Great Britain Journals Press

London Journal of Research In Science: Natural and Formal

General Section

RESEARCH FINGERPRINT

IDENTIFIER
LJRS-227672

PEER REVIEW
Double Blind

SIMILARITY CHECK
Perplexity AI and iThenticate

ACCESS
Open Access

LANGUAGE
English

PRINT ISSN
2631-8490

ONLINE ISSN
2631-8504

EDITION

ABBREVIATION
LJRS

VOLUME
26

ISSUE
8

YEAR
2026

KEY DATES

RECEIVED
2026-05-05

ACCEPTED
2026-05-21

ONLINE PUBLISHED
2026-06-29

PUBLISHED
2026-05-22

CATALOGING

CROSSMARK DOI
10.34257/LJRS227672UK

MSC CLASS
11D41, 11G05

ARXIV CLASS
math.NT

UDC CLASS
511.5

Article Record

Fermat's Last Theorem Revisited: Finding a Simple Proof for FLT using the Two Factors, One Even, the other Odd of $z^n - y^n$ with z and y Odd Numbers

CORRESPONDENCE

AUTHORS & AFFILIATIONS

Dr. John R Szendrey Wisdom *

ABSTRACT

A model for describing and discovering a mathematical solution to a difficult conjecture: the case of Fermat's last theorem. This implies observation, data analysis, heuristics, intuition, and sometimes serendipity. We shall provide some ideas into finding a solution to the last theorem. The important thing is not only to follow known methods of proof but also to see the problem in a different light, and look in many directions. We shall endeavour to suggest a simple proof for the case of n = 3. Femat's Last Theorem (FLT) stipulates correctly that there is no integer solution for $z^n = x^n + y^n$ when n > 2, in terms of z, x, and y whole numbers. The main search has been to find a counterexample or prove that there is none, so if $z^n - y^n = x^n$, and $z^n - y^n$ / A and B, when $A = a^n$ and $B = b^n$, we can make $A = 2^n$, divide the equation and find B, and show that when a is an integer, b cannot be an integer, but rather an irrational number, however for x to be an integer, a and b must be integers, and that is not possible. Moreover we have also found a way of showing that x is irrational.

Index Terms: data analysis • heuristics • serendipity • Diophantine equations • Gödel's theorem • Euler's proof • Wiles proof • modus tollens

FUNDING
No external funding was declared for this work.

CONFLICTS
The author declares no conflicts of interest regarding the publication of this paper.

AI USAGE
No generative AI was used for analysis or results.

HOW TO CITE
Wisdom (2026). Fermat's Last Theorem Revisited: Finding a Simple Proof for FLT using the Two Factors, One Even, the other Odd of $z^n - y^n$ with z and y Odd Numbers. London Journal of Research In Science: Natural and Formal, 26(8), 1-10. DOI: 10.34257/LJRS227672UK

METADATA CONTINUATION

AUTHOR CONTACT QR LEDGER

Dr. John R Szendrey
Wisdom*

ARCHIVAL RECORD

LJRS · Vol 26 · Issue 8 · 2026

Article ID LJRS-227672 · DOI 10.34257/LJRS227672UK

Print ISSN 2631-8490 · Online ISSN 2631-8504

CROSSREF DOI 10.34257/LJRS227672UK

RESEARCH ARTICLE

Fermat's Last Theorem Revisited: Finding a Simple Proof for FLT using the Two Factors, One Even, the other Odd of $z^n - y^n$ with z and y Odd Numbers

Dr. John R Szendrey Wisdom*

Abstract

A model for describing and discovering a mathematical solution to a difficult conjecture: the case of Fermat's last theorem. This implies observation, data analysis, heuristics, intuition, and sometimes serendipity. We shall provide some ideas into finding a solution to the last theorem. The important thing is not only to follow known methods of proof but also to see the problem in a different light, and look in many directions. We shall endeavour to suggest a simple proof for the case of n = 3. Femat's Last Theorem (FLT) stipulates correctly that there is no integer solution for $z^n = x^n + y^n$ when n > 2, in terms of z, x, and y whole numbers. The main search has been to find a counterexample or prove that there is none, so if $z^n - y^n = x^n$, and $z^n - y^n$ / A and B, when $A = a^n$ and $B = b^n$, we can make $A = 2^n$, divide the equation and find B, and show that when a is an integer, b cannot be an integer, but rather an irrational number, however for x to be an integer, a and b must be integers, and that is not possible. Moreover we have also found a way of showing that x is irrational.

Keywords: *data analysis, heuristics, serendipity, Diophantine equations, Gödel's theorem, Euler's proof, Wiles proof, modus tollens*

Correspondence: Dr. John R Szendrey Wisdom

1 Introduction

Fermat was working with Pythagorean triples when he wrote: "It is impossible to separate a cube into two cubes, or a fourth power into two fourth powers, or in general, any power higher than the second, into two like powers. I have discovered a truly marvellous proof of this, which this margin is too narrow to contain."

Fermat was studying Diophantus's major work Arithmetica, which seemingly inspired Fermat's conjecture. The book had been translated into Latin and published in 1621 by Claude Bachet. Fermat was working on Problem II.8 of Arithmetica which raises the question: how can a given square number be split into two other squares; in other words, for a given rational number k, find rational numbers u and v such that $k^2 = u^2 + v^2$.

Now Diophantus chose an even square 16, and he showed how to solve this sum-of-squares problem for $k = 4$ (the solutions being $u = 16/5$ and $v = 12/5$). However, the difference between u and v, $u^2 - v^2$, , has a solution in natural numbers: $16 = 5^2 - 3^2$, and corresponds to the first Pythagorean triple known. Thus, we can reformulate the problem in these terms: if we have $w^2 = u^2 - v^2$, where w is even, and u and v are odd, then if there is an integer solution for $w^2 = u^2 - v^2$, there will not be one for $w^2 = u^2 + v^2$, and this observation leads as to the case of $w^4 = u^4 - v^4$, which splits up into: $w^4 = (u^2 - v^2)(u^2 + v^2)$ which we shall develop later.

We find Fermat's comments on Livre II, problem 8 in E. Bassine [1], p. 53.

This is what Fermat wrote in the margin: Décomposer un cube en deux autres cubes, une quatrième puissance, et généralement une puissance quelconque en deux puissances du même nom, est une chose impossible, et j'en ai assurément trouvé l'admirable démonstration. La marge trop exiguë ne la contiendrait pas.

The problem of Fermat's conjecture can be stated as follows:

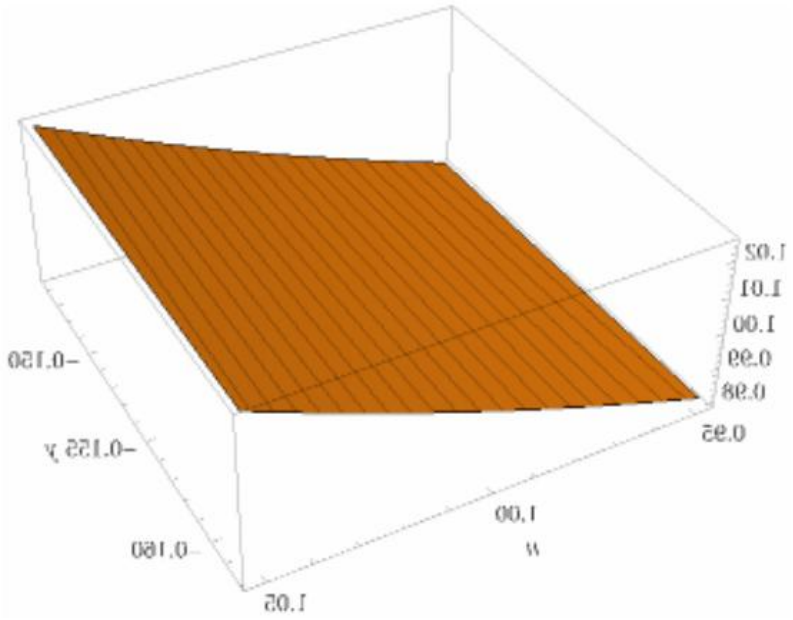
With $n, x, y, z \in \mathbb{N}$ and $n > 2$, the equation $x^n + y^n = z^n$ has no integer solutions. In other words, we must prove that there is no counterexample, which Wiles indeed proved, but the proof was outside the realm of 17^{th} century mathematics, and used the logic of modus tollens, so how did Fermat arrive at this conjecture? Why did the ancient Greeks take no notice of it? There are an infinite number of triples for $n = 2$ and none for $n = 3$ or n greater than 3. Today we have counterexamples for $n = 4$, with 3 terms equal to a fourth term, or $n = 5$, with 4 terms equal to a fifth one. But Fermat was not aware of these examples, as they were found using the computer. Many values of n have been proved starting with Euler in 1770 for $n = 3$.

Andrew Wiles [2] finally proved the conjecture which became known as the Fermat Wiles theorem in 1995. However, the proof was not explicit, but implicit requiring the epsilon theory implying that if the Frey Curve did exist, there would be a counterexample for FLT. However the Frey curve, if it existed would not be modular, and Wiles, by proving the modular theorem, showed that all elliptic curves are modular, ruled out the possibility of the existence of the Frey curve, and thus proved Fermat's conjecture to be true.

Wiles' proof is based on modus tollens. If we can demonstrate that something is true, and this implies that something else is false, in this case the Frey curve, this implies that there is no counterexample to FLT. In fact, if a specific curve does not exist, then FLT has no counterexample, thus it has been proved. Maybe there is another direction we can take to demonstrate the theorem.

$$B = [(y + 2^n)^n - y^n]/2^n$$

The even number (z − y) divides the equation leaving B.



Graph 1: The second factor of the FLT equation: $[(y + 2^n)^n - y^n]/2^n$

This was from Wolfram Alpha. We shall meet this equation later.

Computer programs allow us to test results and find and explore new patterns that might emerge unexpectedly.

Here is a program with Excel. We will use this to verify our hypothesis concerning the division of the equation by A and B, the even and odd factors.

Program for finding b with $b^n = [(y + 2^n)^n - y^n]/2^n$. This is given below in Table 1. Finding the value of b will be dealt with when we show that b cannot be an integer. Note that z and y are odd integers, and the equation $z^n - y^n = x^n$ (1) with $z - y = 2^n$, and $z = y + 2^n$. We shall show that when we divide equation (1) by 2^n, and when the odd factor $B = b^n$, b cannot be an integer. In fact $x^n = a^n b^n$ so if we make $a = 2$, $x = 2b$, and as b is not a natural number, x cannot be a whole number either, so there is no possible counter example for FLT. Program 1 beneath allows us to find the value of B and b for any integer value of y, and n.

		imput	
n	exponent	3	
y	first value	5	
z	equal to	13	
	$y + 2^n$		
equation	$z^n - y^n$		2072
Divided by 2^n	B		259
n^{th} root of B	b		6,374311

Program 1: Finding the value of B, the odd factor of $(y + 2^n)^n - y^n$ and the value of b

2 Background of FLT

2.1 Infinite descent

A proof by infinite descent is a proof by contradiction. This was developed by Fermat around 1637, and is used to prove that "certain properties or relations are impossible for whole numbers, by proving that if they held for any numbers, they would hold for some smaller numbers, then by the same argument they would hold for some numbers that were smaller still, and so forth ad infinitum, which is impossible because a sequence of positive whole numbers cannot decrease infinitely. This would lead to an infinite descent and ultimately a contradiction." H. M. Edwards [3]. This method is used to prove FLT for $n = 3$.

A proof by infinite descent is a type of proof by contradiction. As natural numbers are well ordered $(1, 1+1, 2+1 \ldots)$, there can only be finite numbers smaller than any given number. ($1 < 2 < 3 \ldots$.). One begins with an initial premise that a solution to a problem exists. Then if such a relationship existed between two or more natural numbers, it would exist between two or more smaller numbers (analogy), and so on until we reach rock bottom.

Using mathematical induction, this process could go on but not infinitely. Thus, there would be a contradiction between the original premise and the result of the descent.

The process of descent can be shown to prove the irrationality of $\sqrt{2}$.

The square root of 2 cannot be expressed as a fraction of two integers. For example, the diagonal of a square cannot be measured in terms of integers.

Using the theorem of Pythagoras, if a square has sides each of length a, then $a^2 + a^2 = b^2$, so we can find the diagonal, b, with $b^2 = 2a^2$. Consequently, $b = a\sqrt{2}$.

2.1.1 Proof by descent.

Let us suppose that $\sqrt{2}$ was rational.

It could be written as $\sqrt{2} = p/q$ where p and q are two natural numbers. Square each side, we have: $2 = p^2/q^2$, and $2q^2 = p^2$. Consequently 2 must be a factor of p^2 and therefore p. As 2 is a factor of p, we can express p as twice some number, for example r.

Thus, $p = 2r$. Now $2q^2 = p^2 = (2r)^2 = 4r^2$ and $q^2 = 2r^2$.

Let the descent begin: 2 must be a factor of q. So, q can be equal to $2s$, where s is some natural number. Therefore, p/q can be expressed as $2r/2s$. Consequently, p and q are not the smallest natural numbers in the equation $\sqrt{2} = p/q$, but $\sqrt{2} = r/s$. Thus $r < p$, $s < q$. If $\sqrt{2}$ were rational, it could be expressed with even smaller numbers. However, this process cannot go on forever. As a conclusion, there is a contradiction with the initial premise, so $\sqrt{2}$ is irrational.

Supposition → Descent → Contradiction → Conclusion

Diagram 1: The four stages of infinite descent

2.1.2 Fermat's proof for $n = 4$ (Proof by descent).

There are no integer solutions to $x^4 + y^4 = z^4$ where $xyz \neq 0$.
We can assume that x^2, y^2, z are co-primes and rewrite the equation $(x^2)^2 + (y^2)^2 = z^2$.
Using Pythagorean Triples, there exist two numbers p, q with $p > q > 0; x^2 = 2pq$.

$$y^2 = p^2 - q^2$$
$$z = p^2 + q^2$$

We find another triple since $y^2 + q^2 = p^2$.
Consequently, there must exist numbers a, b such that:

$$q = 2ab$$
$$y = a^2 - b^2$$
$$p = a^2 + b^2$$

a and b are relatively prime.
Combining the above equations, we have:
Since ab and $a^2 + b^2$ are relatively prime, they must both be squares as they equal a square number. So, there exists a number r such that $r^2 = a^2 + b^2$.
Here begins the infinite descent since:

$$r^2 = a^2 + b^2 = p < p^2 + q^2 = z < z^2.$$

This can go on and on but must stop as the descent of natural numbers is not infinite.
Noguès, R. [4]
Consequently, a solution to the initial equation implies the existence of another smaller square that has the same properties.
Natural numbers form a coherent framework within the Pythagorean triple system.
Consequently, there can be no numbers outside that this system might provide solutions for. We must look for proof of Fermat's conjecture within this framework. The manner of proving the theorem to be correct, and Fermat's conjecture to be right, did not study the relations between natural numbers but the algebra of equations. Fermat's equation and proof for $n = 4$ interesting as it is, could have been approached in a different way.
Many if not all of the proofs for FLT with different values of n made use of the method of infinite descent.

2.1.3 Euler's Proof for $n = 3$.

We shall now examine the proof presented by Euler in 1774.
Theorem: the sum or the difference between two cubes cannot be a cube.
To begin with, we must bear in mind the factoring of two cubes:

$$x^3 + y^3 = (x + y)(x^2 - xy + y^2)$$

If two numbers are the sums of two squares, then their product is also the sum of two squares.

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2.$$

Leonard Euler (1707–1783) gave a proof of Fermat's theorem for $n = 3$, but this was considered incomplete. Our source is Noguès [4] and Edwards [3]. Both writers set out the proof and explain it.
Table 1 sets out the different proofs of FLT. We see that the researchers concentrated on specific values of n, using infinite descent. But there is no general proof.

Table 1. Proof for other values of n

Exponent	Solver	Year
4	Fermat	1640
3	Euler	1753
5	Legendre	1825
7	Lamé	1839
37	Kummer	1847
< 100	Kummer	1857
$< 125,000$	Wagstaff	1978
$< 4,000,000$	Buhler et al.	1993

2.2 Comments on Andrew Wiles' proof

2.2.1 Andrew Wiles' career.

In May 2018, Wiles was appointed Regius Professor of Mathematics at Oxford.
The British Mathematician Andrew Wiles was born on 11th April 1953; he is the son of Maurice Frank Wiles and Patricia Wiles. He received his Bachelor's degree in Mathematics at Merton College (Oxford). He also carried out research at Clare College, Cambridge and finally got his PhD in 1980[1].His mathematical research was on the methods of the Iwasawa Theory[2] to work on the arithmetic of elliptic curves with complex multiplication.
He continued the idea of proving the Fermat Theorem in 1986, when Ribet had already proven Serre's ϵ-conjecture and as a result had formulated a connection between Fermat's Last theorem and the Taniyama-Shimura conjecture. Andrew Wiles presented this idea in 1993 publicly in a conference at Cambridge, but there was a shortcoming within the proof. Consequently, with the help of his ex-student, Richard Taylor, in 1994 he was able to fully support the proof which was published in *Annals of Mathematics*[3].

2.2.2 The structure of the proof.

It is required to prove the modularity theorem (MT) for elliptic curves. If this is proved, then the Frey curve[4] (FC), given by the equation $y^2 = x(x - a)(x + b)$ is impossible as it is not modular, and all elliptic curves are modular if MT is true. If this is so, there is no counterexample for FLT.
If MT is true, then FC is not true (modus tollens).

$$MT \Rightarrow \neg FC$$

If the FC is true, then a counterexample, CE, exists for FLT (modus ponens).

$$FC \Rightarrow CE$$

Wiles proved MT, and consequently there is no counterexample for FLT
The modularity theorem
Modularity: The modularity theorem, also known as the Taniyama—Shimura conjecture, asserts that every elliptic curve defined over the rational numbers is modular. This means that it has no cusps. A semistable elliptic curve may be described as an elliptic curve that has bad reduction only of a multiplicative type. This is the case where the reduced curve has one singular point with two distinct tangents. We see this in Figure 2 below.

[1]source https://www.famous-mathematicians.com/andrew-wiles/
[2]chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/http://staff.ustc.edu.cn/~yiouyang/iwasawa.pdf by Yi Ouyang, Department of Mathematical Sciences Tsinghua University
[3]Modular elliptic curves and Fermat's Last Theorem From Volume 141 (1995), Issue 3 by Andrew Wiles
[4]https://en.wikipedia.org/wiki/Frey_curve

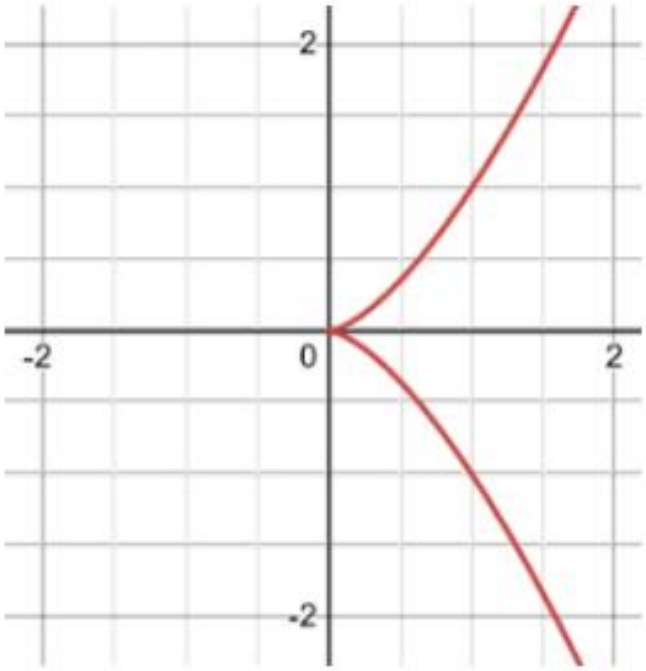


Figure 2. An example of a curve with bad reduction[5]

Curiously, Fermat proposed the following equation and the solutions.

$$y^3 = x^2 + 2$$

Solutions are $y = 3$, $x = \pm 5$. We do not have Fermat's proof.

Here is Wiles' introduction to his paper proving the Modular Theorem and consequently implicitly proving FLT. However this was made possible by the findings of other scientists.

"An elliptic curve over $\mathbb{Q}$ is said to be modular if it has a finite covering by a modular curve of the form $X_0(N)$. Any such elliptic curve has the property that its Hasse-Weil zeta function has an analytic continuation and satisfies a functional equation of the standard type. If an elliptic curve over $\mathbb{Q}$ with a given j-invariant is modular then it is easy to see that all elliptic curves with the same j-invariant are modular (in which case we say that the j-invariant is modular). A well-known conjecture which grew out of the work of Shimura and Taniyama in the 1950's and 1960's asserts that every elliptic curve over $\mathbb{Q}$ is modular. However, it only became widely known through its publication in a paper of Weil in 1967 [We] (as an exercise for the interested reader!), in which, moreover, Weil gave conceptual evidence for the conjecture. Although it had been numerically verified in many cases, prior to the results described in this paper it had only been known that finitely many j-invariants were modular. In 1985 Frey made the remarkable observation that this conjecture should imply Fermat's Last Theorem. The precise mechanism relating the two was formulated by Serre as the ϵ-conjecture and this was then proved by Ribet in the summer of 1986. Ribet's result only requires one to prove the conjecture for semistable elliptic curves in order to deduce Fermat's Last Theorem."

We shall now examine the case of the Frey Curve which leads us to the proof of FLT.

The Frey Curves

In 1975, Yves Hellegouarch [5], a French mathematician from the Ecole Normale (ULM) wrote a paper on elliptic curves in *Acta Arithmetica*[6]. Those curves were associated with Fermat's last theorem. Hellegouarch associated solutions (a, b, c) with FLT. The curve consists of all points in the plane whose coordinates (x, y) satisfy the relation: $y^2 = x(x - a^n)(x + b^n)$. Such an elliptic curve would have very special properties. But it would not be modular, and as Wiles proved all elliptic curves are modular, this curve would not exist, and there would therefore be no counterexample for FLT. This curve has become known as a Frey curve.

A **Frey curve**[7] is given by the equation $y^2 = x(x - a)(x + b)$ related to an A, B, C triple. In other words, elliptic curves may provide solutions to equations. It was Yves Hellegouarch, who in 1975 put forward the idea and its relationship to Fermat's equation. "Given a prime number, p, we know there exists a constant $C(p)$ such that no abelian curve, defined under Q, allows for any rational point of order p^h for $h > C(p)$; nevertheless, the numerical value of $C(p)$, for any p is not known." (*Acta Arithmetica*, XXVI, 1975).

Gerhard Frey [6] (1982) found that the curve had unusual properties. Fermat's conjecture was now related to the Taniyama-Shimura-Weil conjecture and essentially **if there were a counterexample to Fermat's Last Theorem, there would exist a curve that would not be modular**. Frey in 1986 suggested that the Taniyama-Shimura-Weil conjecture implies Fermat's Last Theorem. In 1985, Jean-Pierre Serre proposed that a Frey curve could not be modular. This showed that a proof of the semi-stable case of the Taniyama-Shimura conjecture would imply Fermat's Last Theorem. This was the challenge given to Wiles: prove the Taniyama-Shimura-Weil conjecture.

[5] https://golem.ph.utexas.edu/category/224/03/counting_points_on_elliptic_cu.html
[6] Points d'ordre $2p^h$ sur les courbes elliptiques
[7] https://en.wikipedia.org/wiki/Frey_curve

Table 2. Theorems that allowed Wiles to prove FLT

Theorem	Discovered by	Proved by	Content	Date
Elliptic curves: Modularity theorem for semi-stable elliptic curves	Taniyama–Shimura–Weil conjecture	Andre Wiles and completed by Breuil, Conrad, Diamond & Taylor, in 2001	All semi-stable elliptic curves are modular. If A and B are whole numbers, then $y^2 = x(x - A)(x + B)$ is modular.	1993 1999
Frey–Hellegouarch curves	Any four numbers able to disprove FLT could also be used to make a semi-stable elliptic curve that could never be modular.		A counter example of FLT would create an elliptic curve which would not be modular. It remains to prove that all semi-stable elliptic curves are modular, so the Frey curve creating the counter example could not exist.	1975
Ribet's theorem	Epsilon conjecture	Ribet	$E_{a,b,c}$ is not modular.	1986
The Frey curve could not be modular		Serre Ribet		1982 1990

2.3 A study of Fermat's remarks on Diophantus

We find his remarks in Bassine's Précis des Oeuvres Mathématiques et de l'Arithmetique de Diophante, translated from Latin into French. and published in 1621 by Claude Bachet. The important question was finding the sum of two odd squares equal to 16. Now we know that the difference between two odd squares equals 16 or $\bar{4}^2$ but not the sum of two odd squares in terms of natural whole numbers. It was the study of this problem that allowed Fermat to put forward his conjecture without giving a proof. Bassine [1]. Fermat was studying Arithmetica, which seemingly inspired Fermat's conjecture. Fermat was working on Problem II.8 of Arithmetica which raises the question: how can a given square number be split into two other squares; in other words, for a given rational number $\mathbf{k}$, find rational numbers u and v such that $\hat{\mathbf{k}^2} = \mathbf{u}^2 + \mathbf{v}^2$. Now Diophantus chose an even square 16 and shows how to solve this sum-ofsquares problem for k = 4 (the solutions being $\mathrm{u} = 16/5$ and $\mathbf{v} = 12/5$). However, However, the difference between u and v, $u^2 - v^2$, has a solution in natural numbers: $16 = 5^2 - 3^2$, and corresponds to the first Pythagorean triple known. Thus, we can reformulate the problem in these terms: if we have $w^2 = u^2 - v^2$, where w is even, and u and v are odd, then if there is an integer solution for $w^2 = u^2 - v^2$, there will not be one for $w^2 = u^2 + v^2$, and this observation leads as to the case of $w^4 = u^4 - v^4$, which splits up into: $w^4 = (u^2 - v^2)(u^2 + v^2)$. We can therefore split $u^4 - v^4$ into two factors, $u^2 - v^2$, which has integer solutions, and $u^2 + v^2$, which does not.
Proof by Diophantus: To divide a given square into a sum of two squares:
We first let the square = 16 and divide 16 into a sum of two squares.
Let the first summand $\mu = x^2$, and the second $\Gamma = 16 - x^2$, which is to be a square. We make the square of the difference of an arbitrary multiple of x which is diminished by the root of 16 which is = 4.
We find the square of $(2x - 4)$, $(2x - 4)^2$ which is $4x^2 - 16x + 16$. Let this expression be equal to $16 - x^2$. Thus $4x^2 + 16 - 16x + 16 = 16 - x^2$ (artifact in OCR). Actually $4x^2 - 16x + 16 = 16 - x^2$.
Now add to both sides $x^2 + 16x$ then subtract 16. Thus, we obtain $5x^2 = 16x$, hence $x = 16/5$.
We now have 256/25 and 144/25. The sum of these numbers is 16 and each summand is a square. Thus $(16/5)^2 + (12/5)^2 = 16 = 4^2$.

2.3.1 One possible proof for $n = 4$.

Splitting the equation:
Let $z^4 + y^4 = x^4$ with z, y and x relatively prime in $N > 0$ and $z > y$.
We begin with $z^4 + y^4 = (z^2 - y^2)(z^2 + y^2) = (z - y)(z + y)(z^2 + y^2)$.
Let $A = (z^2 - y^2) = (z - y)(z + y)$ and $B = (z^2 + y^2)$. We need only prove that B is not an integer square if A is a square.
Let $z = p^2 + q^2$ and $y = p^2 - q^2$ according to the Euclid formula.
Therefore $A = (z - y)(z + y) = [(p^2 + q^2) - (p^2 - q^2)][(p^2 + q^2) + (p^2 - q^2)] = 2q^2 \cdot 2p^2$, the square root of which is $2pq$.
$B = z^2 + y^2 = (p^2 + q^2)^2 + (p^2 - q^2)^2 = 2(p^4 + q^4)$. So, A is a square, but not B.
Can we conclude that $z^4 + y^4 \neq x^2$ so not equal to x^4.

2.3.2 Statement for FLT with $n > 2$.

FLT can be stated thus: With $n, x, y, z \in \mathbb{N}$ and $n > 2$, and $x, y, z \neq 0$, the equation $x^n + y^n = z^n$ has no integer solutions. We chose z and y to be odd numbers and integers, and we must show why x is not a whole number but an irrational one.
We shall now endeavour to find a method allowing us to prove FLT. We need to show why x is not an integer, and we shall use the two factors of $z^n - y^n$ to prove this.
When $x^n = a^n b^n$, both a and b must be integers, otherwise x cannot be an integer, and we have a possible proof of Fermat's conjecture.
Let $B = z^2 + yz + y^2$. Now A is even because $z - y$, being two odd numbers is even and must be an n^{th} term to divide $z^n - y^n$, in the present case $n = 3$.
If $z^3 - y^3$ is divisible by A which itself is an even cube, we are left with B which we must prove, cannot divide (1) (which is equal to $z^3 - y^3$) with b an integer cube root, at the same time as A, when $A = a^3$. If both A and B divide (1), and are both integer cubes, then we have a counterexample, since the third term x, would also be a cube. It is easy to find values of z and y which allow A to divide (1) and leave a residual B since $z - y = 8$, and $z - y$ is the even factor of equation (1). Let us show happens. Let $z - y = 2^3 = 8$, then, $z = y + 8$. We can now take z out of the equations and see what might be the result.
We begin, by substituting $y + 8$ for z, with $z^3 - y^3 = (y + 8)^3 - y^3 = 24y^2 + 192y + 512$.
We now divide by $A = z - y = 8$ and consequently, we find $B = 3y^2 + 24y + 64$.
Let us examine this result. If $y = 1$, $B = 3 + 24 + 64 = 27 + 64 = 3^3 + 4^3$. Surprisingly we have the sum of 2 cubes. In this case, however, $B = 91$, so, b is not an integer cube root when $B = b^3$. If $y = 3$, $z = 11$, then $B = 27 + 72 + 64 = 163$.
Generalizing, for any integer value of n:

$$B = (z^n - y^n)/2^n \textbf{ if and only if } z - y = 2^n.$$

We can show this numerically using a computer program.

We can conclude that the second term of the multiples of equation (1), $B = z^2 + yz + y^2$, and we let $B = b^3$. However, b must be an integer to find the counterexample.
Let us attempt to show why B does not have an integer cube root.
Now $B = z^2 + yz + y^2 = z^2 + 2yz + y^2 - yz = (z + y)^2 - zy$ by squaring $z + y$ and subtracting zy.
Let $z + y = g$. We can see that B is not a cube with b an integer.
We can test this. If $y = 1$, then $(z + y)^2 - zy = 100 - 9 = 91$, when $z - y = 8$. For $y = 3$, $z = 11$, then $(z + y)^2 - yz = 13^2 - 33 = 136$. We can see that, in cases where $z = y + 8$, $(z + y)^2 > yz$.
When $y = 3$, $((y + 8)^3 - y^3)/8 = (3y^2 + 24y + 64)$.
For $n = 5$, we have the expansion $(z - y)(z^4 + z^3y + z^2y^2 + zy^3 + y^4)$. As $z = y + 32$.
Let $y = 1$, $z = 33$. We now have $(z^5 - y^5)/32 = (33^5 - 1^5)/32 = 122981$.
For $n = 7$, $(z^7 - y^7)/128$. If $y = 1$, $z = 129$. So, $(129^7 - 1^7)/128 = 4163092657543$.
The factors of $z^7 - y^7$ are $(z + y)(z^6 - z^5y + z^4y^2 - z^3y^3 + z^2y^4 - zy^5 + y^6)$.
So $B = (z^6 - z^5y + z^4y^2 - z^3y^3 + z^2y^4 - zy^5 + y^6)$. Proving that b is not an integer when $B = b^7$ would be difficult, but when we divide the equation by 2^7, we find B, providing $z = 2^7 + y$.

2.3.3 Generalizing for $n > 3$.

There is an easy way to prove that if a is an integer, and we chose 2 for our examples, b, the n^{th} root of B is not an integer but an irrational number.
$z^n - y^n = x^n$, and $z^n - y^n = AB = a^nb^n$.
Now $x^n = a^nb^n$, so $x = ab$. If a or b or both are not natural numbers, then x is not a whole number and the theory is proved. We can make $a = 2$ and we now have $x = 2b$.
We are now required to prove that b is an irrational number. If for example factor $A = 2^m$ and not 2^n, the theorem would also be proved without looking for the value of b.
In general, for $z^n - y^n$ we can factorise in the following way:

$$z^n - y^n = (z - y)(z^{n-1} + yz^{n-2} + y^2z^{n-3} + \cdots + z^{n-1}).$$

The even factor A always divides the Fermat equation when we choose $z - y = 2^n$.
So, we choose $z - y = 2^n$. Therefore $z = y + 2^n$. We can easily find B through division of A.
Let the first factor be $A = (z - y)$, even, the second one be $B = z^{n-1} + yz^{n-2} + y^2z^{n-3} + \cdots + z^{n-1})$ odd. With this choice of values of y and z, 2^n divides $z^n - y^n$ and the quotient is B with $B \in \mathbb{N}$. We have seen that when we divide $(z^n - y^n)$ by 2^n, the quotient is an odd natural number. It is convenient to begin with the division by 2^n, and we find B without having to calculate it from the formula. The question now is how can we prove that B has no integer n^{th} root.
We must choose z and y with $z = y + 2^n$. Otherwise a would not be an integer.
What we need to prove is that factor B does not have an integer n^{th} root.
The following equation is the one we need to solve to prove that there is no counterexample:

3 Theorem

Let us try this demonstration.
First, we let $z - y = 2^n$. So, $A = z - y$ has an n^{th} root 2, which divides equation (1), and leaves the odd number B. It would be difficult if not impossible to prove directly from the expansion of $B = b^n$, with b, an integer, that could divide the equation and leave A.
Let $[(y + 2^n)^n - y^n] = x^n = a^nb^n$. We know that $z - y = 2^n$, so, we have z in terms of y. We substitute $z = y + 2^n$ and we only keep y.

3.1 Proof of FLT

Object: To prove that A and B divide the equation $z^n - y^n = x^n$, with a a natural number, and b an irrational number, thus x is irrational since $x = ab$.
We shall now try the following method to prove this theorem. The same applies for z and y if they are the unknown values using a similar equation.
Let $z^n - y^n = 2^nb^n = A^*B$ and $z^n - y^n/A^*B = 1$.
We wish to show that b is not an integer. We divide the equation by b^n.
We now have $2^n = (z^n - y^n)/b^n$.
We divide z^n and y^n separately by b^n.
Thus $z^n/b^n - y^n/b^n = 2^n$.
And changing sides for y^n/b^n, we now have the key to our proof.
Thus $z^n/b^n = 2^n + y^n/b^n$.
We find the n^{th} root of both sides.

$$z/b = \sqrt[n]{2^n + y^n/b^n}, \text{ equation (2)}$$

and therefore, equation (2), $b = z/\sqrt[n]{2^n + y^n/b^n} = (y + 2^n)/\sqrt[n]{2^n + y^n/b^n}$ substituting $y + 2^n$ for z. The important element is $y^n/b^n = \Delta$, which will always be smaller than 1. $\Delta = y^n/b^n$ is a positive decimal and smaller than 1. Δ is also a rational number and a fraction.
Why is $\Delta < 1$? The odd factor B is in fact much larger than A. If we look at the factors for $n = 3$, we find $A = z - y$ and $B = z^2 + y^2 + zy$. On one hand, we have a subtraction of z and y, on the other the addition of two squares $z^2 + y^2$ and the product zy. This is true whatever the value of $n > 2$. Consequently, $z - y < z^2 + y^2 + zy$ and so $A < B$.

Let $\sqrt[n]{2^n + y^n/b^n} = \lambda$. Now λ must be an integer and must divide $y + 2^n$ (or z) for b to be an integer. However, B divides $z^n - y^n$ leaving 2^n. Moreover, B lies between z^n and y^n, as $z = y + 2^n$, so b^n (or B) lies between $z^n - y^n$, so $b^n > y^n$ and $b > y$. In fact, $B > A$.
Consequently, y^n/b^n is a fraction, and so λ is not an integer and cannot divide z leaving a whole number. This is the key point.
Thus, there is no counterexample for FLT, and x cannot be an integer, since $x = 2b$ and b we have shown to be irrational.
Consequently, as b cannot be an integer, and $x = 2b$, x is irrational.
We could choose $A = 2^n d^n g^n$, but the result for b would be the same. For instance, $A = 2^n 3^n 5^n$ would divide the equation and leave B but b would not be an integer as shown above.

3.2 Testing the results numerically

Let us look at some examples. Here are some numerical examples that confirm the results of our equation.

1. Let $n = 3, z - y = 8, z = y + 8$.

   If $y = 3, z = 11$. Consequently $11^3 - 3^3 = 1331 - 27 = 1304$. To find B we divide by 8, and we have 163. Using the formula, $b = z/\sqrt[3]{2^3 + y^3/b^3} = 11/\sqrt[3]{2^3 + 27/163}$.

   Now $27/163 = 0.165644172$, so $\lambda = \sqrt[3]{2^3 + 0.165644172} = \sqrt[3]{8.165644172} = 2.0137094912$.

   Now $z/\lambda = 11/2.0137094912 = 5.462555557123$.

   Let us check with the cube root of $163 = 5.46255557128$.

   Therefore, our equation allows us to find the value of b, which is irrational and indicates why it is so.

   Note that $B > A$.

2. Let us take the example of $n = 5, y = 5, z = 37$, and $z - y = 2^5$.

   Now $(37^5 - 5^5)/32 = (69343957 - 3125)/32 = 69340832/32 = 2166901 = B$. $b = z/\sqrt[5]{2^5 + y^5/b^5} = 37/\sqrt[5]{32 + 3125/2166901} = 37/\sqrt[5]{32.001442152} = 37/2.0000186 = 18.4998310429$.

   $\sqrt[5]{2166901} = 18.4998332557$. Both are identical to five decimal places.

3. Let $A = 2^3 \cdot 13^3$. We have made $a = 6$, and $A = 17576$. Now $z - y = 17576$. So, $z = y + 17576$. Let $y = 5, z = 17581$. $17581^3 - 5^3 = 5434138733941 - 125 = 543438733816$. $543438733816/17576 = 309179491 = B$. $\lambda = \sqrt[3]{15776 + 0.0000568635933992} = \sqrt[3]{15776.0000568635933992} = 25.0802753$. Now $z/\lambda = 17581/25.0802753 = 700.989116$. Cube root of $B = 700.989116$. So, when A is equal to an n^{th} root of an even number, then we can see that b is not an integer.

Example shows that when n or y become greater and greater, the value of y^n/b^n which we call Δ, becomes smaller and smaller and probably tends to 0.

3.2.1 Direct demonstration of the irrationality of x.

The following demonstration shows directly why x is irrational whatever the value of $n > 2$.
We use the same algorithm we used to find b: express the equation, divide by the RHS. Take the second term to the RHS. Find the n^{th} root of both sides, and express the result equal to x. We can clearly see why x is irrational, and cannot therefore be a natural number, consequently, there can be no counterexample for FLT.
Let $z^n - y^n = x^n$, where z and y are odd, x is even. We wish to show that x is not an integer and is in fact irrational. We will use the same method and equation above to prove b is irrational.
Now $z^n/x^n - y^n/x^n = 1$.
Therefore, $z^n/x^n = 1 + y^n/x^n$
We now take the n^{th} root of both sides, and we have $z/x = \sqrt[n]{1 + y^n/x^n}$, where $\lambda = \sqrt[n]{1 + y^n/x^n}$.
Therefore $x = z/\sqrt[n]{1 + y^n/x^n}$, equation (3), or z/λ. Where $\lambda = \sqrt[n]{1 + y^n/x^n}$ or $\sqrt[n]{1 + \Delta}$
Now we know that x^n is a natural number since it is the difference between two odd natural z^n and y^n, but what about x?
We now have $x = z/\lambda$ and as λ is irrational, and Δ is getting smaller as z becomes greater and greater with respect to y and tending to zero.
We can verify the exactitude of the above equation.
The data. Let $n = 3, z = 5, y = 3$, and $z^3 - y^3 = 98 = x^3$.
We find $x = 4.610436292$ and $\lambda = \sqrt[3]{1 + 27/98} = \sqrt[3]{1.2755102104} = 1.084496061$.
Now $x = z/\lambda = 5/1.084496061 = 4.61046292$. Consequently, our equation holds.
We assume that our equation is exact for all natural numbers, z and y, odd and for all values of $n > 2$.
We also noticed that if z or y is the number we are looking for, and the other two terms are natural numbers, then, using the same method as explained above:
We find that $y = z/\sqrt[n]{1 + x^n/y^n}$, and $z = x/\sqrt[n]{1 - y^n/z^n}$. and z, or y, or x are irrational numbers.
One point remains, is x a natural number when $n = 2$.
Let $z = p^2 + q^2$, $y = p^2 - q^2$, and $x = 2pq$ from the Euclid equation.
We now substitute in equation (3), p and q for z, y, and x as indicated above.

$$x = \frac{z}{\sqrt[n]{1+y^n/x^n}} = \frac{z}{\sqrt[2]{1+y^2/x^2}} = \frac{(p^2+q^2)}{\sqrt[2]{1+(p^2-q^2)^2/(2pq)^2}}$$
$$= \frac{(p^2+q^2)}{\sqrt[2]{[(2pq)^2+(p^2-q^2)^2]/(2pq)^2}} = 2pq \text{ since } (2pq)^2+(p^2-q^2)^2 = (p^2+q^2)^2.$$

Thus, x is a natural number when we use p and q to find Pythagorean triples, otherwise x is an irrational number.

4 Discussion

The key point in giving a proof of FLT is in fact the relationship between the non-modular semi-stable elliptic curve or Frey curve and the equation $z^n = x^n + y^n$, where z, x, y, and n are nontrivial natural numbers. Indeed $z^n = x^n + y^n$ corresponds to the curve given by

$$y^2 = x(x-a^n)(x+b^n)$$

If all semi-stable elliptic curves are modular, then the Frey curve could not exist because it is non-modular, so FLT is proved if the Modularity Theorem is proved. This was accomplished by Wiles. Without the suggestion given by Hellegouarch, and the proof that the Frey curve could not be modular, by Jean-Pierre Serre, FLT would not have been proved. Consequently, a group of mathematicians made it possible to prove FLT along with many other theorems: the logic is as follows, if the Frey curve is related to FLT, and if it is not modular, whereas all semi-stable elliptic curves are modular, then Frey curves do not exist and FLT is proved, there are no integer solutions for x, y, and z..
As Gödel had proved: Every logically consistent system of arithmetic contains at least one proposition that cannot be proven or disproven within the system itself. This means that no formal system can be complete in the sense of containing all true statements (First Theorem). This seems to be the case of FLT. It was necessary to find the proof outside the domain of classical algebra, using modus tollens and with reference to many recent discoveries in number theory.

5 Conclusion

We believe we developed a way of proving the theorem with intuition, a heuristic, and a little serendipity.
If $z^3 - y^3 = (z-y)(z^2+zy+y^2)$, we have two factors, the first, A, is even, and the second B is odd. Consequently, to find a counterexample of FLT, A and B must be cubes, and their cube roots must be integers. All we had to do is set $z - y = 2^3$. Thus, we could divide out the even numbers, and we were left with the odd factor. We knew then that A divided equation (1); we had to show that B did not have an integer root, b. This could be applied to $n > 2$. Our proof was given by the equation:

$$b = z/\sqrt[n]{2^n + y^n/b^n}$$

Fermat's intuition began with the study of Pythagorean triples which we explored in different ways in our preparatory research and especially the problem raised by Diophantus, concerning the possibility of an even square being the sum of two odd squares, which probably lead to Fermat's proof for $n = 4$.
I was also interested by the way Wiles, with the discoveries of Hellegouarch (who found a relationship between elliptic curves and FLT), Serre, Frey, and Ribet who proved that such a relationship was exact, had found the missing link that would allow him to prove FLT.
We hope our attempt can be verified and show that for FLT, we remained inside the scope of 17^{th} century mathematics.
We also found a simple direct way of showing why x was not an integer, but an irrational number using our equation: $x = z/\sqrt[n]{1+y^n/x^n}$.

ACKNOWLEDGEMENTS

I would like to thank Pr. Matthieu Manant and Pr. Antoine Auberger for their help and advice in my research. And especially my thesis supervisor Jean-Marc Labat, Sorbonne professor in IT, and my alma mater, Ecole National Supérieur des Telecoms (Telecom Paris), and of course the University of Oxford where I still study (Calculus, Astrophysics, and Ancient Greek). Also, Dr. Myriam Wisdom for her encouragements and patience. And I must not forget my ex-aequo at the Agrégation, Pr. Florent Gusdorf, former professor at the Ecole Polytechnique and the director of Languages and International communication, for his long-term friendship and his encouragement.

REFERENCES

[1] Bassine, E., *Précis des Oeuvres Mathématiques et de l'Arithmétique de Diophante par Pierre Fermat*, Ed. Jacques Gabay, Paris 2005. pp. 167.

[2] Wiles, Andrew, Modular elliptic curves and Fermat's Last Theorem, *Annals of Mathematics*, 141 (1995), 443–551, http://www.scienzamedia.uniroma2.it/~eal/Wiles-Fermat.pdf

[3] Edwards H. M., Fermat's Last Theorem, a Genetic Introduction to Algebraic Number Theory, Springer-Verlag, 2000, New York, pp. 410

[4] Noguès, R., Théorème de Fermat, son histoire, Editions Jacques Gabay, Paris, 1992, pp. 172

[5] Hellegouarch, Yves, Points d'ordre $2p^h$ sur les courbes elliptiques, *Acta Arithmetica*, XXVI (1975).

[6] Frey, Gerhard, Links between stable elliptic curves and certain diophantine equations, https://cir.nii.ac.jp/crid/1572824499114802432

[7] Alvarez, A, Alberti M., La créativité en mathématiques, fonctionnement d'unesprit d'exception, RBA, Barcelone, 2019, pp. 159.

[8] Cornell, G., Silverman, J. H., Stevens, G., *Modular Forms and Fermat's Last Theorem*, Springer 1997.

[9] Courant, Richard and Robbins, Herbert, *What Is Mathematics? An Elementary Approach to Ideas and Methods*, Oxford: Oxford University Press, 1941.

[10] Dehaene, Stanislas, The Number Sense: How the Mind CreatesMathematics, Oxford: Oxford University Press, 1997, pp.151.

[11] Duvillié, B, Sur les traces de l'homo mathematicus, Ellipse poche,Paris 2000, pp. 453.

[12] Feferman, S. John W.Dawson, Jr., Stephen et ali. Gödel Kurt, Collected Works: Volume I, Publications 1929-1936, Edited by, Oxford University Press.

[13] Henderson Greek Mathematics 1, From Thales to Euclid, translated by Ivor Thomas, Harvard University Press, Cambridge, Mass., 1991, pp.511.

[14] Hofstader, D, Sander, E., Surfaces and Essence, analogy as the fuel and fire ofthinking, Basic Books, 2013, New York pp. 557.

[15] Kasner, Edward and Newman, James, *Mathematics and the Imagination*, New York, Simon and Schuster, 1940.

[16] Poincaré, H., « L'Invention mathématique » in *Mathematics in the Modern World*, Scientific American, 1974.

[17] Poincaré, H., *La science et l'Hypothèse*, Paris, Flammarion, 1902.

[18] Polya, G Comment résoudre un problème?, Paris Dunod, 1979.

[19] Stillwell, J., Numbers and Geometry, Springer, New York, 2000, pp. 339.

[20] Stillwell, J., Mathematics and its History, Springer, New York, 2010.

[21] Wiles, A. J., Taylor, R., Ring theoretic properties of certain Hecke algebras, Annals of Mathematics, 142 (1995), 553-572.

[22] Wiles, A. J., Modular elliptic-curves and Fermat's Last Theorem, Annals of Mathematics, 142 (1995), 443-551.