Nonlinearity, The *Jeśmanowicz Conjecture* And The Equations $a^2+b^2=c^2$, And ax+by=cz.

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, several joint-properties of the equations $a^2+b^2=c^2$, and *ax+by=cz*, are introduced.

Keywords: Nonlinearity; *Jeśmanowicz Conjecture*; Number Theory; Prime Numbers; Dynamical Systems; Mathematical Cryptography; Primitive Pythagorean Triples.

1. Introduction.

On the *Jeśmanowicz Conjecture* which has generated substantial debate for decades, see: Guo & Le (1995), Miyazaki (2011; 2013), Miyazaki, Yuan & Wu (2014); Miyazaki & Terai (2015), Takakuwa (1996), and Terai (2014). On various approaches for solving related diophantine equations, see: Bennett & Skinner (2004). On Pythagorean numbers, see: Jeśmanowicz (1955/1956). On other approaches to solving Diophantine Equations, see: Rahmawati, Sugandha, et. al. (2019), Darmon & Merel (1997) and Ibarra & Dang (2006).

On Homomorphisms, see: Wang & Chin (2012). Chu (2008) and Lu & Wu (2016) studied dynamical systems pertaining to Diophantine equations (and *equations such as* $a^2+b^2=c^2$, and *ax+by=cz* can approximate Dynamical Systems). Luca, Moree & Weger (2011) discussed *Group Theory*. Elia (2005), Jones, Sato, et. al. (1976) and Matijasevič (1981) noted that primes can be represented as Diophantine equations or as polynomials (ie. and each of the *equations* $a^2+b^2=c^2$, and *ax+by=cz*, can represent a prime). On uses of Diophantine Equations in Cryptography, see: Ding, Kudo, et. al. (2018), Okumura (2015), and Ogura (2012) (each of the equations $a^x+b^y=c^z$ and **ax+by=cz** can be used in cryptoanalysis and in creation of public-keys). Zadeh (2019) notes that Diophantine equations have been used in analytic functions.

For the equation $\mathbf{a^x+b^y=c^z}$ in positive integers, the following are combinations of a,b,c, x,y and z; but for each such combination, $\mathbf{(a^x+b^y)/c^z}$ ≈1.0000000000000000000000 (the equation is not exactly equal to 1.000000000000000000000000 like in pythagorean triples):

i) a = 3; b= 5; c = 7; **x= 6**; **y = 7; z= 7;** and $\mathbf{(a^x+b^x)/c^x = 1.018206700}$.
ii) a = 60; b= 80; c = 461; **x= 6**; **y = 7; z= 7;** and $\mathbf{(a^x+b^x)/c^x = 1.009462982}$.
iii) a = 434,500; b= 425,000; c = 75,696,000; **x= 6**; **y = 7; z= 7;** and $\mathbf{(a^x+b^x)/c^x = 1.007764426}$.
iv) a = 37,566; b= 24,844; c = 461; **x= 23**; **y = 40; z= 66;** and $\mathbf{(a^x+b^x)/c^x = 1.010647596}$.
v) a = 567,000; b= 424,410; c = 2,575; **x= 23**; **y = 40; z= 66;** and $\mathbf{(a^x+b^x)/c^x = 1.000292303}$.

Given the foregoing, *Jesmanowicz's Conjecture* 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*.

2. The Theorems.

Theorem-1: **Jeśmanowicz Conjectured That For Any Primitive Pythagorean Triple (a, b, c), The Equation $\mathbf{a^x+b^y = c^z}$ Has The Unique Solution (x, y, z) = (2, 2, 2) In Positive Integers x, y and z; But Its Conjectured Here That For Any Pythagorean Equation $\mathbf{a^x+b^y=c^z}$ That Satfisfies The *Jesmanowicz Conjecture* (and a,b,c,x,y And z Are Integers), The Equation ax+by=cz Doesn't Have The Unique Solution (x, y, z)=(2, 2, 2) In Positive Integers, If: (a–b)= ±1.**

Proof:
The equation (a–b)= ±1 is henceforth referred to as the "*(a-b) Conditions*".

1.1) Assuming that (x,y,z) = (2,2,2); then ax+by=cz is
2a+2b=2c. Dividing both sides by 2, the result is:
1.2) a+b=c.
1.3) Its easy to see that for any positive integers a, b and c, if a+b=c, then $a^2+b^2 \neq c^2$.

If (a-b) = 1, then:
1.4) a=(1+b)
1.5) ax+by = cz = (1+b)x+by = x+b(x+y) = $z(a^2+b^2)^{1/2}$ =
1.6) (1+b)x+(a-1)y = cz = x+xb+ay-y
1.7) Thus, x+xb+ay-y = x+bx+by = cz
1.8) and: (ay-y) = (by) = (cz-x-bx)
by dividing both sides of the first two terms by y, the result is:
1.9) b = (a-1)
1.10) 1= (a-b)
Since by = cz-ax
1.11) cz-ax = cz-x-bx

Let: a=(1+b) (this is the first *(a-b) Condition*).
The next step is to substitute 1=(a-b); x,y,z=2; and other preceding equations into equation $a^2+b^2 =c^2$.
1.12) Then if the *(a-b) Condition* is true, and if as mentioned above a+b=c, then $(a^2+b^2) = c^2 = (a+b)^2$ But that is incorrect because:
1.13) $(a+b)^2 = (a+b)(a+b) = a^2+ab+ab+b^2 = a^2+2ab+b^2$; and $(a^2+b^2) \neq a^2+2ab+b^2$
1.14) Furthermore, if the *(a-b) Condition* is true, by substituting 1=(a-b) into $a^2+b^2 =c^2$, then: $(a^2+b^2) = [(1+b)^2+b^2] = c^2 = (a+b)^2$
1.15) Which implies that $1+2b+2b^2 = a^2+2ab+b^2$, which is clearly incorrect.

Similarly, assume (a-b)=-1 (the second *(a-b) Condition*); and thus a= (b-1).
The next step is to substitute [-1=(a-b)], and [x,y,z=2] into equation $a^2+b^2 =c^2$.
If the second *(a-b) Condition* is true then: $(a^2+b^2) = [(b-1)^2+b^2] = c^2$
1.16) $(a^2+b^2) = a^2+2ab+b^2$.
1.17) $[(b-1)^2+b^2] = 2b^2-2b+1$
1.18) But $2b^2-2b+1 \neq a^2+2ab+b^2$.
Thus, both *(a-b) Conditions* are false. ■

Theorem-2: **For $a^2+b^2=c^2$, And Where a,b,c,x,y, and z Are Positive Integers, The Equation And Condition ax+by=cz Can Be Valid And Can Have A Solution.**
Proof:
If: ax+by=cz, then let:
2.1) a = (cz-by)/x
2.2) b = (cz-ax)/y
2.3) c = (ax+by)/z
2.4.) x = (cz-by)/a
2.5) y = cz-ax/b
2.6) z= (ax-by)/c

If $a^2+b^2=c^2$ (the unique solution in the *Jesmanowicz Conjecture*) then by substitution:
2.7) $[(cz-by)/x]^2 + [(cz-ax)/y]^2 = [(ax+by)/z]^2$; and:

2.8) $[(cz-by)^2/x^2] + [(cz-ax)^2/y^2] = [(ax+by)^2/z^2]$; and:
2.9) $[(cz-by)^2/((cz-by)/a)^2] + [(cz-ax)^2/((cz-ax)/b)^2] = [(ax+by)^2/((ax-by)/c)^2]$; and thus:

$a^2 + b^2 = c^2$
Thus, if $[a^2+b^2=c^2]$, then the equation and condition [ax+by=cz] holds for some (a,b,c,x,y,z). ■

Theorem-3: **Generally, if $a^2+b^2 = c^2$; from which:**
$a_1^2+b_1^2=c_1^2$; from which:
$a_2^2+b_2^2=c_2^2$; from which:
$a_3^2+b_3^2=c_3^2$; then: $c^2 = c_1^2= c_2^2=c_3^2$.

Proof:
The above conditions are henceforth referred to as "*Vertical Equalization*" and they can simultaneously hold *iff*:
a_3^2 is derived from (an expansion or substitution of) a_2^2 which is derived from (an expansion or substitution of) a_1^2 which is derived from (an expansion or substitution of) a^2; and
b_3^2 is derived from (an expansion or substitution of) b_2^2 which is derived from (an expansion or substitution of) b_1^2 which is derived from (an expansion or substitution of) b^2; and
c_3^2 is derived from (an expansion or substitution of) c_2^2 which is derived from (an expansion or substitution of) c_1^2 which is derived from (an expansion or substitution of) c^2;
then by "*vertical equalization*" (a new theory introduced here):
$c^2 = c_1^2= c_2^2=c_3^2$. ■

Theorem-4: For $a^2+b^2=c^2$, And Where a,b,c,x,y, and z Are Positive Integers; The Equation ax+by=cz Has The Non-Unique Solutions (a,b,c,)=(0;0;0) Or (x; y; z)=(1;1;1), Or (x,y,z)= (0;0;0), *iff:* (z>y,x) And (c>b>a).
Proof:

Let:
4.1) a = (cz-by)/x
4.2) b = (cz-ax)/y
4.3) c = (ax+by)/z
4.4) x = (cz-by)/a
4.5) y = cz-ax/b
4.6.) z= (ax-by)/c
4.7) c>b> a, because a, b and c constitute a Pythagorean triple.
4.8) z>y>x or z>y,x because a, b and c constitute a Pythagorean triple.

If $a^2+b^2=c^2$, then by substitution:
4.9) $[(cz-by)/x]^2 + [(cz-ax)/y]^2 = \mathbf{[(ax+by)/z]^2}$; and from that:
4.10) $[(cz-by)^2/x^2] + [(cz-ax)^2/y^2] = \mathbf{[(ax+by)^2/z^2]}$; and then from that:
4.11) $[(cz-by)^2y^2] + [(cz-ax)^2x^2] = \mathbf{[((ax+by)^2x^2y^2)/z^2]}$, and by inspection, z>y,x (and also because a, b and c constitute a Pythagorean triple).
4.12) Its easy to see that for any positive integers a, b and c, if a+b=c, then $a^2+b^2\neq c^2$.
Thus, the above equations imply that by *Vertical Equalization*:
4.13) $[(ax+by)/z]^2 = [((ax+by)^2x^2y^2)/z^2]$, which can be true *iff* (a,b,c) = (0,0,0); or (x,y,z)= (0;0;0).
4.14) Also, $[(cz-by)^2/x^2] + [(cz-ax)^2/y^2] = [(ax+by)^2/z^2]$; and thus:
4.15) $[(cz-by)^2/((cz-by)/a)^2] + [(cz-ax)^2/((cz-ax)/b)^2] = [(ax+by)^2/((ax-by)/c)^2]$; and:
$a^2+ b^2 = c^2$ ■

3. Conclusion.

The foregoing are several important “joint” properties of the equations $a^2+b^2= c^2$, and ax+by=cz. Both equations have potentially wide applications in Computer Science, Applied Math, Game Theory and Physics.

4. Bibliography.

Bennett, M. & Skinner, C. (2004). Ternary Diophantine equations via Galois representations and modular forms. *Canadian Journal Of Mathematics*, 56, 23–54.

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.

Guo, Y. & Le, M. (1995). A note on Jeśmanowicz’ conjecture concerning Pythagorean numbers. *Comment. Mat., Univ. St. Pauli*, 44, 225–228.

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

Jeśmanowicz, L. (1955/1956). Some remarks on Pythagorean numbers, *Wiadom. Mat*., 1 (1955/1956), 196–202 (in Polish).

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

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

Matijasevič, Y. (1981). Primes are nonnegative values of a polynomial in 10 variables. *Journal of Soviet Mathematics*, _________.

Miyazaki, T. (2011). Jeśmanowicz’ conjecture on exponential Diophantine equations. *Functional Approximation, Comment. Math*., 45, 207–229.

Miyazaki T. (2013). Generalizations of classical results on Jeśmanowicz’ conjecture concerning primitive Pythagorean triples. *Journal Of Number Theory*, 133, 583–595.

Miyazaki, T., Yuan, P. & Wu, D. (2014). Generalizations of classical results on Jeśmanowicz’s conjecture concerning Pythagorean triples II. *Journal of Number Theory*, 141, 184–201.

Miyazaki, T. & Terai, N. (2015). On Jeśmanowicz’ conjecture concerning primitive Pythagorean triples, II. *Acta Mathematica Hungarica*, 147(2), 286–293.

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

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

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.

Takakuwa, K. (1996). A remark on Jeśmanowicz’ conjecture. *Proc. Japan Acad. Ser. A Math. Sci.*, 72, 109–110.

Terai, N. (2014). On Jeśmanowicz’ conjecture concerning primitive Pythagorean triples. *Journal Of Number Theory*, 141, 316–323.

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

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