Algebraic Rigidity and Quadratic Residue Asymmetry in Legendre Intervals

Ruqing Chen

GUT Geoservice Inc., Montréal, Canada

ruqing@hotmail.com

Repository: https://github.com/Ruqing1963/legendre-spin-asymmetry

February 2026

Abstract

We prove that Legendre intervals $\mathcal{I}_n = [(n-1)^2, n^2]$ whose length $p = 2n-1$ is prime possess a rigid algebraic structure: the interior integers $\mathcal{I}_n^\circ = \{(n-1)^2+1, \ldots, n^2-1\}$ form a *punctured complete residue system* modulo p, missing exactly the quadratic residue class $r \equiv n^2 \pmod{p}$. As a consequence, the Legendre symbol distribution over $\mathcal{I}_n^\circ$ exhibits a universal *spin asymmetry*: the number of quadratic non-residues exceeds the number of quadratic residues by exactly 1. This theorem is verified computationally for all qualifying $n \leq 2000$ (549 instances, 100% confirmation). We complement this algebraic result with empirical measurements of the *discrete Wronskian volume*—the radical compression ratio of maximal prime-free subsequences near n^2—and observe that this ratio stabilizes near 1.20 as $n \to \infty$, well below the Szpiro threshold. Together, these findings reveal previously unobserved algebraic and arithmetic rigidity constraints on the internal structure of Legendre intervals.

1 Introduction

1.1 Legendre's Conjecture and interval structure

Legendre's Conjecture asserts that for every $n \geq 1$, the interval $[n^2, (n+1)^2]$ contains at least one prime. Equivalently (by a shift of index), for every $n \geq 2$, the interval $\mathcal{I}_n = [(n-1)^2, n^2]$ contains a prime. While the Prime Number Theorem predicts approximately $n/\log n$ primes in $\mathcal{I}_n$, no unconditional proof of even a single prime has been achieved.

Most approaches to Legendre's Conjecture focus on *counting* primes via sieve methods or zero-free regions of the Riemann zeta function. In this paper, we take a fundamentally different approach: we study the *algebraic structure* of the interval itself, specifically its behavior as a residue system modulo its own length $p = 2n-1$.

1.2 Main result: the Spin Asymmetry Theorem

When $p = 2n-1$ is prime, the $p-1$ integers in the interior of $\mathcal{I}_n$ form a remarkable algebraic object: a complete residue system modulo p with exactly one class removed. We prove (Theorem 2.5) that the removed class is *always* a quadratic residue, creating a universal asymmetry in the Legendre symbol distribution.

This asymmetry is not a statistical phenomenon—it is an *exact algebraic identity* that holds for every n with $2n-1$ prime.

1.3 Complementary evidence: Wronskian compression

We also study the multiplicative structure of maximal prime-free subsequences ("prime vacuums") within $\mathcal{I}_n$ by computing the ratio of the logarithmic volume $\log \prod C_i$ to the logarithmic radical $\log \operatorname{rad}(\prod C_i)$ for sequences of consecutive composites. This ratio, which we call the *discrete Wronskian compression*, measures the degree to which prime factors are shared among consecutive composites. We observe empirically that this ratio stabilizes near 1.20 across six orders of magnitude in n.

1.4 Context within the Titan Project

In a companion paper [4], we proved the function field analogue of Legendre's Conjecture via monodromy and the Chebotarev density theorem. The algebraic structure uncovered here—quadratic residue asymmetry governed by the interval length—has no direct analogue in the function field setting, where the parameter space is an affine variety rather than a residue system. The present paper thus provides a complementary, specifically integer-theoretic perspective on the problem. The conductor rigidity phenomena studied in [1, 2, 3] established that classical L-function methods encounter structural barriers for additive prime number problems. The quadratic residue framework developed here may offer a route that circumvents these barriers.

2 The Spin Asymmetry Theorem

2.1 Setup and notation

Definition 2.1 (Legendre interval)**.** For $n \geq 2$, the *Legendre interval* is $\mathcal{I}_n = [(n-1)^2,\, n^2]$. Its *interior* is $\mathcal{I}_n^\circ = \{(n-1)^2+1, \ldots, n^2-1\}$. The interval has total length $|\mathcal{I}_n| = 2n-1$ (inclusive of endpoints) and interior cardinality $|\mathcal{I}_n^\circ| = 2n-3$.

Remark 2.2. The interval $[(n-1)^2, n^2]$ contains $n^2-(n-1)^2+1 = 2n$ integers (inclusive of both endpoints). If $p := 2n-1$ is prime, then $|\mathcal{I}_n| = p+1 = 2n$ and $|\mathcal{I}_n^\circ| = p-1 = 2n-2$.

Definition 2.3 (Spin)**.** Let p be an odd prime. For an integer a, the *spin* of a modulo p is the Legendre symbol $\left(\frac{a}{p}\right) \in \{-1, 0, +1\}$. We say a has *positive spin* if $\left(\frac{a}{p}\right) = +1$ (quadratic residue), *negative spin* if $\left(\frac{a}{p}\right) = -1$ (quadratic non-residue), and *zero spin* if $p \mid a$.

2.2 The punctured residue system

Lemma 2.4. *Let $n \geq 2$ and $p = 2n-1$. Set $r \equiv n^2 \pmod{p}$. Then:*

(i) $(n-1)^2 \equiv n^2 \equiv r \pmod{p}$.

(ii) The interior $\mathcal{I}_n^\circ$ consists of $p-1$ consecutive integers, and its elements represent every residue class modulo p except *r. In particular, exactly one element of $\mathcal{I}_n^\circ$ is divisible by p.*

(iii) $\gcd(n,p) = 1$, *so $r \equiv n^2 \pmod{p}$ is a nonzero quadratic residue:* $\left(\frac{r}{p}\right) = +1$.

Proof. **(i)** $(n-1)^2 = n^2-2n+1 = n^2-(2n-1) = n^2-p$, so $(n-1)^2 \equiv n^2 \pmod{p}$.

(ii) The set $\{(n-1)^2, (n-1)^2+1, \ldots, (n-1)^2+(p-1)\} = \{(n-1)^2, \ldots, n^2-1\}$ has exactly p elements (since $(n-1)^2+(p-1) = n^2-1$), hence covers every residue class modulo p exactly once. Removing the first element $(n-1)^2$ (which has residue r) yields $\mathcal{I}_n^\circ = \{(n-1)^2+1, \ldots, n^2-1\}$, which covers all residues *except* r. Since $r \neq 0$ (see (iii)), the class 0 is represented, so exactly one element of $\mathcal{I}_n^\circ$ is divisible by p.

(iii) $\gcd(n, 2n-1) = \gcd(n, -1) = 1$, so $p \nmid n$, hence $r = n^2 \bmod p \neq 0$. Since $r \equiv n^2 \pmod{p}$ is explicitly a perfect square modulo p, we have $\left(\frac{r}{p}\right) = +1$. $\square$

2.3 The main theorem

Theorem 2.5 (Spin Asymmetry). *Let $n \geq 2$ be an integer such that $p = 2n-1$ is prime. Denote by N^+, N^-, N^0 the numbers of elements of $\mathcal{I}_n^\circ$ with positive, negative, and zero spin modulo p, respectively. Then:*

$$N^+ = \frac{p-3}{2} = n-2, \qquad N^- = \frac{p-1}{2} = n-1, \qquad N^0 = 1. \tag{1}$$

In particular,

$$N^- - N^+ = 1 \tag{2}$$

for every such n. Quadratic non-residues always exceed quadratic residues by exactly one.

Proof. By Lemma 2.4(ii), the elements of $\mathcal{I}_n^\circ$ represent all residue classes modulo p except r. Among the p residue classes modulo p:

- Class 0: spin 0. Count: 1.
- Nonzero QR classes: spin $+1$. Count: $(p-1)/2$.
- Nonzero NR classes: spin -1. Count: $(p-1)/2$.

Total: $1 + (p-1)/2 + (p-1)/2 = p$.

The interior $\mathcal{I}_n^\circ$ covers all classes *except* r, which is a nonzero QR (Lemma 2.4(iii)). Therefore:

$$\begin{aligned} N^0 &= 1, \\ N^+ &= \frac{p-1}{2} - 1 = \frac{p-3}{2} = n-2, \\ N^- &= \frac{p-1}{2} = n-1. \end{aligned}$$

Hence $N^- - N^+ = (n-1) - (n-2) = 1$. $\square$

Remark 2.6. The proof is entirely elementary, using only the structure of quadratic residues modulo a prime and the coincidence of endpoints modulo p. The key arithmetic input is the identity $(n-1)^2 \equiv n^2 \pmod{2n-1}$, which is trivially verified.

2.4 Computational verification

Proposition 2.7. *The Spin Asymmetry Theorem has been verified computationally for all $n \leq 2000$ such that $2n-1$ is prime (549 instances). In every case, $N^- - N^+ = 1$ and $N^0 = 1$.*

Example 2.8. For $n = 4$, $p = 7$, $\mathcal{I}_4^\circ = \{10, 11, 12, 13, 14, 15\}$. The residues modulo 7 are $\{3, 4, 5, 6, 0, 1\}$, missing $r = 16 \bmod 7 = 2$. The QRs modulo 7 are $\{1, 2, 4\}$; NRs are $\{3, 5, 6\}$. Among the represented nonzero residues $\{1, 3, 4, 5, 6\}$: QRs $= \{1, 4\}$ ($N^+ = 2$), NRs $= \{3, 5, 6\}$ ($N^- = 3$), plus $\{0\}$ ($N^0 = 1$). Indeed $N^- - N^+ = 1$.

Example 2.9. For $n = 100$, $p = 199$, $\mathcal{I}_{100}^\circ$ has 198 elements covering all residues modulo 199 except $r = 10000 \bmod 199 = 50$. Since 50 is a QR modulo 199 (as $50 \equiv 100^2 \pmod{199}$): $N^+ = 98$, $N^- = 99$, $N^0 = 1$.

3 Structural Implications

3.1 The asymmetry as an algebraic constraint

The Spin Asymmetry Theorem reveals that when $p = 2n-1$ is prime, the Legendre interval is not merely a collection of consecutive integers: it is a structured algebraic object whose internal residue distribution is *exactly* determined by n.

This structure constrains any prime-free realization of the interval. If all elements of $\mathcal{I}_n$ were composite, these $p-1$ composites would need to simultaneously satisfy:

(a) *Divisibility:* every element has at least two prime factors (counted with multiplicity).
(b) *Residue coverage:* the composites cover all residue classes modulo p except r, including exactly one multiple of p itself.
(c) *Spin asymmetry:* the Legendre symbols of these composites reproduce the exact $(n-2, n-1, 1)$ distribution.

Conditions (a)–(c) are individually easy to satisfy, but their *simultaneous* satisfaction across $p-1$ consecutive integers is a nontrivial structural constraint.

3.2 Density of qualifying intervals

The theorem applies whenever $p = 2n-1$ is prime. By the Prime Number Theorem, the number of primes of the form $2n-1$ up to x is $\sim x/(2\log x)$. Thus the theorem governs a positive proportion of all Legendre intervals, and the qualifying n have no essential gaps.

3.3 Limitations

We emphasize what the Spin Asymmetry Theorem does *not* prove: it does not, by itself, establish that $\mathcal{I}_n$ contains a prime. The quadratic residue structure modulo p constrains the *algebraic shape* of the interval but does not directly control the *multiplicative structure* of individual elements. Converting the algebraic constraint into a proof of prime existence would require additional input, potentially from sieve theory or character sum estimates.

4 Discrete Wronskian Volume and Radical Compression

4.1 Definition

To quantify the multiplicative structure of prime-free subsequences, we introduce the following measurement.

Definition 4.1 (Discrete Wronskian compression)**.** Let $C_1, C_2, \ldots, C_k$ be a maximal sequence of consecutive composite numbers contained in $\mathcal{I}_n$. The *discrete Wronskian compression ratio* of this sequence is

$$q_W = \frac{\displaystyle\sum_{i=1}^{k} \log C_i}{\log \operatorname{rad}\left(\displaystyle\prod_{i=1}^{k} C_i\right)} = \frac{\log\left(\prod C_i\right)}{\log \operatorname{rad}\left(\prod C_i\right)}. \tag{3}$$

This ratio measures how much the prime factorizations of the composites "overlap": shared prime factors reduce the radical relative to the product.

Remark 4.2. If all C_i were squarefree and pairwise coprime, then $\operatorname{rad}(\prod C_i) = \prod C_i$ and $q_W = 1$. Values $q_W > 1$ indicate nontrivial sharing of prime factors among the composites.

4.2 Experimental results

For each target n, we located the longest maximal prime-free sequence within $\mathcal{I}_n$ and computed its Wronskian compression.

Table 1: Discrete Wronskian compression of maximal prime vacuums in Legendre intervals.

n	Max gap length	log(Volume)	log(Radical)	q_W
100	27	248.64	179.26	1.3871
500	39	484.68	371.44	1.3049
1,000	55	759.78	607.50	1.2507
10,000	103	1897.32	1546.25	1.2270
100,000	173	3983.47	3318.88	1.2002
200,000	247	6029.80	5006.12	1.2045

4.3 Observations

(O1) Stabilization of q_W near 1.20. As n increases across six orders of magnitude (from 10^2 to 2×10^5), the Wronskian compression ratio decreases monotonically and stabilizes in the range 1.20–1.21 (Table 1). This is far below the individual Szpiro threshold $\sigma = 6$ and even below the squarefree baseline $\sigma = 3/2$.

(O2) Sub-logarithmic gap growth. The maximal gap length grows as approximately $k_{\max} \sim (\log n)^2$ (consistent with Cramér's conjecture), while the compression ratio *decreases*. This means longer gaps do *not* lead to more compressed radicals; rather, longer sequences of composites incorporate *more* distinct prime factors, keeping the radical large.

(O3) Self-regulation. The stabilization of q_W suggests a self-regulating mechanism: the natural distribution of primes prevents the formation of long composite sequences whose collective radical is highly compressed. This is consistent with the heuristic that "the primes are as regularly distributed as possible, subject to divisibility constraints" (cf. the Cramér model [5]).

4.4 Comparison with the spin asymmetry

The Spin Asymmetry Theorem (Section 2) provides an *algebraic* structural constraint on Legendre intervals, while the Wronskian compression provides a *multiplicative* constraint. These two constraints operate on different axes:

- **Algebraic axis:** The Legendre symbol distribution is rigidly asymmetric, with $N^- = N^+ + 1$.
- **Multiplicative axis:** The radical of consecutive composites is bounded from below, with q_W converging to ≈ 1.20.

A proof of Legendre's Conjecture via this framework would require showing that these two constraints are *jointly incompatible* with the absence of primes.

5 Discussion

5.1 What is proven vs. what is observed

To maintain clarity, we distinguish sharply between proven results and empirical observations:

Proven (Theorem 2.5): Whenever $p = 2n - 1$ is prime, the interior of the Legendre interval has exactly one more quadratic non-residue than quadratic residue modulo p. This is an unconditional algebraic identity.

Observed (Table 1): The Wronskian compression of maximal prime vacuums stabilizes near $q_W \approx 1.20$. This is an empirical observation, not a theorem.

Conjectured: The combination of algebraic rigidity and multiplicative self-regulation provides an obstruction to the existence of prime-free Legendre intervals. Formalizing this obstruction remains an open problem.

5.2 Relation to character sum methods

The Spin Asymmetry Theorem is closely related to classical character sum estimates. The excess of non-residues over residues in an interval is measured by

$$\sum_{a \in \mathcal{I}_n^\circ} \left(\frac{a}{p}\right) \;=\; N^+ - N^- \;=\; -1.$$

This is a *complete* character sum (over a full set of $p-1$ consecutive integers), which is why it evaluates exactly. Incomplete character sums over shorter sub-intervals of $\mathcal{I}_n$ are governed by the Pólya–Vinogradov inequality and its refinements [6], and connecting our result to these bounds is a natural direction for future work.

5.3 Open questions

(1) *Non-prime lengths.* When $2n-1$ is composite, the residue analysis modulo $2n-1$ becomes more complex (the Jacobi symbol replaces the Legendre symbol, and the symmetry of QR/NR breaks down). Can a useful structural theorem be obtained in this case?

(2) *Joint constraints.* Can the algebraic constraint (spin asymmetry) and the multiplicative constraint (Wronskian stabilization) be combined into a single obstruction that rigorously excludes prime vacuums?

(3) *Character sum refinement.* The global identity $\sum \left(\frac{a}{p}\right) = -1$ is exact but "diffuse" (it sums over the whole interval). Do partial sums over sub-intervals of $\mathcal{I}_n$ exhibit additional structure beyond Pólya–Vinogradov?

(4) *Higher-order residue symbols.* Does the cubic or quartic residue symbol distribution over $\mathcal{I}_n^\circ$ exhibit analogous asymmetries?

Data and code availability

All source code, experimental data, and the LaTeX manuscript are available at `https://github.com/Ruqing1963/legendre-spin-asymmetry`.

References

[1] R. Chen, "Conductor incompressibility for Frey curves associated to prime gaps: rigidity obstructions to the Wiles paradigm in additive prime number theory," Zenodo, 2026. `https://zenodo.org/records/18682375`

[2] R. Chen, "On Landau's fourth problem: conductor rigidity and Sato–Tate equidistribution for the n^2+1 family," Zenodo, 2026. `https://zenodo.org/records/18683712`

[3] R. Chen, "The 2-2 coincidence: conductor rigidity for primes in arithmetic progressions and the Bombieri–Vinogradov barrier," Zenodo, 2026. `https://zenodo.org/records/18684151`

[4] R. Chen, "The geometry of prime vacuums: Legendre's conjecture in function fields via monodromy and Chebotarev density," Zenodo, 2026.

[5] H. Cramér, "On the order of magnitude of the difference between consecutive prime numbers," *Acta Arith.* **2** (1936), 23–46.

[6] G. Pólya, "Über die Verteilung der quadratischen Reste und Nichtreste," *Gött. Nachr.* (1918), 21–29; I. M. Vinogradov, "On a general theorem concerning the distribution of the residues and non-residues of powers," *Trans. Amer. Math. Soc.* **29** (1927), 209–217.