World Academy of Science, Engineering and Technology
International Journal of Mathematical and Computational Sciences
Vol:7, No:10, 2013

Fermat's Last Theorem a Simple Demonstration

Jose William Porras Ferreira

Abstract**—**This paper presents two solutions to the Fermat's Last Theorem (FLT). The first one using some algebraic basis related to the Pythagorean theorem, expression of equations, an analysis of their behavior, when compared with power $n = 2$ and power $n > 2$ and using " the "Well Ordering Principle" of natural numbers it is demonstrated that in Fermat equation $z \notin \mathbb{Z}^+ - \{0\}$. The second one solution is using the connection between $n!$ and $n$power through the Pascal's triangle or Newton's binomial coefficients, where de Fermat equation do not fulfill the first coefficient, then it is impossible that:

$$z^n = x^n + y^n \text{for} n > 2 \text{ and } (x, y, z) \in \mathbb{Z}^+ - \{0\}.$$

Keywords**—**Fermat's Last Theorem, Pythagorean Theorem, Newton Binomial Coefficients, Pascal's Triangle, Well Ordering Principle.

I. Introduction

THIS document serves the matter with regard to Pierre de Fermat: Would be certain his claim that he had a "wonderful demonstration" of Fermat's Last Theorem in 1637? [3]:

"*Cubumautem in duos cubos, autquadrato quadratum in duos quadrate quadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est divider cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.*" Pierre de Fermat [3]

"*It is impossible to decompose a cube into two cubes, a biquadratic in two biquadrate, and in general any power other than the square, two powers of the exponent. I found a really wonderful demonstration, but the margin of the book is too small to put it.*" Pierre de Fermat [3].

Wiles (1995) demonstration uses elliptic curves, schemes of groups, Hecks' Algebra, Iwasawa theory, Von Neumann-Bernays-Gödel' theory, Zermelo-Fraenkel' theory and others complex mathematical tools, all developed many years after Fermat's lived [7]. This document shows a short, simple demonstration using procedures known in the 17th century.

II. Fermat's Last Theorem

Fermat's last theorem or Fermat-Wiles's theorem is one of the most famous theorems in the history of mathematics [3] and [6]. The search for a demonstration spurred the development of algebraic number theory in the nineteenth century and the proof of the theorem of modularity in the twentieth century. Using modern notation, Fermat's last theorem can be stated as follows:

If n is an integer greater than 2, then you cannot find three natural numbers *x*, *y* and *z* such equality is met $(x, y) > 0$ in:

$$x^n + y^n = z^n$$

Pierre de Fermat (1667), showed the case of *n*=4, using the infinite descent technique [5]; Leonard Euler (1735), demonstrated the n=3 case confirmed in 1770 [8]. Later Germain stated that if *p* and 2*p*+1 are both primes, then the expression for the power Fermat conjecture *p* meant that one of the *x*, *y* or z would be divisible by *p* [8]. Germain tested for number *n*<100 and Legendre, extended their methods for *n*<197 [8]. In 1825, Dirichlet and Legendre, extended the case of n=3 to n=5. More recently, Lame (1839), proved the case of *n*=7 [8].

A. The Graph of Fermat's Equation

Fig. 1 shows a representation of Fermat's equation, built dividing the equation by z^n, transforming:

$$x^n + y^n = z^n$$

To the equation:

$$\xi^n + \beta^n = 1,$$

where:

$$\xi = \frac{x}{z} \text{and } \beta = \frac{y}{z}$$

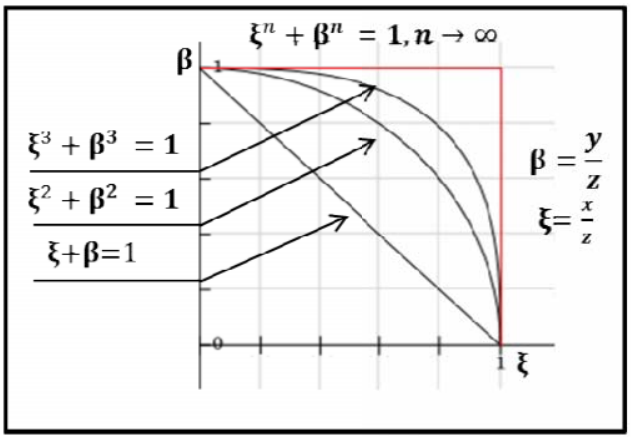

Fig. 1 Graphical representation of Fermat's equation

Three equations can be extracted from this graph:

1. The equation of the straight line $\xi + \beta = 1$, for $n = 1$
2. The equation of the circle $\xi^2 + \beta^2 = 1$, for $n = 2$
3. Fermat's Last Equation in the form $\xi^n + \beta^n = 1$, for $n > 2$

III. Pythagorean Triplets

A primitive Pythagorean is composed of three integers (*x*, *y*,

Jose William Porras Ferreira is with the Escuela Naval de Cadetes Colombia (e-mail: jwporras@balzola.org).

z) such that $x^2 + y^2 = z^2$. Although the Babylonians knew how to generate such triads in certain cases, the Pythagoreans extended the study of the topic finding results as: "*any odd integer is a member of a primitive Pythagorean triple*" [3]. However, the complete solution to this problem was not obtained until the 13th century when Fibonacci found a way to generate all possible Pythagorean triples [2].

There are different ways for generating primitive Pythagorean triples [1], [2] and [4], but we show another way of finding Pythagorean triples (*x, y, z*) below.

Applied to right triangles of sides and hypotenuse whole, Pythagorean theorem establishes that the following equation:

$$x^2 + y^2 = z^2 \quad (1)$$

It is satisfied by natural numbers $(x, y, z) > 0$

In (1), one of the two variables ($x$or y) must be larger than the other and they cannot be the same, because when they are the same would be $z^2 = 2x^2 = 2y^2$ and z would not be a natural number, (the square root of two is an irrational number with an infinite mantissa, which continues to be irrational by multiplying it by a natural number).

Assuming that ($x < y$) then z must be greater than y ($z > y$) to make equation (1) solution, i.e., $z > y > x$, and therefore, we can write:

$$z = y + m \quad \Rightarrow \quad m \in \mathbb{Z}^+ - \{0\} \quad (2)$$

where $x > m > 0$. If m equal to or greater than x, Equation (1), would have not solution with (2).

Fig. 2 shows a graphical representation of this equation.

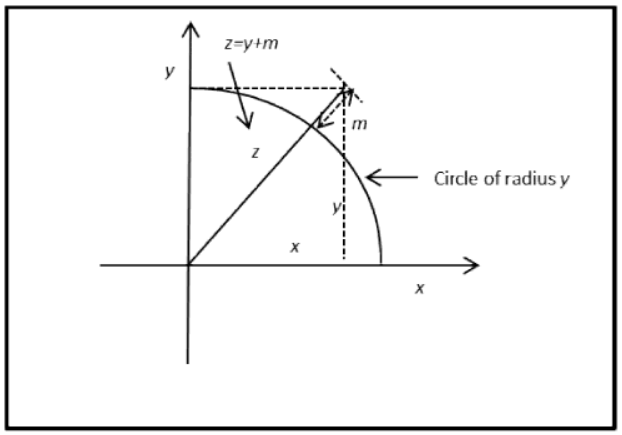

Fig. 2 Graphic representation of (2)

Theorem 1:

In (1) and (2) $m < x$

Proof:

1. $z > y > x$, $z = y + m \Rightarrow x^2 + y^2 = (y + m)^2 = z^2$, $(x, y, z, m) \in \mathbb{Z}^+ - \{0\}$
2. Suppose $m \geq x > 0 \Rightarrow m = x + u$, $u \geq 0$
3. $x^2 = 2ym + m^2$……..…….According to 1.
4. $x^2 = 2y(x+u) + (x+u)^2$… substituting into 3., *m* for $x + u$ ……..……..……..…According to 3.
5. $x^2 = 2yx + 2yu + x^2 + 2xu + u^2$……According to 4.
6. $0 = 2yx + 2yu + 2xu + u^2$……..…According to 5.
7. $2yx = -2yu - 2xu - u^2$ and this is an absurd (a positive number cannot be equal to a negative or 0 when $u \geq 0$).
8. Therefore, assumption 2 is incorrect. ……. According to 7.
9. Therefore: $m < x$…..…….…...… According to 8.

Q.E.D[1].

In (2) according to the Good Ordering Principle, m must contain a minimum element within the natural numbers and to be of first grade it must be met for all $m > 0$, being their lowest element number 1. Additionally with $m > 0$, it is possible to find all Pythagorean triples, because z would be among the natural numbers, other values of $m \notin \mathbb{Z}^+ - \{0\}$, would also give $z \notin \mathbb{Z}^+ - \{0\}$.

Replacing (2) in (1) would be:

$$x^2 + y^2 = (y + m)^2 = y^2 + 2ym + m^2$$
$$(x^2 - m^2)/(2m) = y \quad (3)$$

Primitive Pythagorean triples of x, y and z with odd x, are found, replacing $m=1$ in (2) and (3), leaving:

$$z = y + 1 \quad (4)$$

$$\frac{x^2 - 1}{2} = y \quad (5)$$

Primitive Pythagorean triples of x, y and z with even x, are found, replacing $m=2$ in (2) and (3), leaving:

$$z = y + 2 \quad (6)$$

$$\frac{x^2 - 4}{4} = y \quad (7)$$

Equations (4)-(7) let us find primitive Pythagorean triples a, b and c, where a, b and c values correspond to the values found for x, y and z, respectively, with these equations and $(a, b, c) \in Z^+$.

Larger bases x, y and z as Pythagorean triples are calculated using (8), with $k>1$, $k \in \mathbb{Z}^+$ and a, b and c are primitive Pythagorean triples. With odd a, $m = k$ and with even a, $m = 2k$:

$$(ak)^2 + (bk)^2 = (ck)^2 = z^2 \quad (8)$$

Tables I and II, shows examples of the above:

[1]From latín - ***Quod erat demonstrandum***

TABLE I
PRIMITIVE PYTHAGOREAN TRIPLES AND LARGER BASES WITH ODD $x = a$

Primitive Pythagorean triples odd $xk=1$ ($m=1$ (4) and (5))									
x	*a*=3	*a*=5	*a*=7	*a*=9	*a*=11	*a*=13	*a*=15	*a*=17	*a*=19
y	*b*=4	*b*=12	*b*=24	*b*=40	*b*=60	*b*=84	*b*=112	*b*=144	*b*=180
z	*c*=5	*c*=13	*c*=25	*c*=41	*c*=61	*c*=85	*c*=113	*c*=145	*c*=181
Larger Pythagorean triples: (8) *k*=2 (*m*=2 (8)									
x	6	10	14	18	22	26	30	34	38
y	8	24	48	80	120	168	224	288	360
z	10	26	50	82	122	170	226	290	362
Larger Pythagorean triples: (8) *k*=3 (*m*=3 (8))									
x	9	15	21	27	33	39	45	51	57
y	12	36	72	120	180	252	336	432	540
z	15	39	75	123	183	255	339	435	543
Larger Pythagorean triples: (8) *k*=4 (*m*=4 (8))									
x	12	20	28	36	44	52	60	68	76
y	16	48	96	160	240	336	448	576	720
z	20	52	100	164	244	340	452	580	724

TABLE II
PRIMITIVE PYTHAGOREAN TRIPLES AND LARGER BASES WITH EVEN *X=A*

Primitive Pythagorean triples even *x*,*k*=1 (*m*=2 (6) and (7))										
x	*a*=6	*a*=8	*a*=10	*a*=12	*a*=14	*a*=16	*a*=18	*a*=20	*a*=22	***a*=24**
y	*b*=8	*b*=15	*b*=24	*b*=35	*b*=48	*b*=63	*b*=80	*b*=99	*b*=120	***b*=143**
z	*c*=10	*c*=17	*c*=26	*c*=37	*c*=50	*c*=65	*c*=82	*c*=101	*c*=122	***c*=145**
Larger Pythagorean triples: (8) *k*=2 (*m*=4 (8))										
x	12	16	20	**24**	28	32	36	40	44	48
y	16	30	48	**70**	96	126	160	198	240	286
z	20	34	52	**74**	100	130	164	202	244	290
Larger Pythagorean triples: (8) *k*=3 (*m*=6 (8))										
x	18	**24**	30	36	42	48	54	60	66	72
y	24	**45**	72	105	144	189	240	297	360	429
z	30	**51**	78	111	150	195	246	303	366	435
Larger Pythagorean triples: (8) *k*=4 (*m*=8 (8))										
x	**24**	32	40	48	56	64	72	80	88	96
y	**32**	60	96	140	192	252	320	396	480	572
z	**40**	68	104	148	200	260	328	404	488	580

This method is simple but very valuable. For example with *x*= 24, there are only four solutions of *x*<*y* with natural numbers so that *z* is a natural number and *y*=143, 70, 45, 32, and *z*=145, 74, 51, 40 respectively, all values obtained with (4)-(8), (see numbers highlighted in black in Table II), solutions with *m*=2, 4, 6, 8 all dividers of 24. Values *x*>*y* and *z* as a natural numbers are equivalent and give the same *z*, just as if it had been $z^2 = y^2 + x^2$ where $x > y$, for example *x*=24, *y*=18, *z*=30 is equivalent to *y*=24, *x*=18, *z*=30 but they have not been taken as solutions because $x > y$, ($x < y$ has been always considered). Although m=12 is a divisor of 24 and solves x=24, y=18, z=30 it also corresponds to a similar Pythagorean triple of x=18, y=24 and z=30 with m=6.

There are other primitive Pythagorean triples (shown in [1], [2] and [4]) which can also be obtained with *m*>2 (3) or with following equations:

$$x^2+y^2=z^2 \Rightarrow x=2uv,\ y=u^2-v^2,\ z=u^2+v^2,\ (\text{for these equations } m=2v^2) \quad (9)$$

where *u* and *v* are prime numbers together, one of them is even and the other odd.

Example with *m*=8 from (9):

$x=20,\ y=21,\ z-y=m=8=2v^2,\ v=2,\ u=20/4=5$ and $z = u^2 + v^2 = 5^2 + 2^2 = 29 = y + m = 21 + 8$

Table III gives some examples:

TABLE III
EXAMPLES OF PRIMITIVE PYTHAGOREAN TRIPLES WITH SEQUENCES OF PRIME NUMBERS, ONE OF THEM EVEN ACCORDING TO (9)

Primitive Pythagorean triples with sequence of prime numbers						
m=8	***v***=2, ***u***=7	***v***=2, ***u***=11	***v***=2, ***u***=13	***v***=2, ***u***=17	***v***=2, ***u***=19	***v***=2, ***u***=23
x	28	44	52	68	76	92
y	45	117	165	285	357	525
z	53	125	173	293	365	533
m=8	***v***=2, ***u***=29	***v***=2, ***u***=31	v=2, u=37	v=2, u=41	v=2, u=43	v=2, u=47
x	126	124	148	164	172	184
y	837	957	1365	1677	1845	2205
z	845	965	1373	1685	1853	2213

For cases where *u* and *v* are primes and both are odd, primitive Pythagorean triples can be obtained using the following equations:

$$x^2+y^2=z^2 \Rightarrow x=uv,\ y=\tfrac{1}{2}(u^2-v^2),\ z=\tfrac{1}{2}(u^2+v^2),\ (\text{for these equations } m=v^2) \quad (10)$$

For all numbers *x*, *y* that are not within Pythagorean triples, z is irrational with infinite mantissa. Its calculation comes from a root of 2, ($z = \sqrt[2]{x^2 + y^2}$), that means *m* from (2) is irrational with an infinite mantissa (x, y)> 0 and natural numbers. Therefore:

z(irrational with infinite mantissa)= y(natural number) $+m$
(the mantissa must be also infinite).

Another important analysis is that ξ and β remain constant both for primitive Pythagorean triples, as its projection in the

larger Pythagorean triples:

$$\xi = x/z = (xk)/(zk) = ak/ck = a/c$$
$$\beta = y/z = (yk)/(zk) = bk/ck = b/c$$

The importance of (2) and (3) is that any primitive Pythagorean triple can be found easily. By using the Good Ordering Principle of natural numbers, the minimum elements of (2) and (3) inside the set of natural numbers would be: $x = 3,\ y = 4,\ z = 5$ and $m = 1$. Additionally with (2) and (3) can be formed any right triangle sides $x = \sqrt{a}$ where $a \geq 3$ and odd number, $y \geq 1$ and $z \geq 2$ where $(x^2, y, z, m = 1) \in \mathbb{Z}^+ - \{0\}$ and $x \notin \mathbb{Z}^+ - \{0\}$. The resulting equation has the same form of (1), i.e. $z^2 = x^2 + y^2$, but here $z > x > y$ and $z = y + m = y + 1$. This is important, because it helps showing that Fermat's Last Theorem is true in a simple way.

IV. Solution for Fermat's Last Theorem

A. First Solution

A solution using $z=y+q$ to solve $z^n = x^n + y^n$, for $n>2$, similar to the procedure followed to find primitive Pythagorean triples, in the previous chapter, demonstrating that $z \notin \mathbb{Z}^+ - \{0\}$ is as follows:

Theorem 2

In equation $x^n + y^n = {z_n}^n$ *is always true that: (*z_n *for* $n = 2$*)>(*z_n *for n>2)*$\Rightarrow z_{n=2} \in \mathbb{Z}^+ - \{0\}$

Proof:

1. $x^n + y^n = {z_n}^n$ for $n>1$
2. Let's $\boldsymbol{z_2}$ the solution of ${z_2}^2 = x^2 + y^2$ for $n = 2$ and z_n the solution of ${z_n}^n = x^n + y^n n > 2$ and assuming that z_2 is solution of $z_n \Rightarrow (x^2, y^2) \in \mathbb{Z}^+ - \{0\}$
3. $z_2 \in \mathbb{Z}^+ - \{0\}$
4. ${z_n}^2 = x^2 + y^2 = {z_2}^2$…… According to 2.
5. $x^n + y^n = {z_2}^2 {z_n}^{n-2}$……..…According to 1, 2, 3 and 4.
6. $x^n + y^n = (x^2 + y^2){z_n}^{n-2}$ ……According to 4 and 5.
7. $x^{n-2}x^2 + y^{n-2}y^2 = {z_n}^{n-2}x^2 + {z_n}^{n-2}y^2$ According to 6.
8. $x^{n-2} < {z_n}^{n-2} < y^{n-2}$ ……..…… According to 7.
9. $x < z_n < y$……..…… According to 8.
10. ${z_n}^n = {z_2}^2 {z_n}^{n-2} < {z_2}^2 {z_2}^{n-2} = {z_2}^n$.. According to 9.
11. $z_2 > z_n$ ……....……..… According to 10.

Q.E.D.

Corollary one: In the equation:

$${z_n}^n = x^n + y^n \text{ for } n \geq 1$$
always: $z_{n=1} > z_{n=2} > z_{n=3} > z_{n=4} > z_{n=5} \ldots$
$$(z_{n=1}, z_{n=2}) \in \mathbb{Z}^+ - \{0\}$$

Corollary two: The theorem 2 also applies to equations ${z_2}^2 = x^2 + y^2$ where $(x^2,\ y^2,\ z^2) \in \mathbb{Z}^+ - \{0\}$ and (x or y or both) $\notin \mathbb{Z}^+ - \{0\}$, because $x^{n-2} < {z_n}^{n-2} < y^{n-2}$.

Theorem 3

$$z^n = x^n + y^n \Longrightarrow x, y > 0 \text{ and coprimes}, n > 2, (x, y, n) \in \mathbb{Z}^+ - \{0\},\ z \notin \mathbb{Z}^+ - \{0\}$$

Proof:

1. Assuming that equation $z^n = x^n + y^n$, has integer solutions, where $n > 2$, $(x, y, z) \in \mathbb{Z}^+ - \{0\}$ and (x, y) are coprimes.
2. Assuming one of the variables (x or y) is smaller than the other ($x < y$). It can not be the same because it leads to $z = \sqrt[n]{2}x$ therefore $z \neq \mathbb{Z}^+ - \{0\}$).
3. Then $x < y < z$……..…… According to 1 and 2.
4. If z has integer solutions we can do:
   $z = y + q$, where q must be an integer number, but $q < m$ (theorem 2)

$$z^n = x^n + y^n = (y + q)^n = y^n + p_1 + q^n$$
$$p_1 + q^n = x^n \qquad (11)$$

$$p_1 = \sum_{k=1}^{n-1} \binom{n}{k} y^{n-k} q^k \ \Rightarrow 1 \leq k \leq n-1$$
$$\text{and } \binom{n}{k} = \frac{n!}{k!(n-k)!}$$

From (11) it is clear that $q < x$ and we are assuming q is integer number.

5. From 3:

$$y = x + s \ \Rightarrow s \in \mathbb{Z}^+ - \{0\}$$
$$y^n = (x + s)^n = x^n + p_2 + s^n$$
$$p_2 = \sum_{k=1}^{n-1} \binom{n}{k} x^{n-k} s^k \ \Rightarrow 1 \leq k \leq n-1$$
$$\text{and } \binom{n}{k} = \frac{n!}{k!(n-k)!}$$
$$y^n - x^n = p_2 + s^n \qquad (12)$$

6. Looking (11) and (12), both have the same form because in (11) it has assumed that q is integer (only differ is in the name of variables), that means if $p_1 + q^n = x^n$ then:

$$p_2 + s^n = t^n = y^n - x^n$$
$$y^n = x^n + t^n \qquad (13)$$

7. Equation (13) has the same form of the Fermat's equation $z^n = y^n + x^n$ but with even lower values ($y < z$) which leaves us in the path of the infinite descent, (if there is a minimum integer, then with (13), would be another minor integer, which contradicts the well-ordering principle of the natural numbers, therefore $z \notin \mathbb{Z}^+ - \{0\}$ and also $t \notin \mathbb{Z}^+ - \{0\}$.
8. Applying Theorem 2 and the well-ordering principle of the natural numbers:

Starting with the original equation (Fig. 3):

$${z_n}^n = x^n + y^n \Rightarrow (x < y) \in \mathbb{Z}^+ - \{0\} n > 2$$
$${z_2}^2 = x^2 + y^2$$

$z_2 > z_n$ (theorem 2)

$z_n{}^2 = x_1{}^2 + y_1{}^2 \Rightarrow z_n = y + q$

$(x_1{}^2, y_1{}^2)$must be inside of $\mathbb{Z}^+ - \{0\}$ if not $z_n \notin z^+ - \{0\}$

$z_n{}^n = z_n{}^2 z_n{}^{n-2} = (x_1{}^2 + y_1{}^2) z_n{}^{n-2} \equiv z_n{}^n = x^n + y^n$

By the well-ordering principle of the natural numbers, z_n must have a minimuminteger solution, then it is necessary to look the minimum solution inside of:

$$z_n{}^2 = x_1{}^2 + y_1{}^2$$

There are four cases:

a. $(x_1, y_1) \notin \mathbb{Z}^+ - \{0\}but(x_1{}^2, y_1{}^2) \in \mathbb{Z}^+ - \{0\}$

The minimum solution for$x_1 < y_1$is:

$x_1 = \sqrt{2}$and$y_1 = \sqrt{3}$, then$z_n{}^2 = 5$, but $z_n \notin \mathbb{Z}^+ - \{0\}$ because $\sqrt{5}$ is irrational.

$x_1 = \sqrt{2}$and$y_1 = \sqrt{7}$ then $z_n{}^2 = 9$, $z_n = 3$ but $z_n{}^n = 3^2 \cdot 3^{n-2} \neq z_n{}^n = x^n + y^n$ with $x = [1,2]$ and $y = [2,3]$ then z_n for $z_n{}^n = x^n + y^n$ is irrational (don't have a minimum solution)

b. $x_1 \notin \mathbb{Z}^+ - \{0\}but(x_1{}^2, y_1, y_1{}^2) \in \mathbb{Z}^+ - \{0\}$

The minimum solution for$x_1 < y_1$is:

$x_1 = \sqrt{2}$and $y_1 = 3$, then$z_n{}^2 = 11$, but $z_n \notin \mathbb{Z}^+ - \{0\}$ because $\sqrt{11}$ is irrational.

$x_1 = \sqrt{2}$and$y_1 = 7$ then $z_n{}^2 = 9$, $z_n = 3$ but $z_n{}^n = 3^2 \cdot 3^{n-2} \neq z_n{}^n = x^n + y^n$ with $x = [1,2]$ and $y = [2,3]$ then z_n for $z_n{}^n = x^n + y^n$ is irrational (don't have a minimum solution)

c. $y_1 \notin \mathbb{Z}^+ - \{0\}but(x_1, x_1{}^2, y_1{}^2) \in \mathbb{Z}^+ - \{0\}$

The minimum solution for$x_1 < y_1$is:

$x_1 = 1$and $y_1 = \sqrt{2}$, then$z_n{}^2 = 3$, but $z_n \notin \mathbb{Z}^+ - \{0\}$ because $\sqrt{3}$ is irrational.

$x_1 = 2$and$y_1 = \sqrt{7}$ then $z_n{}^2 = 9$, $z_n = 3$ but $z_n{}^n = 3^2 \cdot 3^{n-2} \neq z_n{}^n = x^n + y^n$ with $x = [1,2]$ and $y = [2,3]$ then z_n for $z_n{}^n = x^n + y^n$ is irrational (don't have a minimum solution)

d. $(x_1, y_1) \in \mathbb{Z}^+ - \{0\}$then$(x_1{}^2, y_1{}^2) \in \mathbb{Z}^+ - \{0\}$

The minimum solution for$x_1 < y_1$is:

$x_1 = 3$and$y_1 = 4$, then$z_n{}^2 = 25$, and$z_n = 5$, but:

$z_n{}^n = 5 \cdot 5^{n-2} \neq z_n{}^n = x^n + y^n$with$x = [1,2,3]$ and $y = [2,3,4]$ then z_n for $z_n{}^n = x^n + y^n$ is irrational (don't have a minimum solution)

That means the Fermat's equation $z_n{}^n = x^n + y^n$ must not have minimum solution where $(x_1{}^2 + y_1{}^2) \in \mathbb{Z}^+ - \{0\}$

9. Therefore it assumed in 1 is false and Fermat's Last Theorem is demonstrated, because $z \notin \mathbb{Z}^+ - \{0\}$

Q.E.D.

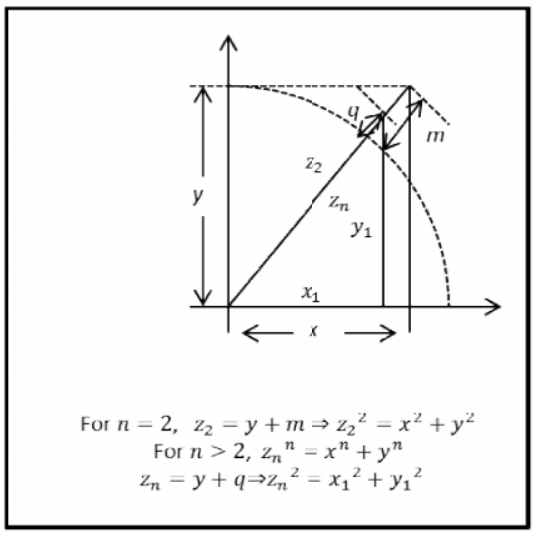

Fig. 3 Graphic representation of Fermat's equation $z_n{}^n = x^n + y^n$, $(x, y) \in \mathbb{Z}^+ - \{0\}, x > y,\ n > 2$

The following graph shows a comparison between the Pythagorean equation $z_2{}^2 = x^2 + y^2 = (y + m)^2$ and Fermat's equation $z^n = x^n + y^n = (y + q)^n$ for $n > 2$.

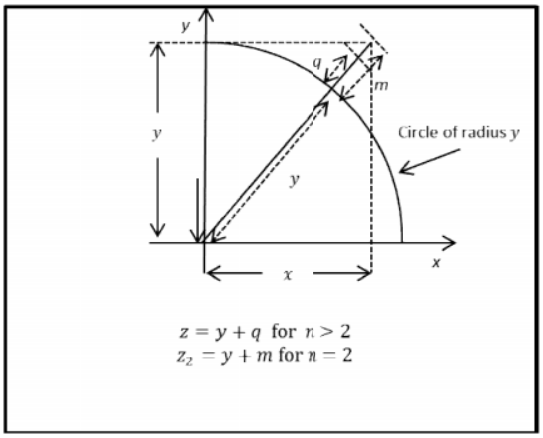

Fig. 4 Graphic where $z = y + q$ and $z_2 = y + m$ with $z_2{}^2 = (y + m)^2 = x^2 + y^2$ and $z^n = (y + q)^n = x^n + y^n$ for n>2

Fermat's Last Triangle

Fermat´s Last Theorem can be showed as a triangle of sides $(x, y, z = y + q)$, when joining the straight lines x, y and $z = y + q$, and where $60^0 < \Omega < 90^0$ (Ω is the angle opposited to side $z = y + q$). This triangle, has been named as Fermat's Last Triangle in his honor. A graphic representation is shown in Figure 5. Here $z^2 = x^2 + y^2 - 2xy\cos\Omega$. Only z could be a natural number when $\Omega = 90^0$ and (x, y) belong to a Pythagorean triples, condition that never fullfills $z = \sqrt[n]{x^n + y^n}$, because $z < z_2$.

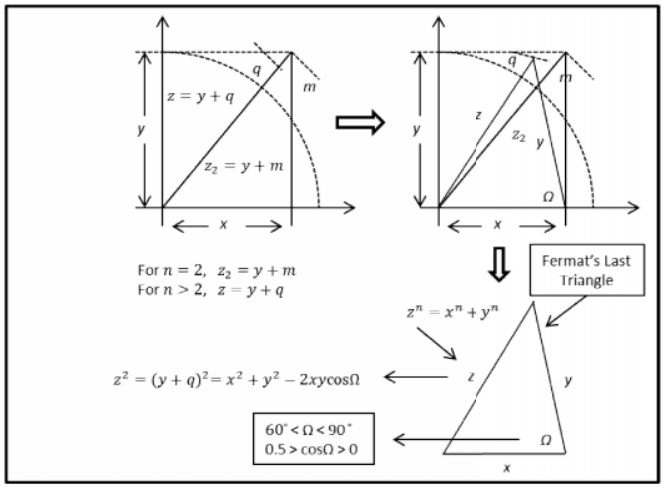

Fig. 5 Graphic representation of Fermat's Last Triangle

The Fermat's Last Triangle is part of Scalene Triangles. See Fig. 6.

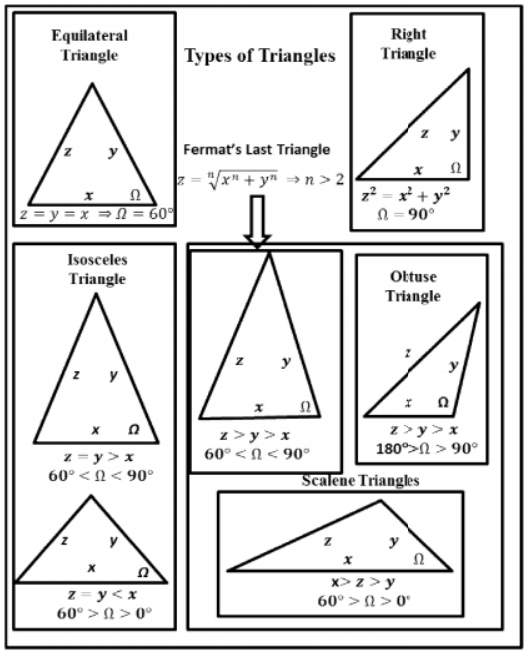

Fig. 6 Types of Triangles

Verification of Theorem 3 inside of Fermat's Last Triangle

In Fig. 7, there are the following three triangles:

1. Fermat's Last Triangle sides x, y, $z = \sqrt[n]{x^n + y^n} \Rightarrow n > 2$
2. Right Triangle with sides $x_a, y_a, z = \sqrt[n]{x^n + y^n} \Rightarrow z > y_a > x_a$
3. Right Triangle with sides $x_b, y_a, y \Rightarrow y > y_a > x_b$

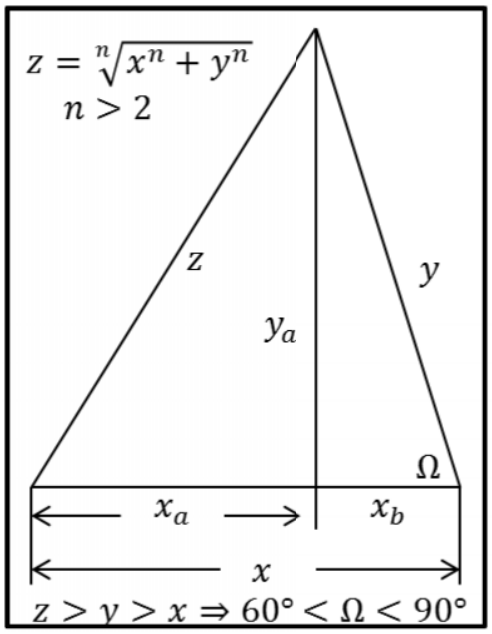

Fig. 7 Graphic representation of Fermat's Last Triangle to verify the theorem 3

Analyzing the two right triangles that form the Fermat´s Last Triangle it is possible to demonstrate that:

$z \notin \mathbb{Z}^+ - \{0\} \Rightarrow z > y > x$ with $(x, y) \in z^+ - \{0\}$ and coprimes.

Proof:

1. Assuming $(z,\ x_a,\ x_b,\ y_a) \in \mathbb{Z}^+ - \{0\}$:

$$z^2 = {x_a}^2 + {y_a}^2 \text{ and } y^2 = {x_b}^2 + {y_a}^2$$
$$z^2 + y^2 = {x_a}^2 + {y_b}^2 + 2{y_a}^2$$
$$x = x_a + x_b \Rightarrow x^2 = {x_a}^2 + {x_b}^2 + 2x_a x_b$$
$$z^2 + y^2 = x^2 - 2x_a x_b + 2{y_a}^2$$
$$x^2 = z^2 + y^2 + 2(x_a x_b - {y_a}^2)$$

This equation to have an integer solution, x must be: $x > z > y$, but it is not the Fermat's Last Triangle, then $z \notin \mathbb{Z}^+ - \{0\}$.

Examples are given in Table IV and Fig. 7.

TABLE IV
EXAMPLES FOR EQUATION:
$x^2 = z^2 + y^2 + 2(x_a x_b - y_a)$

y_a	24		
x_b	32	32	32
y	40	40	40
x_a	45	70	143
z	51	74	145
x	77	102	175

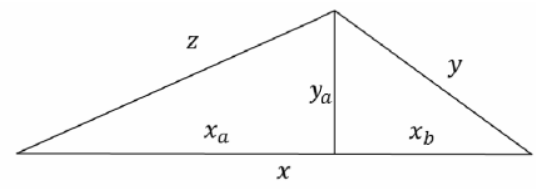

Fig. 8 The Triangles formed with $x^2 = z^2 + y^2 + 2(x_a x_b - y_a)$ and $(x, y, z, x_a, x_b, y_a) \in \mathbb{Z}^+ - \{0\}$

2. Assuming (z, x_a, x_b) $\in \mathbb{Z}^+ - \{0\}$ and $y_a \notin \mathbb{Z}^+ - \{0\}$ (irrational number)but${y_a}^2 \in \mathbb{Z}^+ - \{0\}$.
   $z^2 = {x_a}^2 + {y_a}^2$ *and* $y^2 = {x_b}^2 + {y_a}^2$. There is only one integer solution with ${y_a}^2$ at the same time($y = z$) and correspond to Isosceles Triangles (Fig. 5). Other solution$z \notin \mathbb{Z}^+ - \{0\}$.
3. Assuming ($z \in \mathbb{Z}^+ - \{0\}$, $(x_b, y_a) \notin \mathbb{Z}^+ - \{0\}$ (irrational numbers), but $({x_b}^2, {y_a}^2) \in \mathbb{Z}^+ - \{0\}$Then:
$$y^2 = {x_b}^2 + {y_a}^2$$
$$x_a = x - x_b$$
$${x_a}^2 = x^2 - 2x \cdot x_b + {x_b}^2 \Rightarrow {x_a}^2 \notin \mathbb{Z}^+ - \{0\}$$
$$z^2 = {x_a}^2 + {y_a}^2 \Rightarrow z \notin \mathbb{Z}^+ - \{0\}$$
4. Assuming ($z \in \mathbb{Z}^+ - \{0\}$, $(x_a, x_b) \notin \mathbb{Z}^+ - \{0\}$ (rational numbers):
$$x = \frac{d+e}{c} = \frac{d}{c} + \frac{e}{c} = x_a + x_b \Rightarrow x_a = \frac{d}{c} \text{and} x_b = \frac{e}{c}$$
$y^2 = {x_b}^2 + {y_a}^2 = \left(\frac{e}{c}\right)^2 + {y_a}^2 \Rightarrow y_a = \frac{f}{c}$to have integer solution then:
$$y^2 = \left(\frac{e}{c}\right)^2 + \left(\frac{f}{c}\right)^2$$
$$y = \frac{\sqrt{e^2 + f^2}}{c}$$
$$z^2 = \left(\frac{d}{c}\right)^2 + \left(\frac{f}{c}\right)^2$$
$$z = \frac{\sqrt{d^2 + f^2}}{c}$$
The solution $z = \frac{\sqrt{d^2+f^2}}{c}$ is not the minimum solution, there is another $y = \frac{\sqrt{e^2+f^2}}{c}$ then:
$$z \notin \mathbb{Z}^+ - \{0\}$$
5. There are no more possibilities to be studied then:
$$z \notin \mathbb{Z}^+ - \{0\}$$

Q.E.D.

B. Second Solution

This section will show another analytic proof that shows that Fermat's last theorem is true.

Relationship between *n* power of a number and the *n*! (factorial number), which allows the demonstration of the Fermat's Last Theorem.

The author found a relationship between any natural number ($x > 0$) raised to a power $n > 0$, (x^n), and their corresponding n factorial (*n!*), where *x* and *n* are natural numbers.

Table V shows how this relationship was found. In this table is possible to see how power n keeps a close relationship with $n!$. Table IV shows that the power of a number for $x \geq n$, will always be $n!$ in the column $n + 1$(power 2 gives 2! that is 2, power 3 gives 3! that is 6, power 4 gives 4! that is 24, power 5 gives 5! that is 120, power 6 gives 6! which is 720 and so on). Boxes highlighted in Table IV, shows another interesting relationship: they contain rows and columns of n by n and in its lower right corner always will be $n!$.

Table V was constructed as follows:

- $x$is the number to raise to power n.
- The first column of $n$is x^n.
- The second column of n is the difference between $x^n$and $(x-1)^n$, that means $\{x^n - (x-1)^n\}$.
- The third column of $n$is constructed similarly to differences in the values found in the second column of n, that means $[x^n - (x-1)^n] - [(x-1)^n - (x-2)^n]$ and so on until column $n + 1$.
- The bottom of the column $n + 1$ is always $n!$ from the row $x = n$.

The coefficients of $x^n, a(x-1)^n, b(x-2)^n, c(x-3)^n, d(x-4)^n$, ..., as a result of this operations, a polynomial up to $n!$ will be generated where coefficients $(a, b, c, d, ...)$ of the polynomial would be given in Fig. 9.

n	Coefficients
1	1
2	1 -2 1
3	1 -3 3 -1
4	1 -4 6 -4 1
5	1 -5 10 -10 5 -1
6	1 -6 15 -20 15 -6 1
7	1 -7 21 -35 35 -21 7 -1
8	1 -8 28 -56 70 -56 28 -8 1
9	1 -9 36 -84 126 -126 84 -36 9 -1

Fig. 9 Pyramidal representation of coefficients a, b, c, d... of the polynomial series until $n!$

TABLE V
RELATIONSHIP OF n POWER WITH N!

x	n=1		n=2			n=3			
0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1
2	2	1	4	3	2	8	7	6	5
3	3	1	9	5	2	27	19	12	6
4	4	1	16	7	2	64	37	18	6
5	5	1	25	9	2	125	61	24	6
6	6	1	36	11	2	216	91	30	6
7	7	1	49	13	2	343	127	36	6
8	8	1	64	15	2	512	169	42	6
9	9	1	81	17	2	729	217	48	6
10	10	1	100	19	2	1000	271	54	6

x	n=4					n=5					
0	0	0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1	1	1
2	16	15	14	13	12	32	31	30	29	28	27
3	81	65	50	36	23	243	211	180	150	121	93
4	256	175	110	60	24	1024	781	570	390	240	119
5	625	369	194	84	24	3125	2101	1320	750	360	120
6	1296	671	302	108	24	7776	4651	2550	1230	480	120
7	2401	1105	434	132	24	16807	9031	4380	1830	600	120
8	4096	1695	590	156	24	32768	15361	6930	2550	720	120
9	6561	2465	770	180	24	53043	26281	10320	3390	840	120
10	10000	3439	974	204	24	1E+05	40951	14670	4350	960	120

Taking this relationship of the polynomial as an equation, can be expressed as follows:

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} (x-k)^n = n! \quad \text{where} \binom{n}{k} = \frac{n!}{k!\,(n-k)!} \tag{14}$$

The factor $(-1)^k$ of (14) is to indicate that alternate the signs of the coefficients: $\binom{n}{k}$. These coefficients are exactly Newton's binomial coefficients of:

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} a^{n-} d = (a-d)^n \quad \text{where} \binom{n}{k} = \frac{n!}{k!\,(n-k)!} \tag{15}$$

Or, in the following equation:

$$\sum_{k=0}^{n} \binom{n}{k} a^{n-} d = (a+d)^n \quad \text{where} \binom{n}{k} = \frac{n!}{k!\,(n-k)!} \tag{16}$$

The only difference is that the coefficients of (16) are all positive, while the coefficients of (14) and (15), have alternating signs, starting with the positive sign.

This relationship of the coefficients of (14), (15) and (16) is because we can always get exactly the root n of a^n, $(a-b)^n$ or $(a+b)^n$, or when an equation in polynomial form contains those coefficients in the same way. Later it will be showed that Fermat's equation does not contain these coefficients in the same way.

Theorem 4

For any natural number c that is between x^n and $(x+1)^n$ its n root is irrational, where $x \in \mathbb{Z}^+ - \{0\}$

Proof:

1. Let c be the integer that is in: $x^n<c<(x+1)^n$ where $x \in \mathbb{Z}^+ - \{0\}$
2. If $z=\sqrt[n]{c}$
3. $z^n = c$ ……. According to 2.
4. $x^n < z^n < (x+1)^n$ ……..…..According to 1 and 3.
5. $x < z < (x+1)$ ……..According to 4.
6. $z$will be a radical (comes from the n root) ……..……..……..According to 4 and 5.
7. Assume that the solution of $z = \sqrt[n]{c} = \frac{a}{b}$, where $\frac{a}{b}$ is an irreducible fraction (a and b are coprime factors), where $(a, b) \in \mathbb{Z}^+ - \{0\}$.
8. Raising to the power n is obtained: $z^n = c = \left(\frac{a^n}{b^n}\right) = \left(\frac{a}{b}\right)^n$
9. If $b = 1$ then $z^n = c = a^n$, but then $z = a$,but it would be contrary to that found in 5.
10. If $b \neq 1$, then$c$ is not natural number, which contradict to 1.

11. Therefore, c is not a perfect power for $n > 1$, ($\sqrt[n]{c} \neq racional\ number$), then, its n root is irrational. According to 9 and 10

Q.E.D.

Corollary 1: the n root for $n > 1$ of a prime number will be always irrational.

Corollary 2: the numbers that are between x^n and $(x+1)^n$for $n \geq 1$ not comply with (11)

Corollary 3: the n root of an integer c which is not a perfect power of another integer number is irrational ($a = \sqrt[n]{c} \rightarrow a$ is irrational).

For example, for $n = 2$, 99 do not comply (with $x = 9, x^2 = 9^2 = 81,$ and $(x+1) = 9+1 = 10, (x+1)^2 = 10^2 = 100,\ 81 < 99 < 100$), and to build Table IV with 99 instead of 100 (10^2), it fails that $n! = 2$, so the root 2 of 99, would be an irrational number. ($\sqrt[2]{99} = 9{,}949874371$ ....)

$$9 < 9{,}949874371 \ldots . < 10$$

Any natural number c that have the exact n root, can be expressed by (12) or (13), where the coefficients correspond to Newton's binomials and also fulfill (11):

If $z = \sqrt[n]{c}$, where zis a natural number

$$z^n = c$$

$z = a + d$, where *a* and *d* are natural numbers

$$z^n = (a+d)^n = c$$

$$z^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-}d \qquad \text{where } \binom{n}{k} = \frac{n!}{k!\,(n-k!)}$$

The coefficients structure is exactly equal to Pascal's triangle as in Fig. 10.

n	Coefficients
1	1
2	1 2 1
3	1 3 3 1
4	1 4 6 4 1
5	1 5 10 10 5 1
6	1 6 15 20 15 6 1
7	1 7 21 35 35 21 7 1
8	1 8 28 56 70 56 28 8 1
9	1 9 36 84 126 126 84 36 9 1

Fig. 10 Newton's binomial coefficients or Pascal's triangle

If z is not a natural number, it cannot be expressed as the sum of two integers. If z^n, is a natural number to be expressed in the form of Newton's coefficients where $z^n = (a+b)^n$, it must contain the same coefficients of Newton's binomial, (14), or (15) and (16), i.e. the power n of the sum or difference of two natural numbers.

Equation (16) can be written in the following form:

$$z^n = a^n + p + d^n \tag{17}$$

$$p = \sum_{k=1}^{n-k} \binom{n}{k} a^{n-}d \qquad \text{where } \binom{n}{k} = \frac{n!}{k!\,(n-k!)}$$

Equation (17) complies with the structure of Newton's binomial coefficients and the structure of the coefficients of (14) and therefore z will be a natural number.

In the case of Fermat's Last Theorem it is through the simple fact that $z^n = x^n + y^n$, cannot be expressed maintaining the structure of Newton's coefficients for $n > 2$. The first coefficient is 2, therefore z would not be an integer, thus also proving Fermat's Last Theorem (it cannot meet (14), (15) or (16)).

Reviewing these concepts in Fermat's Last Theorem:

$$z^n = x^n + y^n \tag{18}$$

where $(x, y) > 0$ and natural numbers, $z \notin \mathbb{Z}^+ - \{0\}$ for $n > 2$.

Proof:

Assuming ***x<y***

$$y = x + s, \text{ where } s \in \mathbb{Z}^+ - \{0\}$$
$$y^n = (x+s)^n$$
$$y^n = x^n + p + s^n \tag{19}$$
$$p = \sum_{k=1}^{n-k} \binom{n}{k} x^{n-}s \text{ where } \binom{n}{k} = \frac{n!}{k!\,(n-k!)}$$

Note that the structure of Newton's binomial stays in (16) and root n of y^n would be exact, i.e., has not changed and remains a natural number.

Replacing y^n from (19) into (18) we have:

$$z^n = x^n + x^n + p + s^n = 2x^n + p + s^n$$
$$z^n = 2x^n + p + s^n \tag{20}$$

The first coefficient of x^n is not 1, it is 2 in (20), the structure of Newton's binomial coefficients in this equation is no longer equal to the structure of the coefficients in (14), (16) or (17) to make root n of z^n exact and thus $z$would not be a natural number. If z was a natural number, it would be saying that $\sqrt[n]{2x^n + p + s^n}$(Ec. 20) and $\sqrt[n]{x^n + p + s^n}$ (Ec. 17), are the same and between these two equations there is a contradiction: the polynomial equation given by Newton's binomial and the basic principle of the connection of *n* with *n!* through Newton's binomial coefficients, indicate that the first coefficient is 1 and not 2. ***This also proves Fermat's Last Theorem.***

V. Conclusion

The known standard method to find primitive Pythagorean triples, is that of the succession of prime numbers, (9) and (10). Exploring another method of demonstration of Pythagoras's Theorem, employing equation $z = y + m$for $n = 2$, primitive Pythagorean triples can be obtained when m

is a natural number, (1,2,3,4...⇒∞). Comparing them with the method of succession of prime numbers, it could be established that is easier to employ $z = y + m$, because in a very simple form it could compute any primitive Pythagorean triple ordered for any even or odd x. By applying this method in a similar way for $n > 2$, and using the mathematical Well-ordering Principle in natural numbers, the demonstration of Fermat's Last Theorem was possible.

The formation of Fermat's Last Triangleis shown and the verifications of Theorem 3 inside of Fermat's Last Triangle sides (x, y, z) with$(x, y) \in \mathbb{Z}^+ - \{0\}$ theyall meet:$z \notin \mathbb{Z}^+ - \{0\}$.

Furthermore, using the connection of $n!$ with $(a+b)^n$ through Newton's binomial, for $n > 2$ the demonstration of Fermat's Last Theorem was also shown.

ACKNOWLEDGMENT

The author wantas to thank my professors at the Colombian Naval Academy and at the Naval Postgraduate School, Monterey California, USA for providing me the mathematical background to pursue the investigations that has led to this article.

The author is grateful to Prof. Giraldo Ospina for his comments and shares of his previous studies on the Fermat's last theorem and to many mathematicians and colleagues for their numerous comments along many years of research.

The author is especially thankful to Dr. Carlos Alberto Andrade-Amaya, who critically ordered these demonstrations and was most helpful in expressing the manuscript in a better scientific way.

REFERENCES

[1] Carmichael, R. D. The Theory of numbers and Diophantine Analysis. Dover N.Y., 1959
[2] Dantzig, Tobias. The Bequest of the Greeks. London: Allen &Unwin. ISBN0837101602. 1955
[3] Durán Guardeño, Antonio José. I. Matemáticas y matemáticos en el mundo griego. El legado de las matemáticas. De Euclides a Newton: los genios a través de sus libros. Sevilla. ISBN9788492381821.
[4] Leveque, W. J. Elementary Theory of numbers.. Addison-Wesley Publishing Company, 1962
[5] Plaza, Sergio. Aritmética Elemental una introducción (otra más). Depto de Matemática, Facultad de Ciencias, Universidad Santiago de Chile. Casilla 307-Correo 2.
[6] Singh, Simon. El enigma de Fermat. Tercera Edición Planeta ISBN9788408065722 2010
[7] Wiles, Andrew. Modular elliptic curves and Fermat's Last Theorem (PDF). Annals of Mathematics 141 (3): pp. 443-531. Doi: 10.2307/211855, May 1995.
[8] WEB1: http://www.mathworld.wolfram.com/Fermatlasttheorem.html. Accessed: January 4, 2011.

José Willliam Porras is a retired Admiral from the Colombian Navy. He is a Naval Electronics engineer, MSc. Electrical Engineer and EE in Electrical Engineer at the U.S. Naval Postgraduate School, Monterey, California, USA. (phone +54-315-7437915; e-mail: jwporras@balzola.org).