The Mathematics Education **ISSN 0047-6269**
Volume - LV, No. 1, March 2021
Refereed and Peer-Reviewed Quarterly Journal
Journal website : www.internationaljournalsiwan.com

A Brief Review of the Solution of Fermat's Last Theorem

by **Md. Shamshad Alam,** *Research Scholar,*
Department of Mathematics,
Jai Prakash University, Chapra - 841301
E-mail : md.786shamshadalam@gmail.com
&
L.B. Singh, *Retd. Associate Professor,*
Department of Mathematics,
Jai Prakash University, Chapra - 841301
E-mail : lbsdmjpu@gmail.com

Abstract :

In this paper, we deal with a historical note concerning Fermat's last theorem. Erickson Martin & Vazzana Anthony : Introduction to number theory, Chapman & Hall / CRC, Taylor & Francis Group, Boca Raton London, First Indian Reprint 2009 [1]. First we consider it in historical perspective. We consider an important theorem and graph of elliptic curves.

Keywords : Non-zero positive integers, elliptic curve, graph of curves.

1. Introduction :

A historical note concerning Fermat's last theorem :

Definition : If a, b, c are non-zero positive integers, Gauss and Euler shown that the equation

$$a^3 + b^3 = c^3$$

has no solution. Fermat showed in 1637 that the equation

$$a^4 + b^4 = c^4$$

has no solution.

In case of exponent 5 i.e.

$$a^5 + b^5 = c^5$$

It was shown to be unsolvable by Dirichet and Legendre. But according to Fermat's last theorem the equation

$$a^n + b^n = c^n$$

has no solution in positive integer if $n \geq 3$.

This theorem was stated more than 350 years. But after that many mathematicians tried to solve it but got no success. But in that process they made important contributions. Sophie Germain in 1823 prove that if both p and $2p + 1$ are primes then the equation $a^p + b^p = c^p$ has no solution in integers a, b, c with p not dividing abc. In 1909, A. Wieferich came to some conclusion if $2p - 2$ is not divisible by p^2. In later part of 19th century some eminent mathematicians like Dedekind, Kummer, etc. developed a new branch of mathematics called algebraic number theory. With its help they could solve Fermat's last theorem for many exponents. But they could not give general proof. In 1985, L.M. Adleman, D.R. Heath Brown and E. Fouvry used Germain's Criterion to prove that there are infinitely many primes p such that $a^p + b^p = c^p$ has no solutions with p not dividing abc.

In 1986, Gerhard Frey gave a different line of attack to solve Fermat's theorem. He used a notion called modularity and theory of elliptic curves.

Elliptic curves are third degree equations of form $y^2 = x^3 + ax^2 + bx + c$

Where numbers a, b, c are fixed and we have to find values of x and y.

Elliptic curves are also called "abelian varieties of dimension one". Some of the curves are

$$E_1 : y^2 = x^3 + 17$$

$$E_2 : y^2 = x^3 + x$$

$$E_3 : y^2 = x^3 - 4x^2 + 16.$$

Above examples have solution in integers, as given below :

E_1 has the solutions (-2, 3), (-1, 4) and (2, 5)

E_2 has the solution (0, 0)

E_3 has the solutions (0, 4) and (4, 4)

These solutions can be found by trial and error. In cases of E_1 and E_3 we start with small values of x and check if cubic turns out to be a perfect square.

Case of E_2 is different and we give a formal proof.

Theorem (1.I) : Only $(x, y) = (0, 0)$ is the point with rational co-ordinates on the elliptic curve $y^2 = x^3 + x$.

Proof : Let us suppose that there is a non-zero rational solution. Let $x = \frac{a}{b}, y = \frac{c}{d}$, a, b, c, d being all non-zero integers, and fractions $\frac{a}{b}$ and $\frac{c}{d}$ are in lowest terms.

Then $\dfrac{c^2}{d^2} = \dfrac{a^3}{b^3} + \dfrac{a}{b}$

$$\Rightarrow \quad c^2b^3 = a^3b^2 + ab^2d^2 \tag{1}$$

Let $ad - bc = m$ and $a + d = n$

Then m, n are integers.

Also, $d = n - a$ and $a(n - a) - bc = m$

Hence $bc = an - a^2 - m$

Also $ad = an - a^2$

(1) can be written as

$$(bc)^2b = (ad)^2a + (ad)(b^2d)$$

Hence $(an - a^2 - m)^2b = (an - a^2)^2a + (an - a^2)b^2(n - a)$

Let $an - a^2 = l$, an integer

Then $(l - m)^2b = l^2a + \frac{l^2b^2}{a}$

Since l, m are integers, so is $l - m$.

Now rationalising above equation $(l - m)^2ba = l^2a^2 + l^2b^2$

Or $$l^2b^2 - (l - m)^2ba + l^2a^2 = 0$$

This is a quadratic in b whose discriminant is

$$(l - m)^4\, a^2 - 4l^2.l^2a^2 = a^2[(l - m)^4 - 4l^4]$$

For integral value of b, this expression must be a perfect square i.e.

$$(l - m)^4 - 4l^4 = k^2,\ k \text{ being an integer}$$

$$\Rightarrow \quad (l - m)^4 = 4l^4 + k^2$$

Putting $k = x$, $l = v$ and $u = l - m$, we get

$$x^2 + 4v^4 = u^4$$

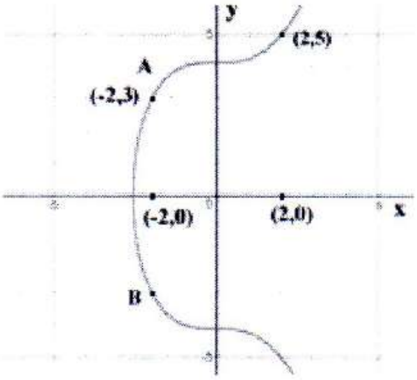
In Silverman's book [4], on P. 206, we get this equation whose solution has been proved to be impossible.

Hence b does not have integral value. So there is no non-zero rational solution. This means that (0, 0) is the only point with rational co-ordinates.

2. Graphs of Curves :

To visualise three curves we give graphs of elliptic curves

When $x = 0, y^2 = 17$ or $y = \pm\sqrt{17}$ $(\sqrt{17} > 4)$



$$E_1 : y^2 = x^3 + 17$$

Thus points A and B on y-axis are $(0, \sqrt{17})$ and $(0, -\sqrt{17})$

$$y = 0 \Rightarrow x^3 = -17 \Rightarrow x = -(17)^{1/3}$$

For point C on x-axis, its co-ordinates are $(-(17)^{1/3}, 0)$. Clearly $-(17)^{1/3} < -2$.

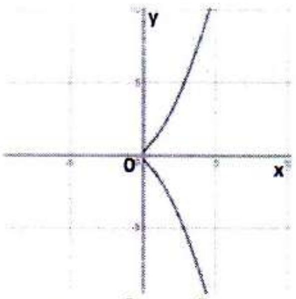
Curve is symmetrical about x axis since if (x, y) is on curve, then $(x, -y)$ is also on the curve.

If x Increases indefinitely, then y also Increases indefinitely.

As we see curve passes through origin and is symmetrical about x axis since

$$y^2 \geq 0, x + x^3 \geq 0$$

$$\Rightarrow \quad x \geq 0.$$



$$E_2 : y^2 = x^3 + x$$

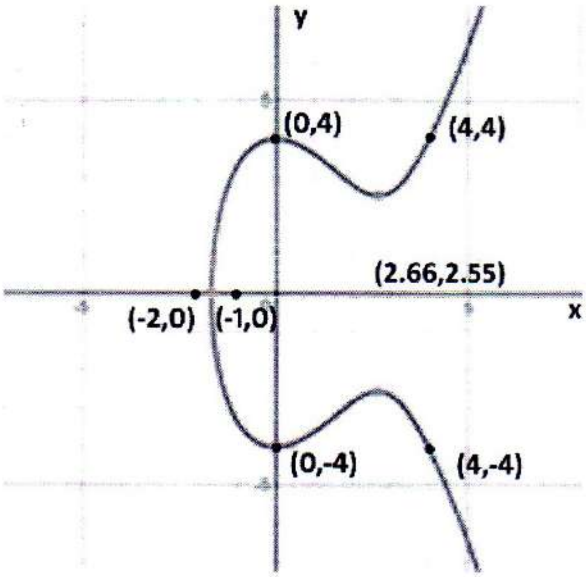
As x Increases indefinitely, so does y.

Here $y^2 = x^2(x - 4) + 16$

So when $x = 0$ or $x = 4$, $y^2 = 16$

$\Rightarrow \quad y = \pm 4$

Hence (0, 4), (0, -4), (4, 4), (4, -4) lie on curve.



$$E_3 : y^2 = x^3 - 4x^2 + 16$$

Also if $x = -1$, $y^2 = -5 + 16 = 11$

$x = -2$, $y^2 = 4(-6) + 16 = -8$

Hence curve meets x axis between points (-1, 0) and (-2, 0).

Let $f(x) = x^3 - 4x^2 + 16$

Then $f'(x) = 3x^2 - 8x = x(3x - 8)$ and $f''(x) = 6x - 8$

Hence $f'(x) = 0$ when $x = 0$ and $x = \dfrac{8}{3}$

If $x = 0$, $f''(x) = -8 < 0$ i.e. maximum value of $f(x)$.

Hence for maximum value of y, $y^2 = 16$

$$\Rightarrow \quad y = 4 \text{ at point } A.$$

If $x = \frac{8}{3}$, $f''(x) = 6 \times \frac{8}{3} - 8 = 8 > 0$.

So minimum y is attained on the right side of x axis when $x = \frac{8}{3}$

Then $y^2 = \frac{64}{9}\left(-\frac{4}{3}\right) + 16 = \frac{176}{27} = 6\frac{14}{27}$ then $2 < y < 3$, $y \cong 2.55$.

References :

1. Erickson Martin & Vazzana Anthony : Introduction to number theory, Chapman & Hall / CRC, Taylor & Francis Group, Boca Raton London, First Indian Reprint 2009.

2. Kishan Hari : Number theory, Krishna Prakashan Media (P) Ltd., Krishn House 11, Shivaji Road, Meerut - 250001 (U.P.), India.

3. Malik, S.B. : Basic Number theory, Second Revised Edition, Vikas Publishing House (P) Ltd., Noida (U.P.), India.

4. Silverman J.H. : A friendly Introduction to Number Theory, Pearson Prentice Hall, (3rd edition 2006).