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

G. G. Nyambuya

Department of Applied Physics, National University of Science and Technology, Bulawayo, Republic of Zimbabwe

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 efforts to prove it. 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 which make use of Pythagoras theorem, we demonstrate conclusively that *Fermat's Last Theorem* actually yields to our efforts to prove it.

> "*Arithmetic is where the answer is right and everything is nice and you can look out of the window and see the blue sky, or the answer is wrong and you have to start over and try again and see how it comes out this time.*"
>
> **Carl August Sandburg (1878 – 1967)**

1. Introduction

The pre-eminent French lawyer and amateur mathematician, the late Advocate – Pierre *de* Fermat (1607 – 1665) in 1637, famously in the margin of a

Email address: golden.nyambuya@nust.ac.zw (G. G. Nyambuya)

copy of the famous book *Arithmetica* which was written by Diophantus of Alexandria ($\sim 201 - 215$ AD), 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:

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

where the triple $(x, y, z) \neq 0$, is piecewise coprime, and $\mathbb{N}^{+}$ 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.

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 (see *e.g.* Cox, 1994) 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 Andrew John Wiles (1953−), in 1995 Wiles (1995).

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[1] 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*,

[1] 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.

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 Koshy (2001):

> *"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. Pythagorean Triples

The great Euclid (b.300 BC) of Alexandria – Egypt; provided a fundamental formula for generating primitive Pythagorean triples given an arbitrary pair of positive integers p and q with $(p > q)$ such that $(p-q)$ is odd. The formula states that the integers X, Y and Z:

$$\begin{array}{lcl} X & = & p^2 - q^2 \\ Y & = & 2pq \\ Z & = & p^2 + q^2 \end{array} , \tag{2}$$

constituent a primitive Pythagorean triple. A primitive Pythagorean triple is one in which X, Y and Z are piecewise co-prime. By piecewise co-prime, we mean that any combination of the triple X, Y and Z has no common factor other than unity. Below is the proof that the numbers X, Y and Z do yield Pythagoras's formula:

$$\begin{array}{ccccc} (p^2+q^2)^2 & \equiv & (p^2-q^2)^2 & + & (2pq)^2 \\ \Downarrow & & \Downarrow & & \Downarrow \\ Z^2 & = & X^2 & + & Y^2 \end{array} . \tag{3}$$

Clearly, there are infinitely many primitive Pythagorean triples. Invariably – this means that, there must exist infinitely many piecewise co-prime triples $(X, Y, Z) \in \mathbb{N}^+$ where $\mathbb{N}^+$ is the set of all positive integers. An important fact to note, a fact directly emergent from the foregoing is that ***all*** primitive Pythagorean triples yield to Euclid's formula and further, Euclid's set of primitive Pythagorean triples comprises ***all*** the primitive Pythagorean triples that exist in *Nature*.

3. Lemma

If $[(a, b) \in \mathbb{N}^+]$ such that:

$$a\sqrt{b} = c + d, \tag{4}$$

for some numbers (c, d), then, insofar as whether or not $\sqrt{b}$ is an integer or not, there are two conditions, and these are:

1. $(\sqrt{b} \in \mathbb{N}^+)$.

2. $(\sqrt{b} \notin \mathbb{N}^+)$. That is, $(\sqrt{b} \in \mathbb{I}^+)$ is an irrational number: $\mathbb{I}^+$ is the set of all positive irrational numbers.

—

1. If, $(\sqrt{b} \in \mathbb{N}^+)$, then, one can always find some (c, d) such that $[(c, d) \in \mathbb{N}^+]$.

2. If, $(\sqrt{b} \notin \mathbb{N}^+)$, then $\sqrt{b}$ is a surd – it is an irrational number and $[(c, d) \notin \mathbb{N}^+]$; and there must exist some $[[(c_1 < c)$ *&* $(d_1 < d)] \in \mathbb{N}^+]$ such that $(c = c_1\sqrt{b})$ and $(d = d_1\sqrt{b})$ so that $(a\sqrt{b} = c_1\sqrt{b} + d_1\sqrt{b})$, which implies that:

$$a = (c_1 + d_1) \in \mathbb{N}^+. \tag{5}$$

While (c_1, d_1) are not necessarily integers, one can always find some (c_1, d_1) such that $[(c_1, d_1) \in \mathbb{N}^+]$ for as long as $[(a > 1) \in \mathbb{N}^+]$. The above stated *Lemma* §(3) is a self evident truth which is not only necessary but vital and pivotal for the proof that we now give below. Before that – using this *Lemma* §(3), we shall set-up a *Theorem* that is necessary for this proof.

4. Theorem

For any piecewise coprime triple of integers (x, y, z) each greater than unity such that z is not a perfect square *i.e.* $(\sqrt{z} \in \mathbb{I}^+)$, the equation:

$$z^{2^\ell n} = x^2 + y^2, \tag{6}$$

admits no solutions for $[(n > 2) \in \mathbb{O}^+]$ for any $[(\ell \geq 0) \in \mathbb{N}^+]$.

4.1. Proof

We will prove for two cases, the first of which is for $(\ell = 0)$ and the second which is for $(\ell > 0)$.

4.1.1. Case $(\ell = 0)$

As a starting point, we will consider the case $(\ell = 0)$. When $(\ell = 0)$, then (6) becomes:

$$z^n = x^2 + y^2. \tag{7}$$

Let us assume that (7) admits a solution for the stated conditions. Since $[(n > 2) \in \mathbb{O}^+]$, we can write $(n = 2k + 1)$ where $[(k > 0) \in \mathbb{N}^+]$. With $(n \;=\; 2k + 1)$, (6) can be rewritten as:

$$\left(z^k \sqrt{z}\right)^2 = x^2 + y^2. \tag{8}$$

From the decomposition method used in the method of obtaining Pythagorean triples presented in §(2), we know that for any $[(x, y, z) > 1]$ we can always find a pair of positive numbers (p, q) which are not necessarily integers and these numbers (p, q) are such that:

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

Given that ($\sqrt{z} \in \mathbb{I}^{+}$), it follows from the z-component of equation (9) [*i.e.*, ($z^{k}\sqrt{z} = p^{2} + q^{2}$)] and from *Lemma* §(3) that there must exist a pair of integer numbers ($a > b$) each greater than unity which are such that ($p^{2} = a\sqrt{z}$) and ($q^{2} = b\sqrt{z}$); from which we obtain that ($p = \sqrt{a\sqrt{z}}$) and ($q = \sqrt{b\sqrt{z}}$); and substituting these into (9), we will have:

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

Since ($\sqrt{z} \in \mathbb{I}^{+}$); the x-component of (10) is telling us that x must both be an integer and an rational number, that is to say, the integer number ($x > 1$) must equal the irrational number $[(a - b)\sqrt{z}]$ since $[x = (a-b)\sqrt{z}]$. We know very well that this is an impossibility because there does not exist such a number that is both an integer and an irrational number (or stated otherwise, a number that is both an integer and non-integer); hence, by way of contradiction, we conclude that for the conditions investigated here, our initial supposition that (7) has a solution is wrong, thus the initial statement for the conditions investigated must certainly be true since its contrary leads to a clear contradiction.

4.1.2. Case ($\ell > 0$)

(a) If for (6) [($\ell > 0$) such that ($\ell - 1 \neq 0$)], then, (6) can be rewritten as:

$$\left(z^{2^{\ell-1}n}\right)^{2} = x^{2} + y^{2}, \tag{11}$$

hence ($x, y, z^{2^{\ell-1}n}$) is a primitive Pythagorean triple thus, according to the method of Pythagorean triples presented in §(2) [$\exists(p_1, q_1) \in \mathbb{N}^{+}$: ($p_1 > q_1 > 1$)], where these integers (p_1, q_1) are coprime and are such that [$(p_1 - q_1) \in \mathbb{O}^{+}$]; hence:

$$\begin{pmatrix} x \\ y \\ z^{2^{\ell-1}n} \end{pmatrix} = \begin{pmatrix} p_1^{2} - q_1^{2} \\ 2p_1q_1 \\ p_1^{2} + q_1^{2} \end{pmatrix}. \tag{12}$$

At this point, we are going to extract the z-component of (12) namely ($z^{2^{\ell-1}n} = p_1^{2} + q_1^{2}$). If ($\ell - 1 = 0$) for this equation *i.e.* ($z^{2^{\ell-1}n} = p_1^{2} + q_1^{2}$); then ($z^{n} = p_1^{2} + q_1^{2}$). Clearly the equation ($z^{n} = p_1^{2} + q_1^{2}$) is similar to

(7) which we have shown to have no solution, therefore, it follows that ($z^n = p_1^2 + q_1^2$) has no solution as-well. However, if ($\ell - 1 > 0$), then the equation ($z^{2^{\ell-1}n} = p_1^2 + q_1^2$) can be rewritten as:

$$\left(z^{2^{\ell-2}n}\right)^2 = p_1^2 + q_1^2. \tag{13}$$

(b) If ($\ell - 2 = 0$), then, (13) will become ($z^{2n} = p_1^2 + q_1^2$) and the triple (p_1, q_1, z^n) is a primitive Pythagorean triple hence by the method of Pythagorean triples presented in §(2), we will have:

$$\begin{pmatrix} p_1 \\ q_1 \\ z^n \end{pmatrix} = \begin{pmatrix} r_1^2 - s_1^2 \\ 2r_1s_1 \\ r_1^2 + s_1^2 \end{pmatrix}. \tag{14}$$

The z-component of (14) namely the equation ($z^n = r_1^2 + s_1^2$) is similar to (7) which we have shown to have no solution since ($\sqrt{z} \in \mathbb{I}^+$); therefore, it follows that ($z^n = p_1^2 + q_1^2$) has no solution as-well.

However if ($\ell - 2 > 0$), then, the triple ($p_1, q_1, z^{2^{\ell-2}n}$) is a primitive Pythagorean triple. We know from the decomposition method used in the method of obtaining Pythagorean triples presented in §(2), that we can always find some coprime integer numbers (p_2, q_2) which are such that $[(p_2 < p_1, q_2 < q_1) : (p_2 - q_2) \in \mathbb{O}^+]$, such that:

$$\begin{pmatrix} p_1 \\ q_1 \\ z^{2^{\ell-2}n} \end{pmatrix} = \begin{pmatrix} p_2^2 - q_2^2 \\ 2p_2q_2 \\ p_2^2 + q_2^2 \end{pmatrix}. \tag{15}$$

Again as before, we are going to extract the z-component of (15) namely ($z^{2^{\ell-2}n} = p_2^2+q_2^2$). If ($\ell-2 = 0$) for this equation *i.e.* ($z^{2^{\ell-2}n} = p_2^2+q_2^2$); then ($z^n = p_2^2 + q_2^2$). Clearly the equation ($z^n = p_2^2 + q_2^2$) is similar to (7) which we have shown to have no solution, therefore, it follows that ($z^n = p_2^2 + q_2^2$) has no solution as-well. However, if ($\ell - 2 \neq 0$), then the equation ($z^{2^{\ell-2}n} = p_2^2 + q_2^2$) can be rewritten as:

$$\left(z^{2^{\ell-3}n}\right)^2 = p_2^2 + q_2^2. \tag{16}$$

(c) If ($\ell - 2 = 0$), then, (16) will become ($z^{2n} = p_2^2 + q_2^2$) and the triple (p_2, q_2, z^n) is a primitive Pythagorean triple hence by the method of Pythagorean triples presented in §(2), we will have:

$$\begin{pmatrix} p_2 \\ q_2 \\ z^n \end{pmatrix} = \begin{pmatrix} r_2^2 - s_2^2 \\ 2r_2 s_2 \\ r_2^2 + s_2^2 \end{pmatrix}. \tag{17}$$

The z-component of (17) namely the equation $(z^n = r_2^2 + s_2^2)$ is similar to (7) which we have shown to have no solution since $(\sqrt{z} \in \mathbb{I}^+)$; therefore, it follows that $(z^n = p_2^2 + q_2^2)$ has no solution as-well.

However, if $(\ell - 3 > 0)$, then, the triple $(p_2, q_2, z^{2^{\ell-3}n})$ is a primitive Pythagorean triple. We know from the decomposition method used in the method of obtaining Pythagorean triples presented in §(2), that we can always find some coprime integer numbers (p_3, q_3) which are such that $[(p_3 < p_2, q_3 < q_2) : (p_3 - q_3) \in \mathbb{O}^+]$, such that:

$$\begin{pmatrix} p_2 \\ q_2 \\ z^{2^{\ell-2}n} \end{pmatrix} = \begin{pmatrix} p_3^2 - q_3^2 \\ 2p_3 q_3 \\ p_3^2 + q_3^2 \end{pmatrix}. \tag{18}$$

Again as before, we are going to extract the z-component of (18) namely $(z^{2^{\ell-3}n} = p_3^2+q_3^2)$. If $(\ell-3 = 0)$ for this equation *i.e.* $(z^{2^{\ell-3}n} = p_3^2+q_3^2)$; then $(z^n = p_3^2 + q_3^2)$. Clearly the equation $(z^n = p_3^2 + q_3^2)$ is similar to (7) which we have shown to have no solution, therefore, it follows that $(z^n = p_3^2 + q_3^2)$ has no solution as-well. However, if $(\ell - 3 > 0)$, then the equation $(z^{2^{\ell-3}n} = p_3^2 + q_3^2)$ can be rewritten as:

$$\left(z^{2^{\ell-4}n}\right)^2 = p_3^2 + q_3^2. \tag{19}$$

(d) At this point we believe that the reader notices that this cycle will continue up-till that point where $(\ell - j = 0)$. At each j^{th} stage before we have $(\ell - j = 0)$; we obtain the z-component equation which reads:

$$z^{2^{\ell-j}n} = p_j^2 + q_j^2, \tag{20}$$

and the integer number $(p_j > q_j > 1)$ are coprime and are such that $[(p_j, q_j) \in \mathbb{O}^+]$ and $(p_j < p_{j-1}; q_j < q_{j-1})$. Once $(\ell - j = 0)$, (20) becomes:

$$z^n = p_j^2 + q_j^2. \tag{21}$$

At this point, the downward descent can not continue any more since we have the equation (21) is similar to (7) which we have shown to have no solution, therefore, it follows that (21) has no solution as-well.

Summary

Since in both cases $(\ell = 0)$ and $(\ell > 0)$ we arrive at a clear contradiction, it therefore follows that contrary to the initial supposition, (6) admits no integer solutions for ***all*** $[(n > 2) \in \mathbb{O}^+]$. ***Q.E.D.***

4.2. Corollary

A corollary that can be deduced from the x-component of (9) is that the equation $(x = p^2 - q^2)$, admits no solutions for any coprime triple $[\{(x, p, q) > 1\} \in \mathbb{N}^+]$ for which $(x : \sqrt{x} \in \mathbb{I}^+)$. Stated more formally – the equation:

$$z = x^2 - y^2, \tag{22}$$

admits no solutions for any coprime triple $[\{(x, y, z) > 1\} \in \mathbb{N}^+]$ for which $(z : \sqrt{z} \in \mathbb{I}^+)$. This fact will become helpfull in the reading Nyambuya (2014b), when we confront the proof of *Beal's Conjecture via* the method of Pythagorean triples.

5. Fermat's Proofs for the Case $(n = 4)$

Fermat was the first to provide a proof for the case $(n = 4)$ which stated that for all non-zero piecewise coprime triple $(x, y, z) \in \mathbb{N}^+$, the equation $x^4 + y^4 = z^4$ 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. Further, 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. Gambioli, 1901; Legendre, 1823; Hilbert, 1897; Lebesgue, 1853; Kronecker, 1901, amongst many others). Even after Sir Professor Andrew Wiles's 1995 breakthrough Wiles (1995), researchers are still publishing variants of the proof for the case $(n = 4)$ (*cf.* Grant and Perella, 1999; Dolan, 2011; Barbara, 2007). Below, we present Fermat's proof.

The equation $x^4 + y^4 = z^4$ – with coprime $[\{(x, y, z) > 1\} \in \mathbb{N}^+]$; can be written equivalently as:

$$Z^2 = X^4 - Y^4, \tag{23}$$

where $[\{(X, Y, Z) > 1\} \in \mathbb{N}^+]$ is a set of coprime numbers; and further, this equation can be rewritten as:

$$Z^2 = (X^2 + Y^2)(X^2 - Y^2). \tag{24}$$

Since X and Y are coprime, the greatest common divisor of $(X^2 + Y^2)$ and $(X^2 - Y^2)$ is either 2 (Case A) or 1 (Case B). The theorem is proven separately for these two cases.

5.0.1. Case A

In this case, both X and Y can only be odd with Z being even. Since the coprime triple (X^2, Y^2, Z) form a primitive Pythagorean triple (remember $X^4 = Y^4 + Z^2$), they can be decomposed into:

$$\begin{array}{rcl} Y^2 & = & p^2 - q^2 \\ Z & = & 2pq \\ X^2 & = & p^2 + q^2 \end{array} \tag{25}$$

where p and q are coprime integers and $(p > q > 1)$ with $[(p - q) \in \mathbb{O}^+]$. From (25), it follows that:

$$(XY)^2 = p^4 - q^4. \tag{26}$$

In (26) we have produced another solution (p, q, XY) which is such that $(0 < p < X)$. By the above argument that solutions cannot be shrunk indefinitely and as we all know, this is impossible hence, this proves that the original solution is impossible.

5.0.2. Case B

In this case, the two factors $[(X^2 + Y^2)$ and $(X^2 - Y^2)]$ are coprime. Since their product is a square $[i.e.\ (X^2 + Y^2)(X^2 - Y^2) = Z^2]$, they must each be a squares, *i.e.*:

$$\begin{aligned} p^2 &= X^2 + Y^2 \\ q^2 &= X^2 - Y^2 \end{aligned} \tag{27}$$

The numbers p and q are both odd, since $(p^2 + q^2 = 2X^2)$ is an even number, and since X and Y cannot both be even. Therefore, the sum and the difference of p and q are likewise even numbers, one can define integers u and v as:

$$\begin{aligned} u &= \tfrac{1}{2}(p+q) \\ v &= \tfrac{1}{2}(p-q) \end{aligned} \tag{28}$$

Since p and q are coprime, so are u and v; only and only one of them can be even. Since $(p^2 - q^2 = 2Y^2)$, it follows that $Y^2 = 2uv$, hence, exactly one of them (u, v) is even. For illustration, let u be even; then the numbers may be written as $u = 2m^2$ and $v = k^2$. Since (u, v, X) form a primitive Pythagorean triple, *i.e.*:

$$\frac{1}{2}(p^2 + q^2) = u^2 + v^2 = X^2 \tag{29}$$

they can be expressed in terms of smaller integers g and h using Euclid's formula

$$\begin{aligned} v &= g^2 - h^2 \\ u &= 2gh \\ X &= g^2 + h^2 \end{aligned} \tag{30}$$

Since $u = 2m^2 = 2gh$, and since g and h are coprime, they must be squares themselves, $g = r^2$ and $h = s^2$. From this we obtain the equation:

$$v = g^2 - h^2 = r^4 - s^4 = k^2 \tag{31}$$

The triple (r, s, k) is another solution to the original equation – *albeit*, smaller than the original solution *i.e.* $(0 < g < h < X)$. Applying the same procedure to (r, s, k) would produce another solution, still smaller, and so on. But this is impossible, since natural numbers cannot be shrunk indefinitely. Therefore, the original solution (X, Y, Z) is impossible.

6. Proof of Fermat's Last Theorem (II)

As with the previous proofs in the presiding chapter, the proof that we are going to provide of FLT is a proof by contradiction. We assume the statement:

$$\exists\ (x > 1, y > 1, z > 1, n) \in \mathbb{N}^{+} :\ \ x^n + y^n = z^n,\ \ \text{for all}\ \ (n > 2), \qquad (32)$$

to be true. The triple (x, y, z) is piecewise *coprime*, the meaning of which is that the greatest common divisor [gcd()] of this triple or any arbitrary pair of the triple is unity.

That is, 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 just one of the numbers of the quadruplet (x, y, z, n) can not belong to the set of integers, we will have proved *Fermat's Last Theorem*. In our approach to the problem (proof), we split it into two parts, *i.e.*:

- **Case (I) :** This case proves for all powers of $[(n\ >\ 4) \in \mathbb{E}^{+}]$ where $\mathbb{E}^{+}$ is the set of all positive even integer numbers. The case $(n = 4)$ is considered to have been proved by Fermat as presented in §(5). Actually, in-order for us to prove FLT for even indices, the present proof requires us to make a separate proof for $(n = 4)$. Given that Fermat did provide a proof for $(n = 4)$ and claimed to have discovered a general proof for FLT, these simple facts strongly point to the idea that the proof that we here provide may very well be the proof Fermat claimed to have discovered.

- **Case (II) :** This case proves for all powers of $[(n\ >\ 2) \in \mathbb{O}^{+}]$ where $\mathbb{O}^{+}$ is the set of all positive odd integer numbers.

Since the set $[(n > 2) \in \mathbb{N}^{+}]$ contains only odd and even values of n, to prove that there does not exist an even and odd $[(n > 2) \in \mathbb{N}^{+}]$ that satisfies (32) is a proof that there does not exist $[(x, y, z, n) \in \mathbb{N}^{+} :\ \ x^n + y^n\ =\ z^n,\quad (n\ >\ 2)]$. This is a proof of the original statement (1).

6.1. Case (I): Even Powers of $(n > 4)$

If $[(n > 4) \in \mathbb{E}^{+}]$, then we can write $(n = 2^{\ell}k)$ where $[(\ell = 1, 2, 3, 4, \ldots\, etc) \in \mathbb{N}^{+}]$ and $[(k \;=\; 3, 5, 7, \ldots\, etc) \in \mathbb{O}^{+}]$ is an odd number greater than two. With $(n = 2^{\ell}k)$, then, under the given conditions, we know that (32) can be rewritten as:

$$x^{2^{\ell}k} + y^{2^{\ell}k} = z^{2^{\ell}k}, \tag{33}$$

and this can further be rewritten as:

$$\left(x^{2^{\ell-1}k}\right)^2 + \left(y^{2^{\ell-1}k}\right)^2 = \left(z^{2^{\ell-1}k}\right)^2, \tag{34}$$

where $(x^{2^{\ell-1}k}, y^{2^{\ell-1}k}, z^{2^{\ell-1}k})$ is a piecewise coprime triple. As long as $(\ell - 1 \geq 0)$, all the members of the piecewise coprime triple $(x^{2^{\ell-1}k}, y^{2^{\ell-1}k}, z^{2^{\ell-1}k})$ are all positive integers thus, the triple $(x^{2^{\ell-1}k}, y^{2^{\ell-1}k}, z^{2^{\ell-1}k})$, is a primitive Pythagorean triple.

As is well known from §(2), namely Euclid's formula for generating primitive Pythagorean triples that, since $(x^{2^{\ell-1}k}, y^{2^{\ell-1}k}, z^{2^{\ell-1}k})$, is a primitive Pythagorean triple, there must exist a pair of coprime integers $(p > q > 1)$, which are such that $(p_1 - q_1)$ is odd, such that:

$$\begin{pmatrix} x^{2^{\ell-1}k} \\ y^{2^{\ell-1}k} \\ z^{2^{\ell-1}k} \end{pmatrix} = \begin{pmatrix} p^2 - q^2 \\ 2pq \\ p^2 + q^2 \end{pmatrix}. \tag{35}$$

From (35), we extract the z-component of this equation, *i.e.* $(z^{2^{\ell-1}k} = p_1^2 + q_1^2)$, and we will write this equation as:

$$z^{2^{\ell-1}k} = p^2 + q^2. \tag{36}$$

Since z is such that $\sqrt{z} \in \mathbb{I}^{+}$ or $\sqrt{z} \in \mathbb{N}^{+}$, we can write $z = \zeta^{2^m}$ where $(m \geq 0)$. If $\sqrt{z} \in \mathbb{I}^{+}$, then $(m = 0)$; and, if $\sqrt{z} \in \mathbb{N}^{+}$, then $(m > 0)$. Therefore, substituting $z = \zeta^{2^m}$ into (36), we will have:

$$\zeta^{2^{\ell+m+1}k} = p^2 + q^2. \tag{37}$$

According to the theorem presented in §(4), equation (37) has no solution. It therefore follows that we clearly have demonstrated that for $[(n > 2) \in \mathbb{E}^{+}]$ the statement (32) can not be true as initially supposed, hence *Fermat's Last Theorem* is true for $[(n > 2) \in \mathbb{E}^{+}]$.

6.2. *Case (II): Odd Powers of* $(n > 2)$

Now, we have to prove for the case $[(n > 2) \in \mathbb{O}^+]$. The fact that $[(n > 2) \in \mathbb{O}^+]$, this implies that we can set $n = 2k + 1$ where $k = 2, 3, 4, 5, \ldots, etc \Rightarrow (k > 1)$ if n is to be greater than 2. With $n = 2k + 1$, the equation $x^n + y^n = z^n$ can now be rewritten as $x^{2k+1} + y^{2k+1} = z^{2k+1}$ and this can further be rewritten as:

$$\left(x^k\sqrt{x}\right)^2 + \left(y^k\sqrt{y}\right)^2 = \left(z^k\sqrt{z}\right)^2. \tag{38}$$

The triplet, trio or the three numbers $(x^k\sqrt{x}, y^k\sqrt{y}, z^k\sqrt{z})$ are not necessarily integers, thus this triple is not a Pythagorean triple in the traditional parlance of mathematics. However, this handicap does not stop us (or anyone for that matter) from finding real numbers $(p, q : p > q)$ which are not necessarily integers, where these numbers (p, q) are such that:

$$\begin{pmatrix} x^k\sqrt{x} \\ y^k\sqrt{y} \\ z^k\sqrt{z} \end{pmatrix} = \begin{pmatrix} p^2 - q^2 \\ 2pq \\ p^2 + q^2 \end{pmatrix}. \tag{39}$$

As in the case for the proof for even powers of $(n > 2)$, our focal point here is the z-component of (39). For z, we have two and only two cases (conditions) and these are:

- **Case (1):** $(\sqrt{z} \in \mathbb{N}^+)$.

- **Case (2):** $(\sqrt{z} \notin \mathbb{N}^+)$. That is, $\sqrt{z}$, is an irrational number.

We will provide proofs for the two cases as stated above.

6.2.1. *Case (1): Proof for the Case* $(\sqrt{z} \in \mathbb{N}^+)$

If $(\sqrt{z} = w \in \mathbb{N}^+)$, clearly, it follows that $(p > q > 1) \in \mathbb{N}^+$. If $(p, q) \in \mathbb{N}^+$, then $(\sqrt{x} = u) \in \mathbb{N}^+$ and $(\sqrt{y} = v) \in \mathbb{N}^+$. From this, it follows that (38) will now become:

$$u^{2(2k+1)} + v^{2(2k+1)} = w^{2(2k+1)}. \tag{40}$$

According to the proof we have given in §(6.1) for even n *i.e.* for $(n > 2) \in \mathbb{E}^+$, it follows that (40) admits no solutions.

6.2.2. Case (2): Proof for the Case ($\sqrt{z} \in \mathbb{I}^{+}$)

In the case where ($\sqrt{z} \in \mathbb{I}^{+}$), it follows from *Lemma* §(3) that for the z-component of (39), there must exist some $(a > b > 1) \in \mathbb{N}^{+}$, such that ($p^2 = a\sqrt{z}$) and ($q^2 = b\sqrt{z}$), *i.e.*, ($z^k\sqrt{z} = a\sqrt{z} + b\sqrt{z}$). Thus, from, ($p^2 = a\sqrt{z}$) and ($q^2 = b\sqrt{z}$), it follows that ($p = \sqrt{a\sqrt{z}}$) and ($q = \sqrt{b\sqrt{z}}$). Substituting all this into (39), we will have:

$$\begin{pmatrix} x^k\sqrt{x} \\ y^k\sqrt{y} \\ z^k\sqrt{z} \end{pmatrix} = \begin{pmatrix} (a-b)\sqrt{z} \\ 2\sqrt{a}\sqrt{b}\sqrt{z} \\ (a+b)\sqrt{z} \end{pmatrix}. \tag{41}$$

Clearly, from (41), it follows that ($\sqrt{x} \notin \mathbb{N}^{+}$) because ($z \propto x$), that is to say ($z = s^2x$) for some $[(s > 1) \in \mathbb{N}^{+}]$. To see this is not difficult a thing at all. We know that ($x^k \in \mathbb{N}^{+}$) but (41) is telling us that $[x^k = (a-b)\sqrt{z/x}]$. Since $[(a-b) \in \mathbb{N}^{+}]$, for $[x^k = (a-b)\sqrt{z/x} \in \mathbb{N}^{+}]$, we must have $[\sqrt{z/x} = s \in \mathbb{N}^{+}]$ *i.e.* ($z = s^2x$). This means that x and z share a common factor ($s^2 > 1$), the meaning of which is that the triple (x, y, z) is not piecewise coprime. Since our initial assertion runs contrary to our final conclusion, hence, by way of contradiction, it follows that our initial assertion is wrong as it has lead us to an illogical conclusion. Hence, for $[(x, y, z) \in \mathbb{N}^{+}]$ (32) admits no solutions under the given conditions since the piecewise coprime triple (x, y, z) can not be piecewise coprime as initially assumed.

Alternatively, since ($\sqrt{z} = \zeta \in \mathbb{I}^{+}$), the z-component of (41) can also be written as:

$$\zeta^{2k+1} = p^2 + q^2. \tag{42}$$

According to the theorem presented in §(4), equation (42) has no solution since ($\zeta \in \mathbb{I}^{+}$) and $[(2k+1) \in \mathbb{O}^{+}]$. It therefore follows that for $[(x, y, z) \in \mathbb{N}^{+}]$ (32) admits no solutions under the given conditions.

Summary

Combining the two proofs for the case $[(n > 2) \in \mathbb{O}^{+}]$; for the sub-cases ($\sqrt{z} \in \mathbb{N}^{+}$) and ($\sqrt{z} \in \mathbb{I}^{+}$), it follows that, equation (32) admits no integer solutions for any non-zero piecewise coprime triple $[(x, y, z) \in \mathbb{N}^{+}]$ for all $[(n > 2) \in \mathbb{O}^{+}]$.

6.3. Summary of the Two Proofs

In §(6.1) and (6.2), we have proved that (32) admits no integer solutions for any $[(x, y, z) > 1]$ and $[(x, y, z) \in \mathbb{N}^+]$ for all powers of $[(n > 2) \in \mathbb{E}^+]$ and for all powers $(n > 2) \in \mathbb{O}^+$. Combining these two proofs, it follows from the foregoing as stated and outlined at the beginning of this section, that (32) admits no integer solutions for any $[(x, y, z) > 1]$ and $[(x, y, z) \in \mathbb{N}^+]$ for all powers of $[(n > 2) \in \mathbb{N}^+]$. Hence, *Fermat's Last Theorem* is here proved in a simpler, much more general and truly marvellous manner.

7. General Discussion

If the proof we have provided herein stands the test of time and experience, then, it is without a shred or dot of doubt that Fermat's claim to have had a '*truly marvellous*' proof may very well resonate with truth. Our reasons for thinking this are justified by the fact that Fermat himself provided a proof for the case $(n = 4)$. The question is "*Why did he provide this proof for the case* $(n = 4)$*?*" As in the proof that we have provided, was not Fermat's proof for the case $(n = 4)$ part of a general proof for the case $[(n > 2) \in \mathbb{O}^+]$? Our proof here requires a separate proof for the case $(n = 4)$ and there-after a more general proof for $(n > 4)$ is possible. One can not thus rule out that Fermat provided the proof for the case $(n = 4)$ as part of a more general proof for the case $[(n > 2) \in \mathbb{O}^+]$.

The second reason for strongly siding with Fermat is that the present proof employs the method of Pythagorean triples which Fermat knew very well and he used this in the proof for the case $(n = 4)$. The subtlety in finding a more general and elegant proof lies in *Lemma* §(3); a fact that Fermat (as one of the greatest number theorists) must have known. Off cause, we can never know for sure whether the present proof is what Fermat had at hand, or whether his claimed proof contained as flaw. But, with the present proof in place, it is difficult to now dismiss that Fermat's claim may very well be true because our proof employs mathematical tools available in Fermat's days.

As to ourself – given the present light, we do not want to take away the fact that 'Fermat's claim may very well be true'. He most certainly had the proof, the problem is that the bare mathematical truth in the form of *Lemma* §(3) may not have crossed the minds of mathematicians in search of Fermat's claimed proof – it simply was overlooked. Clearly, 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. Given that an arithmetic proof is very easy to judge as either correct or wrong using 16^{th} century arithmetic, few – if any; would believe that this is possible for one to obtain an arithmetic proof of *Fermat's Last Theorem*. 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. In the reading Nyambuya (2014a), we have provided an even much simpler proofs of *Fermat's Last Theorem* and as well *Beal's Conjecture*.

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 pass its judgement on 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. Further, allow us to that that, it strongly appears that the great physicist and philosopher – Albert 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.

8. Conclusion

We hereby put forward the following conclusion:

1. By use of the method of 'Pythagorean triples', we have demonstrated that a solution to *Fermat's Last Theorem* exists in the realm of elementary arithmetic.

2. This proof employs elementary arithmetic tools and methods that were certainly accessible to Fermat, thus making it highly likely that Fermat's claim that he possessed a 'truly marvellous' proof may very be true.

Acknowledgments: We are grateful to the National University *of* Science *&* Technology (NUST)'s Research *&* Innovation Department and Research Board for their unremitting support rendered toward our research endeavours; of particular mention, Prof. Dr. P. Mundy, Dr. P. Makoni. Dr. D. J. Hlatswayo, and Prof. Y. S. Naik's unwavering support. We must make mention of the fact that this work was inspired some twenty two years ago by Marist Brothers Secondary School, Dete, Zimbabwe;'s then mathematical prodigy and now medical practitioner *DR. Charles Muzondi*. This reading is dedicated to my mother *Setmore Nyambuya* and to the memory of departed father *Nicholas Nyambuya* (*27.10.1947*− *23.09.1999*).

9. References

Barbara, R., July 2007. Fermat's Last Theorem in the Case $n = 4$. Mathematical Gazette 91, 260–262.

Cox, D. A., 1994. Introduction to Fermat's Last Theorem, http://math.stanford.edu/ lekheng/flt/cox.pdf.
URL `http://math.stanford.edu/ lekheng/flt/cox.pdf`

Dolan, S., July 2011. Fermat's Method of Descente Infinie. Mathematical Gazette 95, 269–271.

Gambioli, D., 1901. Memoria Bibliographica Sull'ultimo Teorema di Fermat. Period. Mat. 16, 145–192.

Grant, M., Perella, M., July 1999. Descending to the Irrational. Mathematical Gazette 83, 263–267.

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.

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

Kronecker, L., 1901. Vorlesungen Über Zahlentheorie. Leipzig: Teubner I, 33–38, reprinted by New York: Springer-Verlag in 1978.

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.

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.

Nyambuya, G. G., May 2014a. A Simple and General Proof of Beal's Conjecture (I). Advances in Pure Mathematics 4 (9), 1–4.

Nyambuya, G. G., 2014b. A Simple and General Proof of Beal's Conjecture (II), http://vixra.org/abs/1405.0023.
URL `http://vixra.org/abs/1405.0023`

Wiles, A., 1995. Modular Elliptic Curves and Fermat's Last Theorem. Annals of Mathematics 141 (3), 443–551, doi:10.2307/2118559.