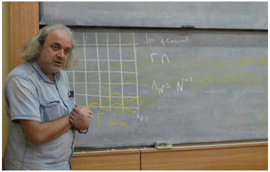
Twisted rational zeros of linear recurrences

Florian Luca

Paderborn, July 10, 2022

My co-authors




Yu. Bilu J. Nieuwveld J. Ouaknine J. Worrell

The p-adic order of an integer

Let p be a prime. For a nonzero integer n we write

$$\nu_p(n) = a \quad \text{where} \quad p^a \mid n \quad \text{but} \quad p^{a+1} \nmid n.$$

Example

When $n = 12 = 2^2 \times 3$, we have

$$\nu_2(12) = 2, \quad \nu_3(12) = 1 \quad \text{and} \quad \nu_p(12) = 0 \quad \text{for primes} \quad p \geq 5.$$

The p-adic order of Fibonacci numbers

The Fibonacci sequence $\{F_n\}_{n\geq 0}$ is given by

$$F_0 = 0, \qquad F_1 = 1 \quad \text{and} \quad F_{n+2} = F_{n+1} + F_n \quad \text{for all} \quad n \geq 0.$$

Is there a formula for $\nu_p(F_n)$? Yes, there is.

Let $z(p)$ be the index of appearance of p in the Fibonacci sequence. This is the smallest positive integer k such that

$$p \mid F_k.$$

Then, the following holds.

Theorem

If p is odd then:

$$\nu_p(F_n) = \begin{cases} 0 & \text{if} \quad n \not\equiv 0 \pmod{z(p)}; \\ \nu_p(F_{z(p)}) + \nu_p(n/z(p)) & \text{if} \quad n \equiv 0 \pmod{z(p)}. \end{cases}$$

When $p = 2$, $z(2) = 3$, and for $n = 3k$ we have

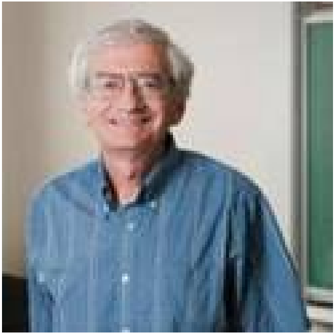
$$\nu_2(F_{3k}) = \begin{cases} 1 & \text{if} \quad k \equiv 1 \pmod{2}; \\ 2 + \nu_2(k) & \text{if} \quad k \equiv 0 \pmod{2}. \end{cases}$$

The Tribonacci sequence

The Tribonacci sequence $\{T_n\}_{n\in\mathbb{Z}}$ is defined by the recurrence

$$\begin{aligned} &T(0)=0, \qquad T(1)=T(2)=1,\\ &T(n+3)=T(n+2)+T(n+1)+T(n) \qquad \text{for all} \quad n\in\mathbb{Z}. \end{aligned}$$

Is there a formula for $\nu_p(T_n)$? The answer is yes for $p=2$.



T. Lengyel

D. Marques

The 2-adic valuation of Tribonacci numbers

In **2014**, Lengyel and Marques proved the following formula concerning $\nu_2(T_n)$:

Theorem

For $n \geq 1$, we have

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

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

Conjecture

(LM) Let p be prime.There exists a positive integer Q such that for every $i \in \{0, 1, \ldots, Q-1\}$ *one of the following holds:*

(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* $a_i \in \mathbb{Z}, \quad \kappa_i \in \mathbb{Z}, \quad \mu_i \in \mathbb{Z}_{>0}$ *satisfying*

$$\nu_p(a_i - i) \geq \nu_p(Q), \tag{1}$$

such that for all but finitely many $n \equiv i \pmod{Q}$ *we have*

$$\nu_p(T(n)) = \kappa_i + \mu_i \nu_p(n - a_i). \tag{2}$$

Informally, the conjecture predicts that

- 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;
- in the case (L) (“linear”) it is a linear function of $\nu_p(n - a_i)$.

The 3-adic valuation of the Tribonacci numbers

Already the case $p = 3$ looks encouraging.

Theorem

For $n \geq 1$, we have

$$\nu_3(T_n) = \begin{cases} 0, & \text{if} \quad n \not\equiv 0, 7, 9, 12 \pmod{13}; \\ 1, & \text{if} \quad n \equiv 7 \pmod{13}; \\ \nu_3(n) + 2, & \text{if} \quad n \equiv 0 \pmod{13}; \\ \nu_3(n+1) + 2, & \text{if} \quad n \equiv 12 \pmod{13}; \\ 4, & \text{if} \quad n \equiv 9 \pmod{39}; \\ \nu_3(n+17) + 4, & \text{if} \quad n \equiv 22 \pmod{39}; \\ \nu_3(n+4) + 4, & \text{if} \quad n \equiv 35 \pmod{39}. \end{cases}$$

A parametric set of counterexamples

However, the following theorem shows that Conjecture LM fails for infinitely many primes.

Theorem

There is an infinite set[a] *of prime numbers congruent to* $2 \pmod 3$ *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*
$$\nu_p(T(n)) \geq \nu_p(n + 5/3).$$

[a] This set of primes is not only infinite, but is of relative density $1/12$ in the set of all primes.

Why is the above theorem a counter-example to the conjecture?

Clearly, Theorem 6 contradicts Conjecture LM. Indeed, let p be as in the theorem, and let $(n_k)_{k\geq 1}$ be a sequence of integers satisfying

$$n_k \equiv 1/3 \pmod{(p-1)p^k}.$$

If Conjecture LM is true for this p then for some $i \in \{0, \ldots, Q-1\}$ the residue class $i \pmod{Q}$ 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 LM:

$$\nu_p(T(n_k)) = \kappa_i + \mu_i \nu_p(n_k - a_i).$$

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

Modifying the conjecture?

One may still hope to rescue Conjecture LM by allowing a_i to be rational numbers.

Conjecture

(RLM) 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

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

Even the modified conjecture fails sometimes

However, even this weaker conjecture fails for many primes.

Theorem

(i) *Conjecture LM fails for* $p \in [5, 599] \setminus \{11, 83, 103, 163, 397\}$.

(ii) *Conjecture LM holds for* $p = 83, 397$ *in the form*

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

with

$$\mathcal{Z}_{\mathbb{Z}}(T) = \{0, -1, -4, -17\},$$

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

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

Theorem

(i) *Conjecture* RLM *fails for* $p \in [5, 599]$, *except for*

$$\{11, 47, 53, 83, 103, 163, 269, 397, 401, 419, 499, 587\}.$$

(ii) *Conjecture* RLM *holds for* $p = 269, 401, 419, 499, 587$ *in the form*

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

where

$$\mathcal{Z}_{\mathbb{Q}}(T) = \{0, -1, -4, -17, 1/3, -5/3\};$$

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

For $p = 47, 53, 103, 163$, we failed to decide if Conjecture RLM holds.

The initial purpose of our paper was to provide a method to decide for which primes p Conjectures LM and RLM hold and for which they fail. As seen above, 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, μ_i, κ_i) for those $i = \{0, \ldots, Q-1\}$ for which option (L) takes place.

The Binet formula

Let

$$\Lambda = \{\lambda_1, \lambda_2, \lambda_3\} \subset \overline{\mathbb{Q}}$$

be the set of roots of the polynomial

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

For $\lambda \in \Lambda$ define

$$c_\lambda = \frac{\lambda}{P'(\lambda)} = \frac{\lambda}{3\lambda^2 - 2\lambda - 1}.$$

For $n \in \mathbb{Z}$, the Tribonacci number

$$T(n) = \sum_{\lambda \in \Lambda} c_\lambda \lambda^n \quad \text{for all} \quad n \in \mathbb{Z}.$$

Rational zeros of the Tribonacci sequence

The following is a result of Mignotte and Tzanakis of **1991**.

Theorem

If $T_n = 0$ *then*

$$n \in \mathcal{Z}_{\mathbb{Z}}(T) = \{0, -17, -4, -1\}.$$

It turns out that in addition to the above zeros, the Tribonacci sequence also "vanishes" at some non-integral rational numbers.

Proposition

For some definition of the cubic roots

$$\lambda^{1/3} \qquad (\lambda \in \Lambda) \tag{3}$$

we have

$$\sum_{\lambda \in \Lambda} c_\lambda \lambda^{1/3} = 0. \tag{4}$$

Similarly, for some definition of the cubic roots (3) *we have*

$$\sum_{\lambda \in \Lambda} c_\lambda \lambda^{-5/3} = 0.$$

Proof. Consider the polynomial

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

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

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

A direct verification shows that

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

and, similarly,

$$F(\beta_1, \beta_2, \beta_3) = 0.$$

Since $F(X_1, X_2, X_3)$ factors as

$$F(X_1, X_2, X_3) = (X_1 + X_2 + X_3)(X_1 + \zeta X_2 + \bar{\zeta}X_3)(X_1 + \bar{\zeta}X_2 + \zeta X_3),$$

where $\zeta, \bar{\zeta}$ are the primitive cubic roots of unity, the result follows.

Call $r \in \mathbb{Q}$ a *rational zero* of T if for some definition of the rational powers

$$\lambda_1^r, \quad \lambda_2^r, \quad \lambda_3^r$$

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

$$\lambda_1^r, \quad \lambda_2^r, \quad \lambda_3^r$$

and for some roots of unity ξ_1, ξ_2, ξ_3, we have

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

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

Theorem

We have

$$\mathcal{Q}_{\mathbb{Z}}(T) = \mathcal{Z}_{\mathbb{Z}}(T) \cup \{1/3, -5/3\} = \{0, -1, -4, -17, 1/3, -5/3\}.$$

Moreover, if $r \in \mathcal{Q}_{\mathbb{Q}}(T)$ *and the powers* $\lambda_1^r, \lambda_2^r, \lambda_3^r$ *are suitably defined, then for the roots of unity* ξ_1, ξ_2, ξ_3 *satisfying*

$$\sum_{i=1}^{3} \xi_i c_{\lambda_i} \lambda_i^r = 0,$$

we have $\xi_1 = \xi_2 = \xi_3$.

Proof

Let us fix notations. We put

$$x = n/q, \qquad \gcd(n,q) = 1, \qquad q \geq 2.$$

Any two determinations of $\lambda_1^{1/q}$ differ by a root of unity which can be incorporated into ζ_1. So, we pick $\lambda_1^{1/q}$ to be real. Let d be the degree of $\lambda_1^{1/q}$. That is, d is the degree of the irreducible factor of

$$X^{3q} - X^{2q} - X^q - 1$$

having $\lambda_1^{1/q}$ as a root. Let $e,\ f$ be the number of conjugates of $\lambda_1^{1/q}$ lying on the circles

$$|z| = \lambda_1^{1/q} \qquad \text{and} \qquad |z| = \lambda_1^{-1/2q},$$

respectively. Then $e + f = d$ and by the Viéte relations

$$\lambda_1^{e/q}\lambda_1^{-f/2q} = 1,$$

so $f = 2e$. Thus, $e = d/3$.

Next we write $\lambda_2^{1/q}$ for a fixed algebraic conjugate of $\lambda_1^{1/q}$ and $\lambda_3^{1/q}$ for its complex conjugate. Then

$$\lambda_1^{1/q}\lambda_2^{1/q}\lambda_3^{1/q} = \lambda_1^{1/q}|\lambda_2|^{2/q} = 1.$$

We divide across by ζ_1 and have

$$c_1\lambda_1^{n/q} + c_2\lambda_2^{n/q}\eta + c_3\lambda_3^{n/q}\eta' = 0.$$

We show that $\overline{\eta} = \eta'$. For this we subtract the above relation from

$$c_1\lambda_1^{n/q} + c_2\lambda_2^{n/q}\eta + c_3\lambda_3^{n/q}\overline{\eta} \in \mathbb{R}$$

getting

$$(\eta' - \overline{\eta})c_3\lambda_3^{n/q} \in \mathbb{R}.$$

Assuming $\eta' - \overline{\eta} \neq 0$, we can conjugate the above relation and manipulate these relations to get

$$(c_2\lambda_2^{n/q})/(c_3\lambda_3^{n/q}) = -\eta'/\eta,$$

so c_2 and c_3 are *associated*, which is false.

Next,

$$c_1\lambda_1^{n/q} + c_2\lambda_2^{n/q}\eta + c_3\lambda_3^{n/q}\eta^{-1} = 0,$$

which can be written as

$$\eta^2 + (c_1/c_2)(\lambda_2/\lambda_1)^{n/q}\eta + (c_3/c_2)(\lambda_3/\lambda_2)^{n/q} = 0.$$

This shows that η is at most quadratic over $\mathbb{K}$, but in fact it is in $\mathbb{K}$. Thus, given $\lambda_2^{1/q}$, the number η is uniquely determined.

Next let $\lambda_1^{1/q}\eta_i$, $\eta_i = e^{2\pi i\ell_i/q}$ for $i = 1, \ldots, e$ be conjugates of $\lambda_1^{1/q}$ for $i = 1, \ldots, e$, with $\ell_1 = 0$. Let σ_i take

$$\lambda_1^{1/q} \qquad \text{to} \qquad \lambda_1^{1/q}\zeta_i.$$

Assume it takes

$$\lambda_2^{1/q} \qquad \text{to} \qquad \lambda_{2+j}^{1/q}e^{2\pi i m_i/q},$$
$$\lambda_3^{1/q} \qquad \text{to} \qquad \lambda_{3-j}^{1/q}e^{2\pi i n_i/q},$$

where $j \in \{0, 1\}$. Assume $j = 0$ (the other case is similar). Assume further that $\sigma_i(\eta) = \eta^{a_i}$. Applying σ_i we get

$$c_1\lambda_1^{n/q}e^{2\pi i\ell_i n/q} + c_2\lambda_2^{n/2}e^{2\pi i m_i n/q}\eta^{a_i} + c_3\lambda_3^{n/q}e^{2\pi i n_i n/q}\eta^{-a_i} = 0.$$

We thus get

$$c_1\lambda_1^{n/q} + c_2\lambda_2^{n/q}\eta^{a_i}e^{2\pi i(m_i-\ell_i)n/q} + c_3\lambda_3^{n/q}e^{2\pi i(n_i-\ell_i)n/q}\eta^{-a_i} = 0.$$

From the unicity of η we get

$$e^{2\pi i(m_i-\ell_i)n/q}\eta^{a_i} = \eta \qquad \text{and} \qquad e^{2\pi i(n_i-\ell_i)n/q}\eta^{-a_i} = \eta^{-1}.$$

We thus get

$$e^{2\pi i(m_i+n_i-2\ell_i)n/q}=1, \qquad \text{so} \qquad e^{2\pi i(3n\ell_i)/q}=e^{2\pi i(\ell_i+m_i+n_i)/q}=1,$$

where the last relation follows from

$$\begin{aligned} 1 &= \sigma(1)=\sigma(\lambda_1^{1/q}\lambda_2^{1/q}\lambda_3^{1/q}) \\ &= (\lambda_1^{1/q}e^{2\pi i\ell_i/q})(\lambda_2^{1/q}e^{2\pi i m_i/q})(\lambda_3^{1/q}e^{2\pi i n_i/q}) \\ &= (\lambda_1^{1/q}\lambda_2^{1/q}\lambda_3^{1/q})(e^{2\pi i(\ell_i+m_i+n_i)/q})=e^{2\pi i(m_i+n_i+\ell_i)/q}. \end{aligned}$$

Since $(n,q)=1$, we get that ζ_i is a cubic root of 1. Thus, $e\le 3$, so $d\in\{3,6,9\}$.

We still need q. We use a result of Voutier, **1996**, to the effect that

$$\lambda_1^{1/q} \geq 1 + \frac{1}{2d}\left(\frac{\log\log d}{\log d}\right)^3 \geq 1 + \frac{1}{18}\left(\frac{\log\log 9}{\log 9}\right).$$

Since $\lambda_1 \leq 1.84$, we get $q \leq 240$. We checked that

$$X^{3q} - X^{2q} - X^q - 1$$

is irreducible for all $q \in [1, 240]$. Hence, $d = 3q \leq 9$, so $q \leq 3$. The case $q = 2$ gives that the conjugates of $\lambda_1^{1/2}$ on the circle of radius $|z| = \lambda_1^{1/2}$ are $\lambda_1^{1/2}$ and $-\lambda_1^{1/2}$ and -1 is not a cubic root. So, $q = 3$. We need η. Since $\mathbb{K}$ does not contain roots of unity we get that $\eta \in \{\pm 1\}$. We want to show that $\eta = 1$. If $\eta = -1$, we then get

$$c_1\lambda_1^{n/2} - c_2\lambda_2^{n/2} - c_3\lambda_3^{n/2} = 0.$$

This gives

$$c_1^3\lambda_1^n - c_2^3\lambda_2^n - c_3^3\lambda_3^n - 3c_1c_2c_3 = 0.$$

This makes

$$c_1^3\lambda_1^n - c_2^3\lambda_2^n - c_3^3\lambda_3^n \in \mathbb{Q}$$

but this is not Galois stable (by Galois automorphisms leads to $c_1^3\lambda_1^n = c_2^3\lambda_2^n$ and we saw that this is not possible).
So, $\eta = 1$ and we need to solve

$$c_1\lambda_1^{n/3} + c_2\lambda_2^{n/3} + c_3\lambda_3^{n/3} = 0.$$

It is better to shift to

$$W_n = c_1^3\lambda_1^n + c_2^3\lambda_2^n + c_3^3\lambda_3^n - 3c_1c_2c_3.$$

This verifies the recurrence

$$W_{n+4} = 2W_{n+3} - W_n \qquad \text{for} \qquad n \in \mathbb{Z}.$$

Further, it is better to work with $(U_n)_{n\in\mathbb{Z}}$, where $U_1 = 11W_n$. We have

$$U_0 = 0,\ U_1 = 0,\ U_2 = 1,\ U_3 = 4.$$

Now we use SKOLEM.

SKOLEM: Solves the Skolem Problem for simple integer LRS

System Explanation Show/Hide

- On the first line write the coefficients of the recurrence relation, separated by spaces.
- On the second line write an equal number of space-separated initial values.
- The LRS must be simple, non-degenerate, and not the zero LRS.
- The tool will output all zeros (at both positive and negative indices), along with a completeness certificate.

Input Format

$a_1\ a_2\ \cdots\ a_k$
$u_0\ u_1\ \cdots\ u_{k-1}$

where:
$u_{n+k} = a_1 \cdot u_{n+k-1} + a_2 \cdot u_{n+k-2} + \cdots + a_k \cdot u_n$

Input area

Auto-fill examples: Show/Hide

Zero LRS | Degenerate LRS | Non-simple LRS | Trivial | Fibonacci | Tribonacci | Berstel sequence [1] | Order 5 [3] | Order 6 [3] | Reversible order 8 [3]

LRS input:

```
2,0,0,-1
0,0,1,4
```

- Always render full LRS (otherwise restricted to 400 characters)
- I solemnly swear the LRS is non-degenerate (skips degeneracy check, it will timeout or break if the LRS is degenerate!)
- Use GCD reduction (reduces initial values by GCD)
- Use leapfrogging algorithm of [2]
  - Factor subcases (merges subcases into single linear set, sometimes requires higher modulo classes)
  - Use fast identification of mod-m (requires GCD reduction; may result in non-minimal mod-m argument)

Go | Clear | Stop

Output area

Leapfrogging result

Zeros: -51, -12, -5, -3, 0, 1

👈 click on each subsequence on left for more information.

Zero at 0 in $(0+1\mathbb{Z})$ hide/show

- p-adic non-zero in $(0+13\mathbb{Z}_{\neq 0})$
- Zero at 1 in $(1+13\mathbb{Z})$ hide/show
  - p-adic non-zero in $(1+39\mathbb{Z}_{\neq 0})$ ($(0+3\mathbb{Z}_{\neq 0})$ of parent)
  - Non-zero mod 14 in $(14+39\mathbb{Z})$ ($(1+3\mathbb{Z})$ of parent)
  - Zero at -12 in $(27+39\mathbb{Z})$ ($(2+3\mathbb{Z})$ of parent) hide/show

Let $(U_n)_{n\in\mathbb{Z}}$ be a linearly recurrent sequence of integers satisfying

$$U_{n+k} = a_1 U_{n+k-1} + \cdots + a_k U_n$$

for $n \ge 0$, where $a_1, \ldots, a_k, U_0, \ldots, U_{k-1}$ are in $\mathbb{Z}$. Assume that it has a Binet formula

$$U_n = \sum_{i=1}^{s} f_i(n)\lambda_i^n,$$

where $f_i(X)$ are polynomials in $\mathbb{K} = \mathbb{Q}(\lambda_1, \ldots, \lambda_s)$.

Definition

We say that $x \in \mathbb{Q}$ is a *twisted rational zero* of $(U_n)_{n\in\mathbb{Z}}$ if for some definition of $\lambda_1^x, \ldots, \lambda_s^x$ and some roots of unity $\zeta_1, \ldots, \zeta_s$ we have

$$\sum_{i=1}^{s} \zeta_i f_i(x)\lambda_i^x = 0.$$

Finiteness of twisted rational zeros

Theorem

Given a nondegenerate linearly recurrent sequence $(U_n)_{n\in\mathbb{Z}}$, there are only finitely many twisted rational zeros x. Their denominator is effectively bounded.

We now describe the bounds.
For a number $\alpha \in \mathbb{K}$ which is not zero or a root of unity let $\rho_{\mathbb{K}}(\alpha)$ be the Kummer exponent of α in $\mathbb{K}$, which is the largest n such that $\alpha \in \mathbb{K}^n$.
Note that $\rho_{\mathbb{K}}(\alpha) = \infty$ if $\alpha = 0$ or is a root of unity but it is finite otherwise.

Let N be the Chevalley-Bass number of $\mathbb{K}$ given below.

Theorem

Let $\mathbb{K}$ be a number field of degree d. There exists a positive integer N depending on d such that for every positive integer n the following holds: If $\alpha \in \mathbb{K}$ is an Nnth power in $\mathbb{K}(\zeta_{Nn})$, then α is an nth power in $\mathbb{K}$. In symbols

$$\mathbb{K}(\zeta_{Nn})^{Nn} \cap \mathbb{K} \subset \mathbb{K}^n.$$

The above theorem is due to Chevalley, **1951** and Bass, **1965**. The number N is effective. Bilu, **2023** shows that

$$N \leq \exp\left(d + \frac{9d}{\log(d+1)}\right).$$

Bounding the denominator of a twisted zero

Proposition

Assume that $x = a/b$ is a twisted rational zero of $(U_n)_{n\geq 0}$. Then either x is a root of one of the $f_i(X)$ for $i = 1, \ldots, s$, or

$$b \mid Nlcm_{i\neq j}[\rho_{\mathbb{K}}(\lambda_i/\lambda_j)],$$

where $N := N_{\mathbb{K}}$ is the Chevalley, Bass number of $\mathbb{K}$.

Example

Let $U_n = 2^n T(mn)$ for all $n \in \mathbb{Z}$ for some fixed positive integer m. Then

$$\mathcal{Z}_{\mathbb{Q}}(U) = \{-17/m, -4/m, -5/(3m), -1/m, 0, 1/(3m)\}.$$

In particular,

$$\mathbb{L} = \bigcup_q \mathbb{K}((\lambda_i/\lambda_j)^{1/q} : 1 \le i \ne j \le s),$$

where the above union is over the denominators of all possible twisted rational zeros of $(U_n)_{n\in\mathbb{Z}}$ is a number field.
It follows from a theorem of Dvornicich, Zannier, **2000** that setting $\zeta_1 = 1$, there are only finitely many s-tuples $(\zeta_2, \ldots, \zeta_s, x)$ with x rational such that

$$\sum_{i=1}^{s} \zeta_i f_i(x)(\lambda_i/\lambda_1)^x = 0$$

and no proper subsum is zero. The orders of these roots of unity are explicitly bounded in terms of $\mathbb{L}$ and s.

In particular, one may fix q, $\zeta := (\zeta_2, \ldots, \zeta_s)$ and $(\lambda_i/\lambda_1)^{1/q}$ for $i = 2, \ldots, s$ and work with the linearly recurrent sequence of algebraic numbers

$$U_{q,\zeta}(n) = \sum_{i=1}^{s} \zeta_i f_i(n/q)((\lambda_i/\lambda_1)^{1/q})^n,$$

which by the Skolem-Mahler-Lech theorem has only finitely many zeros n. These are not effective.

p-adic analytic functions

Let us go back to Conjecture LM. We used p-adic analysis. We give a brief detour below.

Let p be a prime number and let $\mathbb{K}$ be a finite extension of $\mathbb{Q}_p$. We extend the standard p-adic absolute value $|\cdot|$ from $\mathbb{Q}_p$ to $\mathbb{K}$, so that

$$|p|_p = p^{-1}.$$

We will also use the additive valuation ν_p defined by

$$\nu_p(z) = -\frac{\log |z|_p}{\log p} \quad \text{for} \quad z \in \mathbb{K}^{\times},$$

with the convention $\nu_p(0) = +\infty$.

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

$$\begin{aligned} \mathcal{D}(a, r) &= \{z \in \mathbb{K} : |z - a|_p < r\}, \\ \bar{\mathcal{D}}(a, r) &= \{z \in \mathbb{K} : |z - a|_p \leq r\}. \end{aligned}$$

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

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

We call $f : \mathcal{O} \mapsto \mathcal{O}$ an analytic function if there is a sequence

$$\alpha_0, \alpha_1, \alpha_2, \ldots \in \mathcal{O} \quad \text{with} \quad \lim_{n \to \infty} |\alpha_n|_p = 0 \quad \text{such that}$$

$$f(z) = \sum_{n=0}^{\infty} \alpha_n z^n \qquad (z \in \mathcal{O}).$$

Note that for any $b \in \mathcal{O}$ we have

$$f(z) = \sum_{k=0}^{\infty} \beta_k (z-b)^k, \quad \text{where} \quad \beta_k = \frac{f^{(k)}(b)}{k!} = \sum_{n \geq k} \binom{n}{k} \alpha_n b^{n-k}. \tag{5}$$

Functions exp and log in the p-adic domain

We denote

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

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

$$\begin{aligned} |\exp(z) - 1|_p &= |z|_p, \\ \exp(z+w) &= \exp(z)\exp(w), \\ \exp'(z) &= \exp(z). \end{aligned}$$

1. 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

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

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

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

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

$$\log(\exp(z)) = z.$$

A remark

Note that, when $p > 2$ and p is unramified in $\mathbb{K}$, we have

$$\mathcal{D}(0,\rho) = \mathcal{D}(0,1), \qquad \mathcal{D}(1,\rho) = \mathcal{D}(1,1), \qquad \bar{\mathcal{D}}(0,1) = \mathcal{D}(0,p^{-1}).$$

This will always be the case for us. This excludes the primes $p = 2, 11$ from our analysis.

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

Recall that

$$T(n) = \sum_{\lambda \in \Lambda} c_\lambda \lambda^n, \qquad c_\lambda = \frac{\lambda}{P'(\lambda)}.$$

Note that, since $p \neq 2, 11$, we have

$$c_\lambda \in \mathcal{O}^\times \quad \text{for} \quad \lambda \in \Lambda.$$

Recall also that $T(n) = 0$ if and only if $n \in \mathcal{Z}_{\mathbb{Z}}(T)$.
Note that $\Lambda \subset \mathcal{O}^\times$. Let $N = N_p$ be the order of the subgroup of the multiplicative group $(\mathcal{O}/p)^\times$ generated by Λ. 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 $f_\ell : \mathbb{Z}_p \mapsto \mathbb{Z}_p$ defined by

$$f_\ell(z) = \sum_{\lambda \in \Lambda} c_\lambda \lambda^\ell \exp\left(z \log(\lambda^N)\right). \tag{6}$$

Note that by the definition of N we have

$$\lambda^N \in \mathcal{D}(1,1) = \mathcal{D}(1,\rho),$$

so $f_\ell(z)$ is indeed well-defined for $z \in \mathbb{Z}_p$. Furthermore, for $m \in \mathbb{Z}$ we have

$$f_\ell(m) = T(\ell + mN) \in \mathbb{Z}. \tag{7}$$

Since $\mathbb{Z}$ is dense in $\mathbb{Z}_p$ and f_ℓ 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 (7).

Analytic form of Conjectures LM and RLM

.

Theorem

1. *The following three statements are equivalent.*
   - *Conjecture LM holds for the given p.*
   - *For every $\ell \in \{0, \ldots, N-1\}$, the zeros of $f_\ell(z)$ are in $N^{-1}\mathbb{Z}$.*
   - *For every ℓ the following holds: if $b \in \mathbb{Z}_p$ is a zero of $f_\ell(z)$ then $\ell + Nb \in \mathcal{Z}_{\mathbb{Z}}(T)$.*
2. *The following three statements are equivalent.*
   - *Conjecture RLM holds for the given p.*
   - *For every $\ell \in \{0, \ldots, N-1\}$, the zeros of $f_\ell(z)$ are in $\mathbb{Q} \cap \mathbb{Z}_p$.*
   - *For every ℓ the following holds: if $b \in \mathbb{Z}_p$ is a zero of $f_\ell(z)$ then $\ell + Nb \in \mathcal{Z}_{\mathbb{Q}}(T)$.*

This theorem is very useful for producing counter-examples to both conjectures.

More importantly, it provides a clear motivation why the conjectures cannot be expected to hold except for very 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.

Detecting zeros of $f_\ell(z)$

To make use of Theorem 18, 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 $\ell \in \{0, 1, \ldots, N-1\}$.

A non-vanishing condition

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

Proposition

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

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

$$\boxed{p \mid T(\ell).} \tag{8}$$

This will be assumed for the rest.
It will be more convenient to work with the function

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

instead of $f_\ell(z)$ itself.

The second vanishing condition

The second condition that we impose is

$$\boxed{g'(0) \not\equiv 0 \pmod{p}.} \tag{9}$$

Proposition

Assume that (8) *and* (9) *hold. Then* $f_\ell(z)$ *has exactly one zero on* $\mathbb{Z}_p$.

Sufficient conditions for validity and for failure of Conjectures LM and RLM

To implement this in practice, we need to express condition (9) in terms of the Tribonacci numbers $T(n)$ rather than the function $g(z)$. This is not hard. For example, condition (9) is equivalent to

$$\boxed{T(\ell+N) \not\equiv T(\ell) \pmod{p^2}.} \tag{10}$$

Now, to disprove Conjecture LM for some prime number p, we must find ℓ such that both (8) and (10) are satisfied, and such that the resulting zero b of $f_\ell(z)$ satisfies

$$\ell + bN \notin \mathcal{Z}_{\mathbb{Z}}(T).$$

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

$$\ell + b_0 N \not\equiv 0, -1, -4, -17 \pmod{p}.$$

This translates into

$$\boxed{u := \ell - \frac{T(\ell)}{p}\left(\frac{T(\ell+N) - T(\ell)}{p}\right)^{-1} N \not\equiv 0, -1, -4, -17 \pmod{p}.} \tag{11}$$

Similarly, when $p \neq 3$, then Conjecture RLM would fail if

$$\boxed{u \not\equiv 0, -1, -4, -17, 1/3, -5/3 \pmod{p}.} \tag{12}$$

Let us summarize what we proved.

Theorem

Let $p \neq 2, 11$ *be a prime number, and let* $\ell \in \{0, 1, \ldots N_p - 1\}$ *be such that* (8), (10) *and* (11) *hold true. Then Conjecture LM fails for this* p. *Similarly, if* $p \neq 3$ *and* (8), (10) *and* (12) *hold true then Conjecture RLM fails for this* p.

Now let us give sufficient conditions of validity of each conjecture.

Theorem

Let p be a prime number distinct from 2 and 11. Assume that for every ℓ satisfying (8), condition (10) holds true as well, and the following also holds: $\ell \equiv a \pmod{N}$ for some $a \in \mathcal{Z}_{\mathbb{Z}}(T)$. Then Conjecture LM holds for this p.

For Conjecture RLM we will restrict to the primes congruent to 2 modulo 3.

Theorem

Let p be a prime number satisfying $\Lambda \subset \mathbb{Q}_p$ and $3 \nmid N$. Assume that for every ℓ satisfying (8)*, condition* (10) *holds true as well, and the following also holds: $\ell \equiv a \pmod{N}$ for some $a \in \mathcal{Z}_{\mathbb{Q}}(T)$. Then Conjecture RLM holds for this p.*

The disproof of the conjectures for various primes p

We start with the negative parts. We implemented the algorithms implied by Theorem 21 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 ℓ such that (8), (10) and (11) all hold true. This calculation took a few minutes and found such an example ℓ for all $p \leq 600$ except for $p \in \{2, 3, 11, 83, 103, 163, 397\}$. See the table on the next page for the actual data. This proves the negative part of Theorem 8.

p	N	ℓ	u	p	N	ℓ	u	p	N	ℓ	u
5	31	21	2	179	32221	100	114	379	48007	309	76
7	48	5	1	181	10981	25	66	383	147073	219	338
13	168	6	4	191	36673	72	22	389	151711	1739	354
17	96	28	7	193	4656	171	76	401^*	400	265	132
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	5565	83	203	421	420	118	214
31	331	14	22	223	16651	361	38	431	61920	465	51
37	469	19	17	227	17176	34	57	433	62641	385	334
41	560	35	15	229	17557	249	61	439	6424	781	160
43	308	82	11	233	9048	36	126	443	196693	516	21
47^*	46	31	16	239	4760	28	85	449	202051	107	229
53^*	52	33	16	241	29040	506	57	457	34808	858	30
59	3541	64	34	251	63253	304	218	461	35420	192	9
61	1860	68	34	257	256	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
89	8011	109	8	281	13160	536	62	499^*	166	109	331
97	3169	19	51	283	13348	777	193	503	42168	107	497
101	680	186	23	293	28616	458	200	509	259591	1228	433
107	1272	184	52	307	31416	30	163	521	271963	2058	220
109	990	105	62	311	310	123	58	523	273528	237	16
113	12883	172	15	313	32761	29	184	541	58536	633	200
127	5376	586	30	317	100807	36	186	547	149604	104	72
131	5720	79	101	331	36631	188	4	557	103416	509	424
137	18907	11	5	337	16224	320	103	563	52828	87	232
139	3864	34	49	347	40136	156	244	569	53960	322	49
149	7400	10	38	349	17400	1428	33	571	40755	527	155
151	2850	223	142	353	124963	95	38	577	111169	361	85

Conjectures

Let $\mathcal{M}L$ and $\mathcal{N}RLM$ be the subsets of primes p such that Conjecture LM holds and Conjecture RLM fails, respectively. We offer the following conjecture.

Conjecture

Both subsets $\mathcal{M}L$ and $\mathcal{N}RLM$ are infinite. In fact, they are both of positive lower density as subsets of the set of all primes.

HAPPY BIRTHDAY BEN!