Fermat's Last Theorem and Pythagoras as an Eigenvector Problem

Richard J. Miller
richard@urmt.org
Issue 1.1 18/04/2021

Abstract

This paper gives a restatement of Fermat's Last Theorem and Pythagoras in terms of the eigenvector solution to a matrix comprising integer roots of unity. It shows that any FLT counter-example or Pythagoras solution only exists if it satisfies a certain eigenvector equation. The eigenvector equation then leads to three ratio conditions on the counter-example, each of which explicitly contain the reduced exponent $n-2$. From this, it is then seen that the quadratic exponent clearly decouples a dependency of the ratio conditions on any solution. The theory culminates in a restatement of Fermat's Last Theorem as an inner vector product that is zero as a consequence of the orthogonality of the eigenvectors. Although Fermat's Last Theorem was proven by Wiles 1995, this paper offers a clear distinction between Pythagoras and higher order exponents, whilst linking them in the same set of equations. It thus provides insight into how Pythagoras attains its solutions as eigenvectors, and an alternative path for a possible, relatively direct proof of Fermat's Last Theorem using eigenvector methods.

Outline

The paper starts by showing that any FLT counter-example or Pythagoras solution (generally just referred to as a '***solution'*** hereafter), must adhere to certain congruence conditions. This then leads to the conclusion that any solution is an eigenvector, unity eigenvalue, to a unity root matrix, so-named because its elements are integer roots of unity. However, the congruence conditions provide a necessary but insufficient condition such that there may be eigenvectors satisfying the same eigenvector equation that are not solutions. To remedy this, a second 'FLT matrix' is constructed directly from the solution, and this solution is also an eigenvector to this FLT matrix. The unity root matrix and the FLT matrix are then equated to derive three ratio conditions, exclusive to any solution, relating the unity roots to the coordinates raised to a reduced exponent $n-2$. It is subsequently shown these three ratios can be varied by a single integer parameter such that the solution remains invariant to this parameter.

A second eigenvector is introduced that is then related to the eigenvector representing the FLT solution/Pythagoras. The two eigenvectors have unique eigenvalues and are consequently shown to be orthogonal giving a zero inner vector product, this inner product being none other than the original Diophantine equation of FLT. The possible consequences of a non-zero inner product (one of the vectors is no longer a true eigenvector) is briefly considered via the introduction of a second Diophantine equation, termed 'the Coordinate Equation'. This equation is defined such that is satisfies the same congruence relations as that of FLT but, otherwise, is less stringent and has actual solutions enabling a numeric study of the inner product and, indeed, many aspects of the results in the paper.

Lastly, since Pythagoras has an infinite set of solutions, all key results for the quadratic exponent can be verified and, most importantly, these clearly show the simplistic nature of Pythagoras as an eigenvector solution.

Theory

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

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

FLT was first proven by Wiles [1].

The full list of conditions[1] used herein is

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

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 $n \geq 2$.

Firstly, it is assumed one or more FLT solutions, i.e. counter-examples, exist. Given the Pythagorean exponent $n = 2$ is included, this also gives a check on all developments in the paper.

(2) Lemma. Every solution satisfies the following congruences:

$$\begin{aligned} y^n &\equiv z^n \pmod{x} \\ x^n &\equiv z^n \pmod{y} \\ x^n &\equiv -y^n \pmod{z} \end{aligned} \tag{2}$$

Proof. By taking residues of (1) to moduli x, y, z then the three congruences (2) 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[2] and this insufficiency is later removed by theorem (14) and related. See also just prior to and including definition (40).

(3) 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:

$$u^n \equiv \pm 1 \pmod{p} \tag{3}$$

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)

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

$$x = Ry + \overline{Q}z \tag{4a}$$

$$y = \overline{R}x + Pz \tag{4b}$$

$$z = Qx + \overline{P}y \tag{4c}$$

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, albeit (23) gives a notable relation between them. $\overline{P}, \overline{Q}, \overline{R}$ are referred to as the 'conjugates' of P, Q, R and, as will be seen in the Pythagorean case, are identical to P, Q, R barring the sign of $\overline{R}$, see (50) further below.

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 $S(R,\overline{Q},y,z)$:

$$x^n = R^n y^n + \overline{Q}^n z^n + yzS(R,\overline{Q},y,z) \tag{5a}$$

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

$$y^n = \overline{R}^n x^n + P^n z^n + xzT(P,\overline{R},x,z) \tag{5b}$$

$$z^n = Q^n x^n + \overline{P}^n y^n + xyU(\overline{P},Q,x,y) \tag{5c}$$

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

$$\begin{aligned} x^n &\equiv R^n y^n \pmod{z},\ x^n \equiv \overline{Q}^n z^n \pmod{y} \\ y^n &\equiv \overline{R}^n x^n \pmod{z},\ y^n \equiv P^n z^n \pmod{x} \\ z^n &\equiv Q^n x^n \pmod{y},\ z^n \equiv \overline{P}^n y^n \pmod{x} \end{aligned} \tag{6}$$

and the less useful remaining three are

$$\begin{aligned} 0 &\equiv R^n y^n + \overline{Q} z^n + yzS(R,\overline{Q},y,z) \pmod{x} \\ 0 &\equiv \overline{R}^n x^n + P^n z^n + xzT(P,\overline{R},x,z) \pmod{y} \\ 0 &\equiv Q^n x^n + \overline{P}^n y^n + xyU(\overline{P},Q,x,y) \pmod{z} \end{aligned} \tag{7}$$

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 (6) are made consistent with the original congruences (2) by defining the variables P,Q,R and $\overline{P},\overline{Q},\overline{R}$ as unity roots (3), as follows:

$$\begin{aligned} P^n &\equiv 1 \pmod{x},\ Q^n \equiv 1 \pmod{y},\ R^n \equiv -1 \pmod{z} \\ \overline{P}^n &\equiv 1 \pmod{x},\ \overline{Q}^n \equiv 1 \pmod{y},\ \overline{R}^n \equiv -1 \pmod{z} \end{aligned} \tag{8}$$

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

$$P,Q,R \in \mathbb{Z},\ (P,Q,R) \neq (0,0,0),\ \overline{P},\overline{Q},\overline{R} \in \mathbb{Z},\ (\overline{P},\overline{Q},\overline{R}) \neq (0,0,0) \tag{9}$$

Thus, all solutions x, y, z to FLT can be written as three linear equations (4) in terms of the unity roots P,Q,R and $\overline{P},\overline{Q},\overline{R}$.

(10) Definition A ***unity root matrix***, *symbol* $\mathbf{A}$, is defined in terms of the unity roots P,Q,R and their 'conjugates' $\overline{P},\overline{Q},\overline{R}$ as follows:

$$\mathbf{A} = \begin{pmatrix} 0 & R & \overline{Q} \\ \overline{R} & 0 & P \\ Q & \overline{P} & 0 \end{pmatrix} \tag{10}$$

(11) Definition. A column vector **X** is defined as follows in terms of a solution x, y, z:

$$\mathbf{X} = \begin{pmatrix} x \\ y \\ z \end{pmatrix} \tag{11}$$

(12) Theorem. A solution x, y, z to FLT/Pythagoras is an eigenvector **X** (11) to a unity root matrix **A** (10), for unity eigenvalue.

$$\mathbf{AX} = \mathbf{X} \tag{12}$$

Proof: using the definitions of **A** (10) and **X** (11), then the three linear equations (4) can be re-written as the eigenvector equation (12) for unity eigenvalue. Thus, by theorem (4), an FLT solution x, y, z is an eigenvector to a unity root matrix **A** (10), unity eigenvalue.

Although not explicitly required herein, the analytic solution for an eigenvector to **A** (10) for general eigenvalue λ, given in terms of the unity roots, is given in explanatory note [3]**.**

Great care must be taken interpreting this theorem because the eigenvector solutions **X** are actually a superset of solutions (FLT counter-examples or Pythagoras). As noted[2], the original congruences (2) are not sufficient by themselves and, as a consequence, there may (indeed, are) many **X** satisfying the eigenvector equation [3], a subset of which are FLT counter-examples. With this in mind, the following definition and related theorem restrict the remainder of the paper to FLT counter-examples and Pythagoras solutions only.

(13) Definition. An ***FLT matrix***, symbol $\mathbf{F}$, is defined as follows for some integers s,t,u:

$$\mathbf{F} = \begin{pmatrix} 0 & -uy^{n-2} & sz^{n-2} \\ ux^{n-2} & 0 & tz^{n-2} \\ sx^{n-2} & ty^{n-2} & 0 \end{pmatrix} \tag{13}$$

It is of note that this revised matrix is derived completely independent of matrix **A** (10), but will soon be equated to it, see (20) further below.

(14) Theorem. **X** (11) is an eigenvector to an FLT matrix **F** (13) for unity eigenvalue, i.e. $\mathbf{FX} = \mathbf{X}$, if and only if **X** is a solution.

Proof. If a triple x, y, z is a solution then it can be written in the following form, for some s,t,u, possibly rational at this stage:

$$\begin{aligned} x^n &= -ux^{n-1}y^{n-1} + sx^{n-1}z^{n-1} \\ y^n &= uy^{n-1}x^{n-1} + ty^{n-1}z^{n-1} \\ z^n &= sx^{n-1}z^{n-1} + ty^{n-1}z^{n-1} \end{aligned} \tag{15}$$

By forming the sum $x^n + y^n - z^n$, it can be verified that this equates to zero as per a solution (1). That rational s,t,u can always be found comes after the next step. However, s,t,u are not actually required further in the paper and that they can, in principle, be determined is sufficient to justify (15).

Dividing the first in (15) by x^{n-1}, the second by y^{n-1}, and the third by z^{n-1}, none of which are zero (1b), then the following equations are obtained

$$\begin{aligned} x &= -uy^{n-1} + sz^{n-1} \\ y &= ux^{n-1} + tz^{n-1} \end{aligned} \tag{16}$$

$$z = sx^{n-1} + ty^{n-1}$$

The justification that rational s,t,u can always be found comes from the fact that equations (16) can be solved backward for s,t,u and, using *t* as a single free-parameter, gives $u = \left(y - tz^{n-1}\right)/\,x^{n-1}$, $s = \left(z - ty^{n-1}\right)/\,x^{n-1}$. Hence, given x^{n-1} is never zero, as above, a rational solution for *u* and *s*, with *t* as a free parameter, can always be found. As noted above, s,t,u are not required further in this paper.

The equations (16) can be re-written in eigenvector form as

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 & -uy^{n-2} & sz^{n-2} \\ ux^{n-2} & 0 & tz^{n-2} \\ sx^{n-2} & ty^{n-2} & 0 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} \qquad (17)$$

hence, by the definition of **X** (11) and **F** (13)

$$\mathbf{FX} = \mathbf{X} \qquad (18)$$

and thus a solution **X** can be written as an eigenvector, unity eigenvalue, to matrix **F**. Conversely, starting with **X** as an eigenvector, unity eigenvalue to matrix **F**, and working backward, we obtain equations (15), which are true only if **X** is a solution. Hence proving **X** is an eigenvector to an FLT matrix **F** for unity eigenvalue if and only if **X** is an FLT solution.

(19) Theorem. If **X** (11) is a solution then **F** (13) is a unity root matrix **A** (10).

Proof. By theorem (14), if **X** is a solution then it is an eigenvector to a matrix of the form **F** (13), but by theorem (12), all solutions are eigenvectors, for unity eigenvalue, to a unity root matrix **A** (10). Thus, by implication, **F** (13) must be a unity root matrix (10).

(20) Corollary. As a corollary to theorem (19), there exist a particular set of unity roots P,Q,R and $\overline{P},\overline{Q},\overline{R}$ such that the unity root matrix **A** (10) and **F** (13) are equivalent, i.e.

$$\mathbf{A} = \mathbf{F} \Rightarrow \begin{pmatrix} 0 & R & \overline{Q} \\ \overline{R} & 0 & P \\ Q & \overline{P} & 0 \end{pmatrix} = \begin{pmatrix} 0 & -uy^{n-2} & sz^{n-2} \\ ux^{n-2} & 0 & tz^{n-2} \\ sx^{n-2} & ty^{n-2} & 0 \end{pmatrix} \qquad (20)$$

Equating the two thus gives the unity roots as:

$$\begin{aligned} P &= tz^{n-2},\ \overline{P} = ty^{n-2} \\ Q &= sx^{n-2},\ \overline{Q} = sz^{n-2} \\ R &= -uy^{n-2},\ \overline{R} = ux^{n-2} \end{aligned} \qquad (21)$$

Note that the set of unity roots satisfying the equality in (20) is now termed a 'particular' solution because, to reiterate earlier comments, the unity roots are defined through congruences (2) that allow a wide range of eigenvector solutions **X** (11), only a subset of which are FLT counter-examples. Since **A** (10) is formed from these unity roots, it too may have many forms, only a subset of which is valid for an FLT counter-example - this subset being termed the 'particular solution'. In fact, it will be seen shortly that the particular solution is actually only unique to within a single free-parameter, integer *m* (24) further below, and so the particular solution is actually an infinite set parameterised by *m*.

(22) Theorem. Every solution satisfies the following ***ratio conditions*** relating the unity roots $\{P,Q,R,\overline{P},\overline{Q},\overline{R}\}$ to the solution x,y,z

$$\frac{P}{\overline{P}}=\frac{z^{n-2}}{y^{n-2}},\ \frac{\overline{Q}}{Q}=\frac{z^{n-2}}{x^{n-2}},\ \frac{R}{\overline{R}}=-\frac{y^{n-2}}{x^{n-2}} \tag{22}$$

Proof. The ratio conditions (22) are obtained directly by eliminating s,t,u in (21). In doing so, the unity roots are seen to relate directly to the solution in x,y,z with absolutely no dependence on s,t,u. Since equations (21) are true for every solution, as a culmination of theorem's (14), (19) and corollary (22), then every solution must satisfy these relations. Since there has been no explicit restriction of the exponent to $n>2$ in any of the proofs, the conditions are also valid for $n=2$, i.e. Pythagoras.

It is noted that there are no divide-by-zero issues in these relations given neither the coordinates nor unity roots are zero by conditions (1b) and (9).

(23) Lemma. The unity root matrix **F** (13) has a zero determinant and, as such for a particular solution, the unity roots satisfy the condition

$$\det(\mathbf{F})=\det(\mathbf{A})=PQR+\overline{P}\overline{Q}\overline{R}=0 \tag{23}$$

Proof. From the form of **F** (13), it is easily determined that the determinant is zero: working along any of the rows or columns gives just two terms $\pm stux^{n-2}y^{n-2}z^{n-2}$ that cancel upon summation leaving a zero determinant. On the other hand, the determinant of **A** (10) is also $PQR+\overline{P}\overline{Q}\overline{R}$ and thus, given the unity root equalities (21), it is seen that this determinant is therefore also zero, hence proving (23). Note too that by multiplying out the ratios $P/\overline{P}$, $Q/\overline{Q}$ and $R/\overline{R}$ in (22), the coordinate terms x,y,z cancel, also confirming (23).

(24) Definition. A ***global variation*** is defined as the following transformation of the unity roots (8) in terms of a single, arbitrary integer *m*:

$$\begin{gathered} P\rightarrow P+m\overline{Q}\overline{R}x,\ \overline{P}\rightarrow\overline{P}-mQRx,\ m\in\mathbb{Z} \\ Q\rightarrow Q+mQRy,\ \overline{Q}\rightarrow\overline{Q}+m\overline{Q}Ry \\ R\rightarrow R-m\overline{Q}Rz,\ \overline{R}\rightarrow\overline{R}-m\overline{Q}\overline{R}z \end{gathered} \tag{24}$$

(25) Theorem. Every solution is invariant to a global variation (24) in the unity roots.

Proof. Under global variation (24), the ratio conditions (22) become

$$\frac{P+m\overline{Q}\overline{R}x}{\overline{P}-mQRx}=\frac{z^{n-2}}{y^{n-2}},\ \frac{\overline{Q}+m\overline{Q}Ry}{Q+mQRy}=\frac{z^{n-2}}{x^{n-2}},\ \frac{R-m\overline{Q}Rz}{\overline{R}-m\overline{Q}\overline{R}z}=-\frac{y^{n-2}}{x^{n-2}},\ n>2 \tag{25}$$

Starting with the second, $\overline{Q}/Q$ ratio first, there is a common factor $1+mRy$ that cancels top and bottom leaving the original ratio (22). Similarly, the third ratio $R/\overline{R}$ has a common factor $1-m\overline{Q}z$ that also cancels top and bottom to give the original ratio. The first ratio $P/\overline{P}$ requires a little more work: using $PQR+\overline{P}\overline{Q}\overline{R}=0$ (23) to obtain $\overline{Q}\overline{R}=PQR/\overline{P}$, and then substituting for $\overline{Q}\overline{R}$ into the expression for $P/\overline{P}$, gives a common factor $1-mQRx/\overline{P}$ that also cancels top and bottom leaving the original ratios.

Thus, in all three ratios $P/\overline{P}$, $\overline{Q}/Q$ and $R/\overline{R}$, applying the global variation returns the original ratio conditions (22), and so proving, by theorem (22), every FLT solution is invariant to a global variation (24) in the unity roots.

All the work so far has concentrated on the solution in x, y, z and its related eigenvector $\mathbf{X}$ (11). However, there is a second, equally important 'conjugate' eigenvector comprising the solution raised to the power $n-1$.

(26) Definition. A ***conjugate eigenvector*** $\overline{\mathbf{X}}$ is defined as the following row-vector

$$\overline{\mathbf{X}} = \begin{pmatrix} x^{n-1} & y^{n-1} & -z^{n-1} \end{pmatrix} \tag{26}$$

(27) Lemma. The conjugate eigenvector $\overline{\mathbf{X}}$ (26) is a row eigenvector to the FLT matrix $\mathbf{F}$ (13) for eigenvalue -1, i.e.

$$\overline{\mathbf{X}}\mathbf{F} = -\overline{\mathbf{X}} \tag{27}$$

Proof. The proof is a straightforward evaluation of the eigenvector equation using the definitions of $\overline{\mathbf{X}}$ (26) and $\mathbf{F}$ (13), and then comparing with the definitions (15). For example, the first element evaluates as $\overline{\mathbf{X}}\mathbf{F}(1) = uy^{n-1}x^{n-2} - sz^{n-1}x^{n-2}$, and comparing with $x^n = -ux^{n-1}y^{n-1} + sx^{n-1}z^{n-1}$ (15) shows that $\overline{\mathbf{X}}\mathbf{F}(1) = -x^{n-1}$. Similarly evaluating the other two elements gives $\overline{\mathbf{X}}\mathbf{F}(2) = -y^{n-1}$ and $\overline{\mathbf{X}}\mathbf{F}(3) = z^{n-1}$ hence $\overline{\mathbf{X}}\mathbf{F} = \begin{pmatrix} -x^{n-1} & -y^{n-1} & z^{n-1} \end{pmatrix}$ and so $\overline{\mathbf{X}}F = -\overline{\mathbf{X}}$ by definition (26) thus proving (27).

Note that by theorem (19) and its corollary (20), whereby matrix $\mathbf{A}$ (10) is equated to $\mathbf{F}$ if $\mathbf{X}$ is a solution, then (27) can also be written in terms of $\mathbf{A}$, i.e.

$$\mathbf{A} = \mathbf{F} \Rightarrow \overline{\mathbf{X}}\mathbf{A} = -\overline{\mathbf{X}} \tag{28}$$

The conjugate eigenvector $\overline{\mathbf{X}}$ relates to the eigenvector $\mathbf{X}$ via a linear, matrix transformation.

(29) Definition. The ***T operator*** is defined as the following, diagonal-only matrix given in terms of the unity roots:

$$\mathbf{T} = x^{n-2}\begin{pmatrix} 1 & 0 & 0 \\ 0 & -R/\overline{R} & 0 \\ 0 & 0 & -\overline{Q}/Q \end{pmatrix} \tag{29}$$

(30) Lemma. The conjugate eigenvector $\overline{\mathbf{X}}$ (26) is related to the FLT eigenvector solution $\mathbf{X}$ (11) via the following $\mathbf{T}$ operator transformation:

$$\overline{\mathbf{X}} = (\mathbf{TX})^T \tag{30}$$

Proof. Substituting for the diagonal elements in terms of the solution, using the ratio conditions (22), gives

$$\mathbf{T} = \begin{pmatrix} x^{n-2} & 0 & 0 \\ 0 & y^{n-2} & 0 \\ 0 & 0 & -z^{n-2} \end{pmatrix} \tag{31}$$

Multiplying $\mathbf{X}$ (11) by this form of $\mathbf{T}$, and transposing, gives $\overline{\mathbf{X}}$ (26), hence proving (30).

Note that this form (31) is strictly for solutions only, given $\mathbf{X}$ is assumed to be a solution and the ratio conditions in (22) are for solutions only. On the other hand, (29) is valid for a wider range of eigenvectors $\mathbf{X}$ to $\mathbf{A}$, but this fact is of note only and not required further.

(32) Lemma. The **T** operator is invariant to a global variation (24) in the unity roots.

Proof. By theorem (25) every solution x, y, z is invariant to a global variation (24) in the unity roots and thus, from the form of the **T** operator (31), the **T** operator itself is invariant to a global variation in the unity roots.

(33) Lemma. The conjugate eigenvector $\overline{\mathbf{X}}$ (26) is invariant to a global variation (24) in the unity roots.

Proof. By theorem (25) and lemma (32), both the eigenvector solution **X** (11) and **T** operator, respectively, are invariant to a global variation in the unity roots; hence the conjugate eigenvector $\overline{\mathbf{X}}$ is also invariant to a global variation in the unity roots.

(34) Theorem. If x, y, z is a solution then the inner product of the conjugate vector $\overline{\mathbf{X}}$ (26) with **X** (11) is zero, i.e.

$$\overline{\mathbf{X}}\mathbf{X} = 0 \tag{34}$$

Proof. This is simply proven by the inner product definition, which here is the multiplication of the column vector **X** by the conjugate row vector $\overline{\mathbf{X}}$, and given x, y, z is a solution (1), then

$$\overline{\mathbf{X}}\mathbf{X} = x^n + y^n - z^n = 0 \tag{35}$$

Whilst this is seemingly trivial, it is an important restatement of FLT in terms of the inner product of the eigenvector **X**, which is a vector representation of the solution x, y, z, with its conjugate form $\overline{\mathbf{X}}$, related to **X** by (30). Effectively it is the culmination of all the results in the paper, recasting Fermat's Last Theorem in a linear algebraic form involving the eigenvectors to a unity root matrix.

(36) Corollary. As a corollary to theorem (34), the inner product $\overline{\mathbf{X}}\mathbf{X}$ is invariant to a global variation (24) in the unity roots.

Proof. This is simply a consequence of theorem (25) and lemma (33), which state that **X** and $\overline{\mathbf{X}}$ respectively, are invariant to a global variation in the unity roots.

The inner product (34) is actually also a consequence of a standard result in linear algebra [4], namely 'orthogonality of eigenvectors to different eigenvalues'[4]. In this case, the row eigenvector $\overline{\mathbf{X}}$ for eigenvalue -1, and the column eigenvector **X**, for eigenvalue +1.

Most importantly, any new proof of FLT could focus on showing such an integer vector $\overline{\mathbf{X}}$ (26), that is a row eigenvector to a unity root matrix for eigenvalue -1, cannot exist. If it did exist, by orthogonality alone, it would have to be an FLT counter-example.

An FLT-like Diophantine Equation

Although the inner product (34) is zero for any FLT solutions (were they to exist), and Pythagoras, it does have a useful, non-zero value when considering a modified form of FLT, known as the Coordinate Equation (CE), defined next. The CE equation is the general solution to the congruence relations (2) and a formal derivation of this equation, with related theorems, is given in [5]; suffice to say, the CE has solutions for all exponents.

(40) Definition. The ***Coordinate Equation*** is defined in terms of x, y, z (1b) as per eigenvector **X** (11), for integer *k*, as follows:

$$0 = x^n + y^n - z^n + kxyz,\ k \in \mathbb{Z} \tag{40}$$

It can be seen that this equation satisfies the congruence relations (2).

(41) Theorem. There are no solutions to the Coordinate Equation for $k = 0$.

Proof. For $k = 0$ the CE reduces to FLT (1) and hence, by Wiles [1], there are no solutions for $k = 0$.

Nevertheless, for every exponent $n \geq 2$, there are solutions to the CE for which *k* is non-zero, some of which are given in [3]. Not least, for odd exponents, there is always a solution when $z = x + y$, albeit in this case *k* becomes very large very soon, as indeed it does for virtually all other solutions.

Note that a non-zero value for *k* means that **X** is not an FLT counter-example or Pythagoras solution, but it does still have its defining form (11), and it is still an eigenvector to a unity root matrix (12). Whilst $\overline{\mathbf{X}}$ remains strictly defined as in (26), for non-zero *k* it no longer relates to **X** via (30) since the form of the **T** operator (31) is only valid for FLT counter-examples or Pythagoras solutions. Most importantly, for non-zero *k*, $\overline{\mathbf{X}}$ is no longer an eigenvector to the unity root matrix, it is not orthogonal to **X** and, accordingly, the inner product $\overline{\mathbf{X}}\mathbf{X}$ (34) is non-zero. These points have not been proven here and are considered outside the scope of the paper. The important point is that, using the eigenvector inner product $\overline{\mathbf{X}}\mathbf{X}$, the CE (40) can be written as

$$0 = \overline{\mathbf{X}}\mathbf{X} + kxyz \tag{42}$$

and rearranging gives *k* as

$$k = -\frac{\overline{\mathbf{X}}\mathbf{X}}{xyz} \tag{43}$$

Thus, the non-zero inner product $\overline{\mathbf{X}}\mathbf{X}$, suitably scaled by the product $1/xyz$ is, in effect, a measure of the deviation of CE solutions from FLT. A possible FLT proof could therefore show *k* is never zero, albeit its actual non-zero value being of no consequence.

Pythagoras

The above is general, for all exponents $n \geq 2$ and, whilst Wiles [1] proves there are actually no FLT solutions (counter-examples), the relations can easily be verified for Pythagoras by setting the exponent to $n = 2$.

(50) Definition. The ***Pythagoras Conditions*** are given by the ratio conditions (22) for a quadratic exponent $n = 2$, i.e.

$$\overline{P} = P\,,\ \overline{Q} = Q\,,\ \overline{R} = -R\,,\ n = 2 \tag{50}$$

and makes the unity roots $\overline{P}, \overline{Q}, \overline{R}$ identical to P, Q, R barring the sign of $\overline{R}$.

It is notable that there is now no functional dependence of the unity root ratios on the solution x, y, z in this Pythagorean case since the $n-2$ exponent in (22) goes to zero.

Applying the conditions (50) to (21), the integers s, t, u in **A** (13) become identical to the above Pythagorean unity root forms, i.e.

$$t = P\,,\ s = Q\,,\ u = -R\,,\ n = 2 \tag{51}$$

and the two forms of unity root matrix, **A** and **F** in (20), become

$$\mathbf{A} = \mathbf{F} = \begin{pmatrix} 0 & R & Q \\ -R & 0 & P \\ Q & P & 0 \end{pmatrix}, \ n = 2 \tag{52}$$

Applying the Pythagoras Conditions to the global variational terms (24) gives

$$P \to P - mQRx\,,\ Q \to Q + mQRy\,,\ R \to R - mQRz\,,\ n = 2 \tag{53}$$

Given that the factor of QR is now common to all three (53), it can be absorbed into the integer m such that the above transformations become

$$\begin{gathered} m \to mQR\,,\ n = 2 \\ P \to P - mx\,,\ Q \to Q + my\,,\ R \to R - mz \end{gathered} \tag{54}$$

It is seen that, under Pythagoras Conditions, the variational terms $-mx$, my and $-mz$ contain no unity root dependence, unlike (24), and are purely a function of the Pythagorean solution x, y, z.

Under Pythagoras, the conjugate eigenvector $\overline{\mathbf{X}}$ (26) is now almost identical to $\mathbf{X}$ (11), i.e.

$$\overline{\mathbf{X}} = \begin{pmatrix} x & y & -z \end{pmatrix},\ n = 2 \tag{55}$$

and with this, the Pythagoras equation in inner product form is thus

$$\overline{\mathbf{X}}\mathbf{X} = x^2 + y^2 - z^2 = 0,\ n = 2 \tag{56}$$

Of note here, and unlike the FLT solution, $\overline{\mathbf{X}}$ is also a solution, i.e. a Pythagorean triple, and identical to $\mathbf{X}$ (x, y, z) barring the sign of z. That $\overline{\mathbf{X}}$, for FLT $n > 2$, is never a solution is given by Wiles [1], just like $\mathbf{X}$ is never actually a solution.

With $\overline{\mathbf{X}}$ given by (55), it is not surprising that the $\mathbf{T}$ operator (31), as used in (30) to derive $\overline{\mathbf{X}}$ from $\mathbf{X}$, reduces to a constant for all Pythagoras solutions, i.e.

$$\mathbf{T} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix},\ n = 2 \tag{57}$$

To summarise the Pythagorean case, the ratios of the unity roots P, Q, R to their conjugates $\overline{P}, \overline{Q}, \overline{R}$ have no functional dependence on the solution x, y, z (50), whilst the global variational terms have no functional dependence on the unity roots (54). In effect, the Pythagorean case decouples the unity root ratios from the solution.

Summary

Every FLT counter-example and Pythagoras solution can be represented as an eigenvector to a matrix comprising the integer roots of unity. The unity root matrix is arbitrary to within a single integer parameter. Equating the unity root elements of the matrix to the eigenvector solution gives a set of three ratio conditions, whereby the ratio of the unity roots relates to the counter-example/solution raised to the reduced degree $n-2$, thus enabling a clear distinction between Pythagoras and FLT to be made.

The ratio conditions are shown to be invariant to variation by a single 'global' parameter, thus making all pertinent equations in the eigenvectors also invariant to this single parametric variation.

A second 'conjugate' eigenvector is introduced that relates, via a matrix operator, to the eigenvector representing the FLT solution/Pythagoras. Given the two eigenvectors have unique eigenvalues then they are orthogonal with a zero inner vector product, and this orthogonality of eigenvectors becomes an equivalent statement of FLT.

On the other hand, non-orthogonality (when the second vector is no longer a true eigenvector to the unity root matrix) implies a non-zero inner product, which is shown to be a measure of the deviation of legitimate solutions to a second, FLT-like Diophantine equation (the 'Coordinate Equation') from FLT.

Lastly, since Pythagoras has an infinite set of solutions, all key results developed throughout the paper can be verified for the quadratic exponent and, most importantly, show clearly the simplistic nature of Pythagoras as an eigenvector solution. In particular, Pythagoras shows a decoupling of the unity root ratios from the solution, unlike FLT, which has an inherent, linear ($n=3$) and non-linear ($n>3$) dependency relationship.

Conclusion

Fermat's Last Theorem can be formulated as an eigenvector problem in a matrix comprising integer roots of unity. In particular, its mathematical statement is equivalent to the orthogonality of two of the eigenvectors of the unity root matrix to distinct eigenvalues ± 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] Sadri Hassani, Foundations of Mathematical Physics, Prentice-Hall International Editions, 1991, ISBN 0-13-327503-5.

[5] Miller R. J., The Coordinate Equation & Fermat's Last Theorem. See PDF link

http://www.urmt.org/Coordinate_Eqn_FLT.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 (3) 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. It is stressed that Lemma (2) is necessity, not sufficiency, and this is intentional because it allows for solutions to the congruences (2) to be studied within the context of an FLT-like Diophantine Equation derived from (2), known as The 'Coordinate Equation' (40), with numeric solutions given in [3].

3. There are three forms of analytic solution for each eigenvector to **A** (10), eigenvalue λ, given in terms of the unity roots (8) as follows, where $\lambda = 1$ for **X** (11) and $\lambda = -1$ for $\overline{\mathbf{X}}$ (26) - see further below:

$$\text{form 1: } \mathbf{X}_\lambda = \begin{pmatrix} \lambda^2 - P\overline{P} \\ \lambda\overline{R} + PQ \\ \lambda Q + \overline{R}\,\overline{P} \end{pmatrix}, \text{ form 2: } \mathbf{X}_\lambda = \begin{pmatrix} \lambda R + \overline{P}\,\overline{Q} \\ \lambda^2 - Q\overline{Q} \\ \lambda\overline{P} + QR \end{pmatrix}, \text{ form 3: } \mathbf{X}_\lambda = \begin{pmatrix} \lambda\overline{Q} + RP \\ \lambda P + \overline{Q}\,\overline{R} \\ \lambda^2 - R\overline{R} \end{pmatrix}$$

These are unscaled forms and usually contain large common factors. To make them primitive, the GCD in each has to be removed. Since an eigenvector is only unique to within a scale factor, once the GCD is removed (different for each form), they then become one and the same primitive eigenvector.

The matrix **A** (10) has a 'conjugate' symmetry, which means swapping unity roots P, Q, R with conjugates $\overline{P}, \overline{Q}, \overline{R}$ is equivalent to transposing the matrix. Using this fact, the row eigenvectors, e.g. $\overline{\mathbf{X}}$ (26) $\lambda = -1$, can be obtained by swapping the unity roots likewise in the above analytic forms and transposing, e.g. form 1 $\overline{\mathbf{X}}_{\lambda=-1} = \begin{pmatrix} \lambda^2 - P\overline{P} & \lambda R + \overline{P}\,\overline{Q} & \lambda\overline{Q} + RP \end{pmatrix}$. Again, these need GCD removal to make them primitive.

Given the trace of **A** (10) is zero, and that the sum of the eigenvalues is equal to the trace [4], then there is also an eigenvalue $\lambda = 0$. Substituting $\lambda = 0$ in the above analytic solutions gives particularly simple forms since all terms in λ obviously disappear.

4. In this case, because **A** (10) is not symmetric, the orthogonality applies between a row and column eigenvector, i.e. row vector $\overline{\mathbf{X}}$ (26), and column vector **X** (11). Using $\mathbf{AX} = \mathbf{X}$ (12), and multiplying by on the left by row vector $\overline{\mathbf{X}}$ to form the inner $\overline{\mathbf{X}}\mathbf{X}$ product, gives $\overline{\mathbf{X}}\mathbf{AX} = \overline{\mathbf{X}}\mathbf{X}$. Similarly, using $\overline{\mathbf{X}}\mathbf{A} = -\overline{\mathbf{X}}$ (28), and multiplying on the right by **X** to form the same inner product, gives $\overline{\mathbf{X}}\mathbf{AX} = -\overline{\mathbf{X}}\mathbf{X}$. Equating the two results for $\overline{\mathbf{X}}\mathbf{AX}$ implies $\overline{\mathbf{X}}\mathbf{X} = -\overline{\mathbf{X}}\mathbf{X}$ which can only be true if the inner product $\overline{\mathbf{X}}\mathbf{X} = 0$ (34) since the eigenvectors are never trivially all zero.