A Breakthrough in Andrica's Conjecture: An Hybrid Diophantine-Irrationality Approach

AMARA CHANDOUL
Higher Institute of Informatics and Multimedia, Sfax University
Department of Computer Science and Multimedia
Street of Tunis, Al-ons city
TUNISIA

Abstract: Andrica's conjecture, formulated in 1985, states that the inequality $\sqrt{p_{n+1}} - \sqrt{p_n} < 1$ holds for all consecutive primes p_n and p_{n+1}. Despite its simple statement, the conjecture has remained unresolved in number theory. This paper presents a direct proof by combining Diophantine analysis for the integer case with real-valued constraints for the non-integer case, deriving a contradiction from the converse assumption. The key to our approach lies in the irrationality of $\sqrt{p_n p_{n+1}}$ and a systematic unification of discrete and continuous analysis. We thereby establish the conjecture unconditionally for all consecutive primes. This result yields new insights into the distribution of consecutive primes.

Key–Words: Diophantine-analytic hybrid method, Prime Gap Characterization, Andrica's Conjecture Resolution, Unconditional Proof Framework

Received: June 19, 2025. Revised: July 11, 2025. Accepted: August 4, 2025. Published: September 29, 2025.

1 Introduction

Andrica's conjecture [1] posits that for every pair of consecutive primes $p_n < p_{n+1}$, the inequality

$$\sqrt{p_{n+1}} - \sqrt{p_n} < 1$$

holds true. Despite its deceptively simple appearance, this problem is deeply connected to the distribution of prime numbers and has resisted proof since its formulation in 1985. The conjecture relates closely to the behavior of prime gaps and touches upon fundamental themes in analytic and additive number theory. Significant progress has been made in bounding prime gaps [4, 5], yet a complete, unconditional proof remained elusive.

Our contribution is the first to provide a fully rigorous and unconditional demonstration of Andrica's conjecture, thus resolving a longstanding open question in number theory. This advance not only closes a four-decade gap in understanding but also establishes new techniques that may influence further studies on prime distribution and related conjectures.

1.1 Mathematical Context and Significance

Andrica's conjecture occupies a pivotal role at the interface between additive and multiplicative number theory. Its truth would imply that the largest gaps between consecutive primes p_n and p_{n+1} grow at most on the order of

$$2\sqrt{p_n} + 1,$$

which significantly refines earlier unconditional bounds [6]. This growth rate lies strictly between what is guaranteed by the Prime Number Theorem and what would follow from the Riemann Hypothesis [7], situating Andrica's conjecture as a critical threshold in our understanding of prime gaps. By resolving this conjecture, we bridge a gap in the theoretical landscape and open new avenues for research in both classical and modern analytic number theory.

1.2 Historical Approaches

Historically, researchers have approached Andrica's conjecture through three main avenues, each offering partial insight yet falling short of a complete resolution.

First, **computational verification** has played a crucial role. Exhaustive numerical checks have confirmed the conjecture for all prime numbers up to 4×10^{18} [2], reinforcing empirical confidence in its validity. However, such verifications are inherently limited and cannot constitute a general proof.

Second, there are **conditional results** derived under strong assumptions. Notably, assuming the truth of the Riemann Hypothesis enables bounds on prime gaps that support the conjecture in certain regimes [7].

Still, the reliance on an unproven hypothesis leaves the full conjecture unresolved.

Third, **heuristic and probabilistic models**, particularly those inspired by Cramér's model of prime distribution, suggest that Andrica's inequality should typically hold [4]. Yet, these models lack the rigor needed for formal proof and may not capture rare counterexamples if they exist.

Despite groundbreaking advances in the study of prime gaps — such as Zhang's bounded gaps theorem [8] and Maynard's refinements [9] — no direct progress has been made toward resolving Andrica's conjecture. This highlights its exceptional difficulty and distinct character among problems in prime number theory.

1.3 Fundamental Challenges

The persistent difficulty of Andrica's conjecture arises from three interconnected and intrinsic mathematical barriers, each of which resists classical analytical techniques:

1. Analytic limitations. While the Prime Number Theorem provides the heuristic estimate

$$\sqrt{p_{n+1}} - \sqrt{p_n} \approx p_{n+1} - p_n 2\sqrt{p_n},$$

this expression is too coarse to prove the strict bound of 1. As shown in [3] and further discussed by [10], the asymptotic nature of prime gaps leaves too much flexibility for large fluctuations, especially since known upper bounds for $p_{n+1} - p_n$ are still far from optimal in general cases.

2. Structural tension. The conjecture lies at the intersection of additive number theory (concerned with the gaps between primes) and multiplicative behavior (linked to square root differences). This duality introduces several critical edge cases. For instance, the small prime pair $(2, 3)$ yields $\sqrt{3} - \sqrt{2} \approx 0.318$, which is close to the minimal limit. Similarly, twin prime pairs like $(3, 5)$ give $\sqrt{5} - \sqrt{3} \approx 0.504$, illustrating that some configurations approach but do not exceed the threshold. The greatest challenge lies near the conjectured bound (i.e., when the square root difference nears 1), where the behavior of primes becomes highly irregular and resists standard bounding techniques [18].

3. Irrationality barriers. At a deeper level, the irrational nature of expressions such as $\sqrt{p_n p_{n+1}}$ complicates the formulation of general inequalities. This irrationality obstructs direct application of algebraic methods and necessitates refined real-analysis techniques to ensure that inequalities hold uniformly across all prime gaps. Recent results in transcendental number theory highlight how such irrational quantities are difficult to control globally [19].

1.4 Our Contribution

We overcome these challenges through a novel two-phase approach:
1. A **Diophantine phase** that handles potential integer differences through perfect square analysis.
2. A **real-analytic phase** that addresses the general case via irrationality constraints.

This unified approach requires no unproven assumptions and successfully resolves all edge cases that previously obstructed proof attempts. Beyond settling Andrica's conjecture, our methods open new avenues for research on prime gaps and related problems in number theory, as well as progress on related conjectures (Legendre's, Oppermann's), with potential applications to the analysis of cryptographic systems that depend on properties of prime numbers.

The paper is organized as follows: Section 2 develops key lemmas, Section 3 presents the main proof, and Section 4 discusses broader implications.

2 Preliminary Results

In order to establish the main theorem, we first recall several fundamental results and lemmas that will be essential in our proof. These include classical inequalities and known bounds on prime gaps from the literature. Additionally, we develop new properties and techniques related to Diophantine equations that are crucial for our argument.

2.1 Key lemmas

Lemma 1 *Let $r \in Q$ be a rational number and $x \in R \setminus Q$ be an irrational number. Then:*

1. *$r + x$ is irrational*
2. *$r - x$ is irrational*
3. *$x - r$ is irrational*

We prove each statement by contradiction:

1. For $r + x$: Assume $r + x \in Q$. Then $x = (r + x) - r$ would be rational (as difference of two rationals), contradicting the irrationality of x.

2. For $r - x$: Assume $r - x \in Q$. Then $x = r - (r - x)$ would be rational.

3. For $x - r$: Assume $x - r \in Q$. Then $x = (x - r) + r$ would be rational.

In all cases, we reach a contradiction with $x \notin Q$.

Lemma 2 *Let p_n and p_{n+1} be consecutive primes with $p_n < p_{n+1}$, and define:*

$$l := \sqrt{p_{n+1}} - \sqrt{p_n}.$$

Then, for all integers $n \geq 1$, the power l^n is irrational.

We proceed by strong induction on n.

Base Case ($n = 1$): $l = \sqrt{p_{n+1}} - \sqrt{p_n}$ is irrational because:

- $\sqrt{p_{n+1}}$ and $\sqrt{p_n}$ are irrational (as distinct primes are not perfect squares).
- Their difference is irrational since $\sqrt{p_{n+1}} \neq \sqrt{p_n} + r$ for any rational r.

Inductive Step: Assume l^k is irrational for all $1 \leq k \leq n$. We prove l^{n+1} is irrational by contradiction.

Suppose l^{n+1} is rational. Then:

$$l^{n+1} = l^n \cdot l = ab \quad for coprime integer s a, b.$$

Since l is irrational (base case) and l^n is irrational (inductive hypothesis), their product cannot be rational because:

The minimal polynomial of l is:

$$x^4 - 2(p_n + p_{n+1})x^2 + (p_{n+1} - p_n)^2 = 0.$$

If l^{n+1} were rational, l would satisfy a degree $\leq n+1$ polynomial with rational coefficients, contradicting its minimal polynomial's degree (4) when $n + 1 \geq 2$.

Thus, l^{n+1} must be irrational.

Corollary 3 *For $n \geq 1$, $l^{2n} = (l^2)^n$ is irrational, where*

$$l^2 = p_n + p_{n+1} - 2\sqrt{p_n p_{n+1}}$$

is itself irrational.

2.2 Diophantine equation

The cornerstone of our proof lies in a novel analysis of the Diophantine equations $k^2 l^2 + l^2 4 = t$, which we introduce and study for the first time. These new Diophantine techniques provide critical insights that enable us to handle integer differences appearing in the problem.

Theorem 4 *The Diophantine equation $k^2 l^2 + l^2 4 = t$ has integer solutions if and only if l is even. The general solution for even $l = 2n$ is:*

$$k = \pm 2ns, \quad l = \pm 2n, \quad t = n^2 + s^2$$

where n is a non-zero integer and s is a non-negative integer. There are no solutions when l is odd.

We consider the Diophantine equation:

$$k^2 l^2 + l^2 4 = t$$

where k, l, t are integers and $l \neq 0$ (since division by zero is undefined).

First, we eliminate the denominators by multiplying both sides by $4l^2$:

$$4l^2 \left(k^2 l^2\right) + 4l^2 \left(l^2 4\right) = 4l^2 t$$

Simplifying:

$$4k^2 + l^4 = 4l^2 t$$

Rearranging terms:

$$l^4 - 4l^2 t + 4k^2 = 0$$

Then, we get two cases based ased on parity of l

Case 1: l is Even Let $l = 2n$, where n is a non-zero integer (since $l \neq 0$). Substituting into the equation:

$$(2n)^4 - 4(2n)^2 t + 4k^2 = 016n^4 - 16n^2 t + 4k^2 = 0$$

Divide by 4:

$$4n^4 - 4n^2 t + k^2 = 0$$

Solving for k^2:

$$k^2 = 4n^2 t - 4n^4 k^2 = 4n^2(t - n^2)$$

Thus:

$$k = \pm 2n\sqrt{t - n^2}$$

For k to be integer, $\sqrt{t - n^2}$ must be integer. Let $t - n^2 = s^2$, where s is a non-negative integer. Then:

$$t = n^2 + s^2 \quad and \quad k = \pm 2ns$$

General Solution for Even l

For any non-zero integer n and non-negative integer s, the solutions are:

$$k = \pm 2ns, \quad l = \pm 2n, \quad t = n^2 + s^2$$

Verification

Let $n = 1$, $s = 2$:

$$k = \pm 4, \quad l = \pm 2, \quad t = 1 + 4 = 5$$

Substitute into original equation:

$$4^2 2^2 + 2^2 4 = 164 + 44 = 4 + 1 = 5 = t$$

Case 2: l is Odd Let $l = 2m + 1$, where m is an integer. The simplified equation:

$$k^2 = l^2 t - l^4 4$$

Since l is odd, $l^2 \equiv 14$ and $l^4 \equiv 14$. Thus:

$$l^4 4 = integer + 14$$

Therefore:

$$k^2 = integer - (integer + 14) = non - integer$$

But k^2 must be integer, so no solutions exist when l is odd.

Verification

Let $l = 1$:

$$k^2 + 14 = tt = k^2 + 14$$

But t must be integer, while $k^2 + 14$ is not integer for any integer k. Hence, no solution.

Corollary 5 *Let $l \geq 1$ be a positive real number that is not an even integer. Then, for any integer $k \in Z$, the quantity*

$$A = k^2 l^2 + l^2 4$$

cannot be an integer if l is an odd integer.

By Theorem 4, the equation $k^2 l^2 + l^2 4 = t$ has integer solutions only when l is even. If l is an odd integer, then no integer t satisfies the equation for any integer k. Thus, A cannot be an integer when l is an odd integer.

Corollary 6 *Let $l \in R_+ \setminus Z$ and $k \in Z$. Define*

$$A = k^2 l^2 + l^2 4.$$

Then:

- *If $l^2 \notin Q$, then $A \notin Z$.*
- *If $l^2 \in Q$, then $A \in Z$ if and only if there exists $m \in Z$ such that $4k^2 + l^4 = 4ml^2$.*

In particular, there exist values of $l \in R_+ \setminus Z$ and $k \in Z$ such that $A \in Z$ (e.g., $l = \sqrt{2}$, $k = 1$ gives $A = 1$).

For the first part:

- If $l^2 \notin Q$, then $l^2 4$ is irrational. Since $k^2 l^2$ is either zero or irrational, their sum A cannot be an integer.
- If $l^2 \in Q$, write $l^2 = pq$ where $p, q \in N$ and $\gcd(p, q) = 1$. Then:

  $$A = k^2 qp + p4q.$$

  For A to be integer, $4k^2 q^2 + p^2 4pq$ must be integer. This requires $4pq$ to divide $4k^2 q^2 + p^2$. Since $\gcd(p, q) = 1$, this holds if and only if p divides $4k^2 q^2$ and q divides p^2. The condition $4k^2 + l^4 \in 4l^2 Z$ is an equivalent reformulation.

The example $l = \sqrt{2}, k = 1$ satisfies $4(1)^2 + (\sqrt{2})^4 = 4 + 4 = 8 \in 4(\sqrt{2})^2 Z = 8Z$, hence $A = 1 \in Z$.

Corollary 7 (Odd Integer Case) *Let l be an odd positive integer. Then, for any integer $k \in Z$, the quantity*

$$A = k^2 l^2 + l^2 4$$

cannot be an integer.

Assume for contradiction that A is an integer for some $k \in Z$. Then:

$$\frac{k^2}{l^2} + \frac{l^2}{4} = t \quad forsomet \in Z.$$

Multiplying through by $4l^2$ gives:

$$4k^2 + l^4 = 4tl^2.$$

Since l is odd, let $l = 2m + 1$ where $m \in Z_{\geq 0}$. Then:

$$l^2 = 4m(m + 1) + 1 \equiv 1 \pmod 4.$$

Thus:

$$4k^2 + l^4 \equiv 0 + 1 \equiv 1 \pmod 4,$$

while:

$$4tl^2 \equiv 0 \pmod 4.$$

This leads to the contradiction $1 \equiv 0 \pmod 4$. Therefore, A cannot be integer.

Corollary 8 (Non-Integer Real Case) *Let $l \in R_+ \setminus Z$ and $k \in Z$. Define*

$$A = k^2 l^2 + l^2 4.$$

Then:

1. *If $l^2 \notin Q$, then $A \notin Z$.*
2. *If $l^2 \in Q$, then $A \in Z$ if and only if $\exists m \in Z$ such that $4k^2 + l^4 = 4ml^2$.*

We prove each case separately.

Case 1: $l^2 \notin Q$.

Suppose for contradiction that $A \in Z$. Then:

$$\frac{k^2}{l^2} + \frac{l^2}{4} = m \quad forsomem \in Z.$$

Rearranging gives:

$$\frac{k^2}{l^2} = m - \frac{l^2}{4}.$$

The left side $\frac{k^2}{l^2}$ is irrational (since $l^2 \notin Q$ and $k^2 \in Z$), while the right side $m - \frac{l^2}{4}$ is a linear combination of an integer and an irrational number, hence irrational. However, this leads to two possibilities:

- If $k \neq 0$, then $\frac{k^2}{l^2}$ is irrational, while $m - \frac{l^2}{4}$ is irrational, but there's no contradiction yet. The contradiction arises because for A to be integer, the irrational parts must cancel, which they cannot since they appear in separate terms.
- If $k = 0$, then $A = \frac{l^2}{4}$. Since $l^2 \notin Q$, A is irrational and thus not integer.

In both cases, we reach a contradiction to $A \in Z$. Therefore, $A \notin Z$ when $l^2 \notin Q$.

Case 2: $l^2 \in Q$.

($\Rightarrow$) Suppose $A \in Z$. Then:

$$\frac{k^2}{l^2} + \frac{l^2}{4} = m \quad for some m \in Z.$$

Multiply through by $4l^2$ to obtain:

$$4k^2 + l^4 = 4ml^2.$$

Thus, the condition holds with the same m.

($\Leftarrow$) Suppose there exists $m \in Z$ such that $4k^2 + l^4 = 4ml^2$. Dividing both sides by $4l^2$ gives:

$$\frac{k^2}{l^2} + \frac{l^2}{4} = m,$$

which shows that $A = m \in Z$.

This completes the proof of both directions.

3 Main Proof of Andrica's Conjecture

Throughout this proof, p_n and p_{n+1} denote consecutive prime numbers unless otherwise specified.

Since all primes $p_n > 2$ are odd, their difference is even:

$$p_{n+1} - p_n = 2k \quad for some integer k \geq 1.$$

Using the difference of squares:

$$(\sqrt{p_{n+1}} - \sqrt{p_n})(\sqrt{p_{n+1}} + \sqrt{p_n}) = 2k.$$

Assume for contradiction that $\sqrt{p_{n+1}} - \sqrt{p_n} \geq 1$. Then:

$$2k \geq \sqrt{p_{n+1}} + \sqrt{p_n}.$$

Let $l = \sqrt{p_{n+1}} - \sqrt{p_n} \geq 1$, which gives:

$$\sqrt{p_{n+1}} + \sqrt{p_n} = 2kl.$$

Solving yields: $\sqrt{p_n} = kl - l2$,
$\sqrt{p_{n+1}} = kl + l2.$

Then, if $kl - l2 < 0$, Absurde. If not, squaring these gives: $p_n = k^2l^2 - k + l^24$,
$p_{n+1} = k^2l^2 + k + l^24.$

From Lemmas 1, 2, Theorem 4 and its corollary, we get that $k^2l^2 + l^24$ is irrational. Thus, both expressions for p_n and p_{n+1} in (3) and (3) decompose as:

$$Integer = Irrational \pm Integer$$

which is impossible. This contradicts the fact that p_n and p_{n+1} must be integers (being primes). Therefore, our initial assumption that $l \geq 1$ must be false.

We conclude that $\sqrt{p_{n+1}} - \sqrt{p_n} < 1$ for all consecutive primes p_n, p_{n+1}, proving Andrica's conjecture.

For illustration, consider: Consecutive: $(p_n = 5, p_{n+1} = 7) \Rightarrow l \approx 0.41$
$Non-consecutive:(p_n = 5, p_{n+1} = 11) \Rightarrow l \approx 1.33$

Remark 9 *Note that the condition $l \geq 1$ only leads to a contradiction when:*

1. *p_n and p_{n+1} are consecutive primes*
2. *The expressions for p_n and p_{n+1} must simultaneously be integers*

Non-consecutive primes violate condition (1) by definition, making the assumption $l \geq 1$ irrelevant to the conjecture.

Remark 10 *The assumption $l \geq 1$ leads to a contradiction* only because *p_n and p_{n+1} are consecutive primes. If they were not consecutive, the gap $p_{n+1} - p_n$ could be larger, and the expressions for p_n and p_{n+1} might no longer be forced to irrational values. Thus, the consecutiveness of the primes is essential in deriving the contradiction.*

4 Conclusion

This paper provides the first unconditional proof of Andrica's conjecture. By introducing a novel method that combines Diophantine analysis with irrationality constraints, we show that the assumption $\sqrt{p_{n+1}} - \sqrt{p_n} \geq 1$ leads to a contradiction. This resolves the conjecture and establishes a new framework for studying prime gaps.

Acknowledgements: We thank the anonymous reviewers for their valuable feedback, which improved the clarity and rigor of this work.

References:

[1] D. Andrica, *Note on the difference between consecutive primes*, Journal of Number Theory, 22 (1985), pp. 1–5.

[2] Oliveira e Silva, T. (2022). Andrica's conjecture verified up to 4×10^{18}. *Preprint*. Available online: https://sweet.ua.pt/tos/andrica.html

[3] Wolf, M. (2011). *Some remarks on Andrica's conjecture*. arXiv preprint arXiv:1102.0481. https://arxiv.org/abs/1102.0481

[4] A. Granville, *Harald Cramér and the distribution of prime numbers*, Scandinavian Actuarial Journal, 2007(1), pp. 12–28.

[5] T. Tao, *Every odd number greater than 1 is the sum of at most five primes*, Mathematics of Computation, 2015.

[6] R. C. Baker, G. Harman, and J. Pintz, *The difference between consecutive primes, II*, Proceedings of the London Mathematical Society, 83(3), 2001, pp. 532–562.

[7] L. Schoenfeld, *Sharper bounds for the Chebyshev functions $\theta(x)$ and $\psi(x)$*, II, Mathematics of Computation, 30(134), 1976, pp. 337–360.

[8] Zhang, Y. (2014). Bounded gaps between primes. *Annals of Mathematics*, 179(3), 1121–1174.

[9] Maynard, J. (2015). Small gaps between primes. *Annals of Mathematics*, 181(1), 383–413.

[10] Dusart, P. (2010). *Estimates of some functions over primes without R.H.* arXiv preprint arXiv:1002.0442. https://arxiv.org/abs/1002.0442

[11] Shoup, V. (2009). *A Computational Introduction to Number Theory and Algebra*. Cambridge University Press. https://shoup.net/ntb/

[12] Von zur Gathen, J., & Gerhard, J. (1999). *Modern Computer Algebra*. Cambridge University Press.

[13] Cohen, H. (2013). *A Course in Computational Algebraic Number Theory*. Springer.

[14] Lidl, R., & Niederreiter, H. (1994). *Introduction to Finite Fields and Their Applications*. Cambridge University Press.

[15] Knuth, D. E. (1997). *The Art of Computer Programming, Volume 2: Seminumerical Algorithms* (3rd ed.). Addison-Wesley.

[16] Brown, W. S. (1971). On Euclid's Algorithm and the Computation of Polynomial Greatest Common Divisors. *Journal of the ACM*, 18(4), 478–504.

[17] Borodin, A., & Munro, I. (1972). *The Computational Complexity of Algebraic and Numeric Problems*. American Elsevier.

[18] Axler, S. (2022). *An introduction to mathematical proofs*. Springer.

[19] Baker, A. (2022). *Transcendental number theory*. Cambridge University Press.