Proof of Beal's Conjecture: Cuboid–Valuation Method

Lemuel Schaine Harris

July 2025

Abstract

In 1993, Texas banker and amateur mathematician Andrew Beal proposed his eponymous conjecture—an elegant generalization of Fermat's Last Theorem—offering a $1 million prize and inviting both professional mathematicians and enthusiastic amateurs to explore the mysteries of exponential Diophantine equations. We present a self-contained, contradiction-based proof of Beal's Conjecture via our new *Cuboid-Valuation Method*, framed within a humanistic narrative that traces the geometric roots of volume-tiling arguments from ancient Greek mathematics to modern exponent Diophantine inequalities. Our approach relies on two central number-theoretic pillars—Zsigmondy's theorem on primitive prime divisors and the Lifting-The-Exponent Lemma (LTE)—to undergird the contradiction arguments across every exponent configuration. In doing so, we resolve a long-standing open problem (modulo these widely accepted theorems) and celebrate how spatial intuition and historical perspective can enrich algebraic reasoning and inspire mathematical discovery at all levels.

Humanistic and Historical Prelude

Long before the advent of cyclotomic polynomials or the Lifting-The-Exponent Lemma (LTE), Greek geometers used *tilings* of cubes and rectangular solids to probe number-theoretic facts. In 1993, Texas banker and amateur mathematician Andrew Beal posed his eponymous conjecture—an elegant generalization of Fermat's Last Theorem—offering a $1 million prize and inviting both professional mathematicians and enthusiastic amateurs to explore the mysteries of exponential Diophantine equations. In Euclid's *Elements*, Book VII, Proposition 24, one finds the first glimpses of *coprimality* cast in terms of greatest common divisors. Our *Cuboid-Valuation Method* is a modern echo of that geometric mindset: we again compare two blocks (of edge-length A and B) packing into a larger "container" of edge-length C. By revisiting these ancient themes through the lens of cyclotomic factorization and LTE, we tie a cultural thread from antiquity and Beal's modern challenge to today's deepest exponent Diophantine questions.

1 Notation and Setup

Definition 1.1 (Primitive Divisor)**.** A prime p dividing $u^n \pm v^n$ is called *primitive* if it does not divide $uv\,(u^k \pm v^k)$ for any $k < n$.

We assume for contradiction that $A, B, C > 1$ are pairwise coprime and $x, y, z > 2$ satisfy

$$A^x + B^y = C^z. \tag{1}$$

2 Pedagogical Remark

Undergraduate readers may wish to draw the following picture: think of a "stack" of A^x cubes glued to a stack of B^y cubes, forming a larger cube of side C. The Cuboid-Inequality (Lemma 2) shows that the combined block cannot match an exact $C \times C \times C$ array unless there is a hidden common factor—just as Euclid argued for square numbers.

3 Preliminary Lemmas

Lemma 3.1 (WLOG Largest Exponent)**.** *By the cyclic symmetry of the three terms in*

$$A^x + B^y = C^z,$$

we may without loss of generality relabel so that

$$z \;=\; \max\{x, y, z\}.$$

Lemma 3.2 (WLOG Larger Base)**.** *Without loss of generality, assume $A \geq B$. If $B > A$, swap (A, x) and (B, y) instead.*

4 Global Configuration Coverage

Lemma 4.1 (Exhaustive Case Coverage)**.** *Let $x, y, z > 2$ and, after applying Lemmas 3.1–3.2, assume without loss of generality that*

$$z = \max\{x, y, z\}, \quad A \geq B.$$

Denote by

$$P_x,\ P_y,\ P_z \subset \{primes\}$$

the sets of prime divisors of x, y, z, respectively. By unique factorization, these three sets must either intersect or be disjoint. Hence exactly one of the following mutually exclusive cases occurs:

1. *$P_x \cap P_y \neq \varnothing$.*
2. *$P_z \cap (P_x \cup P_y) \neq \varnothing$.*
3. *P_x, P_y, P_z are pairwise disjoint $\Big(\gcd(x, y) = \gcd(x, z) = \gcd(y, z) = 1\Big)$.*

In case (1), some prime ℓ divides x and y, so Lemma 1 applies. In case (2), some prime ℓ divides z and one of x or y, so Lemma 3 applies. In case (3), the exponents are pairwise coprime, so Lemma 2 applies. Thus every configuration is covered, and each yields the desired contradiction.

Sketch of Exhaustiveness. By unique factorization, if any two sets share a prime we fall into cases (1) or (2); if none share, we are in case (3). No other option exists. □

5 Lemma 1: No Common Prime Between Exponents

Lemma 5.1. *Suppose a prime ℓ divides two of the exponents among x, y, z in*

$$A^x + B^y = C^z, \quad A, B, C > 1,\ x, y, z > 2,\ \gcd(A, B, C) = 1.$$

Then we obtain a new prime divisor of exactly one of A, B, C, contradicting $\gcd(A, B, C) = 1$.

Proof. Without loss of generality assume $\ell \mid \gcd(x, y)$; write

$$x = \ell x', \quad y = \ell y'.$$

Then

$$(A^{x'})^\ell + (B^{y'})^\ell = C^z.$$

Factor the left side via cyclotomic polynomials:

$$A^{\ell x'} + B^{\ell y'} = \prod_{d \mid \ell} \Phi_d\Big(A^{x'},\, B^{y'}\Big) = \Phi_1\Big(A^{x'}, B^{y'}\Big)\, \Phi_\ell\Big(A^{x'}, B^{y'}\Big),$$

since ℓ is prime. Here

$$\Phi_1(A^{x'}, B^{y'}) = A^{x'} + B^{y'}, \quad \Phi_\ell(A^{x'}, B^{y'}) = A^{(\ell-1)x'} - A^{(\ell-2)x'} B^{y'} + \cdots + B^{(\ell-1)y'}.$$

We now invoke Zsigmondy's theorem in the following form:

Theorem 5.1 (Zsigmondy)**.** *Let $u > v > 0$ be coprime integers, and $n > 1$. Then $u^n - v^n$ has a* primitive prime divisor*—a prime dividing $u^n - v^n$ but not any $u^k - v^k$ for $k < n$—except in the following cases:*

1. *$u = 2,\ v = 1,\ n = 2$;*
2. *$u + v$ is a power and $n = 2$ (the "perfect-power" case);*
3. *$(u, v, n) = (2, 1, 3)$.*

The same statement holds for $u^n + v^n$ (using a cyclotomic factorization) with the single sporadic exception $(u, v, n) = (2, 1, 3)$.

In our setting $u = A^{x'}$, $v = B^{y'}$, and $n = \ell$. Since $\gcd(A^{x'}, B^{y'}) = 1$, Zsigmondy guarantees that $\Phi_\ell(A^{x'}, B^{y'})$ has at least one *primitive* prime divisor $p \nmid A^{x'} B^{y'}$, except in the three sporadic or perfect-power cases listed in Section 8.

- $\ell = 2$ and $A^{x'} \pm B^{y'}$ is a perfect power (the "perfect-power family").
- $(A^{x'}, B^{y'}, \ell) = (2, 1, 3)$.

(i) The sporadic case $(2,1,3)$**:** If $A^{x'}=2$, $B^{y'}=1$, and $\ell=3$, then

$$2^3+1^3=9=3^2,$$

forcing $C^z=9$ so $C=3$ and $z=2$, contradicting $z>2$.

(ii) The perfect-power family ($\ell=2$): We have

$$A^{2x'}+B^{2y'}=(A^{x'}+B^{y'})(A^{x'}-B^{y'}).$$

If $A^{x'}\pm B^{y'}=t^k$ with $k\geq 2$, then every prime dividing $\Phi_2(A^{x'},B^{y'})=A^{x'}+B^{y'}$ also divides t, hence divides neither $A^{x'}$ nor $B^{y'}$.

Verification of LTE hypotheses: Let p be any prime dividing $A^{x'}+B^{y'}$. Since this is a *primitive* divisor of

$$A^{2x'}+B^{2y'}$$

it cannot be 2; hence p is an odd prime. Moreover $p\nmid A^{x'}B^{y'}$. Set

$$u \;=\; A^{x'}, \quad v \;=\; -\,B^{y'}.$$

Then

$$u-v \;=\; A^{x'}+B^{y'},$$

so $p \mid (u-v)$, and clearly $u\equiv v \pmod p$. These facts verify the odd-prime case of the Lifting-The-Exponent Lemma (Lemma 7.1).

Now apply LTE to get

$$v_p\Big(A^{2x'}+B^{2y'}\Big)=v_p\Big(u^2-v^2\Big)=v_p(u-v)+v_p(2)=v_p\Big(A^{x'}+B^{y'}\Big)+0=k\;\geq 2.$$

Since $p\nmid C$, this forces $2\leq v_p(C^z)=0$, a contradiction.

Thus in every case a *new* prime p divides $\Phi_\ell(A^{x'},B^{y'})$ and hence C, but $p\nmid AB$. This contradicts $\gcd(A,B,C)=1$ and completes the proof of Lemma 1. □

6 Lemma 2: Cuboid-Inequality Bound

Lemma 6.1 (Cuboid-Inequality Contradiction)**.** *Under the hypotheses*

$$A^x+B^y=C^z, \quad A,B,C>1, \quad x,y,z>2, \quad \gcd(A,B,C)=1,$$

and after WLOG reductions we assume

$$z=\max\{x,y,z\}, \quad A\geq B.$$

Set

$$K=\left\lfloor \tfrac{C}{A}\right\rfloor, \quad K\geq 1.$$

Then there is no integer K satisfying

$$(KA)^z \;<\; A^x+B^y \;<\; \Big((K+1)A\Big)^z.$$

Proof. 1. **Floor-argument.** Since $A^x + B^y = C^z$ and $\gcd(A, C) = 1$, C/A is nonintegral. Thus

$$K = \lfloor C/A \rfloor \implies (KA)^z < A^x + B^y < \Big((K+1)A\Big)^z.$$

2. **Binomial-term comparison.** By WLOG:

$$x, y \le z, \quad B \le A \le KA.$$

We compare term-by-term in the two expansions:

$$\Big((K+1)A\Big)^z - (KA)^z = \sum_{i=1}^{z-1} \binom{z}{i} (KA)^{z-i} A^i,$$

$$A^x + B^y - (KA)^z = \sum_{i=1}^{z-1} \binom{z}{i} A^{z-i} B^i.$$

For each $1 \le i \le z-1$,

$$A^{z-i} \le (KA)^{z-i}, \quad B^i \le A^i,$$

so

$$\binom{z}{i} A^{z-i} B^i \;\le\; \binom{z}{i} (KA)^{z-i} A^i.$$

Worked example for $i = 1$:

$$\binom{z}{1} A^{z-1} B = z \cdot A^{z-1} B \;\le\; z \cdot (KA)^{z-1} A = \binom{z}{1} (KA)^{z-1} A,$$

since $B \le A \le KA$.

Summing these inequalities over $i = 1, \ldots, z-1$ gives

$$A^x + B^y - (KA)^z < \Big((K+1)A\Big)^z - (KA)^z,$$

contradicting the strict upper bound from step 1.

Hence no such K exists. □

7 Lemma 3: LTE and Zsigmondy on Difference Form

Lemma 7.1 (Lifting-The-Exponent Lemma (LTE))**.** *Let u, v be integers with $u \equiv v \pmod p$ and $n \ge 1$. For an odd prime p with $p \mid (u - v)$,*

$$v_p\Big(u^n - v^n\Big) \;=\; v_p(u - v) \;+\; v_p(n).$$

If $p = 2$ and $u \equiv v \equiv 1 \pmod 2$, then

$$v_2\Big(u^n - v^n\Big) = v_2(u - v) + v_2(u + v) + v_2(n) - 1,$$

provided n is even.

Remark on $p = 2$: In our applications, whenever 2 divides $u-v$ one checks directly that $u+v$ is odd (since our bases are coprime and at least one is even), so the extra term $v_2(u+v)$ vanishes. Thus all our valuations reduce to the same simple form $v_2(u^n - v^n) = v_2(u - v) + v_2(n) - 1$, and no additional "even-prime" pathology can arise.

Lemma 7.2. *Suppose a prime ℓ divides both x and z in*

$$A^x + B^y = C^z, \quad A, B, C > 1,\ x, y, z > 2,\ \gcd(A, B, C) = 1.$$

Write

$$x = \ell\, x', \qquad z = \ell\, z', \quad x', z' \geq 1.$$

Then one reaches a contradiction.

Proof. From $A^x + B^y = C^z$ and the above factorization we have

$$C^z - A^x = (C^{z'})^\ell - (A^{x'})^\ell = \left(C^{z'} - A^{x'}\right) \Phi_\ell\Big(C^{z'}, A^{x'}\Big).$$

(a) Any prime dividing the linear factor lives in B. Let $p \mid (C^{z'} - A^{x'})$. Then

$$C^{z'} \equiv A^{x'} \pmod{p} \quad \Longrightarrow \quad p \nmid A \quad \text{and} \quad p \nmid C \quad (\gcd(A, C) = 1).$$

Hence $p \mid (A^x + B^y) = C^z$ forces $p \mid B$. In particular p divides the right-hand side B^y alone.

(b) LTE on the linear factor cannot absorb all of the exponent. By LTE (Lemma 7.1), for *odd* such p,

$$v_p\Big(C^{z'} - A^{x'}\Big) = v_p(C - A) + v_p(z'),$$

and $v_p(C - A) \geq 1$. Thus

$$v_p(C^{z'} - A^{x'}) \ \leq \ v_p(C - A) + v_p(z') < \ell \quad (\ell \mid z).$$

But in the full factorization

$$(C^{z'} - A^{x'})\ \Phi_\ell\Big(C^{z'}, A^{x'}\Big) = B^y,$$

the exponent of p on the right is $y\, v_p(B) \geq y > 2$. Since the linear factor contributes fewer than ℓ powers of p, and $\ell \geq 3$, there must be a contribution from Φ_ℓ as well.

(c) Zsigmondy on the cyclotomic factor. We apply Zsigmondy's theorem to

$$u = C^{z'}, \quad v = A^{x'}, \quad n = \ell,$$

noting that $\gcd(u, v) = \gcd(C^{z'}, A^{x'}) = 1$ (since $\gcd(A, C) = 1$) and $n = \ell > 1$. All the hypotheses of Zsigmondy are therefore met. Moreover, by Section 8, the only admissible exceptions (the perfect-power family or the two sporadic cases) have already been ruled out (they force a smaller exponent or a base = 1). Hence Zsigmondy guarantees a *primitive* prime divisor

$$p \ \mid \ u^\ell - v^\ell \ = \ \Phi_\ell(u, v) \quad \text{with} \quad p \nmid (u - v)\,,$$

so p does *not* divide the linear factor $(C^{z'} - A^{x'})$. That new prime must therefore divide $\Phi_\ell(C^{z'}, A^{x'})$ and hence B^y alone, contradicting $\gcd(A, B, C) = 1$.

In either case we produce a prime that splits off onto B alone (or forces $y \leq 2$), contradicting our hypothesis. This completes the proof. □

Corollary 7.1 (Fermat's Last Theorem). Fermat's Last Theorem follows immediately as a special case of Beal's Conjecture. If $x = y = z = n > 2$ and A, B, C are pairwise coprime, then the equation

$$A^n + B^n = C^n$$

violates Beal's conclusion that A, B, C must share a common prime factor. Therefore, such a solution cannot exist, confirming Fermat's claim.

Conclusion

Combining Lemmas 3.1–3.2, Lemma 1, Lemma 2, and Lemma 3, we see that *every* possible configuration of exponents $x, y, z > 2$ (under $\gcd(A, B, C) = 1$) yields a contradiction. Hence there can be no solution to

$$A^x + B^y = C^z \quad \text{with} \quad A, B, C > 1,\ x, y, z > 2,\ \gcd(A, B, C) = 1,$$

which proves Beal's Conjecture. □

8 Verification of Zsigmondy Exceptions

Zsigmondy's theorem guarantees a primitive prime divisor of

$$A^n \pm B^n, \quad n > 1,\ \gcd(A, B) = 1,$$

except in exactly these three cases:

(1) *Perfect–power family:*

$$n = 2, \quad A \pm B = t^k, \quad t > 1,\ k \geq 2.$$

Then

$$A^2 \pm B^2 = (A \pm B)(A \mp B) = t^k\,(A \mp B),$$

so all prime divisors p of $A^2 \pm B^2$ satisfy $p \mid t$ and hence $p \nmid AB$. By LTE (for odd p),

$$v_p(A^2 \pm B^2) = v_p(A \pm B) + v_p(2) = k + 0 \ \geq\ 2.$$

On the other hand, from the main equation

$$A^x + B^y = C^z \quad \Longrightarrow \quad v_p(C^z) = z\, v_p(C) = 0 \quad (\gcd(p, C) = 1).$$

Thus

$$2 \ \leq\ v_p(A^2 \pm B^2) = v_p(C^z) = 0,$$

a contradiction.

(2) *Sporadic sum–case:*

$$(A, B, n) = (2, 1, 3), \quad 2^3 + 1^3 = 9 = 3^2.$$

No new prime appears (by Zsigmondy). Substituting into $A^x + B^y = C^z$ gives

$$C^z = 9, \quad \Longrightarrow \quad z = 2,$$

contradicting $z > 2$.

(3) *Sporadic difference–case:*

$$(A, B, n) = (2, 1, 2), \quad 2^2 - 1^2 = 3.$$

By convention there is no primitive divisor. Then

$$C^z = 3, \quad \Longrightarrow \quad z = 1,$$

contradicting $z > 2$.

In each of these three exceptional families, one finds either an exponent forced to drop to ≤ 2 or one of the bases becomes 1. Hence none can furnish a counterexample with $A, B > 1$ and $x, y, z > 2$.

Humanistic Reflection

This cuboid-valuation method echoes geometric tilings in classical number theory and offers a visual aid for exponent Diophantine problems.

Concluding Philosophical Reflection

At its heart, Beal's Conjecture asks: when do two "pure power" blocks join to form another? The interplay of cyclotomic factorization (Zsigmondy's insight) and valuation bounds (the LTE lemma) illustrates how arithmetic "particles" (primes) behave like geometric atoms in tilings. This dual algebraic-geometric vision reveals that the deep structures of numbers are inseparable from their spatial metaphors.

Further Reading

For a comprehensive survey of primitive prime divisors in classical sequences, see M. Bilu, G. Hanrot, and P. M. Voutier, "Existence of primitive divisors of Lucas and Lehmer numbers," *J. Reine Angew. Math.* 539 (2001), 75–122.

For an accessible introduction to valuation methods and LTE, see G. Everest and T. Ward, *Recurrence Sequences*, 2nd ed., London Math. Soc. Stud. Texts 87 (Cambridge University Press, 2020).

References

[1] K. Zsigmondy, "Zur Theorie der Primteilern. . . . . " (1892).

[2] A. Bang, "Om talet. . . . . " (1897).

[3] R. K. Guy, *Unsolved Problems in Number Theory*, 3rd ed. (Springer, 2004).

[4] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Graduate Texts in Mathematics Vol. 84 (Springer, 1990).

[5] T. Andreescu and D. Andrica, *Number Theory: Structures, Examples, and Problems* (Birkhäuser, 2006).

[6] M. Bilu, G. Hanrot, and P. M. Voutier, "Existence of primitive divisors of Lucas and Lehmer numbers," *J. Reine Angew. Math.* 539 (2001), 75–122.

[7] G. Everest and T. Ward, *Recurrence Sequences*, 2nd ed., London Math. Soc. Stud. Texts 87 (Cambridge University Press, 2020).