The Coordinate Equation & Fermat's Last Theorem

Richard J. Miller
richard@urmt.org
Issue 1.1 05/05/2021

Abstract

This paper presents a Diophantine equation, known as the Coordinate Equation, which is identical in form to that of Fermat's Last Theorem barring a modification that permits solutions for all exponents, quadratic and higher. The modification adds an extra term containing a factor such that, when the factor is zero, the equation reduces to Fermat's Last Theorem. It is then shown that any FLT counter-example, exponent *n*, is a solution to the Coordinate Equation, with a non-zero factor, for all higher order exponents *mn*, arbitrary odd *m*, three or greater.

Theory

(1) Definition. The ***Coordinate Equation*** (CE) is defined as follows in terms of three, non-zero integers x, y, z, exponent *n*, for some integer k:

$$0 = x^n + y^n - z^n + kxyz \tag{1}$$

The full list of conditions[1] used herein is

$$x, y, z, k, n \in \mathbb{Z},\ n \geq 2,\ 1 < x < y < z \tag{1b}$$
$$\gcd(x, y) = \gcd(y, z) = \gcd(z, x) = 1$$

The exponent purposefully includes the $n = 2$ Pythagorean case since this too is covered in the work. There is no restriction on *n* being odd, even or composite, just $n \geq 2$.

(2) Fermat's Last Theorem states that there are no solutions to the following Diophantine equation (hereafter referred to as The FLT Equation) for exponent $n > 2$ and positive integers $0 < x, y, z$:

$$0 = x^n + y^n - z^n \tag{2}$$

FLT was first proven by Wiles [1] but, nevertheless, it is assumed one or more FLT solutions, i.e. counter-examples, exist. Given the Pythagorean exponent $n = 2$ is included in (1), which does, of course, have solutions, this also gives a check on all developments in the paper.

(3) Lemma. Every FLT solution satisfies the following congruences:

$$\begin{aligned} y^n &\equiv z^n \pmod{x} \\ x^n &\equiv z^n \pmod{y} \\ x^n &\equiv -y^n \pmod{z} \end{aligned} \tag{3}$$

Proof. By taking residues of (1) to moduli x, y, z then the three congruences can be seen to be true and, therefore, every solution must necessarily satisfy them. The congruences by themselves are not sufficient to only define solutions x, y, z. That they are not sufficient can be seen by solving the congruences to give, for some arbitrary integers a, b, c,

$$\begin{aligned} y^n - z^n &= ax \\ z^n - x^n &= by \end{aligned} \tag{4}$$

$$x^n + y^n = cz$$

These three equations can only agree with FLT (2) for the unique values $a = x^{n-1}$, $b = y^{n-1}$ and $c = z^{n-1}$, whereas the congruences have an infinite set of solutions for arbitrary integers a,b,c. Hence the congruences are not a sufficient condition to only give counter-example solutions to FLT.

In contrast to FLT (2), the CE (1) is derived such that the above congruences are both necessary and sufficient as in the next theorem.

(5) Theorem: All solutions to the congruences (3) are solutions to the CE[2]

Proof. Keeping with the expansion of the congruences (4), the most general form for the integers a,b,c are arbitrary polynomials of up to degree $n-1$ in x,y,z. Given a,b,c multiply linear factors x,y,z respectively, then taking the modulus x,y,z, respectively, reduces ax,by,cz to zero regardless of the polynomial forms of a,b,c.

Without loss of generality, the polynomials a,b,c are expanded in the following form, for some polynomials *f*, *g* and *h*, and non-zero integers s,t,u, both discussed shortly:

$$\begin{aligned} ax &= -sx^n - xf(x,y,z) \\ by &= ty^n + yg(x,y,z) \\ cz &= uz^n - zh(x,y,z) \end{aligned} \tag{6}$$

Looking at, for example, the first of these terms, i.e. $-sx^n - xf(x,y,z)$, all that has been done here is to separate-out the x^n term in ax, and $f(x,y,z)$ is another arbitrary polynomial in all three variables of degree $n-1$. Note that the multiplicative factor of *x* implies the term $xf(x,y,z)$ has no constant term, i.e. the lowest degree term in ax is *x*, and the highest degree term is x^n. The other two equations are explained likewise.

Substituting (6) into (4) gives

$$\begin{aligned} y^n &= z^n - sx^n - xf(x,y,z) \\ z^n &= x^n + ty^n + yg(x,y,z) \\ x^n + y^n &= uz^n - zh(x,y,z) \end{aligned} \tag{7}$$

and rearranging these into a common form as follows:

$$\begin{aligned} 0 &= sx^n + y^n - z^n + xf(x,y,z) \\ 0 &= x^n + ty^n - z^n + yg(x,y,z) \\ 0 &= x^n + y^n - uz^n + zh(x,y,z) \end{aligned} \tag{8}$$

immediately shows that for all three to be simultaneously satisfied, and hence the congruences (3) to be simultaneously satisfied, the integers s,t,u must all be unity, i.e.

$$s = t = u = 1 \tag{9}$$

and all three equations must have a common polynomial form '$xyzk(x,y,z)$' for some polynomial 'constant' $k(x,y,z)$ as in

$$\begin{aligned} xf(x,y,z) &= xyzk(x,y,z) \\ yg(x,y,z) &= yxzk(x,y,z) \\ zh(x,y,z) &= zxyk(x,y,z) \end{aligned} \tag{10}$$

Combining all three equations (8) using (9) and (10) gives one and the same Diophantine equation, i.e.

$$0 = x^n + y^n - z^n + xyzk(x, y, z) \tag{11}$$

which is just the CE (1), whereby $k(x, y, z)$ is hereafter abbreviated to just k, i.e. $k = k(x, y, z)$.

Thus, proving by its construction[2], all solutions to the congruences (3) are solutions of the CE.

(12) Theorem. Every solution to FLT (2) is a solution to the CE (1)

Proof. By Theorem (5), the CE (1) captures every solution to the congruences (3) and, given every FLT solution must satisfy these congruences by Lemma (3), then every FLT solution must be a solution to the CE in the special case when $k = 0$.

(13) Definition. An ***integer root of unity u***, simply termed a ***unity root*** hereafter, to exponent *n*, mod *p*, is defined as follows, where *p* is an integer greater than one but not necessarily prime:

$$u^n \equiv \pm 1 \pmod{p} \tag{13}$$

The modulus *p* is restricted to the set of the three integers x, y, z in (1), which are all greater than one by (1b)

(19) Theorem. There exist unity roots P, Q, R and $\overline{P}, \overline{Q}, \overline{R}$ such that every CE solution satisfies the following three linear equations:

$$x = Ry + \overline{Q}z \tag{14a}$$
$$y = \overline{R}x + Pz \tag{14b}$$
$$z = Qx + \overline{P}y \tag{14c}$$

Symbols P, Q, R and $\overline{P}, \overline{Q}, \overline{R}$ are just labels here for six distinct unity roots, and no special significance or relevance is assigned to the over-struck bar within the context of this paper.

Proof. Firstly, taking *x* as an example, then given the GCD condition (1b), *x* can be written as the linear superposition (4a) in terms of *y* and *z* for some integers, denoted here as *R* and $\overline{Q}$. This is merely a statement that, for co-prime x, y, z, there exist some integers *R* and $\overline{Q}$ such that the above linear Diophantine equation (4a) has solutions [2].

Raising *x* (4a) to the exponent *n* gives an equation of the following form, for some $n-2$ degree polynomial $S(R, \overline{Q}, y, z)$:

$$x^n = R^n y^n + \overline{Q}^n z^n + yzS(R, \overline{Q}, y, z) \tag{15a}$$

Likewise, for *y* (4b) and *z* (4c), raising to the exponent *n* then, for some $n-2$ degree polynomials $T(P, \overline{R}, x, z)$ and $U(\overline{P}, Q, x, y)$, gives

$$y^n = \overline{R}^n x^n + P^n z^n + xzT(P, \overline{R}, x, z) \tag{15b}$$
$$z^n = Q^n x^n + \overline{P}^n y^n + xyU(\overline{P}, Q, x, y) \tag{15c}$$

Taking residues mod x, y, z gives nine separate congruences, six of which are

$$x^n \equiv R^n y^n \pmod{z}, \; x^n \equiv \overline{Q}^n z^n \pmod{y}$$
$$y^n \equiv \overline{R}^n x^n \pmod{z}, \; y^n \equiv P^n z^n \pmod{x} \tag{16}$$

$$z^n \equiv Q^n x^n \pmod{y},\ z^n \equiv \overline{P}^n y^n \pmod{x}$$

and the less useful remaining three are

$$\begin{aligned} 0 &\equiv R^n y^n + \overline{Q} z^n + yzS(R,\overline{Q},y,z) \pmod{x} \\ 0 &\equiv \overline{R}^n x^n + P^n z^n + xzT(P,\overline{R},x,z) \pmod{y} \\ 0 &\equiv Q^n x^n + \overline{P}^n y^n + xyU(\overline{P},Q,x,y) \pmod{z} \end{aligned} \tag{17}$$

These last three congruences merely serve as defining conditions on the polynomials $S(R,\overline{Q},y,z)$, $T(P,\overline{R},x,z)$ and $U(\overline{P},Q,x,y)$, and are of no further use given the polynomials require no further definition.

The six congruences (16) are made consistent with the original congruences (3) by defining the variables P,Q,R and $\overline{P},\overline{Q},\overline{R}$ as unity roots (4), as follows:

$$\begin{aligned} P^n &\equiv 1 \pmod{x},\ Q^n \equiv 1 \pmod{y},\ R^n \equiv -1 \pmod{z} \\ \overline{P}^n &\equiv 1 \pmod{x},\ \overline{Q}^n \equiv 1 \pmod{y},\ \overline{R}^n \equiv -1 \pmod{z} \end{aligned} \tag{18}$$

Given the above definitions, then none of the unity roots is ever zero, i.e.

$$P,Q,R \in \mathbb{Z},\ (P,Q,R) \neq (0,0,0),\ \overline{P},\overline{Q},\overline{R} \in \mathbb{Z},\ (\overline{P},\overline{Q},\overline{R}) \neq (0,0,0) \tag{19}$$

Thus, all solutions x,y,z to FLT can be written as three linear equations (14) in terms of the unity roots P,Q,R and $\overline{P},\overline{Q},\overline{R}$.

Note that the three linear equations (19) can also be written as an eigenvector equation, unity eigenvalue, for the following eigenvector **X** and matrix **A** comprising the unity roots (18):

$$\mathbf{A} = \begin{pmatrix} 0 & R & \overline{Q} \\ \overline{R} & 0 & P \\ Q & \overline{P} & 0 \end{pmatrix},\ \mathbf{X} = \begin{pmatrix} x \\ y \\ z \end{pmatrix} \tag{20}$$

$$\mathbf{AX} = \mathbf{X}$$

This eigenvector approach is detailed in [4] but not required further herein.

(21) Example. An example solution x,y,z to the CE (1), constant *k*, for each exponent *n* from quadratic to quintic, is tabulated below, together with their unity roots (18); see [3] for an extensive list of solutions to the CE equation.

n	x	y	z	k	P	Q	R	$\overline{P}$	$\overline{Q}$	$\overline{R}$
2	4	3	5	0	-1	2	-2	-1	2	2
3	9	31	70	16	-155	273	-11	-77	5	1209
4	15	16	17	-8	8	-1	2	2	-1	-8
5	5	11	31	16695	1	4	-8	1	3	-4

(30) Theorem. For every odd exponent $n = 2p+1,\ p \in \mathbb{Z},\ p \geq 1$, arbitrary x,y (1b), the Coordinate Equation has a solution of the following form:

$$z = x + y \tag{30}$$

Proof. Using $z = x + y$, then expanding z^n by the binomial theorem gives

$$z^n = (x+y)^n = x^n + y^n + \sum_{r=1}^{n-1} {}^nC_r x^{n-r} y^r \tag{31}$$

where ${}^nC_r$ is the usual combinatorial expression ${}^nC_r = n!/(n-r)!r!$.

By the remainder theorem for polynomials, for odd exponent n, a factor of $(x^n + y^n)$ on the right of (31) is $(x+y)$, since $x=-y$ is a solution to $(x^n + y^n) = 0$. As the left of (31) is also a power of $(x+y)$, it is concluded that the summation term on the right also factors by $(x+y)$, for some function $f(x,y)$, as follows:

$$\sum_{r=1}^{n-1} {}^nC_r x^{n-r} y^r = (x+y) f(x,y) \tag{32}$$

Furthermore, since the summation has terms of minimum, first degree in x and y, then it can be factored further, for some function $g(x,y)$, as

$$\sum_{r=1}^{n-1} {}^nC_r x^{n-r} y^r = xy(x+y)g(x,y) \tag{33}$$

Substituting this summation and $z = x+y$ (30) into the binomial expansion (31) gives

$$z^n = x^n + y^n + xyzg(x,y) \tag{34}$$

This is the same as the Coordinate Equation (1), where polynomial $k(xyz)$ and function $g(x,y)$ are identical, i.e.

$$k(x,y,z) \equiv g(x,y) \tag{35}$$

Hence, the solution $z = x+y$ is a solution to the CE for arbitrary, odd exponent n. Given this, it remains to show that theorem (19) is also satisfied, i.e. unity roots P, Q, R and $\overline{P}, \overline{Q}, \overline{R}$ (18) can always be found for arbitrary x, y (1b). Indeed, by choosing the following unity roots:

$$P = 1,\ \overline{P} = 1,\ Q = 1,\ \overline{Q} = 1,\ R = -1,\ \overline{R} = -1 \tag{36}$$

and applying these unity root values to linear equations (14) gives the following three equations:

$$\begin{aligned} R = -1,\ \overline{Q} = 1 &\Rightarrow x = -y + z \\ \overline{R} = -1,\ P = 1 &\Rightarrow y = -x + z \\ Q = 1,\ \overline{P} = 1 &\Rightarrow z = x + y \end{aligned} \tag{37}$$

It is seen that these are all just rearrangements of the single equation $z = x+y$, hence the $z = x+y$ solution is valid for the particular choice of unity roots (36). However, these unity roots satisfy their definitions (18) for all moduli x, y, z with no restriction on x, y, z barring conditions (1b), and thus satisfying Theorem (19) that there exists a set of unity roots for every CE solution.

Thus, the solution $z = x+y$ (30) is a solution to the Coordinate Equation for arbitrary odd exponent $n \geq 3$, arbitrary x, y (1b), for which a set of unity roots (36) can always be found.

(38) Corollary. The value of k for the $z = x+y$ solution to the Coordinate Equation is always positive.

Proof. This is almost trivially proven since the summation term in (31) is identical to the $kxyz$ term in the CE (1), i.e. rearranging (31) using (1) implies

$$z^n - \left(x^n + y^n\right) = \sum_{r=1}^{n-1} {}^nC_r x^{n-r} y^r = kxyz \tag{39}$$

and given ${}^nC_r > 0$ for $1 \le r \le n-1$, and $1 < x < y$ (1b), then every term in the summation is positive, and so the entire sum is always positive, i.e.

$$\sum_{r=1}^{n-1} {}^nC_r x^{n-r} y^r > 0 \Rightarrow k > 0 \tag{40}$$

Note that the solution $z = x + y$ is valid only for odd exponent $n \ge 3$, excluding all even exponents.

(41) Corollary. For a cubic exponent $n = 3$, the $z = x + y$ (30) solution to the Coordinate Equation has a constant value $k = 3$ for all x, y (1b).

Proof. For $n = 3$, the polynomial expansion of (31) in Theorem (30) gives

$$z^3 = x^3 + y^3 + 3xy(x + y) \tag{42}$$

and, since $z = x + y$, this simply becomes

$$z^3 = x^3 + y^3 + 3xyz \tag{43}$$

Comparing this with the CE form (34), it is seen that the polynomial $g(x, y)$ is just a constant value $g(x, y) = 3$ and so, by (35), *k* is just the constant value $k = 3$ for all solutions x, y.

This smallest of odd exponents is the only value which has such a simple, constant value of *k*. For higher order, odd exponents $n \ge 5$, *k* grows rapidly, see [3].

(44) Theorem. If x, y, z is an FLT counter-example or Pythagoras solution, exponent $n \ge 2$, then for arbitrary odd, integer $m = 2p + 1$, $p \in \mathbb{Z}$, $p \ge 1$, it is also a CE solution for exponent $mn \ge 6$, with a positive *k*.

Proof. Defining X, Y, Z as follows:

$$X = x^n,\ Y = y^n,\ Z = z^n \tag{45}$$

then, since x, y, z is a solution (2) for $n \ge 2$,

$$z^n = x^n + y^n \Rightarrow Z = X + Y \tag{46}$$

However, by Theorem (30), for arbitrary x, y, and hence too arbitrary X, Y, for odd exponent *m*, then $Z = X + Y$ is a solution to

$$0 = X^m + Y^m - Z^m + kXYZ \tag{47}$$

Substituting back for X, Y, Z in terms of x, y, z and rearranging gives

$$0 = \left(x^n\right)^m + \left(y^n\right)^m - \left(z^n\right)^m + \left(kx^{n-1}y^{n-1}z^{n-1}\right)xyz \tag{48}$$

A new CE 'k-value' constant k_n is defined as follows:

$$k_n = kx^{n-1}y^{n-1}z^{n-1} \tag{49}$$

and since, by Corollary (38), k in (47) is positive for the $Z = X + Y$ solution, then so too is k_n given $1 < x < y < z$ (1b), i.e. $k > 0 \Rightarrow k_n > 0$

Re-writing (48) in terms of k_n and tidying gives

$$0 = x^{nm} + y^{nm} - z^{nm} + k_n xyz \tag{50}$$

Thus, in this form it is seen that x, y, z is now a CE solution (1), exponent mn, for positive constant k_n, hence proving the theorem.

The converse of this theorem is that if there exist CE solutions X, Y, Z for odd exponent m (47), whereby $X = x^n$, $Y = y^n$, $Z = z^n$ (45), then x, y, z is an FLT counter-example, for $n > 2$, or a Pythagorean triple for $n = 2$. For $n > 2$ Wiles [1] tells us there are no such solutions. Nevertheless, this gives another restatement of FLT, namely that there are no CE solutions of the form X, Y, Z (45) for all odd exponents $m \geq 3$.

(51) Corollary: Every FLT counter-example x, y, z, exponent n, is a CE solution, positive constant k_n (50), exponent $3n$.

Proof. Since Theorem (44) is true for all odd exponents $m \geq 3$, then it is true for the smallest, cubic exponent $m = 3$. In this case, the composite exponent $mn = 3n$, and the CE equation (50) becomes, in terms of constant k_n (determined next),

$$0 = x^{3n} + y^{3n} - z^{3n} + k_n xyz \tag{52}$$

By Corollary (41), $k = 3$ for $m = 3$, so that constant k_n (49) has the following positive, non-zero value:

$$k_n = 3x^{n-1}y^{n-1}z^{n-1} \tag{53}$$

Therefore proving x, y, z is a CE solution (52), for exponent $3n$ and positive constant k_n (49).

(54) Example. Since theorem (44) includes Pythagoras solutions for exponent $n = 2$, corollary (51) is easily demonstrated for exponent $m = 3$, as in the following numbers for the Pythagorean triple (4,3,5); see also Example (21) further above for the full unity root solution:

$$\begin{gathered} n = 2 \\ x = 4,\ y = 3,\ z = 5, \\ 0 = 4^2 + 3^2 - 5^2 \ (2) \\ X = 16,\ Y = 9,\ Z = 25 \ (45) \end{gathered} \tag{54}$$

$$\begin{gathered} m = 3 \\ 0 = 16^3 + 9^3 - 25^3 + 3.16.9.25,\ k = 3 \ (47) \end{gathered}$$

$$\begin{gathered} mn = 6 \\ k_n = k.4.3.5 = 180 \ (49) \\ 0 = 4^6 + 3^6 - 5^6 + 180.4.3.5 \ (50) \end{gathered}$$

and for $m = 5$, $m = 7$

$$mn = 10,\ 0 = 4^{10} + 3^{10} - 5^{10} + 144300.4.3.5,\ k = 144300$$

$$mn = 14,\ 0 = 4^{14} + 3^{14} - 5^{14} + 97171620.4.3.5,\ k = 97171620$$

Summary

A Diophantine equation, known as the Coordinate Equation, has been derived as the general solution to a set of congruences that any FLT counter-example or Pythagoras solution must satisfy. Unlike FLT, this Coordinate Equation has solutions, a special case being the $z = x + y$ solution valid for all odd exponents, and arbitrary *x* and *y*. Using this special solution, it is shown that any FLT counter-example or Pythagoras solution is also a solution to the Coordinate Equation to a higher order exponent *mn*, whereby *m* is an arbitrary odd integer, and $n = 2$ for Pythagoras or $n \geq 3$ (odd or even) for FLT.

To summarise this algebraically...

If x, y, z is an FLT counter-example or Pythagoras solution, exponent *n*, i.e.

$$0 = x^n + y^n - z^n,\ n \geq 2 \tag{2}$$

then defining X, Y, Z as follows:

$$X = x^n,\ Y = y^n,\ Z = z^n \tag{45}$$

such that the FLT equation (2) is now written as

$$Z = X + Y$$

then X, Y, Z is a solution to the CE (47) for all odd exponent *m*, $m = 2p + 1$, $p \in \mathbb{Z}$, $p \geq 1$, and some non-zero integer *k*

$$0 = X^m + Y^m - Z^m + kXYZ \tag{47}$$

In addition, by defining constant k_n in terms of *k* and x, y, z as follows:

$$k_n = kx^{n-1}y^{n-1}z^{n-1} \tag{49}$$

then x, y, z is a solution to the CE (1) for composite exponent $mn \geq 6$,

$$0 = x^{nm} + y^{nm} - z^{nm} + k_n xyz \tag{50}$$

Conclusion

Every FLT counter-example or Pythagoras solution x, y, z is a special '$Z = X + Y$' solution, where $X = x^n$, $Y = y^n$, $Z = z^n$, $n \geq 2$, to the CE equation $0 = X^m + Y^m - Z^m + kXYZ$, for some integer constant *k*, odd $m \geq 3$, and therefore also a solution to the CE, composite exponent $mn \geq 6$, such that $0 = x^{nm} + y^{nm} - z^{nm} + k_n xyz$, where $k_n = kx^{n-1}y^{n-1}z^{n-1}$.

References

[1] Wiles A., Modular elliptic curves and Fermat's Last Theorem. 1995 Annals of Mathematics 142 p443-551.

[2] An Introduction to the Theory of Numbers, I.Niven, S.Zuckerman, H.L.Montgomery , 5th Edition, John Wiley & Sons, Inc 1991. ISBN 0-471-54600-3.

[3] Miller R. J., Numeric Solutions to the Coordinate Equation. See PDF link http://www.urmt.org/urmt_numeric_solutions.pdf

[4] Miller R. J., Fermat's Last Theorem and Pythagoras as an Eigenvector Problem. See PDF link http://www.urmt.org/FLT_pythag_eigenvector.pdf

Addendum. Explanatory Notes

1. The list of conditions is almost identical to those of FLT, barring the proof is valid for quadratic exponents, whilst FLT is stated for cubic and higher order exponents. In addition, FLT is usually restricted to positive integers greater than zero, whereas the proof is restricted to positive integers greater than one. This is because the proof uses the integers x, y, z as moduli, and these are greater than one to avoid triviality as in the fact that every non-zero integer is congruent to zero modulo one, and thus unity roots (4) have no meaning for a unit modulus - such roots being essential in this paper. Furthermore, restricting to integers greater than one, rather than greater than zero, has absolutely no consequence for exponents $n \geq 2$ since there cannot possibly be any solutions with the smallest integer (x here by convention) being one. If $x = 1$, then it implies, that there are integers y and z, ($z > y > x = 1$) such that $z^n = 1 + y^n$. This is not the case for $y > 2$ or more since, rearranging FLT, this implies $z^n - y^n = 1$, i.e. the difference of two nth powers is unity. Indeed, the difference of two numbers raised to an nth power is always much greater than unity and to see this (rather obvious fact), one need only expand z^n binomially using $z = y + a$ for some integer $a > 0$, whereby $z^n - y^n > ay^{n-1} \geq ay$ for $n \geq 2$. Given $a > 0$ and $y > 2$ then this is clearly always greater than one.

2. Theorem (5) and its following Theorem (12) are intended to prove that every solution to FLT is a solution to the CE (1) and there are no possible solutions to FLT outside of the CE. To that end, the CE has to capture ALL solutions that satisfy the congruences (3), i.e. there must be no solutions to the congruences, that are not solutions to the CE, and therefore also FLT. It is the intention that this is achieved by the construction of the CE so that it is effectively reverse-engineered from the congruences as their most general solution. Indeed, the 'catch-all' nature of the k term in the CE switches FLT in and out of the CE by its zero and non-zero value respectively.