A New Proof Of *Fermat's Last Conjecture*, And A Corrected Solution For $ax^2+bx+c=0$.

Michael C. Nwogugu
Address: Enugu 400007, Enugu State, Nigeria
Emails: mcn2225@gmail.com; mcn2225@aol.com
Skype: mcn1112
Phone: 234-909-606-8162 or 234-814-906-2100.

Abstract.
In this article, a new proof for *Fermat's Last Conjecture* is introduced. Also the widely popular "traditional" solution for the quadratic equation $ax^2+bx+c=0$, is corrected (a new solution is introduced).

Keywords: Nonlinearity; *Fermat's Last Conjecture*; Quadratic Equations; Mathematical Cryptography; Prime Numbers; Adomian's Method; *Beal Conjecture*; Iterated Solutions.

1. Introduction.

Fermat's Last Conjecture has generated substantial debate during the last few centuries, and most proofs offered have been un-necessarily convoluted and inaccurate. See: Darmon & Merel (1997), Cai, Chen & Zhang (2015), Jones & Rouse (2013), Kumar (2014), Joseph (2015), Rahmawati, Sugandha, et. al. (2019), Ibarra & Dang (2006), Nemron (2008), Zhang (1991); Wiles (1995), and Faltings (1995). The large volume of post-1995 Mathematicians' published/un-published attempts to solve *Fermat's Last Conjecture* implies that many researchers don't believe or understand the 1993-1995 Wiles-related proofs of *Fermat's Last Conjecture* (see Faltings (1995) and Wiles (1995)). Lolja (2018) categorially explained why *Fermat's Last Conjecture* had not be proved as of 2018.

Chu (2008) and Lu & Wu (2016) studied dynamical systems pertaining to Diophantine equations. Luca, Moree & Weger (2011) discussed *Group Theory* as it relates to Diophantine Equations. On Homomorphisms, see: Wang & Chin (2012). Elia (2005), Jones, Sato, et. al. (1976) and Matijasevič (1981) noted that primes can also be represented as Diophantine equations or as polynomials (such as in Fermat's equation). On uses of Diophantine Equations in Cryptography, see: Ding, Kudo, et. al. (2018), Okumura (2015), and Ogura (2012). Zadeh (2019) notes that Diophantine equations have been used in analytic functions.

The quadratic equation $ax^2+bx+c=0$, and its standard solutions are perhaps some of the most widely used equations. The error in its standard solutions is corrected in this article (a new solution is introduced). See: Adomian (1985), Abbaoui & Cherruault (1994), Otadi & Mosleh (2011), Kajania, Asady & Vencheh (2005), López, Robles & Martínez-Planel (2016), and Sastry (1988).

2. *Fermat's Last Conjecture.*

For the equation $\mathbf{a^x+b^x=c^x}$ in positive integers, the following are combinations of a,b,c and x that appear to nullify *Fermat's Last Conjecture* (but only in the *Domain-Of-Real-Numbers*), but the issue is that for each such combination, $(c/a)^x-(b/a)^x \approx 1.0000000000000000000000$ (the equation is not exactly equal to 1.000000000000000000000000 like in pythagorean triples):

i) a = 71; b= 72; c = 90; **x=3**; and $\mathbf{(c/a)^x-(b/a)^x = 0.993967774}$.
ii) a = 380; b= 412; c = 500; **x=3**; and $\mathbf{(c/a)^x-(b/a)^x = 1.003525878.}$
iii) a = 3,816; b= 4,110; c = 5,000; **x=3**; and $\mathbf{(c/a)^x-(b/a)^x = 1.000097655.}$
iv) a = 482,950; b= 613,000; c = 700,000; **x=3**; and $\mathbf{(c/a)^x-(b/a)^x = 1.000088826.}$
v) a = 3,811,500; b= 4,113,160; c = 5,000,000; **x= 3**; and **(c/a)x-(b/a)x = 1.000749834.**
vi) a = 56,590,000; b= 62,199,000; c = 75,000,000; **x= 3**; and **(c/a)x-(b/a)x = 1.000106785.**
vii) a = 583,000,000; b= 680,202,900; c = 800,500,000; **x=3**; and $\mathbf{(c/a)^x-(b/a)^x = 1.000463103}$.

viii) a = 280,010; b= 357,010; c = 360,060; **x=10**; and **$(c/a)^x-(b/a)^x$ = 1.007959.**
ix) a = 2,800,100; b= 3,570,100; c = 3,600,390; **x=10**; and **$(c/a)^x-(b/a)^x$ =1.000752.**
x) a = 2,800,100; b= 3,570,100; c = 3,600,360; **x=10**; and **$(c/a)^x-(b/a)^x$ =0.999723.**
xi) a = 42,400; b= 42,500; c = 43,443; **x= 30**; and **$(c/a)^x-(b/a)^x$ = 0.99986336.**
xii) a = 4,240,000; b= 4,250,000; c = 4,345,000; **x= 30**; and **$(c/a)^x-(b/a)^x$ = 1.009908.**
xiii) a = 43,448; b= 43,379; c = 43,000; **x= 150**; and **$(c/a)^x-(b/a)^x$ = 1.004094906.**
xiv) a = 4,300,000; b= 4,337,990; c = 4,344,850; **x= 150**; and **$(c/a)^x-(b/a)^x$ =1.000648.**
xv) a = 424,400; b= 425,000; c = 425,005; **x= 2,500**; and **$(c/a)^x-(b/a)^x$ = 1.020488.**
xvi) a = 42,440,000; b= 42,500,006; c = 42,500,496; **x= 2,500**; and **$(c/a)^x-(b/a)^x$ = 1.000135569.**
xvi) a = 424,999,999; b= 425,004,800; c = 425,007,071; **x= 70,000**; and **$(c/a)^x-(b/a)^x$ = 1.0002.**
xvii) a = 42,499,992; b= 42,500,002; c = 42,500,293; **x= 100,000**; and **$(c/a)^x-(b/a)^x$ = 1.006591792.**
xviii) a = 425,006,108; b= 425,006,999; c = 425,007,011; **x= 1,500,000**; and **$(c/a)^x-(b/a)^x$ = 1.0042.**
xix) a = 42,500,228,000; b= 42,500,229,000; c = 42,500,231,800; **x= 9,000,000**; and **$(c/a)^x-(b/a)^x$ = 1.000173356.**
xx) a = 4,250,069,400; b= 4,250,069,990; c = 4,250,070,110; **x= 9,000,000**; and **$(c/a)^x-(b/a)^x$ = 1.0092.**
xxi) a = 36,500,228,969; b= 36,500,230,385; c = 36,500,230,857; **x= 25,000,000**; and **$(c/a)^x-(b/a)^x$ = 1.006653657.**
xxii) a = 425,006,999,145; b= 425,006,999,280; c = 425,007,011,000; **x= 25,000,000**; and **$(c/a)^x-(b/a)^x$ = 1.0004.**

See the results and cited articles in Jones & Rouse (2013). Given the foregoing, *Fermat's Last Conjecture* is or can be valid only in the *Domain-Of-Integers*, but not in the *Domain-Of-Real-Numbers*. Lolja (2018) explained the differences between the *Domain-of-Integers* and the *Domain-Of-Lines*. The new proof introduced here pertains only to the Domain-Of-Integers.

Theorem-1: *Fermat's Last Conjecture* Which States That No Three Positive Integers *a, b* And *c* Satisfy The Equation $a^x+b^x=c^x$ (Where *x>2* Is A Positive Integer) Is Correct Only In The *Domain-Of-Integers*.

Proof:

In order for $a^x+b^x=c^x$, to be valid, the two conditions c>b,a; and c>b≥a must hold, partly because $1= (c/a)^x-(b/a)^x$.

$a^x+b^x=c^x$, and then divide both sides of the equation by a^x, and subtract 1 from each side of the equation:
$b^x/a^x = (c^x/a^x)-1$; and $1= (c/a)^x-(b/a)^x$.
$(b/a)^x = (c^x/a^x)-1$, and $(b/a) = \sqrt[x]{[(c^x/a^x)-1]}$,

In equation $b^x/a^x = (c^x/a^x)-1$, for all positive integers (a,b,c) ε (1,+∞) and *x* ε (3,+∞), integer ***x*** cannot be less than three because of the following reasons:

i) $b^x/a^x = (c^x/a^x)-1$ is equivalent to $1 = (c/a)^x-(b/a)^x$. The two terms $[b^x/a^x]$ and $[(c^x/a^x)-1]$ must be equal, or the condition $1=(c/a)^x-(b/a)^x$ must exist and that cannot occur if x>2 because c>b>a, and because of compounding implicit in the polynomial. See Chapters 4, 5, 7 & 8 in Nwogugu (2017). That is, because c>b>a, and for all x>2, as (a,b,c,x)→+∞, [(c/a)-(b/a)]→+∞; and $[\{(c/a)^x-(b/a)^x\}>1]\rightarrow+\infty$; and $[(c/a)^x-(b/a)^x]\neq1$. There is a threshold at which such compounding takes effect and the smallest positive-integer value at which compounding can possibly start is x=2; and the smallest positive-integer values at which compounding can substantially distort the equation is x=2,3. Thus, *Fermat's Last Conjecture* is correct in the Domain-Of-Integers.

ii) $a^x/b^x = 1/[(c^x/a^x)-1]$; and $(a/b)^x = 1/[(c^x/a^x)-1]$; and thus:
$\text{Ln}(a/b)^x = \exp(1/[(c^x/a^x)-1])$. However, this foregoing condition doesn't hold.
For all x>2, the term $(1/[(c^x/a^x)-1])$ will always be greater than one and $\exp(1/[(c^x/a^x)-1])$ will be in the (2.718, +∞) range.

On the other hand, (a/b) will always be less than one because c>b>a, and for all x>2, $(a/b)^x$ will also be less than one. As $x\rightarrow+\infty$, $(a/b)^x\rightarrow 0$. Thus, $Ln(a/b)^x$ is likely to be less than one for all x>2. Therefore, $Ln(a/b)^x \neq \exp(1/[(c^x/a^x)-1])$ for all x>2; and thus, *Fermat's Last Conjecture* is correct in the Domain-Of-Integers.

Also:
$(b/a)^x = (c^x/a^x)-1$, and $(b/a) = {}^x\sqrt{[(c^x/a^x)-1]}$,
$a^x/b^x = 1/[(c^x/a^x)-1]$; and $(a/b)^x = 1/[(c^x/a^x)-1]$;
$a/b = {}^x\sqrt{\{1/[(c^x/a^x)-1]\}}$;
$a= b* {}^x\sqrt{\{1/[(c^x/a^x)-1]\}}$;
$b = a/ {}^x\sqrt{\{1/[(c^x/a^x)-1]\}}$; or $b = a* {}^x\sqrt{[(c^x/a^x)-1]}$,

Given the foregoing, the following additional are component "Sub-Theorems" (each of which can be presented as a separate complete theorem) that prove that *Fermat's Last Conjecture* is correct in the *Domain-Of-Integers*.

Sub-Theorem #1:
First, in equations $a^x+b^x=c^x$ and $b^x/a^x = (c^x/a^x)-1$, for all positive integers *(a,b,c)* ε $(1,+\infty)$ and *x* ε $(3,+\infty)$, as $x,a,b,c\rightarrow+\infty$, (and for medium and large values of [x,a,b,c]), $1+b^x/a^x \rightarrow b^x/a^x$, and the above implies that $b^x/a^x = c^x/a^x$, or that $b^x = c^x$, which is wrong because that condition/equation can exist *iff* a=0. Thus, *Fermat's Last Conjecture* is correct in the Domain-Of-Integers.

Sub-Theorem #2:
Second, in equation $a^x+b^x=c^x$, $c>b\geq a$, and for all positive integers *(a,b,c)* ε $(1,+\infty)$ and *x* ε $(3,+\infty)$, as $(a,b,c,x)\rightarrow+\infty$ (and for medium and large values of [x,a,b,c]), $a= b* {}^x\sqrt{\{1/[(c^x/a^x)-1]\}}$ becomes:
$a= b* {}^x\sqrt{\{1/[(c/a)^x]\}}$ which is equivalent to $a= b* \{1/(c/a)\}$ which is equivalent to a= (ba)/c, or 1=b/c; all of which are not feasible since c>a,b; and $c>b\geq a$. Thus, *Fermat's Last Conjecture* is correct in the Domain-Of-Integers.

Sub-Theorem #3:
Third, in equation $a^x+b^x=c^x$, $c>b\geq a$, and for all positive integers *(a,b,c)* ε $(1,+\infty)$ and *x* ε $(3,+\infty)$, the amount ***a*** cannot be a positive integer, because in equation $\boldsymbol{a}= b* {}^x\sqrt{\{1/[(c^x/a^x)-1]\}}$, the amount $\{1/[(c^x/a^x)-1]\}$, will always be greater than one (c>b>a) but may or may not be an integer, and thus the amount ${}^x\sqrt{\{1/[(c^x/a^x)-1]\}}$ may or may not be an integer. Also, the amount ${}^x\sqrt{\{1/[(c^x/a^x)-1]\}}\rightarrow-\infty$ as $x\rightarrow+\infty$, thus ***a*** is not guaranteed to be an integer for all x ε $(3,+\infty)$. Thus, *Fermat's Last Conjecture* is correct in the Domain-Of-Integers.

Sub-Theorem #4:
Third, in equation $a^x+b^x=c^x$, $c>b\geq a$, and for all positive integers *(a,b,c)* ε $(1,+\infty)$ and *x* ε $(3,+\infty)$, the amount *b* cannot be a positive integer, because in equation $b = a* {}^x\sqrt{[(c^x/a^x)-1]}$, and for all x>2, the amount $[(c^x/a^x)-1]$ will be greater than 1, and the amount ${}^x\sqrt{[(c^x/a^x)-1]}$, may or may not be an integer and thus *b* is not guaranteed to be an integer for all *x* ε $(3,+\infty)$. Thus, *Fermat's Last Conjecture* is correct.

■

<u>3. A Critique Of The Traditional Solution For The Equation $ax^2+bx+c=0$ And Why Its Wrong.</u>

Theorem-2: The Quadratic Equation $ax^2+bx+c=0$, Has The Solutions $x = [-2ab\pm(\{\sqrt{-(c/a)} + (b/2a)^2\}*4a^2)]$.
Proof:
In the existing literature, the quadratic equation $ax^2+bx+c=0$ is traditionally solved as follows.

Divide both sides of the equation by a:
2.1) $x^2+bx/a +c/a = 0$

Move the last term in the left hand side to the right hand side of the equation:

2.2) $x^2 + bx/a = - c/a$

Add $(b/2a)^2$ to both sides of the equation:

2.3) $x^2 + bx/a + (b/2a)^2 = -(c/a) + (b/2a)^2$

Convert the left hand side into an equation of the type $(x+y)^2$:
2.4) $[x+(b/2a)]^2 = -(c/a) + (b/2a)^2$

Use square-root format to simplify both sides of the equation:
2.5) $x+(b/2a) = \sqrt{}\{-(c/a)+(b/2a)^2\}$

Subtract (b/2a) from both sides of the equation
2.6) $x = -(b/2a) \pm \sqrt{}\{-(c/a)+(b/2a)^2\}$
However, the foregoing purportedly results in the traditional and popular simplification $x=\{-b\pm (\sqrt{}(b^2 - 4ac)\}/2a$, which is wrong. The mistake in the traditional calculation is that its erroneously assumed that:

2.7) $\{\sqrt{}(x +y)\}*a = [\sqrt{}\{(x*a)+(y*a)\}]$

On the contrary, the correct simplification is as follows:

Multiply the right hand side of the equation by 2a/2a:
2.8) $x = -(2ab/4a^2) \pm \sqrt{}\{-(c/a)+(b/2a)^2\}$

Use a common denominator $(4a^2)$ for all terms in the right hand side of the equation:

2.9) $x = [-2ab \pm (\{\sqrt{}-(c/a) + (b/2a)^2\}*4a^2)]$

The above is the correct simplification. $\blacksquare$

4. Conclusion.
Fermat's Last Conjecture is or can be correct but only in the Domain-Of-Integers, and the correct solution to the quadratic equation $ax^2+bx+c=0$, is introduced herein.

5. Bibliography.
Abbaoui, K. & Cherruault, Y. (1994). Convergence of Adomian's method applied to nonlinear equations. *Mathematical & Computer Modelling*, 20(9), 69-73.

Adomian, G. (1985). On the Solution of Algebraic Equations by the Decomposition Method. *Journal Of Mathematical Analysis And Applications*, 105, 141-166.

Cai, T., Chen, D. & Zhang, Y. (2015). A new generalization of Fermat's Last Theorem. *Journal of Number Theory*, 149, 33-45.

Chu, M. (2008). Linear algebra algorithms as dynamical systems. *Acta Numerica*, 17, 1-86.

Darmon, H. & Merel, L. (1997). Winding quotients and some variants of Fermat's last theorem. *J. Reine Angew. Math.*, 490, 81–100.

Ding, J., Kudo, M., et. al. (2018). Cryptanalysis of a public key cryptosystem based on Diophantine equations via weighted LLL reduction. *Japan Journal of Industrial and Applied Mathematics*, 35, 1123–1152.

Elia, M. (2005). Representation of primes as the sums of two squares in the golden section quadratic field. *Journal of Discrete Mathematical Sciences and Cryptography*, 9(1).

Faltings, G. (1995). The Proof of Fermat's Last Theorem by R. Taylor and A. Wiles. *Notices of the AMS*, 42(7), 743–746.

Ibarra, O. & Dang, Z. (2006). On the solvability of a class of diophantine equations and applications. *Theoretical Computer Science*, 352(1–3), 342-346.

Jones, M. & Rouse, J. (2013). Solutions of the cubic Fermat equation in quadratic fields. *International Journal of Number Theory*, 9, 1579-1591.

Jones, J. P., Sato, D., et. al. (1976). Diophantine Representation of the Set of Prime Numbers. *American Mathematical Monthly*, 83, 449-464.

Joseph, J.E. (2015). A proof of Fermat's last theorem using elementary algebra. *International Journal of Algebra and Statistics*, 4(1), 39-41.
Kajania, M., Asady, B. & Vencheh, H. (2005). An iterative method for solving dual fuzzy nonlinear equations. *Applied Mathematics & Computation*, 167(1), 316-323.

Kumar, V. (2014). Proof of Fermat Last Theorem based on Odd-Even Classification of Integers. *International Journal Of Open Problems In Computer Mathematics*, 7(4), 23-34.

Lolja, S. (2018). The Proof of the Fermat's Conjecture in the Correct Domain. *Ratio Mathematica*, 35, 53-74

López, J., Robles, I. & Martínez-Planel, R. (2016). Students' understanding of quadratic equations. *International Journal of Mathematical Education in Science and Technology*, 47(4), 552-556.

Lu, F. & Wu, J. (2016). Diophantine analysis in beta-dynamical systems and Hausdorff dimensions. *Advances in Mathematics*, 290, 919-937.

Luca, F., Moree, P., & Weger, de, B. M. M. (2011). Some Diophantine equations from finite group theory: $\Phi_m (x) = 2p^n -1$. *Publicationes Mathematicae* (Institutum Mathematicum Universitatis Debreceniensis), 78(2), 377-392.
Matijasevič, Y. (1981). Primes are nonnegative values of a polynomial in 10 variables. *Journal of Soviet Mathematics*, _________.

Nemron, I. (2008). An original abstract over the twin primes, the Goldbach conjecture, the friendly numbers, the perfect numbers, the Mersenne composite numbers, and the Sophie Germain primes. *Journal of Discrete Mathematical Sciences and Cryptography*, 11(6), 715-726.

Nwogugu, M. (2017). *Anomalies In Net Present Value, Returns And Polynomials, And Regret Theory In Decision Making* (Palgrave MacMillan, 2017).

Ogura, N. (2012). *On Multivariate Public-key Cryptosystems*. PhD thesis, Tokyo Metropolitan University (2012).

Okumura, S. A (2015). Public key cryptosystem based on diophantine equations of degree increasing type. *Pacific Journal of Industrial Mathematics*, 7(4), 33–45.

Otadi, M. & Mosleh, M. (2011). Solution of fuzzy polynomial equations by modified Adomian decomposition method. *Soft Computing*, 15, 187–192.

Rahmawati, R., Sugandha, S., et. al. (2019). The Solution for the Nonlinear Diophantine Equation $(7k-1)^x + (7k)^y = z^2$ with k as the positive even whole number. *Journal of Physics: Conference Series*, Volume 1179. The 1st International Conference on Computer, Science, Engineering and Technology 27–28 November 2018, Tasikmalaya, Indonesia.

Sastry, K. (1988). The Quadratic Formula: A Historic Approach. *The Mathematics Teacher*, 81(8), 670-672.

Wang, L. & Chin, C. (2012). Some property-preserving homomorphisms. *Journal of Discrete Mathematical Sciences and Cryptography*, 15(2-3).

Wiles, A. (1995). Modular elliptic curves and Fermat's Last Theorem. *Annals of Mathematics*, 141(3), 443–551.

Zadeh, S. (2019). Diophantine equations for analytic functions. *Online Journal of Analytic Combinatorics*, 14, 1-7.

Zhang, X.S. (1991). Fermat’s Last Theorem proved by a simple method. *Engineering Fracture Mechanics*, 39(2), 235-240.