On Some Properties Of $x^2+y^2+z^2+v^2=dXYZV$; And $x^2+y^2+z^2+v^2+u^2=dXYZVU$, And $x^i+y^i+z^i+v^i=dXYZV$.

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 develops "existence" properties for the equations $x^2+y^2+z^2+v^2=dXYZV$; ***And*** $x^2+y^2+z^2+v^2+u^2=dXYZVU$, and $x^i+y^i+z^i+v^i=dXYZV$ (where *i* is a positive integer). Collectively and individually, these equations have wide applications in Computer Science, Physics, Applied Math and Finance/Economics.

Keywords: *Markoff Equation*; Prime Numbers; Dynamical Systems; Mathematical Cryptography; *Beal Conjecture*; Diophantine Equations; Nonlinear Equations.

1. Introduction.

Equations such as $x^2+y^2+z^2+v^2=dXYZV$; and $x^2+y^2+z^2+v^2+u^2=dXYZVU$; and $x^i+y^i+z^i+v^i=dXYZV$ (where *i* is a positive integer) have not been studied in detail in the literature.

2. Existing Literature.

Silverman (1990), Abram, Lapointe & Reutenauer (2020), Bourgain, Gamburd & Sarnak (2016), Chen & Chen (2013), Gaire (2018), González-Jiménez & Tornero (2013), Jiang, Gao & Cao (2020), McGinn (2015) and Togbe, Kafle & Srinivasan (2020) analyzed the *Markoff Equation* $X^2 + Y^2 + Z^2 = aXYZ$; which perhaps is the most popular equation that is structurally similar to the equations studied in this article. However, the properties and methods introduced herein are new.

On other approaches to solving Diophantine Equations, see: Rahmawati, Sugandha, et. al. (2019), and Ibarra & Dang (2006). *On Homomorphisms*, see: Wang & Chin (2012). Zadeh (2019) notes that Diophantine equations have been used in analytic functions. Chu (2008) and Lu & Wu (2016) studied dynamical systems pertaining to Diophantine equations (and equations such as $x^2+y^2+z^2+v^2=dXYZV$, and $x^2+y^2+z^2+v^2+u^2=dXYZVU$, and $x^i+y^i+z^i+v^i=dXYZV$ 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 also be represented as Diophantine equations or as polynomials (ie. each of the equations $x^2+y^2+z^2+v^2=dXYZV$, and $x^2+y^2+z^2+v^2+u^2=dXYZVU$, and $x^i+y^i+z^i+v^i=dXYZV$, can represent a prime). On uses of Diophantine Equations in Cryptography see: Ding, Kudo, et. al. (2018), Okumura (2015), and Ogura (2012) (ie. each of the the equations $x^2+y^2+z^2+v^2=dXYZV$, and $x^2+y^2+z^2+v^2+u^2=dXYZVU$, and $x^i+y^i+z^i+v^i=dXYZV$ can be used in cryptoanalysis, and in the creation of public-keys). Zadeh (2019) notes that Diophantine equations have been used in analytic functions.

The *Beal Conjecture* states that if *a*, *b*, *c*, *x*, *y*, and *z* are positive integers where $a^x+b^y=c^z$, and $x, y, z > 2$, then *a*, *b* and *c* have a common prime factor. The methods introduced in this article may help resolve the *Beal Conjecture* and similar problems.

3. The Theorems.

Theorem-1: **For the equation $X^2+Y^2+Z^2+V^2=XYZVg$, if (*n-f*) is a multiplicative component of each of X, Y, V & Z (each of X,Y, V and Z are derived by multiplying (*n-f*) by another real number), then XYZV*g* = (*n-f*), for some real number *g*.**
Proof:

Let:
X = (n-f)a
Y = (n-f)b
Z = (n-f)c
V = (n-f)j
Let: X/a = Y/b = Z/c =V/j= (n-f) = XYZVg

Where $-\infty<n,f,a,b,c,j< +\infty$; and n,f,a,b, j and c are real numbers.

$X^2 = (n-f)a*(n-f)a = (n-f)(n-f)a^2 = (n^2-nf-nf+f^2)a^2 = n^2a^2-2nf(a^2)+f^2a^2$
$Y^2 = (n-f)b*(n-f)b = (n-f)(n-f)b^2 = (n^2-nf-nf+f^2)b^2 = n^2b^2-2nf(b^2)+f^2b^2$
$Z^2 = (n-f)c*(n-f)c = (n-f)(n-f)c^2 = (n^2-nf-nf+f^2)c^2 = n^2c^2-2nf(c^2)+f^2c^2$
$V^2 = (n-f)j*(n-f)j = (n-f)(n-f)j^2 = (n^2-nf-nf+f^2)j^2 = n^2j^2-2nf(j^2)+f^2j^2$

Thus:
$X^2+Y^2+Z^2+V^2 = n^2(a^2+b^2+c^2+j^2)-2nf(a^2+b^2+c^2+j^2)-f^2(a^2+b^2+c^2+j^2) = (n^2-2nf-f^2)(a^2+b^2+c^2+j^2)$

Then:
a = 1/YZVg
b = 1/XZVg
c = 1/XYVg
j = 1/XYZg

$X^2+Y^2+Z^2+V^2 = (n^2-2nf-f^2)(a^2+b^2+c^2+j^2) = (n-f)(n-f)(a^2+b^2+c^2+j^2) = (XYZVg)^2(a^2+b^2+c^2+j^2)$
$= [(XYZVg)^2(1/(YZVg)^2)]+[(XYZVg)^2(1/(XZVg^2))]+[(XYZVg)^2(1/(XYVg)^2)]+[(XYZVg)^2(1/(XYZg)^2)]$
$= [(XYZVg)^2/(YZVg)^2]+[(XYZVg)^2/XZVg^2)]+[(XYZVg)^2/(XYVg)^2)]+[(XYZVg)^2/(XYZg)^2)]$
$= X^2+Y^2+Z^2+V^2$ ■

Theorem-2: **For the equation $X^2+Y^2+Z^2+V^2=?$, and for all values of X, Y, V and Z that are real numbers, if (n-f)=gXYZV, and (n-f) is a multiplicative component of each of X,Y, V and Z, then there exists a real number *d* such that $X^2+Y^2+Z^2+V^2$ = dXYZV; where for all g that are real numbers, g ϵ d.**
Proof:
As stated herein and above:
X/a = Y/b = Z/c =V/j= (n-f) = XYZVg
a = 1/YZVg
b = 1/XZVg
c = 1/XYVg
j = 1/XYZg
(n-f) = gXYZV

Thus, gXYZV is a multiplicative component of each of X, Y, V and Z. That is:
X=(gXYZV)(a); and Y=(gXYZV)(b); and Z=(gXYZV)(c); and V=(gXYZV)(j)

If: $X^2+Y^2+Z^2+V^2$ = dXYZV;

Then by substitution: $[(g^2X^2Y^2Z^2V^2)(a^2)]+[(g^2X^2Y^2Z^2V^2)(b^2)]+[(g^2X^2Y^2Z^2V^2)(c^2)]+[(g^2X^2Y^2Z^2V^2)(j^2)] =$ dXYZV

Then by dividing both sides of the equation by dXYZV and substituting a=(1/YZg), b=(1/XZg) and c=(1/XYg), and j = 1/XYZg, the result is:
$\{[(g^2X^2Y^2Z^2V^2)(1/(Y^2Z^2V^2g^2))]/dXYZV\}+\{[(g^2X^2Y^2Z^2V^2)(1/(X^2Z^2V^2g^2))]/dXYZV\}+$
$\{[(g^2X^2Y^2Z^2V^2)(1/(X^2Y^2V^2g^2))]/dXYZV\}+\{[(g^2X^2Y^2Z^2V^2)(1/(X^2Y^2Z^2g^2))]/dXYZV\} = 1;$
and thus: [(X/dYZV)+(Y/dXZV)+(Z/dXYV)+(V/dXYZ)] = 1

By taking a common denominator dXYZV for the left-hand side of the equation, the result is:
$[(X^2+Y^2+Z^2+V^2)/dXYZV] = 1;$
and by multiplying both sides of the equation by dXYZV, the result is: $X^2+Y^2+Z^2+V^2= dXYZV$

d can be expressed solely in terms of g, X, Y, V and Z as follows:
$\{[((g^2X^2Y^2Z^2V^2)(1/(Y^2Z^2V^2g^2)))]+[((g^2X^2Y^2Z^2V^2)(1/(X^2Z^2V^2g^2)))]+[((g^2X^2Y^2Z^2 V^2)(1/(X^2Y^2V^2g^2)))]$
$+[((g^2X^2Y^2Z^2V^2)(1/(X^2Y^2Z^2g^2)))]\}/XYZV = d;$

Similarly, *d* can also be expressed solely in terms of X, Y, V and Z as follows:
$\{[((X^2Y^2Z^2V^2)(1/(Y^2Z^2V^2g^2)))/XYZV]+[((g^2X^2Y^2Z^2V^2)(1/(X^2Z^2V^2g^2)))/XYZV]+[((g^2X^2Y^2Z^2V^2)(1/(X^2Y^2V^2g^2)))$
$/XYZV]+ [((g^2X^2Y^2Z^2V^2)(1/(X^2Y^2Z^2g^2)))/XYZV]\}= d = [(X/YZV)+(Y/XZV)+(Z/XYV)+(V/XYZ)]$

Given the foregoing and since X=(gXYZV)(a); and Y=(gXYZV)(b); and Z=(gXYZV)(c); and V=(gXYZV)(j); and $X^2+Y^2+Z^2+V^2=$ dXYZV, for all *g*, X, Y, Z and V that are real numbers, *g*<*d*; and *g* ϵ *d*. ■

Theorem-3: **For The Equation $X^i+Y^i+Z^i+V^i$=?, And Given Theorem-7 Above, And For All Values Of X, Y, V And Z That Are Real Numbers, If (n-f)=gXYZV, And (n-f) Is A Multiplicative Component Of Each Of X,Y, V and Z, Then There Exists A Real Number *d* Such That $X^i+Y^i+Z^i +V^i$= dXYZV; Where For All g, X, Y, V and Z That Are Real Numbers, g ϵ d; And *d* Can Be Expressed as *d* = $[(X^{(i-1)}/YZV)+(Y^{(i-1)}/XZV)+(Z^{(i-1)}/XYV)+(V^{(i-1)}/XYZ)]$.**
Proof: The proof is straightforward and follows from prior proofs above.

■

Theorem-4: **For The Equation $X^2+Y^2+Z^2+V^2+U^2$=?, If (*n-f*) Is A Multiplicative Component Of Each Of X, Y, V, U And Z (Each Of X,Y, V, U And Z Are Derived By Multiplying (*n-f*) By Another Real Number), Then XYZVU*g* = (*n-f*), For Some Real Number *g*.**
Proof:

Let:
X = (n-f)a
Y = (n-f)b
Z = (n-f)c
V = (n-f)j
U= (n-f)k

Where -∞<n,f,a,b,c,j<+∞ are real numbers.

$X^2 = (n-f)a*(n-f)a = (n-f)(n-f)a^2 = (n^2-nf-nf+f^2)a^2 = n^2a^2-2nf(a^2)+f^2a^2$
$Y^2 = (n-f)b*(n-f)b = (n-f)(n-f)b^2 = (n^2-nf-nf+f^2)b^2 = n^2b^2-2nf(b^2)+f^2b^2$
$Z^2 = (n-f)c*(n-f)c = (n-f)(n-f)c^2 = (n^2-nf-nf+f^2)c^2 = n^2c^2-2nf(c^2)+f^2c^2$
$V^2 = (n-f)j*(n-f)j = (n-f)(n-f)j^2 = (n^2-nf-nf+f^2)j^2 = n^2j^2-2nf(j^2)+f^2j^2$

$U^2 = (n-f)k*(n-f)k = (n-f)(n-f)k^2 = (n^2-nf-nf+f^2)k^2 = n^2k^2-2nf(k^2)+f^2k^2$

Thus:
$X^2+Y^2+Z^2+V^2 +U^2 = n^2(a^2+b^2+c^2+j^2+k^2)-2nf(a^2+b^2+c^2+j^2+k^2)-f^2(a^2+b^2+c^2+j^2+k^2)= (n^2-2nf-f^2)(a^2+b^2+c^2+j^2+k^2)$

Given the foregoing, let:
X/a = Y/b = Z/c =V/j= U/k = (n-f) = XYZVUg
Then:
a = 1/YZVUg
b = 1/XZVUg
c = 1/XYVUg
j = 1/XYZUg
k = 1/XYZVg

$X^2+Y^2+Z^2+V^2 +U^2 = (n^2-2nf-f^2)(a^2+b^2+c^2+j^2+k^2) = (n-f)(n-f)(a^2+b^2+c^2+j^2+k^2) = (XYZVUg)^2(a^2+b^2+c^2+j^2+k^2)$
$=$
$[(XYZVUg)^2(1/(YZVUg)^2)]+[(XYZVUg)^2(1/(XZVUg^2))]+[(XYZVUg)^2(1/(XYVUg)^2)]+[(XYZVUg)^2(1/(XYZUg)^2)] +[(XYZVUg)^2(1/(XYZVg)^2)]$

$= [(XYZVUg)^2/(YZVUg)^2]+[(XYZVUg)^2/XZVUg^2)]+[(XYZVUg)^2/(XYVUg)^2)]+[(XYZVUg)^2/(XYZUg)^2)] +[(XYZVUg)^2/(XYZVg)^2)]$
$= X^2+Y^2+Z^2+V^2 +U^2$ ■

Theorem-5: **For The Equation $X^2+Y^2+Z^2+V^2+U^2$=?, And For All Values Of X, Y, V, U And Z That Are Real Numbers, If (n-f)=gXYZVU, And (n-f) Is A Multiplicative Component Of Each Of X,Y, V, U And Z, Then There Exists A Real Number *d* Such That $X^2+Y^2+Z^2+V^2+U^2$ = dXYZVU; Where For All g That Are Real Numbers, g ϵ d.**
Proof:
As stated herein and above:
X/a = Y/b = Z/c =V/j= U/k = (n-f) = XYZVUg
a = 1/YZVUg
b = 1/XZVUg
c = 1/XYVUg
j = 1/XYZUg
k = 1/XYZVg
(n-f) = gXYZVU

Thus, gXYZVU is a multiplicative component of each of X, Y, V and Z. That is:
X=(gXYZVU)(a); and Y=(gXYZVU)(b); and Z=(gXYZVU)(c); and V=(gXYZVU)(j); and U=(gXYZVU)(k)

If: $X^2+Y^2+Z^2+V^2+U^2$ = dXYZVU;
Then by substitution: $[(g^2X^2Y^2Z^2V^2U^2)(a^2)]+[(g^2X^2Y^2Z^2V^2U^2)(b^2)]+[(g^2X^2Y^2Z^2V^2U^2)(c^2)]+[(g^2X^2Y^2Z^2V^2U^2)(j^2)] +[(g^2X^2Y^2Z^2V^2U^2)(k^2)] = dXYZVU$

Then by dividing both sides of the equation by dXYZVU and substituting a=(1/YZVUg), b=(1/XZVUg) and c=(1/XYVUg), and j = 1/ XYZUg, and k = 1/XYZVg into the result, the result is:
$\{[(g^2X^2Y^2Z^2V^2U^2)(1/(Y^2Z^2V^2U^2g^2))]/dXYZVU\}+\{[(g^2X^2Y^2Z^2V^2U^2)(1/(X^2Z^2V^2U^2g^2))]/dXYZVU\}+ \{[(g^2X^2Y^2Z^2V^2U^2)(1/(X^2Y^2V^2U^2g^2))]/dXYZVU\}+\{[(g^2X^2Y^2Z^2V^2U^2)(1/(X^2Y^2Z^2U^2g^2))]/dXYZVU\} +\{[(g^2X^2Y^2Z^2V^2U^2)(1/(X^2Y^2Z^2U^2g^2))]/dXYZVU\} = 1;$
and thus: [(X/dYZVU)+(Y/dXZVU)+(Z/dXYVU)+(V/dXYZU)+(U/dXYZV)] = 1

By taking a common denominator dXYZVU for the left-hand side of the equation, the result is:
$[(X^2+Y^2+Z^2+V^2+U^2)/dXYZVU] = 1$;
and by multiplying both sides of the equation by dXYZVU, the result is: $X^2+Y^2+Z^2+V^2+U^2= dXYZVU$

d can be expressed solely in terms of g, X, Y, V, U and Z as follows:
$\{[((g^2X^2Y^2Z^2V^2U^2)(1/(Y^2Z^2V^2U^2g^2)))]+[((g^2X^2Y^2Z^2V^2U^2)(1/(X^2Z^2V^2U^2g^2)))]+[((g^2X^2Y^2Z^2V^2U^2)(1/(X^2Y^2V^2U^2g^2)))] +[((g^2X^2Y^2Z^2V^2U^2)(1/(X^2Y^2Z^2U^2g^2)))] +[((g^2X^2Y^2Z^2V^2U^2)(1/(X^2Y^2Z^2V^2g^2)))]\}/XYZVU = d$;

Similarly, *d* can also be expressed solely in terms of X, Y, V, U and Z as follows:
$\{[((g^2X^2Y^2Z^2V^2U^2)(1/(Y^2Z^2V^2U^2g^2)))]+[((g^2X^2Y^2Z^2V^2U^2)(1/(X^2Z^2V^2U^2g^2)))]+[((g^2X^2Y^2Z^2V^2U^2)(1/(X^2Y^2V^2U^2g^2)))] +[((g^2X^2Y^2Z^2V^2U^2)(1/(X^2Y^2Z^2U^2g^2)))] +[((g^2X^2Y^2Z^2V^2U^2)(1/(X^2Y^2Z^2V^2g^2)))]\}/XYZVU = d = [(X/YZVU)+(Y/XZVU)+(Z/XYVU)+(V/XYZU)+(U/XYZV)]$

Given the foregoing and since X=(gUYZV)(a); and Y=(gXYZV)(b); and Z=(gXYZV)(c); and V=(gXYZU)(j); and U=(gXYZV)(k); and $X^2+Y^2+Z^2+V^2+U^2 =dXYZVU$, for all *g*, X, Y, Z, U and V that are real numbers, $g<d$; and $g \in d$. ■

Conclusion.

Some relevant properties of the equations $\boldsymbol{x^2+y^2+z^2+v^2=dXYZV}$, and $\boldsymbol{x^2+y^2+z^2+v^2+u^2=dXYZVU}$ and $\mathbf{x^i+y^i+z^i + v^i =dXYZV}$ (where *i* is a positive integer), have been introduced and which can help in solving those and related equations.

Bibliography.

Abram, A., Lapointe, M. & Reutenauer, C. (2020). Palindromization and construction of Markoff triples. *Theoretical Computer Science*, 80924, 21-29.

Bourgain, J., Gamburd, A. & Sarnak, P. (2016). Markoff triples and strong approximation. *Comptes Rendus Mathematique*, 354, 131-135.

Chen, F. & Chen, Y. (2013). On the Frobenius conjecture for Markoff numbers. *Journal of Number Theory*, 133, 2363-2373.

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).

Gaire, Y. (2018). On the Unicity Conjecture for Generalized Markoff Equation. *Journal of Advanced College of Engineering and Management*, 3, 137-145.

González-Jiménez, E. & Tornero, J. (2013). Markoff–Rosenberger triples in arithmetic progression. *Journal of Symbolic Computation*, 53, 53-63.

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

Jiang, K., Gao, W. & Cao, W. (2020). Counting solutions to generalized Markoff-Hurwitz-type equations in finite fields. *Finite Fields and Their Applications*, 62, in-press.

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

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

McGinn, D. (2015). Generalized Markoff equations and Chebyshev polynomials. *Journal of Number Theory*, 152, 1-20.

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

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.

Silverman, J. (1990). The *Markoff Equation* $X^2+Y^2+Z^2 = aXYZ$ over quadratic imaginary fields. *Journal of Number Theory*, 35(1), 72-104.

Togbe, A., Kafle, B. & Srinivasan, A. (2020). Markoff Equation with Pell components. *Colloquium Mathematicum*, 159(2020), 61-69.

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.