hexagon:2611.01310v1

SHORTEST PROGRESSION WINDOWS FOR THREE RESIDUES IN A CYCLIC GROUP: FIXED-ORDER MINIMA, CLASSIFICATION OF $2L$ EXTREMALS, AND PRIME–COMPOSITE DICHOTOMY

ROBERT KADLEC

Abstract. Given three residues modulo n, we determine the shortest arithmetic progression covering them whose step has a prescribed additive order. At order em, where m is the order of the subgroup generated by the differences, the exact minimum length is $1 + eR$, with R the minimum hexagonal span of a modulo-m primitive vector in a two-dimensional congruence lattice. Contrasting composite moduli with the prime-modulus affine-diameter regime of Straus, Rødseth, and Lev, we prove three extremal theorems: (i) for every proper factorization $m = pq$, the generating triple $\{0, 1, q\}$ has exact span $R = q$, giving $\max R(S; m) \geq m/\operatorname{lpf}(m)$ and breaking the $O(\sqrt{p})$ prime bound; (ii) for every even modulus $m = 2L$ ($L \geq 2$), every generating triple satisfies $R(S; 2L) \leq L$, with equality iff S contains an antipodal pair, equivalently iff S lies in the unique affine orbit of $\{0, 1, L\}$; and (iii) for every $k \geq 1$ and $m = 3k^2+3k+1$, $\{0, k+1, 2k+1\}$ attains the sharp hexagonal bound $R = 2k + 1 = \lfloor \frac{2}{\sqrt{3}}\sqrt{m} \rfloor$. Theorems (i)–(iii) are formally verified in Lean 4.33.1 with standard axioms only.

1. Problem and Notation

Given a subset $S \subset \mathbb{Z}/n\mathbb{Z}$, a *window* of length W and step $h \in \mathbb{Z}/n\mathbb{Z}$ is an arithmetic progression $u, u + h, \ldots, u + (W - 1)h$ covering S. Its *span* is $W - 1$ (the number of steps). When $n = p$ is prime, every nonzero step generates $\mathbb{F}_p$: Straus [7] initiated the affine-diameter problem for k-element subsets of $\mathbb{F}_p$, Rødseth [6, §3, p. 183] studied the minimal covering length d of an affine image inside $[0, d - 1]$ (counting positions, i.e. W), and Lev [4]

Date: November 28, 2026.

2020 *Mathematics Subject Classification.* Primary 11B25; Secondary 11A07, 11H06.

Key words and phrases. arithmetic progressions, cyclic groups, covering by progressions, affine diameter, lattice minima, formal verification.

ORCID: 0009-0003-9245-8130. Purely AI-generated research directed and supervised by the author, by whom full scholarly responsibility for the integrity, accuracy, and publication of all reported results is assumed (all mathematical derivations, Lean 4 formalizations, verification scripts, audits, and manuscript prose were executed by AI systems; see Section 5). This paper forms part of a broader research project investigating the respective competencies of humans and large language models.

established sharp simultaneous-approximation and covering asymptotics in $\mathbb{F}_p$ (counting span $W-1$).

At composite moduli n, two phenomena absent at prime moduli govern the problem: steps may generate proper subgroups of order $q \mid n$, and even among generators of $\mathbb{Z}/m\mathbb{Z}$, admissible lattice lifts must satisfy a *visibility* (modulo-m primitivity) condition. Section 2 establishes the exact fixed-order formula $1+ER$ and an infinite obstruction family showing that dropping visibility underestimates R by an unbounded factor. Section 3 proves the linear composite blowup $m/\operatorname{lpf}(m)$, completely classifies all extremal triples at even moduli $m=2L$, and compares composite and prime moduli via a sharp realization of the centered-hexagonal constant $\frac{2}{\sqrt{3}}\sqrt{m}$. Section 4 gives an $O(2^{\omega(m)}\log^2 m)$ algorithm after factoring m, and Section 5 records the scope of our Lean 4.33.1 formalization and its motivating connection to `HostThickOrbit`.

2. Fixed-Order Minimum and Composite Obstruction

Let $n \geq 1$ and $0 \leq H < n$. A permitted step in $\mathbb{Z}/n\mathbb{Z}$ has additive order strictly greater than H. For three distinct residues $S \subset \mathbb{Z}/n\mathbb{Z}$, translate one residue to 0 and write the other two as $A, B \in \mathbb{Z}$. Set

$$d := \gcd(n, A, B), \qquad m := \frac{n}{d}, \qquad a := \frac{A}{d}, \qquad b := \frac{B}{d},$$

so $\gcd(a, b, m) = 1$, and define $E := \min\{e : e \mid d,\ em > H\}$. For $(x, y) \in \mathbb{Z}^2$, define the hexagonal span norm

$$N(x, y) := \max(0, x, y) - \min(0, x, y) = \max(|x|, |y|, |x - y|),$$

the congruence lattice $\mathcal{L} := \{(x, y) \in \mathbb{Z}^2 : bx \equiv ay \pmod m\}$, and the minimum visible span

$$R(S; m) := \min\big\{N(x, y) : (x, y) \in \mathcal{L},\ \gcd(x, y, m) = 1\big\}.$$

Theorem 2.1 (Fixed-Order Minimum)**.** *Before imposing the order cutoff H, the attainable step orders of windows covering S are precisely em with $e \mid d$. Among steps of order em, the exact minimum window length is $1 + eR(S; m)$, and the overall minimum length over steps of order $> H$ is $1 + ER(S; m)$.*

Proof. A coset of $\langle h\rangle$ contains S if and only if the subgroup of order $q = \operatorname{ord}(h)$ contains A and B, i.e. $m \mid q \mid n$. Writing $q = em$ and $h = (d/e)v$ with $v \in (\mathbb{Z}/em\mathbb{Z})^\times$, the marked indices relative to 0 are $0, eua, eub \pmod{em}$, where $u \equiv v^{-1} \pmod m$; every $u \in (\mathbb{Z}/m\mathbb{Z})^\times$ is attained by Chinese Remainder lifting $v \equiv u^{-1} \pmod m$ and $v \equiv 1 \pmod p$ for primes $p \mid e$ with $p \nmid m$. Circular gaps scale by e, reducing the problem to unit-step windows modulo m. Choosing Bézout integers $sa + tb \equiv 1 \pmod m$, the correspondence $(x, y) \mapsto u \equiv sx + ty \pmod m$ bijects signed lifts of (ua, ub) with pairs $(x, y) \in \mathcal{L}$ satisfying $\gcd(x, y, m) = 1$, matching the modular-symbol identification of $\mathbb{P}^1(\mathbb{Z}/m\mathbb{Z})$ [5, §2.3], [3, §2.2]. □

Proposition 2.2 (Unbounded Visibility Obstruction)**.** *For every odd $k \geq 5$, $n = 2k$, and $S = \{0, 1, k+2\}$, we have $d = 1$ and $(2, 4) \in \mathcal{L}$ has span $N(2, 4) = 4$, yet $R(S; 2k) = (k+1)/2$.*

Proof. Since $y \equiv (k+2)x \pmod{2k}$, visibility $\gcd(x, y, 2k) = 1$ forces x to be odd, hence $y - 2x \equiv k \pmod{2k}$ and $k \leq |y - 2x| \leq |y - x| + |x| \leq 2N(x, y)$, giving $R \geq (k+1)/2$. Equality is attained by $(x, y) = ((k+1)/2, 1)$ when $k \equiv 1 \pmod 4$ and $((k-1)/2, -1)$ when $k \equiv 3 \pmod 4$. □

3. Extremal Spans: $2L$ Classification and Prime–Composite Dichotomy

Theorem 3.1 (Linear Composite Blowup)**.** *Let $m = pq$ with $p \geq 2$ and $q \geq 2$. Then the generating triple $S = \{0, 1, q\} \subset \mathbb{Z}/m\mathbb{Z}$ has exact minimum visible span $R(S; m) = q$. In particular, for every composite $m \geq 4$,*

$$\max_{|S|=3,\ \langle S-S\rangle=\mathbb{Z}/m\mathbb{Z}} R(S; m) \geq \frac{m}{\mathrm{lpf}(m)}.$$

Proof. Taking $u = 1$ places $\{0, 1, q\} \subset [0, q]$, so $R \leq q$. Conversely, for any unit $u \in (\mathbb{Z}/pq\mathbb{Z})^\times$ and any lift $y \equiv uq \pmod{pq}$, we have $y \not\equiv 0 \pmod{pq}$ (as $0 < q < pq$) and $q \mid y$, whence $|y| \geq q$ and $N(x, y) \geq |y| \geq q$. □

To classify all equality cases at even moduli $m = 2L$, we first record a self-contained four-line lemma on the lower-half cyclotomic subset $\Phi_d := \{t \in (\mathbb{Z}/d\mathbb{Z})^\times : 1 \leq t < d/2\}$.

Lemma 3.2 (Primitivity of Φ_d for Odd $d \geq 3$)**.** *For every odd integer $d \geq 3$, if $w \in (\mathbb{Z}/d\mathbb{Z})^\times$ satisfies $w \cdot \Phi_d \subseteq \Phi_d$, then $w = 1$.*

Proof. Since $1 \in \Phi_d$, the canonical representative $w_0 \in [1, d-1]$ satisfies $w_0 < d/2$. If $w_0 \geq 2$, choose the largest $k \geq 0$ with $2w_0 \cdot 2^k < d$. Because d is odd, $t := 2^{k+1}$ is a unit modulo d with $2t \leq 2w_0 \cdot 2^k < d$, so $t \in \Phi_d$. Yet $d < 2w_0 \cdot 2^{k+1} < 2d$, so $w_0 t \in (d/2, d)$ and $w \cdot t \notin \Phi_d$, a contradiction. □

Theorem 3.3 (Complete Classification of $m = 2L$ Equality Cases)**.** *Let $L \geq 2$ and let $S = \{0, a, b\} \subset \mathbb{Z}/2L\mathbb{Z}$ be any generating triple of three distinct residues ($\gcd(a, b, 2L) = 1$). Then:*

1. *$R(S; 2L) \leq L$.*
2. *$R(S; 2L) = L$ if and only if S contains an antipodal pair ($a \equiv L$, $b \equiv L$, or $b - a \equiv L \pmod{2L}$), which holds if and only if S lies in the* unique *affine orbit of $\{0, 1, L\}$.*
3. *If S contains no antipodal pair, then $R(S; 2L) \leq L - 1$.*

Proof. Suppose first that S contains an antipodal pair; after translating and swapping we may assume $b \equiv L \pmod{2L}$, so $\gcd(a, L) = 1$. Every unit $u \in (\mathbb{Z}/2L\mathbb{Z})^\times$ is odd and therefore fixes L modulo $2L$, giving $R(S; 2L) \geq L$ as in Theorem 3.1. If a is odd, then $a \in (\mathbb{Z}/2L\mathbb{Z})^\times$ and $a^{-1}S = \{0, 1, L\}$; if a is even, then L must be odd and $L - a$ is an odd unit modulo $2L$, so $L - (L-a)^{-1}S = \{L, 1, 0\} = \{0, 1, L\}$. Thus every antipodal generating triple

lies in the unique affine orbit of $\{0, 1, L\}$ and attains $R = L$. Conversely, any affine image of $\{0, 1, L\}$ preserves the antipodal difference L.

Now suppose $S = \{0, a, b\}$ has no antipodal pair. Because $\gcd(a, b, 2L) = 1$, among the three differences $a, b, b-a$ exactly one is even and two are odd. Translating and swapping if needed, assume $p := a$ is even, $q := b$ is odd, and $p, q, q-p \not\equiv 0, L \pmod{2L}$.

Case 1: L is even ($4 \mid 2L$). Choose $s \in \{1, -1\}$ so that $(sp \bmod 2L) \in (0, L)$. If $(sq \bmod 2L) < L$, then $sS \subset [0, L-1]$ and $R \le L-1$. Otherwise $(sq \bmod 2L) \in (L, 2L)$, and the unit involution $w := 1+L \in (\mathbb{Z}/2L\mathbb{Z})^\times$ fixes the even residue sp while translating the odd residue sq by L into $(0, L)$, placing $wsS \subset [0, L-1]$.

Case 2: $L \ge 3$ is odd ($2L \equiv 2 \pmod 4$). Suppose for contradiction that no unit $u_2 \in (\mathbb{Z}/2L\mathbb{Z})^\times$ places both $u_2 p$ and $u_2 q$ into $(0, L)$. Applying this failure to both u_2 and $-u_2$ yields the equivalence

$$(u_2 p \bmod 2L) < L \iff (u_2 q \bmod 2L) > L \qquad \forall\, u_2 \in (\mathbb{Z}/2L\mathbb{Z})^\times.$$

Writing $p = 2p'$ and $B := 2^{-1} q \in \mathbb{Z}/L\mathbb{Z}$, Chinese Remainder reduction to $u \in (\mathbb{Z}/L\mathbb{Z})^\times$ gives $(u_2 p \bmod 2L) = 2(up' \bmod L)$, whereas the odd residue $u_2 q \bmod 2L$ exceeds L if and only if $(uq \bmod L)$ is even, i.e. if and only if $2(uB \bmod L) < L$. Thus for every $u \in (\mathbb{Z}/L\mathbb{Z})^\times$,

$$2(up' \bmod L) < L \iff 2(uB \bmod L) < L.$$

Set $g_1 := \gcd(p', L)$, $d_1 := L/g_1$ and $g_2 := \gcd(B, L)$, $d_2 := L/g_2$. Both $d_1, d_2 \ge 3$ are odd (since $p \not\equiv 0$ and $q \not\equiv L \pmod{2L}$), and the two sides pull back translates of Φ_{d_1} and Φ_{d_2} along $(\mathbb{Z}/L\mathbb{Z})^\times \to (\mathbb{Z}/d_i\mathbb{Z})^\times$. By Lemma 3.2, invariance of Φ_{d_1} under $\ker((\mathbb{Z}/L\mathbb{Z})^\times \to (\mathbb{Z}/d_2\mathbb{Z})^\times)$ forces $d_1 \mid d_2$: for any prime r with $v_r(d_1) > v_r(d_2)$, CRT supplies a unit $k \equiv 1 \pmod{L/r^{v_r(L)}}$ satisfying $k \equiv 1 \pmod{r^{v_r(d_2)}}$ and $k \not\equiv 1 \pmod{r^{v_r(d_1)}}$. Symmetrically $d_2 \mid d_1$, so $d_1 = d_2$ and $g_1 = g_2$. Since $\gcd(2p', q, 2L) = 1$, we obtain $g_1 = g_2 = 1$, whence $p', B \in (\mathbb{Z}/L\mathbb{Z})^\times$. Lemma 3.2 now forces $p' \equiv B \pmod L$, i.e. $2p' \equiv q \pmod L$. As $q - 2p'$ is odd, this forces $q - p \equiv L \pmod{2L}$, contradicting the no-antipodal hypothesis. Hence some u_2 places $u_2 S \subset [0, L-1]$, proving $R(S; 2L) \le L-1$. □

Comparison with Straus, Rødseth, and Lev at Prime Moduli. For a prime modulus $p \ge 3$, consider the positive-definite hexagonal quadratic form $Q(x, y) := x^2 - xy + y^2$, whose Gram matrix $\left(\begin{smallmatrix} 1 & -1/2 \\ -1/2 & 1 \end{smallmatrix}\right)$ has determinant $3/4$. On the index-p congruence sublattice $\mathcal{L} \subset \mathbb{Z}^2$ ($\det \mathcal{L} = p$), the restricted quadratic form has determinant $\frac{3}{4}p^2$. By Hermite's constant $\gamma_2 = 2/\sqrt{3}$ in dimension 2, there exists a nonzero lattice vector $(x, y) \in \mathcal{L}$ satisfying

$$x^2 - xy + y^2 \le \gamma_2 \sqrt{\tfrac{3}{4}p^2} = p.$$

Using the algebraic identities

$$x^2 - xy + y^2 = \tfrac{3}{4}x^2 + \left(y - \tfrac{1}{2}x\right)^2 = \tfrac{3}{4}y^2 + \left(x - \tfrac{1}{2}y\right)^2 = \tfrac{3}{4}(x-y)^2 + \tfrac{1}{4}(x+y)^2,$$

we obtain $x^2 - xy + y^2 \geq \frac{3}{4}\max(|x|, |y|, |x-y|)^2 = \frac{3}{4}N(x,y)^2$, and hence $N(x,y) \leq \frac{2}{\sqrt{3}}\sqrt{p}$. Since $p \geq 3 > 4/3$, we have $\frac{2}{\sqrt{3}}\sqrt{p} < p$, so (x,y) cannot be divisible by p and is automatically visible modulo p ($\gcd(x,y,p) = 1$). Because $N(x,y)$ is an integer, it follows immediately that

$$R(S;p) \leq \left\lfloor \frac{2}{\sqrt{3}}\sqrt{p} \right\rfloor$$

for every triple $S \subset \mathbb{F}_p$, matching the $\Theta(\sqrt{p})$ affine-diameter regime established for general k-element sets by Straus [7], Rødseth [6] (in covering-length convention $W = R + 1$), and Lev [4] (in span convention R). By contrast, Theorem 3.1 shows that composite moduli with bounded least prime factor $\mathrm{lpf}(m)$ jump from $\Theta(\sqrt{m})$ to linear growth $m/\mathrm{lpf}(m)$, while composite moduli with large $\mathrm{lpf}(m)$ (such as $m = 49 = 7^2$ in Table 1) can still exceed $m/\mathrm{lpf}(m)$ and reach the hexagonal scale $\lfloor \frac{2}{\sqrt{3}}\sqrt{m} \rfloor$. The next theorem proves by a pure integer Eisenstein-norm argument that the constant $\frac{2}{\sqrt{3}}\sqrt{m}$ is attained sharply along an infinite quadratic sequence, including all centered-hexagonal primes $p = 7, 19, 37, 61, 127, \ldots$.

Theorem 3.4 (Sharp Centered-Hexagonal Realization)**.** *For every integer $k \geq 1$ and $m = 3k^2 + 3k + 1$, the generating triple $S_k := \{0, k+1, 2k+1\} \subset \mathbb{Z}/m\mathbb{Z}$ has exact minimum visible span*

$$R(S_k; m) = 2k + 1 = \left\lfloor \frac{2}{\sqrt{3}}\sqrt{m} \right\rfloor.$$

Proof. The lift $(x,y) = (2k+1, k+1)$ gives $R \leq 2k+1$. Conversely, let $(x,y) \in \mathcal{L}$ be any visible vector, so $x \equiv u(2k+1)$ and $y \equiv u(k+1) \pmod{m}$ for some $u \in (\mathbb{Z}/m\mathbb{Z})^\times$. Then $(k+1)x \equiv (2k+1)y \pmod{m}$. Multiplying $kx + (k+1)y$ by $2k+1$ gives $(3k^2+3k+1)x \equiv 0 \pmod{m}$, and $\gcd(2k+1, m) = 1$ forces $m \mid (kx + (k+1)y)$. Setting $a := (kx + (k+1)y)/m$ and $b := ((2k+1)y - (k+1)x)/m$ yields $(a,b) \in \mathbb{Z}^2 \setminus \{(0,0)\}$ with $x = (2k+1)a - (k+1)b$, $y = (k+1)a + kb$, and the Eisenstein-norm identity

$$x^2 - xy + y^2 = m(a^2 - ab + b^2).$$

Elementary sign analysis gives $x^2 - xy + y^2 \leq N(x,y)^2$, and $(2a-b)^2 + 3b^2 = 8$ has no integer solution, so $a^2 - ab + b^2 \neq 2$. If $a^2 - ab + b^2 = 1$, then $(a,b) \in \{\pm(1,0), \pm(0,1), \pm(1,1)\}$, and all six lifts have $N(x,y) = 2k+1$. If $a^2 - ab + b^2 \geq 3$, then $N(x,y)^2 \geq 3m = 9k^2 + 9k + 3 > (2k+1)^2$, so $N(x,y) \geq 2k+2$. Finally, $3(2k+1)^2 = 4m - 1 < 4m < 3(2k+2)^2$, proving $2k+1 = \lfloor \frac{2}{\sqrt{3}}\sqrt{m} \rfloor$. □

4. Computing the Minimum via Euclidean Floor Sums

Anchor an optimal interval at its first hit by trying each of the three residues as left endpoint and taking its normalized differences (a,b). By

TABLE 1. Prime vs. composite extremal spans $\max_S R(S;m)$ across all generating triples (exhaustive Python computation for all moduli $m \le 61$ and all even moduli $m = 2L \le 72$). Composite moduli with small $\mathrm{lpf}(m)$ jump from $\Theta(\sqrt{m})$ to linear $m/\mathrm{lpf}(m)$; centered-hexagonal primes $p = 3k^2+3k+1$ attain $\lfloor \frac{2}{\sqrt{3}}\sqrt{p} \rfloor$ sharply.

Modulus m	Type	$\max R(S;m)$	$m/\mathrm{lpf}(m)$	$\lfloor \frac{2}{\sqrt{3}}\sqrt{m} \rfloor$
$7 = 3\cdot 1^2+3\cdot 1+1$	Prime (hex)	3	1	3
$19 = 3\cdot 2^2+3\cdot 2+1$	Prime (hex)	5	1	5
$37 = 3\cdot 3^2+3\cdot 3+1$	Prime (hex)	7	1	7
53	Prime	7	1	8
$61 = 3\cdot 4^2+3\cdot 4+1$	Prime (hex)	9	1	9
$2L$ $(2 \le L \le 36)$	Even (unique $\{0,1,L\}$)	L	L	$\lfloor\sqrt{8L/3}\rfloor$
$15 = 3\cdot 5$	Odd composite	5	5	4
$33 = 3\cdot 11$	Odd composite	11	11	6
$49 = 7^2$	Odd composite	8	7	8
$55 = 5\cdot 11$	Odd composite	11	11	8
$57 = 3\cdot 19$	Odd composite	19	19	8

Möbius inversion on the visibility condition $\gcd(x,y,m)=1$, a visible solution with $1 \le x, y \le r$ exists if and only if

$$\sum_{t \mid m} \mu(t)\, D_{m/t}\Big(\Big\lfloor \frac{r}{t} \Big\rfloor, \Big\lfloor \frac{r}{t} \Big\rfloor\Big) > 0,$$

where $D_q(X,Y)$ counts solutions of $bx \equiv ay \pmod q$ with $1 \le x \le X$, $1 \le y \le Y$. Writing $g = \gcd(q,a)$, $P = q/g$, and $v \equiv b(a/g)^{-1} \pmod P$ (for $P > 1$), the count

$$D_q(X,Y) = \sum_{j=1}^{\lfloor X/g \rfloor} \left(\left\lfloor \frac{Y - vj}{P} \right\rfloor - \left\lfloor \frac{-vj}{P} \right\rfloor \right)$$

evaluates in $O(\log q)$ arithmetic operations via the Euclidean floor-sum recurrence [2]. Binary searching over $r \in [1, m-1]$ therefore determines $R(S;m)$ in $O(2^{\omega(m)} \log^2 m)$ arithmetic operations after factoring m, plus $O(\tau(d))$ to select E.

5. Formal Verification Scope and Origin in HostThickOrbit

The extremal theorems in Section 3 are formally verified in a standalone Lean 4.33.1 module (`OrbitEquality2L.lean`, 1,765 lines), containing zero `sorry`, zero `native_decide`, and zero custom axioms. All six exported target theorems covered by the accompanying five-check receipt (`OrbitEquality2L_VERIFICATION.json`) depend solely on the three standard axioms `propext`, `Classical.choice`, and `Quot.sound`:

- `isLeast_composite_divisor_span` (Theorem 3.1),

- `isLeast_antipodal_2L` and `unitWindow_even_le_L_sub_one` (Theorem 3.3),
- `hypCMType_stab_trivial_of_odd` (Lemma 3.2),
- `even_extremal_classification_2L` (Theorem 3.3),
- `centered_hexagonal_exact_span` (Theorem 3.4).

To reduce single-checker trust, `OrbitEquality2L.lean` and its `lean4 export` environment stream were checked across five verification invocations covering four distinct codebases: `lean 4.33.1` and `leanchecker` (sharing the official Lean kernel), together with the independent export checkers `con-leche --verified` (9,513 declarations accepted), `con-ron --verified` (9,513 declarations accepted), and `nanoda_bin` (10,316 declarations checked with zero typechecker errors under a strict three-axiom permit configuration; `nanoda_bin` records one non-fatal pretty-printer diagnostic regarding axiom printing). Exact artifact checksums and verification receipts are provided in the accompanying software archive rather than in this text. By contrast, the companion files `OrderWindow.lean` and `CyclicTheoremSix.lean` (formalizing Theorem 2.1), Proposition 2.2 (the visibility obstruction), Table 1 (an exhaustive Python census for all moduli $m \leq 61$ and all even moduli $m = 2L \leq 72$), and the complexity analysis in Section 4 lie outside the six-target `OrbitEquality2L_VERIFICATION.json` receipt.

Remark 5.1 (Motivating origin in `HostThickOrbit`)**.** This problem arose from inspecting the predicate `HostThickOrbit` in Alpöge's Lean 4 Riemann Hypothesis archive [1], which derives two orbit separation tests from $4Ls < n$ and the integer separation hypothesis `NoRel`. For $T = \{0, 1, 2\}$, $L = 2$, and $n \geq 17$, both orbit tests hold even though $2(1-0) = 1(2-0)$ violates `NoRel`, demonstrating that `NoRel` is sufficient but not necessary for small-window orbit separation.

AI Provenance and Scholarly Responsibility. Purely AI-generated research directed and supervised by the author (Robert Kadlec, Masaryk University, Brno), by whom full scholarly responsibility for the integrity, accuracy, and publication of all reported results is assumed (all mathematical derivations, Lean 4 formalizations, verification scripts, cross-model audits, and manuscript prose were executed by AI systems). This paper forms part of a broader research project investigating the respective competencies of humans and large language models.

References

[1] L. Alpöge and collaborators, *Riemann Hypothesis Lean Archive*, November 2026, publicly archived repository.

[2] AtCoder Library, *Mathematics module: `floor_sum` specification and Practice Contest 2 editorial*, `https://atcoder.github.io/ac-library/production/document_en/math.html`.

[3] J. E. Cremona, *Algorithms for Modular Elliptic Curves*, 2nd ed., Cambridge Univ. Press, 1997, §2.2.

[4] V. F. Lev, *Simultaneous approximations and covering by arithmetic progressions in* $\mathbb{F}_p$, J. Combin. Theory Ser. A **92** (2000), 103–118.
[5] Yu. I. Manin, *Parabolic points and zeta-functions of modular curves*, Math. USSR-Izvestiya **6** (1972), 19–64, §2.3.
[6] Ø. J. Rødseth, *Sums of distinct residues mod p*, Acta Arith. **65** (1993), 181–184, §3.
[7] E. G. Straus, *Differences of residues (mod p)*, J. Number Theory **8** (1976), 40–42.

Masaryk University, Brno, Czech Republic
Email address: kadlecr@mail.muni.cz