B.N. Pathak

Proof to "Fermat's Last Equation"

by B.N. Pathak

1. Introductory:-

1.1 Fermat's Last Theorem also known as FLT, states that the equation $x^n + y^n = z^n$ holds good, i.e. will have innumerable equations/solutions for all integral x, y and z when n=2, but does not hold good for integral values of x, y and z, when n > 2, where n is an integer.

1.2 We will write FLT as:-

$$x^n + y^n = z^n \qquad \ldots. (1.0)$$

1.3 We will prove FLT through the following workings.

2. Preliminary Examination of FLT:-

2.1 Let x, y and z be all positive quantities.

2.2 A simple examination of the equation $x^n + y^n = z^n$ will lead us to the conclusion that x (or y) < z, since x^n (or y^n) = $z^n - y^n$ (or x^n), i.e.

x (or y) = $[z^n - y^n \text{ (or } x^n)]^{(1/n)}$

2.3 Similarly from FLT, we have $x \neq y$, since if it is so, i.e. if x=y, we have from FLT
$x^n + x^n = 2x^n = z^n$ or

$z = x * 2^{(1/n)}$

Since $2^{(1/n)}$ for n > 1, is always a surd or non-integer, z will be non-integer for integral values of x. Alternately, to keep z as an integer, we must have:-
$x = a * 2^{(n-1)/n}$ x will become non-integral even with a as an integer
* - multiplication sign

3. <u>Modus Operandi</u>:-

3.1 We will assume x and y to be any two positive integers and n also to be a positive integer. Let us also initially assume/expect z to be an integer. From the very further workings of FLT we will prove that at n = 2 only, z will be an integer, when x and y are positive integers, confirming the initial assumption of z as an integer. Of course, it will also be seen that n = 2, when FLT holds good, x, y and z will have certain relationship amongst themselves. Similarly, it will be seen at n > 2, when x and y are integers, z shall not be an integer, which will thus contradict the initial assumption of z to be an integer. This will prove Fermat's Last Theorem (FLT).

3.2 Since as per para 2.3, $x \neq y$, let $y = p + x$, where let p also be a positive integer, alongwith x and y as positive integers, whence $y > x$ (say). From FLT, we have :-

$$z^n = x^n + y^n = x^n + (p+x)^n = p^n + {}^nC_1p^{n-1}x + {}^nC_2p^{n-2}x^2 + --- + {}^nC_{n-1}px^{n-1} + 2x^n \qquad ---- (1.01)$$

3.2/1 For integral values of z, for $n \geq 2$, we shall have $p \neq x$, since if $p = x$, then from eqn.(1.01), we shall have :-

$$z^n = x^n + (p + x)^n = x^n + (2x)^n = x^n (1 + 2^n)$$

or

$$z = x(1 + 2^n)^{1/n} \qquad …. (1.01)/1$$

As $(1 + 2^n)^{1/n} \neq$ an integer for $n \geq 2$, z will become a non-integer as per equation (1.01)/1, since x = an integer.

It can be easily shown that for $n \geq 2$, value of $(1 + 2^n)^{1/n} \neq$ an integer, since if this is a positive integer(with which alone we are dealing all along), say = m, then we shall have;-

$$1 + 2^n = m^n$$

or

$$1 = m^n - 2^n = (m -2)(m^{n-1} + m^{n-2}.2 + …..+ m.2^{n-2} + 2^{n-1}) \qquad …. (1.01/2)$$

In RHS of eqn. (1.01)/2, in order to maintain the same positive sign therein, as in LHS of this equation, the minimum integral value of m can be put equal to 3, i.e m = 3, whence we will have from (1.01)/2, the following:-

$$1 = 3^{n-1} + 3^{n-2}.2 + …. + 3.2^{n-2} + 2^{n-1} \qquad …. (1.01)/3$$

Since the above is an absurd and unacceptable result, we shall have

$(1 + 2^n)^{1/n} \neq$ an integer for $n \geq 2$.

From all the above it is concluded that for $n \geq 2$, in FLT, for all integral values of z, we shall have $p \neq x$. Alternatively, it will follow that for p=x, value of z will in turn always be non-integral for $n \geq 2$

3.2.1 From binomial theorem, we have:-

$$(1-x)^n = 1 - {}^nC_1x + {}^nC_2x^2 - {}^nC_3x^3 + \dots + (-1)^{n-1}\, {}^nC_{n-1}\, x^{n-1} + (-1)^n\, {}^nC_nx^n$$

Putting x = 1 in above equation, we have:-

$$0 = 1 - {}^nC_1 + {}^nC_2 - {}^nC_3 + \dots + (-1)^{n-1}\, {}^nC_{n-1} + (-1)^n\, {}^nC_n$$

or

$$1 = {}^nC_1 - {}^nC_2 + {}^nC_3 - {}^nC_4 + \dots - (-1)^{n-1}\, {}^nC_{n-1} - (-1)^n\, {}^nC_n \quad \text{---- (1.01.1)}$$

Using equation (1.01.1), we can write p^n in equation (1.01) as follows:-

$$p^n = p^n\, [{}^nC_1 - {}^nC_2 + {}^nC_3 - {}^nC_4 + \dots - (-1)^{n-1}\ {}^nC_{n-1} - (-1)^n], \text{ since } {}^nC_n = 1$$

Putting the above value of p^n in equation (1.01) and rearranging them we have :-

$$z^n = -(-1)^n\, p^n + {}^nC_1\, p^{n-1}\, (x+p) + {}^nC_2\, p^{n-2}\, (x^2 - p^2) + {}^nC_3\, p^{n-3}\, (x^3+p^3) + \dots + {}^nC_{n-1}\, p[x^{n-1} - (-1)^{n-1}\, p^{n-1}] + 2x^n$$

or

$$z^n = p^n - [1 + (-1)^n]\, p^n + {}^nC_1\, p^{n-1}\, (x+p) + {}^nC_2\, p^{n-2}\, (x^2 - p^2) + \dots + {}^nC_{n-1}p[x^{n-1} - (-1)^{n-1}\, p^{n-1}] + 2x^n \quad \dots\dots (2.0)$$

Further rearranging aforesaid equation (2.0) we have :-

$$z^n = p^n + {}^nC_1\, p^{n-1}\, (x+p) + {}^nC_2\, p^{n-2}\, (x^2 - p^2) + {}^nC_3\, p^{n-3}\, (x^3+p^3) + \dots + {}^nC_{n-1}\, p[x^{n-1} - (-1)^{n-1}\, p^{n-1}] + + [2\, x^n - \{ 1 + (-1)^n\}\, p^n] \quad \dots\dots. (2.1)$$

$$= Q^n \text{ (say)} \quad \dots.. (2.2)$$

$= (p + t)^n$ (say) ….. (2.3)

3.2.2 As the R.H.S. of equation (2.1) has (n +1) terms and first n terms are associated with their respective coefficients (including unity with first term i.e. p^n) with descending powers of p starting from p^n, as also the various terms are respectively associated with $^nC_0$ (with p^n, as $^nC_0 = 1$), $^nC_1$, $^nC_2$, …. $^nC_{n-1}$ and ^nC_n (since again $^nC_n = 1$) with the last $(n+1)^{th}$ term, AND the L.H.S. of equation (2.1) is n^{th} power of a quantity i.e. equal to z^n, for FLT to hold good the R.H.S. should also be the n^{th} power of a quantity say Q, whence we shall have $z^n = Q^n$, as written in equation (2.2) above.

Proof

3.2.3 Since equations (2.2) & (2.1) have been derived from the original equation (1.0) of FLT, wherefrom we have $z^n = x^n + y^n = x^n + (p+x)^n$ whence $z^n > y^n$ i.e. $z > y$ or $z > (p + x)$ or $z > p$. Since as per equation (2.2) $z^n = Q^n$ or $z = Q$, Q must also be > p, i.e. $Q > p$. Let $Q = (p + t)$. Thus we have $z^n = Q^n = (p + t)^n$ as stated/ written at equation (2.3), whence $z = Q = (p + t)$

3.2.4 Since p has been assumed to be an integer (along with x and y); for z to be an integer t must also be an integer. It will now be shown that t is an integer only at n = 2, whence z is an integer (as also x and y being integers as assumed earlier) at n = 2 only, whereas for n > 2, we shall have t ≠ An integer, i.e. a non-integer, whence for $z = (p + t) \neq$ An integer. This will prove FLT.

From all the above proceedings, we have:-

$Z^n = Q^n$

$= (p + t)^n$

$= p^n + {}^nC_1\, p^{n-1}\, t + {}^nC_2\, p^{n-2}\, t^2 + {}^nC_3\, p^{n-3}\, t^3 + \ldots + {}^nC_{n-1}\, p\, t^{n-1} + t^n$ …… (3.0)

Comparing the coefficients of equal powers of p in different terms in R.H.S. expressions of equations (2.1) and (3.0), we have :-

$t = x + p$ …. (i) }

$t^2 = x^2 - p^2$ …. (ii) .

…. (3.01)

$t^3 = x^3 + p^3$ …. (iii) .

.

.

.

$t^{n-1} = x^{n-1} - (-1)^{n-1} p^{n-1}$ …. (n-1) }

and

$t^n = 2x^n - \{1 + (-1)^n\} p^n$ …. (3.02)

4. Vertically multiplying the various (n-1) subequations of both L.H.S. and R.H.S. of equation (3.01), we have only the following valid and acceptable equation incorporating all the aforesaid (n-1) relationships.

$$t^{1+2+3+\ldots+(n-1)} = t^{n(n-1)/2} = (x+p)(x^2 - p^2)(x^3 + p^3) \ldots [x^{n-1} - (-1)^{n-1} p^{n-1}] \quad \ldots. (4.0)$$

|……(n-1) terms ………|

or

$$t = [(x + p)(x^2 - p^2)(x^3 + p^3) \;\ldots.\; \{x^{n-1} - (-1)^{n-1} p^{n-1}\}]^{2/\{n(n-1)\}} \quad \ldots.(4.01)$$

|……………..(n-1) terms………………………………|

Since as per para 3.2/1 , we have $p \neq x$, whence $t \neq 0$

4.1 We will now examine values of t from equations (4.0), (4.01) and (3.02) for different values of n and will find when t becomes integral. From equation (4.0) we find that the R.H.S. has (n-1) terms i.e. at n = 2, the R.H.S. of equation (4.0) will have only one term, at n = 3, the R.H.S. will have two terms and so on.

4.2 We will now examine value of t at n = 2. From equation 4.0 we have the following at n = 2. As stated earlier, the R.H.S. of this equation will have only one term at n = 2.

$t^{n(n-1)/2} = t = x + p$ …. (4.0 / 2)

i.e. $t^2 = (x+p)^2$ …. (4.0 / 2.1)

also from equation (3.02) we have at n = 2

$t^n = 2x^n – [1 + (-1)^n]p^n$

or

$t^2 = 2x^2 – 2p^2 = 2(x^2 – p^2)$ …. (3.02 / 2)

Equating (4.0 / 2.1) and (3.02 / 2) we have at n = 2 :-

$t^2 = (x + p)^2 = 2(x^2 – p^2) = 2(x+p)(x-p)$ …. (4.0 / 2.1.1)

Since x and p are both positive integers, $x + p \neq 0$, whence canceling x + p from both sides of above equation, we have

$x + p = 2(x – p)$

or

$x = 3p$ …. (4.0 / 2.2)

4.2.1 From para (3.2),
Since y = p + x, we have at n = 2 :-
$y = p + x = 4p$ …. (4.0 / 2.3)

Also, since from FLT at n = 2, we have :-

$z^2 = x^2 + y^2 = (3p)^2 + (4p)^2 = 25p^2$

or

$z = 5p$ …. (4.0 / 2.4)

4.2.2 Thus at n = 2, we have from FLT :-

x = 3p }
y = 4p . …… All integers, since p = An integer …. (4.0 / 2.5)
z = 5p }

4.2.3 Giving different values to p say 1, 2, 3, etc., we shall have following equations for FLT at n = 2.

$z^2 = x^2 + y^2$

$5^2 = 3^2 + 4^2$

$10^2 = 6^2 + 8^2$

$15^2 = 9^2 + 12^2$

…. and so on …

4.2.4 A more general all integral values of x, y and z of FLT at n = 2 can be had from following equations by assuming $x = b(2a + b)$ and $p = 2a^2 - b^2$ in equation (1.01), where a and b are two positive integers.

$$\left.\begin{aligned}
&x = b\,(2a + b)\\
&p = 2a^2 - b^2\\
&\text{As per para (3.2), we have : -}\\
&y = p + x = 2a(a + b)\\
&\text{Also as per FLT at n = 2, we have :-}\\
&z = (x^2 + y^2)^{1/2} = a^2 + (a + b)^2\\
&\text{Also as per para 3.2.3, we have :-}\\
&z = p + t \quad \text{whence}\\
&t = z - p = a^2 + (a+b)^2 - 2a^2 + b^2\\
&\qquad\quad = 2b(a + b)
\end{aligned}\right\} \quad \text{…. (4.0 / 2.5.1)}$$

4.2.5 Thus we will have a more general all integral values of x, y and z of FLT at n = 2 as follows :-

$$\left.\begin{aligned}
&x = b(2a + b)\\
&y = 2a(a + b)\\
&z = a^2 + (a + b)^2
\end{aligned}\right\} \quad \text{…. (4.0 / 2.6)}$$

From above we have for n = 2, the following equations of FLT.

(i) $5^2 = 3^2 + 4^2$ for $\left.\begin{aligned}&x = 3\\&y = 4\\&z = 5\end{aligned}\right\}$ …. at a = b = 1

(ii) $13^2 = 5^2 + 12^2$ for $x = 5$ }

$y = 12$ } …. at $a = 2$ and $b = 1$ and so on …

4.2.6 Thus FLT holds good for all integral x y and z for $n = 2$.

4.3 We will now examine various values of t for other values of $n > 2$. At $n = 3$, we have from equation (3.02):-

$$t^n = 2x^n - [1 + (-1)^n]\, p^n \quad \text{…. (3.02)}$$

i.e. $$t^3 = 2x^3 - [1 - 1]\, p^3 = 2x^3 \quad \text{…. (3.02 / 3)}$$

or $$t = x(2)^{1/3} \quad \text{…. (3.02 / 3.1)}$$

4.3.1 From above we find that at n=3, t will be a non-integer, since x as assumed earlier is an integer and $(2)^{1/3}$ is a surd. Thus at $n = 3$, we will have as per para 3.2.3, $z = p + t$ = A non integer, since p = An integer and $t \neq$ An integer.

4.3.2 Similarly for all odd values of $n > 2$, i.e. for $n = 3, 5, 7, …,$

$2m + 1$, etc., t will always be found to be non-integral, as in equation (3.02), the coefficient of p^n will be 0, whence we will have :-

$t^n = 2x^n$ or $t = x(2)^{1/n}$ = A non-integer, since $(2)^{1/n}$ = A non-integer or surd for all values of $n \geq 2$ and x = An integer.

Thus for all odd values of $n > 2$, we have from $z = p + t$ = A non-integer.

4.4 We will now examine general values of t for all values of $n > 2$. From equation (4.01), we have :-

$$t = [\,(x + p)(x^2 - p^2)(x^3 + p^3) \;….\; \{x^{n-1} - (-1)^{n-1} p^{n-1}\}\,]^{2/\{n(n-1)\}} \quad \text{…. (4.01)}$$

| ………………(n-1) terms) …………………..|

$$= A^{2/\{n(n-1)\}} \quad \text{(say)}$$

4.4.1 The R.H.S. of equation (4.01) has (n-1) terms and the index of 'A' or the total bracketed figure of R.H.S. is always a fraction less than unity for values of $n > 2$. the denominator of this fractional index shall always be a multiple of n, whence for t to be an integer the first requirement will be that at least the rational/integral n^{th} root of 'A' could be taken out. This is however just not possible as the R.H.S. of equation (4.01) has only (n-1) terms, each being different integers for assumed integral values of x and p and as after the first term no two consecutive terms are fully divisible amongst themselves, and though the first term divides all other terms, but neither the respective results of divisions are equal, the various terms being different from each other, nor the results of divisions individually or combinedly form squares, cubes, etc. of the same quantity/term, whence no n factors of same integer can be equal to the value of A or total bracketed figure of R.H.S. of equation (4.01) whence rational/integral n^{th} root of "A" is not possible at all. This means that t will never be an integer for values of $n > 2$, whence $z = p + t = A$ non integer for all values of $n > 2$, where p is an integer and t is a non-integer.

4.4.2 Thus FLT shall not hold good for all integral x, y and z for $n > 2$, where z will always be non-integral even if x and y are maintained as integers for $n > 2$.

4.4.3 Incidentally for $n = 2$, we have the following relationship from equation (4.01), as in this case the R.H.S. will have only one term.

$$t = (x + p)^{2/\{n(n-1)\}} = (x + p)^{2/\{2(2-1)\}} = x + p \quad \ldots. (4.01/n)$$

The above equation is the same as the equation (4.0/2) which was derived for $n = 2$.

5. Conclusion :-

Thus we have seen that FLT holds good, vide para 4.2.6, for all integral x, y and z for $n = 2$ and does not hold good, vide para 4.4.2, for all integral x, y and z for $n > 2$.

This proves Fermat's Last Theorem (FLT).