RESEARCH ARTICLE

On a Simpler, Much More General and Truly Marvellous Proof of Fermat's Last Theorem (I)

G. Gadzirayi Nyambuya

Correspondence:
physicist.ggn@gmail.com
Department of Applied Physics, National University of Science and Technology, Cnr Gwanda Rd and Cecil Ave, Bulawayo, Republic of Zimbabwe
Full list of author information is available at the end of the article

Abstract

English mathematics Professor, Sir Andrew John Wiles of the University *of* Cambridge finally and conclusively proved in 1995 Fermat's Last Theorem which had for 358 years notoriously resisted all gallant and spirited efforts to prove it even by three of the greatest mathematicians of all time – such as Euler, Laplace and Gauss. Sir Professor Andrew Wiles's proof employs very advanced mathematical tools and methods that were not at all available in the known World during Fermat's days. Given that Fermat claimed to have had the 'truly marvellous' proof, this fact that the proof only came after 358 years of repeated failures by many notable mathematicians and that the proof came from mathematical tools and methods which are far ahead of Fermat's time, this has led many to doubt that Fermat actually did possess the 'truly marvellous' proof which he claimed to have had. In this short reading, *via* elementary arithmetic methods, we demonstrate conclusively that Fermat's Last Theorem actually yields to our efforts to prove it. This proof is so elementary that anyone with a modicum of mathematical prowess in Fermat's days and in the intervening 358 years could have discovered this very proof. This brings us to the tentative conclusion that Fermat might very well have had the 'truly marvellous' proof which he claimed to have had and his 'truly marvellous' proof may very well have made use of elementary arithmetic methods.

Keywords: Fermat's Last Theorem; Fundamental Theorem of Arithmetic

1 Introduction

The pre-eminent French lawyer and amateur[1] mathematician, Advocate – Pierre *de* Fermat $(1607-1665)$ in 1637, famously in the margin of a copy of the famous book *Arithmetica* which was written by Diophantus of Alexandria $(\sim 201-215$ AD), Fermat 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.*"

In the parlance of mathematical symbolism, this can be written succinctly as:

$$\nexists\ (x,y,z,n)\in\mathbb{Z}^{+}:\ \ x^{n}+y^{n}=z^{n}\ \ \text{for}\ \ (n>2), \tag{1}$$

where the triple $[(x,y,z)\neq 0]$, is piecewise coprime, and $\mathbb{Z}^{+}$ is the set of all positive integer numbers. This theorem is classified among the most famous theorems in

[1] While Fermat is ranked as one of the greatest mathematicians of the World, he modestly considered himself an amateur in the field.

all History *of* Mathematics and prior to 1995, proving it was – and is; ranked in the *Guinness Book of World Records* as one of the "*most difficult mathematical problems*" known to humanity. Fermat's Last Theorem is now a true theorem since it has been proved, but prior to 1995 it was only a *conjecture*. Before it was proved in 1995, it is only for historic reasons that it was known by the title "*Fermat's Last Theorem*".

Rather 'notoriously', it stood as an unsolved riddle in mathematics for well over three and half centuries. Many amateur and great mathematicians tried but failed to prove the conjecture in the intervening years $1637 - 1995$; including three of the World's greatest mathematicians such as Italy's Leonhard Euler $(1707 - 1783)$, France's Pierre-Simon, marquis *de* Laplace $(1749 - 1827)$, and the celebrated mathematical prodigy, genius and Crown Prince *of* Mathematics, Germany's Johann Carl Friedrich Gauss $(1777 - 1855)$, amongst many other notable and historic figures of mathematics.

Without any doubt, the conjecture or Fermat's Last Theorem is in-itself – as it stands as a bare statement, deceptively simple mathematical statement which any agile 10 year old mathematical prodigy can fathom with relative ease. As already said, Fermat famously – *via* his bare marginal note; stated he had solved the riddle around 1637. His claim was discovered some 30 years later after his death in 1665, as an overly simple statement in the margin of the famous copy *Arithmetica*. As is well known from the history of mathematics, Fermat wrote many notes in the margins and most of these notes were 'theorems' he claimed to have solved himself. Some of the proofs of his assertions were found. For those that were not found, all the proofs save for one resisted all intellectually spirited efforts to prove it and this was the marginal note pertaining the so-called Fermat's Last Theorem.

This marginal note dubbed Fermat's Last Theorem, was the last of the assertions made by Fermat whose proof was needed, and for this reason that it was the last of Fermat's statement that stood unproven, it naturally found itself under the title 'Fermat's Last Theorem'. Because all of the many of Fermat's assertions were eventually proved, most people believed that this last assertion must – too; be correct as Fermat had claimed. Few – if any; doubted the assertion may be false, hence the confidence to call it a theorem. Simple, the proof Fermat claimed to have had, had to be found! Alas, reality could prove otherwise, that, the proof was not a mere summer walk in the park.

So the question is: *Did Fermat actually posses the so-called 'truly marvellous' proof which he claimed to have had?* This is the question many have justly and rightly asked over the years and this reading makes the temerarious endeavour to vindicate Fermat, that he very well might have had the '*truly marvellous*' proof he claimed to have had and this we accomplish by providing a proof that employs elementary arithmetic methods that were available in Fermat's day.

Surely, there are just reasons to doubt Fermat actually had the proof and this is so given the great many notable mathematicians that tried and monumentally failed and as-well, given the number of years it took to find the first correct proof. The first correct proof was supplied only 358 years later by the English Professor of mathematics at the University *of* Cambridge – Sir Professor Andrew John Wiles, in 1995 [23].

To add salt to injury *i.e.* add onto the doubts on whether or not Fermat actually had his so-called '*truly marvellous*' proof is that Sir Professor Andrew Wiles's proof[2] employs highly advanced mathematical tools and methods that were not at all available in the known World during Fermat's days. Actually, these tools and methods were invented (discovered) in the relentless effort to solve this very problem. Herein, we supply a very simple proof of Fermat's Last Theorem.

That said, we must hasten to say that, as a difficult mathematical problem that so far yielded only to the difficult, esoteric and advanced mathematical tools and methods of Sir Professor Andrew Wiles – Fermat's Last Theorem, as any other difficult mathematical problem in the History *of* Mathematics, it has had a record number of incorrect proofs of which the present may very well be an addition to this long list of incorrect proofs. In the words of historian of mathematics – Howard Eves [10]:

> *"Fermat's Last Theorem has the peculiar distinction of being the mathematical problem for which the greatest number of incorrect proofs have been published."*

With that in mind, allow us to say, we are confident the proof we supply herein is water-tight and most certainly correct and that, it will stand the test of time and experience.

As stated in the *ante-penultimate* above, is that, in this rather short reading, we make the temerarious endeavour to answer this question – of whether or not Fermat actually possessed the proof he claimed to have had. This we accomplish by supplying a simple and elementary proof that does not require any advanced mathematics but mathematics that was available in the days of Fermat. Sir Professor Andrew Wiles's acclaimed proof, is at best very difficult and to the chagrin of they that seek a simpler understanding – the proof is nothing but highly esoteric. The question thus 'forever' hangs in there to the searching and inquisitive mind: "*Did Fermat really possess the proof he claimed to have had?*" The proof that we supply herein leads us to strongly believe that Fermat might have had the proof and this proof most certainly employed elementary methods of arithmetics!

2 Proofs for Specific Indices

Before we go into the main business of the day, we shall give a short history of some notable efforts in finding a proof to Fermat's Last Theorem. As is well known, the case for $(n = 3)$, for all non-zero (x, y, z) and $(x, y, z) \in \mathbb{Z}^+$, the equation $x^3 + y^3 = z^3$ admits no solutions. This was first proved by the great Italian mathematician Leonhard Euler in 1770 [17], that is, 133 years after Fermat set into motion Fermat's Last Theorem. Euler used the technique of *infinite descent*. Euler's proof is not the only proof possible as other authors have published their independent proofs [*cf.* 3, 4, 9, 15, 16, amongst many others].

Fermat was the first to provide a proof for the case $(n = 4)$ which stated that for all non-zero piecewise coprime triple $(x, y, z) \in \mathbb{Z}^+$, the equation $x^4 + y^4 = z^4$

[2] The proof by Sir Professor Wiles is well over 100 pages long and consumed about seven years of his research time. For this notable achievement of solving Fermat's Last Theorem, he was Knighted *Commander of the Order of the British Empire* in 2000 by Her Majesty Queen Elizabeth (II), and received many other honours around the World.

admits no solutions. This proof by Fermat is the only surviving proof of Fermat's Last Theorem and as is the case with Euler's proof for the case $(n = 3)$, Fermat's proof makes use of the technique of infinite descent. One wonders whether or not Fermat conducted this proof as part of a more general proof for all $(n > 2)$. As is the case with Euler's proof for $(n = 3)$, Fermat's proof is not the only proof possible as other authors have published their independent proofs [see *e.g.* Refs. 4, 8, 11, 14, 15, amongst many others]. Even after Sir Professor Andrew Wiles's 1995 breakthrough [23], researchers are still publishing variants of the proof for the case $(n = 4)$ [*cf.* 1, 2, 7].

The case $(n = 5)$ was first proved independently by the French mathematician Adrien-Marie Legendre $(1752-1833)$ and the German mathematician Johann Peter Gustav Lejeune Dirichlet $(1805-1859)$ around 1825 and alternative and independent proofs were developed in the later years by others [*cf.* 4–6, 12, 13, 19–22, amongst many others].

3 Lemma (I)

If $[(a > 1); (a_j \leq a); (b > 1); (c > 1); (n > 2)] \in \mathbb{Z}^+$ where $(b > c)$ and a_j is one of the prime factors of a, then, the following will hold true always:

$$a^n = a_j(b \pm c). \tag{2}$$

The above statement is clearly evident and needs no proof. However, below we demonstrate that this statement is true. This demonstration does not constitute a proof.

What this statement really means is that the number a^n [for any $(n > 2)$ and $(a > 1)$], can always be written as a sum or difference of two numbers p and q where $[(p, q) \in \mathbb{Z}^+]$ are not co-prime, *i.e.*:

$$a^n = p \pm q : \gcd(p, q) \neq 1, \tag{3}$$

since one can always find some (p, q) such that a will always be a common factor of (p, q), that is to say:

$$a^n = a(g \pm h), \tag{4}$$

in which case we will have $p = ag$ and $q = ah$ where $(g \pm h) = a^{n-1} \geq 4$ such that $(g, h) \in \mathbb{Z}^+$ and $(g > h)$. To see this, we know that if $\{a_1, a_2, a_3 \ldots a_j \ \ldots a_m\}$ is the set of all the prime factors of a, then $(a = a_j e)$ where $(e \leq a)$. Substituting all this into (4), we will have:

$$a^n = a_j(eg \pm eh). \tag{5}$$

Setting $(b = eg)$ and $(c = eh)$, (5) leads us to (2). As we did with *Beal's Conjecture* in [18], equipped with this simple fact, we will demonstrate that as we did with that *Fermat's Last Theorem* yields to a proof in the simplest imaginable manner.

Proof.

If $[(a > 1) \in \mathbb{Z}^+]$, then, according to the fundamental theorem of arithmetic, we can decompose the number a into its prime factors *i.e.*:

$$a = a_1^{\alpha_1} \cdot a_2^{\alpha_2} \cdot a_3^{\alpha_3} \cdots a_j^{\alpha_j} \cdots a_n^{\alpha_n}, \tag{6}$$

where $[\alpha_j \in \mathbb{Z}^+ \cup \{0\}]$ and the a_k's are the prime factors of a and these are such that $(1 < a_j \leq a : k = 1, 2, 3 \dots)$. We will have $(a_j = a)$ *if and only if* a is prime.

Now, $(a^n = a \cdot a^{n-1})$ and since $(a > 1)$ and $(n > 2)$, it is clear that $(a^{n-1} \geq 4)$. Clearly, if $(a^{n-1} \geq 4)$, we can write $(a^{n-1} = b \pm c \geq 4)$ where $[(b, c) > 1]$. From the foregoing, it follows from $(a^n = a \cdot a^{n-1})$ and $(a^{n-1} = b \pm c \geq 4)$, that $[a^n = a(b \pm c)]$. From (6), it follows that:

$$\begin{aligned} a^n &= a_1^{\alpha_1} \cdot a_2^{\alpha_2} \cdot a_3^{\alpha_3} \cdots a_j^{\alpha_j} \cdots a_n^{\alpha_n}(b \pm c), \\ &= a_j \left[a_1^{\alpha_1} \cdot a_2^{\alpha_2} \cdot a_3^{\alpha_3} \cdots a_j^{\alpha_j - 1} \cdots a_n^{\alpha_n} b \pm a_1^{\alpha_1} \cdot a_2^{\alpha_2} \cdot a_3^{\alpha_3} \cdots a_j^{\alpha_j - 1} \cdots a_n^{\alpha_n} c) \right], \\ &= a_j(g \pm h). \end{aligned} \tag{7}$$

where $(g = a_1^{\alpha_1} \cdot a_2^{\alpha_2} \cdot a_3^{\alpha_3} \cdots a_j^{\alpha_j - 1} \cdots a_n^{\alpha_n} b)$ and $(h = a_1^{\alpha_1} \cdot a_2^{\alpha_2} \cdot a_3^{\alpha_3} \cdots a_j^{\alpha_j - 1} \cdots a_n^{\alpha_n} c)$ where $(\alpha_j > 1)$. Hence result is proven. Now we proceed to the main task of the present reading.

4 Proof of Fermat's Last Theorem (I)

Now, the proof that we are going to provide of FTL is a proof by contradiction and this proof makes use of *Lemma* §(3) whereby we demonstrate that the triple (x, y, z) is such that it will always have a common factor if the equation, $(x^n + y^n = z^n)$ for all $(n > 2)$; is to hold true. We begin by assuming the statement:

$$x^n + y^n = z^n \ \dots\dots \ [\forall n > 2], \tag{8}$$

to be true for some piecewise co-prime triple $[(x, y, z) > 1] \in \mathbb{Z}^+$, the meaning of which is that the greatest common divisor of this triple or any pair of the triple is unity *i.e.*, $\gcd(x, y) = \gcd(x, z) = \gcd(y, z) = \gcd(x, y, z) = 1$.

1 We must realise that if just one of the members of the triple (x, y, z) is equal to unity for any $(n > 2)$, then, the other two members of this triple can not be integers, hence, from this it follows that if a solution exists, then, all the members of this triple will be greater than unity *i.e.* $[(x > 1; y > 1; z > 1) \in \mathbb{Z}^+]$.

2 By way of contradiction, we assert that there exists a set of positive integers $[(x, y, z) > 1]$ that satisfy the simple relation $(x^n + y^n = z^n)$ for some piecewise co-prime triple $[(x, y, z) > 1]$. Having made this assumption, if we can show that $[\gcd(x, y, z) > 1]$, then, by way of contradiction FTL holds true.

3 If the statement (8) holds true, then – clearly; there must exist some $[(p, q) \in \mathbb{Z}^+]$ such that $[\gcd(p, q) = 1]$, such that x^n, y^n and z^n can be decomposed as follows:

$$\begin{pmatrix} x^n \\ y^n \\ z^n \end{pmatrix} = \begin{pmatrix} p - q \\ 2q \\ p + q \end{pmatrix}. \tag{9}$$

4 According to the *Lemma* §(3), the equation $z^n = p + q$; for any $(z > 1)$ and for any $(n > 2)$, this equation, can always be written such that $p = az_j$ and $p = bz_j$ for some $(a > 1; b > 1) \in \mathbb{Z}^+$ and $z_j : (1 < z_j \leq z)$ is any of the prime factors of z. Putting everything together, we will have $z^n = (a + b)z_j$. Substituting $p = az_j$ and $q = bz_j$ into (9), we will have:

$$\begin{pmatrix} x^n \\ y^n \\ z^n \end{pmatrix} = \begin{pmatrix} (a - b)z_j \\ 2bz_j \\ (a + b)z_j \end{pmatrix}. \tag{10}$$

5 From (10), it is clear that $\gcd(x^n, y^n, z^n) \neq 1$ since there exists a common divisor [cd()] of the triple (x^n, y^n, z^n) which is $(z_j > 1)$, that is to say, $(z_j > 1)$ is a common divisor of the triple (x^n, y^n, z^n). If $\gcd(x^n, y^n, z^n) \neq 1$, consequently, $\gcd(x, y, z) \neq 1$ and this is in *complete violation of the critical, crucial and sacrosanct assumption that* $\gcd(x, y, z) = 1$. ***Q.E.D.***

Alternatively, according to the *Lemma* §(3), the equation $x^n = p - q$ for any $(n > 2)$ and for any $(x_j > 1)$, this equation, can always be written such that $p = ax_j$ and $q = bx_j$ for some $(a > 1; b > 1) \in \mathbb{Z}^+$ and $x_j : (1 < x_j \leq x)$ is any of the prime factors of x; putting everything together, we will have $x^n = (a - b)x_j$. Now, substituting $p = ax_j$ and $q = bx_j$ into (9), we will have:

$$\begin{pmatrix} x^n \\ y^n \\ z^n \end{pmatrix} = \begin{pmatrix} (a - b)x_j \\ 2bx_j \\ (a + b)x_j \end{pmatrix}. \tag{11}$$

Again, from (11), it is clear that $[\gcd(x, y, z) \neq 1]$ since the $\mathrm{cd}(x^n, y^n, z^n) = x_j$, that is to say, x_j is a common divisor of triple (x^n, y^n, z^n). From the foregoing, it follows that the prime factors of (x, z) are common divisors of the triple (x^n, y^n, z^n), the meaning of which is that $[\gcd(x, y, z) \neq 1]$.

Therefore, by way of contradiction, Fermat's Last Theorem is true since we arrive at a contradictory result that $[\gcd(x, y, z) \neq 1]$. What this effectively means is that the equation $(x^n + y^n = z^n)$ for $(n > 2)$ has a solution and this solution is such that the triple (x, y, z) always has a common factor as is the case with all those values of x, y, z that satisfy *Fermat's Last Theorem*.

5 General Discussion

If the proof we have provided herein stands the test of time and experience, then, it is without a doubt that Fermat's claim to have had a 'truly marvellous' proof may very well resonate with truth. The proof provided herein is not only simple, but surprisingly simple, so simple that one wonders how great mathematicians would have missed this. All this simplicity is embodied in *Lemma* (3). As we anxiously await the *World* to judge our proof, effort and work, we must — if this be permitted at this point of closing, say that, we are confident that – simple as it is or may appear, this proof is flawless, it will stand the test of time and experience. It strongly appears that the great physicist and philosopher – Albeit Einstein $(1879-1955)$, was probably right in saying that "*Subtle is the Lord. Malicious He is not.*" because in *Lemma* §(3), there exists deeply embedded therein, a subtlety that resolves and does away with the malice and notoriety associated with *Fermat's Last Theorem* in a simpler and truly marvellous and general manner.

6 Conclusion

Given that the method used here to prove Fermat's Last Theorem are so elementary, it is very much possible that Fermat actually processed the correct proof.

References

1. Barbara, R. [2007], 'Fermat's Last Theorem in the Case $n = 4$', *Mathematical Gazette* **91**, 260–262.
2. Dolan, S. [2011], 'Fermat's Method of Descente Infinie', *Mathematical Gazette* **95**, 269–271.
3. Duarte, F. J. [1944], 'Sobre la Ecuaci on $x^3 + y^3 + z^3 = 0$', *Ciencias Fis. Mat. Naturales* (Caracas) **8**, 971–979.
4. Gambioli, D. [1901], 'Memoria Bibliographica Sull'ultimo Teorema di Fermat', *Period. Mat.* **16**, 145–192.
5. Gambioli, D. [1903/4], 'Intorno all'ultimo teorema di Fermat', *Pitagora* **II**(10), 11–13, 41–42.
6. Gauss, J. C. F. [1875], *Neue Theorie der Zerlegung der Cuben*, Vol. II, 2^{nd} edn, (Zur Theorie der complexen Zahlen, Werke) Königl. Ges. Wiss. Göttingen. (Published posthumous).
7. Grant, M. and Perella, M. [1999], 'Descending to the Irrational', *Mathematical Gazette* **83**, 263–267.
8. Hilbert, D. [1897], *Die Theorie der Algebraischen Zahlkörper*, Vol. 4, Jahresbericht der Deutschen Mathematiker-Vereinigung. Reprinted in 1965 in Gesammelte Abhandlungen, Vol. I by New York: Chelsea.
9. Kausler, C. F. [1802], 'Nova Demonstratio Theorematis nec Summam, nec Differentiam Duorum Cuborum Cubum esse Posse', *Novi Acta Acad. Petrop* **13**, 245–253.
10. Koshy, T. [2001], *Elementary Number Theory With Applications*, New York: Academic Press (ISBN 978-0124211711), UK. p. 544.
11. Kronecker, L. [1901], 'Vorlesungen Über Zahlentheorie', *Leipzig: Teubner* **I**, 33–38. Reprinted by New York: Springer-Verlag in 1978.
12. Lamé, G. [1847], 'Mémoire sur la Résolution en Nombres Complexes de Léquation $A^5 + B^5 + C^5 = 0$', *J. Math. Pures Appl.* **12**(137-171).
13. Lebesgue, V. A. [1843], 'Thèorémes nouveaux sur l'équation indéterminée $x^5 + y^5 = az^5$', *J. Math. Pures Appl.* **8**, 49–70.
14. Lebesgue, V. A. [1853], 'Rèsolution des Équations biquadratiques $z^2 = x^4 \pm 2^m y^4, z^2 = 2^m x^4 y^4, 2^m z^2 = x^4 \pm y^4$', *J. Math. Pures Appl.* **18**, 73–86. Lebesgue, V. A. (1859). Exercices d'Analyse Numrique. Paris: Leiber et Faraguet. pp. 83-84, 89. Lebesgue, V. A. (1862). Introduction à la Théorie des Nombres. Paris: Mallet-Bachelier. pp. 71-73.
15. Legendre, A. M. [1823], 'Recherches sur Quelques Objets D'analyse Indéterminée, et Particulièrement sur le Théorème de Fermat', *Mém. Acad. Roy. Sci. Institut France* **6**, 1–60.
16. Legendre, A. M. [1930], *Théorie des Nombres*, Vol. II, 3rd edn, Paris: Firmin Didot Frères. Reprinted in 1955 by A. Blanchard (Paris).
17. Leonhard, E. [1770], 'Vollständige Anleitung zur Algebra', *Royal Academy of Sciences* (St. Petersburg) .
18. Nyambuya, G. G. [2014], 'A Simple and General Proof of Beal's Conjecture (I)', *Advances in Pure Mathematics* **4**(9), 1–4.
19. Rychlik, K. [1910], 'On Fermat's Last Theorem for $n = 5$ (in Bohemian)', *Časopis Pěst. Mat.* **39**, 185–195, 305–317.
20. Terjanian, G. [1987], 'Sur une Question de V. A. Lebesgue', *Ann. Inst. Fourier* **37**(3), 19–37. doi:10.5802/aif.1096.
21. van der Corput, J. G. [1915], 'Quelques Formes Quadratiques et Quelques Équations Indéterminées', *Nieuw Archief Wisk.* pp. 45–45.
22. Werebrusow, A. S. [1905], 'On the equation $x^5 + y^5 = Az^5$ (in Russian)', *Moskov. Math. Samml.* **25**, 466–473.
23. Wiles, A. [1995], 'Modular Elliptic Curves and Fermat's Last Theorem', *Annals of Mathematics* **141**(3), 443–551. doi:10.2307/2118559.