ISSN: 2754-6705

Journal of Mathematical & Computer Applications

Review Article

Open Access

A Simple Elementary Proof of Fermat's Last Theorem

Chandramohanan MR

Former Professor of Mathematics, Narayanaguru College of Engineering, Manjalummood, Tamil Nadu, India

ABSTRACT

In this article we attempt to describe a short proof of Fermat's Last Theorem. The Fermat's diophantine equation $x^n = y^n + z^n$ gives rise to an equation of $(n\text{-}1)^{th}$ degree, which can be proved to have no positive rational roots. This proves the case for any odd prime n. For $n = 4$ we use the principle of *reductio-ad-absurdum* along with a polynomial equation of degree 3. Further Beal's conjecture is examined and proved to be true.

***Corresponding author**

Chandramohanan MR, Former Professor of Mathematics, Narayanaguru College of Engineering, Manjalummood, Tamil Nadu, India.

Received: July 17, 2024; **Accepted:** July 23, 2024, **Published:** August 30, 2024

Keywords: Standard Notations of Algebra, FLT stands for Fermat's Last Theorem

Historical Introduction

Pierre de Fermat (20th August 1601-12th January 1665), a Frenchman of Paris had no Mathematics training and he evinced no interest in its study until he was past 30 [2,3,5].

To him it was merely a hobby to be cultivated in leisure time. Yet no practitioner of his day made greater discoveries or contributed more to the advancement of Mathematics. By profession he was a lawyer and a politician. His contributions to number theory overshadow all else. Adamently refusing to bring his work to the state of perfection and their publication, he thwarted the several efforts of others to make the results available in print under his name [2,3]. Most of what little we know about his investigations, is found in the letters to his friends or notes in the margin of whatever book he happened to be using. This habit of communicating results piece meal, usually as challenges, was particularly annoying to the Parisian Mathematicians. At one point they angrily accused Fermat of posing impossible problems and threatened to break off correspondence unless more details were forthcoming. Because his parliamentary duties demanded an ever-greater portion of his time, Fermat was given to inserting notes on the margins of his personal copy of the Bachet edition of Diophantus-Arithmatica, many of his theorems in number theory.

These were discovered five years after his death by his son Samuel, who brought out a new edition of *Arithmatica*, incorporating his father's celebrated marginalia. By far the most famous is the one written in 1637 in the margin of *Arithmatica*, which states that: It is impossible to write a cube as a sum of two cubes, a fourth power as a sum of two fourth powers and in general, any power beyond the second, as a sum of two similar powers in non-zero integers. For this, I discovered a truly wonderful proof, but the margin is too small to contain it. The above statement of Fermat is known as Fermat's Last Theorem (hereafter we write in short FLT). Despite efforts of many mathematicians and amateurs, it couldn't be proved for about 350 years. In 1955 Yuataka Taniyama of Japan announced a theory on elliptic curves, which turned out later as a link leading to a proof of FLT. After some hectic research, he published his findings in 1955 along with a conjecture, known as *Yutaka Taniyama Conjecture* (now known as Modularity Theorem). It states that, for every elliptic curve $y^2 = ax^3 + bx + c$ over the rational field $\mathbb{Q}$, there exists non-constant modular functions, $f(z)$ and $\phi(z)$ such that

$$f(z)^2 = a\phi(z)^3 + b\phi(z) + c$$

He died in 1958. Goro Shimura, a close friend of Taniyama, tried very hard for about 25 years in search of a proof of this, but could not succeed. Later Kenneth Ribet of USA made intensive research on the conjecture, but could not find the connection between the Taniyama Conjecture and the FLT. But he arrived at the conclusion that — If the Taniyama–Shimura Conjecture is true, then it should imply that the FLT is also true. During the year 1986, Andrew Wiles of Cambridge, UK got the journal in which Ribet's research was published.

On 23rd June 1993, Andrew Wiles announced a proof of FLT, but it had some flaw [5]. When all his efforts to correct the flaw failed, he returned to avail of the assistance of Richard Taylor who was once a student of Andrew Wiles and later his colleague, in research on rectifying the flaw. Together, Andrew Wiles and Richard Taylor published their proof of FLT, for international scrutiny in May 1995. The proof consists of two parts: Modular Elliptic Curves and FLT by Andrew Wiles and Ring Theoretic properties of some Hecke Algebras by Richard Taylor. Wile's proof is based on one significant point in the paper by Richard Taylor. This approach was much simpler and shorter than Wile's original proof of 1993 [5]. Still the number of pages is more than 200, whereas the original proof contained about 1000 pages. The Taniyama Conjecture was fully proved by C. Breuil, B. Conrad, F. Diamond and R. Taylor in 1999, based on the Wile's work. Now the conjecture has become a Theorem known as the Modularity Theorem.

Andrew Wiles came to the conclusion that Fermat could never have proved FLT with the limited methods available to him and that Fermat's claim of having a simple proof, was far from truth [5].

When $n = pk$ where p is prime, the Fermat's equation $x^n = y^n + z^n$ becomes $(x^k)^p = (y^k)^p + (z^k)^p$ which is of the form $u^p = v^p + w^p$. If this equation cannot have a non-trivial integer solution, then there will be no solution of the form $u = x^k$, $v = y^k$, $w=z^k$, implying that $x^n=y^n+z^n$ will not have non-zero integer solution. Thus, it is sufficient to prove FLT for n=4 and n= an odd prime. Fermat used his method of `infinite descent' to prove the impossibility of satisfying $x^4=y^4+z^4$. Euler proved FLT for $n$=3 in 1770 by using the method of `infinite descent'. Kummer proved FLT for all prime between 3 and 100 except 37, 59, 67 which are called irregular primes [5].

In this paper, we attempt to present some arguments which is probably the method for the simple proof of FLT, anticipated by Fermat in 1637.

Fermat's Last Theorem

The diophantine equation

$$x^n = y^n + z^n \tag{1}$$

has no non-trivial integer solution when n is a positive integer greater than 2.

For $n = 1$, it is trivially true, since $(p + q,p,q)$ satisfies (1) where p,q are co-primes.

For $n = 2$ we can rewrite (1) as

$$u^2 - v^2 = 1 \tag{2}$$

Where $u = \frac{x}{z}, v = \frac{y}{z}$. That is,

$$(u-v)(u+v) = 1 \tag{3}$$

Assuming x,y,z are integers, u and v will be rational numbers so that $u - v$ and $u + v$ are also rational. Therefore, we may take

$u - v = \frac{p}{q}$ and $u + v = \frac{q}{p}$, where p and q are co-primes.

Solving the last two equations we see that

$$\frac{x}{z} = u = \frac{q^2+p^2}{2qp} \quad \text{and} \quad \frac{y}{z} = v = \frac{q^2-p^2}{2qp} \tag{4}$$

so that $x = q^2 + p^2$, $y = q^2 - p^2$ and $z = 2pq$ will satisfy $x^2 = y^2 + z^2$

As a general statement we can say that $x^2 = y^2 + z^2$ has infinitely many solutions in Pythagorean triples as (i) integers (ii) rational numbers (iii) real numbers.

FLT for n = 3

$x^3 = y^3 + z^3$ implies $u^3 - v^3 = 1$ (5)

where $u = \frac{x}{z}$ and $v = \frac{y}{z}$. Also, we let $x - y = hp$, $z = hq$ where h, p, q are positive integers and p, q are coprimes. Factoring the last equation

$$(u-v)(u^2+uv+v^2) = 1 \tag{6}$$

As in Section 2, u and v are rational numbers satisfying

$$n - v = \frac{p}{q} \tag{7}$$

and then

$$u^2 + nv + v^2 = \frac{q}{p} \tag{8}$$

Since $x < y + z$ it follows that $x - y < z$ and $p < q$.

It will be shown that the last two equation (7) and (8) have no positive rational solution.

The solution of (5) will be the common solution of (7) and (8) which can be found by determining the equation of the pair of lines joining origin to the points of intersection of (7) and (8) along with (7). The required pair of lines will have equation in the form, after homegenizing the right-hand side of (8) by using (7).

$$u^2 + uv + v^2 = \frac{q}{p}(u-v)^2 \frac{q^2}{p^2}$$

$$\text{i.e. } u^2\left(\frac{q^3}{p^3} - 1\right) - 2uv\left(\frac{q^3}{p^3} + \frac{1}{2}\right) + v^2\left(\frac{q^3}{p^3} - 1\right) = 0$$

$$\text{i.e. } au^2 - 2huv + v^2 = 0 \tag{9}$$

where

$$h = \frac{q^3}{p^3} + \frac{1}{2} \tag{10}$$

and

$$a = \frac{q^3}{p^3} - 1 \tag{11}$$

Clearly h and a are rationals and $h > a > 0$ since $\frac{1}{2} > -1$ and $q > p$. By (10) and (11) we have

$$h - a = \frac{3}{2} \tag{12}$$

and

$$h + a = 2\frac{q^3}{p^3} - \frac{1}{2} \tag{13}$$

The slope $m = \frac{v}{u}$ of the lines contained in (9) is given by

$$m = \frac{h \pm \sqrt{h^2 - a^2}}{a} = \frac{h}{a} \pm \frac{b}{a} \tag{14}$$

where $b = \sqrt{h^2 - a^2} \geq 0 \Rightarrow h^2 = a^2 + b^2$ so that (h,a,b) form a Pythagorean triple of real numbers with h and a rational; it will be shown that b cannot be rational. For if b is rational then (h,a,b) is a rational Pythagorean triple, so that there exist rational numbers λ, μ such that

i) $h=\lambda^2+\mu^2, a=\lambda^2-\mu^2, b=2\lambda\mu$ or

ii) $h=\lambda^2+\mu^2, a=2\lambda\mu, b=\lambda^2-\mu^2$ or

iii) $b=0, h^2=a^2$

Case (i)

$h=\lambda^2+\mu^2, a=\lambda^2-\mu^2, b=2\lambda\mu$ (15)

In this case $h+a=2\lambda^2=\frac{2q^3}{p^3}-\frac{1}{2}$ and $h-a=2\mu^2=\frac{3}{2}$ by using (12) and (13).

That is $\mu=\frac{\sqrt{3}}{2}$ and $\lambda=\sqrt{\frac{q^3}{p^3}-\frac{1}{4}}\Rightarrow$

μ is irrational, contradicting the assumption that both λ and μ are rational $\Rightarrow (h,a,b)$ cannot be a rational Pythogorean triple $\Rightarrow b$ is irrational. Now $m=\frac{h}{a}\pm\frac{b}{a}$ is clearly irrational, since b is irrational and h,a are rational, whereas $m=\frac{v}{u}$ must be rational where $v=\frac{y}{z}$, $u=\frac{x}{z}$ and x,y,z are positive integers satisfying $x^3=y^3+z^3$.

Hence equation (9) cannot have any positive rational solution, so that (7) and (8) and hence (5) cannot have a positive rational solution ⇒ Equation (1) cannot have any positive integral solution for $n = 3$.

Alternatively, if

$$\lambda=\sqrt{\frac{q^3}{p^3}-\frac{1}{4}}=\frac{A}{B}$$

where A and B are coprimes then we have

$$A^2=4q^3-p^3 \text{ and } B^2=4p^3$$

so that B is even $=2B_0$ say

$$\Rightarrow 4B_0^2=4p^3 \text{ or } p^3=B_0^2\Rightarrow A^2+B_0^2=4q^3\Rightarrow$$

A and B_0 are both odd or both even.

If $A=2k-1$ and $B_0=2k_0-1$ are odd then we have

$$M(4)+2+M(4)=M(4) \text{ or } M(4)=2$$

a contradiction. If A and B_0 are even then A and $B=2B_0$ are also even so that 2 is a common factor of A and B . This contradiction proves that λ cannot be rational. $\therefore\lambda$ is irrational. Similarly

$$\mu=\sqrt{\frac{3}{4}}=\frac{\sqrt{3}}{2}$$

is irrational.

Now

$$b=2\lambda\mu=\sqrt{3\left(\frac{q^3}{p^3}-\frac{1}{4}\right)}=\sqrt{\frac{3\left(4q^3-p^3\right)}{4p^3}}=\frac{C}{D}$$

say where C and D are coprimes ⇒

$$C=M(3)=3C_0 \quad\text{and}\quad D=M(2)=2D_0$$

$$\therefore\frac{3C_0}{2D_0}=\sqrt{\frac{3\left(4q^3-p^3\right)}{4p^3}}\Rightarrow\frac{C_0}{D_0}=\sqrt{\frac{4q^3-p^3}{3p^3}}\Rightarrow D_0=M(3)$$

$\Rightarrow D=2D_0=M(6)\Rightarrow C$ and D are $M(3)$ a contradiction. This contradiction proves that $b=2\lambda\mu$ is irrational.

$$\therefore m=\frac{h}{a}\pm\frac{b}{a}$$

is irrational since h and a are rational but b is irrational. This proves case (i).

Case (ii)

$h=\lambda^2+\mu^2, a=2\lambda\mu, b=\lambda^2-\mu^2$ (16)

In this case we have

$$h+a=(\lambda+\mu)^2=\frac{2q^3}{p^3}-\frac{1}{2}$$

$$h-a=(\lambda-\mu)^2=\frac{3}{2} \text{ by using } (12) \text{ and } (13)$$

$$\therefore\lambda+\mu=\sqrt{\frac{2q^3}{p^3}-\frac{1}{2}} \text{ and } \lambda-\mu=\sqrt{\frac{3}{2}}$$

These imply

$4\lambda\mu=(\lambda+\mu)^2-(\lambda-\mu)^2=\frac{2q^3}{p^3}-2$ (17)

is rational but $\lambda-\mu$ is irrational ⇒ Both λ and μ cannot be rational, a contradiction to the assumption that both λ and μ are rational. Now

$$m=\frac{h}{a}\pm\frac{b}{a}=\left(\lambda^2+\mu^2\right)\pm\left(\lambda^2-\mu^2\right)=\frac{2\lambda^2}{2\lambda\mu},\frac{2\mu^2}{2\lambda\mu}$$

$\therefore m=\frac{v}{u}=\frac{\lambda}{\mu},\frac{\mu}{\lambda}$ cannot be rational, since both λ, μ cannot be rational, nor rational multiples of a monomial surd. As in case (i) it follows that (5) cannot have a positive rational solution so that FLT for n =3 holds in this case.

Alternatively, we have

$$\lambda-\mu=\sqrt{\frac{3}{2}}$$

and

$$\lambda+\mu=\sqrt{\frac{2q^3}{p^3}-\frac{1}{2}}=\frac{A}{B}$$

say where A and B are coprimes.

$$\therefore\ A^2=4q^3-p^3 \text{ and } B^2=2p^3$$

$\therefore\ B$ is even $=2B_0$ say

$$\therefore \quad 4B_0^2 = 2p^3 \text{ or } p^3 = 2B_0^2$$

and

$$A^2 = 4q^3 - 2B_0^2$$

is even ⇒ A is even. Thus, both A and B are even, a contradiction.

$\therefore$ $\lambda + \mu$ is irrational. Similarly, $\lambda - \mu$ is also irrational.

Hence if λ is rational

$$\mu = \sqrt{\frac{2q^3}{p^3} - \frac{1}{2}} - \lambda$$

is irrational and if μ is rational, then $\lambda = \mu + \sqrt{\frac{3}{2}}$ is irrational.

Also if λ and μ are rationals then both $\lambda + \mu$ and $\lambda - \mu$ are rationals. ⇒ Both λ and μ cannot be rational according to the values of $\lambda + \mu$ and $\lambda - \mu$ ⇒ Both λ and μ cannot be rational ⇒ $\frac{\lambda}{\mu}$, and $\frac{\mu}{\lambda}$ cannot be rational.

$$\therefore m = \frac{h}{a} \pm \frac{b}{a} = \frac{\lambda}{\mu}, \frac{\mu}{\lambda}$$

cannot be rational, i.e., m is irrational. This proves case (ii).

Case (iii)

$$b = 0, h^2 = a^2$$

$$\therefore h = \pm a \Rightarrow$$

$$\frac{q^3}{p^3} + \frac{1}{2} = \pm\left(\frac{q^3}{p^3} - 1\right)$$

$$\therefore \frac{q^3}{p^3} + \frac{1}{2} = -\left(\frac{q^3}{p^3} - 1\right) \Rightarrow 1\frac{q^3}{p^3} = \frac{1}{4}$$

$\therefore \frac{p}{q} = 3\sqrt{4}$ is irrational, a contradiction, since p and q are positive integer ⇒ (7) and (8) and hence (5) cannot have a positive rational solution ⇒ FLT for n=3 holds in this case. Thus, FLT holds for $n = 3$. Before considering the proof for odd $n > 3$, we need a lemma proved below.

Lemma

When n is an odd prime greater than 3

$$\tan^2\left(\frac{r\pi}{n}\right), \sin^2\left(\frac{r\pi}{n}\right) \text{ and } \cos^2\left(\frac{r\pi}{n}\right)$$

are all irrational for any positive integer r such that $0 < r \leq n$.

$$\text{Let } \theta = \frac{r\pi}{n} \text{ or } n\theta = r\pi \Rightarrow \tan n\theta = 0$$

$$\therefore \binom{n}{1} \tan\theta - \binom{n}{3}\tan^3\theta + \binom{n}{5}\tan^5\theta + \cdots + (-1)^t \tan^n\theta = 0 \quad (18)$$

where $t = \frac{n-1}{2}$

$$\therefore \binom{n}{1} - \binom{n}{3}\tan^2\theta + \binom{n}{5}\tan^4\theta + \cdots + (-1)^t \tan^{2t}\theta = 0 \quad (19)$$

The LHS is a polynomial in $\tan^2\theta$ with integer coefficients and is also a polynomial in $\tan\theta$ of degree $2t$. Since n divides each of $\binom{n}{1}, \binom{n}{3} \cdots \binom{n}{n-2}$ and n does not divide $(-1)^t$ and n^2 does not divide $\binom{n}{1}$ the polynomial in (19) is irreducible over Q the field of rational numbers, by Eisenstein's criterion [1,2,4] and the equation has no rational value for $\tan^2\theta$, for $n>3$.

Since

$$\sin^2\theta = \frac{\tan^2\theta}{1+\tan^2\theta}; \cos^2\theta = \frac{1}{1+\tan^2\theta}$$

the assertion of the lemma is true.

FLT for an Odd Prime n > 3

Assume $n = 2t + 1$ where $t \geq 2$, is a positive integer and n is a prime.

In this case, it will be proved that

$$u^n - v^n = 1 \quad (20)$$

has no positive rational solution. By factorization of (20) we can rewrite it as [5]

$$(u-v)\prod_{r=1}^{t}\left[u^2 - 2ur\cos\left(\frac{2r\pi}{n}\right) + v^2\right] = 1 \quad (21)$$

As in Sections 2 and 3 we assume

$$n - v = \frac{p}{q} \quad (22)$$

$$u^2 - 2uv\cos\left(\frac{2r\pi}{n}\right) + v^2 = \frac{q_r}{p_r} \quad (r = 1, 2, \ldots, t) \quad (23)$$

where $\frac{q_r}{p_r}$ are real numbers satisfying

$$\frac{q_1}{p_1}, \frac{q_2}{p_2}, \ldots, \frac{q_t}{p_t} = \frac{q}{p} \quad (24)$$

With each of the t quadratic equations contained in equation (23) we can adjoin equation (22) to have t pairs of simultaneous equations in u v. The common solutions of these pairs will be the solution of equation (20). By showing that none of the t pairs have a positive rational solution, it will follow that equation (20) has no positive rational solution and hence equation (1) has no non-trivial integer solution.

The above equations imply that

$$u^2 - 2uv\cos\left(\frac{2r\pi}{n}\right) + v^2 - (u-v)^2 = \frac{q_r}{p_r} - \frac{p^2}{q^2}$$

$$\text{i.e. } 4uv\sin^2\left(\frac{r\pi}{n}\right) = \frac{p^2}{q^2}\left(\frac{q^2 q_r}{p^2 p_r} - 1\right)$$

$$\text{i.e. } \frac{q^2 q_r}{p^2 p_r} - 1 = 4uv\left(\frac{q^2}{p^2}\right)\sin^2\left(\frac{r\pi}{n}\right)$$

is irrational, since $\sin^2\left(\frac{r\pi}{n}\right)$ is irrational irrespective of u, v being rational or not, for $n > 3 \Rightarrow \frac{q_r}{p_r}$ is irrational and so is

$$\frac{q^2 q_r}{p^2 p_r} - \cos^2\left(\frac{r\pi}{n}\right) = 1 + 4uv\left(\frac{q^2}{p^2}\right)\sin^2\left(\frac{r\pi}{n}\right) - \cos^2\left(\frac{r\pi}{n}\right)$$

For any particular value of r, the lines joining origin to the points of intersection of (22) and (23) is of the form

$$u^2 - 2uv\cos\left(\frac{2r\pi}{n}\right) + v^2 = \frac{q_r}{p_r}(u-v)^2\frac{q^2}{p^2}$$

That is

$$u^2\left(\frac{q^2 q_r}{p^2 p_r} - 1\right) - 2uv\left[\frac{q^2 q_r}{p^2 p_r} - \cos\left(\frac{2r\pi}{n}\right)\right] + v^2\left(\frac{q^2 q_r}{p^2 p_r} - 1\right) = 0$$

$$\text{i.e. } a_r u^2 - 2h_r uv + a_r v^2 = 0 \qquad (25)$$

where

$$h_r = \frac{q^2 q_r}{p^2 p_r} - \cos\left(\frac{2r\pi}{n}\right) \qquad (26)$$

$$a_r = \frac{q^2 q_r}{p^2 p_r} - 1 \qquad (27)$$

Clearly $h_r > a_r \geq 0$ since $1 \geq \cos\left(\frac{2r\pi}{n}\right), q > p$ $q_r > p_r$ by choice and h_r and a_r are irrational.

From (26) and (27)

$$h_r - a_r = 1 - \cos\left(\frac{2r\pi}{n}\right) = 2\sin^2\left(\frac{r\pi}{n}\right) \qquad (28)$$

and

$$h_r + a_r = \frac{2q^2 q_r}{p^2 p_r} - 2\cos^2\left(\frac{r\pi}{n}\right)$$

$$2\left[\left(\frac{q^2 q_r}{p^2 p_r}\right) - \cos^2\left(\frac{r\pi}{n}\right)\right] \qquad (29)$$

The slope $m = \frac{v}{u}$ of the lines contained in (25) is given by

$$m = \frac{h_r \pm \sqrt{h_r^2 - b_r^2}}{a_r} \qquad (30)$$

By letting $b_r = \sqrt{h_r^2 - b_r^2} \geq 0$ we have

$$m = \frac{h_r \pm b_r}{a_r} \qquad (31)$$

and

$$h_r^2 = a_r^2 + b_r^2 \qquad (32)$$

for $(r = 1, 2, \ldots, t)$

Thus (h_r, a_r, b_r) from a Pythogorean triple of real number so that there exist real numbers λ_r, μ_r such that

(i) $h_r = \lambda_r^2 + \mu_r^2$, $a_r = 2\lambda_r\mu_r$, $b_r = \lambda_r^2 - \mu_r^2$ or

(ii) $h_r = \lambda_r^2 + \mu_r^2$, $a_r = \lambda_r^2 - \mu_r^2$, $b_r = 2\lambda_r\mu_r$ or

(iii) $b_r = 0$ and $h_r = \pm a_r$

Case (i) $h_r = \lambda_r^2 + \mu_r^2, a_r = 2\lambda_r\mu_r, b_r = \lambda_r^2 - \mu_r^2$

In this case,

$$h_r + a_r = (\lambda_r + \mu_r)^2 = 2\left[\frac{q^2 q_r}{p^2 p_r} - \cos^2\left(\frac{r\pi}{n}\right)\right]$$

$$h_r - a_r = (\lambda_r - \mu_r)^2 = 2\sin^2\left(\frac{r\pi}{n}\right)$$

by using (28) and (29)

$$\therefore 4\lambda_r\mu_r = (\lambda_r + \mu_r)^2 - (\lambda_r - \mu_r)^2 = 2\left[\frac{q^2 q_r}{p^2 p_r} - 1\right]$$

is irrational ⇒ Both λ_r and μ_r cannot be rational, and cannot be monomial surds. This is a contradiction to the assumption that $m = \frac{v}{u}$ is rational, where $v = \frac{y}{z}$, $u = \frac{x}{z}$ are both rational when equation (1) has a positive integral solution.

∴ From (31)

$$m = \frac{(\lambda_r^2 + \mu_r^2) \pm (\lambda_r^2 - \mu_r^2)}{2\lambda_r\mu_r} = \frac{\lambda_r}{\mu_r}, \frac{\mu_r}{\lambda_r}$$

cannot be rational. The above contradiction proves that m cannot be rational. It follows that FLT holds in this case.

Case (ii) $h_r = \lambda_r^2 + \mu_r^2, a_r = \lambda_r^2 - \mu_r^2, b_r = 2\lambda_r\mu_r$

In this case

$$h_r + a_r = 2\lambda_1^2 = 2\left[\frac{q^2 q_r}{p^2 p_r} - \cos^2\left(\frac{r\pi}{n}\right)\right]$$

$$h_r - a_r = 2\mu_r^2 2\sin^2\left(\frac{r\pi}{n}\right)$$

$$\therefore \lambda_r = \sqrt{\frac{q^2 q_r}{p^2 p_r} - \cos^2\left(\frac{r\pi}{n}\right)} \text{ and } \mu_r = \sin\left(\frac{r\pi}{n}\right)$$

But $a_r = (\lambda_r^2 - \mu_r^2) = \frac{q^2 q_r}{p^2 p_r} - 1$ is irrational.

Hence both $(\lambda_r - \mu_r)$ and $(\lambda_r + \mu_r)$ cannot be rational.

$$\therefore m = \frac{h_r \pm b_r}{a_r} = \frac{(\lambda_r^2 + \mu_r^2) \pm 2\lambda_r\mu_r}{\lambda_r^2 - \mu_r^2}$$

$$\frac{(\lambda_r \pm \mu_r)^2}{\lambda_r^2 - \mu_r^2} = \frac{\lambda_r + \mu_r}{\lambda_r - \mu_r}, \frac{\lambda_r - \mu_r}{\lambda_r + \mu_r}$$

cannot be rational since both $(\lambda_r + \mu_r)$ and $(\lambda_r - \mu_r)$ cannot be rational, and cannot be monomial surds. This is a contradiction to the assumption that $m=\frac{v}{u}$ is rational, where $v=\frac{y}{z}, u=\frac{x}{z}$ are both rational when equation (1) has a positive integral solution. This contradiction proves that m is irrational for each r such that $0<r\le t$. As in Case (i) it follows that FLT holds in this case also.

Case (iii) $b_r=0$ and $h_r=\pm a_r$

Hence

$$\frac{q^2q_r}{p^2p_r}-\cos\left(\frac{2r\pi}{n}\right)=\pm\left(\frac{q^2q_r}{p^2p_r}-1\right)$$

$$\therefore \frac{q^2q_r}{p^2p_r}=\cos^2\left(\frac{r\pi}{n}\right) \text{ or } \cos\left(\frac{2r\pi}{n}\right)=1$$

Discarding the second condition and by letting $r=1,2,\ldots,t$ in succession and multiplying we have

$$\frac{q^{2t}q_1q_2\ldots q_t}{p^{2t}p_1p_2\ldots p_t}=\prod_{r=1}^{t}\cos^2\left(\frac{r\pi}{n}\right)$$

$$\Rightarrow \frac{q^{2t}q}{p^{2t}p}=\prod_{r=1}^{t}\cos^2\left(\frac{r\pi}{n}\right)$$

by using (24)

$$\therefore \frac{q^n}{p^n}=\prod_{r=1}^{t}\cos^2\left(\frac{r\pi}{n}\right) \qquad (33)$$

From [6] for any odd integer n we have

$$\frac{x^n-1}{x-1}=\prod_{1}^{t}\left[x^2-2x\cos\left(\frac{2r\pi}{n}\right)+1\right]$$

By letting x=-1 implies

$$1=2^{2t}\prod_{1}^{t}\cos^2\left(\frac{r\pi}{n}\right)$$

$$\Rightarrow \prod_{1}^{t}\cos^2\left(\frac{r\pi}{n}\right)=\frac{1}{2^{2t}}\frac{2}{2^n}$$

$$i.e.\quad \left(\frac{q}{p}\right)^n=\frac{2}{2^n}\Rightarrow \frac{q}{p}=\frac{1}{2}\left(\sqrt[n]{2}\right)$$

is irrational a contradiction since p,q are positive integers. Hence (22) cannot hold and (20) has no positive rational solution for each r such that $0<r\le$ t and hence FLT holds in this case also. FLT holds for $n>3$ in all the three cases.

Thus, FLT holds for all odd prime $n>3$.

FLT for $n = 4$

By letting $n=4$ in equations (5) to (10), the equation (10) becomes

$$1-m^4\frac{q^4}{p^4}(1-m)^4$$

Letting $m=\lambda+1$ or $\lambda=m-1=\left(\frac{-hp}{x}\right)$ we have

$$(\lambda+1)^4-1+\frac{q^4}{p^4}\lambda^4=0\Rightarrow\left(1+\frac{q^4}{p^4}\right)\lambda^4+4\lambda^2+6\lambda^2+4\lambda=0$$

$$\left(p^4+q^4\right)\lambda^3+2p^4\left(2\lambda^2+5\lambda+2\right)=0 \quad (34)$$

$$\left(p^4+q^4\right)\left(\frac{-h^3p^3}{x^3}\right)+2p^4\left[2\left(\frac{h^2p^2}{x^2}\right)-3\left(\frac{hp}{x}\right)+2\right]$$

$$\therefore\frac{(p^4+q^4)h^3}{p}=2x\left[2h^2p^2-3hpx+2x^2\right] \qquad (35)$$

Similarly

$$\frac{(p'^4+q'^4)}{p'}h'^3=2x\left[2h'^2p'^2-3h'p'x+2x^2\right] \qquad (36)$$

From $x^4=y^4+z^4$ we have $x\equiv y+z$ mod 2 so that x-$y\equiv z$ mod 2 and $x-z\equiv y$ mod 2 or

$$h(q-p)\equiv 0\equiv h'\left(q'-p'\right) \text{ mod } 2 \qquad (37)$$

In order to prove the falsity of $h'\equiv 0$ mod2, we consider the possibilities (i) $h'\equiv 0\equiv h$ mod2 and (ii) $h'\equiv 0\equiv (q-p)$ mod2 and prove that these conditions are invalid.

In the former possibility, we have $x-z\equiv 0\equiv$ y mod 2 and $x-y\equiv 0\equiv$ z mod 2 implying that x, y, z are even positive integers. This contradiction proves that possibilities (i) is invalid. In the possibility (ii) we have $h'\equiv 0$ mod2 and q $\equiv p$ mod2 so that h' is even and p, q are odd positive integers, since they are coprimes. Also y = $h'q'$ is even and hence x, z are odd, $h'p'$ is also even.

If q' is even then $y=h'q'=M(4)=4y_1$, say

$$\therefore x^4-z^4=(4y_1)^4 \Rightarrow (x-z)(x+z)\left(x^2+z^2\right)=256y_1^4$$

Let $x-z=2k_1y_1, x+z=2k_2y_1$ so that

$$2\left(x^2+z^2\right)=4\left(k_1^2+k_2^2\right)y_1^2 \quad\text{and}\quad x^2+z^2=2\left(k_1^2+k_2^2\right)y_1^2\Rightarrow$$

$$8k_1k_2\left(k_1^2+k_2^2\right)y_1^4=256y_1^4\Rightarrow$$

$$k_1k_2\left(k_1^2+k_2^2\right)=32 \quad (38)$$

$\therefore (k_1k_2)$ and $\left(k_1^2+k_2^2\right)$ are factors of 32.

There are five possibilities to be considered

(i) $k_1k_2 = 1$ and $k_1^2 + k_2^2 = 32$. The first condition means $k_1 = k_2 = 1$ which does not satisfy the second condition.

(ii) $k_1k_2 = 2$ and $k_1^2 + k_2^2 = 16$. This means $(k_2 + k_1)^2 = 16 + 4 = 20 \Rightarrow k_2 + k_1$ cannot be a positive integer.

(iii) $k_1k_2 = 4$ and $k_1^2 + k_2^2 = 8 \Rightarrow k_1 = k_2 = 2 \Rightarrow z = 0 \Rightarrow$ The solution for (x, y, z) is trivial with z=0.

(iv) $k_1k_2 = 8$ and $k_1^2 + k_2^2 = 4 \Rightarrow (k_2 + k_1)^2 = 20$ so that $k_2 + k_1$ cannot be a positive integer.

(v) $k_1k_2 = 16$ and $k_1^2 + k_2^2 = 2 \Rightarrow (k_2 + k_1)^2 = 34$ so that $k_2 + k_1$ cannot be a positive integer. Hence equation (38) cannot have any positive integral solution so that the assumption that q' is even, is false. $\Rightarrow q'$ is odd.

Similarly p' is odd

From (36) it may be noted that the $\text{LHS} = M(2^3)$

$$\Rightarrow x\left[2h'^2p'^2 - 3h'p'x + 2x^2\right] = M(4)$$

$$\Rightarrow 4 \text{ is a factor of } \left[2h'^2p'^2 - 3h'p'x + 2x^2\right]$$

$$\Rightarrow 2x^2 - 3h'p'x = M(4)\ (\text{since } h'p' \text{ is even})$$

$$\therefore 2x - 3h'p' = M(4)$$

so that x is even, when $h' = M(4)$ or $p' = M(2) \Rightarrow h' = M(2)$ and p' is odd.

Now RHS of (36) is $xM(4)$ and LHS = $M(8)$ at least.

$\therefore x.M(4) = M(8) \Rightarrow x$ is even.

This contradicts the earlier assertion that x is odd. This proves that the possibility (ii) is also invalid. Hence by the principle of symbolic logic we must have $h' \not\equiv 0 \bmod 2$ Similarly we can prove that $h \not\equiv 0 \bmod 2$. Now equations (37) implies $(q - p) \equiv 0 \equiv (q' - p') \bmod 2$so that p, q are odd, since they are coprimes and similarly p', q' are odd. Thus h,p,q and h', p', q' are all odd positive integers. Hence $y = h'q'$, z=hq are odd integers and hence x must be an even positive integer. We shall show that this statement is invalid. Suppose $x^4 = y^4 + z^4$ where x, y, z are positive integers such that their GCD = 1. Letting $X = x^2$, $Y = y^2, Z = z^2$ we have $X^2 = Y^2 + Z^2$ so that (X, Y, Z) form a Pythagorean triple with solution

$$X = Q^2 + P^2,\ \mathrm{Y} = Q^2 - P^2,\ Z = 2QP$$

where P, Q are coprimes (with $Q > P$) in which Y and Z can be exchanged due to symmetry. Clearly Z / Y is even so that X must be an odd integer.

$\therefore x^2$ and hence x must be an odd integer. Hence the requirement that x is even and y,z are odd, cannot be satisfied. Also y / z is even implies q / q' is even contradicting the earlier assertion that q and q' are odd. These contradictions prove that $x^4 = y^4 + z^4$ has no positive integral solution i.e. FLT is true for $n = 4'$.

The method of simple proof of FLT might be the method explained in the above Sections 3, 4 and 5.

Comparison between Beal's Conjecture and FLT

Inspired by the FLT, Andrew Beal, a banker from Texas, USA [5] proposed the following conjecture: If $x^a = y^b + z^c$ where a,b,c are positive integers and may be different as well as greater than 2 and x, y, z are positive integers, have solutions then x, y, z have a common factor greater than 2. The dissimilarity between FLT and Beal's equation is that in FLT we consider values of x, y, z such that any two of them must be co-primes, whereas in Beal's equation, no two of them are co-primes but all of them have a common factor greater than 2.

Without loss of generality we assume Max$(a,b,c) > 2$ and there is an initial solution of Beal's equation without a common factor of x, y, z. Let L = LCM (a,b,c) so that there exists positive integers a', b', c' such that $L = aa' = bb' = cc'$. Choose m= Min (a', b', c'). Multiplying the initial Beal's equation by p^L where p is any odd prime or an even integer from the set {2,4,8,16,32,...} if m ≥ 2 or from the set {4,8,16,32,...} if $m = 1$. We note that p^m will be a common factor of the new x,y,z since $p^Lx^a = (p^{a'}x)^a$, $p^Ly^b = (p^{b'}y)^b$ and $p^Lz^c = (p^{c'}z)^c$ implies that p^m is common for the new values of x,y,z. Since L has either an odd prime or 4 as a factor when Max $(a,b,c) > 2$ there will be at least one choice of p such that p^m is a common factor of new x, y, z after multiplication of the initial Beal's equation by p^L. As examples, consider

$$3^2 = 2^3 + 1^3 \qquad \text{(i)}$$

and

$$5^3 = 11^2 + 2^2 \qquad \text{(ii)}$$

Multiplying these by 3^6 the results are $81^2 = 18^3 + 9^3$ and $45^3 = 297^2 + 54^2$ so that the common factor is 9. Multiplying (i) and (ii) by 2^6 the results are $24^2 = 8^3 + 4^3$ and $20^3 = 88^2 + 16^2$ so that the common factor is 4. Hence Beal's conjecture is true in general since Max (a, b, c) > 2 and p is chosen as stated above.

References

1. Archbold J (1972) Algebra, ELBS and Pitman, London.
2. https://archive.org/details/algebra0000arch/page/n5/mode/2up
3. Burton DM (2007) The History of Mathematics, an Introduction, McGrew Hill, New York.
4. Escofier JP (2001) Galois Theory, Springer-Verlag, New York.
5. Hassanabba BA (2015) Incredible Mathematical Stories, Prism Books Pvt. Ltd., Bangaluru.
6. Loney S (2019) Plain Trignometry (Parts I & II), AITBS Publishers, Delhi.

Copyright: ©2024 Chandramohanan MR. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.