ON THE COMPOSITES AMONG $[\xi 7^n]$

RALF STEPHAN

Abstract. We prove that for every real $\xi > 0$ the sequence of integer parts $[\xi 7^n]$, $n = 0, 1, 2, \ldots$, contains infinitely many composite numbers. This is the case $a = 7$ of a problem going back to Forman and Shapiro (1967), stated by Dubickas and Novikas to be open for every integer $a \geq 7$. By the same certificate, applied to prime chains directly, there is no infinite right truncatable prime in base 7.

The proof reduces the problem to a single finite computation: modulo $M = \prod_{p \leq 31} p$, the digraph of residues traversed by a sequence avoiding all prime factors of M has a core in which no strongly connected component contains two distinct cycles, so every avoiding digit word is ultimately periodic and an elementary return theorem of Dubickas produces composite terms. The set $\{p \leq 31\}$ is *not* an unavoidable set of divisors — the method succeeds although, for this base, no unavoidable set is expected to exist.

All results, including the finite computation, are verified in Lean 4; the computation is checked by three quarantined `native_decide` evaluations, and everything else depends only on Lean's three standard axioms.

1. Introduction

Throughout, $[x]$ and $\{x\}$ denote the integer part and the fractional part of $x \in \mathbb{R}$. Following [Dub09, p. 273], a negative integer a is said to be composite if $|a|$ is composite; for the sequences considered below all terms are eventually positive, so nothing hinges on the convention. A sequence $u_0, u_1, u_2, \ldots$ is *ultimately periodic* if there is a $t \geq 1$ with $u_{n+t} = u_n$ for all sufficiently large n, and *purely periodic* if this holds for all $n \geq 0$ [Dub09, §2].

1.1. **The problem and known results.** Forman and Shapiro [FS67] proved in 1967 that the sequences $[(3/2)^n]$ and $[(4/3)^n]$ contain infinitely many composite numbers, and conjectured a general mechanism (their "pseudo-random difference equations") from which the same would follow for $[a^n]$ for every rational $a > 1$. For an integer base a the question is trivial at $\xi = 1$ but not for general ξ: by a metrical theorem of Koksma [Kok35], for every fixed $\xi > 0$ and almost every $a > 1$ the sequence $[\xi a^n]$ contains infinitely many composite terms, yet specific bases resist. Dubickas and Novikas [DN05] settled $a \in \{2, 3, 4, 6\}$ by exhibiting finite *unavoidable sets of divisors* and

Date: August 15, 2026.

Institute for Globally Distributed Open Research and Education (IGDORE).

settled $a = 5$ by a different, two-case argument (their Theorem 2), writing: "At the moment, we cannot prove that the integer parts $[\xi a^n]$, $n = 1, 2, \ldots$, where ξ is an arbitrary positive number and $a \geq 7$ is an integer, are composite for infinitely many $n \in \mathbb{N}$" [DN05, p. 637]. Dubickas [DubOst06] then framed the integer case as a conjecture.

Conjecture 1.1 ([DubOst06, Conjecture 2])**.** *If $b \geq 2$ is an integer then, for any real $\xi > 0$, the sequence $[\xi b^n]$, $n = 0, 1, 2, \ldots$, contains infinitely many composite numbers.*

The same paper introduces *infinite right truncatable primes*: an infinite word $u_0 u_1 u_2 \ldots$, where $u_0 \in \mathbb{N}$ is arbitrary and $u_1, u_2, \cdots \in \{0, 1, \ldots, b-1\}$, such that every prefix value $u_0 b^n + u_1 b^{n-1} + \cdots + u_n$ is prime. (A finite prefix of such a word is a *right truncatable prime* in the classical sense of Angell and Godwin [AG77]: a prime that stays prime under successive removal of its rightmost digit. In base 10 there are exactly 83 of them, the largest being 73939133.)

Conjecture 1.2 ([DubOst06, Conjecture 1])**.** *If $b \geq 2$ is an integer then there are no infinite right truncatable primes in base b.*

Dubickas proves in [DubOst06, §3] that Conjectures 1.1 and 1.2 are equivalent for every base. A finite set S of primes is called *unavoidable with respect to b* if for every $\xi > 0$ the sequence $[\xi b^n]$ contains infinitely many elements divisible by some $p \in S$ [DubOst06, §2]; an unavoidable set clearly proves Conjecture 1.1 for its base, and this is how $b \in \{2, 3, 4, 6\}$ were settled. But no unavoidable set exists for $b = 5$ [DN05, §5], nor for any $b \geq 3$ with $b - 1$ not squarefree [DubOst06, Theorem 4], and Conjecture 3 of [DubOst06] predicts that none exists for any $b \notin \{2, 3, 4, 6\}$ — in particular not for $b = 7$. So for $b = 7$ the divisor-set method is expected to be unavailable, and the base was left "open in both directions."

Most recently, Miller, Peng, Popescu, Siktar and Wattanawanichkul proved [MPP+24, Lemma A.1], in the language of prime walks, that it is impossible to walk to infinity on primes in bases $3, 4, 5, 6$ by appending a single digit at a time to the right — precisely Conjecture 1.2 for $b \leq 6$ (their argument collapses the digit alphabet by hand and finishes with Fermat's little theorem). The base $b = 7$ is the first one out of reach of such hand collapses: modulo small primes its admissible digit alphabet retains branching, and no single congruence collapse exists.

1.2. **Results.** We settle base 7, in both formulations.

Theorem A. *For every real $\xi > 0$ the sequence $[\xi 7^n]$, $n = 0, 1, 2, \ldots$, contains infinitely many composite numbers.*

Theorem B. *There is no infinite right truncatable prime in base 7: no infinite sequence of primes $p_0, p_1, p_2, \ldots$ satisfies $p_{n+1} = 7p_n + d_n$ with digits $d_n \in \{0, \ldots, 6\}$, for any starting prime p_0.*

Theorem A is the case $a = 7$ of the problem of [FS67] and [DN05] and the first open case of Conjecture 1.1; Theorem B is the corresponding case of Conjecture 1.2 and the next case after [MPP+24, Lemma A.1]. Theorem B is *not* obtained from Theorem A through the equivalence of [DubOst06, §3]: the certificate below applies to prime chains directly, and the exceptional $(b-1)^\infty$ digit tail that [DubOst06] must treat separately (by a Fermat argument) never arises on this route; see Remark 7.4.

1.3. **Method: a finite certificate.** Fix a finite set $\mathcal{P}$ of primes with modulus $M = \prod_{p\in\mathcal{P}} p$. If all large terms of $[\xi 7^n]$ are prime, they are eventually coprime to M, so their residues walk along the digraph[1] on the units of $\mathbb{Z}/M\mathbb{Z}$ with edges $r \to br + d$, $d \in \{0, \dots, b-1\}$, both ends coprime to M. The certificate, denoted $C(\mathcal{P})$, asks that after discarding the states not lying on bi-infinite admissible paths, *no strongly connected component of the graph contains two distinct cycles* — equivalently, every cyclic strongly connected component is a simple cycle, the spectral radius of the core is 1, and the topological entropy of the subshift is 0. If $C(\mathcal{P})$ holds for a single finite $\mathcal{P}$, then every infinite admissible path is ultimately periodic, so the digit word of any hypothetical prime-producing ξ is ultimately periodic — and an ultimately periodic digit word forces composite values infinitely often, by an elementary and completely general return theorem of Dubickas [Dub09, Theorem 4] (Theorem 2.1 below). One finite check therefore settles the base.

The computation reported here finds that $C(\mathcal{P})$ *fails* for base 7 at every $\mathcal{P} = \{p \le y\}$ with $y \le 29$ and *holds* at $\mathcal{P} = \{p \le 31\}$, i.e. at the modulus

$$M_{31} \;=\; \prod_{p\le 31} p \;=\; 200\,560\,490\,130.$$

Two points deserve emphasis. First, $C(\mathcal{P})$ is strictly weaker than the existence of an unavoidable set: an unavoidable set requires the core to be *empty*, whereas $C(\mathcal{P})$ tolerates surviving cycles — they correspond to ultimately periodic digit words, which the return theorem kills. Indeed the core at $y = 31$ is far from empty (it has 371 702 states; see Section 6), and the certificate does not refute [DubOst06, Conjecture 3] at $b = 7$; the surviving cycles are witnesses *for* that conjecture (Section 8). The cleanest calibration is base 5: there no unavoidable set can ever exist [DN05, §5], yet $C(\{2, 3, 5\})$ holds (Proposition 4.10) — the certificate succeeds on a base where the divisor-set method is provably impossible. Second, the certificate degenerates gracefully on the known bases: for $b = 3, 4, 5, 6$ it holds at hand moduli and reproves the results of [DN05] and [MPP+24], while for the open base $b = 10$ it fails at the same moduli (Proposition 4.11), so the machinery does not spuriously settle what is genuinely open.

[1] We are not aware of standard terminology for this digraph and call it the *coprimality graph* $\Gamma_b(M)$; its bi-infinite admissible paths form a subshift of finite type in the standard sense of symbolic dynamics.

1.4. **Formal verification.** Every statement in this paper, including the finite computation at M_{31}, has been verified in the Lean 4 proof assistant. The certificate data and Lean files are available at a github repo. The reduction — Sections 2–5 — depends on nothing beyond Lean's three standard axioms (propositional extensionality, choice, quotient soundness; abbreviated *std3*), with no cited-literature axioms: in particular [Dub09, Theorem 4] is *proved*, not assumed. The finite computation is checked by three evaluations of compiled Lean code (`native_decide`), which enlarges the trusted base by the Lean compiler on exactly those three runs; the checker is designed so that its witness data and search procedures require no correctness proofs — corrupt data can only make the check fail, never make a false statement provable. Appendix A records the Lean name and status of every statement and discusses the trusted base; kernel-checked alternatives were measured and do not reach this problem size.

Appendix B records, separately from the certified development, a closed form for the cycle set that lets a reader regenerate the whole witness from five short digit patterns. Appendix C gives an estimate for the resources necessary to tackle the $b = 10$ case.

2. The return theorem

The engine that disposes of every ultimately periodic digit word is the following theorem of Dubickas. We reproduce its proof, since the formalization follows it and the argument is short.

Theorem 2.1 ([Dub09, Theorem 4])**.** *Let $d \geq 1$, let $F \in \mathbb{Z}[z_1, \dots, z_{d-1}]$, let $c \neq 0$ be an integer, and let $x_0, x_1, x_2, \dots$ be integers satisfying*

$$x_{n+d} \;=\; c\,x_n + F(x_{n+1}, \dots, x_{n+d-1}) \qquad \text{for every } n \geq 0. \tag{2.1}$$

Then:

(i) *for every $q \geq 1$ with $\gcd(c, q) = 1$ the sequence is purely periodic modulo q: there is a $T > 0$ with $x_{n+T} \equiv x_n \pmod q$ for all $n \geq 0$;*
(ii) *if moreover $|x_n| \to \infty$, the sequence contains infinitely many composite terms.*

Proof sketch. (i) The window vectors $(x_n, \dots, x_{n+d-1})$ take finitely many values modulo q, so two of them agree, and (2.1) propagates the agreement forward: the sequence is ultimately periodic mod q. Both directions of propagation are carried by the single congruence $x_{n+d+t} - x_{n+d} \equiv c\,(x_{n+t} - x_n) \pmod q$, valid when the intermediate window entries already agree; since c is invertible modulo q, the same congruence read backwards pushes the period down to $n = 0$, by downward induction. (ii) Beyond the point where $|x_n| > |c|$, either all terms are composite — done — or some $|x_m|$ is a prime $q > |c|$. Then $\gcd(c, q) = 1$, so by (i) the sequence is purely periodic mod q and q divides x_{m+jT} for all j; those terms eventually exceed q in absolute value, hence are composite. □

Remark 2.2. The formalization proves Theorem 2.1 for any F that *descends to* $\mathbb{Z}/q\mathbb{Z}$ — congruent arguments give congruent values — which is all the proof uses; that every integer polynomial has this property is proved separately, so the statement above is recovered. The instances consumed later are the $d = 1$ cases with constant F.

3. Digit dynamics and ultimately periodic words

Fix an integer base $b \geq 2$ and a real $\xi > 0$, and set $x_n = [\xi b^n]$. Writing $d_n = [b\,\{\xi b^n\}]$ for the $(n+1)$-st digit of the b-adic expansion of ξ, one has the append-a-digit recurrence

$$x_{n+1} \;=\; b\,x_n + d_n, \qquad 0 \leq d_n \leq b-1, \tag{3.1}$$

and $|x_n| \to \infty$. Thus ξ enters only through its digit word $d_0 d_1 d_2 \ldots$, and the whole question is which digit words can avoid composite values.

Proposition 3.1. *Let a be a nonzero integer and let (x_n), (d_n) be integer sequences with $x_{n+1} = a\,x_n + d_n$ for all n, with (d_n) ultimately periodic and $|x_n| \to \infty$. Then (x_n) contains infinitely many composite terms.*

Proof sketch. Say $d_{m+L} = d_m$ for $m \geq n_0$, $L \geq 1$. Iterating the recurrence L steps gives, for the subsequence $y_k = x_{n_0+kL}$,

$$y_{k+1} \;=\; a^L\,y_k + C, \qquad C = \sum_{i<L} a^{L-1-i}\,d_{n_0+i},$$

where C is independent of k by the periodicity. This is (2.1) with $d = 1$, $c = a^L \neq 0$ and constant F, and $|y_k| \to \infty$, so Theorem 2.1(ii) gives infinitely many composite y_k. □

Note that no bound on the d_n is needed in Proposition 3.1, and that rationality of any generating ξ is never used: ultimate periodicity of the digit word feeds Theorem 2.1 directly. This is one step shorter than the classical route "periodic word $\Rightarrow \xi \in \mathbb{Q} \Rightarrow$ composites," and it is what later lets the certificate act on prime chains that come from no real number at all (Section 7).

For rational ξ the digit word is always ultimately periodic — this is the easy direction of [Dub09, Lemma 6], by finiteness of the orbit $\{\xi b^n\}$ — so Proposition 3.1 already settles the rational case of Conjecture 1.1, uniformly in the base:

Corollary 3.2 (essentially [Dub09, proof of Theorem 3])**.** *For every integer $b \geq 2$ and every rational $\xi > 0$ the sequence $[\xi b^n]$ contains infinitely many composite terms.*

4. The coprimality graph and two finite certificates

4.1. **The graph.**

Definition 4.1. Let $b \geq 2$ and let $M \geq b$ be a positive integer. The *coprimality graph* $\Gamma_b(M)$ is the digraph whose vertices are the residues $r \in \mathbb{Z}/M\mathbb{Z}$ coprime to M, with an edge $r \to t$ labelled by the digit $d \in \{0, \ldots, b-1\}$ whenever $t = br + d$ in $\mathbb{Z}/M\mathbb{Z}$ and t is coprime to M. Such edges are called *admissible steps*.

If all terms x_n of a sequence obeying (3.1) are, from some index on, coprime to M — as they are when all large terms are primes exceeding M — then their residues form an infinite path in $\Gamma_b(M)$. Two finite certificates about $\Gamma_b(M)$ will each force such a path to be ultimately periodic. Since $0 \leq d_n < b \leq M$, the digits are determined by the residues (two digits congruent modulo M and both in $[0, b)$ are equal), so an ultimately periodic residue path makes the digit word ultimately periodic, and Proposition 3.1 applies.

4.2. **The rank certificate.**

Definition 4.2. A *rank certificate* for $\Gamma_b(M)$ is a function $\rho\colon \mathbb{Z}/M\mathbb{Z} \to \mathbb{N}$ such that along every admissible step $r \to t$ one has $\rho(t) \leq \rho(r)$, and every vertex has at most one admissible successor of equal rank: if $r \to t$ and $r \to u$ are admissible with $\rho(t) = \rho(r) = \rho(u)$, then $t = u$. We write $C(\mathcal{P})$ for the assertion that a rank certificate exists for $\Gamma_b\big(\prod_{p\in\mathcal{P}} p\big)$.[2]

Proposition 4.3. *Let S be a finite set with a relation $\to$ on it, and let $\rho\colon S \to \mathbb{N}$ satisfy the two conditions of Definition 4.2 for $\to$. Then every infinite path $s_0 \to s_1 \to s_2 \to \cdots$ in S is ultimately periodic.*

Proof sketch. Along the path ρ is non-increasing, hence eventually constant, say from n_1 on. By finiteness two later states coincide, $s_p = s_q$ with $n_1 \leq p < q$; and past n_1 the path is deterministic — s_{m+1} and s_{m+L+1} are admissible successors of the same state, both of equal rank, hence equal — so the repetition propagates forever. □

Theorem 4.4. *Let $b \geq 2$ and $M \geq b$, and suppose a rank certificate exists for $\Gamma_b(M)$. Then for every real $\xi > 0$ the sequence $[\xi b^n]$ contains infinitely many composite terms; that is, one finite certificate settles Conjecture 1.1 for the base b.*

Proof sketch. Suppose only finitely many terms were composite. Since $[\xi b^n] \to \infty$, all large terms are primes exceeding M, hence coprime to M, so the residue path is an infinite admissible path of $\Gamma_b(M)$. By Proposition 4.3 it is ultimately periodic; the digits are pinned down by the residues, so the digit word is ultimately periodic; and Proposition 3.1 produces infinitely many composite terms — a contradiction. □

[2] $C(\mathcal{P})$ is equivalent to the graph-theoretic statement of Section 1.3: taking $\rho(r)$ to be the height of the strongly connected component of r in the condensation of $\Gamma_b(M)$, edges between components strictly drop the height and edges inside preserve it, so the uniqueness clause says exactly that no vertex has two outgoing edges inside its own component, i.e. every cyclic component is a simple cycle. Conversely such a ρ exists whenever that holds. The rank form is the one a proof kernel can check with no graph algorithms.

4.3. **The compressed-core certificate.** The computation for base 7 produces something smaller than a rank function: a list of cycles. The following second certificate form consumes exactly that.

Definition 4.5. Let K be a set of residues modulo M. Consider the two conditions:

(a) K *catches every cycle*: every residue lying on a cycle of $\Gamma_b(M)$ belongs to K;
(b) K *is deterministic*: for every $r \in K$ and digits $d_1, d_2 \in \{0, \dots, b-1\}$, if $br + d_1$ and $br + d_2$ both lie in K then $br + d_1 = br + d_2$ in $\mathbb{Z}/M\mathbb{Z}$. (Admissibility of the two steps is not required; this is the form the checker of Section 6 verifies.)

Lemma 4.6. *Every sequence in a finite set eventually takes only* recurrent *values, i.e. values that reappear arbitrarily late.*

Proposition 4.7. *If K satisfies (a) and (b), then every infinite admissible path in $\Gamma_b(M)$ is ultimately periodic.*

Proof sketch. By Lemma 4.6, every sufficiently late state of the path is recurrent; a recurrent state lies on a cycle (follow the path from one occurrence to the next), hence lies in K by (a). From there the path is forced by (b), so a repetition, supplied by finiteness, propagates forever. □

Theorem 4.8. *Let $b \geq 2$ and $M \geq b$, and suppose some set K of residues modulo M satisfies (a) and (b). Then for every real $\xi > 0$ the sequence $[\xi b^n]$ contains infinitely many composite terms.*

The proof is that of Theorem 4.4 with Proposition 4.7 in place of Proposition 4.3. When every unit has at most one unit successor, one may take $K =$ all units, condition (a) being automatic; this is the situation for bases 3 and 5 below.

Remark 4.9 (The two forms are incomparable). Condition (b) is strictly stronger than $C(\mathcal{P})$ in one respect: $C(\mathcal{P})$ allows an edge from one cycle to another (the rank drops across it), while (b) forbids it. Base 4 modulo 6 is a worked, kernel-checked example: both units are fixed points under the digit 3 (the map $r \mapsto 4r+3$ fixes 1 and 5 modulo 6), and the admissible edge $1 \to 5$ (digit 1) joins the two cycles, so the rank certificate exists (with $\rho(1) = 1$, $\rho(5) = 0$) but (b) fails for every K containing the cycle states. Conversely (a) is a global statement no local check sees. Using the core form for base 7 is justified by a measured fact: in the certified core at $\mathcal{P} = \{p \leq 31\}$ there are no edges between distinct cycles at all (Section 6).

4.4. **Bases 3–6 in the kernel, and two controls.** For the bases settled in [DN05] and [MPP+24] the certificate holds at hand moduli, with explicit rank functions checked by Lean's kernel decision procedure; the entire pipeline of Theorem 4.4 then runs end to end with no compiled code involved. Nothing below is new; the point is calibration and non-vacuity of the machinery.

Proposition 4.10. *$C(\{2,3\})$ holds for the bases 3 and 4, and $C(\{2,3,5\})$ holds for the bases 5 and 6. Explicit certificates: modulo 6 the constant rank works for $b = 3$ (every unit has a unique admissible successor), and $\rho = \mathbf{1}_{\{1\}}$ works for $b = 4$; modulo 30 the constant rank works for $b = 5$, and $\rho(r) = 2\,(4 - (r \bmod 5)) + \mathbf{1}_{\{r\equiv 1\,(3)\}}$ works for $b = 6$. Consequently, for every real $\xi > 0$ and $b \in \{3,4,5,6\}$ the sequence $[\xi b^n]$ contains infinitely many composite terms.*

Note that $b = 4$ and $b = 6$ genuinely need a non-constant rank: their graphs contain surviving cycles (e.g. $x \mapsto 4x + 3$ fixes 1 modulo 6), which the certificate tolerates precisely because a periodic word is harmless. For $b = 5$ the modulus 30 is exactly where the alphabet collapse in the proof of [DN05, Theorem 2] lives, and — the calibration promised in Section 1.3 — the certificate succeeds although no unavoidable set exists for this base [DN05, §5].

Proposition 4.11. *No rank certificate exists modulo 30 for base 7, nor for base 10. Specifically, if a vertex r has two distinct admissible successors that both return to r, no rank function can satisfy Definition 4.2; for $b = 7$ the residue 1 has the returning successors 7 (digit 0; return $7 \to 19 \to 13 \to 1$) and 11 (digit 4; return $11 \to 17 \to 1$), and for $b = 10$ the residue 13 has the returning successors 13 (digit 3, a fixed point) and 19 (digit 9; return $19 \to 13$).*

The control matters in both directions: the certificate does not fire early on base 7 (consistently with the ladder of Section 6, which finds it only at $y = 31$), and it does not appear to settle base 10, the open base singled out in [DubOst06].

Remark 4.12 (What the obstruction is, and what it is not). The mechanism behind Proposition 4.11 is worth isolating, because it also explains which arrangements of several cycles the certificate tolerates.

Suppose a strongly connected component contains two distinct cycles. Then some state of it has two outgoing admissible edges that both stay in the component — for if every state had exactly one, the forward orbit of any state would be forced, and being strongly connected it would have to return, so the component would be a single simple cycle. At such a branch point every visit offers a genuine choice, and the choices are unconstrained: one may go round the first cycle n_1 times, take the exit, go round the next n_2 times, and so on, for an *arbitrary* sequence (n_k). Choosing (n_k) aperiodic yields an infinite admissible path that is not ultimately periodic — precisely what the reduction of Theorems 4.4 and 4.8 cannot survive — and counting the choices shows the entropy is positive. Even the sparsest such arrangement is expensive: three states r_1, r_2, r_3, each a fixed point and each with one further edge $r_i \to r_{i+1}$ cyclically, has adjacency matrix of characteristic polynomial $(1 - \lambda)^3 + 1$ and hence Perron root exactly 2. A rank function detects all of this without computing cycles at all: when two

distinct successors of r both return to r, the rank is squeezed to be constant on all three states, and the uniqueness clause of Definition 4.2 then collapses the two successors into one.

What the certificate does *not* forbid is several cycles chained *one way*. There the cycles lie in distinct components, the rank strictly drops from each to the next, and an infinite path falls through finitely many of them before being trapped in the last one forever — so it is ultimately periodic after all. This is not a marginal case but the actual shape of the base-7 core at M_{31}, whose measured condensation rank of 241 says such chains run up to that length. The whole distinction is the direction of the closing edge, which is why the certificate is stated in terms of components rather than of cycles; Figure 1 shows the two configurations side by side. In the language of symbolic dynamics: a strongly connected digraph has topological entropy zero if and only if every vertex has out-degree 1, that is, if and only if it is a single simple cycle.

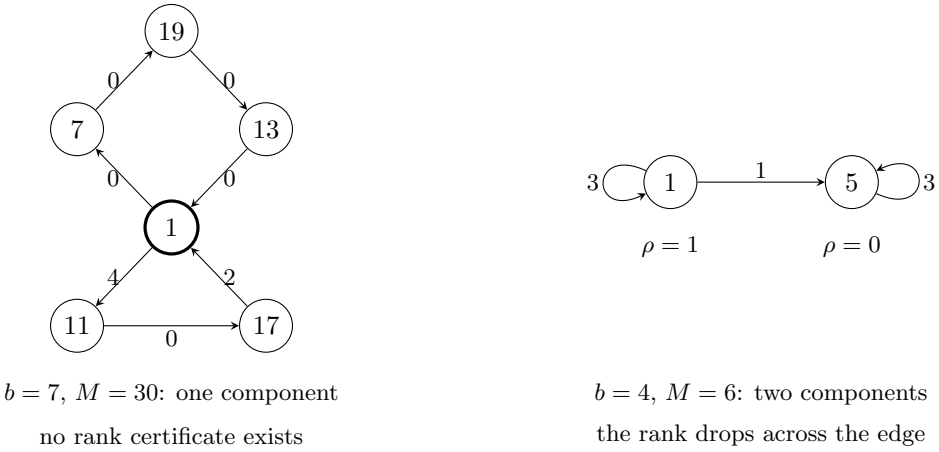

FIGURE 1. Two cycles in one component, and two cycles in two. On the left, the control of Proposition 4.11: modulo 30 in base 7 the residue 1 lies on the two distinct cycles $1 \to 7 \to 19 \to 13 \to 1$ and $1 \to 11 \to 17 \to 1$, so all six residues form a single strongly connected component, branching at the state drawn heavy. Loop counts may be chosen freely, admissible paths need not be ultimately periodic, and no rank function exists. On the right, base 4 modulo 6: both units are fixed points under the digit 3, but the digit-1 edge $1 \to 5$ runs one way, so the two cycles are separate components and the rank ρ certifies the base. Edge labels are the appended digits; every edge is an admissible step $t \equiv br + d$ with both ends coprime to M.

5. The ladder

Condition (a) of Definition 4.5 quantifies over the whole residue ring, which at the modulus $M_{31} \approx 2 \times 10^{11}$ is far beyond any direct check. This section reduces it to a chain of finite checks — one per prime of $\mathcal{P}$ — whose largest link involves about 2.2×10^7 residues. Two ingredients do all the work.

5.1. **Rank certificates for cycle confinement.**

Lemma 5.1. *Let C and K be sets of states with C containing every state that lies on a cycle, and let ρ be a rank such that along every admissible step $r \to t$ with $r, t \in C$ one has $\rho(t) \le \rho(r)$, with strict inequality whenever $r \notin K$. Then every state lying on a cycle belongs to K. The same conclusion holds with all inequalities reversed ($\rho(r) \le \rho(t)$, strict when $t \notin K$).*

Proof sketch. Every state visited by a cycle is itself on a cycle, so a cycle through some $r \notin K$ stays inside C; following it once around gives $\rho(r) < \rho(r)$. The reversed form follows by applying this to the reversed relation, under which cycles are cycles. □

Both orientations are needed. Peeling states with no admissible successor (and iterating) certifies confinement to the *forward-surviving* set, which is much coarser than the set of cycle states — at the fourth rung below, forward peeling leaves 2 704 992 states where only 748 621 survive in both directions. Peeling the reversed graph *of the forward survivors* closes the gap exactly, and a third stage is provably empty: forward-then-backward survival already characterizes the states with bi-infinite admissible paths.

5.2. **Projection.**

Lemma 5.2. *Let $M' \mid M$. The canonical ring homomorphism $\mathbb{Z}/M\mathbb{Z} \to \mathbb{Z}/M'\mathbb{Z}$ maps admissible steps of $\Gamma_b(M)$ to admissible steps of $\Gamma_b(M')$, hence cycles to cycles. Consequently, if K' catches every cycle modulo M', then the preimage $\pi^{-1}(K')$ catches every cycle modulo M.*

Proof sketch. Units map to units under a ring homomorphism, and the edge relation $t = br + d$ is preserved since b and d are integers. □

5.3. **The rung.**

Theorem 5.3. *Let $M' \mid M$, let K' catch every cycle of $\Gamma_b(M')$, and let K and ρ satisfy the hypotheses of Lemma 5.1 with candidate set $C = \pi^{-1}(K')$. Then K catches every cycle of $\Gamma_b(M)$.*

The obligation of Theorem 5.3 is finite in a strong sense: every residue with $\pi(r) \in K'$ is $r' + kM'$ for its own projection $r' \in K'$ and a unique $0 \le k < M/M'$, so the two rank conditions need to be checked at exactly $|K'| \cdot (M/M')$ explicit residues (times b digits), and the full residue ring is never enumerated. Iterating down a chain $M_0 \mid M_1 \mid \cdots \mid M_k = M$ turns

condition (a) at M into a nest of such loops. Two further economies matter in practice: an admissible successor is coprime to M, hence (when $2, 7 \mid M$ and $b = 7$) odd and not divisible by 7, which forces the digit into $\{2, 4, 6\}$ by an arithmetic test on r and d alone; and the certificate data C, K, ρ enter the formal statements as arbitrary functions of the residue — in the implementation, array lookups — about which nothing is assumed, so the arrays may be produced by an unverified program and a wrong entry can only make the check fail. (In the formal development the certificates are stated in natural-number arithmetic with a single bridge lemma to $\mathbb{Z}/M\mathbb{Z}$; the smallest instance of the whole mechanism, base 3 modulo 6 with exact cycle set $\{5\}$ and rank $\mathbf{1}_{\{r\neq 5\}}$, is kernel-checked as a sanity witness.)

6. The certificate at $\mathcal{P} = \{p \le 31\}$

We now fix $b = 7$ and $M = M_{31} = \prod_{p\le 31} p$ and assemble Theorem A. The certified chain has three links: the ladder confines every cycle to a computed core (Theorem 6.1); a condensation rank on that core confines every cycle to a stored cycle set K (Theorem 6.3); and K is deterministic (Theorem 6.2). Theorem 4.8 then applies.

6.1. **The five rungs.**

The ladder ascends through the moduli

$$M_0 = \prod_{p\le 17} p = 510\,510, \qquad M_1 = M_0 \cdot 19, \qquad M_2 = M_1 \cdot 23,$$

$$M_3 = M_2 \cdot 29, \qquad M_4 = M_3 \cdot 31 = M_{31}.$$

At the bottom, the candidate set is all units of $\mathbb{Z}/M_0\mathbb{Z}$, for which condition (a) is automatic. At each level the witness generator computes, by layered worklist peeling, a forward rank (the round at which a state is removed for lack of an admissible successor among the survivors, a fixed cap marking the survivors) and then a backward rank on the reversed graph of the forward survivors; Lemma 5.1 in both orientations certifies each stage, and Lemma 5.2 with Theorem 5.3 lifts the result to the next modulus, the candidate set being the fibre of the previous level's survivor set intersected with the units at the new prime. All ten stage checks (two per rung) are evaluated in a single run of the compiled checker.

Theorem 6.1. *Every residue lying on a cycle of $\Gamma_7(M_{31})$ belongs to the computed survivor set of the fifth rung — the states of the fibre grid that survive forward and backward peeling at every level.*

The survivor set of Theorem 6.1 — henceforth *the core* — is a property of the shipped witness arrays; its measured cardinality is 371 702, a number that appears in no formal statement. The measured peeling depths are at most 528 forward and 319 backward, comfortably below the cap of 1024.

6.2. **The cycle set and its determinism.** The second witness is a list of 849 cycles carrying 365 761 residues, each cycle stored as a base residue and its digit word over $\{2, 4, 6\}$. (Those digit words turn out to be repetitions of just five short patterns, so the entire list is regenerable from one line of data; Appendix B records this, and it is used nowhere below.) The certified checker *defines* K as the set of residues at which a membership search into the decoded, sorted array answers positively; the search reports an index and the array is asked what is stored there, so a positive answer literally exhibits the element, and neither the decoder nor the search needs a correctness proof — nor even the claim that the array lists exactly the cycles.

Theorem 6.2. *K is deterministic in the sense of Definition* 4.5(b).

K must be the cycle set rather than the core: measured on the witness, 147 of the core states have two successors inside the core, so condition (b) is false for the core itself.

6.3. **From the core to the cycles.** The remaining gap between Theorems 6.1 and 6.2 is the 5 941 core states outside K (transient states sitting on paths between cycles). One more instance of Lemma 5.1 closes it: weight an edge of the core by 0 if both ends lie in K and by 1 otherwise, and let $\rho(r)$ be the longest weighted path out of r, computed by worklist relaxation over the reversed core. Out of a state not in K every edge has weight 1, so ρ strictly drops, and it never increases along any core edge; the computed array (measured: $\rho \le 241$) is verified against exactly these inequalities. A divergent relaxation would fail the check rather than certify anything false.

Theorem 6.3. *Every residue lying on a cycle of $\Gamma_7(M_{31})$ belongs to K.*

6.4. **Proof of Theorem A.** By Theorems 6.3 and 6.2, the set K satisfies conditions (a) and (b) of Definition 4.5 for $\Gamma_7(M_{31})$, and $7 \le M_{31}$. Theorem 4.8 gives, for every real $\xi > 0$, infinitely many composite terms in $[\xi 7^n]$. □

6.5. **The computation, and what is certified.** Only the Boolean verdicts of the three checks above are certified; every cardinality, spectral quantity and timing in this subsection is a measurement, reported for context and reproduced independently (each number below has been re-derived by at least one outside implementation working only from Definition 4.1). The ladder data:

rung	core states	grid states	candidate residues	$C(\{p \le y\})$
$y = 17$	6 228	510 510	92 160	fails
$y = 19$	53 218	118 351	112 104	fails
$y = 23$	377 594	1 224 037	1 170 796	fails
$y = 29$	748 621	10 950 255	10 572 632	fails
$y = 31$	371 702	23 207 282	22 458 630	**holds**

Against the 2×10^{11} residues of the naive quantifier, the whole ladder enumerates about 3.4×10^7 candidates — a factor of roughly 10^4. At every failing

rung the base-7 graph carries exactly *one* branching strongly connected component (measured Perron roots $\lambda = 1.149522$, 1.102168, 1.055294, 1.013061 at $y = 17, 19, 23, 29$); at $y = 31$ the branching vanishes, the core splits into 849 simple cycles with no edges between distinct cycles, and the spectral radius is exactly 1 — a combinatorial fact (0 branching components, $|E| = |V|$ on every cyclic component), not a floating-point one. The verdict is stable one rung higher: at $y = 37$ the core grows twelvefold (to 4 454 022 states) yet remains at spectral radius 1. By contrast the same pipeline run on the open base 10 fails with a *growing* branching count ($1, 2, 4, 8$ across the first four rungs), while it certifies bases $3, 4, 6$ at the smallest modulus and base 5 exactly from the modulus at which the collapse of [DN05, Theorem 2] kicks in. The first-moment heuristic $\bar{\lambda}(y) = 7\prod_{p\le y}(1 - 1/p)$, which crosses 1 near $y = 43$, is what suggested looking at moduli in this range; it is not the Perron root and plays no role in any statement.

7. Truncatable primes

We now derive Theorem B from the same certificate, without passing through the equivalence of [DubOst06, §3].

Definition 7.1 ([DubOst06, §1])**.** An *infinite right truncatable prime* in base b is an infinite sequence of primes $p_0, p_1, p_2, \ldots$ with $p_{n+1} = b\,p_n + d_n$ for some digits $d_n \in \{0, \ldots, b-1\}$ — equivalently, an infinite digit word all of whose prefix values are prime. The starting prime p_0 is arbitrary (it need not be a single digit), and the appended digits are not required to be prime; both choices make the nonexistence statements below stronger, and match the "from any starting prime" form of [MPP+24, Lemma A.1].

The certificate machinery never used more about $x_n = [\xi b^n]$ than the three facts: $x_{n+1} = bx_n + d_n$ with $0 \le d_n < b$, and $|x_n| \to \infty$. A prime chain supplies all three — growth is free, since $p_{n+1} \ge b\,p_n \ge p_n + 2$ — so the reduction applies verbatim to the abstract recurrence:

Proposition 7.2. *Let $b \ge 2$ and $M \ge b$, and suppose $\Gamma_b(M)$ admits either a rank certificate or a set K satisfying (a) and (b). Then no integer sequence with $x_{n+1} = b\,x_n + d_n$, $0 \le d_n < b$ and $|x_n| \to \infty$ consists entirely of primes.*

Proof sketch. All terms beyond the point where $|x_n| > M$ are primes exceeding M, hence coprime to M, so the residue path is admissible and the certificate makes the digit word ultimately periodic (Propositions 4.3, 4.7). By Proposition 3.1 some term is composite — contradicting primality of all terms. □

Proof of Theorem B. Apply Proposition 7.2 at $M = M_{31}$ with the certified set K of Theorems 6.3 and 6.2. □

Corollary 7.3 ([MPP+24, Lemma A.1])**.** *There is no infinite right truncatable prime in base 3, 4, 5 or 6.*

Proof sketch. Proposition 7.2 against the kernel-checked certificates of Proposition 4.10. The hand proofs of [MPP+24] collapse the alphabet to a constant digit by congruences and kill the constant word by Fermat's little theorem; here the collapse is subsumed by the certificate and the Fermat step is the period-1 case of the return theorem. □

Remark 7.4 (Why §3 of [DubOst06] is bypassed). The implication Conjecture 1.1 ⇒ Conjecture 1.2 in [DubOst06, §3] builds $\xi = \lim p_n/b^n$ from a prime chain and identifies $[\xi b^n]$ with p_n. The identification fails on exactly one family: when the digit word ends in $(b-1)^\infty$ one has $\xi b^n = p_n + 1$ exactly, the floor is off by one, and [DubOst06] closes that branch with a separate Fermat argument. Applying the certificate to the chain itself, there is no real number, no series and no branch: an all-$(b-1)$ word is ultimately periodic like any other, and Proposition 3.1 disposes of it with everything else. The exceptional family is thus an artefact of passing through ξ, not of the problem. We use nothing of [DubOst06, §3], and the general-base equivalence proved there is not reproved here.

Remark 7.5 (Non-vacuity). A routine enumeration (not part of the formal development) finds exactly 19 right truncatable primes in base 7, the longest chain being $2 \to 19 \to 139 \to 977 \to 6841$, i.e. $6841 = (25642)_7$ — the base-7 analogue of the 83 base-10 right truncatable primes of [AG77] topped by 73939133. Theorem B quantifies over arbitrary prime starting points, so it asserts strictly more than the finiteness this enumeration exhibits.

8. Concluding remarks

What the certificate does not establish. The set $\{p \le 31\}$ is not an unavoidable set of divisors for base 7, and the present method cannot make it one: the core at M_{31} is nonempty, and the whole design of $C(\mathcal{P})$ is that it does not need to be. Nor is [DubOst06, Conjecture 3] refuted at $b = 7$ — on the contrary. Of the 849 certified cycles, a measured 176 are the all-6 digit words (the non-terminating representations of terminating 7-adic rationals, not floor expansions of any ξ); the remaining 673 cycles — those whose digit word is built from one of the four non-constant patterns of Appendix B — are floor expansions of explicit periodic rationals ξ whose sequences $[\xi 7^n]$ avoid every prime $p \le 31$ forever. Each is a witness *for* Conjecture 3, exactly as the theory predicts: avoidance survives, but only periodically, and periodic avoidance produces composites by the return theorem rather than primes.

The one-line summary of the method. For base 5, no unavoidable set can exist [DN05, §5], yet $C(\{2,3,5\})$ holds; for base 7, Conjecture 3 predicts no unavoidable set exists, and $C(\{p \le 31\})$ holds. The zero-entropy certificate is the divisor-set method with its one false demand — an empty core — removed.

Acknowledgements

The formalization and the write-up were carried out in collaboration with Claude Code. An anonymous outside reviewer re-derived the full ladder from the transition rule alone, exposing an encoding discrepancy in earlier core-size bookkeeping and confirming every number in Section 6.5.

Appendix A. Formalization

The certificate data and Lean files are available at `https://github.com/rwst/On-Composites/`. Every numbered statement of Sections 2–7 is verified in Lean 4; the measured quantities of Sections 6.1–6.5 and Remarks 7.5 and the cycle classification of Section 8 are computations outside the kernel, labelled as such where they occur. The development lives in the directory `DubC/` of the author's Lean corpus (namespace `DubC`), in thirteen modules; the statements below name the file without the `DubC.` prefix. "std3" abbreviates Lean's three standard axioms (propositional extensionality, choice, quotient soundness). No cited-literature axiom occurs anywhere in the development: [Dub09, Theorem 4] is proved in `ReturnEngine.lean`, not assumed.

A.1. **The trusted base.** Three statements are checked by `native_decide`, which compiles the checker and trusts the Lean compiler for that evaluation:

- N_1 = `Rungs.chkAll_true` — the ten rung stages over 22 458 630 candidate residues (1 159 s);
- N_2 = `Y31.checkDet_true` — determinism of the 365 761-state K (16 s);
- N_3 = `Cycles.chkCyc_true` — the condensation rank on the core (410 s for the module).

These three files are quarantined: nothing std3 imports them, and `#print axioms` names the dependency at every use site. The design keeps the trusted reasoning minimal in a specific sense: all witness data (the peeling ranks, the cycle list, the relaxation array) and all search procedures (binary search, decoding) are *unverified by construction* — membership answers exhibit their own witness, and the certified statements quantify over whatever the arrays contain — so corrupt data can only make a check evaluate to `false`, never prove a false theorem. What must be believed beyond the compiler is a handful of small kernel-checked bridge lemmas between array indices and residue arithmetic.

The kernel-only alternatives were measured and do not reach this scale. Lean's kernel special-cases `Nat` and `String` only, so an array reduces structurally and the $\approx 1.8 \times 10^5$ membership queries of the determinism check alone cost $\approx 7 \times 10^{10}$ reduction steps; the kernel-checked call-by-value evaluator (std3-only) constructs $\approx$118 kB of proof term per reduction step, putting the 365 761-step cycle walk near 43 GB before any membership work, and represents arrays as terms, so a single lookup into even a 10^4-element array

costs ≈1.5 s against $\approx 2.5 \times 10^6$ lookups needed. A higher rung does not help: at $y = 37$ the core grows rather than shrinks (Section 6.5). The choice at this size is compiler trust or no theorem; the response is quarantine. (Timings: Lean 4.32.0-rc1, single workstation, 30 GB.)

A.2. **Statement index.** Status "std3+N_i" means the statement additionally depends on the named evaluation(s) of Appendix A.1.

Reduction and certificates (§2–§5).

Statement	Lean identifier	File	Status
composite integer	`CompositeInt`	`ReturnEngine`	def
recurrence (2.1)	`IsReturnRec`	`ReturnEngine`	def
Thm. 2.1(i)	`purely_periodic_mod_of_coprime`	`ReturnEngine`	std3
Thm. 2.1(ii)	`infinite_composites`	`ReturnEngine`	std3
Rem. 2.2	`CongrPreserving`	`ReturnEngine`	def
—	`congrPreserving_mvPolynomial`	`ReturnEngine`	std3
(3.1)	`floorPow_succ`, `floorDigit_nonneg/lt`	`DigitRecurrence`	std3
Prop. 3.1	`infinite_composites_of_periodic_digits`	`DigitRecurrence`	std3
—	`isReturnRec_progression`	`DigitRecurrence`	std3
Cor. 3.2	`infinite_composites_floorPow_of_rat`	`DigitRecurrence`	std3
Def. 4.1	`Cop`, `Step`	`Certificate`	def
Def. 4.2	`CertOK`	`Certificate`	def
Prop. 4.3	`eventually_periodic_of_rank`	`Certificate`	std3
Thm. 4.4	`infinite_composites_floorPow_of_certOK`	`Certificate`	std3
Def. 4.5	`CoreClosed`, `CoreDet`	`CoreCertificate`	def
Lem. 4.6	`exists_tail_recurrent`	`CoreCertificate`	std3
Prop. 4.7	`eventually_periodic_of_core`	`CoreCertificate`	std3
Thm. 4.8	`infinite_composites_floorPow_of_coreCert`	`CoreCertificate`	std3
— (K = units)	`infinite_composites_floorPow_of_unitDet`	`CoreCertificate`	std3
Rem. 4.9	`certOK_four`, `not_coreDet_four_six`	`Verdict`	std3
Prop. 4.10	`certOK_three/four/five/six`	`Verdict`	std3
—	`infinite_composites_three/four/five/six`	`Verdict`	std3
Prop. 4.11	`not_certOK_of_two_returning_successors`	`Verdict`	std3
—	`not_certOK_seven_thirty`, `not_certOK_ten_thirty`	`Verdict`	std3
Lem. 5.1	`transGen_self_of_rank`, `coreClosed_of_rankOn/RevOn`	`Ladder`	std3
Lem. 5.2	`step_proj`, `onCycle_proj`, `coreClosed_comap`	`Ladder`	std3
Thm. 5.3	`coreClosed_of_ladder`	`Ladder`	std3
— (fibres)	`forall_of_forall_lift`, `forall_lift_nat`	`Ladder`, `Rung`	std3
— (ℕ-forms)	`coreClosed_of_rankNat/RevNat`, `digit_guards`	`Rung`	std3

The base-7 certificate and the main theorems (§6–§7).

Statement	Lean identifier	File	Status
M_{31}	`primorial31`	`Verdict`	def
Thm. 6.1	`Rungs.cc4`	`Rungs`	std3+N_1
K	`Y31.Kset`	`Y31`	def
— (search soundness)	`Y31.bmem_sound`	`Y31`	std3
Thm. 6.2	`Y31.coreDet_seven`	`Y31`	std3+N_2
Thm. 6.3	`Cycles.coreClosed_seven`	`Cycles`	std3+$\mathsf{N}_1, \mathsf{N}_3$
Thm. A	`Cycles.infinite_composites_seven`	`Cycles`	std3+N_1–N_3
Def. 7.1	`InfiniteTruncatablePrime`	`Truncatable`	def
digit recurrence	`IsDigitRec`	`Truncatable`	def
— (chains qualify)	`exists_digitRec_of_truncatable`	`Truncatable`	std3
Prop. 7.2	`not_forall_prime_of_certOK/coreCert`	`Truncatable`	std3
Thm. B	`no_infiniteTruncatablePrime_seven`	`Truncatable`	std3+N_1–N_3
Cor. 7.3	`no_infiniteTruncatablePrime_three/.../six`	`Truncatable`	std3

The Lean statements of Theorems 6.1, 6.2 and 6.3 quantify over the shipped witness arrays and mention no cardinalities; the counts 371 702, 365 761, 849, 147, 5 941 and the rank bound 241 are measurements of those arrays, reproduced by outside implementations. Four statements of this paper are deliberately *not* formalized and are flagged where they occur: the equivalence of Conjectures 1.2 and 1.1 for general b ([DubOst06, §3]; bypassed, Remark 7.4), the enumeration of Remark 7.5, the cycle classification of Section 8, and Proposition B.4 of Appendix B.

Appendix B. The cycle set in closed form

The certified statements of Section 6 quantify over the shipped witness arrays and say nothing about their contents, which is what keeps the witness untrusted. The arrays are nevertheless far from arbitrary, and this appendix records the structure we find in them: the whole cycle set is generated by *five* digit patterns, so a reader can regenerate all 365 761 residues from one line of data, in milliseconds, without obtaining any file. Proposition B.4 is a computation, not a formalized theorem, and nothing in Sections 2–7 rests on it.

B.1. **Periodic digit words.**

Definition B.1. Let $u = u_0 u_1 \cdots u_{\ell-1}$ be a nonempty word of length ℓ over $\{2, 4, 6\}$, and let $m \geq 2$. The *u-walk* from a residue x modulo m is the sequence

$$r_0 = x, \qquad r_{n+1} \equiv 7\, r_n + u_{n \bmod \ell} \pmod m,$$

and x is *u-admissible modulo m* if every r_n is coprime to m and $r_{k\ell} = x$ for some $k \geq 1$. We write $S_m(u)$ for the set of such x.

A u-admissible residue lies on a cycle of $\Gamma_7(m)$ whose digit word is u^k, and conversely a cycle whose digit word has minimal period ℓ makes each of its states u-admissible for the corresponding rotation of u. The point of Definition B.1 is that admissibility factors completely over the primes.

Lemma B.2. *Let m be squarefree. Then $x \in S_m(u)$ if and only if $x \bmod q \in S_q(u)$ for every prime $q \mid m$; that is, $S_m(u)$ is the image of $\prod_{q\mid m} S_q(u)$ under the Chinese remainder isomorphism.*

Proof. Reduction modulo q carries the u-walk from x to the u-walk from $x \bmod q$, and for squarefree m a residue is coprime to m exactly when it is nonzero modulo every $q \mid m$. The walk is a map on the finite set $(\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/\ell\mathbb{Z})$ which is the product over $q \mid m$ of the corresponding maps, and a point of a finite product system is periodic precisely when each of its coordinates is. □

Each set $S_q(u)$ is computed by following the walk on the at most $q \cdot \ell$ pairs $(r, n \bmod \ell)$ and keeping the starting residues whose orbit is periodic and never meets 0 — for $q \le 31$ and $\ell \le 17$ that is at most 527 pairs, so the whole computation is done by hand or by a dozen lines of code.

Two of the eleven factors can be written down in closed form, and they are the two that explain the shape of the answer. The first is $q = 3$, where the condition is purely combinatorial: it constrains the *word*, not the residue.

Lemma B.3. *For a nonempty word u of length ℓ over $\{2, 4, 6\}$,*

$$|S_3(u)| = \begin{cases} 2, & u = \mathtt{6}^\ell, \\ 1, & u \text{ is not constant and, read cyclically, its letters} \\ & \text{other than } \mathtt{6} \text{ alternate between } \mathtt{2} \text{ and } \mathtt{4}, \\ 0, & \text{otherwise.} \end{cases}$$

In particular a word admissible modulo 3 carries as many 2*'s as* 4*'s, and exactly $2^\ell - 1$ of the 3^ℓ words of length ℓ survive this single prime.*

Proof. Since $7 \equiv 1$ and $\mathtt{2}, \mathtt{4}, \mathtt{6} \equiv 2, 1, 0 \pmod 3$, the u-walk modulo 3 is $r_{n+1} \equiv r_n + u_n$, and admissibility means $r_n \in \{1, 2\}$ throughout. The letter 6 fixes the state. The letter 4 sends $1 \mapsto 2$ and $2 \mapsto 0$, so it is legal only at state 1; the letter 2 sends $2 \mapsto 1$ and $1 \mapsto 0$, so it is legal only at state 2. Hence after a 4 the state is 2, and stays 2 across any run of 6's, so the next letter other than 6 must be a 2; symmetrically the next non-6 letter after a 2 must be a 4. Read cyclically the two alternate, and therefore occur equally often. Conversely, for an alternating word the starting state is forced by the first non-6 letter, the walk then never leaves $\{1, 2\}$, and it returns after one period because the letters sum to 0 modulo 3; for the constant word both states serve. Counting: the constant word, together with $2\binom{\ell}{2k}$ words for each placement of $2k > 0$ non-6 letters, gives $1 + 2\big(2^{\ell-1} - 1\big) = 2^\ell - 1$. □

All five words of Proposition B.4 below obey the alternation, the longest visibly so: the non-6 letters of 24242664624662466 read 2, 4, 2, 4, 2, 4, 2, 4, 2, 4.

B.2. **The classification.**

Proposition B.4 (computational)**.** *Put*

$$\mathcal{U} = \{\, \mathtt{6},\ \mathtt{24},\ \mathtt{2466},\ \mathtt{26646},\ \mathtt{24242664624662466} \,\}.$$

A residue lies on a cycle of $\Gamma_7(M_{31})$ if and only if it is u-admissible modulo M_{31} for some cyclic rotation u of some member of $\mathcal{U}$. Equivalently, the set K of Section 6.2 is

$$K \;=\; \bigcup_{u\in\mathcal{U}} \bigcup_{i<|u|} S_{M_{31}}(\sigma^i u), \qquad \sigma = \textit{cyclic shift},$$

and each of the five words is the minimal period of the digit word of the cycles it produces.

The five words account for the 849 cycles as follows, where the third column is the product $\prod_{q\le 31} |S_q(u)|$ over the eleven primes and the number of states is $|u|$ times that product, one factor per rotation.

u	$\lvert u\rvert$	$\prod_q \lvert S_q(u)\rvert$	states	cycles	cycle lengths
6	1	11 264	11 264	176	1, 3, 7, 15, 21, 105
24	2	32 760	65 520	186	4, 12, 28, 44, 84, 132, 308, 924
2466	4	68 040	272 160	378	60, 240, 420, 1680
26646	5	3 360	16 800	108	35, 70, 105, 210
24242664624662466	17	1	17	1	17
			365 761	849	

As a checksum for an independent implementation, the eleven factors for $u = \mathtt{6}$, at the primes $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31$ in order, are

$$1,\ 2,\ 1,\ 1,\ 1,\ 1,\ 1,\ 16,\ 1,\ 22,\ 16.$$

The last row of the table is a single cycle: every $|S_q|$ equals 1, so the Chinese remainder theorem pins down one residue, and its 17 states are the only cycle of $\Gamma_7(M_{31})$ whose digit word is not a proper power.

The first row needs no checksum at all, being the second factor available in closed form.

Lemma B.5. *For every prime $q \neq 7$,*

$$|S_q(\mathtt{6})| \;=\; q - \operatorname{ord}_q(7),$$

where $\operatorname{ord}_q(7)$ *is the multiplicative order of* 7 *modulo q, while $|S_7(\mathtt{6})| = 1$. Consequently $S_m(\mathtt{6}) \neq \emptyset$ for every squarefree m: at* every *modulus the graph $\Gamma_7(m)$ carries a cycle whose digit word is constant.*

Proof. Substituting $s = r+1$ turns $r \mapsto 7r+6$ into $s \mapsto 7s$, so $r_n = 7^n(x+1)-1$. Let $q \neq 7$. Multiplication by 7 is then a bijection of $\mathbb{Z}/q\mathbb{Z}$, so every orbit is periodic and $S_q(\mathtt{6})$ is exactly the set of x whose orbit avoids 0. Now $r_n \equiv 0$ for some $n \ge 0$ if and only if $x+1 \in \{7^{-n} : n \ge 0\} = \langle 7\rangle$, the cyclic subgroup generated by 7 in $(\mathbb{Z}/q\mathbb{Z})^\times$, which has $\operatorname{ord}_q(7)$ elements; so precisely $\operatorname{ord}_q(7)$ residues are excluded. Since $\operatorname{ord}_q(7) \le q-1$ the complement is nonempty, and it always contains the fixed point $x = -1$. For $q = 7$ the walk satisfies

$r_{n+1} \equiv 6$, so $x = 6$ is the only periodic residue, and it is nonzero. The final assertion now follows from Lemma B.2. □

The eleven factors displayed above are thus $q - \mathrm{ord}_q(7)$ at $q = 2, 3, 5, 11, 13, 17, 19, 23, 29, 31$ — the orders being $1, 1, 4, 10, 12, 16, 3, 22, 7, 15$ — together with the exceptional 1 at $q = 7$; and $11\,264 = 2 \cdot 16 \cdot 22 \cdot 16$. Two consequences are worth recording. Lemma B.5 says that the peeling of Section 5 can never terminate with an empty core, at any $\mathcal{P}$ whatsoever, which is the expected behaviour for base 7 in view of [DubOst06, Conjecture 3] and is the reason the present method aims at zero entropy rather than at an unavoidable set (Remark 7.5). And since $x_{n+1} = 7x_n + 6$ gives $x_n = 7^n(x_0 + 1) - 1$ outright, these cycles are the non-terminating base-7 representations of terminating rationals and are the floor expansion of no ξ at all; the genuine content of the table is its remaining four rows.

B.3. **Verification, and what this does not do.** Proposition B.4 was checked by regenerating $\bigcup_{u,i} S_{M_{31}}(\sigma^i u)$ from the five words through Lemma B.2 and comparing it with the shipped witness: the two sets are *identical*, not merely of equal size, both against `core_y31_cycles.txt`, whose SHA-256 is

`1de51f37c91da0993128724d37f3852797fd69a7a0220808f170cf4a104ab29c`,

and against the array `cyclesData` of `DubC/Y31Data.lean` that the Lean development actually decodes. The regenerated set was also verified to be a disjoint union of cycles on its own terms, without reference to either file: every one of its residues is coprime to M_{31} and has *exactly* one successor and exactly one predecessor inside the set, which decomposes it into the 849 cycles of the table.

Lemma B.3 moreover makes the classification checkable by brute force over the words themselves, with no witness of any kind. Only $2^\ell - 1$ of the 3^ℓ words of length ℓ pass the prime 3, so an exhaustive sweep of all cyclic words of length at most 26 — some 1.3×10^8 words, each tested against the eleven primes through Lemma B.2 — costs minutes. It returns precisely the rotations of the powers of the five members of $\mathcal{U}$, and nothing else: no sixth pattern of period at most 26 exists. It is only the absence of patterns of larger period that Proposition B.4 still takes from the shipped witness.

Remark B.6. Three consequences, and one caution.

(i) The genuine cycles are the four non-constant words. The word `6` produces exactly the 176 all-6 cycles discussed in Section 8, carrying 11 264 states; the remaining $186+378+108+1 = 673$ cycles, with 354 497 states, are the ones that are floor expansions of genuine periodic ξ. The split recorded there is thus the split between the constant word and the other four.

(ii) The witness need not be transmitted. Regeneration costs eleven walks of at most 527 steps per rotation followed by a Chinese remainder pass, so

a referee can rebuild the certificate from the displayed $\mathcal{U}$ and check Theorem 6.2 directly, with no downloaded artifact and no search. This is what makes the $y = 31$ check replicable in minutes.

(iii) It would shrink the quarantine, not remove it. Defining K by $\mathcal{U}$ rather than by a 365 761-element array turns membership into a local computation, which may put Theorem 6.2 within reach of the kernel and retire the evaluation N_2 of Appendix A.1. It does nothing for N_1, the ladder, which is the expensive one and whose witness is the peeling rank over 2.2×10^7 candidates rather than the cycle set. The trusted base of Theorems A and B is therefore unchanged by this appendix.

Caution. Proposition B.4 is a measurement of the witness, in the same status as the cardinalities of Section 6.5: it has been verified by computation and against an independent decoding, but it is not a Lean theorem and no statement of this paper depends on it. In particular it is *not* used to prove Theorems 6.3 or 6.2, which quantify over the arrays as shipped.

Appendix C. Other bases

Appendix B used the value 7 only through arithmetic: Lemma B.2 is base-free and the proof of Lemma B.5 merely substitutes $s = r + 1$. We record here what the same reading gives for other bases, and close with the numbers for $b = 10$, the base left open in [DubOst06].

C.1. **The reduced alphabet.** Two kinds of prime occur in $\mathcal{P}$. If $p \mid b$ then $br + d \equiv d \pmod p$, so the p-coordinate of the state is the last digit and carries no memory; all that p contributes is the requirement $p \nmid d$. When b is odd the prime $p = 2$ behaves the same way: a unit is odd and br is odd, so d must be even and the 2-coordinate is constantly 1. Every other $p \in \mathcal{P}$ carries a genuine state. Setting

$$A_b = \big\{\, d < b \;:\; \gcd(d, \operatorname{rad} b) = 1, \text{ and } d \text{ even when } b \text{ is odd} \,\big\},$$

the alphabet is A_b once and for all, and $\Gamma_b(M)$ may be read on the remaining coordinates alone. For $b = 7$ this is the passage from $\{0, \dots, 6\}$ to $\{2, 4, 6\}$ used throughout.

Lemma C.1. *Let q be prime and let S_q be formed with b in place of 7 in Definition B.1. Then $|S_q(\mathtt{b{-}1})| = q - \operatorname{ord}_q(b)$ for $q \nmid b$, and $|S_q(\mathtt{b{-}1})| = 1$ for $q \mid b$. In particular the constant word $\mathtt{b{-}1}$ is admissible modulo every squarefree m, in every base.*

Proof. Verbatim that of Lemma B.5: the substitution $s = r + 1$ turns $r \mapsto br + (b - 1)$ into $s \mapsto bs$, the excluded residues are the coset $\langle b \rangle - 1$, and $\operatorname{ord}_q(b) \le q - 1$. For $q \mid b$ one has $r_{n+1} \equiv b - 1 \equiv -1$, which is a nonzero fixed value. □

Hence no base is settled by emptiness of the core: every base must, like base 7, tolerate surviving cycles, which is why Section 1.3 aims at zero entropy rather than at an unavoidable set.

C.2. **One prime is often enough.** For $b \leq 6$ the alphabet is already so small that a single prime decides the matter — it suffices that every strongly connected component of $\Gamma_b(q \cdot \operatorname{rad} b)$, a digraph on fewer than q vertices, be a simple cycle. The test reproduces Proposition 4.10 including the moduli used there, and identifies base 7 as the first base for which it fails.

b	A_b	$\lvert A_b\rvert$	verdict
3	$\{2\}$	1	digit word forced constant; $C(\{2,3\})$
4	$\{1,3\}$	2	$q=3$ decides; $C(\{2,3\})$
5	$\{2,4\}$	2	$q=3$ decides; $C(\{2,3,5\})$, the collapse of [DN05]
6	$\{1,5\}$	2	$q=5$ decides; $C(\{2,3,5\})$
7	$\{2,4,6\}$	3	no single prime; certificate at $y=31$
8	$\{1,3,5,7\}$	4	no single prime
9	$\{2,4,8\}$	3	no single prime
10	$\{1,3,7,9\}$	4	no single prime
11	$\{2,4,6,8,10\}$	5	no single prime

What varies from base to base is the analogue of Lemma B.3, and it is decisive. In base 7 that lemma rules out the constant words `2` and `4`, since neither alternates, leaving a single constant-word family. In base 10 it rules out nothing.

Lemma C.2. *Every cycle of* $\Gamma_{10}(m)$ *with* $3 \mid m$ *has all of its digits in* $\{3,9\}$.

Proof. Here $A_{10} = \{1,3,7,9\}$, and modulo 3 one has $10 \equiv 1$ and $1,3,7,9 \equiv 1,0,1,0$, so the walk is $r_{n+1} \equiv r_n + d_n$ on $\{1,2\}$. A digit $\equiv 0$ fixes the state, while a digit $\equiv 1$ sends $1 \mapsto 2$ and $2 \mapsto 0$. The state is therefore non-decreasing along an admissible walk and increases strictly whenever a digit $\equiv 1 \pmod 3$ is read, so a closed walk reads none of them. □

Base 10 thus keeps *two* constant-word families where base 7 keeps one: the word `9`, with fixed point -1, and the word `3`, with fixed point $-1/3$; the substitution $s = r + \frac{1}{3}$ gives $\lvert S_q(\mathtt{3})\rvert = q - \operatorname{ord}_q(10)$ for $q \nmid 30$, so both are immortal in the sense of Lemma C.1. The two returning successors of 13 modulo 30 exhibited in Proposition 4.11 are representatives of exactly these two families, and any certificate for base 10 must place them in different strongly connected components.

C.3. **A caution: the cycles are not the certificate.** The sweep described after Proposition B.4 extends to any base and any modulus, at a cost governed by the period cutoff rather than by M; it is therefore available where the digraph itself is not. It does not, however, decide $C(\mathcal{P})$. Run over base 7 at successive moduli it returns, for primitive cycle words of period at most 24 counted with rotations,

$$234\ (y=17),\quad 77\ (y=19),\quad 77\ (y=23),\quad 29\ (y=29),\quad 29\ (y=31),$$

so the five words of $\mathcal{U}$ are already the entire cycle layer at $y = 29$, where the certificate fails. What separates $y = 31$ from $y = 29$ is not the set of cycles but the disappearance of the last component holding two of them —

a property of the transient paths, which a sweep over cycle words cannot see. The sweep gives a cheap one-sided test: a cycle layer still growing with the cutoff proves $C(\mathcal{P})$ false, and nothing more.

C.4. **Base ten.** With that caveat, the sweep of Lemma C.2 over words in $\{3, 9\}$ gives for base 10, again for primitive cycle words of period at most 24,

$$101\ (y = 31), \qquad 26\ (y = 37), \qquad 2\ (y = 41),$$

the two survivors being the constant words 3 and 9, which by the previous subsection survive at every modulus. The cycle layer of base 10 is thus already as small as it can ever become by $y = 41$, and the whole question is whether the branching between the two families eventually stops — the branching count growing across the first rungs, against exactly one branching component at every failing rung for base 7, both as recorded in Section 6.5.

Refining the heuristic $\bar{\lambda}$ of Section 6.5 to the reduced alphabet sharpens the estimate for where that happens. Let λ_q be the Perron root of the transfer matrix of Γ_b modulo q over A_b, and consider the point at which $|A_b| \prod_{q \le y} \lambda_q / |A_b|$ falls below 1. It does so at $y = 29$ for base 7 — one prime early, the certificate arriving at $y = 31$ — and at $y = 67$ for base 10. Calibrating by that one-prime lag puts the base-10 certificate, if it exists at all, near

$$\mathcal{P} = \{p \le 71\}, \qquad M = \prod_{p \le 71} p = 5.579\ldots \times 10^{26},$$

with $\prod_{q \le 71,\ q \nmid 10} (q - 1) = 1.783\ldots \times 10^{25}$ states after reduction, against 2.006×10^{11} and 5.109×10^{9} for base 7 at $y = 31$: larger by a factor near 3×10^{15} in both. The ladder of Section 5 is linear in the number of states, so this is not a matter of a longer run. It is the reason base 10 is stated here as out of reach rather than as merely unattempted.

References

[AG77] I. O. Angell, H. J. Godwin, *On truncatable primes*, Math. Comp. **31** (1977), 265–267.

[DN05] A. Dubickas, A. Novikas, *Integer parts of powers of rational numbers*, Math. Z. **251** (2005), 635–648.

[Dub09] A. Dubickas, *Prime and composite integers close to powers of a number*, Monatsh. Math. **158** (2009), 271–284.

[DubOst06] A. Dubickas, *Truncatable primes and unavoidable sets of divisors*, Acta Math. Univ. Ostrav. **14** (2006), 21–25.

[FS67] W. Forman, H. N. Shapiro, *An arithmetic property of certain rational powers*, Comm. Pure Appl. Math. **20** (1967), 561–573.

[Kok35] J. F. Koksma, *Ein mengentheoretischer Satz über die Gleichverteilung modulo Eins*, Compositio Math. **2** (1935), 250–258.

[MPP+24] S. J. Miller, F. Peng, T. Popescu, J. M. Siktar, N. Wattanawanichkul (the Polymath REU Walking to Infinity group), *Walking to infinity along some number theory sequences*, Integers **24** (2024), #A78.