Int. J. Open Problems Compt. Math., Vol. 7, No. 4, December 2014
ISSN 1998-6262;
www.i-csrs.org

Proof of Fermat Last Theorem based on Odd Even Classification of Integers

Vinay Kumar

Professor, Vivekananda School of Information Technology,
Vivekananda Institute of Professional Studies,
SGG Indraprastha University, New Delhi 110 088, India
e-mail: vinay5861@gmail.com, vinay.kumar@vips.edu

Received 28 May 2014; Accepted 20 October 2014

Abstract

In the middle of 17th century, Pierre de Fermat mentioned that no value of n > 2 could satisfy the equation $x^n + y^n = z^n$, where n, x, y and z are all positive integers. The statement is popularly known as Fermat's last theorem. An acceptable mathematical proof of this theorem is being explored still today. When searched online treasures of resources, one may find various proofs of this theorem. In this paper I am not discussing any historical attempts that failed or partially succeeded. I am going to discuss the approach which I have adopted to proof this theorem. The approach is based on odd-even classification of positive integers. Assumption that the equation $x^n + y^n = z^n$, where n, x, y and z are all positive integers, has a solution for n > 2 leads to some contradiction.

Keywords: *Fermat's last theorem, odd-even classification, Fermat's general proof, method of contradiction.*

1 Introduction

Pierre de Fermat, in 17th century, wrote an equation that is now popularly known as Fermat's Last Theorem (FLT). This he did while studying Arithmetica, an ancient Greek text written in about AD 250 by Diophantus of Alexandria [1, 2]. This is a manual on number theory, the purest form of mathematics, concerned with the study of whole numbers, the relationships between them, and the patterns they form [16]. The page of Arithmetica which inspired Fermat to create the last theorem discussed various aspects of Pythagoras' theorem, which states, "In a right-angled triangle the square of the hypotenuse is equal to the sum of the squares on the other two sides." In symbolic form, the Pythagoras's theorem is written as

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

where z is the length of the hypotenuse, the longest side, and x and y are the lengths of the other two sides in a right angle triangle. In particular, Arithmetica asked its readers to find solutions to Pythagoras' equation, such that x, y, and z could be any whole number, except zero [5, 6]. There are many solutions to this equation as proved in the Section 3 of this paper. The general statement of this equation is known as Fermat's last theorem (FLT), which states that for all *n* greater than 2, there does not exist *x*, *y*, *z* such that

$$x^n + y^n = z^n \quad \text{………………………………………………} (1)$$

Here *x*, *y*, *z* and *n* are positive integers. Until mid-1990s, this was the most famous unsolved problem in Mathematics. Fermat believed he could prove his theorem, but he never committed his proof to paper. After his death, mathematicians across Europe tried to rediscover the proof of Fermat's Last Theorem. It was as though Fermat had buried an incredible treasure, but he had not written down the map [12]. Mathematicians could not resist the lure of such an intellectual treasure and competed to find it first. "I have found a remarkable proof of this fact, but there is not enough space in the margin of the book to write it", Fermat claimed [1, 11]. There are many stories in support and in against of the claim [7, 9, 12]. I am not going to discuss anything like that in this paper. For more than 300 years, no one was able to find a proof although various attempts produced numerous results and some fields of mathematical studies [3, 4].

In summer of 1993, a proof was announced by Princeton University mathematics professor Andrew Wiles. Actually, Wiles announced a proof of a special case of the Shimura-Taniyama Conjecture -a special case that implies FLT [1, 10, 21]. Wiles' proof was 200 pages long and had required more than seven years of dedicated effort. A gap in the proof was discovered later that summer, but Wiles, working with Richard Taylor, was able to fill it by the end of September 1994 [17, 18]. Are mathematicians finally satisfied with Andrew Wiles's proof of Fermat's Last Theorem? Why has this theorem been so difficult to prove? These are still some unanswered questions [13, 14]. Without discussing merits and demerits of the proofs provided by Wiles, I am writing my own proof of FLT.

In this paper, a simple proof is provided for n = 1, n = 2, n = 3, n = 4 and then for n = m. For n = 1, 2 solution exists whereas for n > 2, there is no solution. In Equation (1), we can write y and z as (x + a) and (x + b) respectively for some positive integers a and b such that b > a. This is without any loss of generality. Thus, Equation (1) can be written as below.

$$x^n + (x + a)^n = (x + b)^n \quad \text{………………………………..…………} (2)$$

Where *x*, a, b, *n*, are positive integers. Also for n = 1, x = (b – a) and for n ≥ 2, x > (b – a). The proof consists of two parts: existence of solution for n = 1, 2 and non-existence of solution for n > 2. It is proved in the paper that there exist positive integer x for some positive integers a, b and a < b such that Equation (2) is true when n = 1, 2.

In order to prove the FLT i.e. non-existence of solution to Equation (2) for n > 2, Equation (2) can be written as

$$x^n = (b - a)\left[{}^nC_1 x^{n-1} + {}^nC_2 x^{n-2}(b+a) + {}^nC_3 x^{n-3}(b^2 + a^2 + ab) + \ldots (b^{n-1} + b^{n-2}a + \ldots + a^{n-1})\right]$$

Or, $x^n = (b - a) * q$ ……………………………..……………… (3)

where q is a positive integer and (b – a) << q. Three integers: x, a, b involved in the Equation (3), are either even or odd positive integers. The possible odd-even classification of x, (b – a), q and resultant feasibilities of a solution to Equation (3) are tabulated in the Table 1.

Table 1: Possible even-odd values of variables involved

Sl No	x	a	b	x^n	(b – a)	q	$x^n = (b - a) * q$
1	E	E	E	E	E	E	@
2	E	E	O	E	O	O	Not Possible
3	E	O	E	E	O	O	Not Possible
4	E	O	O	E	E	?	
5	O	E	E	O	E	***D***	Not possible
6	O	E	O	O	O	O	
7	O	O	E	O	O	O	
8	O	O	O	O	E	***D***	Not possible

In the Table 1, ***D*** stands for 'Do not care'. It means that irrespective of whether q is odd or even, product in right hand side of Equation (3) i.e. [q * (b – a)] is even and therefore no solution is feasible in these cases. Similarly no solution is possible in case of serial no. 2 and 3. At the serial no 4, '?' indicates that value could be odd or even depending on whether n is odd or even; and '@', at serial no 1, indicates the case that it is one of the remaining 7 cases after canceling out the even factors from both sides of Equation (3). Thus in order to prove the FLT, we have to prove that there exists no x to satisfy the Equation (3) even in cases at serial no 4, 6 and 7 of the Table 1.

This paper is organized in six sections. The existence of solution for n = 1 and n = 2 is proved in Section 2. The proof of non-existence of solution of the Fermat's Last theorem for n = 3 is described in the Section 3 and for n= 4 in Section 4. The Section 5, deals with general proof of Fermat's Last theorem for any positive integer n > 2. The paper is concluded in the Section 6. Finally, it is mentioned in the Section 7 that the problem is open problem to the extent that another simpler proof may still be found, however the question that there exists no mathematical proof of FLT is solved herewith.

2 Proof of Existence of Solutions for n = 1 and n = 2

Consider the Equation (2) for $n = 1$. It is $x = b – a$. Since integers b and a are positive integers and $b > a$, there exists many positive integers such that

$x + y = z$

It also follows from the closure property of the set of positive integers under the binary operation of addition of integers.

Now let us consider the Equation (2) for $n = 2$. The Equation (2), in this case, becomes

$$x^2 = 2x(b – a) + (b^2 – a^2) \quad \ldots\ldots\ldots\ldots \quad (4)$$

where *x*, a, and b are positive integers. Once the equation is solved for x in terms of a and b, we get

$$x = (b – a) \pm \sqrt{2b(b-a)} \quad \ldots\ldots\ldots\ldots \quad (5)$$

We can find infinite number of pairs of positive integers (a, b) such that x is a positive integers and thereof y and z are positive integers satisfying the Equation (1) for $n = 2$. For instance for $a = 1$, $b = 2$, we have $x = 3$, $y = 4$ and $z = 5$. These values of x, y and z satisfy the Equation (1).

3 Proof of Nonexistence of Solutions for n = 3

Let us now consider the case of $n = 3$. In this case, Equation (3) turns out to be

$$x^3 = (b – a) * q \quad \ldots\ldots\ldots\ldots \quad (6)$$

where

$$q = (3x^2 + 3x(b + a) + b^2 + a^2 + ab) \quad \ldots\ldots\ldots\ldots \quad (7)$$

Take the case 4 of the Table 1, wherein x is even and a and b are odd. In this case $(b – a)$ is even and q is odd. If there exist a positive integer solution of Equation (2) for $n = 3$, then RHS of Equation (6) is a perfect cube of some positive integer i.e. $\exists$ some positive integers a and b such that $(b – a)*q$ is cube of integer x.

Lemma 1: A positive even integer can be written as $2^k * p$, where p is an odd positive integer and k is any positive integer.

Proof: For a positive even integer x, $\exists$ a positive integer m such that $x = 2m$. If m is odd then it is proved otherwise $m = 2m_1$. If m_1 is odd then it is proved otherwise $m_1 = 2m_2$. Similarly, we extend the process to K^{th} steps such that m_k is either 1 or an odd positive integer. Thus x can be written as

$x = 2^k * m_k$ [end of the proof of lemma]

For RHS, in Equation (7), to be a perfect cube, $(b – a)$ must be an odd multiple of 2^{3k} for some positive integer k i.e.

$$(b - a) = 2^{3k} * p \qquad \text{………………………………………} \quad (8)$$

Substituting for $(b – a)$ in Equation (6) from Equation (8), we have

$$x^3 = 2^{3k} * (p * q) \qquad \text{………………………………………} \quad (9)$$

If $p = 1$ and q is a prime number then there is no solution, therefore assume that $(p * q)$ is a composite odd number such that it is a cube of an odd positive integer r i.e. $(p * q) = r^3$. It shows that there is a solution to the Equation (2) for $n = 3$, if and only if q is a composite integer of possibly many factors in such a way that $(p * q)$ is a cube of a positive integer r. Therefore, q can be written as product of two odd integers: q_1 and q_2; i.e.

$$(3x^2 + 3x(b + a) + b^2 + a^2 + ab) = q_1 * q_2 \text{ --------------------- } (10)$$

We can always find two odd integers α and β such that q_1 and q_2 can be written as $(x + \alpha)$ and $(3x + \beta)$ respectively. This implies that $\exists$ some odd integers (either positive or negative) α and β such that Equation (10) is valid. The Equation (10) now can be written as

$$(3x^2 + 3x(b + a) + b^2 + a^2 + ab) = (x + \alpha) * (3x + \beta) \text{ ………}(11)$$

Solving Equation (11) we get,

$$(3x^2 + 3x(b + a) + b^2 + a^2 + ab) = 3x^2 + (\alpha + 3\beta)\, x + \alpha\beta$$

i.e.

$$\alpha + 3\beta = 3(a + b), \text{ and}$$

$$\alpha\beta = b^2 + a^2 + ab$$

Using the two results, we have

$$(\alpha - 3\beta)^2 = -3\,(b - a)^2$$

This is a contradiction, because square of an integer cannot be negative. Thus there exist no integers α & β such that Equation (11) becomes true. This implies that RHS of Equation (6) is not a perfect cube and therefore there exists no solution to Equation (2) for n = 3 when x is even, a is odd and b is odd.

4 Proof of Nonexistence of Solutions for n = 4

Let us now consider the case for n = 4. In this case Equation (3) turns out to be

$x^4 = (b – a) * q$ …..…………………………………… (12)

where

$q = [4x^3 + 6x^2 (b + a) + 4x(b^2 + a^2 + ab) + (b^3 + a^3 + b^2a + ba^2)]$ ..…………(13)

Take the case in serial no. 4 in the Table 1, wherein x is even integer and a & b are odd integers. In this case (b – a) is even and q is also even. If there exist a positive integer solution of Equation (2) for n = 4, then RHS of Equation (12) must be an integral power 4 of positive integer x i.e. ∃ positive integers a and b such that (b – a)*q is integral power of x raised to the power 4.

The expression (b – a)*q in the RHS in Equation (12) is an odd multiple of some integral power of 2 (from lemma 1). For (b – a)*q to be an integral power 4 of x, (b – a)*q must be an odd multiple of 2^{4k} (from lemma 1), for some positive integer k i.e.

$(b – a)*q = 2^{4k} * p$ …..………………………………….. (14)

where p is an odd integer. Using this result in Equation (14), we have

$x^4 = 2^{4k} * p$ ……..………………………(15)

Here p is greater than 1, it is proved in lemma 2 below.

Lemma 2: The odd integer p in Equation (15) is greater than 1.

Proof: When x is even, a is odd and b is odd, (x + a) and (x + b) are odd integers. From Equation (12) it is obvious that (b – a)*q is difference of 4^{th} power of (x + a) and 4^{th} power of (x + b). If (x + a) = 2m + 1 and (x + b) = 2n + 1, then

$(2n + 1)^4 – (2m + 1)^4 = 2^3 (n – m) (n + m + 1) [2m^2 + 2n^2 + 2(m + n) + 1]$ ………. (15A)

Since x is a positive even integer, a & b are positive odd integer and b > a, n and m must be ≥ 1. Therefore irrespective value of n and m, the least odd factor is $[2m^2 + 2n^2 + 2(m + n) + 1]$ and it is > 1 for any such positive integers x, a and b. (End of proof)

If p is a prime number then there is no solution, therefore assume that p is a composite odd number such that it is an integral power 4 of some odd positive integer r i.e. $p = r^4$. This implies that q can be factored into many integers possibly some even and some odd i.e. there is an integer solution to the Equation (2) for n = 4, iff q is a composite integer of at least four positive integers factors. This implies that q can be written as product of three positive integers: q_1, q_2 and q_3; i.e.

$$[4x^3 + 6x^2 (b + a) + 4x(b^2 + a^2 + ab) + (b^3 + a^3 + b^2a + ba^2)] = q_1*q_2*q_3 \quad \ldots.(16)$$

We can always find three integers α, β and γ such that q_1, q_2 and q_3 can be written as $(2x + \alpha)$, $(2x + \beta)$ and $(x + \gamma)$ respectively. This is without loss of any generality. This implies that $\exists$ some integers (either positive or negative) α, β and γ such that Equation (16) is valid and it can be written as

$$[4x^3 + 6x^2 (b + a) + 4x(b^2 + a^2 + ab) + (b^3 + a^3 + b^2a + ba^2)]$$
$$= (2x + \alpha) (2x + \beta) (x + \gamma) \ldots\ldots\ldots\ldots(17)$$

Solving the following Equation (17) we get,

$$[4x^3 + 6x^2 (b + a) + 4x(b^2 + a^2 + ab) + (b^3 + a^3 + b^2a + ba^2)]$$
$$= 4x^3 + 2x^2 (\alpha + \beta + 2\gamma) + x (\alpha\beta + 2\alpha\gamma + 2\beta\gamma) + \alpha\beta\gamma$$

i.e.

$$\alpha + \beta + 2\gamma = 3 (b + a) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots (18)$$

$$\alpha\beta + 2\alpha\gamma + 2\beta\gamma = 4(b^2 + a^2 + ab) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots (19)$$

$$\alpha\beta\gamma = (b^3 + a^3 + b^2a + ba^2) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots (20)$$

Eliminating α and β from Equation (19) using Equations (18) and (20), we get the following cubic Equation in γ,

$$4\gamma^3 - 6\gamma^2 (b + a) + 4\gamma (b^2 + a^2 + ab) - (b^3 + a^3 + b^2a + ba^2) = 0 \ldots\ldots (21)$$

Multiplying the Equation (21) with (b – a) we get,

$$4\gamma^3 (b - a) - 6\gamma^2 (b^2 - a^2) + 4\gamma (b^3 - a^3) - (b^4 - a^4) = 0 \quad \ldots\ldots\ldots (22)$$

Adding and subtracting γ^4 in the LHS of the Equation (22) and rearranging it, we get

$$(\gamma - b)^4 = (\gamma - a)^4 \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (23)$$

It means either b = a or $\gamma = (b + a)/2$. Since $b \neq a$, only possibility is that $\gamma = (b + a)/2$. Using this value of γ in Equations (18) and (19) we get,

$\alpha + \beta = 2(b + a)$, and

$\alpha\beta = 2(b^2 + a^2)$

Using the two results, we have

$(\alpha - \beta)^2 = -4(b - a)^2$

It means $(\alpha - \beta)$ is imaginary i.e. it is not even real. Thus there exists no integers α & β such that Equation (17) becomes true. This implies that RHS of Equation (12) is not an integral power 4 of an integer. Hence there exists no solution for Equation (2) for even x, odd a and odd b when n = 4.

Now consider the cases corresponding to serial no. 6 in the Table 1 wherein x is odd, a is even and b is odd. In this case (b – a) is odd and q is also odd. Similar is the case for serial no. 7 in the Table 1 wherein x is odd, a is odd and b is even. Since (b – a) << q, for Equation (12) to be valid q must be composite number in such a way that (b – a)q is an integral power 4 of some odd integer. Therefore the remaining proof is the same as in the case of row 4 (except that all factors of q in this case are odd integers) of the Table 1. It implies that there is no solution for FLT for n = 4.

5 Proof of Nonexistence of Solutions for n = m

Let us now consider the case of n = m, where m > 4. In this case Equation (3) turns out to be

$$x^m = (b - a) * q \qquad \ldots\ldots (24)$$

where

q =

$$\left[{}^mC_1x^{m-1} + {}^mC_2x^{m-2}(b+a) + {}^mC_3x^{m-3}(b^2 + a^2 + ab) + \ldots(b^{m-1} + b^{m-2}a + \ldots + a^{m-1})\right]$$

Take the case of serial no. 4 in the Table 1, wherein x is even and a and b are odd. In this case (b – a) is even and q is either even or odd depending upon whether k is even or odd. If there exist a positive integer solution of Equation (2) for n > 4, then RHS of Equation (24) is an integral power m positive integer x i.e. $\exists$ some positive integers a and b such that (b – a)*q is integral power of x raised to the positive integer m.

If q is even, then for RHS to be an integral power m of such integer x, (b – a)*q must be an odd multiple of 2^{mk} (from lemma 1), for some positive integer k i.e.

$$(b - a)*q = 2^{mk} * p \qquad \ldots\ldots (25)$$

where p is an odd integer. Using this result in Equation (24), we have

$$x^m = 2^{mk} * p \qquad \ldots\ldots (26)$$

Here p is always greater than 1 as proved in lemma 2. If p is a prime number then there is no solution, therefore assume that p is a composite number such that it is an integral power m of some odd integer i.e. q is a composite integer such that it is product of at least m positive integers. This implies that there is a solution to the Equation (2) for n = m, iff q is a composite integer and it is product of at least m positive integers factors. Therefore, q can also be written as product of two positive integers: q_1 and q_2 such that

$$\left[{}^{m}C_1x^{m-1}+{}^{m}C_2x^{m-2}(b+a)+{}^{m}C_3x^{m-3}(b^2+a^2+ab)+...(b^{m-1}+b^{m-2}a+...+a^{m-1})\right]$$

$$= q_1 * q_2$$

Similarly, if q is odd, then (b – a) being even, must be an odd multiple of 2^{mk} for some positive integer k i.e. $(b – a) = 2^{3k} * t$, for some odd positive integer t. This means t*q is integral power m of some odd positive integer u in such a way that

$$x^m = 2^{mk} * u^m$$

There is a solution to the Equation (2) for n = m, iff q is a composite integer of possibly many positive integer factors. Since there are many integer factors, q can be written as product of two positive integers: q_1 and q_2 such that

$$\left[{}^{m}C_1x^{m-1}+{}^{m}C_2x^{m-2}(b+a)+{}^{m}C_3x^{m-3}(b^2+a^2+ab)+...(b^{m-1}+b^{m-2}a+...+a^{m-1})\right]$$

$$= q_1 * q_2$$

It means that whether q is odd or even, q can be written as product of two positive integers q_1 and q_2. These two integers q_1 and q_2 can be expressed in terms of x as $(mx^{m-2} – \alpha)$ and $(x – \beta)$ respectively. Using this fact, we have

$$\left[{}^{m}C_1x^{m-1}+{}^{m}C_2x^{m-2}(b+a)+{}^{m}C_3x^{m-3}(b^2+a^2+ab)+...(b^{m-1}+b^{m-2}a+...+a^{m-1})\right]$$

$$= (mx^{m-2} - \alpha)\ (x - \beta)$$

$$= mx^{m-1} - m\beta x^{m-2} - \alpha x + \alpha\beta) \qquad \text{………………} (27)$$

From Equation (27), we have

$$- m\beta = {}^{m}C_2\,(b + a) \qquad \text{………………..}(28)$$

$$- \alpha = b^{m-2} + b^{m-3}a + ...+ a^{m-2} \qquad \text{……………….} (29)$$

$$\alpha\beta = b^{m-1} + b^{m-2}a + ... + a^{m-1} \qquad \text{……………………..} (30)$$

From Equations (28) and (29), we get

$$\alpha\beta = \frac{(b^{m-1} - a^{m-1})\ (b+a)\ (m-1)}{2(b-a)}$$

and from Equation (30), we have

$$\alpha\beta = \frac{(b^m - a^m)}{(b-a)}$$

Equating these two values we have,

$$\frac{(b^{m-1} - a^{m-1})\,(b+a)\,(m-1)}{2(b-a)} = \frac{(b^m - a^m)}{(b-a)}$$

Or, $2b^m - 2a^m = (m-1)\,[b^m - ba^{m-1} + ab^{m-1} - a^m]$

Or, $(3-m)\,(b^m - a^m) = (m-1)\,ab\,(b^{m-2} - a^{m-2})$

Or, $$\frac{b^m - a^m}{b^{m-2} - a^{m-2}} = \frac{m-1}{3-m}ab \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ (31)$$

For positive integers a and b such that b > a, LHS of Equation (31) is a positive real number where as RHS of the equation is a negative real number because m > 4 (and therefore 3 – m < 0). Therefore, Equation (31) is a contradiction. This contradiction is because of the initial assumption that equation (2) has a solution for n = m in the case corresponding to serial no. 4 of the Table 1. Hence there is no solution for Equation (2) in this case for n = m.

Now consider the cases corresponding to serial no. 6 in the Table 1 wherein x is odd, a is even and b is odd. In this case (b – a) is odd and q is also odd. Similar is the case corresponding to serial no. 7 in the Table 1 wherein x is odd, a is odd and b is even. Since (b – a) << q, for Equation (24) to be valid q must be composite number in such a way that (b – a)*q is an integral power m of some odd integer. Therefore the remaining proof is the same as in the case of serial no. 4 (except that all factors of q in this case are odd integers) of the Table 1. It implies that there is no solution for FLT for n = m.

6 Conclusion

There can be no problem in the field of physics, chemistry or biology that has so vehemently resisted attack for so many years. E.T. Bell predicted that civilization would come to an end as a result of nuclear war before Fermat's Last Theorem would ever be resolved. Fermat claimed that he had the proof but no record of it has ever been found. Ever since that time, countless professional and amateur mathematicians have tried to find a valid proof (and wondered whether Fermat really ever had one). Then in 1994, Andrew Wiles of Princeton University announced that he had discovered a proof while working on a more general problem in geometry. He came out with a proof that is very lengthy and cumbersome proof. Many doubt it as a mathematical proof of the theorem [13, 15].

There is no royal road to logic. Really valuable ideas can only be had by paying close attention. Nature is innately mathematical and she speaks to us in mathematics. We only have to listen to describe nature in *mathematical form* [8, 9]. The method to express y and z in terms of x has simplified the entire process. Further the odd-even classification has helped in narrowing down the cases where actual proof is required. The approach facilitated to generalize the proof for $n = 3$ and $n = 4$ to a general proof for any positive integer n. The proof is based on the concept of contradiction. I will wait for the time when someone will write a few nice word for me as someone wrote for Andrew Wiles.

7 Open Problem

In this paper a simple proof of Fermat's Last Theorem(FLT) has been presented. The proof is based on odd-even classification of integers. For more than 300 years, no one was able to find a proof although various attempts produced numerous results and some fields of mathematical studies [3, 4].

In summer of 1993, a proof was announced by Princeton University mathematics professor Andrew Wiles. Wiles' proof was 200 pages long and took more than seven years of dedicated effort. Are mathematicians finally satisfied with Andrew Wiles's proof of Fermat's Last Theorem? It is still an open question. Why has this theorem been so difficult to prove? These are still some unanswered questions [13, 14]. Since FLT is number theoretic problem, its proof has to be determined around number theory and not using geometry.

Acknowledgment

Existence of a problem inspires one to think for its solution. A complicated problem has generally a very simple solution. 'How unlearning (or keeping aside higher knowledge for sometimes) helps in solving some problem" is an important lesson learnt here. One has to look around to know the presence of something worth noticing. Special thanks to some of my colleagues who always chant for something new.

References

[1] Aczel, Amir D., (1996). *Fermat's Last Theorem*, Dell Publishing, N. Y., pp. 123 - 134.

[2] Boston, N., (1995). A Taylor-made plug for Wiles' proof. College Mathematics Journal, 26:100–105, 1995.

[3] Cornell, G., Silverman, J., and Stevens, G., (1997) Modular forms and Fermat's last theorem. Springer-Verlag.

[4] Darmon, H., Diamond F. and Taylor R., (1997). Fermat's last theorem, Elliptic curves, modular forms and Fermat's last theorem (Hong Kong, 1993):2–140.
[5] Granville, A. and Monagan, M., (1988). The first case of Fermat's last theorem is true for all prime exponents up to 714, 591, 416, 091, 389. Trans. AMS, 306:329–359, 1988.
[6] Ireland, K., and Rosen, M., (1990). A classical introduction to modern number theory, Second edition, Graduate Texts in Mathematics 84, Springer-Verlag, New York, 1990.
[7] Jacobson, N., (1989). Basic Algebra,II. W.H.Freeman, New York.
[8] Kumar, V., (2010). 'Restricted Backtracked Algorithm to Find Hamiltonian Circuit in Undirected Graph', BVICAM **Int. J. of Information Technology, India,** Vol. 2, No. 2, pp. 23-32.
[9] Kumar, V., (2012). "Mathematics is Science: A Topic Revisited in Context of FCS of India", Int. J. of Modern Education and Computer Science, MECS, Vol. 4, No. 6, pp. 17-26.
[10] Lerman, S., (1996). 'Inter subjectivity in Mathematics Learning: A Challenge to the Radical Constructivist Paradigm?', Journal for Research in Mathematics Education, 27(2), 133-150.
[11] Radford, L., (2006), 'Algebraic Thinking and the Generalization of Patterns: A Semiotic Perspective', in S. Alatorre et al. (Eds.), Proceedings of the 28th Conference of the International Group for the Psychology of Mathematics Education, North American Chapter, Mérida, Vol. 1, pp. 2-21 (Plenary Lecture).
[12] Ribenboim, P., (1999). Fermat's last theorem for amateurs, Springer-Verlag, New York.
[13] Rubin, K., and Silverberg, A., (1994). A report on Wiles' Cambridge lectures, Bulletin of AMS, 31:15–38.
[14] Sfard, A., (1991). 'On the dual nature of mathematical conceptions', Educational Studies in Mathematics, 22, 1-36.
[15] Silverman, J., (1986). Arithmetic of elliptic curves, Graduate Texts in Mathematics, Springer-Verlag, New York.
[16] Stewart, I. and Tall, D., (2002). Algebraic number theory and Fermat's last theorem, Third edition, A K Peters, Ltd., Natick, MA.
[17] Taylor, R., and Wiles, A. (1995). Ring-theoretic properties of certain Hecke algebras Ann. of Math., 141:553–572.
[18] Washington, L., (1997). Galois cohomology, Modular forms and Fermat's last theorem:101–120.
[19] Washington, L., (1997). Introduction to cyclotomic fields, Second edition. Graduate Texts in Mathematics 83, Springer Verlag, New York.
[20] Waterhouse, W., (1979). Introduction to affine group schemes, Graduate Texts in Mathematics 66. Springer-Verlag, New York.
[21] Wiles, A., (1995). Modular elliptic curves and Fermat's last theorem, Ann. of Math, 141:443–551.