SIERPIŃSKI AND RIESEL NUMBERS AMONG REPDIGITS, REPUNITS, REPINTEGERS AND REPSTRINGS: SIX IMPROVED BOUNDS AND TWO QUESTIONS ANSWERED

KOREA SUPERINTELLIGENCE LABS

Abstract. Bispels, Cohen, Harrington, Lowrance, Pontes, Schaumann and Wong asked, for each of eight repetitive shapes of integer, for the smallest base or the smallest repeating block that admits a Sierpiński or a Riesel number of that shape, and answered each of the eight questions only with an upper bound. We improve six of the eight bounds and settle the remaining two exactly. The improvements are $\beta_1 \le 53$, $\beta_2 \le 40$, $\beta_2' \le 39$ and $\beta_1' \le 94$ for the four base questions, against 147, 87, 180 and 16518444216571; and $\kappa \le 16519$, $\kappa' \le 16519$ for the two 2-repinteger block questions, against 18107. For the two 2-repstring questions we prove $\tilde{\kappa} = \tilde{\kappa}' = 1$: the block $k = 1$ already works, so those two questions are closed rather than improved, and the witnesses are Selfridge's and Riesel's own covering systems, reused without changing a single residue class. Three of the improvements are invisible to a search over covering systems whose period divides 144, where all the classical covering systems live; they need period 60, and we isolate the arithmetic reason. Every statement is proved from an explicit covering certificate and has been machine-checked in Lean 4.

1. Introduction

A *Sierpiński number* is an odd positive integer k such that $k \cdot 2^n + 1$ is composite for every $n \ge 1$; a *Riesel number* is an odd positive integer k such that $k \cdot 2^n - 1$ is composite for every $n \ge 1$. The oddness is part of the definition and not a normalisation: it is what stops the question from being trivial, and Section 8 records two searches that produced a valid proof of compositeness for a number that was nonetheless disqualified by it. The classical witnesses are Selfridge's 78557 and Riesel's 509203 [2], and both are proved by a *covering system*: a finite list of residue classes $r \pmod m$ covering $\mathbb{Z}$, each carrying a prime p with $p \mid 2^m - 1$ and $k \cdot 2^r \equiv \mp 1 \pmod p$, so that every $k \cdot 2^n \pm 1$ acquires the divisor p attached to whichever class contains n.

Bispels, Cohen, Harrington, Lowrance, Pontes, Schaumann and Wong [1] asked which Sierpiński and Riesel numbers are *repetitive*. Fix a base $b \ge 2$. A *b-repdigit* is a digit $1 \le k < b$ written t times in base b, that is $k(b^t - 1)/(b - 1)$; a *b-repunit* is the case $k = 1$; a *b-repinteger* repeats a whole block k of $\ell = \lfloor \log_b k \rfloor + 1$ base-b digits; and a *b-repstring* additionally inserts z zeroes between consecutive copies of the block. The paper [1] poses eight questions, each asking for the least base, or the least block, of a given shape that admits a Sierpiński or a Riesel number, and answers each of them only with an upper bound obtained from an explicit construction. We write $\beta_1, \beta_2, \kappa, \beta_1', \beta_2', \kappa'$ for the six quantities of [1, Questions 1.1–1.6] and $\tilde{\kappa}, \tilde{\kappa}'$ for the two of [1, Questions 4.1–4.2]; the precise definitions are recalled in Section 2, and they are listed here in the order in which [1] poses them.

Results. Every quantity below is bounded above by exhibiting one integer of the required shape together with a covering certificate for it. The table records what [1] proves and what is proved here.

	quantity	[1]	here	witness
β_1	least base with a repunit Sierpiński number	≤ 147	≤ 53	$1_{53}^{(29345)}$
β_2	least base with a repdigit Sierpiński number	≤ 87	≤ 40	$17_{40}^{(613)}$
κ	least 2-repinteger Sierpiński block	≤ 18107	≤ 16519	$16519_2^{(33713)}$
β_1'	least base with a repunit Riesel number	≤ 16518444216571	≤ 94	$1_{94}^{(77795)}$
β_2'	least base with a repdigit Riesel number	≤ 180	≤ 39	$29_{39}^{(6079)}$
κ'	least 2-repinteger Riesel block	≤ 18107	≤ 16519	$16519_2^{(111131)}$
$\tilde\kappa$	least 2-repstring Sierpiński block	≤ 659	$= 1$	$1_2^{(35;78557)}$
$\tilde\kappa'$	least 2-repstring Riesel block	≤ 659	$= 1$	$1_2^{(23;509203)}$

The last two lines are equalities, not improved bounds. The quantities are defined as least *positive* integers, so $\tilde\kappa \ge 1$ and $\tilde\kappa' \ge 1$ hold by definition, and a witness with block $k = 1$ closes both questions. The witness is not a new covering system: for every prime p with $\mathrm{ord}_p(2) \mid 36$ one has

$$1_2^{(35;t)} \;=\; \frac{2^{36t}-1}{2^{36}-1} \;=\; 1 + 2^{36} + 2^{72} + \cdots + 2^{36(t-1)} \;\equiv\; t \pmod p,$$

simultaneously at all seven primes $3, 5, 7, 13, 19, 37, 73$ of Selfridge's covering, so choosing $t = 78557$ makes the repstring inherit Selfridge's certificate unchanged. The Riesel side is the same computation with $\mathrm{ord}_p(2) \mid 24$, the six primes $3, 5, 7, 13, 17, 241$ of Riesel's covering, and $t = 509203$. This is Theorem 6.1.

Of the six improved bounds, three — $\beta_1' \le 94$, $\kappa \le 16519$ and $\kappa' \le 16519$ — cannot be reached by any covering system whose period divides 144. That is where all the classical covering systems for $k\cdot 2^n \pm 1$ live, and where the six explicit constructions of [1] live as well; its two remaining constructions use the dyadic period 64, which excludes modulus 5 just as firmly. The restriction is therefore easy to make without noticing. All three witnesses here need period 60 and, in particular, a residue class to a modulus divisible by 5; deleting that single class from any of the three certificates already leaves a residue uncovered (Proposition 8.4). Section 5 isolates the reason base 94 is the answer for β_1': a prime dividing $b-1$ makes a repunit congruent to its own *length* modulo that prime, so the corresponding entry of the certificate is free; and $94 - 1 = 93 = 3 \cdot 31$ with $\mathrm{ord}_3(2) = 2$ and $\mathrm{ord}_{31}(2) = 5$ frees exactly the moduli 2 and 5. Modulus 5 is precisely what $L \mid 144$ forbids.

The improvement to β_1' is by ten orders of magnitude, and that is not an accident of the search. The bound $\beta_1' \le 16518444216571$ of [1] is an artefact of its construction rather than an estimate: the construction requires $b \equiv 16518444216571 \pmod{18446744073709551615}$, so the smallest base it can possibly produce is already astronomical. For the same reason two of the eight bounds of [1], namely $\beta_1 \le 147$ and $\beta_1' \le 16518444216571$, cannot be checked by exhibiting their witnesses: in each case the construction pins the repetition count to a residue modulo a large least common multiple, and the smallest witness it can produce has more than 10^{10} decimal digits in the first case and more than 10^{19} in the second. Both are superseded here, so nothing depends on them. The other six bounds of [1] are reproduced in Section 9.

What is not proved. None of the eight questions is settled from below. Sections 4 and 5 exhibit witnesses; Section 7 records exactly how far the two searches that found them reached, and that record is a statement about covering certificates inside a finite box, not a lower bound on any of $\beta_1, \beta_2, \kappa, \beta_1', \beta_2', \kappa'$. Those six questions remain open. One limit is genuine and period-independent: no covering certificate of the kind used here can ever witness a 2-repdigit Sierpiński number, which is [1, Theorem 3.2] and is Proposition 8.5 below. Whether 2-repdigit — that is, Mersenne — Sierpiński numbers exist is open, and [1] ties it to Erdős' conjecture that the least prime factor of $k \cdot 2^n + 1$ stays bounded.

Machine-checking covering certificates for Sierpiński and Riesel numbers is itself not new: Cowles and Gamboa [4] verified in ACL2, fifteen years ago, that every integer of the given form has a non-trivial factor supplied by a given cover. Nothing is claimed here about the mechanism; what is offered is the targets and the numbers. Likewise, the primes $31, 11, 151, 41, 331, 1321$ used by the

period-60 certificates, whose multiplicative orders $\mathrm{ord}_p(2)$ are $5, 10, 15, 20, 30, 60$, are standard in the Brier-number literature [6]; what is new is their use on a repunit and on a repinteger multiplier.

2. Preliminaries

Throughout, $b \geq 2$ is the base, p a modulus, and all congruences are between non-negative integers. We call x *composite* if it has a divisor d with $1 < d < x$; this is the form in which compositeness is proved below, and it is worth noting that it never requires knowing that d is prime.

Definition 2.1. An odd positive integer k is a *Sierpiński number* if $k \cdot 2^n + 1$ is composite for every $n \geq 1$, and a *Riesel number* if $k \cdot 2^n - 1$ is composite for every $n \geq 1$.

Write

$$S_b(t) \;=\; \sum_{i=0}^{t-1} b^i \;=\; \frac{b^t - 1}{b - 1},$$

the base-b string of t ones. We use the identity $S_b(t)\,(b-1) + 1 = b^t$, which avoids division, and the two recursions $S_b(t+1) = S_b(t) + b^t = 1 + b\,S_b(t)$.

Definition 2.2 ([1])**.** Let $b \geq 2$ and $t \geq 1$.

(1) For $1 \leq k < b$, the *b-repdigit* $k_b^{(t)} = k\,S_b(t) = k(b^t - 1)/(b - 1)$ is the digit k repeated t times in base b. For $k = 1$ we call $1_b^{(t)} = S_b(t)$ the *b-repunit* of length t.

(2) For any $k \geq 1$, put $\ell = \lfloor \log_b k \rfloor + 1$, the number of base-$b$ digits of k. The *b-repinteger* is $k_b^{(t)} = k\,(b^{\ell t} - 1)/(b^\ell - 1) = k\,S_{b^\ell}(t)$, the block k repeated t times.

(3) For $z \geq 0$, the *b-repstring* is $k_b^{(z;t)} = k\,(b^{(z+\ell)t} - 1)/(b^{z+\ell} - 1) = k\,S_{b^{z+\ell}}(t)$: the block k repeated t times with z zeroes inserted between consecutive copies. For instance $1001001 = 1_{10}^{(2;3)}$, with $b = 10$, $k = 1$, $t = 3$, $z = 2$, $\ell = 1$.

For $k < b$ one has $\ell = 1$, so the repinteger of (2) is the repdigit of (1) and the two notations agree; and (3) reduces to (2) at $z = 0$. Every shape in Definition 2.2 is therefore a repdigit in a suitable base: a b-repinteger with block of ℓ digits is a b^ℓ-repdigit, and a b-repstring with z zeroes is a $b^{z+\ell}$-repdigit. All the certificates below are stated for the repdigit shape $k\,S_B(t)$ and applied with $B = b^{z+\ell}$.

Definition 2.3 (the eight quantities of [1])**.** β_1 (resp. β_1') is the least $b \geq 2$ for which some b-repunit is a Sierpiński (resp. Riesel) number; β_2 (resp. β_2') the least $b \geq 2$ for which some b-repdigit is a Sierpiński (resp. Riesel) number; κ (resp. κ') the least $k \geq 1$ for which some 2-repinteger $k_2^{(t)}$ is a Sierpiński (resp. Riesel) number; and $\tilde{\kappa}$ (resp. $\tilde{\kappa}'$) the least $k \geq 1$ for which some 2-repstring $k_2^{(z;t)}$, $z \geq 0$, is a Sierpiński (resp. Riesel) number.

Each of the eight sets is non-empty by [1], so each least element exists. We record the two parity facts that decide the oddness half of the definition, since they are what a search must respect.

Lemma 2.4. *Let $t \geq 1$. If b is even then $S_b(t)$ is odd. If b is odd then $S_b(t) \equiv t \pmod 2$.*

Proof. Both follow from $S_b(t+1) = 1 + b\,S_b(t)$ by induction: for even b the right-hand side is 1 modulo 2, and for odd b it is $1 + S_b(t)$. □

Consequently $k\,S_b(t)$ is odd exactly when k is odd and either b is even, or b is odd and t is odd. All the improved witnesses below fall on the easy side of this: the bases 40, 248, 94, 2^{15}, 2^{24} and 2^{36} are even, so oddness is free, and the two odd-base witnesses $1_{53}^{(29345)}$ and $29_{39}^{(6079)}$ have odd length.

3. Covering certificates

The whole paper rests on one finite, checkable object. Its shape is dictated by the size of the witnesses: the largest is a 3.6 million digit integer, and no step of the verification may evaluate it.

Definition 3.1. An *entry* is a quadruple $e = (r, m, p, d)$ of non-negative integers. Let L, b, k, t be positive integers and $\varepsilon \in \{+1, -1\}$. A finite list C of entries is a *certificate* for $(L, b, k, t, \varepsilon)$ if $t \geq 21$, and

(1) every $e = (r, m, p, d) \in C$ satisfies $0 < m$, $0 \leq r < m$, $m \mid L$, $1 < p < 2^{20}$, $0 < d$, and

$$2^m \equiv 1 \pmod{p}, \qquad p \mid b \text{ or } b^d \equiv 1 \pmod{p}, \qquad k\, S_b(t)\, 2^r \equiv -\varepsilon \pmod{p};$$

(2) the classes cover $\mathbb{Z}/L\mathbb{Z}$: for every $n \in \{0, 1, \ldots, L-1\}$ there is $e = (r, m, p, d) \in C$ with $n \equiv r \pmod{m}$.

Three features of Definition 3.1 deserve comment, because each of them is what makes the check both cheap and unconditional.

No modular inverses. The usual way to write the third condition of (1) is $k \equiv -\varepsilon\, 2^{-r} \pmod{p}$. Written as a divisibility of $k\, S_b(t)\, 2^r + \varepsilon$ it stays inside the non-negative integers, and no inverse has to be computed or justified.

The moduli are never proved prime. Definition 3.1 asks only $1 < p < 2^{20}$. Compositeness needs a divisor strictly between 1 and the number, and nothing more. Dropping primality removes the only step that would have needed either a primality certificate or a trusted external computation. It is not a restriction either, as Proposition 5.3 shows.

The witness is never evaluated. The residue $S_b(t) \bmod p$ is computed from t only through $\lfloor t/d \rfloor$ and $t \bmod d$, by the following reduction; the field d of an entry is what carries it.

Lemma 3.2 (block reduction)**.** *Let b, d, p, t be positive integers with $b^d \equiv 1 \pmod{p}$. Then*

$$S_b(t) \;\equiv\; \left\lfloor \frac{t}{d} \right\rfloor S_b(d) \;+\; S_b(t \bmod d) \pmod{p}.$$

If instead $p \mid b$, then $S_b(t) \equiv 1 \pmod{p}$ for every $t \geq 1$.

Proof. Two identities, both immediate by induction on the second argument: $S_b(u+v) = S_b(u) + b^u S_b(v)$ and $S_b(dq) = S_{b^d}(q)\, S_b(d)$. Write $t = dq + s$ with $q = \lfloor t/d \rfloor$ and $s = t \bmod d$. Then $S_b(t) = S_{b^d}(q) S_b(d) + b^{dq} S_b(s)$. Since $b^d \equiv 1 \pmod{p}$ we have $S_{b^d}(q) \equiv S_1(q) = q$ and $b^{dq} \equiv 1$, which is the displayed congruence. For the last claim, $S_b(t) = 1 + b\, S_b(t-1) \equiv 1 \pmod{p}$ when $p \mid b$. □

The largest d occurring in any certificate in this paper is 264, so every residue in Definition 3.1 is obtained in at most a few hundred steps of arithmetic on integers below 2^{20}, whatever the size of the witness.

Theorem 3.3 (soundness; [1, Equations (2) and (3)])**.** *Let $b \geq 2$, $k \geq 1$, and put $N = k\, S_b(t)$. If C is a certificate for $(L, b, k, t, +1)$ then $N \cdot 2^n + 1$ is composite for every $n \geq 0$. If C is a certificate for $(L, b, k, t, -1)$ then $N \cdot 2^n - 1$ is composite for every $n \geq 1$.*

Proof. Fix n and reduce it modulo L; by (2) of Definition 3.1 there is an entry $e = (r, m, p, d)$ with $n \equiv r \pmod{m}$, because $m \mid L$. Write $n = mj + r'$ with $r' \equiv r$; since $2^m \equiv 1 \pmod{p}$ we get $2^n \equiv 2^r \pmod{p}$. Combining with $N \cdot 2^r \equiv -\varepsilon \pmod{p}$ gives $N \cdot 2^n \equiv -\varepsilon$, i.e. $p \mid N \cdot 2^n + \varepsilon$.

It remains to see that this divisor is proper. From $t \geq 21$ and $b \geq 2$,

$$p \;<\; 2^{20} \;\leq\; 2^{\,t-1} \;\leq\; b^{\,t-1} \;\leq\; S_b(t) \;\leq\; N,$$

the third inequality because b^{t-1} is one of the summands of $S_b(t)$. For $\varepsilon = +1$ this gives $1 < p < N \leq N \cdot 2^n < N \cdot 2^n + 1$. For $\varepsilon = -1$ and $n \geq 1$ we have $N \cdot 2^n - 1 \geq 2N - 1 > N > p$. In both cases p is a divisor strictly between 1 and the number, which is composite. □

Theorem 3.3 is the source's Equations (2) and (3) — the Sierpiński and the Riesel implication — with the divisor-properness made explicit; the clauses $t \geq 21$ and $p < 2^{20}$ of Definition 3.1 exist only to supply the displayed chain of inequalities, and they cost nothing, since every witness below has t in the thousands.

4. Six improved bounds

We now exhibit the witnesses. In each table the entries (r, m, p) of the certificate are listed with the period L; the fourth field d of Definition 3.1, which only controls the cost of the reduction in Lemma 3.2, is omitted.

Theorem 4.1. *The following four integers are Sierpiński or Riesel numbers as indicated, and hence* $\beta_1 \le 53$, $\beta_2 \le 40$, $\beta_1' \le 248$ *and* $\beta_2' \le 39$.

witness	*type*	*digits*	*bound improved*
$1_{53}^{(29345)}$	*Sierpiński*	50,598	$\beta_1 \le 53$, *from* 147
$17_{40}^{(613)}$	*Sierpiński*	982	$\beta_2 \le 40$, *from* 87
$1_{248}^{(11315)}$	*Riesel*	27,091	$\beta_1' \le 248$, *from* 16518444216571
$29_{39}^{(6079)}$	*Riesel*	9,672	$\beta_2' \le 39$, *from* 180

Proof. Each is Theorem 3.3 applied to the certificate below, together with Lemma 2.4 for oddness: bases 40 and 248 are even, and the odd-base witnesses have odd lengths 29345 and 6079 with odd digits 1 and 29. Each certificate is a list of entries (r, m, p); the verification of the conditions of Definition 3.1 is a finite computation, described in Section 10.

witness	L	entries (r, m, p)
$1_{53}^{(29345)}$	48	$(1,2,3)$, $(2,3,7)$, $(2,4,5)$, $(4,8,17)$, $(4,12,13)$, $(0,16,257)$, $(24,48,673)$
$17_{40}^{(613)}$	36	$(0,2,3)$, $(1,3,7)$, $(1,4,5)$, $(5,9,73)$, $(3,12,13)$, $(17,18,19)$, $(11,36,37)$
$1_{248}^{(11315)}$	36	$(0,2,3)$, $(2,3,7)$, $(1,4,5)$, $(7,9,73)$, $(3,12,13)$, $(1,18,19)$, $(31,36,109)$
$29_{39}^{(6079)}$	72	$(1,2,3)$, $(0,3,7)$, $(2,4,5)$, $(0,8,17)$, $(7,9,73)$, $(8,12,13)$, $(10,18,19)$, $(4,72,433)$

In each row the moduli listed divide L and their classes cover $\mathbb{Z}/L\mathbb{Z}$; the reader can check the covering by hand from the table, and the congruences by the reduction of Lemma 3.2. □

Remark 4.2. The improvement $\beta_1 \le 53$ is not the construction of [1] pushed further. The bound $\beta_1 \le 147$ there comes from the dyadic covering $\{2^{j-1} \bmod 2^j : 1 \le j \le 6\} \cup \{0 \bmod 2^6\}$ with the Fermat primes $3, 5, 17, 257, 65537, 6700417$ and $q = 641$, whereas the certificate above uses the moduli $2, 3, 4, 8, 12, 16, 48$ with the primes $3, 7, 5, 17, 13, 257, 673$. It is a different covering system, not the same one better searched, and it should not be described otherwise.

5. Beyond period 144

The certificates of Theorem 4.1 have periods 36, 48 and 72, all dividing 144. So do the classical coverings for 78557 and 509203, and so do the six explicit coverings of [1], all of period 24; the two remaining constructions of [1] run on the dyadic period 64, which has no modulus divisible by 5 either. This section records what happens when that restriction is dropped: three of the six bounds move again, and all three moved witnesses need a modulus divisible by 5.

Theorem 5.1. *The base-*94 *repunit of length* 77795*, an integer of* 153,498 *decimal digits, is a Riesel number. Hence* $\beta_1' \le 94$.

Proof. Apply Theorem 3.3 with $\varepsilon = -1$ to the certificate of period $L = 60$

r	1	2	0	1	8	10	9	2	30
m	2	3	4	5	10	12	15	20	60
p	3	7	5	31	11	13	151	41	1321

Every modulus divides 60; each prime satisfies $p \mid 2^m - 1$ ($\mathrm{ord}_3(2) = 2$, $\mathrm{ord}_7(2) = 3$, $\mathrm{ord}_5(2) = 4$, $\mathrm{ord}_{31}(2) = 5$, $\mathrm{ord}_{11}(2) = 10$, $\mathrm{ord}_{13}(2) = 12$, $\mathrm{ord}_{151}(2) = 15$, $\mathrm{ord}_{41}(2) = 20$, $\mathrm{ord}_{1321}(2) = 60$); the nine classes cover $\mathbb{Z}/60\mathbb{Z}$; and the nine congruences $S_{94}(77795)\, 2^r \equiv 1 \pmod p$ hold. Oddness is free: the base 94 is even, so Lemma 2.4 makes the repunit odd. □

The same certificate validates every length in the arithmetic progression it pins, of which 77795 is the least; the next member is $t = 282395$, and the base-94 repunit of that length is a Riesel number by the same argument. This is how [1] states its own results, as congruence conditions rather than single integers.

Theorem 5.2. *The block* 16519 *— a prime with* 15 *binary digits — gives a* 2*-repinteger Sierpiński number* $16519_2^{(33713)}$ *of* 152,230 *decimal digits and a* 2*-repinteger Riesel number* $16519_2^{(111131)}$ *of* 501,807 *decimal digits. Hence* $\kappa \le 16519$ *and* $\kappa' \le 16519$*.*

Proof. Since 16519 has $\ell = 15$ binary digits, $16519_2^{(t)} = 16519 \cdot S_{2^{15}}(t)$ is a repdigit in base $B = 32768$, and B is even, so the number is odd for every $t \ge 1$ by Lemma 2.4. Apply Theorem 3.3 to the two certificates of period $L = 60$, with $\varepsilon = +1$, $t = 33713$ for the first and $\varepsilon = -1$, $t = 111131$ for the second:

r	1	0	0	4	2	10	11	18	20
m	2	3	4	5	10	12	15	20	30
p	3	7	5	31	11	13	151	41	331

r	0	0	3	1	7	1	14	13	5
m	2	3	4	5	10	12	15	20	30
p	3	7	5	31	11	13	151	41	331

The moduli and primes are the same on both sides; only the residues differ. Both sets of classes cover $\mathbb{Z}/60\mathbb{Z}$. Every period $\mathrm{ord}_p(2^{15})$ occurring here is at most 4, so the reduction of Lemma 3.2 is particularly short. □

Theorem 5.2 corrects a natural but false expectation. A search over covering systems of period dividing 144 finds no 2-repinteger block below 18107 on either side, which invites the conclusion that the bound of [1] is already the best the covering method can do. It is not: the obstruction is the box, not the method, and every one of the five moduli $5, 10, 15, 20, 30$ that the block 16519 needs is invisible to a search restricted to $L \mid 144$.

The next proposition explains why a period-60 covering is available for base 94 at all, and disposes of a natural worry about Definition 3.1, namely that its moduli p are not required to be prime.

Proposition 5.3. (1) *If* $b \equiv 1 \pmod p$ *then* $S_b(t) \equiv t \pmod p$ *for every* t*. In particular, since* $94 - 1 = 93 = 3 \cdot 31$*, one has* $S_{94}(t) \equiv t \pmod 3$ *and* $S_{94}(t) \equiv t \pmod{31}$*, and* $\mathrm{ord}_3(2) = 2$*,* $\mathrm{ord}_{31}(2) = 5$*.*

(2) *Certificates compose: if* C *is a certificate for* $(L, b, k, t, \varepsilon)$ *and* e *is an entry satisfying clause (1) of Definition 3.1, then* e *prepended to* C *is again a certificate for* $(L, b, k, t, \varepsilon)$*.*

(3) *If* $d \mid m$ *and* $n \equiv r \pmod m$*, then* $n \equiv r \pmod d$*. Consequently, if a certificate exists for* $(L, b, k, t, \varepsilon)$ *then one exists all of whose moduli* p *are prime.*

Proof. (1) is the case $b \equiv 1$ of the congruence $S_b(t) \equiv S_{b'}(t)$ for $b \equiv b'$, together with $S_1(t) = t$. (2) holds because clause (1) of Definition 3.1 is a condition on each entry separately and clause (2) is an existential over entries, so adding an entry preserves both. The congruence half of (3) is $n \bmod d = (n \bmod m) \bmod d$ when $d \mid m$. For the consequence, take an entry (r, m, p, d) with p composite and let q be a prime factor of p; then $q \le p < 2^{20}$, $2^m \equiv 1 \pmod q$ and $q \mid N2^r + \varepsilon$. Put $d' = \mathrm{ord}_q(2)$, so $d' \mid m$, and $r' = r \bmod d'$; then $2^{r'} \equiv 2^r \pmod q$, so (r', d', q) satisfies clause (1), and by the congruence half its class $r' \bmod d'$ *contains* the class $r \bmod m$. Replacing each entry this way preserves every congruence and does not shrink the cover. □

Part (1) is the mechanism behind base 94: a prime dividing $b-1$ makes the repunit equal to its own length modulo that prime, so the entry attached to that prime imposes no condition on the choice of t beyond a congruence that can always be met. For $b = 94$ both 3 and 31 divide $b-1$, and $\mathrm{ord}_3(2) = 2$, $\mathrm{ord}_{31}(2) = 5$, so the entries of moduli 2 and 5 are simultaneously free. Base 94 is the smallest base for which that happens. This is an explanation and not a proof: $b = 32$ and $b = 63$ also have $31 \mid b - 1$ and admit no covering at all. Part (3) says that restricting a search to prime moduli loses nothing, so the record of Section 7 is a statement about the covering method and not about a sub-case of it. It is not vacuous: the composite modulus $93 = 3 \cdot 31$, with $\mathrm{ord}_{93}(2) = 10$, does give a legal entry $(1, 10, 93)$

for the base-94 witness, and by part (3) its class 1 mod 10 merely refines the class 1 mod 2 that the certificate already carries.

6. The two repstring questions, answered

Theorem 6.1. *$\tilde{\kappa} = 1$ and $\tilde{\kappa}' = 1$. Witnesses are the 2-repstrings $1_2^{(35;78557)}$, of 851,318 decimal digits, which is a Sierpiński number, and $1_2^{(23;509203)}$, of 3,678,842 decimal digits, which is a Riesel number.*

Proof. Both quantities are defined as least *positive* integers, so $\tilde{\kappa} \geq 1$ and $\tilde{\kappa}' \geq 1$ hold by definition and it suffices to exhibit witnesses with block $k = 1$.

For $k = 1$ and $b = 2$ we have $\ell = \lfloor \log_2 1 \rfloor + 1 = 1$, so $1_2^{(z;t)} = S_{2^{z+1}}(t)$: the 2-repstring with block 1 and z zeroes is exactly the 2^{z+1}-repunit of length t. Its base is even, so it is odd by Lemma 2.4.

Take $z = 35$, so the base is 2^{36}. If p is any prime with $\mathrm{ord}_p(2) \mid 36$ then $2^{36} \equiv 1 \pmod{p}$, so by Proposition 5.3(1)

$$1_2^{(35;t)} = S_{2^{36}}(t) = 1 + 2^{36} + 2^{72} + \cdots + 2^{36(t-1)} \equiv t \pmod{p}.$$

The seven primes of Selfridge's covering for 78557 are $3, 5, 7, 13, 19, 37, 73$, and their orders $\mathrm{ord}_p(2)$ are $2, 4, 3, 12, 18, 36, 9$, all dividing 36; so with $t = 78557$ the repstring is congruent to 78557 modulo every one of them, simultaneously. Selfridge's covering data therefore applies unchanged: the certificate of period $L = 36$ with entries

$$(0, 2, 3),\ (1, 3, 7),\ (1, 4, 5),\ (3, 9, 73),\ (11, 12, 13),\ (15, 18, 19),\ (27, 36, 37)$$

and $\varepsilon = +1$ satisfies Definition 3.1 for $b = 2^{36}$, $k = 1$, $t = 78557$, and Theorem 3.3 gives the conclusion.

The Riesel side is identical, with $\mathrm{ord}_p(2) \mid 24$, the base 2^{24} (so $z = 23$), the six primes $3, 5, 7, 13, 17, 241$ of Riesel's covering for 509203, of orders $2, 4, 3, 12, 8, 24$, and $t = 509203$: the certificate of period $L = 24$ with entries

$$(0, 2, 3),\ (2, 3, 7),\ (1, 4, 5),\ (7, 8, 17),\ (7, 12, 13),\ (3, 24, 241)$$

and $\varepsilon = -1$. □

Two remarks are worth making about Theorem 6.1. First, no new covering system is constructed: the certificates are Selfridge's and Riesel's, unchanged, and the only new ingredient is the observation that a 2-repstring with block 1 and the right number of zeroes is congruent to its own repetition count modulo every prime of those coverings at once. Second, the mechanism generalises: for any k and any period L, if the base $B = 2^{z+\ell}$ satisfies $B \equiv 1 \pmod{p}$ at every prime of a covering for some known Sierpiński or Riesel number K, then choosing t with $kt \equiv K$ at all those primes transports the covering. [1] instead bounds both quantities by 659, in its Theorems 4.3 and 4.4, and tabulates nine blocks in its Table 1 — $659, 727, 1177, 1189, 1549, 1747$ with $z \geq 1$ and $18107, 26267, 32681$ with $z = 0$, the smallest of them being 659 — but it does not consider $k = 1$.

7. The extent of the search

The witnesses above were found by two exhaustive searches over covering certificates. What follows is a record of what those searches covered. It is not a lower bound on any of the eight quantities, and it is stated separately from the theorems for that reason.

The first search fixes a period L, takes the primes $p \leq 5000$ with $\mathrm{ord}_p(2) \mid L$, and sweeps the repetition count t over one full period of $S_b(t)$ modulo all pool primes at once. The relevant finiteness fact is that $S_b(t) \bmod p$ is periodic in t with period 1 if $p \mid b$, p if $b \equiv 1 \pmod{p}$, and $\mathrm{ord}_p(b)$ otherwise; so t need only run over one least common multiple of those periods, doubled to account for the parity of the witness, and the sweep is exhaustive rather than sampled. It was run for $L \in \{12, 24, 36, 48, 72\}$ over bases $2 \leq b \leq 300$ and for $L = 144$ over $2 \leq b \leq 60$, with no base skipped. Inside that box the minima attained are 40 for a repdigit Sierpiński base, 39 for a repdigit Riesel base and 53 for a repunit Sierpiński base, which are the values of Theorem 4.1.

The second search removes all three restrictions at once, and it is what produced Theorems 5.1 and 5.2. It rests on a change in the order of quantifiers. For fixed b, k and ε, and for each pool

prime p and each residue r, the required congruence $k\,S_b(t)\,2^r \equiv -\varepsilon \pmod p$ pins t to a single class modulo the period of $S_b(t) \bmod p$, or is impossible; and the modulus of the entry may always be taken to be exactly $\mathrm{ord}_p(2)$, since a larger multiple covers a smaller class at the same cost, and a prime cannot occur twice. A certificate is then a set of pairs (p, r) whose classes cover $\mathbb{Z}/L\mathbb{Z}$ and whose t-congruences are simultaneously solvable — which, by the Chinese remainder theorem in its general form, is equivalent to *pairwise* solvability, a test on 64-bit integers. The repetition count is therefore never constructed during the search, and no bound on it is imposed. The search covered 84 periods L between 12 and 3024, including every one carrying a factor of $5, 7, 11, 13, 23$ or 29; every prime $p < 2^{20}$ with $\mathrm{ord}_p(2) \mid L$, in pools of 4 to 51 primes; bases $2 \le b \le 250$ for repunits and $2 \le b \le 60$ for every digit $1 \le k < b$; 2-repinteger blocks of at most 15 binary digits, which is all that could beat 18107; certificates of at most 20 entries, and of at most 30 for $b \le 60$; and the oddness of the witness imposed as a congruence on t rather than as a filter applied afterwards. Every run completed its depth-first enumeration without truncation, so each absence of a witness is exhaustive inside the stated box. The minima found over all 84 periods are 40, 39, 53, 94 and 16519 — that is, the three bounds of Theorem 4.1 other than β_1' do not move anywhere in the enlarged space, and β_1', κ and κ' do.

Two checks make the second search believable independently of the first. Run inside the first search's box, it reproduces all four certificates of Theorem 4.1 entry for entry, including their repetition counts 29345, 613, 11315 and 6079 — two different algorithms landing on the same objects. And each witness it reports was reconstructed by the Chinese remainder theorem into an actual repetition count and re-verified on the exact integer, in ordinary large-integer arithmetic, outside the block reduction of Lemma 3.2 that the formal check uses.

What is *not* excluded, and this is the whole list: periods above 3072 or with a prime factor above 29; moduli $p \ge 2^{20}$, which Definition 3.1 cannot carry as it stands, since properness in Theorem 3.3 comes from $p < 2^{20} \le S_b(t)$ — although any such prime has $\mathrm{ord}_p(2) \ge 20$ and so contributes at most $1/20$ of the density a covering needs, enough to patch a gap but not to carry one; certificates longer than the depth bound, where nothing found here needs more than nine entries; bases above 250, and digits $k > 1$ for bases above 60, neither of which can affect the two repdigit questions, which need $b < 40$; and 2-repinteger blocks of more than 15 binary digits, which already exceed 18107. Above all, the whole record concerns covering certificates. A Sierpiński or Riesel repdigit proved by an algebraic factorisation, or by a partial cover completed by a Fermat-style argument, is untouched by any of it.

8. Negative controls

The certificates above are large enough that a reader is entitled to ask what would have caught an error. This section records the checks that were run for that purpose, in increasing order of interest. They are not new mathematics; they are what makes the rest usable.

Proposition 8.1. $1_{10}^{(2;3)} = 1001001$, $7_{10}^{(3)} = 777$ *and* $1_{10}^{(4)} = 1111$, *in accordance with Definition 2.2. Neither* 1 *nor* 3 *is a Sierpiński number and* 3 *is not a Riesel number, since* $1 \cdot 2 + 1 = 3$, $3 \cdot 2 + 1 = 7$ *and* $3 \cdot 2 - 1 = 5$ *are prime. No even number is a Sierpiński or a Riesel number.*

Proposition 8.2. *The certificate of* $17_{40}^{(613)}$ *is load-bearing in each of its parts. Deleting its entry* $(11, 36, 37)$ *leaves the class* $n \equiv 11 \pmod{36}$ *uncovered, and no other class, so the resulting list is not a certificate. The same list of entries is not a certificate for the neighbouring repetition count* $t = 614$, *nor for the neighbouring digit* $k = 19$, *nor for the opposite sign; in each of those three cases the covering is intact and it is the congruences that fail.*

The next proposition is the one that matters, and it is a warning rather than a lemma.

Proposition 8.3 (the oddness near-miss)**.** *Let* $N = 58_{103}^{(61)}$. *The following list of entries, with period* $L = 24$, *is a certificate for* $(24, 103, 58, 61, -1)$*:*

$$(0, 2, 3),\ (2, 3, 7),\ (1, 4, 5),\ (7, 8, 17),\ (7, 12, 13),\ (3, 24, 241).$$

So $N \cdot 2^n - 1$ is composite for every $n \geq 1$. Nevertheless N is even, hence not *a Riesel number, and nothing here bounds β_2'.*

Proof. The certificate satisfies Definition 3.1, and Theorem 3.3 gives the compositeness. For the parity, 103 is odd and 61 is odd, so $S_{103}(61)$ is odd by Lemma 2.4, and $N = 58\,S_{103}(61)$ is even. □

A search that drops the oddness requirement — which is not a side condition but part of the definition of a Sierpiński and a Riesel number — returns base 103 against the 180 of [1], a 43% improvement, in seconds. The covering machinery is entirely sound, the compositeness conclusion is entirely true, and the answer is entirely wrong. No amount of checking the certificate could have detected it: the failure is in the definition, and only carrying the definition through to the conclusion separates the two. The same thing happens again in the enlarged search space, which is the first part of the next proposition.

Proposition 8.4. (1) *For every odd base b and every even t, the repunit $S_b(t)$ is even. In particular there is a certificate for $(144, 171, 1, 147212, -1)$, so $1_{171}^{(147212)} \cdot 2^n - 1$ is composite for every $n \geq 1$; but $1_{171}^{(147212)}$ is even, so it is not a Riesel number and gives no bound on β_1', even though its period 144 was already inside the first search's box.*

(2) *Every one of the nine entries of the certificate of Theorem 5.1, and of the Sierpiński certificate of Theorem 5.2, covers a residue modulo 60 that no other entry of the same certificate covers. Deleting the modulus-5 entry from the first leaves $n \equiv 6$ uncovered, and from the second leaves $n \equiv 14$; deleting it from the Riesel certificate of Theorem 5.2 leaves $n \equiv 41$.*

(3) *Exactly five of the nine moduli of the certificate of Theorem 5.1 fail to divide 144, namely $5, 10, 15, 20, 60$; the four that survive the restriction, $(1, 2, 3)$, $(2, 3, 7)$, $(0, 4, 5)$, $(10, 12, 13)$, do not cover $\mathbb{Z}/60\mathbb{Z}$. The corresponding five for Theorem 5.2 are $5, 10, 15, 20, 30$.*

(4) *Neither certificate of Theorems 5.1 and 5.2 survives a change of one parameter: not a neighbouring repetition count, not the opposite sign, not the neighbouring base 95, and not the neighbouring block 16521.*

Part (3) is the precise sense in which the three bounds of Section 5 are bought by the new moduli and not by a better search of the old ones. We close with the one place the method provably cannot go.

Proposition 8.5 ([1, Theorem 3.2])**.** *There is no certificate for $(L, 2, 1, t, +1)$, for any L and any t. That is, no covering certificate of the kind of Definition 3.1 witnesses a 2-repdigit — equivalently, a Mersenne number $2^t - 1$ — as a Sierpiński number.*

Proof. A covering of $\mathbb{Z}/L\mathbb{Z}$ must in particular cover $n = 0$, and $0 \equiv r \pmod m$ with $0 \leq r < m$ forces $r = 0$. The congruence at that entry then reads $p \mid N + 1$ where $N = S_2(t) = 2^t - 1$, so $p \mid 2^t$ and p is a power of 2, hence even. But $2^m \equiv 1 \pmod p$ makes p odd, a contradiction. □

Proposition 8.5 is a statement about the method and not about Mersenne numbers; whether 2-repdigit Sierpiński numbers exist is open. It does not depend on the period L, so nothing in Section 5 opens that door. It is also the sharpest available control: it shows the machinery of Definition 3.1 is not vacuously strong, since there is a natural target it provably cannot reach.

9. The published witnesses, reproduced

Proposition 9.1. *The following six bounds of* [1] *hold, with the stated witnesses: $41_{87}^{(59)}$ is a Sierpiński number, so $\beta_2 \leq 87$; $101_{180}^{(171)}$ is a Riesel number, so $\beta_2' \leq 180$; $18107_2^{(25)}$ and $18107_2^{(31)}$ are respectively a Sierpiński and a Riesel 2-repinteger, so $\kappa \leq 18107$ and $\kappa' \leq 18107$; and $659_2^{(2;131)}$ and $659_2^{(2;2599)}$ are respectively a Sierpiński and a Riesel 2-repstring, so $\tilde{\kappa} \leq 659$ and $\tilde{\kappa}' \leq 659$.*

These six are the bounds of [1] for which a witness of manageable size exists; they were reproduced as a check on everything else in this paper, and the check is worth describing, because it is stronger than a recomputation. Rather than copying the covering triples printed in [1], each was re-derived from

the witness alone: compute $N \bmod p$, solve $2^r \equiv \mp N^{-1} \pmod p$ by a discrete logarithm inside the group generated by 2, and then verify that the classes so obtained cover $\mathbb{Z}/L\mathbb{Z}$. Every triple obtained this way agreed with the printed triple exactly. The same procedure independently reproduced three rows of the source's Table 1, all of them with $z = 0$: at $k = 18107$ the Sierpiński condition $t \equiv 25$ and the Riesel condition $t \equiv 31$, at $k = 26267$ the Sierpiński condition $t \equiv 9$, and at $k = 32681$ the Riesel condition $t \equiv 5$, every congruence being modulo 56.

The remaining two bounds of [1], $\beta_1 \le 147$ and $\beta_1' \le 16518444216571$, are cited here and not checked, for the reason given in Section 1: their smallest witnesses have more than 10^{10} decimal digits. Both are superseded by Theorems 4.1 and 5.1, so nothing in this paper depends on them.

10. Verification

Every statement in this paper has been machine-checked in Lean 4 [7] against Mathlib [8]: Definition 3.1 as a decidable predicate, Lemma 3.2 and Theorem 3.3 as proofs from the Mathlib development of modular arithmetic, and each individual certificate as a single evaluation of that predicate by the Lean kernel's own reduction. No certificate check uses compiled or native evaluation, and no witness is ever constructed as an integer: by Lemma 3.2 the repetition count enters each residue only through a quotient and a remainder by a period at most 264, so the entire verification of an integer with 3,678,842 decimal digits is a few hundred operations on integers below 2^{20}. The axiom closure of every statement above is the standard one — propositional extensionality, the axiom of choice, and the soundness of quotient types — and the certificate checks themselves use propositional extensionality alone. The formal development consists of four files, is free of unproved assumptions, and compiles in under a minute; repository reference to be added at submission.

References

[1] C. Bispels, M. Cohen, J. Harrington, J. Lowrance, K. Pontes, L. Schaumann and T. W. H. Wong, *On Sierpiński and Riesel repdigits and repintegers*, INTEGERS **26** (2026), #A12. DOI 10.5281/zenodo.18154168. Preprint: arXiv:2505.00778.

[2] H. Riesel, *Några stora primtal*, Elementa **39** (1956), 258–260. The Sierpiński number 78557 is conventionally attributed to J. Selfridge, reported to have found it in 1962 and never to have published it [1, Section 1]. Its covering system $\{3, 5, 7, 13, 19, 37, 73\}$ is not taken on authority here: it is checked in Theorem 6.1.

[3] A. S. Bang, *Taltheoretiske Undersøgelser*, Tidsskrift for Mathematik **5**(4) (1886), 70–80 and 130–137, the volume and page range as cited in [1, Reference 5]. Primitive prime divisors of $2^m - 1$; used here only to motivate the choice of certificate primes, and not needed for any proof, since primality is never established.

[4] J. Cowles and R. Gamboa, *Verifying Sierpiński and Riesel numbers in ACL2*, arXiv:1110.4671 (2011).

[5] A. Mian and S. Siddique, *Kernel-checked exclusions for the Erdős–Selfridge odd covering problem*, arXiv:2607.25628 (2026).

[6] C. Rivera, *Problem 49: Brier numbers*, The Prime Puzzles & Problems Connection, `primepuzzles.net/problems/prob_049.htm`, accessed August 2026.

[7] L. de Moura and S. Ullrich, *The Lean 4 theorem prover and programming language*, in: Automated Deduction — CADE-28, Lecture Notes in Computer Science, Springer, 2021.

[8] The mathlib Community, *The Lean mathematical library*, in: Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs (CPP 2020), ACM, 2020.