RESEARCH ARTICLE

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

G. Gadzirayi Nyambuya

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 proving it.

Keywords: Diophantine equations; Fermat's Last Theorem;

AMS Subject Classification: 11D41

1 Introduction

This is our second version of a simpler, much more general and truly marvellous proof of Fermat's Last Theorem. As already highlighted in the first instalments: the pre-eminent French lawyer and amateur mathematician, the late 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), 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:

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

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 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 by 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*, 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*". As highlighted in the first instalent, our aim is to give a simper proof that makes use of methods that where available in Fermat's days. In this way, we seek to validate Fermat's claim that he had the proof.

Before we proceed to the main business of the day, we write down the well known method for generating

Correspondence: physicist.ggn@gmail.com
National University of Science and Technology
Faculty of Applied Sciences – Department of Applied Physics,
Fundamental Theoretical and Astrophysics Group,
Cnr Gwanda Rd and Cecil Ave – Ascot Bulawayo,
P. O. Box AC 939,
Republic of Zimbabwe
Full list of author information is available at the end of the article

[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.

primitive Pythagorean triples. This method is key to our proof. Thereafter, we give a key Lemma which is vital for our proof. In §(4) we briefly discuss notable attempts at proving Fermat's Last Theorem. Thereafter, we go to the main business of the day where we supply our simpler, much more general and truly marvellous proof of Fermat's Last Theorem.

2 Primitive 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 $(X \in \mathbb{O}^+)$, $(Y \in \mathbb{E}^+)$ and $(Z \in \mathbb{O}^+)$:

$$\begin{array}{rcll} X & = & p^2 - q^2 & \in \mathbb{O}^+ \\ Y & = & 2pq & \in \mathbb{E}^+ \\ Z & = & p^2 + q^2 & \in \mathbb{O}^+ \end{array} , \tag{2}$$

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:

$$\begin{array}{ccccccc} \overbrace{\left(p^2+q^2\right)^2}^{\in\mathbb{O}^+} & \equiv & \overbrace{\left(p^2-q^2\right)^2}^{\in\mathbb{O}^+} & + & \overbrace{\left(2pq\right)^2}^{\in\mathbb{E}^+} & . & (3) \\ \Downarrow & & \Downarrow & & \Downarrow & & \\ Z^2 & = & X^2 & + & Y^2 & & \end{array}$$

Clearly, there are infinitely many primitive Pythagorean triples. Invariably – this means that, there must exist infinitely many piecewise co-prime triples $(X, Y, Z) \in \mathbb{Z}^+$ where $\mathbb{Z}^+$ 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*.

2.1 Corollary

We will strongly emphasis here that if (X, Y, Z) constitute a primitive Pythagorean triple satisfying the Pythagoras equation $(Z^2 = X^2 + Y^2)$, then $(Z \in \mathbb{O}^+)$, while $(X \in \mathbb{E}^+ \,\&\, Y \in \mathbb{O}^+)$ or $(X \in \mathbb{O}^+ \,\&\, Y \in \mathbb{E}^+)$. It is impossible to have a primitive Pythagorean triple for which $(Z \in \mathbb{E}^+)$. This condition will is the sole-root to the proof in §(5.1.2) and (5.2). In these sections (5.1.2 and 5.2), we will generate a primitive Pythagorean triple for which $(Z \in \mathbb{E}^+)$.

3 Lemma

If $[(a, b) \in \mathbb{Z}^+]$ 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 $(\sqrt{b} \in \mathbb{Z}^+)$.

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

—

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

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

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

While (c_1, d_1) are not necessarily integers, one can always find some (c_1, d_1) such that $[(c_1, d_1) \in \mathbb{Z}^+]$ for as long as $[(a > 1) \in \mathbb{Z}^+]$. 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 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 $(x, y, z) \in \mathbb{Z}^+$, 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. 3, 5–8, amongst many others]. Even after Sir Professor Andrew Wiles's 1995 breakthrough [10], researchers are still publishing variants of the proof for the case $(n = 4)$ [*cf.* 1, 2, 4].

Below, we present Fermat's proof. We present this proof for nothing other than instructive purposes. There lies in this proof for $(n = 4)$ something which

when combined with what we have stated in the penultimate of §(2) *i.e.*, on the impossibility of $(Z \in \mathbb{E}^+)$, a solution to FLTs is achieved.

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

$$Z^2 = X^4 - Y^4, \tag{6}$$

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

$$Z^2 = (X^2 + Y^2)(X^2 - Y^2). \tag{7}$$

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.

4.0.1 ***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:

$$\begin{aligned} Y^2 &= p^2 - q^2 \\ Z &= 2pq \\ X^2 &= p^2 + q^2 \end{aligned} \tag{8}$$

where p and q are coprime integers and $(p > q > 1)$ with $[(p - q) \in \mathbb{O}^+]$. From (8), it follows that:

$$(XY)^2 = p^4 - q^4. \tag{9}$$

In (9) we have produced another solution (XY, p, q) which is such that $(0 < p < X)$. The triple (XY, p, q) is another solution to the original equation – *albeit*, smaller than the original solution *i.e.* $(0 < p < q < X)$. Applying the same procedure to (XY, p, q) 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.

4.0.2 ***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, that is to say, $[\ (X^2 + Y^2)(X^2 - Y^2) = Z^2]$, they must each be a squares, *i.e.*:

$$\begin{aligned} p^2 &= X^2 + Y^2 \\ q^2 &= X^2 - Y^2 \end{aligned} \tag{10}$$

The numbers (p, 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:

$$\begin{aligned} u &= \tfrac{1}{2}(p + q) \\ v &= \tfrac{1}{2}(p - q) \end{aligned} \tag{11}$$

Since (p, q) are coprime, so are (u, 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.*:

$$\frac{1}{2}(p^2 + q^2) = u^2 + v^2 = X^2 \tag{12}$$

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

$$\begin{aligned} v &= g^2 - h^2 \\ u &= 2gh \\ X &= g^2 + h^2 \end{aligned} \tag{13}$$

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:

$$v = g^2 - h^2 = r^4 - s^4 = k^2 \tag{14}$$

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.

5 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:

$$\exists\ \{[(x,y,z)>1],n\}\in\mathbb{Z}^{+}:\ x^{n}+y^{n}=z^{n},\quad(\forall n>2), \tag{15}$$

to be true. Throughout this reading, we shall take $(z\in\mathbb{O}^{+})$, $(y\in\mathbb{E}^{+})$ and $(x\in\mathbb{O}^{+})$. 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 $[(n>2)\in\mathbb{O}^{+}]$ where $\mathbb{O}^{+}$ is the set of all positive odd integer numbers.
- **Case (II) :** 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 §(4). 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.

Since the set $[(n>2)\in\mathbb{Z}^{+}]$ contains only odd and even values of n, to prove that there does not exist an even and odd $[(n>2)\in\mathbb{Z}^{+}]$ that satisfies (15) is a proof that there does not exist $[(x,y,z,n)\in\mathbb{Z}^{+}:(x^{n}+y^{n}=z^{n}),\quad(n>2)]$. This is a proof of the original statement (1).

5.1 Case (I): 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:

$$\left(x^{k}\sqrt{x}\right)^{2}+\left(y^{k}\sqrt{y}\right)^{2}=\left(z^{k}\sqrt{z}\right)^{2}. \tag{16}$$

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:

$$\begin{pmatrix} x^{k}\sqrt{x}\\ y^{k}\sqrt{y}\\ z^{k}\sqrt{z}\end{pmatrix}=\begin{pmatrix} p^{2}-q^{2}\\ 2pq\\ p^{2}+q^{2}\end{pmatrix}. \tag{17}$$

Our focal point here is the z-component of (17). For z, we have two and only two cases (conditions) and these are:

- **Case (A):** $(\sqrt{z}\in\mathbb{Q}^{+})$. That is, $\sqrt{z}$, is an irrational number. The set $\mathbb{Q}^{+}$ is the set of positive irrational numbers.
- **Case (B):** $(\sqrt{z}\in\mathbb{Z}^{+})$.

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

5.1.1 *Case (A): Proof for the Case* $(\sqrt{z}\in\mathbb{Q}^{+})$

In the case where $(\sqrt{z}\in\mathbb{Q}^{+})$, it follows that in general we must have:

$$\begin{aligned} p^{2} &= \alpha_{1}z^{k}\sqrt{z}+\beta\\ q^{2} &= \alpha_{2}z^{k}\sqrt{z}-\beta\end{aligned}\ , \tag{18}$$

where the α's are not integers but are positive real numbers and β may or may not be an integer and is such that it is positive number.

With the definition of p and q as given in (18), there are two routes to be taken, and these are:

1 Route (1): For which $(\beta=0)$.
2 Route (2): For which $(\beta\neq0)$.

Below, we will consider the two routes.

5.1.1.1 *Route (1)*

In this case where $(\sqrt{z}\in\mathbb{Q}^{+})$ and $(\beta=0)$, it follows from *Lemma* §(3) that for the z-component of (17), there must exist some $(a>b>1)\in\mathbb{Z}^{+}$,

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 (17), we will have:

$$\begin{pmatrix} x^k\sqrt{x} \\ y^k\sqrt{y} \\ z^k\sqrt{z} \end{pmatrix} = \begin{pmatrix} (a-b)\sqrt{z} \\ 2\sqrt{a}\sqrt{b}\sqrt{z} \\ (a+b)\sqrt{z} \end{pmatrix}. \tag{19}$$

Clearly, from (19), it follows that $(\sqrt{x} \notin \mathbb{Z}^+)$ because $(z \propto x)$, that is to say $(z = s^2x)$ for some $[(s > 1) \in \mathbb{Z}^+]$. To see this is not difficult a thing at all. We know that $(x^k \in \mathbb{Z}^+)$ but (19) is telling us that $[x^k = (a-b)\sqrt{z/x}]$. Since $[(a-b) \in \mathbb{Z}^+]$, for $[x^k = (a-b)\sqrt{z/x} \in \mathbb{Z}^+]$, we must have $[\sqrt{z/x} = s \in \mathbb{Z}^+]$ *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 $[(x, y, z) \in \mathbb{Z}^+]$ (15) admits no solutions under the given conditions since the piecewise coprime triple (x, y, z) can not be piecewise coprime as initially assumed.

5.1.1.2 *Route (2)*

In this case where $(\sqrt{z} \in \mathbb{Q}^+)$ and $(\beta \neq 0)$, then, by substituting p and q as given in (18) into (17), from the z-component, we have $(\alpha_1 + \alpha_2 = 1)$ and from the x-component, we have $(\alpha_1 - \alpha_2 = 0)$; from these two equations, we will have $(\alpha_1 = \alpha_2 = 1/2)$, therefore, for p and q, we will have:

$$\begin{aligned} p^2 &= \tfrac{1}{2}z^k\sqrt{z} + \beta \\ q^2 &= \tfrac{1}{2}z^k\sqrt{z} - \beta \end{aligned}, \tag{20}$$

thus substituting this into (17), we will have:

$$\begin{pmatrix} x^k\sqrt{x} \\ y^k\sqrt{y} \\ z^k\sqrt{z} \end{pmatrix} = \begin{pmatrix} 2\beta \\ 2\left(z^{2k+1}/4 - \beta^2\right) \\ z^k\sqrt{z} \end{pmatrix}. \tag{21}$$

From the x-component of equation (21), we have $(x^{2k+1} = 4\beta^2 \in \mathbb{Z}^+)$ – hence, it follows that $(\beta^2 \in \mathbb{Z}^+)$; from the foregoing, clearly 2 is a factor of x. Going back to our initial assertion, y is an even number the meaning of which that it is divisible by 2. At this point, we will have to stop as we have arrived at our desired contradiction since (x, y) have a common factor 2, thus, by way of contradiction, our initial assertion is certainly wrong. Both routes (1) and (2) have led us to a contradiction. We shall now move to Case (B).

5.1.2 *Case (B): Proof for the Case* $(\sqrt{z} \in \mathbb{Z}^+)$

If $(\sqrt{z} = w \in \mathbb{Z}^+)$, clearly $(p, q) \in \mathbb{Z}^+$. If $(p, q) \in \mathbb{Z}^+$, it follows that $(\sqrt{x} = u) \in \mathbb{Z}^+$ and $(\sqrt{y} = v) \in \mathbb{Z}^+$. From this, it follows that (16) will now become:

$$[u^{(2k+1)}]^2 + [v^{(2k+1)}]^2 = [w^{(2k+1)}]^2. \tag{22}$$

The above equation is equivalent to the Fermat's original equation where $(n \in \mathbb{E}^+)$. Further, the triple $[u^{(2k+1)}, v^{(2k+1)}, w^{(2k+1)}]$ is a primitive Pythagorean triple. It follows that (17) can now be written as:

$$\begin{pmatrix} u^{(2k+1)} \\ v^{(2k+1)} \\ w^{(2k+1)} \end{pmatrix} = \begin{pmatrix} p^2 - q^2 \\ 2pq \\ p^2 + q^2 \end{pmatrix}. \tag{23}$$

We shall not prove that this equation has no solution here – we shall do this §(5.2) below.

Summary

Combining the two proofs for the case $[(n > 2) \in \mathbb{O}^+]$; for the sub-cases $(\sqrt{z} \in \mathbb{Z}^+)$ and $(\sqrt{z} \in \mathbb{Q}^+)$, it follows that, equation (15) admits no integer solutions for any non-zero piecewise coprime triple $[(x, y, z) \in \mathbb{Z}^+]$ for all $[(n > 2) \in \mathbb{O}^+]$.

5.2 Case (II): Even Powers of $(n > 4)$

If $[(n > 4) \in \mathbb{E}^+]$, it is not difficult to see that we can always write $(n = 2^\ell k)$ where $[(\ell = 1, 2, 3, 4, \ldots\ etc) \in \mathbb{Z}^+]$ and $[(k = 3, 5, 7, \ldots\ etc) \in \mathbb{O}^+]$ is an odd number greater than two. For example, for the numbers $(n = 6, \ldots, 24)$, we have:

n	ℓ	k	
6	1	3	$2^1 \times 3$
8	3	1	$2^3 \times 1$
10	1	5	$2^1 \times 5$
12	2	3	$2^2 \times 3$
14	1	7	$2^1 \times 7$
16	4	1	$2^4 \times 1$
18	1	9	$2^1 \times 9$
20	2	5	$2^1 \times 3$
22	1	11	$2^1 \times 11$
24	3	3	$2^3 \times 3$

Now, with $(n = 2^\ell k)$, then, under the given conditions, we know that (15) can be rewritten as:

$$x^{2^\ell k} + y^{2^\ell k} = z^{2^\ell k}, \tag{24}$$

and this can further be rewritten as:

$$\left(x^{2^{\ell-1}k}\right)^2+\left(y^{2^{\ell-1}k}\right)^2=\left(z^{2^{\ell-1}k}\right)^2, \tag{25}$$

where $(x^{2^{\ell-1}k}, y^{2^{\ell-1}k}, z^{2^{\ell-1}k})$ is a piecewise coprime triple and they constitute a primitive Pythagorean triple.

Now, as is well known from §(2), namely Euclid's formula for generating primitive Pythagorean triples, is 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 $(p-q)$ is odd, such that:

$$\begin{pmatrix} x^{2^{\ell-1}k} \\ y^{2^{\ell-1}k} \\ z^{2^{\ell-1}k} \end{pmatrix}=\begin{pmatrix} p^2-q^2 \\ 2pq \\ p^2+q^2 \end{pmatrix}. \tag{26}$$

From (26), we extract the x-component of this equation, *i.e.* $(x^{2^{\ell-1}k}=p^2+q^2)$, and we will write this equation as:

$$x^{2^{\ell-1}k}=p^2-q^2=(p+q)(p-q). \tag{27}$$

The numbers $(p+q)$ and $(p-q)$ are both odd and have no common factor greater than, unity, that is to say, they are coprime. Because of this, it follows that they must be such that:

$$\begin{pmatrix} p+q \\ p-q \end{pmatrix}=\begin{pmatrix} a^{2^{\ell-1}k} \\ b^{2^{\ell-1}k} \end{pmatrix}. \tag{28}$$

Notice that (a,b) are coprime and (a,b,p,q) are coprime as-well.

Now, by addition of these two numbers [*i.e.* $(p+q)$ and $(p-q)$] as defined in (28), it follows that:

$$2p=a^{2^{\ell-1}k}+b^{2^{\ell-1}k}. \tag{29}$$

Now, we need to go to the y-component of (26), that is, $(y^{2^{\ell-1}k}=2pq)$. We know that (p,q) are coprime and one of them is odd and the other is even. Let us chose that p is even and q is odd. It follows that the numbers $2p$ and q must have a $(2^{\ell-1}k)$-th root, that is to say, we must have $q=s^{2^{\ell-1}k}$ and $p=2^{2^{\ell-1}gk-1}r^{2^{\ell-1}k}$ where $[\{(r,s)>1 : g\geq 1\}\in\mathbb{Z}^+]$, so that $(y=2^g rs)$.

From this, is follows that $(2p=2^{2^{\ell-1}gk}r^{2^{\ell-1}k})$: thus, substituting this into (29), we will have:

$$2^{2^{\ell-1}gk}r^{2^{\ell-1}k}=a^{2^{\ell-1}k}+b^{2^{\ell-1}k}. \tag{30}$$

Notice that since the triple (a,b,p) is coprime, the triple $(2^{2^{\ell-1}gk}r^{2^{\ell-1}k}, a, b)$ is coprime as-well.
If $(\ell=1)$, we will have:

$$(2^g r)^k=a^k+b^k. \tag{31}$$

In (31) we have produced another solution $(2^g r, a, b)$, *i.e.*, the triple $(2^g r, a, b)$ is another solution to the original equation – *albeit*, smaller than the original solution. Applying the same procedure to $(2^g r, a, b)$ 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.

Now, if $(\ell>1)$, we will have:

$$\underbrace{\left(2^{2^{\ell-2}gk}r^{2^{\ell-2}k}\right)^2}_{\in\mathbb{E}^+}=\underbrace{\left(a^{2^{\ell-2}k}\right)^2}_{\in\mathbb{O}^+}+\underbrace{\left(b^{2^{\ell-2}k}\right)^2}_{\in\mathbb{O}^+}. \tag{32}$$

Notice that the triple $(2^{2^{\ell-2}gk}r^{2^{\ell-2}k}, a^{2^{\ell-2}k}, b^{2^{\ell-2}k})$ is not only coprime, it is a primitive Pythagorean triple. According to the corollary presented in §(2.1), the number $2^{2^{\ell-2}gk}r^{2^{\ell-2}k}$ ought to be an odd number and not an even number, while one of the two numbers $(a^{2^{\ell-2}k}, b^{2^{\ell-2}k})$ is odd and the other is even. Such primitive Pythagorean triple $(2^{2^{\ell-2}gk}r^{2^{\ell-2}k}, a^{2^{\ell-2}k}, b^{2^{\ell-2}k})$ satisfying (32), is impossible. We thus here arrive at our desired contradiction.

5.3 Summary of the Two Proofs

In §(5.2) and (5.1), we have proved that (15) admits no integer solutions for any $[(x,y,z)>1]$ and $[(x,y,z)\in\mathbb{Z}^+]$ 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 (15) admits no integer solutions for any $[(x,y,z)>1]$ and $[(x,y,z)\in\mathbb{Z}^+]$ for all powers of $[(n>2)\in\mathbb{Z}^+]$. Hence, *Fermat's Last Theorem* is here proved in a simpler, much more general and truly marvellous manner.

6 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 [9], 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.

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.

7 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. Dr. 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*).

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. Gambioli, D. [1901], 'Memoria Bibliographica Sull'ultimo Teorema di Fermat', *Period. Mat.* **16**, 145–192.
4. Grant, M. and Perella, M. [1999], 'Descending to the Irrational', *Mathematical Gazette* **83**, 263–267.
5. 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.
6. Kronecker, L. [1901], 'Vorlesungen Über Zahlentheorie', *Leipzig: Teubner* **I**, 33–38. Reprinted by New York: Springer-Verlag in 1978.
7. 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.
8. 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.
9. Nyambuya, G. G. [2014], 'A Simple and General Proof of Beal's Conjecture (I)', *Advances in Pure Mathematics* **4**(9), 1–4.
10. Wiles, A. [1995], 'Modular Elliptic Curves and Fermat's Last Theorem', *Annals of Mathematics* **141**(3), 443–551. doi:10.2307/2118559.