A parity certificate for a conjectured four-term progression-free digit family

DRAFT • 2 November 2026 • MathDB 356756
Prepared with AI assistance (Codex). No human authorship or affiliation is asserted. Independent review and root acceptance remain separate; this draft carries zero accepted campaign credit.

1. The source problem

Write $Z_m = Z/mZ$. A nonconstant four-term arithmetic progression is x, x+r, x+2r, x+3r with $r \neq 0$. Elsholtz, Klahn and Lipnik [1, Definition 2.1] define, for $D \subseteq Z_m$ and |D| dividing n,

$S(D,n) = \{v \in Z_m{}^n : \text{every } d \in D \text{ occurs exactly } n/|D| \text{ times in } v\}$.

These counts exhaust all n coordinates, so every coordinate is in D. They call D admissible for a progression length when S(D,n) avoids nonconstant progressions of that length in every permitted dimension. We use ℓ for the source's progression length, reserving k for $p = 4k+1$.

Source Theorem 2.2. Let m be an integer, $\ell \geq 5$ odd, and $P^-(m) \geq (\ell+2)/2$, where P^- is the least prime factor. If $\lfloor(\ell-1)m/(\ell+1)\rfloor+1$ divides n, then $D = \{0,\ldots,\lfloor(\ell-1)m/(\ell+1)\rfloor\}$ gives no ℓ-term progression in S(D,n).

Source Theorem 2.3. Let $\ell \geq 4$ be even, $m \equiv -1 \pmod{\ell}$, and $P^-(m) \geq \ell$. If $\lfloor(\ell-2)m/\ell\rfloor+2$ divides n, then $D = \{0,\ldots,\lfloor(\ell-2)m/\ell\rfloor\} \cup \{((\ell-1)m-1)/\ell\}$ gives no ℓ-term progression in S(D,n).

The first theorem excludes $\ell = 4$; at $\ell = 4$ the second requires $m \equiv 3 \pmod 4$. Neither reaches the following source assertion.

Source Conjecture 2.4 [1]. For every prime $p \geq 13$ with $p \equiv 1 \pmod 4$, and every n divisible by $(p+3)/2$, the set $D = \{0,\ldots,(p-1)/2\} \cup \{(p+3)/2\}$ gives no nonconstant four-term progression in S(D,n). Lipnik's thesis [7, Conjecture 4.6, p. 56] repeats this assertion.

We prove the exact admissibility of this family with a uniform integer potential. Primality is unnecessary. The contribution is the explicit treatment of wrapped coordinate progressions, rather than a record general lower bound. The local certificate and the equal-frequency bridge have been checked in Lean; the cardinality consequence and literature comparison below are ordinary mathematics.

mathdb:2611.00019v1 03 Nov 2026

2. Complete classification of wrapped coordinates

Theorem. Let $k \geq 3$ be an integer, $p = 4k+1$, $h = 2k+2$, and $D = \{0,\ldots,2k\} \cup \{h\}$, viewed in Z_p. For every $n \geq 0$ divisible by h, $S(D,n)$ contains no nonconstant four-term arithmetic progression. More generally, four vectors supported on D with the same digit histogram cannot form a nonconstant four-term progression. Their common digit multiplicities need not be equal to one another.

Local classification. Use the representatives $0 \leq a,b,c,d \leq h$ for a coordinate progression. Its second differences $q_1 = a-2b+c$ and $q_2 = b-2c+d$ are multiples of p. Since $|q_i| \leq 2h = p+3 < 2p$, each belongs to $\{-p,0,p\}$. We claim that either both vanish as integers, or the quadruple is

(h−3, 0, h, 3) or (3, h, 0, h−3). (2.1)

Case $q_1 = p$. We have $a+c = p+2b \leq 2h = p+3$, so $b \in \{0,1\}$. If $b = 1$, $a+c = 4k+3$. Two interval digits sum to at most 4k, one h and one interval digit to at most 4k+2, and two h's sum to 4k+4. Thus $b = 1$ is impossible. If $b = 0$, two interval digits cannot sum to p, and two h's do not sum to p. Exactly one is h, and the other is $p-h = h-3$.

For $(a,c) = (h,h-3)$, the fourth residue is $d \equiv 2c-b = p-3 \pmod p$. Its representative $p-3$ exceeds h because $p-3-h = 2k-4 > 0$ for $k \geq 3$. This orientation is impossible. For $(a,c) = (h-3,h)$, the fourth residue is $2h \equiv 3 \pmod p$, giving the first quadruple in (2.1).

Case $q_1 = -p$. The equality $2b = p+a+c$ rules out every $b \leq 2k$, since $2b \leq 4k < p$. Hence $b = h$ and $a+c = 3$. For $c = 0,1,2,3$ the respective representatives $d \equiv 2c-h \pmod p$ are $h-3$, $h-1$, $h+1$, $h+3$. Here $h-1$ is the omitted digit $2k+1$, and the last two exceed h. Only $c = 0$ survives, giving the second quadruple in (2.1).

Case $q_1 = 0$, $q_2 \neq 0$. Reverse the quadruple to (d,c,b,a). Its first second difference is q_2 and its second is q_1. The preceding ±p analysis forces the reversed quadruple to be one of (2.1). But for those quadruples the two second differences are (p,−p) and (−p,p), respectively. This contradicts $q_1 = 0$. Thus no further orientation or one-wrap case has been omitted.

This classification uses only congruences and bounded integer representatives. It does not divide by a residue or invoke primality.

mathdb:2611.00019v1 03 Nov 2026

3. The potential, summation and dual interpretation

Define $\varepsilon(t) = (-1)^t$, for integer t, and use the parity-corrected potential

$E(t) = 4t^2 - (3p-5)\varepsilon(t) = 4t^2 - (12k-2)\varepsilon(t)$. (3.1)

For a coordinate progression put $\Delta = E(a)+E(d)-E(b)-E(c)$. We show $\Delta \geq 0$, with equality exactly for a = b = c = d.

Ordinary case. If both integer second differences vanish, write (a,b,c,d) = (a,a+s,a+2s,a+3s), where s may be negative. Direct expansion gives

$a^2+(a+3s)^2-(a+s)^2-(a+2s)^2 = 4s^2$.

The terms a and c have the same parity, as do b and d. Consequently $\varepsilon(a)+\varepsilon(d)-\varepsilon(b)-\varepsilon(c) = 0$. The parity correction cancels, and $\Delta = 16s^2$. It is zero if and only if s = 0.

Exceptional case. In either quadruple (2.1), the outer terms h−3 and 3 are odd, while the inner terms 0 and h are even. Thus the parity difference is −4. The square difference is $(h-3)^2+9-h^2 = 18-6h = 9-3p$. It follows that

$\Delta = 4(9-3p) + 4(3p-5) = 16 > 0$. (3.2)

Summation. Let A,B,C,F be four vectors with the same histogram on D and satisfying the two coordinatewise progression equations in Z_p. For any such vector v, its total potential is $\Sigma_t\, m_t E(t)$, where m_t is the number of coordinates equal to t. Hence all four potential totals coincide. The sum over coordinates of their local gaps is zero. Each gap is nonnegative by the classification and (3.1)–(3.2); finiteness forces every gap to vanish. Therefore every coordinate progression is constant, and A = B = C = F. This proves the theorem and its histogram strengthening. For n = 0 the same empty-sum argument applies; there is just one empty vector.

Source Section 4. For each nonconstant ℓ-term coordinate progression v in D, let x_v count its occurrences. Equation (4.1) requires $\Sigma_{v:v_i=t}\, x_v = \Sigma_{v:v_j=t}\, x_v$ for each digit t and pair i,j. Write this homogeneous system as Ax = 0 with $x \geq 0$ integral. A nonzero solution yields a vector progression; after balancing common digit counts with constant columns it yields one in S(D,n). Conversely any nonconstant vector progression yields such a solution.

The source uses integer linear programming and row-equivalent matrices B = TA. A row of one sign forces its supported columns to zero; iterated deletion of all columns certifies reducibility. It reports computations for primes $5 \leq p \leq 31$ and lengths $3 \leq \ell \leq 8$, verifying 50 of 54 Table 1 bounds by the stated reducibility choices. Here weighting the digit equations by E and combining positions with signs (+,−,−,+) gives a row-span functional whose value on every nonconstant column is strictly positive. It annihilates Ax = 0, forcing x = 0 even over the nonnegative reals. Thus (3.1) is a uniform dual, or Farkas-type, certificate for this source model.

mathdb:2611.00019v1 03 Nov 2026

4. Diagnostics and the size consequence

The following tests explain the roles of the hypotheses. They are diagnostics, not substitutes for the proof or assertions of global optimality.

The parity correction matters. At $p = 13$, the coordinate progression $(5,0,8,3)$ lies in D and has both second differences divisible by 13. The pure quadratic potential $4t^2$ gives gap $4(25+9-0-64) = -120$. The correction contributes 136 and restores the gap 16. Ordinary quadratic convexity alone therefore fails on this family.

The omitted digit matters. Adding $(p+1)/2 = 7$ at $p = 13$ gives the digit set $\{0,\dots,8\}$. In dimension 9 the following four vectors form a nonconstant progression modulo 13:

$A = (0,1,2,3,4,5,6,7,8)$,
$B = (0,2,8,4,3,6,5,1,7)$,
$C = (0,3,1,5,2,7,4,8,6)$,
$F = (0,4,7,6,1,8,3,2,5)$.

Every row is a permutation of the enlarged digit set. Coordinate subtraction gives $C = 2B-A$ and $F = 2C-B$ modulo 13, with $A \neq B$. Thus the one-digit enlargement is inadmissible. No maximality claim for other digit sets is implied.

A histogram constraint matters. If frequencies are dropped, the scalar progression $0,1,2,3$ is already supported on D. To keep a dimension divisible by h, use vectors all of whose h coordinates are respectively $0,1,2,3$. Equal histograms across the four vectors are enough for the proof; equality of the frequencies of different digits is a sufficient source convention.

Cardinality. For h dividing n, $|S(D,n)| = n! / ((n/h)!)^h$. Stirling's formula, with p fixed, gives $|S(D,n)| \gg_p h^n / n^{(h-1)/2}$. For arbitrary sufficiently large n, set $N = h\lfloor n/h \rfloor$ and append $n-N$ zero coordinates to $S(D,N)$. This embedding preserves nonconstant-progression exclusion; since $n-N < h$, the lost factor h^{n-N} is bounded in terms of p. For prime $p \geq 13$, $p \equiv 1 \pmod 4$,

$$r_4(Z_p^n) \gg_p ((p+3)/2)^n / n^{(p+1)/4}. \quad (4.1)$$

Honest comparison. EHPS [5, Theorem 1.3] gives $r_3(Z_p^n) \geq (p\sqrt{(7/24)})^n/(10^6 p^2 n^3)$. Since the first three terms of a nonconstant four-term progression are distinct for these primes, $r_4 \geq r_3$. Its exponential base exceeds $(p+3)/2$ exactly when $p^2-36p-54 > 0$, namely $p > 18+\sqrt{378} \approx 37.442$. In particular it gives an asymptotically larger bound for every eligible prime $p \geq 41$. A larger progression-free set does not decide admissibility of this prescribed smaller family.

The source's Table 1 already treats $p \leq 31$ computationally: for length 4 it lists sizes 8 at $p = 13$, 10 at $p = 17$, and at least 17 at $p = 29$, exceeding our $h = 16$ there. We make no record-size claim at these primes or in general. The result is the exact uniform admissibility assertion of Conjecture 2.4.

mathdb:2611.00019v1 03 Nov 2026

5. Formal correspondence and reproducibility

The frozen Digits.lean is byte-identical to the submitted certificate (SHA-256 0bb3177a827bb4499b2671253b34ef04bd24899975ada71ae86890986d8727fa). Its namespace is Digits356756. Audit.lean is also preserved byte for byte. The following correspondence distinguishes proved endpoints from ordinary corollaries.

Lean declaration	Mathematical meaning
SourceDigit p t	$t \le (p-1)/2$ or $t = (p+3)/2$, using natural divisions.
SourceSet p n x	Actual vectors Fin n → ZMod p; membership and digit-fibre cardinalities $n/((p+3)/2)$.
energy k t	$4t^2 - (12k-2)\varepsilon(t)$, on integer representatives.
gap_nonneg	Local nonnegativity, with zero gap forcing a=b=c=d.
full_scope	All four SourceSet vectors coincide if both second differences vanish; $p \ge 13$ and $p\%4=1$.
mathdb_356756	Literal prime-modulus source statement; retains primality and h dividing n.
no_affine_progression	Excludes $x+jr$, $j \in$ Fin 4, for every nonzero vector r.

The bridges are explicit: digit_bridge converts the natural divisions at $p = 4k+1$ into the integer Digit predicate; dvd_bridge converts a zero second difference in ZMod into integer divisibility. All listed digits are less than p, so ZMod.val gives precisely the intended representatives. same_histogram and sum_same prove equality of finite potential totals from the fibre counts.

Under h dividing n, Definition 2.1's h required fibres each have size n/h; their disjoint union has size n and therefore exhausts the coordinate index set. The explicit membership conjunct in SourceSet is thus equivalent to the printed definition, rather than a restriction. Zero second differences give $C = 2B-A$ and $F = 3B-2A$; taking $x = A$, $r = B-A$ gives the usual affine description. Conversely the affine description satisfies those equations by ring identities, and $r \neq 0$ is equivalent to $A \neq B$.

full_scope requires neither primality nor the dimension divisibility hypothesis. The source endpoint retains both, with intentionally unused hypothesis names. At n = 0 the vector type has one element, so exclusion holds. The more general histogram assertion follows from the ordinary proof; the frozen module formalizes the equal-frequency SourceSet specialization. Formula (4.1), Stirling's estimate and literature comparisons are not formalized in this packet.

Trust and checks. AuditFull prints the full type, value? body with allowOpaque := true, safety/partial flags and transitive axioms of every Digits declaration, including generated declarations. It rejects local axioms, missing bodies (apart from kernel inductive kinds), unsafe or partial declarations, and any axiom outside propext, Classical.choice, Quot.sound. The replay expects 45 declarations, types and bodies and runs leanchecker separately on Digits, Audit and AuditFull.

The pinned toolchain is Lean 4.34.1, commit 5045d0056413266e57c625dcd7c365b10e377c52; mathlib is d13f23b723b8a846827a245b89c10fc7d3f11612. REPRODUCE.md specifies the read-only dependency cache and portable variables. Strict extracted builds use one Lean thread, two allowed CPUs, 120 CPU seconds, a 140-second wall watchdog, and a sampled 6 GiB RSS cap. Two false Lean controls must fail. Cached upstream oleans, the compiler, checker, operating system and hardware remain trusted: this is not an upstream source rebuild or a priority certificate.

mathdb:2611.00019v1 03 Nov 2026

6. Related work, access limits and bibliography

The quadratic-convexity ancestor is Elsholtz–Pach [2, Theorem 3.10 and its proof]. It supplies a three-term construction on an unextended half interval, with additional norm constraints; its quadratic mechanism does not handle the extra digit here, as the −120 diagnostic shows. Elsholtz–Lipnik [3] develops affine and projective caps and digit-reducibility methods, rather than this four-term family. EPS [4] constructs two-dimensional reducible building blocks for three-term progression avoidance; its manuscript is superseded by EHPS [5]. These are relevant method precedents, and [5] also supplies the stronger asymptotic comparison above.

The line-free paper [6] studies mainly full lines, that is, length p progressions. Avoiding a full line does not imply avoiding four-term progressions when $p \geq 13$. Its general-length result is an upper bound. Lipnik's thesis [7] reproduces the exact target in Chapter 4; the reviewer read the relevant construction and model sections, with caps material in Chapters 3 and 5. A related thesis by Führer [8] was also read in part by the reviewer; we do not claim it was read in full or use it as a mathematical premise here.

Bounded investigation. The candidate, independent reviewer and root read the relevant primary bodies, not only abstracts. This manuscript investigator re-read the source statements and Section 4, the ancestor theorem statement, and the principal later theorem statements from the frozen texts. The independent review additionally records readings of the cited proofs and construction passages. Receipts and exact body copies accompany this dossier. No assertion is made that every page of every work was read.

On 2 November 2026, the recorded searches covered exact conjecture wording and identifiers, author combinations and later follow-ups. Author-list access had a 404 and a timeout, neither retried. An imperfect citing index returned two items and cannot establish exhaustive coverage. The reviewer held the prior-art gate for access limitations; root closed it under a qualified bounded-search standard. Root's registry screens record OpenAI HEAD 4eaee87548250b2682affda7d05d947c05554bae and Omega HEAD c55f6f7c7d7e3cf46b0a7da9efbba687448b29aa. Complete Omega D5/Problems path trees were screened; relevant OpenAI manuscript opening material was read. This is not a complete proof-body audit of either registry. No exact prior resolution was located in bodies read, and no worldwide priority claim follows. This drafting pass performs no new live registry refresh; final acceptance and refresh belong to root.

Bibliography (primary bodies read at the recorded scopes)

[1] C. Elsholtz, B. Klahn and G. F. Lipnik. Large subsets of Z_m^n without arithmetic progressions. Designs, Codes and Cryptography 91 (2023), 1443–1452. DOI: 10.1007/s10623-022-01145-w; arXiv:2211.02588v1 (2022). Source Sections 2–4 and published statement.

[2] C. Elsholtz and P. P. Pach. Caps and progression-free sets in Z_m^n. Designs, Codes and Cryptography 88 (2020), 2133–2170; arXiv:1903.08266v1. Theorem 3.10 and relevant proof (reviewer).

[3] C. Elsholtz and G. F. Lipnik. Exponentially Larger Affine and Projective Caps. arXiv:2211.09772v1 (2022). Theorem 1 and relevant digit/reducibility passages.

[4] C. Elsholtz, L. Proske and L. Sauermann. New lower bounds for three-term progression free sets in F_p^n. arXiv:2401.12802v1 (2024). Theorems 1.1–1.2 and lifting/reducibility passages; superseded by [5].

[5] C. Elsholtz, Z. Hunter, L. Proske and L. Sauermann. Improving Behrend's construction: Sets without arithmetic progressions in integers and over finite fields. arXiv:2406.12290v1 (2024). Theorems 1.2–1.3, construction overview and Section 3 (reviewer).

[6] C. Elsholtz, J. Führer, E. Füredi, B. Kovács, P. P. Pach, D. G. Simon and N. Velich. Maximal line-free sets in F_p^n. arXiv:2310.03382v2 (2024). Sections 1–3 and related discussion (reviewer).

[7] G. F. Lipnik. On integer partitions, caps, progression-free sets and q-regular sequences. Doctoral thesis, TU Graz (March 2023). DOI: 10.3217/s837t-7bq41. Chapter 4, especially Conjecture 4.6.

[8] J. Führer. Combinatorial questions on arithmetic progressions in multi-dimensional spaces and hypercube tilings. Doctoral thesis, TU Graz (September 2024). Introduction and Chapter 2 (reviewer). Repository record havzx-grn51. The cached filename sieb-thesis.pdf is misleading; authorship is taken from its title page.

mathdb:2611.00019v1 03 Nov 2026