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

Golden Gadzirayi Nyambuya
Department of Applied Physics, National University of Science and Technology, Bulawayo, Republic *of* Zimbabwe
Email: physicist.ggn@gmail.com

Received ****; revised ****; accepted* ****

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, Proof.

"*Subtle is the Lord.*
Malicious He is not."

Albert Einstein $(1879 - 1955)$.

1. Introduction

The pre-eminent French lawyer and amateur 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 $(\sim 201 - 215 \text{ AD})$, 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:

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

where the triple $(x, y, z) \neq 0$, is piecewise coprime, and $\mathbb{N}^+$ is the set of all positive integer numbers. This theorem is classified among the most famous theorems in 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 genius and Crown Prince *of* Mathematics, Germany's Johann Carl Friedrich Gauss $(1777 - 1855)$, amongst many other notable and historic figures of mathematics.

* This paper is accepted to the *American Journal of Mathematics and Mathematical Sciences* (India)
* G. G. Nyambuya

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. 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*. 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!

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 aswell, 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 Andrew John Wiles $(1953-)$, in 1995 [1].

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* 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 [2]:

> *"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. Lemma

If $(a > 1, b > 1; c > 1; n > 2) \in \mathbb{N}^+$ where $(b > c)$, then, the following will hold true always:

$$a^n = a(b + c) \quad \text{or} \quad a^n = a(b - c). \tag{2}$$

The above statement is clearly evident and needs no 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 $p \in \mathbb{N}^+$ and $q \in \mathbb{N}^+$ are not co-prime, *i.e.*:

$$a^n = p + q \ \text{ or } \ a^n = p - q : \gcd(p, q) \neq 1, \tag{3}$$

since one can always find some (p, q) such that a will always be a common factor of (p, q). Equipped with this simple fact, we will demonstrate that Fermat's Last Theorem yields to a proof in the simplest imaginable manner.

* 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.

3. Proof

The proof that we are going to provide is a proof by contradiction and this proof makes use of Lemma §(2.) 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 $(n > 2)$; is to hold true. We begin by assuming that the statement:

$$\exists\ (x, y, z, n) \in \mathbb{N}^+ :\ \ x^n + y^n = z^n,\ \ \text{for}\ \ (n > 2), \quad (4)$$

to be true where the triple (x, y, z) is assumed to be piecewise *coprime*, the meaning of which is that the greatest common divisor of this triple or any arbitrary pair of the triple is unity (*i.e.*, $\gcd(x, y, z) = 1$).

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

Now, for our proof, by way of contradiction, we assert that there exists a set of positive integers (x, y, z, n) that satisfies the simple relation $x^n + y^n = z^n$ for all $(n > 2)$. Having made this assumption, if we can show that $\gcd(x, y, z) > 1$, then, by way of contradiction *Fermat's Last Theorem* holds true.

If the statement (4) holds true, then – clearly; there must exist some $(p, q) \in \mathbb{N}^+$ such that $\gcd(p, q) = 1$, such that:

$$\begin{pmatrix} x^n \\ y^n \\ z^n \end{pmatrix} = \begin{pmatrix} p - q \\ 2q \\ p + q \end{pmatrix}. \quad (5)$$

Now, according to the Lemma §(2.), the equation $z^n = p + q$ for any $(n > 2)$ and for any $(z > 1)$, this equation, can always be written such that $p = az$ and $p = bz$ for some $(a > 1; b > 1) \in \mathbb{N}^+$ *i.e.* $z^n = z(a + b)$. Substituting $p = az$ and $p = bz$ into (5), we will have:

$$\begin{pmatrix} x^n \\ y^n \\ z^n \end{pmatrix} = \begin{pmatrix} z(a - b) \\ 2bz \\ z(a + b) \end{pmatrix}. \quad (6)$$

From (6), it is clear that $\gcd(x^n, y^n, z^n) \neq 1$ since $\mathrm{cd}(x^n, y^n, z^n) = z$, that is to say, z is a common divisor of the triple (x^n, y^n, z^n).

Alternatively, according to the Lemma §(2.), the equation $z^n = p + q$ for any $(n > 2)$ and for any $(x > 1)$, this equation, can always be written such that $p = ax$ and $p = bx$ for some $(a > 1; b > 1) \in \mathbb{N}^+$ *i.e.* $x^n = x(a + b)$. Now, substituting $p = ax$ and $p = bx$ into (5), we will have:

$$\begin{pmatrix} x^n \\ y^n \\ z^n \end{pmatrix} = \begin{pmatrix} x(a - b) \\ 2bx \\ x(a + b) \end{pmatrix}. \quad (7)$$

Again, from (7), it is clear that $\gcd(x^n, y^n, z^n) \neq 1$ since $\mathrm{cd}(x^n, y^n, z^n) = x$, that is to say, x is a common divisor [cd()] of triple (x^n, y^n, z^n). From the foregoing, it follows that (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 $n > 2$ may have a solution and this solution is such that the triple (x, y, z) always has a common factor.

4. Discussion and Conclusion

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. If this proof employed the use of Pythagoras theorem as in the present case, then, for any book, the standard '*margin is [certainly] too narrow*' to contain the present proof, the meaning of which is that Fermat was most certainly right in his famous claim.

Clearly, the problem with the proof is not that it is difficult and only accessible to the highly esoteric, no! We ourselves (*i.e.*, amateur and seasoned mathematicians alike) have made this problem appear very difficult, highly esoteric and only accessible to the foremost and advanced mathematical minds. Without the historic and personal encodes that will soon follow, this proof (*i.e.*, the morass substance of the present reading) can be typed using a standard font size of between $10-12$, *back-to-back* on a single standard *a4-page*. Few – if any; would believe that this is possible. The level difficulty and esoteric nature associated with this problem has been – until the present reading, placed very high and beyond the intellectual reach of mortals of modest means.

What could have happened leading to the elevation of this problem to a point where it came to become one of the most difficult problems in all History *of* Mathematics is that – perhaps; the plethora of maiden failures to provide a proof must have led people to think that this problem must be very difficult. Failure after failure and especially so by great mathematicians must then have led to it [Fermat's Last Theorem] achieving 'international, worldwide and historic notoriety' as a very difficult problem that eluded even great minds like Euler, Laplace and Gauss. With this kind of background, certainly, when people approached this problem, they most probably did so with in mind that it was a very difficult problem probably to be solved by 'real super geniuses' and not mortals of modest means *e.g.* ourself.

If someone told you that a given problem is so difficult, so much that it has thus far eluded the finest, advanced and most esoteric minds that have attempted to find its solution, one naturally tries to use higher advanced methods to prove it. Further, if someone told you that a given problem is so difficult, so much that it have eluded the finest, advanced and most esoteric minds that have attempted to

find its solution, one naturally is discouraged from using simple elementary methods to prove it because the feeling one has is that, if it can be solved *via* a simple method, surely, advanced minds before me must have discovered this, thus leading one to try and climb higher than those before them. If what we have presented stands the test of time and experience, then, the way we approach difficult problems may need recourse, especially the way the public media projects and posts the level difficulty and the supposed esoteric effort required in-order to solve these problems.

Our approach to solving so-called outstanding problems is that one must not be let down by the *public media projections* of the level difficult and the supposed esoteric effort required in-order to solve the problem. First, as we climb the ladder of level difficultly, we tackle it [problem] from a level simplicity accessible to the 'layman' and step-by-step as we move up the ladder. To us, we have come to realise that this has helped us in understanding the problem at a much deeper level. At each level, we make sure we exhaust 'all' the possible avenues. As to how one knows they have exhausted all the possible avenues, this is a difficult question to answer but the most potent and virile tool for us has been a deep and strong inner intuition, unshakable confidence in the solubility of the problem and singular conviction that victory is certain if one persists.

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* §(2.), 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.

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] Andrew Wiles. Modular elliptic curves and fermat's last theorem. *Annals of Mathematics*, 141(3):443–551, 1995. doi:10.2307/2118559.

[2] T. Koshy. *Elementary Number Theory With Applications*. New York: Academic Press (ISBN 978-0124211711), UK, 2001. p. 544.

[3] Euler Leonhard. Vollständige anleitung zur algebra. *Royal Academy of Sciences* (St. Petersburg), 1770.

[4] C. F. Kausler. Nova demonstratio theorematis nec summam, nec differentiam duorum cuborum cubum esse posse. *Novi Acta Acad. Petrop*, 13:245–253, 1802.

[5] D. Gambioli. Memoria bibliographica sull'ultimo teorema di fermat. *Period. Mat.*, 16:145–192, 1928.

[6] A. M. Legendre. Recherches sur quelques objets d'analyse indéterminée, et particulièrement sur le théorème de fermat. *Mém. Acad. Roy. Sci. Institut France*, 6:1–60, 1823.

[7] A. M. Legendre. *Théorie des Nombres*, volume II. Paris: Firmin Didot Frères, 3rd edition, 1930. Reprinted in 1955 by A. Blanchard (Paris).

[8] F. J. Duarte. Sobre la ecuaci on $x^3+y^3+z^3=0$. *Ciencias Fis. Mat. Naturales* (Caracas), 8:971–979, 1944.

[9] D. Hilbert. Die theorie der algebraischen zahlkörper. 4:175–546, 1897. Reprinted in 1965 in Gesammelte Abhandlungen, Vol. I by New York: Chelsea.

[10] V. A. Lebesgue. 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, 1853. Lebesgue, V. A. (1859). Exercices d'Analyse NumÃl'rique. Paris: Leiber et Faraguet. pp. 83-84, 89. Lebesgue, V. A. (1862). Introduction à la Théorie des Nombres. Paris: Mallet-Bachelier. pp. 71-73.

[11] L. Kronecker. Vorlesungen über zahlentheorie. I:33–38, 1901. Reprinted by New York: Springer-Verlag in 1978.

[12] M. Grant and M. Perella. Descending to the irrational. *Mathematical Gazette*, 83:263–267, July 1999.

[13] S. Dolan. Fermat's method of descente infinie. *Mathematical Gazette*, 95:269–271, July 2011.

[14] R. Barbara. Fermat's last theorem in the case $n=4$. *Mathematical Gazette*, 91:260–262, July 2007.

[15] J. C. F. Gauss. *Neue Theorie der Zerlegung der Cuben*, volume II. (Zur Theorie der complexen Zahlen, Werke) Königl. Ges. Wiss. Göttingen, 2^{nd} edition, 1875. (Published posthumous).

[16] V. A. Lebesgue. Thèorémes nouveaux sur l'équation indéterminée $x^5+y^5=az^5$. *J. Math. Pures Appl.*, 8:49–70, 1843.

[17] G. Lamé. Mémoire sur la résolution en nombres complexes de léquation $a^5+b^5+c^5=0$. *J. Math. Pures Appl.*, 12(137-171), 1847.

[18] D. Gambioli. Intorno all'ultimo teorema di fermat. *Pitagora*, II(10):11–13, 41–42., 1903/4.

[19] A. S. Werebrusow. On the equation $x^5+y^5=az^5$ (in russian). *Moskov. Math. Samml.*, 25:466–473, 1905.

[20] K. Rychlik. On fermat's last theorem for $n=5$ (in bohemian). *Časopis Pěst. Mat.*, 39:185–195, 305–317, 1910.

[21] J. G. van der Corput. Quelques formes quadratiques et quelques Ãl'Équations indéterminées. *Nieuw Archief Wisk.*, pages 45–45, 1915.

[22] G. Terjanian. Sur une question de v. a. lebesgue. *Ann. Inst. Fourier*, 37(3):19–37, 1987. doi:10.5802/aif.1096.