# A versatile proof of Fermat's last theorem

M.Meyyappan[#1]

*Professor of Physics (Retd), Alagappa Government Arts College,Karaikudi-630001, India*

***Abstract***

*A simple and multi-purpose proof is proposed with well known arithmetic axioms to explain not only the Fermat's assertion but also the non-existence of square triples (a,b,c) satisfying $a^n + b^n = c^n$ for all exponents including n = 2, reason for certain allowed and forbidden relations among equal sum of like powers and Beal conjecture (Mauldin/Tijdeman-Zagier conjecture) altogether successfully in a single frame.*

**Key words**

*Fermat's Last Theorem - arithmetic axioms equal power relations – Multi-power relation - Beal conjecture.*

## I. Introduction

For all exponents greater than 2 , the numerical relation in the form $a^n + b^n = c^n$ cannot exist when a,b and c are restricted to have whole integers which is called Fermat's Last Theorem (FLT) , but is true when irrational and complex numbers are allowed for at least one or two members. After the Fermat's assertion, many people [1,2,3] attempted to prove FLT for different values of exponent and verified with the help of number theory. After the introduction of computer technology people attempted to support the proof of FLT for a wide range of exponents 3 - 4,000,000 [4]. A proof of FLT was given by Taylor and Wills [5,6] with the help of modern concepts of mathematics – elliptic curve and modular theory. In general there must be two or more ways to get the same result for a given mathematical problem. Since the law of nature is always as simple as possible, there must be more natural and naive proof for FLT. This paper describes the attempt undertaken to disclose the naive and accessible proof of FLT with the help of well known arithmetic axioms and number theory. The unequivocal representation reveals its versatility of the methodology.

## II.Arithmetic axioms

1.In $a^n + b^n = c^n$ , c is always greater than both a and b but $c^m$ is less than $a^m + b^m$ when m < n, and greater when m > n. This is true even when m is a fraction

2.The conservation of odd-evenness in the three member equal sum of like powers necessitates that the allowed and irreducible set of triples (a,b,c) must be with (odd, even, odd), where as the apparently allowed triples with (odd, odd, even) is forbidden due to non-conservation of odd-evenness of the relation, as a doubly even component cannot be balanced with a singly even component, and it is found to be true for all exponents. This restriction is given up in multi-power relations.

3.If a is prime in a three member equal power relation, then c - b will invariably be equal to 1

4.The product of any two powers to give a single power follows some rules. If $a^x \times b^y = c^z$, either the base numbers must be same or some of its power or the exponents must be same or some of its multiple. When b is equal to $a^\alpha$, where α may have any integer value, then $z = x + \alpha y$ and c = a. When y is equal to αx, then z = x and $c = ab^\alpha$.

5.In $a^x = b^y$, if a,b and the exponents are all whole integers, then $a = \alpha^y$ and $b = \alpha^x$, so that $a^x = b^y = \alpha^{xy}$

## III.Proof of Fermat's Last Theorem

In $a^n + b^n = c^n$, $a^n$ is equal to a product of two factors $(c^{n/2} - b^{n/2})(c^{n/2} + b^{n/2})$ and $a^{n/2} > c^{n/2} - b^{n/2}$, one can ingeniously separate these two factors as $(c^{n/2} - b^{n/2}) = a^{n/2}/k$ where $k > 1$ , not necessary to be an integer and

may have all possible values (axiom 1), then $(c^{n/2} + b^{n/2}) = k\, a^{n/2}$. Solving for $b^n$ and $c^n$ in terms of $a^n$ we get $b^n = a^n [ (k^2 – l) /2k]^2$ and $c^n = a^n [( k^2 + 1) / 2k]^2$. In the same manner one can solve for $a^n$ and $c^n$ in terms of $b^n$ also, which gives mathematically identical result. $a^n + b^n = c^n$ is then rearranged with its internal constituents as $[(2k)^{2/n}a]^n + [(k^2-1)^{2/n} a]^n = [ (k^2 + 1)^{2/n} a]^n$ where 'a' is found to be a common prime factor of the triple with an inherent condition $1 + [ (k^2 – l) /2k]^2 = [( k^2 + 1) / 2k]^2$. Mathematically speaking such equal power relations have a common prime factor, since any two members can be expressed in terms of the other member. They are reducible due to this common prime factor. An irreducible set of triple for an exponent n will not have any common prime factor at all. Besides that at least two members will be either irrational or complex instead of being whole integers. But the common prime factor remains in all the three member multi-power relations as stated in Beal conjecture, because it cannot be reduced as done in equal power relations. When reduced it becomes a generator of multi-power relation which will not have the common prime factor.

Whatever may be the way by which a member is factorized with respect to the remaining members, the internal constituents may differ, but in general, the structure of the basic relation will be same. If a = p, a prime, then the relation becomes, $p^n + [(p^n – 1)/2]^2 = [(p^n + 1)/2]^2$, where the difference c - b = 1 (axiom-3), where no common prime factor exists. If a = pq where p < q, then $(c^{n/2} - b^{n/2}) = p^n$ and $(c^{n/2} + b^{n/2}) = q^n$ ,it gives yet another form of the above expression $(2^{2/n} pq)^n + (q^n – p^n)^2 = (q^n + p^n)^2$, where the common prime factor may or may not exist.

In fact all the three member equal or unequal power relations have the following general form $a^n + a^n [x^2] = a^n [y^2]$, where $[x^2]$ and $[y^2]$ may have any integer or a quantum of value or fractional value but with same denominator satisfying the condition $1 +[x^2] = [y^2]$. For a given value of the exponent, one can change the base numbers only. Due to this limitation, the formation of $a^n + (\beta a)^n = (\gamma a)^n$ is practically impossible as both $\beta^n$ and $\gamma^n$ cannot be whole integer simultaneously. By choosing a quantum of value for $[x^2]$, one term can be converted into a modified power as required, but it is not possible for the other with $(1 +[ x^2])$. Even by adding any equal quantum of value in both side, the condition fails to support the relation. For example, by adding q both sides, the balance of the relation will not be affected. $(a^n\beta) + q = m^n$ and $a^n ( 1 + \beta) + q = n^x$ which demands $1 = n^x - m^x$ and for which no integer solutions are available.

Any known relation with whole integers such as Pythagorean relation can even be considered for this purpose. It can be used as a key to solve problems related to equal sums of like and unlike powers with same or different number of terms in each side. The scope of this paper is restricted only to three member equal and unequal power relations.

## IV.General Proof of FLT

Consider a basic relation $(2k)^2 + (k^2-1)^2 = (k^2 + 1)^2$,To convert it into an equal power relation with an exponent n, the requirements are $k^2 = a^n/4$, $(k^2 -1)^2 = b^n$ and $(k^2 + 1)^2 = c^n$ , with a condition $c^{n/2} - b^{n/2} = 2$.This is valid only when n = 2 for whole integral values of c and b. When $a^n + a^n [x^2] = a^n [y^2]$ represents the equal power relation, the condition is $1+ b^n = c^n$ . It is found that the relation becomes distinct when $n \leq 2$ and $n \geq 3$. When n = 2, the terms within each bracket will be whole integral number and will not have any common prime factor in its irreducible form and the condition reduces to c – b = 2, which is practically possible. In the other case the condition is possible when b and c are fractions with equal denominator. When n is greater than 2, the condition becomes unrealistic and all the members cannot be expressed as whole integral number simultaneously.

It is found that the terms inside each of the brackets can be made to be whole integer only when n = 2, which is the case of Pythagorean triples. When $n \geq 3$ , not all the three members will be whole integers simultaneously and one or more members will invariably be irrational or complex. It explains the argumentative support put forwarded by Pierre de Fermat for cubical and higher power relations and stands as valid proof of FLT.

## V.Non existence of square triples

All the members of a triple (a,b,c) corresponding to any exponent n cannot be squares. It is true even when the exponent n = 2.In fact it is a direct consequence of FLT. The non-existence of square triples can also be taken as an indication of FLT. If all the members of a triple are squares $(a^2,b^2,c^2)$ for an exponent n, then (a,b,c) would be a triple for the exponent 2n.If square triples exist for the exponent 2 than a fourth power must be equal to a sum of two fourth powers which is against the argument of the previous section. In $a^n + (a[x^2]^{1/n})^n = (a[y^2]^{1/n})^n$, if a is a square number say $\alpha^2$ , the other two members will be squares only if $[x^2] = \alpha^{2n}$ and $[y^2] = \beta^{2n}$, which gives again an impossible condition $\beta^{2n} - \alpha^{2n} = 1$. It is not fulfilled even when n = 2.It predicts that all the members can be squares when the exponent is ½. The general form of the possible solution is given by $1^{1/2} + (n^2)^{1/2} = [(n+1)^2]^{1/2}$. From $(2k)^2 + (k^2-1)^2 = (k^2 + 1)^2$ we can arrive at the same conclusion. The condition $c^n - b^n = 1$ does not permit square triples for any exponent.

## VI.Forbidden power relations

In general equal sum of like powers is possible with equal number of terms in each side of the expression for all exponents. Let us restrict our interest to $a^n + b^n = c^n + d^n$ .The basic relation to explain its characteristics is $[x_1]^2 + [y_2]^2 = [x_2]^2 + [y_1]^2$ where $1 + [x_1]^2 = [y_1]^2$ and $1 + [x_2]^2 = [y_2]^2$. In terms of independent variables k, k', m and n it can be expressed as $[(k^2 - m^2)/2mk]^2 + [(k'^2 + n^2)/2nk']^2 = [(k'^2 - n^2)/2nk']^2 + [(k^2 + m^2)/2mk]^2$. This can also be expressed as $(a+b)^2 + (c-d)^2 = (a-b)^2 + (c+d)^2$ with a condition ab = cd. For $n^{th}$ power relation each term must be $n^{th}$ power of an integer. If the two terms in one side of the relation are taken as $a^n + b^n$, then the terms in the other side will be $(a^n +/- 1)$ and $(b^n -/+ 1)$. By adding and subtracting a suitable number without affecting the balance, both the term in the other side can be made to be $n^{th}$ power of different numbers respectively.

But there are some restrictions in the case of unequal number of like powers in each side of the relation. Fermat's assertion, a sum of two $n^{th}$ powers greater than equal to 3 equal to $n^{th}$ power of whole numbers is an unique restriction. This can also be proved algebraically (Annexure). The restrictions are found to be different for different exponents. For example, a sum three squares or three cubes can be shown to be a square or cube respectively

$$(4kk')^2 + [2k'(k^2 - 1)]^2 + [(k^2 + 1)(k'^2 + 1)]^2 = [(k^2 + 1)(k'^2 + 1)]^2$$

where $1 + [(k^2 - 1)/2k]^2 = [(k^2 + 1)/2k]^2$ and $1 + [(k'^2 - 1)/2k']^2 = [(k'^2 + 1)/2k']^2$

But no such expression exists for the exponents n = 4 and 5.However a sum of four fourth or fifth powers equalling a fourth or fifth power respectively exists. It is the self adjustment that determines the possibility of formation of equal sum of like powers balanced with equal and unequal number of terms.

Considering the case where a square is equal to a sum of three squares. $[y^2]^2 = (1 + [x^2])^2 = 1 + [x^2]^2 + 2[x^2]$. To make $2[x^2]$ to be a square, $[x^2]$ must be equal to $2\alpha^2$. For cubical relation $[y^2]^3 = (1 + [x^2])^3 = 1 + [x^2]^3 + 3[x^2][y^2]$, and $3[x^2][y^2]$ to be a cube, it must be equal to $27\alpha^3$. The roots of the quadratic equation $x^2(1+ x^2) = 9\alpha^3$ is given by $x^2 = [-1 \pm \sqrt{(1+ 36\alpha^3)}]/2$, when $\alpha = 2$, we get $x^2 = 8$ or $-9$ which gives a numeral relation $9^3 = 1^3 + 6^3 + 8^3$. Non-existence of equal sum of like powers in the form $a^4 = b^4 + c^4 + d^4$ conjectured by Euler can be explained successfully with the same fundamental expression- $(c^2)^2 = (a^2 + b^2)^2 = a^4 + b^4 + 2a^2b^2$ ,where $2a^2b^2$ cannot be expressed as a fourth power of a whole number with all possible values of a and b.

## VII.Beal conjecture

Even though the conditional equal power relation with three members is unachievable for all exponents $n \geq 3$, it is found that multi-power relations are obtainable. According to Beal conjecture [7,8,9] when the base numbers a,b and c and

the exponents x,y and z greater than 2 in $a^x + b^y = c^z$ are all positive, then a,b,c will invariably have a common prime factor. The secret behind the multi-power relations is making up a power of an integer from the product of two terms - a power of an integer $a^m$ and a number of any kind $[x^2]$ and $[y^2]$ respectively obeying the condition $1 + [x^2] = [y^2]$ .This can be accomplished under certain ways. The product $a^m . [x^2]$ becomes $a^{m+n}$ when $[x^2] =$

$a^n$ , where the base number is unchanged but the exponent gets changed. The product is equal to $(a\alpha)^m$ when $[x^2] = \alpha^m$ where the exponent remains same but the base number is changed. It is equal to $(a\alpha)^{m+n}$ when $[x^2] = a^n \alpha^{n+m}$ where both the base number and exponent are changed. It is $(a\alpha)^n$ when $[x^2] = a^{n-m}\alpha^n$ where $n > m$ and it is equal to $\alpha^n / (a^{m-n})$ where $m > n$ . In all the above cases, the base number of the product is some multiples of the base number in the multiplicand, i.e., the base of the multiplicand preserves the base of the product as its generic character. The product can be made to be equal to $\beta^n$ which may miss the generic character when $[x^2] = \beta^n/a^m$. In such cases both the base and exponent get changed. The acceptable multi-power relations are completely determined by the simultaneous fulfilment of the requirement by both the products $a^m [x^2]$ and $a^m [y^2]$ satisfying the condition $1 + [x^2] = [y^2]$.

Even though $a^m + b^m = c^m$ is not possible when a,b,c are all whole integers and $m \geq 3$ , multi-power relation in the form $a^x + b^y = c^z$ is possible for certain permissible values of x,y,z. Like equal power relations, all the three member multi-power relations have the same basic structure $a^x + a^x[(k^2-1)/2k]^2 = a^x[(k^2+1)/2k]^2$, where a and k are two independent variables. This can be converted into a multi-power relation by properly choosing the values of $[x^2]$ and $[y^2]$ and converting the products to a power of an integer. For example $a^x + a^{x+m} = a^{x+n}$ is not possible with same base number since $1 + a^m \neq a^n$ for all possible values of a,m and n. But $a^x + a^{x+m} = (a\alpha)^x$ is possible due to the soluble condition $1 + a^m = \alpha^x$. When $a = 2, \alpha = 3$, $m = 3$ and $x = 2$, we get $2^2 + 2^5 = 6^2$. Similarly $a^x + (a\alpha)^x = a^{x+m}$ is allowed due to attainable condition $1 + \alpha^x = a^m$ which gives a multi-power relation $3^3 + 6^3 = 3^5$.

From the general form of the three member equal power relation, one can derive one or more conditions for any particular requirement. Its numeral form can be used as a generator for the development of such multi-power relations. In fact three member multi-power relation is not possible for all possible set of exponents due to insoluble condition. Table.1 shows some of the allowed and forbidden 3 member multi-power relations with a typical numerical example.

Table.1.Allowed and Forbidden three member multi-power relations

| $a^x + b^y = c^z$ | conditions | numerical example |
|---|---|---|
| $a^n + (a\alpha)^n = (a\beta)^n$ | $1 + \alpha^n = \beta^n$ | not possible (FLT) |
| $a^3 + (a\alpha)^3 = (a\beta)^4$ | $1 + \alpha^3 = a\beta^4$ | $9^3 + 18^3 = 9^4$ |
| $(a\alpha)^3 + (a\beta)^3 = a^4$ | $\alpha^3 + \beta^3 = a$ | $70^3 + 105^3 = 35^4$ |
| $a^3 + (a\alpha)^4 = (a\beta)^3$ | $1 + a\alpha^4 = \beta^3$ | $7^3 + 7^4 = 14^3$ |
| $(a\alpha)^3 + a^4 = (a\beta)^3$ | $\alpha^3 + a = \beta^3$ | $38^3 + 19^4 = 57^3$ |
| $a^3 + (a\alpha)^3 = (a\beta)^5$ | $1 + \alpha^3 = a^2\beta^5$ | $3^3 + 6^3 = 3^5$ |
| $(a\alpha)^3 + (a\beta)^3 = a^5$ | $\alpha^3 + \beta^3 = a^2$ | $8^3 + 8^3 = 4^5$ |
| $a^5 + (a\alpha)^3 = (a\beta)^3$ | $a^2 + \alpha^3 = \beta^3$ | $13^5 + 91^3 = 104^3$ |
| $a^5 + \alpha^3 = \beta^3$ | $a^5 = (\beta - \alpha)(\beta^2 + \beta\alpha + \alpha^2)$ | not possible |

$a^3 + (a\alpha)^5 = (a\beta)^3$ $\quad$ $1 + a^2\alpha^5 = \beta^3$ $\quad$ $91^3 + 13^5 = 104^3$

$a^3 + (a\alpha)^4 = (a\beta)^5$ $\quad$ $1 = a(a\beta^5 - \alpha^4)$ $\quad$ not possible

---

In fact multi-power relations can be obtained directly from the generator- any simple numeral expression, by multiplying each term with a common multiplier, which provides a common prime factor to the relation. For example, the condition $1 + 1 = 2$ when multiplied by $2^m$ gives $2^m + 2^m = 2^{m+1}$,and the common multiplier $2^{2m}$ gives $4^m + 4^m = 2^{2m+1}$ where as the condition $1 + 7 = 2^3$ gives $7^3 + 7^4 = 14^3$ with a common multiplier $7^3$. $a^n + b^{n+1} = c^n$ is the most common type of multi-power relation. The general form of this type of relation is given by $(2^n-1)^n + (2^n-1)^{n+1} = [2(2^n - 1)]^n$

A generator can provide many multi-power relations each with different multipliers. It is exemplified with few examples

$1 + b^y = c^z \quad \rightarrow \quad 1 + 2^3 = 3^2$

Only certain common multiplier alone can make each term into a power of an integer. 1 is very convenient member as it is the only multiplicand to make product with multiplier of any form. In the above case either $b^z$ or $c^y$ or $\alpha^{zy}$ will be the convenient multipliers.

$[1 + b^y = c^z] \times b^z = b^z + b^{y+z} = (bc)^z \rightarrow 2^2 + 2^5 = 6^2$

$[1 + b^y = c^z] \times c^y = c^y + (cb)^y = c^{y+z} \rightarrow 3^3 + 6^3 = 3^5$

$[1 + b^y = c^z] \times \alpha^{zy} = \alpha^{zy} + (\alpha^z b)^y = (\alpha^y c)^z \rightarrow 7^6 + (98)^3 = (1029)^2$

Similarly, $a^x + b^x = c \rightarrow 1^3 + 3^3 = 28$, multiplying with the common multiplier $c^x$

$[a^x + b^x = c] \times c^x = (ac)^x + (bc)^x = c^{x+1} \rightarrow 28^3 + 74^3 = 28^4$ with common multiplier $28^3$

$\rightarrow 784^3 + 2352^3 = 28^7$ with common multiplier $28^6$

If $a^x + b^y = c^z$ itself is taken as generator, then one of the common multipliers will be $\alpha^{xyz}$

$(a^x + b^y = c^z) \times \alpha^{xyz} = (a\alpha^{yz})^x + (b\alpha^{xz})^y = (c\alpha^{xy})^z$

The generators usually do not have common prime factor, but will have in its reducible form. Hence the generators may or may not have a common prime factor depending upon its reducibility. In fact the generators are irreducible form of multi-power relations. When multiplied with a common multiplier to get a multi-power relation, it acquires a common prime factor.

One can show that the common prime factor is compulsory for all the three member multi-power relations but vanishes in all the three member equal power relations .The common prime factor is not a compulsory requirement in multi-power relations with at least one member is a square or more than three members. The non-existence of common factor in equal power relations for all exponents $n \geq 3$ can also be taken as an indirect proof of FLT

## VIII. Exempted multi-power relations

Beal assertion is not a necessary condition in all multi-power relations with more than three members or one of the members is a square. e.g., ( with more than three members $9^4 = 8^4 + 7^4 + 4^3$ ; $3^5 = 4^3 + 2^3 + 2^3 + 1^3$; $5^4 = 3^4 + 2^5 + 8^3$) and ( with one member is a square $8^3 = 13^2 + 7^3$; $105^3 = 181^2 + 104^3$ ; $17^4 = 161^2 + 240^2$). When one of the members is a square, then the three member multi-power relation becomes

$a^2 + a^2[(k^2 - 1)/2k]^2 = a^2[(k^2 + 1)/2k]^2$

$a^2 + a^y[1/a^{y-2}][(k^2 - 1)/2k]^2 = a^z[1/a^{z-2}][(k^2 + 1)/2k]^2$

$[1/a^{y-2}][(k^2 - 1)/2k]^2 = \alpha^y$ and $[1/a^{z-2}][(k^2 + 1)/2k]^2 = \beta^z$ , from which the required condition can be derived as

$1 = (a^{z-2})\beta^z - (a^{y-2})\alpha^y = a^{y-2}[a^{z-y}\beta^z - \alpha^y]$ which has no integral solution.

When it is converted into a form $a^2 + b^3 = c^3$ , the common factor is either lost or changed by the denominator of $[x^2]$ and $[y^2]$ . When the common multiplier is some multiples of the common denominator of the fraction representing $[x^2]$ and $[y^2]$ , the multi-power relation may lose its common prime factor. That is what is found in multi-power relation with one member is a square.

Like three member equal power relations, in multi-power relations also all the members cannot be squares or any equal higher powers - $a^{2x} + a^{2x}[x^2] = a^{2x}[y^2]$ .Assuming x > y > z, one can construct a multi-power relation as $a^{2x} + a^{2y}(a^{2x-2y}[x^2]) = a^{2z}(a^{2x-2z}[y^2]) \rightarrow a^x + (a\beta)^{2y} = (a\gamma)^{2z}$ , with a condition $1 + \beta^{2y}/(a^{2x-2y}) = \gamma^{2z}/(a^{2x-2z})$.Since the denominators are different $\beta^y$ must be divisible by $(a^{x-y})$ and $\gamma^z$ by $(a^{x-z})$ which gives a modified condition as $1 + m^2 = n^2$ , which has no practical solution for any integer values of m and n. Even by self adjustment also, one cannot make it to be true.

## Reference

[1] Simon Singh, 'Fermat's Last Theorem" Fourth Estate Ltd, (1997)
[2] A.Jackson, "Fermat's Enigma" Review in AMS (1997).
[3] H.M.Edward,"Fermat's Last Theorem – a genetic introduction to the Number Theorey, Germany,Springer,(1997).
[4] S.Wagstaff, AMS Notices, 1976,167,p A-53,244
[5] Andrew Wills, 'Modular elliptic curve and Fermat's last theorem' in Annals of Maths.1995, 141, 443-551.
[6] Gerd Faltings., " The proof of Fermat's Last Theorem by R.Taylor and A.Wills" AMS,1995,42 (7),743-746.
[7] R.Daniel Mauldin, "A generalization of Fermat's Last theorem: The Beal conjecture and prize problem" in AMS, 1997, 44,1436-39
[8] Golden G.Nyambuya, "A simple and general proof of Beal conjecture" in Adv.in Pure. Maths, 2014, 4,518-521.
[9] wimhessellink.nl/fermat/WilesEnglish.htm

---

Annexure.

The algebraic method also confirms FLT. In the case of cubical expression,
$a^3 + b^3 = (a+b)(a^2 - ab + b^2) = c^3$
Since $a+b > c$, $a+b = kc$ where $k > 1$ and $a^2 - ab + b^2 = c^2/k$, Solving for a and b
$a = (kc/2) - (ck/6)[(12/k^3) - 3]^{1/2}$ and $b = (kc/2) + (ck/6)[(12/k^3) - 3]^{1/2}$
when k =1 , the second term becomes c/2 and a = 0, b = c. For all values k > 1, the second term becomes irrational or complex.

---

Acknowledgement

The author is grateful to Pierre de Fermat who gave an open problem to think over at least if not to try to solve by people of all age group. This proof is dedicated to Mahatma Gandhi, a man I love most.