Menemui Matematik (Discovering Mathematics)
Vol. 35, No. 1: 33 - 39 (2013)

A Simple Proof of the Fermat's Last Theorem

Ramappillai Nagarajah

(formerly Chief Engineer, National Electricty Board of the States of Malaya)
6, Jalan Ayam-Ayam, 6/2E, 40000 Shah Alam, Selangor D.E., Malaysia
malini_jeyasingam@yahoo.com

ABSTRACT

The proof that is being presented here makes use of simple concepts of elementary mathematics involving, elementary algebraic expressions and equations, application of Remainder and Factor Theorems, concepts of factorization and a fair knowledge of primes and coprimes. The method of contradiction is applied to the integral solutions of the equation $x^n+y^n=z^n$ where n is a prime number greater than 2 and x, y and z are coprime.

INTRODUCTION

The Fermat's Last Theorem (FLT) which was stated by the well-known seventeenth century French mathematician, Pierre Fermat, had, in spite of attempts by several mathematicians over a period of more than three centuries, not been proved until Wiles and Taylor have been recognized world over as the persons who had closed the case in 1995. However the proof by Wiles (1995) and Wiles and Taylor (1995) made use of very advanced and sophisticated methods in abstract algebra and analysis in the current domain of number theory as such that very few people would be able to follow and satisfied with the proof. In fact many still believe that there must be a simpler method and there has remained a keenness to obtain a simple proof of the theorem. Unlike the proof for the fundamental theorem of algebra whereby the simple proof works only for a small number of cases only. No doubt, the hope and expectation in the case of the FLT arises due to a consideration on the fact that many cases of the exponent of the FLT have already been successfully proven (n =3 by Gauss in 1830s, $n = 4$ is by Hardy and Wright 1959 and even simpler by Swetz 1994, n=5 by Legendre in 1825, $n = 7$ by Lame in 1839, n=regular primes by Kummer in 1840s such as $n = 3,5,7,11,13,17,19,23,29,31$ and in general it is defined in terms of Bernoulli numbers), and hence a multiple of these successful exponents as described by Swetz 1994, all of which using elementary algebra of integers. We believe that our present proof fulfills this expectation.

The Standard Fermat's Last Theorem

It is well known that (see for examples Hardy and Wright 1959, and more recently Swetz 1994), for the FLT to be true, it is sufficient to prove that,

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

has no positive integral solutions of x, y, z such that the triple is coprime, $(x, y, z) = 1$ whenever n is a prime greater than 2, or $n = 4$.

This is referred to as the Standard Fermat's Last Theorem. (Std. FLT). As already mentioned in the introduction of this paper, the case where $n = 4$, has been proved , thus only the case where n is a prime greater than 2, is presented in this paper.

Two Cases

As $(x, y, z) = 1$ (Std. FLT), *n can* either be a factor of one of x, y or z or not be a factor of any one of x, y *or* z.
Thus we have two cases as follows:

Case I In this case *n is* a factor of one of x, y or z
(i) If n is a factor of x, then $(y, z, n) = 1$
(ii) If n is a factor of y, then $(x, z, n) = 1$
(iii)If n is a factor of z, then $(x, y, n) = 1$

Case II In this case n is not a factor of any of x, y or z
and thus $(x, y, z, n) = 1$
For the Case I, it is sufficient to prove the Case I (i) only as other cases can be proved in a very similar way.

A Proof of the Standard Fermat's Last Theorem for Case I (i)

The theorem is proved by contradiction: Suppose $x^n + y^n = z^n$, $n>2$, $(x, y, z)=1$, n is a factor of x, has an integral solution x, y, z, then we would arrive at an absurd result.
we have

$$y^n = z^n - x^n = (z - x)\ f(z, x); \tag{2a}$$

where

$$f(z, x) = z^{n-1} + z^{n-2}\ x + \ldots\ldots + z\,x^{n-2} + x^{n-1} \tag{2b}$$

and

$$z^n = x^n + y^n = (x + y)\ g(x,\ y) \tag{3a}$$

where

$$g(x, y) = x^{n-1} - x^{n-2}\ y + \ldots\ldots - x\,y^{n-2} + y^{n-1} \tag{3b}$$

The factorization in equations (2a) and (3a) is well known and a proof, by mathematical induction, is found in Briggs and Bryan (1964).

The following inequalities, which are very useful in our arguments later on, are derived from equation (1).

(i) As $n > 2$ we have $(x + y)^n > x^n + y^n$
and hence

$$x + y > z \tag{4a}$$

As $x^n + y^n = z^n$ we have $z > x$ and $z > y$ and also either $x > y$ or $y > x$. Thus we can let $x > y$
Hence

$$z > x > y \tag{4b}$$

Note that the case x = y is not acceptable as, if x =y then from equation (3a), $z^n = 2x^n$ which can have integral solutions only when $n = 1$, and this is not in (i) Accordance with Std FLT where $n > 2$. Now we proceed to our proof of the Std FLT for Case 1(i).
From (2a), $y = bq$ (the prime factorization theorem) is equivalent to (by Lemma 0)

$$z - x = b^n,\ f(z, x) = q^n;\ or\ z-x = q^n,\ f(z, x) = b^n$$

and from inequality (4a), $y > z - x$ and hence $bq > b^n$ or $bq > q^n$
or equivalently

$$q > b^{n-1} \quad \text{or } b > q^{n-1} \tag{5a}$$

Similarly, from (3a) , $z = cr$ is equivalent to (by Lemma 0) $x + y = c^n$, $g(x,y)=r^n$; or $(x+y)=r^n$, $g(x,y)=c^n$ and from inequality (4a), $z < x + y$ and hence $cr < c^n$ or $cr < r^n$
or equivalently

$$r < c^{n-1} \text{ or } c < r^n \tag{5b}$$

Hence from the first half of (5a) and (5b), we have

$$q = b^{n-1} + v \tag{6a}$$

and

$$r = c^{n-1} - w \qquad (6b)$$

where v and w are positive integers.

From Lemma 1 (i) and Lemma 1 (ii), in the Appendix 1,

$$\begin{aligned} b^n + c^n &= (z - x) + (x + y) \\ &= y + z \\ &= bq + cr \\ &= b(b^{n-1} + v) + c(c^{n-1} - w) \text{ by equations (6a)} \end{aligned}$$

and

$$(6b) = b^n + bv + c^n - cw$$

Thus

$$bv = cw \qquad (7)$$

From Lemma 1 (iii), in the Appendix 1, as $(b, c) = 1$, it follows from equation (7), that, $v = kc$ and $w = kb$ where k is a positive integer. Hence, equations (6a) and (6b) become

$$q = b^{n-1} + kc \qquad (8a)$$

and

$$r = c^{n-1} - kb \qquad (8b)$$

respectively.

From Lemma 1 (iii), in the Appendix 1, as $(b, c, q) = 1$, from equation (8a), $(k, b) = 1$ and as $(b, c, r) = 1$, from equation (8b), $(k, c) = 1$ and thus it follows that

$$(k, b, c) = 1. \qquad (8c)$$

From Lemma 1(i) and equation (8a),

$$y = b^n + kbc \qquad (9a)$$

Similarly, from Lemma 1(ii) , in the Appendix 1, and equation (8b),

$$z = c^n - kbc \tag{9b}$$

From Lemma 1(i), in the Appendix 1, and equation (9a),

$$x = c^n - b^n - kbc \tag{9c}$$

From equations (9a), (9b) and (9c)

$$x + y - z = kbc \tag{10}$$

From equations (1), (9a), (9b) and (9c) we have

$$(c^n - b^n - kbc)^n + (b^n + kbc)^n = (c^n - kbc)^n \tag{11}$$

where as stated in (8c), $(k, b, c) = 1$.

In equation (11), $c^{n-1} - kb$ (which is a factor of $c^n - kbc$) must be a factor of the expression $(c^n - b^n - kbc)^n + (b^n + kbc)^n = F(kb)$ and thus, in accordance with the factor theorem, the expression must equate to zero when $kb = c^{n-1}$
Hence $(c^n - b^n - c^n)^n + (b^n + c^n)^n = 0$, or equivalently

$$(- b^n)^n + (b^n + c^n)^n = 0 \tag{12}$$

But as b and c are positive integers, equation (12) is absurd!. Thus equation (11) is invalidated
As equation (11) is derived from equation (1) of the Std FLT, it follows that this later equation is contradicted.
Similar result can be obtained using the other half of (6a) and (6b).Thus, the Fermat's Last Theorem, in Case I (i) is proved by contradiction.
Cases I (ii) and I (iii) can be proved in a similar fashion, each has two lemmas similar to Lemma 0 and 1 in the respective Appendix.

Case II

The proof of Case I(i) is sufficient proof of Case II where n is not a factor of x, y or z and $(x, y, n) = 1$. This is in view of the fact that equations (2a) and (3a) and all ensuing discussions based on these two equations in Case I(i) are relevant to Case II and hence Case II is proved. It may also be noted that the proofs of Cases I (ii) and I (iii) are separately sufficient proof of Case II. It may also be noted that the proofs of Cases I (ii) and I (iii) are separately sufficient proof of Case II.

CONCLUSION

We have shown that $x^n + y^n = z^n$ has no positive integral solutions of x, y or z where $(x, y, z) = 1$ and n is a prime greater than 2. The case when $n = 4$ are well known proven long time ago...
hence, the Std FLT is proved.

ACKNOWLEDEMENT

The author extends very special thanks to Dr. Shaharir Mohamad Zain, formerly, Professor of Mathematics, Universiti Kebangsaan Malaysia, for his valuable suggestions and comments which have contributed significantly to the improvement of the presentation of this paper. The author's thanks are also due to many others who have in one way or the other helped him in the presentation of this paper.

APPENDIX 0

Lemma 0: For the Case I(i), the two pairs z-x and f(x,z), and x+y and g(x,y) are coprimes, i.e (z - x,f(x,z)) =1; and (x+y, g(x,y)) =1.

Proof:

Dividing $f(z, x)$ by $z - x$, the remainder is nx^{n-1} and let the quotient be $Q(x,z)$.
Thus, $f(z, x) = (z - x)\, Q(x,z) + nx^{n-1}$.
From this equation, it is seen that , common factors of $(z - x)$ and $f(z, x)$, if any, can only be factors of nx^{n-1}.

In the case presently considered, Case I (i), $(y, z, n) = 1$, and from Std FLT $(x, y, z) = 1$ and so $(n, y) = 1$ and $(x, y) = 1$ thus n and x are not factors of y^n.

From equation (2a), it follows that n and x are not factors of either $(z – x)$ or $f (z, x)$. Therefore $(z – x)$ and $f (z, x)$ have no common factors. Hence $(z – x)$ and $f (z, x)$ are coprime. QED

APPENDIX 1

Lemma 1: If $x^n + y^n = z^n$ where x, y and z *are* positive integers such that $(x, y, z) = 1$, n is a prime greater than 2, and n is a factor of x such that $(y, z, n) = 1$, then there exist positive integers b,c,q and r such that

(i) $y = bq$, and $(b, q, n) = 1;$

(ii) $z = cr$, and $(c, r, n) = 1;$

(iii) $(b, q, c, r, n) = 1$.

Proof:

$y= bq$ for some positive integers b and q, such that one of them is a prime number (a prime factorization theorem). Therefore, by (2a) and (2b), z-x is b^n or q^n ; and $f(z,x)$ is q^n or b^n respectively (by Lemma 0). In either case $(b^n, q^n) =1$ or $(b,q)=1$. Since $(n,y)=1$ then $(b,q,n)=1$. Similarly, $z=cr$ for some positive integers c and r, such that one of them is a prime number. Therefore, by (3a) and (3b), we can conclude that $(c,r)=1$ and $(c,r,n)=1$.
Since a hypothesis of the Lemma is $(y,z,n) =1$ then $(b,q,c,r,n)=1$. *QED*

REFERENCES

Briggs, W. and Bryan, G.H. (1964), *The Tutorial Algebra*, revised and rewritten by G. Walker University Tutorial Press Ltd. 378.

Hardy, G. H. and Wrigh, E.M. (1959), *An Introduction to the Theory of Numbers*. The English Language Book Society and Oxford University Press. 190 – 192.

Swetz, F. J. (1994), *From Five Fingers to Infinity.A Journey through the History of Mathematics*. Chicago: Open Court.

Wiles, A. (1995) Modular Elliptic Curves and Fermat's Last Theorem, *Annals of Mathematics*, **141** : 443 – 551.