Notes on Number Theory and Discrete Mathematics
Print ISSN 1310–5132, Online ISSN 2367–8275
Vol. 27, 2021, No. 4, 154–163
DOI: 10.7546/nntdm.2021.27.4.154-163

A plane trigonometric proof for the case $n = 4$ of Fermat's Last Theorem

Giri Prabhakar

Siemens Technology
Electronics City, Bangalore 560100, India
e-mail: giri.prab@siemens.com

Received: 22 March 2020 **Revised:** 22 August 2021 **Accepted:** 7 October 2021

Abstract: We present a plane trigonometric proof for the case $n = 4$ of Fermat's Last Theorem. We first show that every triplet of positive real numbers (a, b, c) satisfying $a^4 + b^4 = c^4$ forms the sides of an acute triangle. The subsequent proof is founded upon the observation that the Pythagorean description of every such triangle expressed through the law of cosines must exactly equal the description of the triangle from the Fermat equation. On the basis of a geometric construction motivated by this observation, we derive a class of polynomials, the roots of which are the sides of these triangles. We show that the polynomials for a given triangle cannot all have rational roots. To the best of our knowledge, the approach offers new geometric and algebraic insight into the irrationality of the roots.
Keywords: Pythagorean theorem, Diophantine equations, Fermat's Last Theorem.
2020 Mathematics Subject Classification: 51N20, 11D41.

1 Introduction

Let $\phi \geq 1$ be a real number. Let (a, b, c) be a triplet of positive real numbers such that

$$a^{\phi} + b^{\phi} = c^{\phi}. \tag{1}$$

We will call ϕ the *Fermat index* of (a, b, c). We allow ϕ to take values as large as required to satisfy (1). For some choices of the triplet (a, b, c), ϕ might not satisfy (1) at any finite value, however large. In these cases, $a^{\phi} + b^{\phi} - c^{\phi}$ might approach the limiting value of 0 only as ϕ grows unboundedly large. For completeness of our definition of the Fermat index, we acommodate for this possibility and define ϕ to take values from the affinely extended positive real number line greater than or equal to 1 , $\phi \in \bar{\mathbb{R}}_{\geq 1} = \{\mathbb{R}_{\geq 1}\} \cup \{+\infty\}$, following the definition in [3].

It is common knowledge that Fermat's Last Theorem [6], completely proved in 1995 by Andrew Wiles [11], states that if a, b and c are all positive integers, then they cannot satisfy (1) for an integer value of the Fermat index $\phi > 2$. Let the positive integer values of ϕ be represented by n, so that $\phi = n \in \mathbb{Z}_{\geq 1}$. Then (1) for integer Fermat index is

$$a^n + b^n = c^n. \tag{2}$$

In this paper, we specifically analyze (2) for $n = 4$

$$a^4 + b^4 = c^4. \tag{3}$$

While Fermat spoke of a marvelous proof that the margins of his notebook were too narrow to contain, his only known work on this topic is one in which he used his method of infinite descent to prove the case $\phi = 4$ [6]. Since then many mathematicians, amongst them Euler, Legendre, Lebesgue, and Kronecker, have proved this particular case in the past [10]. More recently, Grant and Perella [8], Dolan [5], Barbara [1] and others have addressed this problem.

Traditionally, the strategies for proof that have been adopted have been based either on Fermat's observation that the area of a right triangle with integer sides can never be a perfect square, or on other equivalent forms of Diophantine analysis that are founded upon an algebraic approach. To the best of our knowledge, our approach represents a departure from these methods, in that we adopt a strategy for proof that is based on an understanding of the plane trigonometric implications of (3). We believe that the consequent insights are new and could potentially complement the existing body of work on the subject.

We will first show that (3) represents acute triangles.

Lemma 1.1. *The triplet (a, b, c) satisfying (3) forms an acute triangle with c the longest side.*

Proof. Consider $(a + b)^4 = a^4 + b^4 + 4(a^3b + ab^3) + 6a^2b^2 > a^4 + b^4 = c^4$, hence $a + b > c$. We also see that $c > a$ and $c > b$. Therefore, the triangle inequalities $a + b > c, b + c > a$ and $c + a > b$ are satisfied, and (a, b, c) can be considered as side lengths of a triangle, of which c is the largest side. Assume γ as the largest angle opposite c, and we have $\cos\gamma = (a^2+b^2-c^2)/2ab$, and $(a^2 + b^2)^2 = a^4 + b^4 + 2a^2b^2 > a^4 + b^4 = c^4 = (c^2)^2 \implies (a^2 + b^2 - c^2)(a^2 + b^2 + c^2) > 0$, thus $a^2 + b^2 > c^2$ leading to $\cos\gamma > 0$ and hence (a, b, c) is an acute triangle. $\square$

The main result of our paper is the proof of the following theorem:

Theorem 1.1. *There exists no rational triangle with a Fermat index of* 4.

In Section 2, we establish a framework for the proof of Theorem 1.1, followed by the proof in Section 3.

Degenerate triangles are ruled out by definition, and from Lemma 1.1, obtuse and right triangles are also ruled out. Therefore, for the proof of Theorem 1.1, we need to consider acute triangles alone. We will call a triplet (a, b, c) an *integer triplet* (respectively, *rational triplet*), and the corresponding triangle, if it exists, an *integer triangle* (respectively, *rational triangle*), if, and only if, all of a, b and c are positive integers (respectively, rational numbers). A triplet (a, b, c) (and the corresponding triangle, if it exists) will be called *primitive* if, and only if, it is an integer triplet (respectively, triangle), and the greatest common divisor of a, b and c is 1.

Lemma 1.2. *For any integer triplet* (a, b, c) *satisfying (2),* $a^2 + b^2 - c^2$ *is even.*

Proof. First assume (a, b, c) is primitive. Then all of a, b, and c cannot be even. Neither can any two be even, as the third then cannot be odd. This leaves exactly one of a, b, and c even, and the remaining two odd, thus making $a^2 + b^2 - c^2$ also even, and this can then also be seen to hold when (a, b, c) is not primitive. □

Lemma 1.3. *If* (a, b, c) *is primitive and satisfies (3), then* c *must be odd.*

Proof. Assume c is even, then a and b are odd, and one may consider (a^2, b^2, c^2) a Pythagorean triplet. For some positive integers l, m, let $a^2 = 2l + 1$ and $b^2 = 2m + 1$. Then $(a^2)^2 + (b^2)^2 = 4(l^2 + m^2) + 4(l + m) + 2$ which is divisible by 2 and not by 4, whereas $(c^2)^2$ divisible by 4. This contradicts our assumption, hence c cannot be even. □

2 Framework for the Proof of Theorem 1.1

In this section, we describe establish a framework for the proof of Theorem 1.1, which is based on a geometric construction and the derivation of a class of polynomials which are obtained by relating the law of cosines to (3), for all triangles arising in this construction.

2.1 Construction

We consider a construction as shown in Figure 1 below.

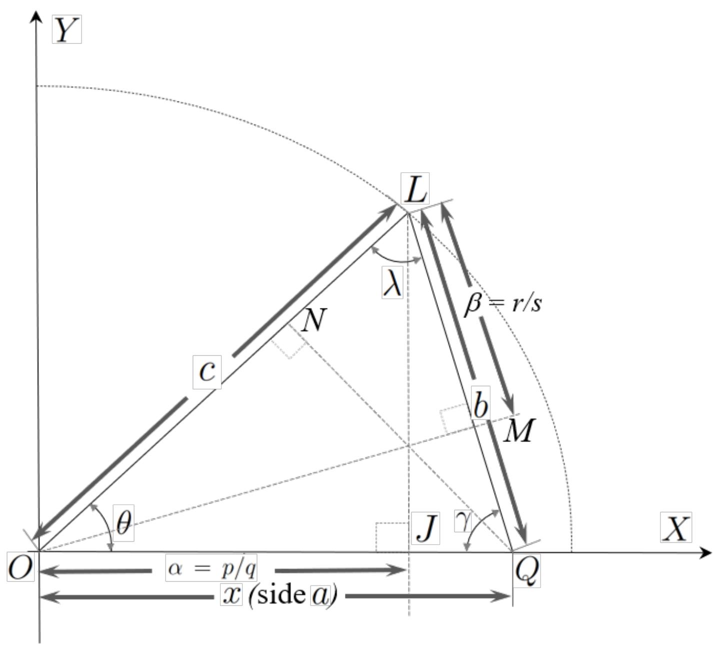

Figure 1. Construction for the proof

At O, the origin of the Cartesian axis in two dimensions, place a line segment OL with length c, at an angle θ to OX. Along OX, mark a line segment OQ of length a (labeled x in the figure). Denote the length of the side LQ in triangle OLQ by b. We will refer to the sides of OLQ by their respective lengths in the rest of the paper. Let the angle opposite side a be λ, that opposite side b be θ, and that opposite side c be γ. Note that, since we are looking for integer (hence rational) values of a and b, we allow $\cos\theta$ to only take on rational values. The projection of c on side a is $\alpha = p/q$, and that on side b is $\beta = r/s$, where p, q (respectively r, s) are either 1 or are positive coprime integers (α, β are either positive integers or irreducible common fractions), and hence $\cos\theta = p/(qc)$, $\cos\lambda = r/(sc)$. We use the notation $x \mid y$ to mean that x divides y. Then, in any integer triangle (a, b, c), from the cosine law, $(a^2 + c^2 - b^2)/(2ac) = p/(qc)$, and from Lemma 1.2, $2 \mid (a^2 + c^2 - b^2)$, and respectively for side b, therefore

$$q \mid a,\ s \mid b. \tag{4}$$

Since we are looking for positive values of a and b, it is sufficient to restrict θ to the first quadrant. Without loss of generality, we will allow c to only take positive integer values. We will define the triangle "rotated" around the altitude QN as axis in Fig. 1, with c at an angle λ to the X-axis, and side b swapped with side a, as the *transposed* triangle, indicated by the operation $(a, b, c)^T = (b, a, c)$.

Theorem 1.1 is now equivalent to

Theorem 2.1. *There exists no primitive triangle with Fermat index* 4.

2.2 Fermat–Pythagoras polynomials

Theorem 2.1 specifies only primitive triangles, because any rational triangle can be scaled to a primitive triangle. Hence, for all possible integer values of c and rational $\cos\theta$, the absence of primitive triangle solutions implies the absence of rational triangle solutions. This is a geometric analog of Gauss's Lemma [7]. The idea of the construction is now to "search" for such acute primitive triangles by continuously increasing x (starting from the position $x = OJ$), for all possible acute triangles with all positive integer values of c at all positive rational values of $\cos\theta$. We enable this search algebraically by equating the Fermat description of the length of side b with the corresponding Pythagorean description (the law of cosines) at constant c and α,

$$\begin{aligned}\Xi_4 = u_4(c, \alpha, x) &= \big(b(x)^2\big)^4 - (c^4 - x^4)^2 \\ &= (c^2 + x^2 - 2\alpha x)^4 - (c^4 - x^4)^2,\end{aligned} \tag{5}$$

where b is a function of x, and hence is denoted by $b(x)$. Clearly, Ξ_4 is a polynomial, which we will call *Fermat–Pythagoras* polynomial. Note that by similar arguments for the transposed triangle $(a, b, c)^T = (b, a, c)$, one may also derive $u_4(c, \beta, x)$ which equates the Fermat and Pythagorean formulae for side a. Henceforth, for simplicity, our analysis will only consider side a, but we note that the same analysis applies to side b also over the transposed triangle. We will point out any differences in the treatment for both sides explicitly, as and when they arise.

Lemma 2.1. *At constant c and $\cos\theta$, if Ξ_4 has non-zero real roots, then it has exactly two positive non-zero real roots, the product of which is c^2.*

Proof. We begin by observing in Fig. 1, that in the interval $-\infty < x < \alpha$, triangle QOL is obtuse. Since (3) can only be satisfied by acute triangles, no solutions can exist in this interval, except for $x = 0$, which is the trivial solution (for which no triangle exists and ϕ is not defined). Furthermore, $x = \alpha$ gives a right triangle (with $\phi = 2$), and is also ruled out. Therefore, we consider only the interval $\alpha < x < +\infty$. We see in (5) that $\Xi_4 = 0$ represents two types of equations: $c^4 - x^4 = \pm b(x)^4$. The first type of Fermat equation is obtained with $+b(x)^4$, and represents what we will call a *Type˜I triangle*,

$$x^4 + b(x)^4 = c^4. \tag{6}$$

Here, c is the greatest side, and $x, b(x) < c$. The second type of Fermat equation is obtained with $-b(x)^4$, and is a *Type˜II triangle*,

$$c^4 + b(x)^4 = x^4, \tag{7}$$

in which $c, b(x) < x$. Therefore, as x increases from an initial value of α in Fig. 1, we expect at first a Type˜I triangle with c as the longest side, which satisfies (6) for some $x = x_1$,

$$x_1^4 + b_1^4 = c^4, \tag{8}$$

where $b_1 = b(x_1)$. For constant c and θ, it is easy to see that (x_1, b_1, c), if it exists, is the only Type˜I triangle that satisfies (8). Fig. 1 shows that at constant c and θ, when $\gamma < \pi/2$ (equivalently, when $x > \alpha$), $b(x)$ is strictly increasing with x since $db/dx = (x - \alpha)/b$, hence $x > x_1 \iff b(x) > b_1$. Since c and θ remain constant, (8) will not be satisfied for any value of $x > x_1$. Therefore, for a given value of c and θ, there is exactly one Type˜I triangle.

At constant c and θ, x exceeds $b(x)$ and c when $x > \max\left(c, c^2/(2\alpha)\right)$. Then it is the longest side of triangle OLQ, in which case, for some $x = x_2$, (7) is satisfied with $b_2 = b(x_2)$,

$$c^4 + b_2^4 = x_2^4. \tag{9}$$

We see that, in fact, the Type˜II triangle in (9) can be obtained from the Type˜I triangle (x_1, b_1, c), by multiplying (8) throughout with $(c/x_1)^4$,

$$c^4 + (b_1 c/x_1)^4 = (c^2/x_1)^4, \tag{10}$$

which can be confirmed by substituting $x = c^2/x_1$ into the law of cosines formula for $b(x)$:

$$\sqrt{c^2 + (c^2/x_1)^2 - 2\alpha c^2/x_1} = (c/x_1)\sqrt{c^2 + x_1^2 - 2\alpha x_1} = b_1 c/x_1.$$

Thus we see that if a Type˜I triangle exists, a corresponding Type˜II triangle must also exist.

Now let us assume that the Type˜II triangle $(x_2, b_2, c) = (c, b_1 c/x_1, c^2/x_1)$ satisfying (9) exists and that there also exists a second value x_3 and correspondingly, $b_3 = b(x_3)$ which together satisfy (7), with (x_3, b_3, c) being one more Type˜II triangle for the given value of c and $\cos\theta$. Then we would have

$$c^4 + b_3^4 = x_3^4, \tag{11}$$

which would result in $c < x_3 \implies c^2/x_3 < c$, and also $b_3 < x_3 \implies b_3c/x_3 < c$, which, taken together, imply that multiplying (11) throughout by $(c/x_3)^4$, one obtains

$$(c^2/x_3)^4 + (b_3c/x_3)^4 = c^4, \tag{12}$$

where $(c^2/x_3, b_3c/x_3, c)$ is a valid Type˜I triangle (as can be verified by substituting $x = c^2/x_3$ into the law of cosines formulation of b_3) at the same values of c and θ as the other two triangles, and it should have been encountered for some $x < x_3$. But we have already seen that for a given c and $\cos\theta$, there is exactly one Type˜I triangle. Hence, it is not possible to have more than one Type˜II triangle, which is simply a Type˜I triangle of sides (x, b, c) scaled by the factor c/x. Furthermore, this proves the converse statement, that if a Type˜II triangle exists, then the corresponding Type˜I triangle must also exist. Therefore, if Ξ_4 has non-zero real roots, then it has exactly two positive real roots of the form $x = x_1 < c$ and $x = x_2 = c^2/x_1 > c$. The product of the two positive real roots of Ξ_4 is c^2, and apart from one trivial zero, the rest of the roots of Ξ_4 are complex. □

Since every Type˜II triangle is a scaled Type˜I triangle, it follows that the set of all Type˜II triangles is a subset of the set of all Type˜I triangles. Hence, Theorem 2.1 is reduced to

Theorem 2.2. *There exists no primitive Type˜I triangle with Fermat index* 4.

This leads to the following fact: to prove Theorem 2.1, it is sufficient to prove Theorem 2.2.

3 Proof of Theorem 2.1

We rewrite (5) as

$$u_4(c, \alpha, x) = -x\big(2x^3 - 4\alpha x^2 + (4\alpha^2 + 2c^2)x - 4c^2\alpha\big)\big(4\alpha x^3 - (4\alpha^2 + 2c^2)x^2 + 4c^2\alpha x - 2c^4\big), \tag{13}$$

which, upon setting $\alpha = p/q$, and in the light of (4), setting $x = qy$,

$$= -4y\big(q^4y^3 - 2pq^2y^2 + (2p^2 + q^2c^2)y - 2c^2p\big)\big(2pq^2y^3 - (2p^2 + q^2c^2)y^2 + 2c^2py - c^4\big). \tag{14}$$

Therefore $u_4(c, \alpha, x) = -4ys_4(c, p, q, y) = -4yg(p, q, y)h(p, q, y)$, where $s_4(c, p, q, y)$ is a sixth degree polynomial, that is factored into two third degree polynomials, $g(p, q, y)$ and $h(p, q, y)$, both of which have integer coefficients.

$$\begin{aligned} g_a = g(p, q, y) &= q^4y^3 - 2pq^2y^2 + (2p^2 + q^2c^2)y - 2c^2p, \\ h_a = h(p, q, y) &= 2pq^2y^3 - (2p^2 + q^2c^2)y^2 + 2c^2py - c^4. \end{aligned} \tag{15}$$

A similar equation may be derived for each of $g_b = g(r, s, z)$ and $h_b = h(r, s, z)$, where $x = sz$, with reference to the transposed triangle, (b, a, c). Therefore, we have two pairs of polynomials associated with each side of the triangle: $s_{4a} = (g_a, h_a)$ and $s_{4b} = (g_b, h_b)$. We will also denote the set of polynomials $s_4 = \{s_{4a}, s_{4b}\}$.

Lemma 3.1. *Every polynomial in the set* s_4 *has exactly one real root, and the real roots of at least one pair of polynomials* s_{4a} *and* s_{4b} *are irrational.*

Proof. Without loss of generality, we us assume that (a, b, c) is a primitive triangle. For simplicity, we consider Fermat–Pythagoras polynomials of side a with the arguments being equally applicable to the polynomials of side b of the transposed triangle (b, a, c). We ignore the trivial solution $x = 0\,(\implies y = 0)$ in $u_4(c, \alpha, x)$, since we are concerned with the interval $\alpha < x < +\infty$. We know that finding primitive triangles satisfying (3) would amount to finding integer roots of Ξ_4 in (5). We have established in Lemma 2.1 that, for a given c and $\cos\theta$, if non-zero real roots of $u_4(c, \alpha, x)$ exist, then there are exactly two positive real roots, with the rest of the roots being complex. If the first root is an integer of the form $x_1 = y_1 q$, then the second root is of the form $x_2 = y_2 q = c^2/x_1$, so that $y_2 = c^2/(y_1 q^2)$. Clearly, with the trivial $y = 0$ being ruled out, $u_4(c, \alpha, x) = 0$ whenever either $g_a = 0$, or $h_a = 0$, or both. Assume $g_a = 0$. We first recall the complex conjugate roots theorem [4], which states that for every complex root of a polynomial (including multiplicity), there must be a corresponding complex conjugate root. Being cubic, g_a must have at least one real root, since there cannot be three complex roots, thus confirming the existence of real roots of Ξ_4. For the same reason, it cannot have two real roots. Three real roots are not possible, as Lemma 2.1 shows that $u_4(c, \alpha, x)$ has exactly two real roots. Therefore, the remaining positive real root of Ξ_4 must be a zero of h_a. We have geometrically shown that one real root is greater than the other in value, therefore, both g_a and h_a cannot be zero simultaneously (reflecting the previously discussed geometric fact that the Type˜I triangle will occur before the Type˜II triangle, as x increases).

Let a polynomial with integer coefficients be defined as follows:

$$Q(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0. \tag{16}$$

The tool we use to verify the existence of integer roots of $Q(x)$ is the rational root theorem, which is a consequence of Gauss's Lemma [2, 7, 9].

Theorem 3.1. *If $Q(x)$ has a rational root of the form p/q, p is a factor of a_0, while q is a factor of a_n. Any integer root of $Q(x)$ must be a factor of a_0 only. These conditions hold irrespective of the sign of the root.*

Lemma 3.2. *If (a, b, c) is primitive and satisfies (2), then a, b, and c are pairwise mutually coprime.*

Since the greatest common divisor of a, b and c is 1, and if there is a common factor between any two, this would render in (2) a fraction equal to an integer [6]. Now let us assume that (a, b, c) satisfies (3). This means that side a cannot have a common factor with c. In particular, with $a = x_1 = y_1 q$, y_1 (respectively, q) must be coprime with c, provided $y_1 > 1$ (respectively, $q > 1$). We identify two cases: *(i)* $q > 1$, and *(ii)* $q = 1$.

Let us consider case *(i)* first, and let $q > 1$. We will establish that, given $a = y_1 q$, $y_1 > 1$. For if $y_1 = 1$, then $a = q$, which means that since $\big(a^2 + (c^2 - b^2)\big)/(2a) = p/q$, a is coprime with $c^2 - b^2$. However, from (3) we see that $a^4 = (c^4 - b^4) = (c^2 - b^2)(c^2 + b^2)$. Note that here $c^2 - b^2 > 1$ since $c = b + 1$ at least. Therefore a is not coprime with $c^2 - b^2$. This is a contradiction, hence $y_1 > 1$, and therefore must be coprime with c. From Lemma 2.1, $y_2 = c^2/(y_1 q^2)$, and since y_1 is coprime with c, and both $y_1, c > 1$, if y_1 is an integer, then y_2 must be a positive rational number in the form of an irreducible common fraction.

From Lemma 1.3, c is odd, and exactly one of a or b must be odd, and the other even. We will first assume that a is odd, without loss of generality (since if a were even, we would simply consider the transposed triangle (b, a, c)). Since $a = y_1 q$, both y_1 and q are odd, and $y_1 > 1$ as already shown. If y_1 were a solution of h_a in (15), then from Theorem 3.1, y_1 would have to be a factor of c. This is not possible since y_1 must be coprime with c as Lemma 3.2 shows. Therefore, y_1 can only be a solution of g_a, and not h_a, in (15), and hence it must be a factor of p in accordance with Theorem 3.1. This is consistent with y_2 being a root of h_a, since Theorem 3.1 shows that if a rational y_2 exists as a common fraction, the numerator and denominator would be factors respectively of the numerator and denominator of c^2/p. Therefore, y_1 is a factor of p. Let $p = y_1 m$ with m a positive integer, and substitute this expression into g_a, to get

$$q^4 y_1^2 - 2mq^2 y_1^2 + 2m^2 y_1^2 + q^2 c^2 - 2c^2 m = 0.$$

Grouping terms we get

$$y_1^2(q^4 - 2mq^2 + 2m^2) = c^2(2m - q^2). \tag{17}$$

The relation (17) can also be written as

$$y_1^2 q^2\big(m^2 + (q^2 - m)^2\big) = c^2\big(m^2 - (q^2 - m)^2\big). \tag{18}$$

Note that $m^2 - (q^2 - m)^2$ and $m^2 + (q^2 - m)^2$ are always odd, regardless of m being odd or even, since q is odd by assumption. Since q is coprime with p, q is coprime with m, and $m^2 - (q^2 - m)^2$ is coprime with $m^2 + (q^2 - m)^2$. Therefore, in (18), $a^2 = m^2 - (q^2 - m)^2$, and $c^2 = m^2 + (q^2 - m)^2$. Moreover, Fig. 1 shows the fact that $a > p/q \implies y_1 q > y_1 m/q$, thus $q^2 > m$. Then the numbers $u = m, v = (q^2 - m)$ are the generating terms for the Pythagorean triplet (a^2, b^2, c^2), with $a^2 = u^2 - v^2, b^2 = 2uv, c^2 = u^2 + v^2$ [6], and the Pythagorean triplet satisfying (3) is

$$a^2 = m^2 - (q^2 - m)^2, b^2 = 2m(q^2 - m), c^2 = m^2 + (q^2 - m)^2. \tag{19}$$

Now let us consider the transposed triangle (b, a, c), with side c making an angle of λ with the X-axis. The line segment LM occurs in place of OJ, and it has a length of

$$\beta = r/s = c\cos\lambda = (c^2 + b^2 - a^2)/(2b). \tag{20}$$

Substituting values from (19) into (20), we get

$$\beta = r/s = q^2/(2m). \tag{21}$$

Since q is odd and coprime with m, $q^2/(2m)$ is already an irreducible fraction. Therefore, $r = q^2$, and $s = 2m$. From (21), and comparing with (15), we see that

$$\begin{aligned} g_b = g(r, s, z) = g(q^2, 2m, z) = 16m^4 z^3 - 8q^2 m^2 z^2 + (2q^4 + 4m^2 c^2)z - 2c^2 q^2, \\ h_b = h(r, s, z) = h(q^2, 2m, z) = 8q^2 m^2 z^3 - (2q^4 + 4m^2 c^2)z^2 + 2c^2 q^2 z - c^4. \end{aligned} \tag{22}$$

Using (4) we let $b = z_1 s$, where z_1 is a positive integer. From (22), the constant term of g_b is $-2c^2 q^2$, while that of h_b is $-c^4$. Further, note from (13) that an additional factor of 2 must now be taken into account (since b is even). Therefore, z_1 might either be a factor of $2c^4$, or $4c^2q^2$. Since a factor of c is ruled out from Lemma 3.2, z_1 is either 2 or a factor of $4q^2$. But z_1 cannot also be a factor of q, since that would result in b having a common factor q with a, contradicting Lemma 3.2. Therefore z_1 can either be 1, 2 or 4. Together with these relations and (19), we set

$$b = z_1 s, \tag{23}$$

and

$$b^2 = z_1^2 s^2 = z_1^2 (2m)^2 = 2m(q^2 - m) \implies q^2 = 3m, 9m, \text{or } 33m. \tag{24}$$

We see in (24) that for $m > 1$ this results in q and m having factors in common, which contradicts our assumption of q and m being coprime. If $m = 1$ then $a^2 < 0$ in (19). Therefore, case *(i)*, $q > 1$, is impossible.

We next consider case *(ii)*, which is $q = 1$. Then, $a = y_1$. Since $y_1 \leq p$ leads to an obtuse (respectively, right) triangle, as can be seen by inspecting Fig. 1, $y_1 > p$. Secondly at $y_1 = 2p$ either a, or b or both are equal to c, and thus (3) cannot be satisfied. Therefore, $p < y_1 < 2p$. This means that no proper factor of $2p$ can equal y_1. Now if $y_1 = 2$, then p being an integer, must be 1. Then that would again lead to one or both of a and b being equal to c (and in any case, a is assumed to be odd). Clearly $y_1 > 1$ because p is at least 1, for which $y_1 = 1$ would lead to a right triangle. In case *(ii)* also, we see that no possible combination of factors of the constant term of g_a can equal y_1.

The above arguments for cases *(i)* and *(ii)* apply for all admissible integer values of c and rational $\cos\theta$. We have shown that no integer value of $a = y_1 q$ can be found for any integer c and rational $\cos\theta$ combination, in a Type˜I triangle, such that b is also an integer. Hence, no primitive Type˜I triangle (a, b, c) can exist as a solution to (3), and this proves Theorem 2.2. Since the set of all Type˜II triangles is a subset of the set of all Type˜I triangles, there is no primitive triangle (a, b, c) (and hence, no rational triangle) that satisfies (3). Therefore, at least one of a and b must be irrational. Hence the roots of at least one pair of polynomials s_{4a} and s_{4b} must be irrational, thus proving Lemma 3.1 and Theorem 2.1. Thus Fermat's Last Theorem for $n = 4$ is proved. □

The primary insight we obtain is that every real positive triplet (a, b, c) that satisfies (3) is an acute triangle; if c and a are restricted to be integers, then due to the constraint that sides of triangle (a, b, c) must satisfy both Pythagorean and Fermat relationships, the possible integer values of b are restricted to those that are non-coprime with either a or c, which renders such integer triplets impossible. The approach that we describe in this paper therefore offers significant fresh trigonometric insight into why Fermat's Last Theorem for $n = 4$ is true, and leads us to believe that it could be explored for application to other integer exponents of the Fermat equation.

Acknowledgements

The author is very grateful to Prof. Y. V. Venkatesh, Fellow of the Indian National Science Academy, and formerly the Dean, Faculty of Engineering, at the Indian Institute of Science, for his valuable counsel. The author is also deeply grateful to Prof. Gian-Carlo Rota, late of the

Massachusetts Institute of Technology, whose very valuable words of encouragement many years ago, has helped the author persevere.

References

[1] Barbara, R. (2007). 91.33 Fermat's Last Theorem in the Case $n = 4$. *The Mathematical Gazette*, 91(521), 260–262.

[2] Bold, B. (1982). *Famous Problems of Geometry and How to Solve Them*. Dover, New York.

[3] Charalambos, D., & Burkinshaw, O. (1998). *Principles of Real Analysis*. Academic Press Inc., San Diego.

[4] Cruikshank, J., McGuire, G., & O'Farrel, A. G. (2013). *Irish Mathematical Olympiad Manual*. Logic Press, Ireland.

[5] Dolan, S. (2011). 95.24 Fermat's method of "descente infinie". *The Mathematical Gazette*, 95(533), 269—271.

[6] Edwards, H. M. (2000). *Fermat's Last Theorem: A Genetic Introduction to Algebraic Number Theory*. Springer-Verlag, New York.

[7] Gauss, C. F. & Clarke, A. A. (1965). Article 42. In *Disquisitiones Arithmeticae* (p. 25). Yale University Press.

[8] Grant, M., & Perella, M. (1999). 83.25 Descending to the Irrational. *The Mathematical Gazette* 83(497), 263–267.

[9] King, J. D. (2006). 90.63 Integer Roots of Polynomials. *The Mathematical Gazette*, 90(519), 455–456.

[10] Ribenboim, P. (2000). *Fermat's Last Theorem for Amateurs*. Springer-Verlag, New York.

[11] Wiles, A. (1995). Modular Elliptic Curves and Fermat's Last Theorem. *Annals of Mathematics*, 141(3), 443–551.