The "Difficulties" in Fermat's Original Discourse on the Indecomposability of Powers Greater Than a Square: A Retrospect

Preprint · September 2025

DOI: 10.13140/RG.2.2.24342.32321

1 author:

Grigoriy Dedenko
Financial University

The "Difficulties" in Fermat's Original Discourse on the Indecomposability of Powers Greater Than a Square: A Retrospect

G. L. Dedenko

Candidate of Physical and Mathematical Sciences (PhD equivalent),

Senior Lecturer, Department of Information Technologies (KIT)

Financial University under the Government of the Russian Federation, Moscow, Russia

E-mail of the corresponding author: GLDedenko@fa.ru

Autor's ORCID identifier is 0000–0002–0418–6389

DOI: 10.13140/RG.2.2.24342.32321

September 23, 2025

Abstract

A possible version of the original proof of the decomposability of whole degrees above the square that Pierre Fermat spoke of has been identified. This reconstructed evidence is discussed with some extra conclusions drawn from it.

Keywords: number theory, Fermat's Big/Last Theorem, Hisitory of Mathematics, Algebra, Proof

Classification code of ACM CSS 1998: D.2.4; F.3.1; F.4.1

Classification code of MSC: 68V20; Secondary: 68V15, 03B35

Competing interests

No, I declare that the authors have no competing interests as defined by Springer, or other interests that might be perceived to influence the results and/or discussion reported in this paper.

The author(s) declare(s) that there are no conflicts of interest regarding the publication of this article.

Consent for publication

I consent to the publication of this article.

Availability of data and material

I declare that the availability of data has type a license of "**CC BY-SA: Creative Commons Attribution-ShareAlike**" under the license agreement for the previous publication of this article in 2019 (the article was unfinished at that time) – the previous unfinished publication of this article is available by link https://iiste.org/Journals/index.php/MTM/article/view/48744

and https://www.fermatslibrary.com/p/0c39c9be

and posted as a preprint some small previous version (October 2023):

https://www.researchgate.net/publication/374350359_The_Difficulties_in_Fermat's_Original_Discourse_on_the_Indecomposability_of_Powers_Greater_Than_a_Square_A_Retrospect

and this current finished version as a preprint is published there at the same link.

The data for this finished article are also available at the following link (you can get all previous versions from this link): https://doi.org/10.31219/osf.io/jbdas

Funding

No funding

Ethics approval and consent to participate.
Not applicable

Authors' contributions
The entire article was written by the first author alone. The acknowledgements are given in the Acknowledgements section.

Acknowledgements
First and foremost, the author expresses gratitude to Almighty God and His moral commandments, which have always supported the author in difficult moments.

The author also wishes to honor the memory of his mother, Natalia Alekseevna Dedenko, whose unwavering faith in him and his work has remained a source of inspiration even years after her passing. Her support and belief in the value of perseverance and intellectual pursuit continue to resonate in this research.

Additionally, the author expresses his deepest gratitude to his father, Leonid Grigoryevich Dedenko, Doctor of Physical and Mathematical Sciences, Professor at the Faculty of Physics of Moscow State University, for his invaluable guidance, mentorship, and foundational influence on the author's scientific development. The author is also grateful to mathematics teacher Kolesnikova V.E. from school No. 533 in Moscow for her early support in mathematical education.

The author expresses appreciation to associate professors of the National Research Nuclear University MEPhI Malov A.F., Ivliev S.V., Makarova I.F., Deputy Head of the Department of Applied Nuclear Physics of the NRNU MEPhI Ryabeva E.V., and IAEA staff member Yurkin P.G. for their insightful discussions and professional support.

Further appreciation is extended to Associate Professor Chernyshev L.N. from the Financial University under the Government of the Russian Federation, Dr. Boris Borisov from the Faculty of Mechanics and Mathematics of Moscow State University, Dr. Pashchenko F.F. and colleagues from IPU RAS, Associate Professor Miloserdin V.Yu. from NRNU MEPhI, and NRNU MEPhI teacher Mukhin V.I. for their valuable feedback and technical discussions. The author acknowledges Sergey P. Klykov, fermentation expert from Alpha-Integrum, Ltd, and Ph.D. Math Coordinator at Lebanese International University Issam Kaddoura for their contributions to certain analytical aspects of the work.

Acknowledgment is also given to the creators of generative neural networks—ChatGPT, Claude, Gemini, DeepSeek, Mistral—for their role in partially verifying and improving the results presented in this article. The author appreciates members of mathematical forums such as dxdy and cyberforum for their critical feedback, which enhanced the quality of the research.

Sincere thanks are also due to the supervisor, Associate Professor Kadilin V.V. of NRNU MEPhI, Dean of the Physical-Technical Faculty of NRNU MEPhI Tikhomirov G.V., and Professors Samosadny V.T., Filippov V.P., Kramer-Ageev E.A., Moore V.D., Petrunin V.F., Bolozdyne A.I., Dmitrenko V.V., Grachev V.M., Mashkovich V.P., Ulin S.E., and Associate Professors Boyko N.V., Evstyuhina I.A., Kaplun A.A., Kutsenko K.V., Kolesnikov S.V., Minayev V.M., Petrov V.I., Samonov A.M., Sulaberidze G.A., and Rostokin V.I. from NRNU MEPhI for their academic support and valuable insights.

Further appreciation is given to Project Director in India of ATOM-STROYEXPORT JSC Angelov V.A., First Deputy Director for the Construction of KUDANKULAM NPP of ATOMSTROYEXPORT JSC Kvasha A.V., and colleagues from the KUDANKULAM NPP Project Management Department of ASE: Amosov A.M., Noshikhin D.V., Fomichev A.V., Galepin K.E., Savin A.N., Malinin D.S., Vasiliev V.V., Spirin V.V., Avdeenko V.V., Preobrazhenskaya A.A., and Matushkina G.L. for their technical discussions and professional insights.

Colleagues at the Financial University under the Government of the Russian Federation, including Dean of the Faculty of Information Technology Feklin V.G., Head of the Department of Big Data and Machine Learning Alyunov A.N., Petrosov D.A., Solovyov V.I., Zholobova G.N., Koroteev M.V., Ivanov M.N., Ivanyuk V.A., and Savinov E.A., are acknowledged for their contributions to the discussion of computational aspects of the work.

The author is also thankful for constructive discussions with research peers, including Kondrashkin I.B., Motorin N.M., Klepikov K.S., Mishchenko A.Yu., Kostenetsky A.L., Shevelev S.E., Isakov S.V., Klementyev A.V., Loginov V.Yu., Volkanov D.Yu., Foliyants E.V., Kondar E.V., Burova V.P., Vasilyeva O.A., Shabelnikov A.V., Serzhantova O.V., Danilova N.V., Khan T.A., Kuzanskii N.V., Khrushchev Yu.V., Egorkin I.A., and pulmonologist Krysin Yu.S. from the Central Clinical Hospital of the Presidential Administration of Russia for their feedback and insightful discussions.

Finally, the author acknowledges the broader scientific and professional community, whose constructive criticism and engagement contributed to the refinement of this work.

Authors' information (optional)

First Author Dr Grigoriy DEDENKO, born in Moscow on 9 July 1971, received his M.S. in nuclear physics and engineering (kinetic phenomena) from the Moscow Engineering and Physics Institute (MEPhI) in February 1995 and his Ph.D. in nuclear instrumentation and control there in September 2005.

At MEPhI he worked in applied nuclear physics as an Assistant (1995-2002), Senior Lecturer (2002-2010) and Associate Professor (2010-mid-2018). From mid-2018 to August 2020 he was a leading specialist on the Kudankulam NPP Project for India at Atomstroyexport JSC. Since September 2020 he has been with the Financial University under the Government of the Russian Federation—serving as Associate Professor (Sept 2020-Dec 2023) and, from January 2024, Senior Lecturer.

Dr Dedenko's research interests range from nuclear science and engineering to pure mathematics, history and philosophy.

1 Introduction

The present work is the result of an attempted reconstruction of Fermat's original discourse along with an explanation of why he might have not written it down. The author had performed it within a two-time period of time– between 1990 and 1993 – trying proving the theorem and the final revision in 2017-2025.[1] When completed, it did look like a proof of Fermat's epoch, as it only involved the knowledge and techniques available and utilised by Fermat's contemporary and pre-Fermat mathematical world.

Not to overburden this text with details of a real historical study, let us briefly recall the history of the conjecture. Around 1637, Fermat wrote his Last Theorem in the margin of his copy of the Arithmetica next to Diophantus' sum-of-squares problem [7]:

Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadra-tos & generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est dividere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

Attempts to prove this conjecture employed a diverse range of methods. Early attempts, including Fermat's own proof for the case $n = 4$, utilized the **method of infinite descent**. A significant step forward was Leonhard Euler's proof for the case $n = 3$, which involved the use of **Gaussian integers** [13]. Subsequent efforts included approaches based on the work of Sophie Germain and other techniques, before Andrew Wiles finally presented a complete proof in 1995, drawing upon deep results from **the theory of modular forms and elliptic curves** [1–6].

Modern methods, such as the theory of modular forms, deal with **the transformation properties of specific curves over particular types of spaces** (e.g., rational numbers), highlighting the **stability of elliptic curves with respect to modular transformations**. While the contemporary formalizations of algebraic curves, spaces, transformations, and groups used in these methods were not present in Fermat's time, mathematicians of that era possessed their own approaches and intuitive understandings for studying the properties of natural numbers (and primes). (More on this can be found in the Conclusions section of this paper.)

Theorem 1 (Conditional on Dedenko's Ansatz)**.** *Assume the following Ansatz: for every $n > 2$ and every integer solution $x^n + y^n = z^n$ there exists an integer $o > 1$ such that $o^n = 2 \cdot n$. Then the Fermat equation $x^n + y^n = z^n$ has no solutions in $\mathbb{N}$ for all $n > 2$.*

[1] *The work was mainly performed on the scholarship of the NRNU MEPhI student in* $1990 - 93$, *final revision in* $2017 - 2025$.

Proof sketch. The Ansatz forces $o^n = 2 \cdot n$. Elementary growth estimates imply $o = 2$ and $n \in \{1, 2\}$ only; hence for $n > 2$ a contradiction. See the accompanying Coq file `FLT.v` for a machine-checked proof.

2 Possible Proof

The statement of the theorem is rather straightforward and as follows:
Neither a cube for two cubes, nor a biquadrate or two biquadrates, and generally no power greater than two can be decomposed into two powers of the same grade. In other words, the equation

$$x^n + y^n = z^n$$

has no solutions in natural numbers if n is an integer greater than 2.
Therefore, first

1). Let's write down the theorem

$$x^n + y^n = z^n \tag{2.1}$$

2). Let's rewrite (2.1)

$$z^n - x^n = y^n \tag{2.2}$$

3). Let's perform the transformation of (2.2) to

$$\left(m^n + p^n\right)^n - \left(m^n - p^n\right)^n = y^n, \tag{2.3}$$

where $n \in \mathbb{N}$, m, p are arbitrary numbers (not necessarily integers; signs arbitrary), and $z, x \in \mathbb{N}$ satisfy

$$\begin{cases} m^n + p^n = z, \\ m^n - p^n = x. \end{cases} \tag{2.4}$$

Raising both identities to the n-th power yields

$$\begin{cases} (m^n + p^n)^n = z^n, \\ (m^n - p^n)^n = x^n. \end{cases} \tag{2.5}$$

Thus (2.4) implies (2.5).

Solving (2.4). Adding and subtracting the equations gives

$$2m^n = z + x, \qquad 2p^n = z - x,$$

so formally

$$m = \sqrt[n]{\frac{z + x}{2}}, \qquad p = \sqrt[n]{\frac{z - x}{2}}.$$

Domain note. Over $\mathbb{R}$: for odd n the roots are unique; for even n we need $(z \pm x)/2 \geq 0$ and there is a sign choice $m = \pm\big((z + x)/2\big)^{1/n}$, $p = \pm\big((z - x)/2\big)^{1/n}$. Over $\mathbb{C}$: there are n branches for the n-th root; once a branch is fixed, the reconstruction is consistent.

Equivalence of (2.4)–(2.5). Forward (2.4) $\Rightarrow$ (2.5)**.** Immediate by raising to the n-th power.

Reverse (2.5) $\Rightarrow$ (2.4)**.** Assume $z, x \in \mathbb{N}$ and

$$z^n = (m^n + p^n)^n, \qquad x^n = (m^n - p^n)^n.$$

Taking n-th roots in the same domain as $m^n \pm p^n$ (principal root over $\mathbb{R}_{\geq 0}$, or a fixed branch over $\mathbb{C}$) gives

$$z = m^n + p^n, \qquad x = m^n - p^n,$$

i.e. (2.4). For even n one fixes consistent signs as above. Hence, (2.4) and (2.5) are equivalent in the chosen number domain once the root/branch convention is fixed.

Proposition 1 (Integer case: necessary & sufficient conditions)**.** *If, in addition, one requires $m, p \in \mathbb{Z}$, then necessarily*

$$z \pm x \text{ are even}, \qquad \frac{z+x}{2} = m^n, \qquad \frac{z-x}{2} = p^n.$$

Conversely, if $z \pm x$ are even and both halves are perfect n-th powers in $\mathbb{Z}$, then the reconstructed m, p are integers (up to signs for even n).

Remark 1. *This separates the general real/complex reconstruction (no parity obstruction) from the integer reconstruction, where parity and perfect-power constraints are essential.*

Example (real domain). For $n = 2$, $m = 3$, $p = 2$:

$$z = 3^2 + 2^2 = 13, \qquad x = 3^2 - 2^2 = 5,$$

hence

$$z^2 = 169, \qquad x^2 = 25,$$

and reversing via $(z \pm x)/2$ returns $m = 3$, $p = 2$.

Counterexample (integer case). For $n = 3$, $z = 2$, $x = 1$ we have $(z + x)/2 = 3/2$, which is not a perfect cube in $\mathbb{Z}$; hence no integer m, p satisfy (2.4), although real m, p exist.

4). Let's ask ourselves the question: what is the number y? Is it positive integer or not? If it is not positive integer, then under what conditions will it be natural number? Does its naturalness depend on the degree of n?

From (2.3) we have the difference:

$$y^n = z^n - x^n = (m^n + p^n)^n - (m^n - p^n)^n = \tag{2.6}$$

that can be expanded or decomposed into a sum according to Newton's binomial [8, 9]:

$$\begin{aligned}
&= [(m^n)^n + C_n^1(m^n)^{n-1}p^n + C_n^2(m^n)^{n-2}(p^n)^2 + \cdots + C_n^{n-1}m^n(p^n)^{n-1} + (p^n)^n] - \\
&-[(m^n)^n - C_n^1(m^n)^{n-1}p^n + C_n^2(m^n)^{n-2}(p^n)^2 \pm \cdots \pm C_n^{n-1}m^n(p^n)^{n-1} \pm (p^n)^n] = \\
&= 2C_n^1(m^n)^{n-1}p^n + 2C_n^3(m^n)^{n-3}(p^n)^3 + \cdots + 2C_n^k(m^n)^{n-k}(p^n)^k + \{2C_n^n(p^n)^n\} = \\
&= 2\sum_{i=0}^{k} C_n^{(2i+1)}(m^n)^{n-(2i+1)}(p^n)^{(2i+1)}
\end{aligned}$$

with $k = (n-1)/2$ if n is odd and $k = (n-2)/2$ if n is even.

Rewrite then (2.6) as

$$z^n = x^n + y^n,$$

$$\text{where } x,\ y,\ z \text{ are } \begin{cases} z = m^n + p^n \\ x = m^n - p^n \\ y = \sqrt[n]{2}\left[\sum_{i=0}^{k} C_n^{(2i+1)}(m^n)^{n-(2i+1)}(p^n)^{(2i+1)}\right]^{1/n} \end{cases}$$

with $k = (n-1)/2$ if n is odd and $k = (n-2)/2$ if n is even;

we know that in common case for $n = 2$ we have

$$\text{where } x,\ y,\ z \text{ are given by } \begin{cases} z = r \cdot (m^2 + p^2), \\ x = r \cdot (m^2 - p^2), \\ y = r \cdot 2mp. \end{cases} \tag{2.7}$$

but in our case, we omit the factor r – is some positive ($r > 0$) integer constant since it is reduced in our calculations. Therefore, we made the transformation (2.3) in order to take into account this case (n=2), known since the time of Pythagoras, since the general case should include a particular solution as a subset.

5). scrutinise now the y:

$$y = \sqrt[n]{2}\left[\sum_{i=0}^{k} C_n^{(2i+1)} (m^n)^{n-(2i+1)} (p^n)^{(2i+1)}\right]^{1/n}. \tag{2.8}$$

In order for the y to maybe a positive integer, $\sqrt[n]{2}$ must leave, since for $n > 1$ $\sqrt[n]{2}$ is an irrational number (see Appendix A). It is thus necessary that the expression

$$\left[\sum_{i=0}^{k} C_n^{(2i+1)} (m^n)^{n-(2i+1)} (p^n)^{(2i+1)}\right]^{1/n} \tag{2.9}$$

contain some common factor that destroys the radical expression $\sqrt[n]{2}$, let's find out what it is. Otherwise, y is not a positive integer due to the presence of $\sqrt[n]{2}$. Consider now what largest divisor this sum may contain and what it is equal to:

$$\begin{aligned}
&\left[\textstyle\sum_{i=0}^{k} C_n^{(2i+1)} (m^n)^{n-(2i+1)} (p^n)^{(2i+1)}\right] = \\
&= C_n^1 (m^n)^{n-1} p^n + C_n^3 (m^n)^{n-3} (p^n)^3 + \cdots + C_n^k (m^n)^{n-k} (p^n)^k + \{C_n^n (p^n)^n\} = \\
&= n(m^n)^{n-1} p^n + \tfrac{n(n-1)(n-2)}{3!} (m^n)^{n-3} p^3 + \cdots + \\
&+ \tfrac{n(n-1)\ldots(n-k+1)}{k!} (m^n)^{n-k} (p^n)^k + \left\{\tfrac{n(n-1)\ldots 2\cdot 1}{n!} (p^n)^n\right\} = \\
&= n \cdot \big[(m^n)^{n-1} p^n + \tfrac{(n-1)(n-2)}{3!} (m^n)^{n-3} p^3 + \ldots + \\
&+ \tfrac{(n-1)\ldots(n-k+1)}{k!} (m^n)^{n-k} (p^n)^k + \left\{\tfrac{(n-1)\ldots 2\cdot 1}{n!} (p^n)^n\right\}\big] = n \cdot l^n
\end{aligned} \tag{2.10}$$

with $k = (n-1)/2$ if n is odd and $k = (n-2)/2$ if n is even,

Hence the conclusion follows: n is a common divisor, and where l is some constant about which we know nothing (it is maybe real in common case or maybe integer), through which we denoted the rest of the radical after the allocation of the common set n.

Since all the terms in the sum (2.10) contain the factor n, the expression is divisible by n.

To show the uniqueness of the decomposition of expression (2.10), we can use the following considerations:

(a) Degree n is a fixed positive integer.

(b) Exponentiation is an unambiguous operation; for any number, there is a unique value for the degree.

(c) Addition and subtraction of real numbers are commutative operations, and the result does not depend on the order of actions.

Based on these properties, it can be argued that for fixed m, p and n there is a single result of calculating the expression (2.10). Rearranging the members will not affect the final answer.

We can see from (2.8 - 2.10) (where l is some constant (which will be it for fixed m, p, n), which we don't know anything about yet)

$$y = \sqrt[n]{2 \cdot n} \cdot l \tag{2.11}$$

As a result, from (2.6-2.11) we see

$$z^n - x^n = (m^n + p^n)^n - (m^n - p^n)^n = y^n \tag{2.12}$$

Substituting expression (2.11) in (2.12), we obtain

$$(m^n + p^n)^n - (m^n - p^n)^n = 2 \cdot n \cdot l^n \tag{2.13}$$

Let's put $m = j \cdot p$, where $j > 1$ is any number.

$$((j \cdot p)^n + p^n)^n - ((j \cdot p)^n - p^n)^n = 2 \cdot n \cdot l^n$$

$$(p^n \cdot (j^n + 1))^n - (p^n \cdot (j^n - 1))^n = 2 \cdot n \cdot l^n$$

$$(p^n)^n \cdot ((j^n + 1)^n - (j^n - 1)^n) = 2 \cdot n \cdot l^n$$

Consider the difference $(j^n + 1)^n - (j^n - 1)^n$, decompose it according to the Newtonian Binomial

$$(j^n + 1)^n - (j^n - 1)^n = \sum_{k=0}^{n} \left(\begin{array}{c} n \\ k \end{array} \right) (j^n)^{n-k} - \sum_{k=0}^{n} \left(\begin{array}{c} n \\ k \end{array} \right) (j^n)^{n-k} (-1)^k$$

Combining the amounts

$$\sum_{k=0}^{n} \left(\begin{array}{c} n \\ k \end{array} \right) (j^n)^{n-k} \left[1 - (-1)^k\right]$$

Simplify the amount. Since $\left[1 - (-1)^k\right]$ it is 2 when k is odd and 0 when k is even, the sum will only include the odd values of k.

Thus, we have:

$$(p^n)^n \cdot 2 \cdot \sum_{k \;\; odd} \left(\begin{array}{c} n \\ k \end{array} \right) (j^n)^{n-k} = 2 \cdot n \cdot l^n$$

Let's denote

$$q^n = 2 \cdot \sum_{k \;\; odd} \left(\begin{array}{c} n \\ k \end{array} \right) (j^n)^{n-k}$$

Therefore

$$\left(p^n\right)^n q^n \; = \; 2 \cdot n \, l^n,$$

i.e.

$$\frac{\left(p^n\right)^n q^n}{l^n} \; = \; 2 \cdot n. \tag{2.14}$$

Considering the explicit expressions for q and l in (2.14), we obtain in fact an identity and hence infinitely many solutions.

From (2.8)–(2.11) we have

$$l^n \; = \; \frac{1}{n} \sum_{\substack{1 \le k \le n \\ k \text{ odd}}} \binom{n}{k} m^{\,n(n-k)} \, p^{nk}.$$

Setting $m = j\, p$ (with $j \in \mathbb{R}$) gives

$$l^n \; = \; (p^n)^n \, \frac{1}{n} \sum_{\substack{1 \le k \le n \\ k \text{ odd}}} \binom{n}{k} \left(j^n\right)^{n-k}.$$

Likewise, from the binomial expansion of $(m^n + p^n)^n - (m^n - p^n)^n$ one isolates the odd part and can write

$$q^n \; = \; 2 \sum_{\substack{1 \le k \le n \\ k \text{ odd}}} \binom{n}{k} \left(j^n\right)^{n-k}.$$

Substituting these into (2.14) cancels the common factor $(p^n)^n$ and yields

$$\frac{(p^n)^n \cdot 2 \sum_{\substack{1 \le k \le n \\ k \text{ odd}}} \binom{n}{k} \left(j^n\right)^{n-k}}{(p^n)^n \cdot \frac{1}{n} \sum_{\substack{1 \le k \le n \\ k \text{ odd}}} \binom{n}{k} \left(j^n\right)^{n-k}} \; = \; 2 \cdot n,$$

which is an identity (for any $p \neq 0$, $j \in \mathbb{R}$). Thus, taken literally, (2.14) admits infinitely many solutions: there is no arithmetic obstruction at this stage.

Introducing a normalizing variable. To proceed, we impose an additional structural constraint and introduce

$$o \;:=\; \frac{p^n\, q}{l}\,.$$

Then (2.14) becomes the single scalar relation

$$o^n \;=\; 2 \cdot n. \tag{2.15}$$

Equivalently,

$$\left(\frac{p^n\, q}{l}\right)^n \;=\; 2 \cdot n, \qquad \text{hence} \qquad \frac{p^n\, q}{l} \;=\; \sqrt[n]{2 \cdot n}\,. \tag{2.16}$$

Why this particular shape for o. The building blocks in the expansion are m^n and p^n, i.e. pure n-th powers. It is therefore natural that the "normalizing" quantity absorbing $\sqrt[n]{2}$ is itself an n-th power. Concretely, we define

$$o \;:=\; \sqrt[n]{2 \cdot n},$$

so that

$$o^n \;=\; 2 \cdot n. \tag{2.21}$$

The crucial point, however, is integrality: the fact that $o \in \mathbb{N}$, $o > 1$ is not a consequence of (2.16)–(2.19) but an additional postulate. This is precisely Dedenko's Ansatz:

$$\exists\, o \in \mathbb{N}, \quad o > 1, \quad o^n = 2 \cdot n.$$

Once assumed, this single hypothesis reduces the problem to an elementary growth comparison analyzed below.

A useful reduction. Define

$$f(n) \;:=\; \sqrt[n]{2 \cdot n}.$$

For each fixed n, (2.16) forces $o = f(n)$. One checks

$$f(1) = 2, \qquad f(2) = 2, \qquad f(n) < 2 \text{ and strictly decreasing for } n > 2,$$

and $f(n) \to 1$ as $n \to \infty$. Thus $o = 2$ is the unique choice that yields the maximal number of integer solutions in n (namely, $n = 1, 2$).

Consequently, analyzing the most "integer-saturated" case amounts to taking $o = 2$, which gives

$$2 \;=\; \sqrt[n]{2 \cdot n}. \tag{2.22}$$

Raising both sides of (2.22) to the n-th power,

$$2^n \;=\; 2 \cdot n, \tag{2.23}$$

or equivalently,

$$n \;=\; 2^{n-1}. \tag{2.24}$$

The function $g(n) = n - 2^{n-1}$ vanishes exactly at $n = 1$ and $n = 2$, and is negative for all integers $n > 2$ (since the exponential 2^{n-1} outgrows the linear n). Hence (2.24) has exactly two positive integer roots, $n = 1$ and $n = 2$.

Conclusion. Under the Ansatz $o \in \mathbb{N}$, $o > 1$, $o^n = 2 \cdot n$, the only possible integer exponent values consistent with (2.21) are $n \in \{1, 2\}$. Therefore for $n > 2$ no such integer o exists, which yields the desired contradiction in the Fermat setting—indeed, this is precisely the kind of succinct "margin" observation Fermat himself might have made: once the reasoning is reduced to $o^n = 2 \cdot n$, only $n = 1, 2$ remain admissible, and thus no solution can occur for any higher exponent.

6.) Verification (without considering the total multiplier r from (2.7), which has been reduced)

(a) Consider the case $n = 1$

$$z = m + p$$
$$x = m - p$$
$$y = 2 \cdot [C_1^1 (m^1)^{1-(2\cdot 0+1)} (p^1)^{(2\cdot 0+1)} = 2[1 \cdot 1 \cdot p] = 2p$$

that is, for the case $n = 1$, we have a solution in natural numbers x, y, z, if m and p - are positive integer numbers and $m > p$.

(b) Consider the case $n = 2$

$$z = m^2 + p^2$$
$$x = m^2 - p^2$$
$$y = \sqrt{2} \cdot [C_1^2 (m^2)^{2-(2\cdot 0+1)} (p^2)^{(2\cdot 0+1)}]^{1/2} = \sqrt{2} \cdot [2m^2p^2]^{1/2} = 2mp$$

that is, for the case $n = 2$, we also have a solution in positive integer numbers x, y, z, if m and p are positive integer numbers and $m > p$, or according to [10], if $m > p$, and m, p are such non-integer numbers that combinations with them will give the positive integer numbers x, y, z, for example: $m = 3/\sqrt{2}$, $p = 1/\sqrt{2}$, in this case, we also get the classical Pythagorean triple:

$$x = m^2 - p^2 = \left(\frac{3}{\sqrt{2}}\right)^2 - \left(\frac{1}{\sqrt{2}}\right)^2 = \frac{9}{2} - \frac{1}{2} = \frac{8}{2} = 4$$
$$y = 2 \cdot m \cdot p = 2 \cdot \frac{3}{\sqrt{2}} \cdot \frac{1}{\sqrt{2}} = 3$$
$$z = m^2 + p^2 = \left(\frac{3}{\sqrt{2}}\right)^2 + \left(\frac{1}{\sqrt{2}}\right)^2 = \frac{9}{2} + \frac{1}{2} = 5$$

We have obtained the classical Pythagorean triple and can see that this formula works.

7). Let us now consider the more general case where r is not reduced to proceed to final formulas like (2.7). If r is a positive integer number, then all the above applies. But according to [10], r – can be a rational number. For example, let's say $r = 0.5$:

(a) Consider the case of $n = 1$, $m = 4$, and $p = 2$

$x = 0.5 \cdot (m - p) = 0.5 \cdot (4 - 2) = 1$

$z = 0.5 \cdot (m + p) = 0.5 \cdot (4 + 2) = 3$

$y = 0.5 \cdot (2 \cdot p) = 0.5 \cdot (2 \cdot 2) = 2$

We see positive integer numbers. That is,, m, p must be such that 7*(a)* is performed similarly. In this case, we can see that the formula 6*(a)* works.

(b) Consider the case *of* $n = 2$, $m = 2 \cdot \sqrt{2}$, $p = \sqrt{2}$,

$x = 0.5 \cdot (m^2 - p^2) = 0.5 \cdot \left((2 \cdot \sqrt{2})^2 - (\sqrt{2})^2\right) = 3$

$z = 0.5 \cdot (m^2 + p^2) = 0.5 \cdot \left((2 \cdot \sqrt{2})^2 + (\sqrt{2})^2\right) = 5$

$y = 0.5 \cdot (2 \cdot m \cdot p) = 0.5 \cdot \left(2 \cdot (2 \cdot \sqrt{2}) \cdot (\sqrt{2})\right) = 4$

We see positive integer numbers. That is,, m, p must be such that 7*(b)* holds similarly. In this case, we can see that the formula 6*(b)* works.

This preserves the generality of solutions for $n = 2$, as seen in the Pythagorean triple example.

8). Therefore, the cases $n = 1$ and $n = 2$ **exhaust all possible integer solutions**, which is consistent with the theorem.
The test showed that for n=*1* or for n=*2*, in all the cases considered, we have solutions of the equation $x^n + y^n = z^n$in the positive integer numbers x, y, z

9). **the equation $x^n + y^n = z^n$ has roots in the positive integer numbers x, y, z only for $n = 1$ and for $n = 2$**

Q.E.D.

3 Remark and corollaries

REMARK. *Note that the expression (2.8) can be simplified, namely*

$$\begin{aligned} y &= \sqrt[n]{2}\left[\sum_{i=0}^{k} C_n^{(2i+1)}(m^n)^{n-(2i+1)}(p^n)^{(2i+1)}\right]^{1/n} = \\ &= \sqrt[n]{2}\left[\sum_{i=0}^{k} C_n^{(2i+1)}\frac{(m^n)^n}{(m^n)^{2i}m^n}(p^n)^{2i}p^n\right]^{1/n} = \\ &= \sqrt[n]{2}m^n\frac{1}{m}p\left[\sum_{i=0}^{k} C_n^{(2i+1)}\left(\frac{p}{m}\right)^{n2i}\right]^{1/n} = \\ &= \sqrt[n]{2}m^{n-1}p\left[\sum_{i=0}^{k} C_n^{(2i+1)}\left(\frac{p}{m}\right)^{2in}\right]^{1/n} \end{aligned} \tag{3.1}$$

with $k = (n-1)/2$ if n is odd and $k = (n-2)/2$ if n is even.

COROLLARY 1. *Consider the case $m = p$, then from the expression (3.1) it can be derived that*

$$\begin{aligned} &x = 0 \\ &z = m^n + m^n = 2m^n \\ &y = \sqrt[n]{2}m^{n-1}m\left[\sum_{i=0}^{k} C_n^{(2i+1)}\left(\frac{m}{m}\right)^{2in}\right]^{1/n} = \sqrt[n]{2}m^n\left[\sum_{i=0}^{k} C_n^{(2i+1)}\right]^{1/n} \end{aligned}$$

with $k = (n-1)/2$ if n is odd and $k = (n-2)/2$ if n is even.
It is obvious that $y = z$

$$\begin{aligned} \sqrt[n]{2}m^n\left[\sum_{i=0}^{k} C_n^{(2i+1)}\right]^{1/n} &= 2m^n \\ \sqrt[n]{2}\left[\sum_{i=0}^{k} C_n^{(2i+1)}\right]^{1/n} &= 2 \end{aligned},$$

whence

$$\sum_{i=0}^{k} C_n^{(2i+1)} = 2^{n-1} \tag{3.2}$$

with $k = (n-1)/2$ if n is odd and $k = (n-2)/2$ if n is even.

COROLLARY 2. *Based on (3.2), the sum of even combinations can be calculated.*
Consider Pascal's triangle [7]:

$$\begin{array}{c} 1 \quad 1 \\ 1 \quad 2 \quad 1 \\ 1 \quad 3 \quad 3 \quad 1 \\ 1 \quad 4 \quad 6 \quad 4 \quad 1 \\ 1 \quad 5 \quad 10 \quad 10 \quad 5 \quad 1 \end{array}$$

Similarly to the above, it is concluded that

$$\sum_{j=0}^{s} C_n^{2i} = 2^{n-1} \tag{3.3}$$

with $k = (n-1)/2$ if n is odd and $k = (n-2)/2$ if n is even.

PROOF.
Expand

$$(m^n + p^n)^n + (m^n - p^n)^n =$$

into a binomial [8, 9]:

$$\begin{aligned} &= [(m^n)^n + C_n^1(m^n)^{n-1}p^n + C_n^2(m^n)^{n-2}(p^n)^2 + \cdots + C_n^{n-1}m^n(p^n)^{n-1} + (p^n)^n] + \\ &+ [(m^n)^n - C_n^1(m^n)^{n-1}p^n + C_n^2(m^n)^{n-2}(p^n)^2 \pm \cdots \pm C_n^{n-1}m^n(p^n)^{n-1} \pm (p^n)^n] = \\ &= 2C_n^0(m^n)^n + 2C_n^2(m^n)^{n-2}(p^n)^2 + \ldots + 2C_n^k(m^n)^{n-k}(p^n)^k + \{2C_n^n(p^n)^n\} = \\ &= 2\sum_{j=0}^{s} C_n^{2j}(m^n)^{n-2j}(p^n)^{2j} \end{aligned}$$

with $s = (n-1)/2$ if n is odd and $s = n/2$ if n is even.

If $m = p$

$$(p^n + p^n)^n + (p^n - p^n)^n = 2\sum_{j=0}^{s} C_n^{2j}(p^n)^{n-2j}(p^n)^{2j}$$

$$(2p^n)^n = 2\sum_{j=0}^{s} C_n^{2j}\frac{(p^n)^n}{(p^n)^{2j}}(p^n)^{2j}$$

$$2^n(p^n)^n = 2(p^n)^n\sum_{j=0}^{s} C_n^{2j}$$

$$2^{n-1} = \sum_{j=0}^{s} C_n^{2j}$$

with $s = (n-1)/2$ if n is odd and $s = n/2$ if n is even.
Corollary 2 is proved.

COROLLARY 3. *Analysing (3.2) and (3.3), it can be concluded that*

$$\sum_{i=0}^{k} C_n^{(2i+1)} = \sum_{j=0}^{s} C_n^{2j} \tag{3.4}$$

with $k = (n-1)/2$, $s = (n-1)/2$ if n is odd and $k = (n-2)/2$, $s = n/2$ if n is even.
Why such borders?

Type of number	Condition	Last constant in equation
Odd	$k = 2((n\text{-}1)/2)+1 = n$	C_n^n
	$s = 2((n\text{-}1)/2) = n\text{-}1$	C_n^{n-1}
Even	$k = 2((n\text{-}2)/2)+1 = n\text{-}1$	C_n^{n-1}
	$s = 2(n/2) = n$	C_n^n

Table 1: Boundaries of binomial coefficients

Conclusion: the sum of even coefficients is equal to the sum of odd ones and is equal to 2^{n-1}, therefore from (3.4) we have

$$\sum_{r=0}^{n} C_n^r = \sum_{i=0}^{k} C_n^{(2i+1)} + \sum_{j=0}^{s} C_n^{2j} = 2 \cdot 2^{n-1} = 2^n \tag{3.5}$$

with $k = (n-1)/2$, $s = (n-1)/2$ if n is odd and $k = (n-2)/2$, $s = n/2$ if n is even.

4 Conclusion

The "difficulties" were for Fermat the lengthiness of the run of his deductions ***put in writing***, as in the first half of the seventeenth century the mathematical notations had been way far from their present concise and diverse shape, many actions had to be written down ***in words. Besides, a purely mathematical challenge was that he had to operate the then entirely new notions of binomials and logarithms***, both having just appeared for use and to be learnt "on the fly".

As mentioned in the introduction, the mathematical methods from Pierre Fermat's era used in this article's proof are accessible to any first-year physics and mathematics student. This contrasts favorably with Andrew Wiles's proof, which is quite complex for the average mathematician due to its use of advanced and intricate modern mathematical tools.

Fermat was obviously "playing" with the new notions, decomposing powers of differences into sums of powers and suddenly found out that as one confines oneself with positive integers in the power, the logarithmic equation yields immediately that $x^n + y^n = z^n$(which is a difference rewritten as a sum) is correct for whole x, y, z only and if only $n = 1$ or 2.

He (would have) had first to introduce the two new notions so as to fully explain his finding. One can imagine ***how much room it would take to put down all the deliberations*** that had led him to his discovery ***on the margins of a book solely without the proper symbolic notations that a contemporary mathematician avails***.

Why Pierre Fermat did not write down all those ideas in a dedicated document is the dedicated question of a dedicated research endeavour. It can come out that he had authored such a separate document indeed, which afterwards was somehow lost or – alternatively – has survived to this day, hidden in an archive or a library or in somebody's unrealised custody.

The author requests the mathematical society to look critically at the deliberations set forth above and to return their assessment.

This paper has been published as a preprint on the ResearchGate platform and on the OSF platform at the following links [11, 12].

References

1. Faltings Gerd, "The Proof of Fermat's last theorem by R. Taylor and A. Wiles". *Notices of the AMS*, 42:7 (1995), 743–746.

2. Wiles, A. (1995). Modular Elliptic Curves and Fermat's Last Theorem. Annals of Mathematics, 141(3), 443–551.

3. Taylor, R., & Wiles, A. (1995). Ring-theoretic properties of certain Hecke algebras. Annals of Mathematics, 141(3), 553–572.

4. Ribet, K. A. (1990). On modular representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms. Inventiones Mathematicae, **100**, 431–476.

5. Mazur, B. (1977). Modular curves and the Eisenstein ideal. Publications Mathématiques de l'IHÉS, 47, 33–186.

6. Serre, J.-P. (1987). Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Duke Mathematical Journal, **54**(1), 179–230.

7. Savin P., Encyclopedic Dictionary of Young Mathematics, Pedagogical, Moscow., 1985

8. Korn G. and Korn T., Handbook of Mathematics for Scientists and Engineers. Science, Moscow, 1977

9. Zaitsev V.V., Ryzhkov V.V., Skanavi M.I., Elementary Mathematics. Science, Moscow, 1976.

10. FERMAT'S LAST THEOREM AND EUCLID'S FORMULAS,
    Sergey P. Klykov, Marina Klykova, Preprint, March 2024,
    DOI: 10.13140/RG.2.2.11109.20967
    https://www.researchgate.net/publication/379445595_FERMAT'S_LAST_THEOREM_AND_EUCLID'S_FORMULAS

11. The "Difficulties" in Fermat's Original Discourse on the Indecomposability of Powers Greater Than a Square: A Retrospect,
    Grigoriy Dedenko, Preprint, September 2024,
    https://www.researchgate.net/publication/374350359_The_Difficulties_in_Fermat's_Original_Discourse_on_the_Indecomposability_of_Powers_Greater_Than_a_Square_A_Retrospect

12. The "Difficulties" in Fermat's Original Discourse on the Indecomposability of Powers Greater Than a Square: A Retrospect,
    Grigoriy Dedenko, Preprint, September 2024,
    https://doi.org/10.31219/osf.io/jbdas

13. Euler, L. (1770). *Vollständige Anleitung zur Algebra.* St. Petersburg: Kayserliche Academie der Wissenschaften.

A Appendix A. Proof of the Irrationality of $\sqrt[n]{2}$ for $n \geq 2$

A.1 Theorem: The number $\sqrt[n]{2}$ is irrational for any integer $n \geq 2$.

A.2 Proof:

We will prove by contradiction. Assume that $\sqrt[n]{2}$ is a rational number. This means it can be represented as an irreducible fraction $\frac{p}{q}$, where p and q are integers, $q \neq 0$, and p and q have no common divisors other than 1.

Thus, we have:

$$\sqrt[n]{2} = \frac{p}{q}$$

Raise both sides of the equation to the power of n:

$$(\sqrt[n]{2})^n = \left(\frac{p}{q}\right)^n$$

$$2 = \frac{p^n}{q^n}$$

Multiply both sides by q^n:

$$2q^n = p^n$$

From this equation, we see that p^n is an even number, since it is equal to $2q^n$. If p^n is even, then p must also be even (if p were odd, then p^n would also be odd).

Since p is even, we can write it as $p = 2k$, where k is some integer. Substitute this expression for p into the equation $2q^n = p^n$:

$$2q^n = (2k)^n$$

$$2q^n = 2^n k^n$$

Divide both sides of the equation by 2 (which is permissible since $n \geq 2$, and therefore 2^n is divisible by 2):

$$q^n = 2^{n-1}k^n$$

Since $n \geq 2$, then $n - 1 \geq 1$. From the last equation, we see that q^n is an even number, since it is equal to $2^{n-1}k^n$, where 2^{n-1} is an even factor. If q^n is even, then q must also be even.

Thus, we have reached the conclusion that both p and q are even numbers. This means they have a common divisor of 2. However, at the beginning of the proof, we assumed that the fraction $\frac{p}{q}$ was irreducible, meaning p and q have no common divisors other than 1.

The resulting contradiction indicates that our initial assumption about the rationality of $\sqrt[n]{2}$ is incorrect.

A.3 Conclusion:

Therefore, the number $\sqrt[n]{2}$ is irrational for any integer $n \geq 2$.

B Appendix B. Proof that the limit of the function $f(n) = \sqrt[n]{2 \cdot n}$ is 1

B.1 Problem Statement

Prove that the limit of the function $f(n) = \sqrt[n]{2 \cdot n}$ as n approaches infinity is equal to 1.

B.2 Solution

Consider the function $f(n) = \sqrt[n]{2 \cdot n}$. Our goal is to find the limit of this function as $n \to \infty$. Let's rewrite the function in the form of a power:

$$f(n) = (2 \cdot n)^{\frac{1}{n}}$$

To find the limit of this function, let's consider the natural logarithm of $f(n)$:

$$\ln(f(n)) = \ln\left((2 \cdot n)^{\frac{1}{n}}\right)$$

Using the properties of logarithms, we get:

$$\ln(f(n)) = \frac{1}{n} \ln(2 \cdot n)$$

Separate the logarithm of the product into the sum of logarithms:

$$\ln(f(n)) = \frac{\ln(2) + \ln(n)}{n}$$

Now, let's find the limit of $\ln(f(n))$ as $n \to \infty$:

$$\lim_{n\to\infty} \ln(f(n)) = \lim_{n\to\infty} \frac{\ln(2) + \ln(n)}{n}$$

This limit has the indeterminate form $\frac{\infty}{\infty}$, so we can apply L'Hôpital's Rule. Take the derivatives of the numerator and denominator with respect to n:

$$\frac{d}{dn}(\ln(2) + \ln(n)) = \frac{1}{n}$$

$$\frac{d}{dn}(n) = 1$$

Thus, the limit becomes:

$$\lim_{n\to\infty} \frac{\frac{1}{n}}{1} = \lim_{n\to\infty} \frac{1}{n} = 0$$

So, we have found that the limit of the natural logarithm of the function is 0:

$$\lim_{n\to\infty} \ln(f(n)) = 0$$

Now, to find the limit of the original function $f(n)$, we use the continuity of the exponential function:

$$\lim_{n\to\infty} f(n) = \lim_{n\to\infty} e^{\ln(f(n))} = e^{\lim_{n\to\infty} \ln(f(n))} = e^0 = 1$$

B.3 Conclusion

Therefore, we have proven that the limit of the function $f(n) = \sqrt[n]{2 \cdot n}$ as n approaches infinity is equal to 1.

C Appendix C. A short proof of monotonicity

It is well known that $\sqrt[n]{2 \cdot n} \to 1$ as $n \to \infty$ (see Appendix B). However, in this appendix we focus on showing that $(2 \cdot n)^{1/n}$ is strictly decreasing for $n \geq 3$. Below is one way to prove this, using the logarithmic derivative:

C.1 Define the function.

Let

$$f(n) \;=\; (2 \cdot n)^{\frac{1}{n}}.$$

It is convenient to work with its natural logarithm:

$$\ln\bigl(f(n)\bigr) \;=\; \ln\bigl((2 \cdot n)^{\frac{1}{n}}\bigr) \;=\; \frac{1}{n}\,\ln(2 \cdot n).$$

Denote

$$g(n) \;=\; \ln\bigl(f(n)\bigr) \;=\; \frac{\ln(2 \cdot n)}{n} \;=\; \frac{\ln(2) + \ln(n)}{n}.$$

C.2 Compute the derivative.

Treating n as a real variable $n > 0$, we have

$$g'(n) \;=\; \frac{d}{dn}\Bigl(\tfrac{\ln(2 \cdot n)}{n}\Bigr).$$

Using the quotient rule,

$$g'(n) = \frac{\frac{d}{dn}[\ln(2 \cdot n)] \cdot n \;-\; \ln(2 \cdot n) \cdot 1}{n^2} = \frac{\frac{1}{n} \cdot n \;-\; \ln(2 \cdot n)}{n^2} = \frac{1 - \ln(2 \cdot n)}{n^2}.$$

(Note that $\frac{d}{dn}[\ln(2 \cdot n)] = \frac{1}{2 \cdot n} \cdot 2 = \frac{1}{n}$.)

C.3 Sign of the derivative.

We want to see where $g'(n) < 0$:

$$g'(n) < 0 \iff 1 - \ln(2 \cdot n) < 0 \iff \ln(2 \cdot n) > 1 \iff 2 \cdot n > e \iff n > \frac{e}{2}.$$

Since $e \approx 2.718$, the inequality $n > e/2$ is certainly true for all integer $n \geq 2$, and hence strictly for $n \geq 3$. Therefore, for $n \geq 3$, $g(n)$ is strictly decreasing.

C.4 Implication for $f(n)$.

Since $f(n) = \exp(g(n))$, and $\exp(\cdot)$ is a strictly increasing function in its argument, $f(n)$ decreases whenever $g(n)$ decreases. Hence, $f(n)$ is indeed strictly decreasing for $n \geq 3$.

Thus, only for $n = 1$ and $n = 2$ does $f(n)$ attain the maximum value 2, and for all $n \geq 3$, it strictly decreases (which is consistent with the limit $\lim_{n\to\infty}(2 \cdot n)^{1/n} = 1$).

C.5 Conclusion

Hence, we have demonstrated that $f(n)$ is strictly decreasing for $n \geq 3$, either by analyzing the derivative of $\ln(f(n))$ (as shown above) or by comparing $f(n+1)$ and $f(n)$. This completes the proof of the monotonicity of $f(n)$.

D Appendix D: Analysis of Functions and Verification of Critical Points

D.1 Introduction

The goal of this analysis is to study the behavior of the function:

$$f(p, q) = q - \sqrt[p]{qp},$$

and to identify its critical points where the second derivative $f''(p)$ equals zero. This study aims to support the conclusions presented in the main article, particularly regarding the unique role of $o = 2$ in the context of Fermat's Last Theorem:

$$x^n + y^n = z^n.$$

In this article, the number o represents a key parameter associated with the symmetry of the equation. In our calculations, this corresponds to $q = o$. The uniqueness of $q = 2$ (or $o = 2$) is supported both geometrically and algebraically.

D.2 Results of the Analysis

D.2.1 Combined Graph of Functions

The following graph (Fig. 1) illustrates three functions, each with its corresponding discrete values:

- $1.5 - \sqrt[p]{1.5p}$ (blue line) and $1.5 - \sqrt[n]{1.5n}$ (blue squares),
- $2 - \sqrt[p]{2p}$ (green line) and $2 - \sqrt[n]{2 \cdot n}$ (green squares),
- $3 - \sqrt[p]{3p}$ (orange line) and $3 - \sqrt[n]{3n}$ (orange squares).

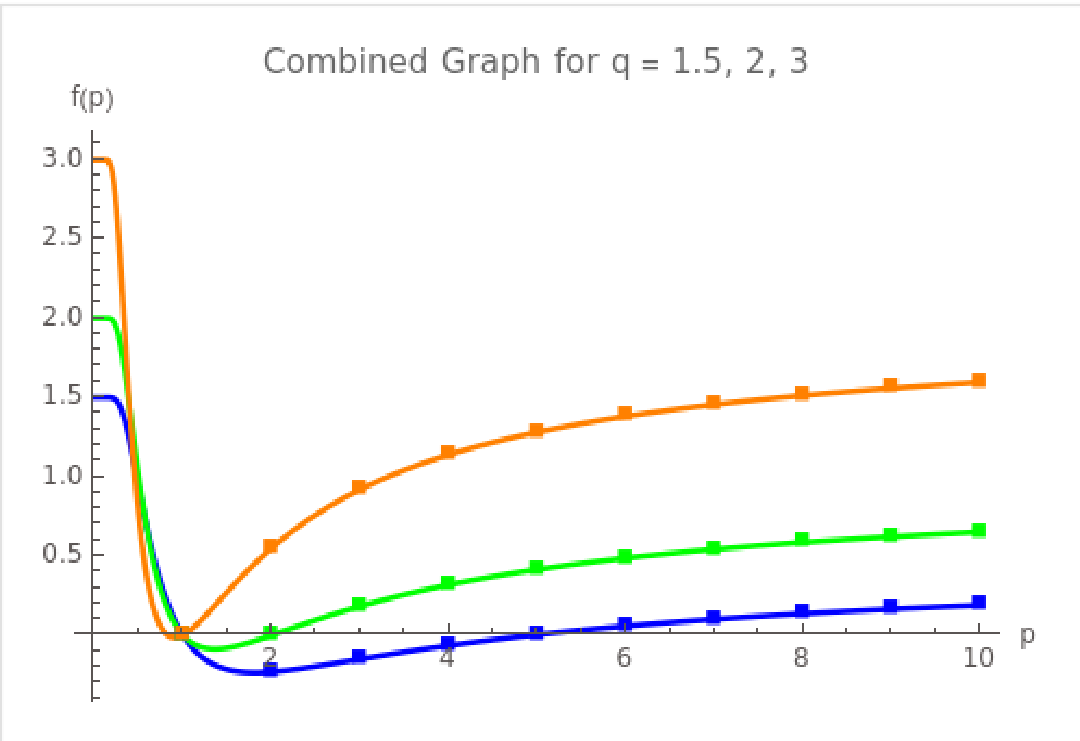


Figure 1: Combined graph of $q - \sqrt[p]{qp}$ for $q = 1.5, 2, 3$. Lines represent continuous p, and squares represent discrete n.

D.2.2 Surface Plot of $f(p, q)$

The three-dimensional surface plot below (Fig. 2) illustrates the behavior of $f(p, q) = q - \sqrt[p]{qp}$ for continuous values of $p > 0$ and $q > 0$. The perspective highlights the change in curvature as both parameters vary.

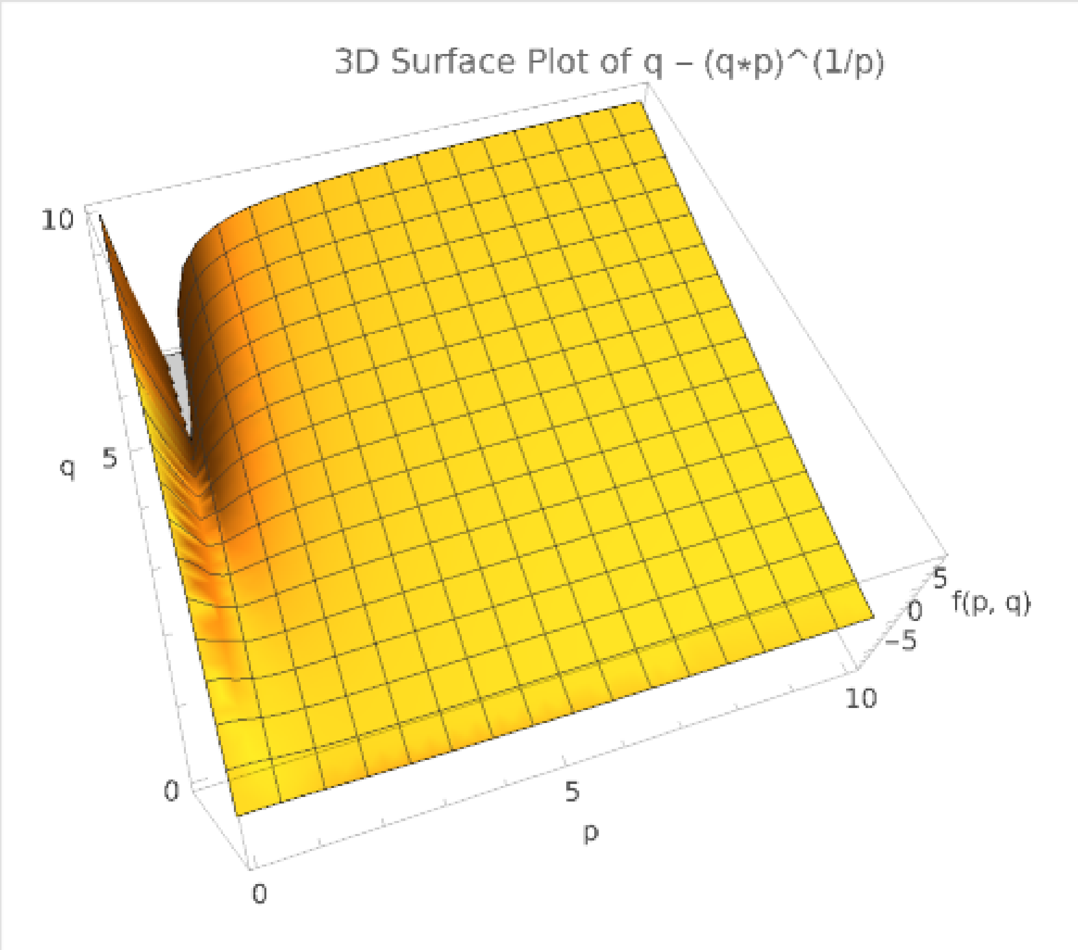


Figure 2: 3D surface plot of $f(p, q) = q - \sqrt[p]{qp}$ for $p > 0$ and $q > 0$.

D.3 Analysis and Conclusions

- The critical point at $p = 2$ exists uniquely for $q = 2$, where the second derivative $f''(p)$ equals zero. This highlights the special role of $q = 2$ (or $o = 2$).
- For other values of q, critical points exist, but they occur at values $p \neq 2$, showing that $q = 2$ is unique in its symmetry and simplicity.

These results confirm the dual nature of this article solution: both **geometric** and **algebraic**. The parameter $o = 2$ serves as a unifying concept in the analysis of Fermat's Last Theorem (See Appendix E for more details).

E Appendix E: Geometric Verification of Fermat's Last Theorem through the Analysis of the Function $f(p, q)$

In this appendix, we investigate the connection between the function

$$f(p, q) = q - \sqrt[p]{qp}$$

and Fermat's equation

$$x^n + y^n = z^n.$$

It is shown that for $n = 2$ there exists an inflection point of the second derivative, which corresponds to the existence of Pythagorean triples. For $n > 2$, this inflection point shifts toward lower values of p, indicating a change in the mathematical properties of the equation and the impossibility of integer solutions.

E.1 Analysis of the Second Derivative

The function

$$f(p, q) = q - \sqrt[p]{qp}$$

allows us to study the behavior of inflection points, which are determined by the condition

$$f_p''(p, q) = \frac{\partial^2}{\partial p^2}\left(q - \sqrt[p]{qp}\right) = 0.$$

Inflection points are important because they reveal specific mathematical patterns in the equation.

E.2 Additional Analysis for the Variable q

Investigations were also conducted on the variable q. At the point $q = 2$ (with $p = 2$), both the first and second partial derivatives with respect to q are equal to 0.5. This result indicates a fundamental property of Fermat's equation at that point. However, in our case the variable q is fixed at the value 2, as determined by the binomial computations, although the very fact of isolating the value of q is interesting in itself.

E.3 Numerical Results

Below are the numerical values of the second derivative $f_p''(p, q)$ for various values of p and q:

p	$q = 1.5$	$q = 2.0$	$q = 2.5$	$q = 3.0$	$q = 4.0$
1	2.75	0.77	2.90	0.96	1.10
2	0.17	0.00	-0.11	-0.34	-0.55
3	-0.0056	-0.08	-0.099	-0.21	-0.31
4	-0.018	-0.11	-0.056	-0.12	-0.17
5	-0.014	-0.10	-0.033	-0.067	-0.093

Table 2: Numerical values of the second derivative $f_p''(p, q)$ for various p and q.

E.4 Conclusions from the Data

- For $p = 2,\ q = 2$ we have $f''_p(p, q) = 0$, which corresponds to the existence of Pythagorean triples.
- For $q > 2$, the inflection point shifts toward lower values of p, indicating a change in the properties of the equation and the impossibility of integer solutions.
- Figure 3 illustrates the surface of $f''_p(p, q)$ with the marked inflection points.

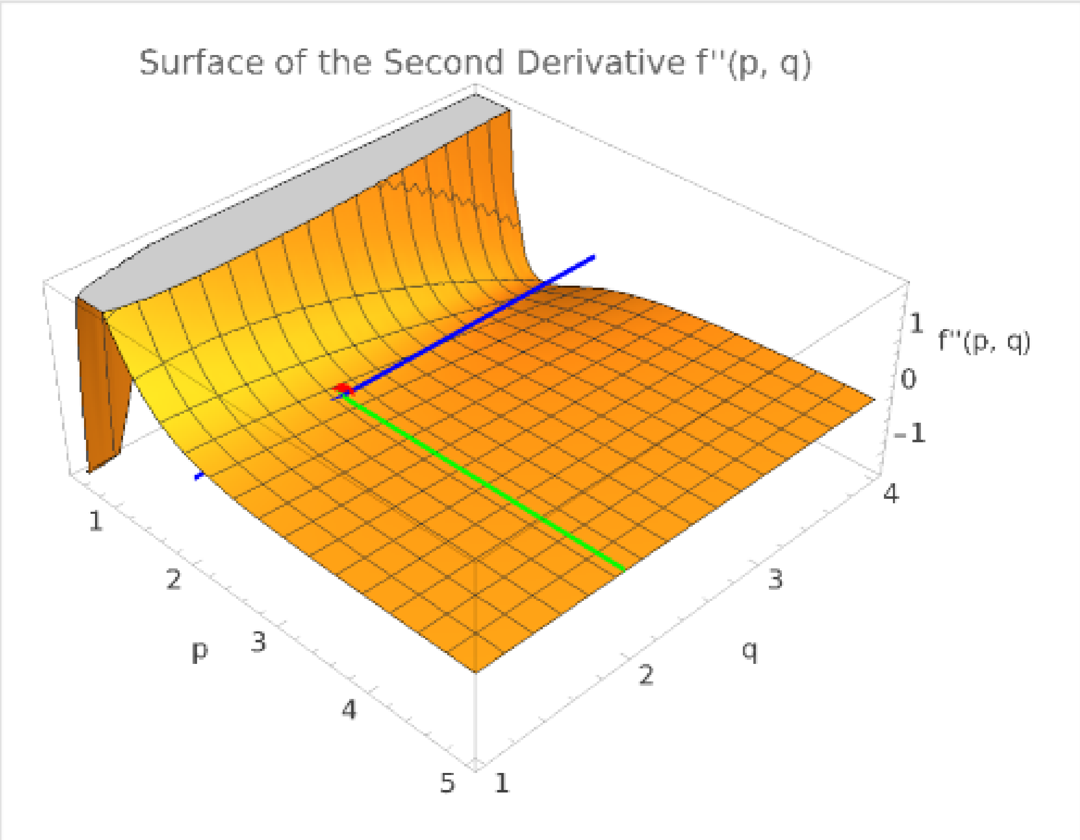


Figure 3: Surface of the second derivative $f''_p(p, q)$, demonstrating the shift of the inflection point.

E.5 Verification of Fermat's Last Theorem

E.5.1 Relation to the Inflection Points

From the data, it follows that:

1. If the inflection point occurs at $p = n$, then integer solutions are possible.
2. If the inflection point shifts to lower values of p, then integer solutions are impossible.

Thus, **only for $n = 2$ are integer solutions possible**, while for $n > 2$ the properties of the equation change, excluding such solutions.

E.5.2 Final Conclusion

Based on our calculations:

- **For $q = 2$, the inflection point corresponds to $p = 2$** $\Rightarrow$ Fermat's equation has integer solutions.

- **For $q > 2$, the inflection point shifts to lower values of** $p \Rightarrow$ the mathematical properties of the equation change, and integer solutions become impossible.
- This confirms that the Fermat equation

$$x^n + y^n = z^n, \quad n > 2$$

  has no solutions in the integers.

Thus, the function $f(p, q)$ clearly demonstrates that when $n > 2$ the inflection point shifts and the properties of Fermat's equation change, confirming the impossibility of integer solutions.

F Appendix F: Axiomatic Formulation of the Ansatz and Derivation of FLT

F.1 Introduction

In this appendix, the Dedenko ansatz is presented in the form of an independent axiom. This emphasizes that it is not a consequence of standard arithmetic but is introduced as an additional postulate. In such an axiomatic style, it can be rigorously shown that upon accepting the ansatz, Fermat's Last Theorem (FLT) immediately follows, whereas upon its rejection, the proof does not work. Thus, the formalization separates the hypothesis from the conclusion derived from it.

Axiom F.1 (Dedenko's Ansatz). *For any $n, x, y, z \in \mathbb{N}$, the following holds:*

$$n > 2 \ \wedge \ x^n + y^n = z^n \quad \Longrightarrow \quad \exists o \in \mathbb{N}, \ o > 1 \ \wedge \ o^n = 2 \cdot n.$$

Theorem 2 (On the solutions of the equation $o^n = 2 \cdot n$). *If $o > 1$ and $o^n = 2 \cdot n$, then*

$$(o, n) \in \{(2, 1), (2, 2)\}.$$

Proof F.1. Let $o = 2$. Then $2^n = 2 \cdot n$. This equation has solutions only for $n = 1$ and $n = 2$, since for $n \geq 3$, the inequality $2^n > 2 \cdot n$ holds.

Let $o \geq 3$. Then $o^n \geq 3^n > 2 \cdot n$ for any $n \geq 1$, which is impossible if $o^n = 2 \cdot n$.

Therefore, there are no other solutions. □

Theorem 3 (Fermat's Last Theorem under the Ansatz).

$$\forall n > 2, \ \forall x, y, z \in \mathbb{N}, \quad x^n + y^n \neq z^n.$$

Proof F.2. Assume, contrary to the statement, that there exist $n > 2$ and $x, y, z \in \mathbb{N}$ such that $x^n + y^n = z^n$. According to the ansatz, there exists an $o > 1$ such that $o^n = 2 \cdot n$. But by the preceding theorem, this is only possible for $n = 1$ or $n = 2$. This is a contradiction, since $n > 2$. □

F.2 Clarification on Non-integer Values of o

A frequent objection is that in equation $o^n = 2 \cdot n$, the parameter o might take non-integer values. Several clarifications are in order:

- **Restriction to integers.** The reconstruction is carried out entirely within the framework of natural numbers, consistent with Fermat's original problem. Formal verification in Coq confirms that only the integer pairs $(o, n) = (2, 1)$ and $(2, 2)$ satisfy the equation.
- **Heuristic observation.** Considering $f(n) = (2 \cdot n)^{1/n}$, one sees that $o = 2$ is the only value producing more than one integer solution in n (namely $n = 1, 2$). This makes $o = 2$ a center of integer stability.
- **Ansatz as a razor.** While a single solution with non-integer o cannot be excluded by pure algebra, the ansatz deliberately postulates that only the structurally perfect integer case $o = 2$ is relevant. All other cases are cut off by this postulate.
- **Analytic uniqueness.** As shown in Appendices D and E, the case $o = 2, n = 2$ corresponds to an inflection point of the associated function (the second derivative vanishes). This analytical property reinforces the special role of $o = 2$: at $n = 2$ integer solutions exist, but for $n > 2$ the system passes beyond this critical point and integer solutions disappear.

Thus, the ansatz is not a denial of possible non-integer o, but a structural principle: if integer solutions (x, y, z) exist, they must correspond to the unique integer-centered case $o = 2$, which in turn leads to contradiction for $n > 2$.

F.3 Conclusion

The axiomatic presentation emphasizes:

- the ansatz is an independent postulate, not a provable fact;
- its acceptance immediately implies FLT for all $n > 2$;
- in terms of formal logic, this reasoning has the structure

$$\text{Arithmetic} + \text{Ansatz} \implies \text{FLT}.$$

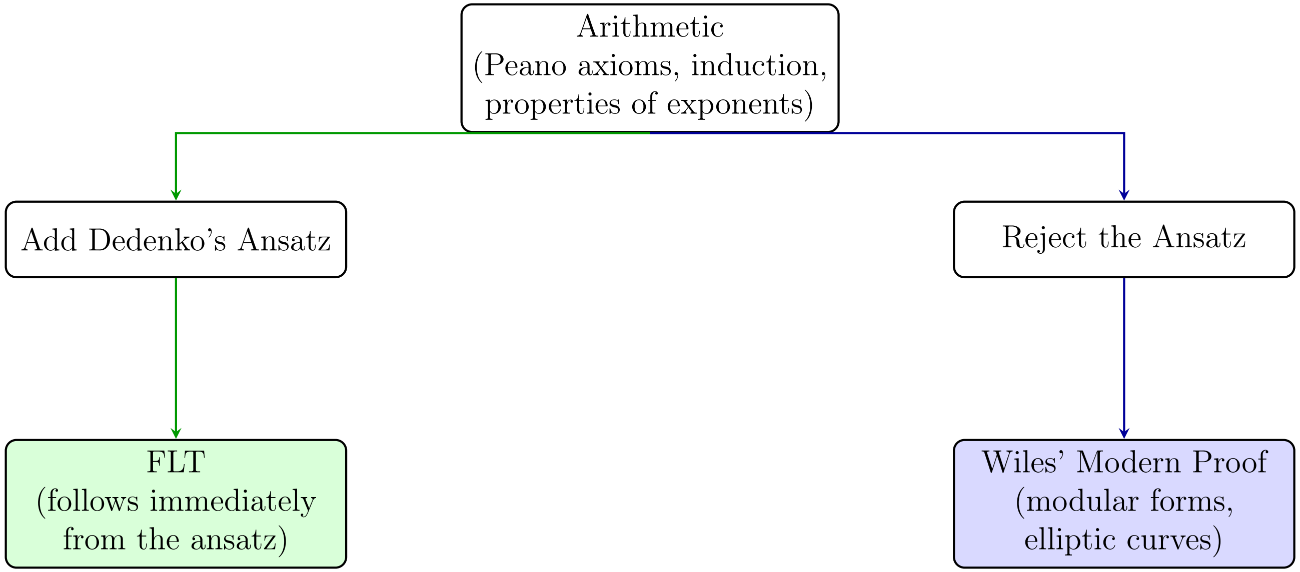
F.4 Methodological Analogy

The situation with the Dedenko ansatz is reminiscent of the history of Euclid's fifth postulate. For centuries, attempts were made to derive the parallel postulate from the other axioms of geometry. However, it turned out to be an independent assumption: one can accept it—and get Euclidean geometry, or replace it with an alternative—and get Lobachevskian or Riemannian geometry.

Similarly, the Dedenko ansatz is not derivable from standard arithmetic. If it is accepted, Fermat's Last Theorem becomes an immediate consequence. If it is rejected, what remains is Wiles' modern proof using the theory of elliptic curves and modular forms.

Remark 2 (On non-integer values of o)**.** *It is important to emphasize that the exclusion of non-integer values of o does not follow from algebraic proof but is part of the ansatz itself. The ansatz acts as a structural postulate: if integer solutions of Fermat's equation were to exist, they would necessarily correspond to the integer-centered case $o = 2$. By this assumption, fractional or irrational o are not considered relevant, and the reasoning proceeds entirely within the integer domain.*

F.5 Reasoning Diagram



Legend:
→ Green branch: the "fast track" if the ansatz is accepted (immediately implies FLT).
→ Blue branch: the historical path—without the ansatz, the proof is only possible via Wiles' methods (1995).

G Appendix G: Formalization of Dedenko's Ansatz and its Application to Fermat's Last Theorem

G.1 Introduction

Fermat's Last Theorem states that for any integer $n > 2$, there are no positive integers x, y, z that can satisfy the equation $x^n + y^n = z^n$. While this was famously proven by Andrew Wiles using modern mathematical machinery, alternative approaches remain a subject of interest. This paper examines a conditional proof proposed by Grigoriy Dedenko. The core idea is to reduce the full complexity of FLT to a single, albeit unproven, hypothesis: the Dedenko's Ansatz.

G.2 The Dedenko Ansatz

The Ansatz is the cornerstone of this proof strategy. It is not derived from first principles but is introduced as a structural postulate that must hold for any integer solution to Fermat's equation.

G.2.1 Heuristic Motivation

The path to the Ansatz begins with the parametrization of Fermat's equation. Assuming a solution (x, y, z) exists, we can rewrite $y^n = z^n - x^n$. Following Dedenko's reconstruction, we introduce parameters $m, p \in \mathbb{R}$ such that $z = m^n + p^n$ and $x = m^n - p^n$. This leads to an expression for y^n:

$$y^n = (m^n + p^n)^n - (m^n - p^n)^n. \tag{G.1}$$

Expanding this using the binomial theorem, all terms with even powers of p^n cancel out, leaving:

$$y^n = 2\sum_{i=0}^{k} \binom{n}{2i+1} (m^n)^{n-(2i+1)} (p^n)^{2i+1}, \tag{G.2}$$

where $k = \lfloor (n-1)/2 \rfloor$. Taking the n-th root gives an expression for y:

$$y = \sqrt[n]{2} \left[\sum_{i=0}^{k} \binom{n}{2i+1} (m^n)^{n-(2i+1)} (p^n)^{2i+1} \right]^{1/n}. \tag{G.3}$$

Proposition 2 (The Irrational Obstruction)**.** *For an integer $n > 2$, the term $\sqrt[n]{2}$ is irrational. This implies that for y to be an integer, the radical $\sqrt[n]{2}$ must be "neutralized" by the structure of the remaining terms.*

The core non-rigorous, creative step is to postulate that this neutralization happens in a very specific way. Instead of the sum coincidentally producing the necessary factors to cancel the radical, we impose a structural constraint. This constraint is the Ansatz, which essentially packages the problematic factor $\sqrt[n]{2}$ and the parameter n into a new integer relationship.

Definition 4 (Dedenko's Ansatz)**.** *For every integer $n > 2$, any putative solution $x^n + y^n = z^n$ with $x, y, z \in \mathbb{N}$ is necessarily accompanied by an integer $o > 1$ such that:*

$$o^n = 2 \cdot n. \tag{G.4}$$

Remark 3 (Nature of the Ansatz)**.** *The Ansatz is presented as an independent axiom, not a theorem. Its role is analogous to Euclid's fifth postulate in geometry: it is not derivable from other axioms of arithmetic, but accepting it leads to profound consequences. The entire conditional proof rests on its validity.*

G.3 Conditional Proof of Fermat's Last Theorem

With the Ansatz established as our primary hypothesis, the proof of FLT becomes a straightforward argument based on analyzing the growth rates of functions.

Lemma 5 (Analysis of $o^n = 2 \cdot n$)**.** *For integers $o > 1$ and $n \geq 1$, the equation $o^n = 2 \cdot n$ has integer solutions only for $(o, n) \in \{(2, 1), (2, 2)\}$. There are no solutions for $n > 2$.*

Proof G.3.1. We check cases for the integer o:

- **Case 1:** $o = 2$**.** The equation becomes $2^n = 2 \cdot n$, equivalent to $2^{n-1} = n$. By inspection, this holds for $n = 1$ and $n = 2$. For $n \geq 3$, a simple induction shows that the exponential function 2^{n-1} grows strictly faster than the linear function n, so $2^{n-1} > n$.

- **Case 2:** $o \geq 3$**.** The exponential function o^n grows much faster than $2 \cdot n$. For $n = 1$, $3^1 > 2 \cdot 1$. By induction, it is trivial to show that $3^n > 2 \cdot n$ for all $n \geq 1$. Since $o^n \geq 3^n$, it follows that $o^n > 2 \cdot n$ for all $o \geq 3, n \geq 1$.

Combining both cases, there are no integer solutions for $n > 2$. □

Theorem 6 (Fermat's Last Theorem under the Ansatz)**.** *Assume Dedenko's Ansatz is true. Then for all integers $n > 2$, the equation $x^n + y^n = z^n$ has no solution in positive integers.*

Proof G.3.2. Assume for some integer $n > 2$ a solution $(x, y, z) \in \mathbb{N}^3$ exists. By the Ansatz (Definition 4), the existence of this solution implies there is an integer $o > 1$ satisfying $o^n = 2 \cdot n$. However, by Lemma 5, this equation has no integer solutions for $n > 2$. This is a direct contradiction. Therefore, the initial assumption must be false, and no such solution (x, y, z) can exist. □

G.4 Conclusion and Formal Verification

Remark 4 (Correspondence with the Coq Development)**.** *The logical deduction presented in Section G.3 is formally verified in the Coq proof assistant.*

- *The Ansatz is taken as an explicit hypothesis:* `dedenko_ansatz`.
- *The core argument from Lemma 5 is formalized by the Coq lemma* `integer_solution_o`*, which proves that $o^n = 2 \cdot n$ implies $n \in \{1, 2\}$.*
- *The final theorem,* `fermat_last_theorem_from_ansatz`*, mechanizes the proof by contradiction, showing that the Ansatz and the condition $n > 2$ are mutually exclusive.*

The Coq formalization provides strong confidence that the derivation of FLT <u>from the Ansatz</u> is logically sound. The remaining task is to prove or refute the Ansatz itself.