Article

Finite Differences of Prime Powers as Cyclotomic Norms: A Structural Bridge from Nicomachus to Euler. Universal Anderson–Faulhaber–Bernoulli Identity: Internal Structure of Perfect Powers and Arithmetic Obstruction via Discrete Calculus

Ibar Federico Anderson *

Posted Date: 4 March 2026

doi: 10.20944/preprints202602.1998.v2

Keywords: Eisenstein integers; cyclotomic binary forms; discrete calculus; centred hexagonal numbers; Fermat cubic; Löschian numbers; Lifting-the-Exponent Lemma

doi:10.20944/preprints202602.1998.v2

Article

Finite Differences of Prime Powers as Cyclotomic Norms: A Structural Bridge from Nicomachus to Euler. Universal Anderson–Faulhaber–Bernoulli Identity: Internal Structure of Perfect Powers and Arithmetic Obstruction via Discrete Calculus

Ibar Federico Anderson

Laboratory of the Department of Industrial Design (LIDDI), Universidad Nacional de La Plata, Argentina; ianderson@empleados.fba.unlp.edu.ar

Abstract

For every prime p and every integer a, the backward finite difference $\delta_p(a) := a^p - (a-1)^p$ equals the cyclotomic binary form $\Phi_p(a, a-1)$, where $\Phi_p(X, Y)$ is the homogenisation of the p-th cyclotomic polynomial, and hence equals the norm $N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(a - \zeta_p(a-1))$. For $p = 3$ this specialises to the identity $\delta_3(a) = N_{\mathbb{Z}[\omega]}(a - \omega(a-1))$, where $\omega = e^{2\pi i/3}$, connecting the individual cubic finite difference—obtained by differencing the classical sum formula of Nicomachus of Gerasa (∼100 CE)—with the Eisenstein norm that appears in Euler's factorisation of $a^3 + b^3$. We develop this identity in three directions: (a) *General cyclotomic framework.* For each prime p, every prime divisor q of $\delta_p(a)$ satisfies $q \equiv 1 \pmod{p}$, imposing an arithmetic sieve whose density $\sim 1/(p-1)$ grows increasingly severe with p. (b) *Arithmetic density.* The values $\{\delta_3(a)\}_{a \geq 1}$ form a thin subfamily of the Löschian numbers (norms in $\mathbb{Z}[\omega]$), with counting function $\sim \sqrt{N/3}$ versus the Landau–Ramanujan asymptotic $CN/\sqrt{\log N}$ for all Löschian numbers up to N. (c) *Three-language equivalence.* For the cubic case we prove a precise equivalence among: (i) divisibility of $\delta_3(a)$, (ii) multiplicative order modulo q, and (iii) splitting of q in $\mathbb{Z}[\omega]$. We also give an elementary proof of the base case $1 + b^3 = c^3$ (no positive-integer solutions), and derive 3-adic constraints on any hypothetical solution to $a^3 + b^3 = c^3$ via the Lifting-the-Exponent Lemma, without invoking unique factorisation in $\mathbb{Z}[\omega]$.

Keywords: Eisenstein integers; cyclotomic binary forms; discrete calculus; centred hexagonal numbers; Fermat cubic; Löschian numbers; Lifting-the-Exponent Lemma

MSC: 11R18, 11D41, 11A07, 11B83, 39A70, 11E25

---

1. Introduction

1.1. Motivation

The sum formula attributed to Nicomachus of Gerasa (∼100 CE),

$$S_3(n) := \sum_{k=1}^{n} k^3 = \left(\frac{n(n+1)}{2} \right)^2 = T_n^2,$$

where $T_n = n(n+1)/2$ is the n-th triangular number, is one of the oldest identities in number theory. Applying the backward-difference operator ∇ yields the individual cubic difference

$$\delta_3(a) = a^3 - (a-1)^3 = 3a^2 - 3a + 1$$

— a formula within reach of any secondary-school student.

More than sixteen centuries later, Euler's factorisation of a^3+b^3 over the ring of Eisenstein integers $\mathbb{Z}[\omega]$ employs the norm of the element $a-\omega(a-1)$. The central observation of this note is that these two objects are the same:

$$\delta_3(a) = N_{\mathbb{Z}[\omega]}(a-\omega(a-1)).$$

This three-line algebraic identity is the bridge between the two traditions. Its interest lies not in the difficulty of the proof but in the interpretive framework it opens: the discrete-calculus footprint of Nicomachus is the algebraic-number-theory footprint of Euler.

The identity is a special case ($p=3$) of a uniform statement valid for every prime p (Theorem 4.1), connecting backward differences of p-th powers to cyclotomic norm forms.

1.2. Scope and Non-Claims

This note does not prove Fermat's Last Theorem (FLT), established by Wiles [1]. It does not supersede Euler's classical argument for $p=3$ [2]: the three-language equivalence (Theorem 6.1) uses the unique-factorisation-domain (UFD) property of $\mathbb{Z}[\omega]$, which is precisely Euler's key ingredient. The contributions are:

(i) the explicit cyclotomic-norm interpretation of $\delta_p(a)$ for all primes p, with consequences for prime-factor sieves (Section 4);
(ii) the three-language equivalence for the cubic case (Section 6);
(iii) the connection to Löschian numbers and Landau–Ramanujan-type density (Section 7);
(iv) an elementary partial result toward FLT $p=3$ via the Lifting-the-Exponent Lemma, without invoking the UFD of $\mathbb{Z}[\omega]$ (Section 8);
(v) an elementary proof of the base case $1+b^3=c^3$ (Section 9).

2. The Cubic Finite Difference

2.1. Nicomachus's Formula

Theorem 2.1 (Nicomachus, ∼100 CE). *For every $n\in\mathbb{N}$,*

$$S_3(n) := \sum_{k=1}^{n} k^3 = T_n^2, \qquad T_n = \frac{n(n+1)}{2}.$$

Proof. Standard induction. □

Remark 2.2. Among all power sums $S_p(n)=\sum_{k=1}^{n} k^p$, the identity $S_3(n)=T_n^2$ is the unique instance that is a polynomial perfect square [5]. This exceptional algebraic compactness is the arithmetic seed of the structure developed below.

The Fundamental Theorem of Discrete Calculus gives $n^3 = \nabla S_3(n) = T_n^2 - T_{n-1}^2$, expressing each perfect cube as the difference of two consecutive triangular squares — a representation with no analogue for any other power n^p, $p\neq 3$.

2.2. The Individual Cubic Difference

Definition 2.3. The *individual cubic finite difference* is

$$\delta_3(a) := a^3-(a-1)^3 = 3a^2-3a+1.$$

The first values $1,7,19,37,61,91,127,169,217,\ldots$ are the centred hexagonal numbers (OEIS A003215 [11]).

doi:10.20944/preprints202602.1998.v2

3. The Eisenstein Norm Identity

3.1. Eisenstein Integers

Let $\omega = e^{2\pi i/3} = \frac{-1+\sqrt{-3}}{2}$, a primitive cube root of unity satisfying $\omega^2 + \omega + 1 = 0$ and $\omega^3 = 1$. The ring of Eisenstein integers is

$$\mathbb{Z}[\omega] = \{u + v\omega : u, v \in \mathbb{Z}\},$$

with norm $N(u + v\omega) = u^2 - uv + v^2$. This ring is a Euclidean domain (hence a UFD) with unit group $\{\pm 1, \pm\omega, \pm\omega^2\}$ [3].

3.2. The Connecting Identity

Theorem 3.1 (Connecting identity)**.** *For every integer a,*

$$\delta_3(a) = a^3 - (a-1)^3 = N_{\mathbb{Z}[\omega]}(a - \omega(a-1)).$$

Proof. Set $\alpha_a = a + (-(a-1))\omega$, so $u = a$ and $v = -(a-1)$. Then

$$\begin{aligned} N(\alpha_a) &= a^2 - a \cdot (-(a-1)) + (-(a-1))^2 \\ &= a^2 + a(a-1) + (a-1)^2 \\ &= 3a^2 - 3a + 1 = \delta_3(a). \quad \square \end{aligned}$$

Remark 3.2. A second proof uses Euler's factorisation directly. Since $x^3 - y^3 = (x-y)(x-\omega y)(x-\omega^2 y)$ over $\mathbb{Z}[\omega]$, setting $x = a$ and $y = a-1$ (so $x - y = 1$) gives

$$\delta_3(a) = \underbrace{(a - \omega(a-1))}_{\alpha_a} \cdot \underbrace{(a - \omega^2(a-1))}_{\bar{\alpha}_a} = N(\alpha_a).$$

The quantity $\delta_3(a)$, arising from Nicomachus's formula via the backward-difference operator, is the norm of precisely the Eisenstein integer that Euler's decomposition of $a^3 - (a-1)^3$ requires.

4. The General Cyclotomic Framework

4.1. Cyclotomic Binary Forms

For a prime p, the p-th cyclotomic polynomial is

$$\Phi_p(t) = \frac{t^p - 1}{t - 1} = t^{p-1} + t^{p-2} + \cdots + t + 1,$$

with homogenisation

$$\Phi_p(X, Y) = Y^{p-1}\Phi_p\left(\frac{X}{Y}\right) = \sum_{j=0}^{p-1} X^j Y^{p-1-j}.$$

For $p = 3$: $\Phi_3(X, Y) = X^2 + XY + Y^2$, the norm form of $\mathbb{Q}(\omega)/\mathbb{Q}$.

4.2. The General Identity

Theorem 4.1. *Let p be a prime and a any integer. Then*

$$\delta_p(a) := a^p - (a-1)^p = \Phi_p(a, a-1) = N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(a - \zeta_p(a-1)),$$

where $\zeta_p = e^{2\pi i/p}$ and $N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}$ is the field norm.

doi:10.20944/preprints202602.1998.v2

Proof. The factorisation over $\mathbb{Q}(\zeta_p)$,

$$x^p - y^p = (x-y)\prod_{j=1}^{p-1}(x - \zeta_p^j y),$$

with $x = a$, $y = a-1$ gives $x - y = 1$ and

$$\delta_p(a) = \prod_{j=1}^{p-1}\big(a - \zeta_p^j(a-1)\big).$$

The product on the right equals $N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}\big(a - \zeta_p(a-1)\big)$ because the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$ permutes the set $\{\zeta_p^j : 1 \le j \le p-1\}$ transitively. The equality $\Phi_p(a, a-1) = \delta_p(a)$ follows from the definition of the cyclotomic binary form (verified directly for $a = 1$; for $a \neq 1$ clear the denominator $(a-1)^{p-1}$ in $\Phi_p(a/(a-1)) \cdot (a-1)^{p-1}$). □

Remark 4.2. For $p = 3$, $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\omega)$ and $N_{\mathbb{Q}(\omega)/\mathbb{Q}}$ coincides with $N_{\mathbb{Z}[\omega]}$, recovering Theorem 3.1. For $p = 2$, $\delta_2(a) = 2a - 1$ and $\Phi_2(a, a-1) = 2a - 1$; the norm is over $\mathbb{Q}(\zeta_2) = \mathbb{Q}$ and is trivially the identity. This is why the quadratic case carries no algebraic constraint: δ_2 sweeps all odd integers.

4.3. Summary Table

Table 1. Structure of $\delta_p(a) = a^p - (a-1)^p$ for small primes.

p	Ring	$\delta_p(a)$	Prime factor constraint
2	$\mathbb{Z}$	$2a - 1$	all odd primes
3	$\mathbb{Z}[\omega]$	$3a^2 - 3a + 1$	$q \equiv 1 \pmod 3$
5	$\mathbb{Z}[\zeta_5]$	$5a^4 - 10a^3 + 10a^2 - 5a + 1$	$q \equiv 1 \pmod 5$
7	$\mathbb{Z}[\zeta_7]$	$\sum_{k=0}^{6}\binom{7}{k+1}(-1)^k a^{6-k}$	$q \equiv 1 \pmod 7$

5. Prime-Factor Constraints

Proposition 5.1. *Let p be a prime and a an integer.*

(a) $\delta_p(a) \equiv 1 \pmod p$ *for every integer a. In particular, $p \nmid \delta_p(a)$.*
(b) *If q is a prime with $q \nmid a(a-1)$ and $q \mid \delta_p(a)$, then $q \equiv 1 \pmod p$.*

Proof. (a) By Fermat's little theorem, $a^p \equiv a \pmod p$ and $(a-1)^p \equiv (a-1) \pmod p$, so $\delta_p(a) \equiv a - (a-1) = 1 \pmod p$.

(b) Set $t \equiv a(a-1)^{-1} \pmod q$ (well-defined since $q \nmid a(a-1)$). Then

$$\delta_p(a) = a^p - (a-1)^p = (a-1)^p(t^p - 1),$$

and since $q \nmid (a-1)$, we have $q \mid \delta_p(a) \Leftrightarrow t^p \equiv 1 \pmod q$, i.e. $\mathrm{ord}_q(t) \mid p$. Since p is prime, $\mathrm{ord}_q(t) \in \{1, p\}$. If $\mathrm{ord}_q(t) = 1$ then $t \equiv 1$, forcing $q \mid (a - (a-1)) = 1$, a contradiction. Hence $\mathrm{ord}_q(t) = p$, and by Fermat's little theorem $p \mid (q-1)$, i.e. $q \equiv 1 \pmod p$. □

Corollary 5.2. *As p grows, the natural density of primes eligible to divide $\delta_p(a)$ is approximately $1/(p-1)$ (by Dirichlet's theorem on primes in arithmetic progressions). The cyclotomic norm structure imposes an increasingly severe sieve on the prime factors of $\delta_p(a)$.*

Example 5.3. For $p = 5$, $a = 4$: $\delta_5(4) = 4^5 - 3^5 = 781 = 11 \times 71$. Indeed $11 \equiv 1$ and $71 \equiv 1 \pmod 5$. For $p = 5$, $a = 3$: $\delta_5(3) = 3^5 - 2^5 = 211$, which is prime and $211 \equiv 1 \pmod 5$.

6. Three-Language Equivalence: the Cubic Case

We now develop the $p = 3$ case in detail, where $\mathbb{Z}[\omega]$ is Euclidean and the theory is cleanest. Recall the splitting of rational primes in $\mathbb{Z}[\omega]$: a prime $q \in \mathbb{Z}$ satisfies $q \equiv 1 \pmod 3$ if and only if $q = \pi\bar{\pi}$ for a non-real Eisenstein prime π [3].

Theorem 6.1 (Three-language equivalence). *Let q be a prime with $q \nmid a(a-1)$, and set $t_a \equiv a(a-1)^{-1} \pmod q$. The following conditions are equivalent:*

(I) $q \mid \delta_3(a)$ *(discrete calculus);*
(II) $\mathrm{ord}_q(t_a) \mid 3$ *(modular arithmetic);*
(III) there exists an Eisenstein prime π above q such that $\pi \mid \alpha_a$ in $\mathbb{Z}[\omega]$, which additionally requires $q \equiv 1 \pmod 3$ (algebraic number theory).

The equivalence (I)⇔(II) *holds for every prime q coprime to $a(a-1)$. Adding the hypothesis $q \equiv 1 \pmod 3$ extends this to the full three-way equivalence.*

Proof. *(I)⇔(II).* This is Proposition 5.1(b) with $p = 3$.

(I)⇔(III) under $q \equiv 1 \pmod 3$. Write $q = \pi\bar{\pi}$ in $\mathbb{Z}[\omega]$. By Theorem 3.1, $N(\alpha_a) = \delta_3(a)$, so $q \mid \delta_3(a)$ iff $\pi\bar{\pi} \mid N(\alpha_a)$, iff $\pi \mid \alpha_a$ or $\bar{\pi} \mid \alpha_a$. For $q \equiv 2 \pmod 3$, q is inert in $\mathbb{Z}[\omega]$ and every element of $\mathbb{F}_q^\times$ is a cube, so condition (II) is vacuous for $\mathrm{ord}_q(t_a) = 1$ (contradicted by the hypothesis), hence no non-trivial constraint from (III) arises. □

The three-way equivalence is summarised as:

$$\underbrace{q \mid \delta_3(a)}_{\text{discrete calculus}} \iff \underbrace{\mathrm{ord}_q(t_a) \mid 3}_{\text{modular arithmetic}} \xRightarrow{q\equiv 1\,(3)} \underbrace{\exists\,\pi \mid \alpha_a \text{ in } \mathbb{Z}[\omega]}_{\text{algebraic number theory}}$$

Table 2. Values of $\delta_3(a)$, their factorisations, and $\alpha_a = a - \omega(a-1)$. Every prime factor satisfies $q \equiv 1 \pmod 3$.

a	$\delta_3(a)$	Factorisation	α_a
1	1	unit	1
2	7	7	$2-\omega$
3	19	19	$3-2\omega$
4	37	37	$4-3\omega$
5	61	61	$5-4\omega$
6	91	$7 \cdot 13$	$6-5\omega$
7	127	127	$7-6\omega$
8	169	13^2	$8-7\omega$
9	217	$7 \cdot 31$	$9-8\omega$

7. Geometry: Centred Hexagonal and Löschian Numbers

7.1. Centred Hexagonal Numbers

The Eisenstein integers $\mathbb{Z}[\omega]$ form a hexagonal lattice in $\mathbb{C}$ with basis $\{1, \omega\}$.

Proposition 7.1. *The a-th centred hexagonal number $H_a = 3a^2 - 3a + 1$ equals the number of lattice points of $\mathbb{Z}[\omega]$ within and on the regular hexagon of hexagonal radius $a - 1$ centred at the origin. The Eisenstein integer $\alpha_a = a - \omega(a-1)$ satisfies $N(\alpha_a) = H_a = \delta_3(a)$.*

Proof. The norm identity is Theorem 3.1. The geometric counting is the standard formula for centred hexagonal numbers in the hexagonal lattice [5]. □

The centred hexagonal numbers are therefore the arithmetic footprint of the hexagonal geometry of $\mathbb{Z}[\omega]$ in the Fermat cubic equation.

7.2. *Löschian Numbers and the Subfamily* $\{\delta_3(a)\}$

The Löschian numbers are the integers representable as $x^2 + xy + y^2$ for some $x, y \in \mathbb{Z}$; they are precisely the norms of elements of $\mathbb{Z}[\omega]$. Since $\delta_3(a) = N(\alpha_a)$, the values $\{\delta_3(a)\}_{a \geq 1}$ form a one-parameter subfamily of the Löschian numbers, parametrised by the line $\{(a, -(a-1)) : a \in \mathbb{Z}\}$ in the Eisenstein lattice.

A standard characterisation: m is Löschian if and only if every prime factor $q \equiv 2 \pmod 3$ of m appears to an even power. By Proposition 5.1(b), the values of δ_3 satisfy the stronger condition: no prime $q \equiv 2 \pmod 3$ divides $\delta_3(a)$ at all, not even to an even power.

7.3. *Arithmetic Density*

Let $L(N) := \#\{m \leq N : m = x^2 + xy + y^2 \text{ for some } x, y \in \mathbb{Z}\}$. By the work of Bernays [8] (extending Landau's theorem from $x^2 + y^2$ to general definite binary quadratic forms),

$$L(N) \sim C \frac{N}{\sqrt{\log N}},$$

where $C > 0$ is the Landau–Ramanujan constant for the form $x^2 + xy + y^2$ (see [9] for explicit computations).

Since $\delta_3(a) = 3a^2 - 3a + 1 \sim 3a^2$ for large a, we have $\#\{a \geq 1 : \delta_3(a) \leq N\} \sim \sqrt{N/3}$. In particular,

$$\frac{\#\{a : \delta_3(a) \leq N\}}{L(N)} \sim \frac{\sqrt{N/3}}{C\,N/\sqrt{\log N}} = \frac{\sqrt{\log N}}{C\sqrt{3N}} \to 0 \quad \text{as } N \to \infty.$$

Thus $\{\delta_3(a)\}$ has natural density zero inside the Löschian numbers.

8. 3-Adic Constraints via the Lifting-the-Exponent Lemma

In this section we derive 3-adic constraints on any hypothetical solution to $a^3 + b^3 = c^3$ using only elementary modular arithmetic and the Lifting-the-Exponent (LTE) Lemma, without invoking the UFD property of $\mathbb{Z}[\omega]$.

Lemma 8.1 (Lifting the Exponent, odd prime case [10])**.** *Let p be an odd prime and $x, y \in \mathbb{Z}$ with $p \nmid x$, $p \nmid y$.*

(a) *If $p \mid (x + y)$, then $v_p(x^p + y^p) = v_p(x + y) + 1$.*
(b) *If $p \nmid (x + y)$, then $v_p(x^p + y^p) = 0$.*

Theorem 8.2. *Let $a, b, c \in \mathbb{Z}_{>0}$ with $\gcd(a, b) = 1$ and $a^3 + b^3 = c^3$. Then:*

(a) *Exactly one of a, b is divisible by 3.*
(b) *$v_3(b) \geq 1$ (assuming $3 \mid b$).*

Proof. *Step 1: establishing $3 \mid c$.* Cubes modulo 9 take values in $\{0, 1, 8\}$ only. If $3 \nmid a$ and $3 \nmid b$, then $a^3 \equiv 1 \text{ or } 8 \pmod 9$ and similarly for b^3, so $a^3 + b^3 \in \{2, 7, 0\} \pmod 9$ (the cases $1+1$, $1+8$ or $8+8$, $8+1$). For $a^3 + b^3 = c^3$ we need $c^3 \in \{2, 7, 0\} \pmod 9$. Since cubes mod 9 are only $\{0, 1, 8\}$, only the value 0 is compatible, forcing $a^3 + b^3 \equiv 0 \pmod 9$. But $a^3 + b^3 \equiv 0 \pmod 9$ with $3 \nmid a$, $3 \nmid b$ requires $a^3 \equiv 1$, $b^3 \equiv 8$ (or vice versa), which gives $a^3 + b^3 \equiv 0 \pmod 9$ and $3 \mid (a + b)$. Now apply LTE with $p = 3$, $x = a$, $y = b$: $v_3(a^3 + b^3) = v_3(a + b) + 1$. Since $a^3 + b^3 = c^3$, we need $v_3(c^3) = 3v_3(c) = v_3(a + b) + 1$. The right side is $\equiv 1 \pmod 3$, but $3v_3(c) \equiv 0 \pmod 3$ — a contradiction. Hence $3 \mid ab$, proving part (a).

Step 2: $v_3(b) \geq 1$. With $3 \mid b$ and $3 \nmid a$: reducing $a^3 + b^3 = c^3$ modulo 9 gives $a^3 \equiv c^3 \pmod 9$, so $a \equiv c \pmod 3$, hence $3 \mid (c-a)$. Writing $c^3 - a^3 = b^3$ and factoring over $\mathbb{Z}$,

$$(c-a)(c^2 + ca + a^2) = b^3.$$

Since $c \equiv a \pmod 3$ we have $c^2 + ca + a^2 \equiv 3a^2 \equiv 0 \pmod 3$, so $v_3(b^3) \geq 1 + 1 = 2$, giving $3v_3(b) \geq 2$, hence $v_3(b) \geq 1$. □

Remark 8.3. *(Bernoulli bound.)* An independent non-circular constraint comes from the elementary estimate: if $h = (a^p + b^p)^{1/p}$ for $a < b$, then

$$h - b < \frac{a^p}{p\, b^{p-1}}.$$

For $p = 3$, if $a^3/(3b^2) < 1$ then $b < h < b + 1$, so $h \notin \mathbb{Z}$. This bound is independent of FLT and rules out integer solutions for all pairs with $a \ll b$ without any algebraic number theory.

Remark 8.4. Theorem 8.2 recovers, by purely elementary means (no UFD), the 3-adic constraints that form the starting point of Euler's infinite descent. Completing the proof of FLT $p = 3$ from here still requires either the UFD property of $\mathbb{Z}[\omega]$ or an equivalent structural ingredient; this remains the central open problem.

9. The Base Case $1 + b^3 = c^3$

Theorem 9.1. *There are no positive integers* b, c *satisfying* $1 + b^3 = c^3$.

Proof. Rewrite as $c^3 - b^3 = 1$ and factor over $\mathbb{Z}$:

$$(c-b)(c^2 + cb + b^2) = 1.$$

Both factors are positive integers (since $c > b > 0$). The only factorisation of 1 as a product of two positive integers is 1×1, so $c - b = 1$ and $c^2 + cb + b^2 = 1$. Substituting $c = b + 1$:

$$(b+1)^2 + (b+1)b + b^2 = 3b^2 + 3b + 1 = 1,$$

giving $3b(b+1) = 0$, which is impossible for $b \geq 1$. □

Remark 9.2. The expression $3b^2 + 3b + 1$ appearing in the proof is $\delta_3(b+1)$. The condition $\delta_3(b+1) = 1$ forces $b + 1 = 1$, i.e. $b = 0$. Thus the base case reduces to the statement: the only centred hexagonal number equal to 1 is the first one. The proof uses only the factorisation $c^3 - b^3 = (c-b)(c^2 + cb + b^2)$ and secondary-school algebra.

10. Structural Comparison: Squares versus Cubes

The contrast between the Pythagorean equation $a^2 + b^2 = c^2$ (infinitely many solutions) and the Fermat cubic $a^3 + b^3 = c^3$ (no solutions) can be read directly from the structure of δ_p for $p = 2$ versus $p = 3$.

Table 3. Structural comparison between the quadratic and cubic cases.

	$p = 2$ (Pythagorean)	$p = 3$ (Fermat)
Individual difference $\delta_p(a)$	$2a - 1$ (linear)	$3a^2 - 3a + 1$ (quadratic)
Norm structure	not a norm in $\mathbb{Z}[i]$	norm in $\mathbb{Z}[\omega]$
Prime factors of $\delta_p(a)$	all odd primes	only $q \equiv 1 \pmod 3$
Cyclotomic ring	$\mathbb{Q}(\zeta_2) = \mathbb{Q}$	$\mathbb{Q}(\omega)$
Solutions to $h^p = a^p + b^p$	infinitely many	none

For $p = 2$, the difference $\delta_2(a) = 2a - 1$ is a linear arithmetic progression: every odd integer appears, giving great flexibility in constructing Pythagorean triples. The Gaussian integers $\mathbb{Z}[i]$ appear in the factorisation of $a^2 + b^2$, but δ_2 itself carries no Gaussian-norm structure.

For $p = 3$, the difference $\delta_3(a) = 3a^2 - 3a + 1$ is a quadratic norm form in $\mathbb{Z}[\omega]$, confining all prime factors to $q \equiv 1 \pmod 3$. This restriction propagates through Euler's factorisation of $a^3 + b^3$ and obstructs solutions: the neighbourhoods $\{a-1, a, a+1\}$ and $\{b-1, b, b+1\}$ sustaining each cube cannot simultaneously merge into a single window $\{c-1, c, c+1\}$ unless $\min(a, b) = 1$.

For general prime $p \geq 5$, $\delta_p(a) = \Phi_p(a, a-1)$ is a norm form of degree $p - 1$ in the cyclotomic ring $\mathbb{Z}[\zeta_p]$, confining prime factors to $q \equiv 1 \pmod p$ (density $\sim 1/(p-1)$). The constraint grows more severe with each prime p, consistent with the non-existence of solutions for all $p \geq 3$.

11. Open Questions

Q1. Elementary proof for $a \geq 2$.

Is there a proof of FLT for $p = 3$ (for $\min(a, b) \geq 2$) that uses only the identity $\delta_3(a) = N(\alpha_a)$, the LTE Lemma, and elementary modular arithmetic — avoiding the UFD property of $\mathbb{Z}[\omega]$ entirely? Theorem 8.2 shows that such an approach recovers the correct 3-adic constraints. The missing ingredient is a way to derive a contradiction from these constraints without factoring in $\mathbb{Z}[\omega]$.

Q2. Regular primes.

For a regular prime $p \geq 5$, can the identity $\delta_p(a) = N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(a - \zeta_p(a-1))$ be combined with the LTE Lemma and the Kummer–Vandiver criterion to give an elementary-flavoured proof of FLT for regular primes, where the non-elementary input is isolated in the regularity condition?

Q3. Density of $\{\delta_3(a)\}$ in the Löschian numbers.

Since $D(N) = \#\{a \geq 1 : \delta_3(a) \leq N\} \sim (N/3)^{1/2}$ and $L(N) \sim CN/\sqrt{\log N}$, we have $D(N)/L(N) \sim (\log N)^{1/2}/(C\sqrt{3N}) \to 0$. What is the precise rate of decay of $D(N)/L(N)$ and do secondary terms carry arithmetic information about the distribution of prime factors of the δ_3-values?

12. Conclusions

The central identity of this note is:

$$\delta_p(a) = a^p - (a-1)^p = \Phi_p(a, a-1) = N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}\big(a - \zeta_p(a-1)\big).$$

For $p = 3$ this specialises to $\delta_3(a) = N_{\mathbb{Z}[\omega]}(a - \omega(a-1))$, providing a structural bridge between five perspectives on the arithmetic of cubes:

1. *Discrete calculus (Nicomachus–Boole).* $\delta_3(a)$ is the term obtained by differencing Nicomachus's sum formula.
2. *Algebraic number theory (Euler–Kummer).* $\delta_3(a)$ is the norm of the Eisenstein integer α_a that Euler's factorisation requires.
3. *Modular arithmetic.* $q \mid \delta_3(a)$ if and only if $\mathrm{ord}_q(a(a-1)^{-1}) \mid 3$.

4. *Hexagonal geometry.* $N(\alpha_a)$ equals the a-th centred hexagonal number H_a, reflecting the hexagonal lattice structure of $\mathbb{Z}[\omega]$.
5. *General cyclotomic framework.* $\delta_p(a) = \Phi_p(a, a-1)$ for every prime p, with prime factors confined to $q \equiv 1 \pmod{p}$.

The equivalences are proved, not merely analogical. The obstruction to extending Pythagorean solutions to cubes has a precise algebraic address in the Eisenstein lattice; whether an elementary proof for the case $\min(a, b) \geq 2$ exists without the UFD of $\mathbb{Z}[\omega]$ remains open.

Acknowledgments: The author thanks the Laboratory of the Department of Industrial Design (LIDDI), Universidad Nacional de La Plata, for institutional support.

References

1. A. Wiles, "Modular elliptic curves and Fermat's last theorem," *Ann. of Math.*, vol. 141, no. 3, pp. 443–551, 1995.
2. H. M. Edwards, *Fermat's Last Theorem: A Genetic Introduction to Algebraic Number Theory*. New York, NY, USA: Springer-Verlag, 1977.
3. K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed. New York, NY, USA: Springer-Verlag, 1990.
4. L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed. New York, NY, USA: Springer-Verlag, 1997.
5. J. H. Conway and R. K. Guy, *The Book of Numbers*. New York, NY, USA: Springer-Verlag, 1996.
6. Nicomachus of Gerasa, *Introduction to Arithmetic*, M. L. D'Ooge, Trans. New York, NY, USA: Macmillan, 1926. (Original work ∼100 CE.)
7. G. Boole, *A Treatise on the Calculus of Finite Differences*. London, UK: Macmillan, 1860.
8. P. Bernays, "Über die Darstellung von positiven, ganzen Zahlen durch die primitiven, binären quadratischen Formen einer nicht quadratischen Diskriminante," Ph.D. dissertation, Georg-August-Universität Göttingen, Germany, 1912.
9. É. Fouvry, C. Levesque, and M. Waldschmidt, "Representation of integers by cyclotomic binary forms," *Acta Arith.*, vol. 184, no. 1, pp. 67–86, 2018.
10. A. Mirzaei, "Lifting the Exponent Lemma (LTE)," preprint, 2011.
11. OEIS Foundation, "Sequence A003215: Centred hexagonal numbers," *The On-Line Encyclopedia of Integer Sequences*. Available: https://oeis.org/A003215.
12. I. F. Anderson, "From Cumulative Sum to Finite Difference: Nicomachus' Cubic Identity as a Manifestation of Discrete Calculus," *Preprints.org*, Feb. 5, 2026. DOI: https://doi.org/10.20944/preprints202602.0367.v1.
13. I. F. Anderson, "From the Pythagorean Dream to the Fermatian Obstruction: Symbolic Representation of $h = \sqrt[3]{a^3 + b^3}$ via an Identity Derived from Nicomachus' Cumulative Sum," *Preprints.org*, Feb. 10, 2026. DOI: https://doi.org/10.20944/preprints202602.0367.v2.
14. I. F. Anderson, "From the Pythagorean Dream to the Fermatian Obstruction: Symbolic Representation of $h = \sqrt[p]{a^p + b^p}$ via an Identity Derived from Nicomachus' Cumulative Sum," *Preprints.org*, Feb. 27, 2026. DOI: https://doi.org/10.20944/preprints202602.0367.v3.
15. I. F. Anderson, "Universal Anderson–Faulhaber–Bernoulli Identity: Internal Structure of Perfect Powers and Arithmetic Obstruction via Discrete Calculus," *Preprints.org*, Feb. 28, 2026. DOI: https://doi.org/10.20944/preprints202602.1998.v1.
16. I. F. Anderson, "From the Pythagorean Dream to the Fermatian Obstruction: Symbolic Representation of $h = \sqrt[3]{a^3 + b^3}$ via an Identity Derived from Nicomachus' Cumulative Sum," *Arch. Cienc. Investig.*, vol. 2, no. 1, pp. 1–11, Feb. 2026.