes has density $1/6$. For them $N \mid p^2 + p + 1$. Let $P(m)$ be the largest prime factor of the positive integer $m$. For each fixed $u \in (0, 1)$, the positive integers $n$ such that $P(n) \leq n^u$ are called smooth. It is known that the set of smooth numbers has a density $\rho(u)$, where $\rho$ is the Dickman function. It is conjectured that numbers of the form $g(p)$ where $g(X)$ is some irreducible polynomial should
behave like random integers with respect to smoothness and in particular that $P(g(p)) > g(p)^u$ should hold for a positive proportion of primes $p$, but this has only been proved for linear polynomials $g(X)$ and values of $u$ not very close to 1 (for example, Fouvy [3] proved that for any nonzero integer $a$ the inequality $P(p - a) > p^{0.67}$ holds for a positive proportion of primes $p$). So, let us assume that there is a positive proportion of primes $p$ such $f(X)$ is irreducible modulo $p$ and $P(p^2 + p + 1) > p^{1.6}$. Let $p$ be such a prime and let $q = P(p^2 + p + 1)$. Then $N | p^2 + p + 1 = 1$ if $q \nmid N$, then $N | (p^2 + p + 1)/q < p^{0.4}$. However, an argument of Erdős and Murty from [3] shows that for any positive real number $X$ the number of primes $p \leq X$ which divide $N_K/Q(\alpha^k)$ for some $k \leq X^{0.4}$ is $O(X^{0.8})$ which is $o(\pi(X))$ as $X \to \infty$. This shows that for most of our primes $p$ (namely, $p \equiv 2 \pmod{3}$, $f(X) \pmod{p}$ is irreducible and $P(p^2 + p + 1) > p^{1.6}$), we have that $q \mid N$. In particular, $N > p^{1.6}$. Now Theorem 7.2 in [5] tells us that

$$\# \{0 \leq \ell \leq N - 1 : T_\ell \equiv 0 \pmod{p} \} = \frac{N}{p} + O(p^{1/2}) = (1 + o(1))\frac{N}{p}.$$ 

Thus, there are many $\ell$ in $[0, N - 1]$ with $T_\ell \equiv 0 \pmod{p}$. Of these not all might create $p$-adic zeros since for example, it might happen that $(T_{N+\ell} - T_\ell)/p \equiv 0 \pmod{p}$, or even if this number is nonzero modulo $p$, it might be that (8.4) is not satisfied. However, since we have no reason to believe that the above numbers are anything but random modulo $p$, we assume that the first condition fails with probability $1/p$ and the second one fails with probability $6/p$, getting in this way that the number of $\ell \in [0, N - 1]$ such that $\ell \not\equiv -17, -4, -1, 0 \pmod{p}$ and both conditions (8.2) and (8.4) hold is $(1 + o(1))N/p + O(N/p^2) = (1 + o(1))N/p$. So, for most of such primes Conjecture 1.6 would fail, which suggests that $NMLR$ is of positive lower density.

**Acknowledgements**

We thank Keith Conrad for helpful advice. Yu. B. and F. L. worked on this paper during a visit at the MPI-SWS in Spring 2022. These authors thank this institution for hospitality and support. Yu. B. was also supported in part by the ANR project JINVARIANT.

**References**

[1] J. W. S. Cassels, *Local fields*, London Mathematical Society Student Texts, vol. 3, Cambridge University Press, Cambridge, 1986. MR 861410

[2] Keith Conrad, *Hensel’s lemma*, https://kconrad.math.uconn.edu/blurbs/gradnumthy/hensel.pdf

[3] Pál Erdős and M. Ram Murty, *On the order of $a \pmod{p}$*, Number theory (Ottawa, ON, 1996), CRM Proc. Lecture Notes, vol. 19, Amer. Math. Soc., Providence, RI, 1999, pp. 87–97. MR 1684594

[4] Florian Luca et al., *Rational zeros of linear recurrent sequence*, in preparation.
[5] Graham Everest, Alf van der Poorten, Igor Shparlinski, and Thomas Ward, *Recurrence sequences*, Mathematical Surveys and Monographs, vol. 104, American Mathematical Society, Providence, RI, 2003. MR 1990179

[6] Étienne Fouvry, *Théorème de Brun-Titchmarsh: application au théorème de Fermat*, Invent. Math. **79** (1985), no. 2, 383–407. MR 778134

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

[8] The OEIS Foundation Inc., *Tribonacci numbers*, The on-line encyclopedia of integer sequences (2022). [https://oeis.org/A000073](https://oeis.org/A000073).

[9] 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

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

[11] 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