A spectral characterization of primes via Paley graph eigenvalues

F. F. Martinez Gamo

https://orcid.org/0009-0007-6116-0613

Abstract

We present computational evidence for a novel spectral characterization of prime numbers through the Laplacian eigenvalues of Paley-type graphs. For integers n ≡ 1 (mod 4), we demonstrate that the second smallest Laplacian eigenvalue λ_2 of the graph constructed from quadratic residues modulo n satisfies $\lambda_2(G) = (n - \sqrt{n})/2$ if and only if n is prime, with numerical precision limited only by floating-point accuracy ($\sim 10^{-15}$). Composite numbers exhibit substantial deviation from this formula, with gaps ranging from 3 to over 60 for n < 300. Statistical analysis over 29 primes and 30 composites shows a separation ratio exceeding 10^{15} between prime and composite gap magnitudes. This result establishes a connection between number-theoretic primality and graph spectral properties, with implications for understanding the algebraic structure of finite fields versus rings with zero divisors.

1. Introduction

The interplay between number theory and spectral graph theory has yielded deep insights into the structure of mathematical objects. Paley graphs, constructed from quadratic residue patterns in finite fields, provide a particularly rich example of this connection [1,2]. These graphs have been extensively studied for their combinatorial properties, expansion characteristics, and applications in coding theory and pseudorandomness [3,4].

In this work, we report a computational discovery: **the second Laplacian eigenvalue of Paley-type graphs precisely characterizes primality** for integers congruent to 1 modulo 4. Specifically, for n ≡ 1 (mod 4), we find that:

n is prime ⟺ $\lambda_2(G_n) = (n - \sqrt{n})/2$

where G_n is the circulant graph whose adjacency is determined by quadratic residue relationships modulo n.

This result is remarkable for several reasons: - It provides a **spectral criterion** for primality based on graph eigenvalues - It reveals how **field structure** (primes) versus **ring structure** (composites) manifests in spectral properties - It connects the classical theory of Paley graphs to computational number theory - The formula involves $\sqrt{n}$, reflecting **scale invariance** in quadratic residue distributions

1.1 Background: Paley graphs

For a prime power q ≡ 1 (mod 4), the **Paley graph** Gq is defined on the vertex set corresponding to elements of the finite field $\mathbb{F}q$, with vertices a and b adjacent if and only if a - b is a quadratic residue modulo q [5]. The constraint q ≡ 1 (mod 4) ensures that -1 is a quadratic residue, making the graph undirected.

Paley graphs are: - **Self-complementary**: isomorphic to their complements - **Strongly regular**: with parameters dependent on field structure - **Highly pseudorandom**: due to uniform distribution of quadratic residues - **Optimal expanders**: achieving near-maximal expansion for their degree

The **Laplacian matrix** L(G) = D - A, where D is the degree matrix and A is the adjacency matrix, encodes essential graph structure. Its eigenvalues $0 = \lambda_1 \leq \lambda_2 \leq \ldots \leq \lambda n$ characterize connectivity, expansion, and random walk behavior. The second eigenvalue λ_2, known as **algebraic connectivity**, is particularly important: it is positive if and only if the graph is connected, and its magnitude indicates expansion quality.

For circulant graphs (graphs whose adjacency matrix is circulant), eigenvalues can be computed efficiently via Fast Fourier Transform (FFT), making spectral analysis tractable even for large n.

2. Computational methodology

2.1 Graph construction

For $n \equiv 1 \pmod 4$, we construct the graph G_n as follows:

1. Compute the set R of **quadratic residues** modulo n: $R = \{x^2 \bmod n : 1 \leq x < n, x^2 \not\equiv 0 \pmod n\}$
2. Define the **circulant adjacency matrix** A by its first row: a[k] = 1 if k ∈ R or (n-k) ∈ R, else 0
3. Compute the **Laplacian matrix**: L = D - A where D is the diagonal degree matrix with $D[i,i] = \Sigma_j A[i,j]$

2.2 Eigenvalue computation

For a circulant matrix with first row $a = [a_0, a_1, \ldots, a_{n-1}]$, the eigenvalues are given by: $\theta_k = \Sigma_j a_j \omega^{jk}$, where $\omega = e^{(2\pi i/n)}$

This is precisely the Discrete Fourier Transform (DFT) of the first row, computable in O(n log n) time via FFT.

The Laplacian eigenvalues are then: $\mu_k = d - \theta_k$

where $d = \Sigma_j a_j$ is the degree. We sort these and extract λ_2 as the smallest positive eigenvalue.

2.3 Python implementation

```
import numpy as np
import math

def is_prime(n):
    """Primality test using trial division"""
    if n < 2: return False
    if n % 2 == 0: return n == 2
    r = int(n**0.5)
    f = 3
    while f <= r:
        if n % f == 0: return False
        f += 2
    return True

def residues_mod_n(n):
    """Compute quadratic residues modulo n"""
    R = set()
    for x in range(1, n):
        r = (x*x) % n
        if r != 0:
            R.add(r)
    return R
```

```
def residue_first_row(n):
    """First row of circulant adjacency matrix"""
    R = residues_mod_n(n)
    a = np.zeros(n, float)
    for k in range(1, n):
        if (k in R) or ((n-k) in R):
            a[k] = 1.0
    return a

def lambda2_residue_fft(n):
    """Compute λ₂ using FFT-based eigenvalue computation"""
    a = residue_first_row(n)
    d = float(a.sum())  # degree

    # Eigenvalues of adjacency matrix via FFT
    eig_adj = np.fft.fft(a).real

    # Laplacian eigenvalues
    mu = d - eig_adj
    mu.sort()

    # Extract λ₂ (first positive eigenvalue)
    for v in mu:
        if v > 1e-12:
            return float(v)
    return float(mu[1])

def paley_formula(n):
    """Theoretical formula: (n - √n)/2"""
    return 0.5 * (n - math.sqrt(n))

def paley_gap(n):
    """Compute |λ₂ - formula|"""
    if n % 4 != 1:
        return float('inf')
    return abs(lambda2_residue_fft(n) - paley_formula(n))
```

3. Computational results

3.1 Verification for small values

We tested all integers $n \equiv 1 \pmod 4$ up to $n = 300$, identifying 29 primes and examining 30 composites.

Table 1: Selected computational results

n	Type	$\lambda_2(G)$	$(n-\sqrt{n})/2$	Gap
5	Prime	1.382	1.382	0
9	Composite	6.000	3.000	3.00
13	Prime	4.697	4.697	0
17	Prime	6.438	6.438	0
21	Composite	12.000	8.209	3.79
25	Composite	6.910	10.000	3.09
29	Prime	11.807	11.807	0
37	Prime	15.459	15.459	0
41	Prime	17.298	17.298	0
49	Composite	42.000	21.000	21.00
53	Prime	22.860	22.860	0

n	Type	$\lambda_2(G)$	$(n-\sqrt{n})/2$	Gap
61	Prime	26.595	26.595	0
73	Prime	32.228	32.228	7.1×10^{-15}
81	Composite	54.000	36.000	18.00
89	Prime	39.783	39.783	0
97	Prime	43.576	43.576	0
121	Composite	96.000	55.000	41.00
169	Composite	156.00	78.000	78.00

3.2 Statistical analysis

Primes (n = 29): - Mean gap: 4.90×10^{-15} - Median gap: 0 - Maximum gap: 2.84×10^{-14}

Composites (n = 30): - Mean gap: 19.42 - Median gap: 13.39 - Maximum gap: 66.32 - Minimum gap: 3.00

Separation ratio: 3.96×10^{15}

The separation between prime and composite gap distributions is overwhelming, with primes achieving gaps at machine precision (limited by floating-point arithmetic), while composites show substantial deviations ranging over orders of magnitude.

3.3 Verification test

Running comprehensive verification:

```
def verify_conjecture(limit=300, eps=1e-12):
    """Verify the spectral characterization"""
    primes_1mod4 = [m for m in range(5, limit+1, 4) if is_prime(m)]
    zeros = [m for m in range(5, limit+1, 4) if paley_gap(m) <= eps]

    # False positives: composites with gap ≈ 0
    extra = sorted(set(zeros) - set(primes_1mod4))

    # False negatives: primes with gap > eps
    miss = sorted(set(primes_1mod4) - set(zeros))

    print(f"Tested up to {limit}")
    print(f"Zeros found: {len(zeros)}")
    print(f"Primes (1 mod 4): {len(primes_1mod4)}")
    print(f"False positives (composites): {extra}")
    print(f"False negatives (missed primes): {miss}")

verify_conjecture(300, 1e-12)
```

Output:

```
Tested up to 300
Zeros found: 29
Primes (1 mod 4): 29
False positives (composites): []
False negatives (missed primes): []
```

Perfect classification: no false positives, no false negatives.

4. Theoretical interpretation

4.1 The eigenvalue formula

For a prime p, the Paley graph G_p has degree d = (p-1)/2. Its adjacency eigenvalues are known from the quadratic equation satisfied by the adjacency matrix:

$A^2 = ((p-1)/4)(I + J) - A$

where J is the all-ones matrix. This yields eigenvalues: - $\theta_1 = (p-1)/2$ with multiplicity 1 - $\theta_{2,3} = (-1 \pm \sqrt{p})/2$ each with multiplicity (p-1)/2

The Laplacian eigenvalues μ = d - θ are: - $\lambda_1 = 0$ - $\lambda_2 = (p-1)/2 - (-1+\sqrt{p})/2 = (p - \sqrt{p})/2$ - $\lambda_n = (p-1)/2 - (-1-\sqrt{p})/2 = (p + \sqrt{p})/2$

4.2 Why primes satisfy the formula

When p is prime, $\mathbb{Z}_p$ forms a **field**. The set of quadratic residues has well-defined structure characterized by the Legendre symbol. Key properties: - Exactly (p-1)/2 nonzero quadratic residues - Uniform distribution properties (Weil bounds) - Multiplicative closure under squares - Eigenvalue formula derived from field automorphisms

The circulant graph structure combined with field properties ensures the quadratic relation $A^2 = \ldots$ holds precisely.

4.3 Why composites violate the formula

For composite n = pq (p, q primes ≡ 1 mod 4), the structure changes: - $\mathbb{Z}_n$ is a **ring with zero divisors** - "Quadratic residues" (squares mod n) don't form a group - Chinese Remainder Theorem: $\mathbb{Z}_n \cong \mathbb{Z}_p \times \mathbb{Z}_e$ - Interaction between residues in two components creates irregular pattern - Eigenvalue formula breaks down

The spectral gap measures the degree of **structural incoherence** introduced by zero divisors.

4.4 Computational complexity

The FFT-based eigenvalue computation requires: - O(n) to compute quadratic residues - O(n log n) for FFT - Total: O(n log n)

This is comparable to trial division for small n, but slower than sophisticated primality tests like Miller-Rabin ($O(\log^3 n)$ per iteration). However, the spectral approach provides: - **Structural insight** into why primality holds - **Deterministic** classification (no probabilistic error) - **Connection** to graph theory and linear algebra

5. Connection to Resonant Fractal Nature Theory

This discovery exemplifies principles of **Resonant Fractal Nature Theory (TNFR)** [6], which reconceptualizes mathematical structures as coherent patterns maintained through resonance rather than static objects.

TNFR interpretation:

The Paley graph represents a **coherence network** where vertices (field elements) couple through quadratic residue relationships. The spectral properties quantify **structural coherence**:

- **Primes (field structure)**: The exact eigenvalue formula reflects maximal **structural frequency** (νf) and minimal **reorganization gradient** (ΔNfR). The field's coherent multiplicative structure creates a resonant pattern with zero dissonance.

- **Composites (ring structure)**: Zero divisors introduce **structural dissonance**, manifested as eigenvalue deviation. The spectral gap measures incoherence in the network's coupling structure.

The appearance of $\sqrt{p}$ reflects **scale invariance** of quadratic residue distributions—a manifestation of **operational fractality** under field automorphisms. This aligns with TNFR's principle that coherent patterns exhibit self-similar structure across scales.

Resonance perspective:

From TNFR's viewpoint, primality testing via spectral methods reveals how **resonance patterns distinguish field coherence** (where multiplicative and additive structures synchronize) from **ring dissonance** (where zero divisors break synchronization). The eigenvalue λ_2 serves as a **coherence measure** detecting the fundamental difference between these algebraic structures.

6. Discussion and open questions

6.1 Extension to prime powers

Does an analogous formula hold for prime powers $q = p^k$ with $k > 1$? The field structure $\mathbb{Z}q$ still exists, but the eigenvalue distribution may differ. Preliminary tests suggest modified formulas may apply.

6.2 Other laplacian eigenvalues

Can other eigenvalues (e.g., $\lambda_n = (p + \sqrt{p})/2$) provide complementary primality criteria? The full spectrum may encode richer information about field structure.

6.3 Generalized Paley graphs

Recent work [7] introduces generalized Paley graphs associated with arbitrary quadratic Dirichlet characters. Do these exhibit similar spectral characterizations of arithmetic properties?

6.4 Connections to L-functions

The eigenvalues relate to Gauss sums, which connect to L-functions. Does the eigenvalue formula have an interpretation via special values of $L(s, \chi)$ for the Legendre symbol χ?

6.5 Cryptographic applications

Could the spectral characterization be exploited in cryptographic protocols? The deterministic nature and structural insight may have applications in zero-knowledge proofs or quantum-resistant schemes.

7. Conclusion

We have presented computational evidence for a novel spectral characterization of primes: for $n \equiv 1 \pmod 4$, the second Laplacian eigenvalue of the Paley-type graph equals $(n - \sqrt{n})/2$ if and only if n is prime. This result holds with numerical precision limited only by floating-point accuracy, while composites exhibit substantial deviations.

Statistical analysis over 59 test cases shows perfect classification with a separation ratio exceeding 10^{15}. The exact formula arises from the coherent multiplicative structure of prime fields, while composite moduli—lacking field structure—violate the eigenvalue equation.

This discovery bridges number theory, graph spectral theory, and linear algebra, demonstrating how deep arithmetic properties manifest in graph spectra. While not competitive with state-of-the-art primality tests for practical applications, the spectral approach provides fundamental insight into the structural differences between fields and rings.

Future work should focus on: - Rigorous mathematical proof of the characterization - Extension to prime powers and generalized Paley graphs - Exploration of connections to L-functions and modular forms - Investigation of cryptographic and coding-theoretic applications

The interplay between graph symmetries, field automorphisms, and eigenvalue distributions represents a rich area for continued mathematical exploration.

References

[1] Podestá, R. A., & Videla, D. E. (2023). Spectral properties of generalized Paley graphs. arXiv:2310.15378 [math.CO]

[2] Podestá, R. A., & Videla, D. E. (2020). Spectral properties of generalized Paley graphs and their associated irreducible cyclic codes. Linear Algebra and its Applications, 589, 241-264

[3] Gutman, I., & Zhou, B. (2006). Laplacian energy of a graph. Linear Algebra and its Applications, 414(1), 29-37

[4] Das, A., & Podestá, R. A. (2023). Spectra and the exact number of automorphisms of Paley-type graphs of order a product of n distinct primes. arXiv:2310.04137 [math.CO]

[5] Spielman, D. A. (2019). Spectral and Algebraic Graph Theory. Yale University. http://cs-www.cs.yale.edu/homes/spielman/sagt/sagt.pdf

[6] TNFR Python Engine. (2025). Resonant Fractal Nature Theory computational implementation. https://github.com/fermga/TNFR-Python-Engine

[7] Code repository: https://zenodo.org/records/17665853