The *Qu (2018) Conjectures*, The *Yang & Fu (2018) Conjectures*, The *Jiang (2020) Conjecture*, The *Tao (2016) Conjectures*, The *Cipu (2007) Conjecture*, The *Cipu & Mignotte (2007) Conjecture* And The Simultaneous Pell Equations $x^2-(a^2-1)y^2=1$ and $y^2-pz^2=1$.

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.

This article shows that the *Qu (2018) conjectures*, the *Yang & Fu (2018) conjectures*, the *Jiang (2020) Conjecture-#1*, the *Tao (2016) Conjecture-#1*, the *Cipu & Mignotte (2007) Conjecture* and the *Cipu (2007) Conjecture* [all of which pertain to the system of Simultaneous Pell equations $x^2-(a^2-1)y^2=1$ and $y^2-pz^2=1$] are wrong.

Keywords: Simultaneous Pell Equations; Nonlinearity; Mathematical Cryptography; Prime Numbers; Dynamical Systems; Diophantine Equations; Number Theory.

1. Introduction.

Qu (2018) supposedly proved that:

i) where p is a prime number, the system of simultaneous Pell equations $x^2-(a^2-1)y^2=1$ and $y^2-pz^2=1$ (collectively, the "Simultaneous Pell System") has only a positive integer solution $(x,y,z) = (31,8,3)$ for $p=7$ (the "*Qu (2018) Conjecture-#1*") by using a Baker's lower bound and one lemma from Diophantine approximation to determine the lower and upper bounds respectively, on the variables of the equation; and

ii) there is no positive solution to the Simultaneous Pell System for $a=(2,3)$ (the "*Qu (2018) Conjecture-#2*"); and

iii) the Simultaneous Pell System has a positive integer solution only for $a=4$ which is $(x,y,z,p)=(31,8,3,7)$ (the "*Qu (2018) Conjecture-#3*").

Yang & Fu (2018) supposedly developed complete solutions for the Simultaneous Pell Equations $x^2-(a^2-1)y^2=1$ and $y^2-pz^2=1$; and they claimed that:

i) if $a \equiv 2$ or $3 \pmod 4$, then the Simultaneous Pell System has no positive integer solutions (x,y,z) (the "*Yang & Fu (2018) Conjecture-#1*"); and

ii) for $1< a< 100$, the Simultaneous Pell System has only the positive integer solutions (a,p,x,y,z) = (4, 7, 31, 8, 3), (5, 11, 49, 10, 3), (12, 23, 287, 24, 5), (13, 3, 337, 26, 15), (24, 47, 1151, 48, 7), (40, 79, 3199, 80, 9), (41, 83, 3361, 82, 9) and (84, 167, 14111, 168, 13) (the "*Yang & Fu (2018) Conjecture-#2*").

Thus, the Yang & Fu (2018) positive integer solutions [(a,p,x,y,z) = (4, 7, 31, 8, 3), (5, 11, 49, 10, 3), (12, 23, 287, 24, 5), (13, 3, 337, 26, 15), (24, 47, 1151, 48, 7), (40, 79, 3199, 80, 9), (41, 83, 3361, 82, 9) and (84, 167, 14111, 168, 13)] nullify the *Qu (2018) Conjecture-#3*, and the *Cipu & Mignotte (2007) Conjecture* and the *Jiang (2020) Conjecture-#1*. The *Ai, Chen, Zhang & Hu (2015)* positive-integer solutions (where a=5) are (x,y,z,p)=(49,10,3,11) and (x,y,z,p)=(485,99,70,2) and they nullify the *Yang & Fu (2018) Conjecture-#2*.

Ai, et. al. (2015) conjectured that the system of simultaneous equations $x^2-24y^2=1$ and $y^2-pz^2=1$, where p is a prime, has at most one integer solution for each p, and that the only solutions for that system of equations are (x,y,z)=(485,99,70) for p=2, and (x,y,z)=(49,10,3) for p=11 (the "*Ai, Chen, Zhang & Hu (2015) Conjecture*"). Note that if a=5, then $x^2-24y^2=1$ is equivalent to $x^2-(a^2-1)y^2=1$.

Tao (2016) conjectured that for the system of simultaneous Pell equations $x^2-24y^2=1$ and $y^2-2pz^2=1$ (where p is an odd prime) there is no positive integer solution (the "*Tao (2016) Conjecture-#1*"); and that for the second system of simultaneous equations $x^2-24y^2=1$ and $y^2-3pz^2=1$ (where p > 3 is a prime), there is no positive integer solution (the "*Tao (2016) Conjecture-#2*").

Cipu (2007) conjectured that for positive integers *m* and *b*, the number of simultaneous solutions to the Simultaneous Pell Equations $x^2-(4m^2-1)y^2=1$, and $y^2-bz^2=1$ in positive integers isn't greater than one (the "*Cipu (2007) Conjecture*"). If 2m=a, then $x^2-(4m^2-1)y^2=1$ is equivalent to $x^2-(a^2-1)y^2=1$.

Cipu (2018) stated that if one of the following conditions holds: (i) $2a^2-1$ is not a perfect square, (ii) $\{p(\text{mod}8),q(\text{mod}8)\}\neq\{1,3\}$; then the equations $x^2-(a^2-1)y^2=1$ and $y^2-bz^2=1$ have solutions in positive integers *iff* $8a^2(2a^2-1)/b$ is a perfect square - and Jiang (2020) claims to completely solve these equations and the Cipu (2018) models when a>1,b are two positive integers where the square-free part of *b* is 2pq and (p, q) are two distinct odd primes (the "*Jiang (2020) Conjecture-#1*").

Cipu & Mignotte (2007) conjectured that for any distinct nonzero integers a,b, the system of simultaneous Diophantine equations $x^2-ay^2=1$ and $y^2-bz^2=1$, has at most one positive integer solution (x,y,z) for $a=4m^2-1$ (collectively, the "*Cipu & Mignotte (2007) Conjecture*"). Note that $(4m^2-1)$ is equivalent to $(\{2m\}^2-1)$.

Yuan (2004) conjectured that for any distinct non-zero integers (a,b), the system of simultaneous Diophantine equations $x^2-ay^2=1$ and $y^2-bz^2=1$, has a maximum of one positive integer solution (x,y,z) for a=4m(m + 1) (the "*Yuan (2004) Conjecture*").

Keskin, Karaatlı, et. al. (2017) and Irmak (2016) also analyzed the system of simultaneous equations $x^2-24y^2=1$ and $y^2-pz^2=1$.

On solutions for Pell Equations, see: Pinch (1988), Catarino (2019), Ddamulira & Luca (2020), Raza & Malik (2018), Nesterenko (2009) and Lenstra (2008). On quantum algorithms for Pell Equations, see: Hallgren (2007).

On the use of Pell Equations in Cryptology, see: Sarma & Avadhani (2011), Bellini & Murru (2018), Raghunandan (2020) and Muhaya (2014) (ie. each of the equations $x^2-(a^2-1)y^2=1$ and $y^2-pz^2=1$ can be used in cryptoanalysis and in the creation of public-keys). Chu (2008) and Lu & Wu (2016) studied dynamical systems pertaining to Diophantine equations (and each of the equations $x^2-(a^2-1)y^2=1$ and $y^2-pz^2=1$ individually and collectively can approximate Dynamical Systems). Luca, Moree & Weger (2011) discussed *Group Theory* as it relates to Diophantine Equations. Zadeh (2019) notes that Diophantine equations have been used in analytic functions. Stewart (1980), Jones, Sato, et. al. (1976) and Matijasevič (1981) noted that primes can also be represented as Diophantine equations or as polynomials (ie. each of the equations $x^2-(a^2-1)y^2=1$ and $y^2-pz^2=1$ can represent a prime).

2. The Proofs.

Theorem-1: **The *Qu (2018) Conjecture-#1*, The *Yang & Fu (2018) Conjecture-#2* And the Cipu (2007) Conjecture Are Wrong.**

Proof:

Qu (2018) supposedly proved that:

i) where *p* is a prime number, the system of simultaneous Pell equations $x^2-(a^2-1)y^2=1$ and $y^2-pz^2=1$ (collectively, the "Simultaneous Pell System") has only a positive integer solution $(x,y,z) = (31,8,3)$ for

p=7 (the "*Qu (2018) Conjecture-#1*") by using a Baker's lower bound and one lemma from Diophantine approximation to determine the lower and upper bounds respectively, on the variables of the equation; and

ii) there is no positive solution to the Simultaneous Pell System for a=(2,3) (the "*Qu (2018) Conjecture-#2*"); and

iii) the Simultaneous Pell System has a positive integer solution only for a=4 which is (x,y,z,p)=(31,8,3,7) (the "*Qu (2018) Conjecture-#3*").

If: $x^2-(a^2-1)y^2=1$ and $y^2-7z^2=1$ (where p=7), then:
$x^2=(a^2-1)y^2+1$, and $a^2 = 1+(x^2-1)/y^2$

The following are derived from simple simulations.
For the equation $y^2 = 7z^2+1$:

If y=1, z=0
If y=2, z^2 = 3/7, and z isn't an integer.
If y=3, z^2 = 8/7, and z isn't an integer.
If y=4, z^2 = 15/7, and z isn't an integer.
If y=5, z^2 = 24/7, and z isn't an integer.
If y=6, z^2 = 35/7, and z isn't an integer.
If y=7, z^2 = 48/7, and z isn't an integer.
If y=8, z^2 = 63/7 or 9 which is an integer, and z=3.

Thus, y=8 is the lowest feasible positive-integer value of y, and z=3 is the lowest feasible positive-integer value of z for which the equation $y^2-7z^2=1$ is valid.

If y=8 and z=3, and $a^2=1+(x^2-1)/y^2$, then:
$a^2 = 1+(x^2-1)/8^2$ and then:

If: x=1, then a= 1.00000000000
If: x=2, then a= 1.023
If: x=31, then a=4.0000000000
If: x=424, then a=53.009
If: x=432, then a=54.009
If: x=440, then a=55.008948
If x=2096, then a=262.001879
If x=2400, then a=300.001641

Thus, x=1 and (p,x,y,z,a)=(7,1,8,3,1) are feasible values for the simultaneous Pell Equations $x^2-(a^2-1)y^2=1$ and $y^2-7z^2=1$, and the *Qu (2018) Conjecture-#1*, the *Yang & Fu (2018) Conjecture-#2* and the *Jiang (2020) Conjecture-#1* and the "*Cipu (2007) Conjecture* are wrong. ■

Theorem-2: **The *Qu (2018) Conjecture-#2* and the *Yang & Fu (2018) Conjecture-#1* are wrong.**
Proof:
The two equations that define the system are $x^2 -(a^2-1)y^2=1$, and $y^2-pz^2=1$.
For $x^2-(a^2-1)y^2=1$:

Where a=2, then $x^2-3y^2=1$, and $y^2=(x^2-1)/3$
Where a=3, then $x^2-8y^2=1$, and $y^2=(x^2-1)/8$

The following are derived from simple simulations.
If a=2 and $x^2-(a^2-1)y^2=1$ (that is, [$y^2=(x^2-1)/3$]), then:

If x=1, then y=0.000
If x=2, then y=1.000
If x=7, then y=4.000

If x=26, then y=15.000
If x=97, then y=56.000

If a=3 and $x^2-(a^2-1)y^2=1$ (that is, $[y^2=(x^2-1)/8]$), then:
If x=99, then y=35.000000
If x=198, then y=70.002679
If x=396, then y=140.007
If x=577, then y=204.000000
If x=1,154, then y=408.000000

Thus, in the equation $x^2-(a^2-1)y^2=1$, and for a=(2,3), there are "qualifying" positive-integer values of x and y, and because there are potentially and infinitely many "qualifying" positive-integer values of p and z in the associated equation $\boldsymbol{y^2-pz^2=1}$ in the interval $(1;+\infty)$, the *Qu (2018) Conjecture-#2* and the *Yang & Fu (2018) Conjecture-#1* are wrong. ■

Theorem-3: **The Qu (2018) Conjecture-#3 that where p is a prime number, the system of simultaneous Pell equations $x^2-(a^2-1)y^2=1$ and $y^2-pz^2=1$ has only one positive integer solution $(x,y,z,p)=(31,8,3,7)$ for $a=4$; is wrong.**
Proof:
Qu (2018) conjectured that:

i) where p is a prime number, the system of simultaneous Pell equations $x^2-(a^2-1)y^2=1$ and $y^2-pz^2=1$ (collectively, the "Simultaneous Pell System") has only a positive integer solution $(x,y,z) = (31,8,3)$ for $p=7$ (the "*Qu (2018) Conjecture-#1*") by using a Baker's lower bound and one lemma from Diophantine approximation to determine the lower and upper bounds respectively, on the variables of the equation; and

ii) there is no positive solution to the Simultaneous Pell System for $a=(2,3)$ (the "*Qu (2018) Conjecture-#2*"); and

iii) the Simultaneous Pell System has a positive integer solution only for $a=4$ which is $(x,y,z,p)=(31,8,3,7)$ (the "*Qu (2018) Conjecture-#3*").

Let a=4, p=7, z=3,
Then:
3.1) $x^2-(a^2-1)y^2=1$ is equivalent to: $(x^2-1)/15=y^2$, and $x^2=15y^2+1$
3.2) $x^2-(a^2-1)y^2=1$ is equivalent to: $[1+(x^2-1)/y^2] = a^2$
3.3) $y^2-pz^2=1$ is equivalent to: $(y^2-1)/7= z^2$, and $y^2=7z^2+1$

The following are derived from simple simulations.
Where: $x^2-(a^2-1)y^2=1$ is equivalent to: $(x^2-1)/15=y^2$, and $x^2=15y^2+1$; if a=4, then:
x=1, where y=0;
x=4, where y=1.000000;
x=31, where y=8.000000000;
x=244, where y=63.00000000
x=1921, where y=496.000000
x=2653, where y=685.0016058;
x=2715, where y=701.0099381;
x=3873, where y=1000.004267;
x=3904, where y=1008.008433;

Where: $(y^2-1)/p= z^2$, and $y^2=7z^2+1$; a=4, x=31, y=8, then:
p=7, where z=3;

p=63, where z=1;
and thus the solutions (a,x,y,z,p)=(4,31,8,3,7) and (a,x,y,z,p)=(4,31,8,1,63) are feasible.

Given that $x^2-(a^2-1)y^2=1$ is equivalent to: $[1+(x^2-1)/y^2] = a^2$, and if y=8, and p=7 and z=3, then:

If x=0, then a=0.992156742
If x=1, then a=1.000000;
If x=31, then a=4.000000;
If x=400, then a=50.009843;
If x=408, then a=51.009650;
If x=416, then a=52.009464;
If x=456, then a=57.008634;
If x=2096, then a=262.001879;
If x=2400, then a=300.001641;
and thus the solutions (a,x,y,z,p)=(1,1,8,3,8) and (a,x,y,z,p)=(4,31,8,3,7) are feasible.

Thus, the *Qu(2018) Conjecture-#3* is wrong. ■

Theorem-4: The Tao (2016) Conjecture-#1 Is Wrong.

Proof: Tao (2016) conjectured that for the system of simultaneous Pell equations $x^2-24y^2=1$ and $y^2-2pz^2=1$ (where p is an odd prime) there is no positive integer solution (the "*Tao (2016) Conjecture-#1*"); and that for the second system of simultaneous equations $x^2-24y^2=1$ and $y^2-3pz^2=1$ (where p > 3 is a prime), there is no positive integer solution (the "*Tao (2016) Conjecture-#2*"). The following are derived from simple simulations.

If a=5 and $x^2-(a^2-1)y^2=1$ (that is, $[y^2=(x^2-1)/24]$), then:

x=1, where y=0.0000000;
x=5, where y=1.000;
x=49, where y=10.000;
x=147, where y=30.0055550;
x=485, where y=99.0000000;
x=534, where y=109.0021024;
x=1,455 where y=297.0005612;
x=2,425 where y=495.0010101

If x=485; y=99, and $y^2-2pz^2=1$ (ie. $z^2=\{y^2-1\}/2p$), then:

2p=2, and z=70;
2p=8, and z=35;
2p=50, and z=14;
2p=98, and z=10;
2p=200, and z=7;
2p=392, and z=5;
2p=9800, and z=1;
and thus, the solution (x,y,z,2p)=(49,10,70,2) is feasible.

If x=485; y=99, and $y^2-3pz^2=1$ (ie. $z^2=\{y^2-1\}/3p$), then:

3p=2, and z=70;
3p=8, and z=35;
3p=50, and z=14;
3p=98, and z=10;
3p=200, and z=7;
3p=392, and z=5;
3p= 9800, and z=1;
and thus, (x,y,z,3p) has no feasible solution where p>3.

If x=49; y=10, and $y^2-2pz^2=1$ (ie. $z^2=\{y^2-1\}/2p$), then:

2p=11, where z=3;
2p=99, where z=1;
and thus, (x,y,z,2p) doesn't have any feasible solution.

If x=49; y=10, and $y^2-3pz^2=1$ (ie. $z^2=\{y^2-1\}/3p$), then:

3p=11, where z=3
3p=99, where z=1;
and thus, (x,y,z,3p) doesn't have any feasible solution where p>3.

Thus, the *Tao (2016) Conjecture-#1* is wrong because the solution (x,y,z,2p)=(485,99,70,2) is feasible. ■

3. Conclusion.

The *Qu (2018) conjectures*, the *Yang & Fu (2018) conjectures*, the *Jiang (2020) Conjecture-#1*, the *Cipu & Mignotte (2007) Conjecture* and the *Cipu (2007) Conjecture* [all of which pertain to the system of Simultaneous Pell equations $x^2-(a^2-1)y^2=1$ and $y^2-pz^2=1$] are wrong. The *Tao (2016) Conjecture-#1* is also wrong and pertains to the similar system of simultaneous Pell equations $x^2-24y^2=1$ and $y^2-2pz^2=1$.

4. Bibliography.

Ai, X., Chen, J., Zhang, S. & Hu, H. (2015). Complete solutions of the simultaneous Pell equations $x^2-24y^2=1$ and $y^2-pz^2=1$. *Journal Of Number Theory*, 147, 103–108.

Barbeau, E. (1999). *Pell's Equation*. Chapter in: "*Pell's Equation*" (Springer, 1999), pp. 0–387.

Bellini, E. & Murru, N. (2018). A *Multifactor RSA-Like Scheme With Fast Decryption Based On Redei Rational Functions Over The Pell Hyperbola*. Available in www.arxiv.org.

Catarino, P. (2019). On K-Pell hybrid numbers. *Journal of Discrete Mathematical Sciences and Cryptography,* 22(1), 83-89.

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

Cipu, M. (2018). Explicit formula for the solution of simultaneous Pell equations $x^2-(a^2-1)y^2=1$, $y^2-bz^2=1$. *Proceedings Of The American Mathematical Society*, 146, 983–992.

Cipu, M. (2007). Pairs of Pell equations having at most one common solution in positive integers. *Ann. Stiint. Univ. Ovidius Constanta Ser. Math.*, 15, 55–66.

Cipu, M. & Mignotte, M. (2007). On the number of solutions to systems of Pell equations. *Journal Of Number Theory*, 125, 356-392.

Ddamulira, M. & Luca, F. (2020). On the x–coordinates of Pell equations which are k– generalized Fibonacci numbers. *Journal of Number Theory*, 207, 156-195.

Hallgren, S. (2007). Polynomial-time quantum algorithms for Pell's equation and the principal ideal problem. *Journal of the ACM*, 54(1).

Irmak, N. (2016). On solutions of the simultaneous Pell equations x2-(a2-1)y2=1 and y2-bz2=1. *Periodica Mathematica Hungarica*, ______.

Jiang, X. (2020). A note on the simultaneous Pell equations x^2-(a^2-1)y^2=1 and y^2-bz^2=1. *Periodica Mathematica Hungarica*, ________.

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

Keskin, R., Karaatlı, O, et. al. (2017). On the determination of solutions of simultaneous Pell equations $x^2-(a^2-1)y^2 = y^2-pz^2=1$. *Periodica Mathematica Hungarica*, ______.

Lenstra, H. (2008). Solving the Pell equation. *Algorithmic Number Theory*, 44(1), 24.

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 non-negative values of a polynomial in 10 variables. *Journal of Soviet Mathematics*, _________.

Muhaya, F. (2014). Cryptanalysis and security enhancement of Zhu's authentication scheme for Telecare medicine information system. *Secur. Commun. Netw*., 8, 149–158

Nesterenko, A. Y. (2009). Determination of integer solutions of a system of simultaneous Pell equations. *Mathematical Notes*, 86, Article number: 556 (2009). The original Russian text © A. Yu. Nesterenko, 2009, was published in *Matematicheskie Zametki*, 2009, 86(4), 588–600.

Pinch, R. (1988). Simultaneous Pellian equations. *Math. Proc. Cambridge Philos. Soc*., 103(1), 35–46.

Qu, Y. (2018). On simultaneous Pell equations $x^2-(a^2-1)y^2=1$ and $y^2-pz^2=1$. *Journal of Number Theory*, 184, 128-132.

Raghunandan, R. (2020). Image Encryption Scheme in Public Key Cryptography Based on Cubic Pells Quadratic Case. *Indonesian Journal Of Electrical Engineering & Computer Science*, 20(1).

Raza, Z. & Malik, H. (2018). Solution of certain Pell equations. *Asian-European Journal of Mathematics*, 11(4), 1850056 (2018).

Sarma, K. & Avadhani, S. (2011). Public Key Cryptosystem based on Pell's Equation Using The GNU MP Library. *International Journal of Advanced Trends in Computer Science and Engineering*, 3(2).

Stewart, C. (1980). On the representation of an integer in two different bases. *Journal fur die reine und angewandte Mathematik*, 319, 63–72.

Tao, L. (2016). A Note on the Simultaneous Pell Equations x^2-24y^2= 1 and y^2-pz^2=1. *Pure Mathematical Sciences*, 5(1), 27–32.

Yang, H. & Fu, R. (2018). Complete Solutions of the Simultaneous Pell's Equations x^2-(a^2-1)y^2=1 and y^2-pz^2=1. *International Journal of Number Theory*, _______.

Yuan, P. (2004). On the number of solutions of $x^2-4m(m+1)y^2 = y^2-bz^2 = 1$. *Proc. Amer. Math. Soc*., 1561-1566.

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