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

Golden Gadzirayi Nyambuya[*]
Department of Applied Physics, National University of Science and Technology, Bulawayo, Republic *of* Zimbabwe
Email: golden.nyambuya@nust.ac.zw

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 which make use of Pythagoras theorem, 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, Pythagoras theorem, Pythagorean triples.

"*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 ($\sim 201 - 215$ 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:

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

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.

[*] **Email for Correspondence:** physicist.ggn@gmail.com
[*] 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 [see *e.g.* 1] 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 [2].

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 [3]:

> *"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. Primitive Pythagorean Triples

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:

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

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:

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

* 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.

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, $\sqrt{b}$ is an irrational number.

—

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 $(c_1, d_1) \in \mathbb{N}^+$. The above stated *Lemma* 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*, we shall set-up a *Theorem* that is necessary for this proof.

4. Theorem

Theorem. For any piecewise coprime triple of integers each greater than unity *i.e.* $(x > 1; y > 1; z > 1) \in \mathbb{N}^+$ such that z is not a perfect square *i.e.* $\sqrt{z} \in \mathbb{I}^+$, the equation:

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

admits no solutions for $(n > 2) \in \mathbb{O}^+$.

Proof. As a starting point, let us assume that (6) has 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:

$$\left(z^k\sqrt{z}\right)^2 = x^2 + y^2. \tag{7}$$

From the decomposition method used in the method of obtaining Pythagorean triples, we know that we can always find some numbers (p, q) with are not necessarily integers such that:

$$\begin{pmatrix} x \\ y \\ z^k\sqrt{z} \end{pmatrix} = \begin{pmatrix} p^2 - q^2 \\ 2pq \\ p^2 + q^2 \end{pmatrix}. \tag{8}$$

Since $\sqrt{z} \in \mathbb{I}^+$, from the z-component of (8) *i.e.* $z^k\sqrt{z} = p^2 + q^2$, we know from *Lemma* §(3.) that there must exist some integer numbers (a, b) such that $p^2 = a\sqrt{z}$ and $q^2 = b\sqrt{z}$ and this implies $p = \sqrt{a\sqrt{z}}$ and $q = \sqrt{b\sqrt{z}}$. Substituting this into (8), we will have:

$$\begin{pmatrix} x \\ y \\ z^k\sqrt{z} \end{pmatrix} = \begin{pmatrix} (a - b)\sqrt{z} \\ 2\sqrt{a}\sqrt{b}\sqrt{z} \\ (a + b)\sqrt{z} \end{pmatrix}. \tag{9}$$

The x-component of (9) is telling us that the rational number x; actually, the integer number x must equal the irrational number $(a - b)\sqrt{z}$ since $x = (a - b)\sqrt{z}$. We know very well that this is an impossibility, hence, by way of contradiction, we conclude that our supposition that this equation has a solution is wrong, hence the initial statement is true.

5. Proof of Fermat's Last Theorem

The proof that we are going to provide is a proof by contradiction. We assume that the statement:

$$\exists\ (x, y, z, n) \in \mathbb{N}^+ :\ \ x^n + y^n = z^n,\ \ \text{for}\ \ (n > 2), \tag{10}$$

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.*:

1. **Case (I) :** This case proves for all powers of $(n > 2) \in \mathbb{E}^+$ where $\mathbb{E}^+$ is the set of all positive even integer numbers.
2. **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 (10) 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).

5.1. Proofs for the Cases $(\mathbf{n = 3, 4\,\&\,5})$

As is well known, the case for $(n = 3)$, for all non-zero (x, y, z) and $(x, y, z) \in \mathbb{N}^{+}$, the equation $x^3 + y^3 = z^3$ admits no solutions. This was first proved by the great Italian mathematician Leonhard Euler in 1770 [4], that is, 133 years after Fermat set into motion Fermat's Last Theorem. Euler used the technique of *infinite descent*. Euler's proof is not the only proof possible as other authors have published their independent proofs [see *e.g.* Refs. 5, 6, 7, 8, 9, amongst many others].

Fermat was the first to provide a proof for the case $(n = 4)$ which stated that for all non-zero piecewise coprime triple $(x, y, z) \in \mathbb{N}^{+}$, 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. 6, 7, 10, 11, 12, amongst many others]. Even after Sir Professor Andrew Wiles's 1995 breakthrough [2], researchers are still publishing variants of the proof for the case $(n = 4)$ [see *e.g.* 13, 14, 15].

The case $(n = 5)$ was first proved independently by the French mathematician Adrien-Marie Legendre (1752 -1833) and the German mathematician Johann Peter Gustav Lejeune Dirichlet (1805 - 1859) around 1825 and alternative and independent proofs were developed in the later years by others [see *e.g.* Refs. 6, 16, 17, 18, 19, 20, 21, 22, 23, amongst many others].

5.2. Case (I): Even Powers of $(\mathbf{n > 2})$

If $(n > 2) \in \mathbb{E}^{+}$, then we can write $n = 2^{\ell}k$ where $(\ell = 2, 3, 4, \ldots\ etc)$ and $(k = 1, 3, 5, 7, \ldots\ etc)$. In the event that $(k = 1)$, then (10) becomes $x^{2^{\ell}} + y^{2^{\ell}} = z^{2^{\ell}}$, and this can be rewritten as:

$$\left(x^{2^{\ell-2}}\right)^4 + \left(y^{2^{\ell-2}}\right)^4 = \left(z^{2^{\ell-2}}\right)^4, \tag{11}$$

where $(\ell - 2 \geq 0)$. We know from Fermat's proof for the case $(n = 4)$ and the other subsequent proofs by others for $(n = 4)$ [see *e.g.* 13, 14, 15], that (11) admits no solution, therefore, we conclude from this that the case $(k = 1)$ admits no solution for the given conditions.

Now that we have demonstrated that the case $(k = 1)$ admits no solution, we proceed to demonstrate for the remainder of the cases which are $(k > 1)$ *i.e.* $k = 3, 5, 7, \ldots\ etc.$ With $n = 2^{\ell}k$ under the given conditions, we know that (10) can be written:

$$x^{2^{\ell}k} + y^{2^{\ell}k} = z^{2^{\ell}k}, \tag{12}$$

and this can be rewritten as:

$$\left(x^{2^{\ell-1}k}\right)^2 + \left(y^{2^{\ell-1}k}\right)^2 = \left(z^{2^{\ell-1}k}\right)^2, \tag{13}$$

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 membebrs 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 Pythagorean triple in the true sense of a Pythagorean triple.

As is well known from Euclid's formula for generating primitive Pythagorean triples that, if $(p_1, q_1) \geq 1$, are some integers that are such that $(p_1 > q_1)$ where p_1 and q_1 are coprime and $p_1 - q_1$ is odd with $p_1 \in \mathbb{E}^{+}$ and $q_1 \in \mathbb{O}^{+}$, the triple $(x^{2^{\ell-1}k}, y^{2^{\ell-1}k}, z^{2^{\ell-1}k})$ is such that:

$$\begin{pmatrix} x^{2^{\ell-1}k} \\ y^{2^{\ell-1}k} \\ z^{2^{\ell-1}k} \end{pmatrix} = \begin{pmatrix} p_1^2 - q_1^2 \\ 2p_1q_1 \\ p_1^2 + q_1^2 \end{pmatrix}. \tag{14}$$

From (14), 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:

$$(z^{2^{\ell-2}k})^2 = p_1^2 + q_1^2. \tag{15}$$

Now, as long as $(\ell - 2 > 0)$, the triple $(p_1, q_1, z^{2^{\ell-2}k})$ is a set comprised of piecewise coprime positive integers thus, this triple $(p_1, q_1, z^{2^{\ell-2}k})$ is a Pythagorean triple in the true sense of a Pythagorean triple.

As before, we known from Euclid's formula for generating primitive Pythagorean triples that, if $(p_2, q_2) \geq 1$, are some integers that are such that $(p_2 > q_2)$ where p_2 and q_2 are coprime and $p_2 - q_2$ is odd with $p_2 \in \mathbb{E}^{+}$ and $q_2 \in \mathbb{O}^{+}$, the triple$(p_1, q_1, z^{2^{\ell-2}k})$ is such that:

$$\begin{pmatrix} p_1 \\ q_1 \\ z^{2^{\ell-2}k} \end{pmatrix} = \begin{pmatrix} p_2^2 - q_2^2 \\ 2p_2q_2 \\ p_2^2 + q_2^2 \end{pmatrix}. \tag{16}$$

Notice that $(p_1 > p_2)$ and $(q_1 > q_2)$.

Now, from the z-component of (16), that is to say $z^{2^{\ell-2}k} = p_2^2 + q_2^2$, we can rewrite this as:

$$(z^{2^{\ell-3}k})^2 = p_2^2 + q_2^2. \tag{17}$$

As before, we know that for as long as $(\ell - 3 > 0)$, the triple $(p_2, q_2, z^{2^{\ell-3}k})$ is a set comprised of piecewise coprime positive integers thus, this triple is a Pythagorean triple in the true sense of a Pythagorean triple.

Again, we known from Euclid's formula for generating primitive Pythagorean triples that, if $(p_3, q_3) \geq 1$, are some integers that are such that $(p_3 > q_3)$ where p_3 and q_3 are coprime and $(p_3 - q_3)$ is odd with $(p_3 \in \mathbb{E}^+)$ and $(q_3 \in \mathbb{O}^+)$, the triple $(p_2, q_2, z^{2^{\ell-3}k})$ is such that:

$$\begin{pmatrix} p_2 \\ q_2 \\ z^{2^{\ell-3}k} \end{pmatrix} = \begin{pmatrix} p_3^2 - q_3^2 \\ 2p_3q_3 \\ p_3^2 + q_3^2 \end{pmatrix}. \tag{18}$$

Again, notice that $(p_1 > p_2 > p_3)$ and $(q_1 > q_2 > q_3)$. If $(\ell - 3 > 0)$, then, as before, we shall have to take the z-component of (18) and go over this same process as happened when $(\ell - 2 > 0)$ and $(\ell - 1 > 0)$. This same process will go on and going up until the ℓ^{th}-time where we will have:

$$\begin{pmatrix} p_{\ell-1} \\ q_{\ell-1} \\ z^k \end{pmatrix} = \begin{pmatrix} p_\ell^2 - q_\ell^2 \\ 2p_\ell q_\ell \\ p_\ell^2 + q_\ell^2 \end{pmatrix}, \tag{19}$$

where $(p_\ell, q_\ell) \geq 1$, are some integers that are such that $(p_\ell > q_\ell)$ where p_ℓ and q_ℓ are coprime and $p_\ell - q_\ell$ is odd with $p_\ell \in \mathbb{E}^+$ and $q_\ell \in \mathbb{O}^+$ and the triple (p_ℓ, q_ℓ, z^k) is coprime.

Just as before, we have to take the z-component of (19) *i.e.*:

$$z^k = p_\ell^2 + q_\ell^2. \tag{20}$$

Having done this, we must realise that (1) $k \in \mathbb{O}^+$, (2) the triple $(p_\ell > 1; q_\ell > 1; z > 1)$ is a triple comprised of piecewise coprime integers, (3) there can only be two scenarios for the integer z is these scenarios:

1. **Scenario (I):** We have that $(\sqrt{z} \in \mathbb{I}^+)$.
2. **Scenario (II):** We have that $(\sqrt{z} \in \mathbb{N}^+)$.

We shall tackle these two scenarios below.

Scenario (I)

If $\sqrt{z} \in \mathbb{I}^+$, and given that (p_ℓ, q_ℓ, z^k) are piecewise coprime integers greater than unity and that $(k > 2) \in \mathbb{O}^+$, it follows from *Theorem* §(4.) that there will be no solution for this case where $\sqrt{z} \in \mathbb{I}^+$.

Scenario (II)

In this scenario we have $\sqrt{z} \in \mathbb{N}^+$. Since $\sqrt{z} \in \mathbb{N}^+$, it therefore follows that z is a perfect square. Since z is perfect square, clearly we can in general write $z = w^{2^\ell}$ where $(w > 1; \ell > 0) \in \mathbb{N}^+$ and $\sqrt{w} \in \mathbb{I}^+$. Substituting $z = w^{2^\ell}$ into (20), we will have:

$$w^{2^\ell k} = p_\ell^2 + q_\ell^2. \tag{21}$$

Let us rewrite the above equation (21) as:

$$\left(w^{2^{\ell-1}k}\right)^2 = p_\ell^2 + q_\ell^2. \tag{22}$$

We know that the triple $(p_\ell, q_\ell, w^{2^{\ell-1}k})$, is a piecewise coprime triple of integers greater than unity – this triple is a Pythagorean triple. Therefore, from the method Pythagorean triples, we know that there exists coprime integers $(r, s) > 1$ such that $(r > s)$ and $r - s \in \mathbb{O}^+$ with $r \in \mathbb{E}^+$ and $s \in \mathbb{O}^+$ such that:

$$\begin{pmatrix} p_\ell \\ q_\ell \\ w^{2^{\ell-1}k} \end{pmatrix} = \begin{pmatrix} r^2 - s^2 \\ 2rs \\ r^2 + s^2 \end{pmatrix}. \tag{23}$$

From this equation (23), we take the w-component *i.e.* $w^{2^{\ell-1}k} = r^2 + s^2$ and we rewrite this as:

$$\left(w^{2^{(\ell-2)}k}\right)^2 = r^2 + s^2. \tag{24}$$

We should take note of the fact that the triple $(r, s, w^{2^{(\ell-2)}k})$ is a piecewise coprime prime triple of integers all greater than unity – this triple is a Pythagorean triple.

Having written down this equation (24), according to the method of generating Pythagorean triples, we know that there must exist some coprime integer numbers $(r_1 > 1\,,\, s_1 > 1) : r_1 > s_1 : r_1 - s_1 \in \mathbb{O}^+$, and these numbers (r_1, s_1) are such that:

$$\begin{pmatrix} r \\ s \\ w^{2^{(\ell-2)}k} \end{pmatrix} = \begin{pmatrix} r_1^2 - s_1^2 \\ 2r_1s_1 \\ r_1^2 + s_1^2 \end{pmatrix}. \tag{25}$$

As before, let us take the w-component of (25), which is $w^{2^{(\ell-2)}k} = r_1^2 + s_1^2$, and realise that this equation can be rewritten as:

$$\left(w^{2^{(\ell-3)}k}\right)^2 = r_1^2 + s_1^2. \tag{26}$$

It should be noted that the triple $(r_1, s_1, w^{2^{(\ell-3)}k})$ is a piecewise coprime triple of integers greater than unity – this triple is a Pythagorean triple.

We begin the process again. According to the method of generating Pythagorean triples, we know that there must exist some coprime integer numbers $(r_2 > 1\,,\, s_2 > 1) : r_2 > s_2 : r_2 - s_2 \in \mathbb{O}^+$, and these numbers (r_2, s_2) are such that:

$$\begin{pmatrix} r_1 \\ s_1 \\ w^{2^{(\ell-3)}k} \end{pmatrix} = \begin{pmatrix} r_2^2 - s_2^2 \\ 2r_2s_2 \\ r_2^2 + s_2^2 \end{pmatrix}. \tag{27}$$

As before, let us take the w-component of (27), which is $w^{2^{(\ell-3)}k} = r_2^2 + s_2^2$, and realise that this equation can be rewritten as:

$$\left(w^{2^{(\ell-4)}k}\right)^2 = r_2^2 + s_2^2. \tag{28}$$

Again, it should be noted that the triple $(r_2, s_2, w^{2^{(\ell-4)}k})$ is a piecewise coprime triple of integers greater than unity, actually, this triple is a Pythagorean triple thus according to the method of generating Pythagorean triples, we know that there must exist some coprime integer numbers

$(r_3 > 1, s_3 > 1) : r_3 > s_3 : r_3 - s_3 \in \mathbb{O}^+$, and these numbers (r_3, s_3) are such that:

$$\begin{pmatrix} r_2 \\ s_2 \\ w^{2^{(\ell-4)}k} \end{pmatrix} = \begin{pmatrix} r_3^2 - s_3^2 \\ 2r_3 s_3 \\ r_3^2 + s_3^2 \end{pmatrix}. \tag{29}$$

At this point, one thing must be clear to the reader and this is the fact that this process can not go on forever – it can only go on ℓ^{th} times before we arrive at:

$$\begin{pmatrix} r_{\ell-2} \\ s_{\ell-2} \\ w^k \end{pmatrix} = \begin{pmatrix} r_{\ell-1}^2 - s_{\ell-1}^2 \\ 2r_{\ell-1} s_{\ell-1} \\ r_{\ell-1}^2 + s_{\ell-1}^2 \end{pmatrix}, \tag{30}$$

where the integer numbers $(r_{\ell-1}, s_{\ell-1})$ are such that $(r_{\ell-1} > 1, s_{\ell-1} > 1)$, $(r_{\ell-1} > s_{\ell-1})$ and $r_{\ell-1} - s_{\ell-1} \in \mathbb{O}^+$. The w-component of (30) now reads:

$$w^k = r_{\ell-1}^2 + s_{\ell-1}^2. \tag{31}$$

Since $\sqrt{w} \in \mathbb{I}^+$ and $k \in \mathbb{O}^+$ it follows from *Theorem* §(4.) that there is no solution to (31). We here have arrived a contradiction. Therefore, by way of contradiction, we conclude that under these conditions, the statement (10) can not be true as initially supposed.

Summary

From the foregoing, we clearly have demonstrated that for $(n > 2) \in \mathbb{E}^+$ the statement (10) can not be true as initially supposed, hence Fermat's Last Theorem is true for $(n > 2) \in \mathbb{E}^+$.

5.3. Case (II): Odd Powers of $(\mathbf{n} > \mathbf{2})$

Now, we have to prove for the case were $(n > 2) \in \mathbb{O}^+$. 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:

$$\left(x^k\sqrt{x}\right)^2 + \left(y^k\sqrt{y}\right)^2 = \left(z^k\sqrt{z}\right)^2. \tag{32}$$

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:

$$\begin{pmatrix} x^k\sqrt{x} \\ y^k\sqrt{y} \\ z^k\sqrt{z} \end{pmatrix} = \begin{pmatrix} p^2 - q^2 \\ 2pq \\ p^2 + q^2 \end{pmatrix}. \tag{33}$$

As in the case for the proof for even powers of $(n > 2)$, our focal point here is the z-component of (33). 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.

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

If $\sqrt{z} = w \in \mathbb{N}^+$, clearly $(p, q) \in \mathbb{N}^+$. 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 (32) will now become:

$$u^{2(2k+1)} + v^{2(2k+1)} = w^{2(2k+1)}. \tag{34}$$

According to the proof we have given in §(5.2.) for even n *i.e.* for $(n > 2) \in \mathbb{E}^+$, it follows that (34) admits no solutions.

Case (2): Proof for the Case $\sqrt{\mathbf{z}} \notin \mathbb{I}^+$

In the case where $\sqrt{z} \notin \mathbb{I}^+$, it follows from *Lemma* §(3.) that for the z-component of (33), there must exist some $(a, b : a > b) \in \mathbb{N}^+$, 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 (33), we will have:

$$\begin{pmatrix} x^k\sqrt{x} \\ y^k\sqrt{y} \\ z^k\sqrt{z} \end{pmatrix} = \begin{pmatrix} (a-b)\sqrt{z} \\ 2\sqrt{a}\sqrt{b}\sqrt{z} \\ (a+b)\sqrt{z} \end{pmatrix}. \tag{35}$$

Clearly, from (35), it follows that $\sqrt{x} \notin \mathbb{N}^+$. In the wisdom of the fact that $(\sqrt{x}, \sqrt{z}) \notin \mathbb{N}^+$, what does equation (35) as a whole mean?

Well, we know that $x^k \in \mathbb{N}^+$ but (35) is telling us that $x^k = (a - b)\sqrt{z/x}$. Since $(a - b) \in \mathbb{N}^+$, for $x^k = (a-b)\sqrt{z/x} \in \mathbb{N}^+$, $\sqrt{z/x} = s \in \mathbb{N}^+$ *i.e.* $z = s^2 x$. This means that x and z share a common factor s^2, 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 $(x, y, z) \in \mathbb{N}^+$ (10) admits no solutions under the given conditions since the piecewise coprime triple (x, y, z) can not be piecewise coprime as initially assumed.

Summary

Combining the two proofs for the case $(n > 2) \in \mathbb{O}^+$ for $\sqrt{z} \in \mathbb{N}^+$ and $\sqrt{z} \in \mathbb{I}^+$, it follows that, equation (10) admits no integer solutions for any non-zero piecewise coprime triple $(x, y, z) \in \mathbb{N}^+$.

5.4. Summary of the Two Proofs

In §(5.2.) and (5.3.), we have proved that (10) admits no integer solutions for any $(x, y, z) > 0$ 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 (10) admits no integer solutions for any $(x, y, z) > 0$ 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.

6. 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. In the readings [24, 25], we have provided 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 judge our proof, effort and work, we must — if this be permitted at this point of closing, say that, we are confident that – simple as it is or may appear, this proof is flawless, it will stand the test of time and experience. It strongly appears that the great physicist and philosopher – Albeit Einstein $(1879 - 1955)$, was probably right in saying that "*Subtle is the Lord. Malicious He is not.*" because in *Lemma* §(3.), there exists deeply embedded therein, a subtlety that resolves and does away with the malice and notoriety associated with Fermat's Last Theorem in a simpler and truly marvellous and general manner.

Conclusion

We hereby make 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.

REFERENCES

[1] D. A. Cox. Introduction to fermat's last theorem. pages 1–12, 1994.

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

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

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

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

[6] D. Gambioli. Memoria bibliographica sull'ultimo teorema di fermat. *Period. Mat.*, 16:145–192, 1901.

[7] 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.

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

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

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

[11] 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.

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

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

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

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

[16] 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).

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

[18] 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.

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

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

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

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

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

[24] G. G. Nyambuya. On a simpler, much more general and truly marvellous proof of fermat's last theorem. *Advances in Pure Mathematics*, pages 1–5, May 2014. In Press.

[25] G. G. Nyambuya. A simple and general proof of beal's conjecture. *Advances in Pure Mathematics*, pages 1–5, May 2014. In Press.