**Notes on Number Theory and Discrete Mathematics**
**Print ISSN 1310–5132, Online ISSN 2367–8275**
**2025, Volume 31, Number 2, 410–428**
**DOI: 10.7546/nntdm.2025.31.2.410-428**

# Extending the plane trigonometric proof of Fermat's Last Theorem to the case $n = 3$

**Giri Prabhakar**

Siemens Technology
Electronics City Phase 2, Bangalore 560100, India
e-mail: giri.prab@siemens.com

**Received:** 26 June 2024 **Revised:** 7 May 2025
**Accepted:** 4 June 2025 **Online First:** 16 June 2025

**Abstract:** We extend the plane trigonometric approach that we used to prove the case $n = 4$ of Fermat's Last Theorem, to the case $n = 3$. We show that all real positive triplets satisfying $a^\phi + b^\phi = c^\phi$ for $\phi > 1$ are triangles. As in the case of $n = 4$, we equate the Pythagorean and Fermat descriptions of the triangles for a particular smaller side while fixing the other sides, with $\phi = n$ being any positive integer. We hence show the existence of Fermat–Pythagoras polynomials for $n \geq 3$. For the case $n = 3$, we explicitly derive an analytic expression for the roots of the polynomials. We prove from this expression that the real roots, which are equal to the length of the sides, are irrational.

**Keywords:** Pythagorean theorem, Diophantine equations, Fermat's Last Theorem.
**2010 Mathematics Subject Classification:** 51N20, 11D41.

## 1 Introduction

Fermat's Last Theorem, completely proved by Wiles [12] in 1995, has a long and interesting history. Numerous proofs for smaller exponents have been provided over time by mathematicians such as Euler, Legendre, Lamé and others [3, 5, 10]. In every case, the problem is to prove Fermat's statement true or false [5]: that there exist no positive integers $(a, b, c)$ for a positive integer exponent $n > 2$ such that $a^n + b^n = c^n$. Historically and traditionally, the proofs for smaller exponents and special cases have used the algebraic techniques of Diophantine analysis. A fundamental strategy element is the use of Fermat's method of infinite descent [4]. A distinction in the present approach is that it is trigonometric, which to the best of our knowledge departs from traditional approaches, and offers interesting additional insights.

In [9], we proved that the Fermat equation for $n = 4$, $a^4 + b^4 = c^4$, with $(a, b, c) \in \mathbb{R}_{>0}$, represents acute triangles. By means of a geometric construction that fixes two sides (including the largest side) of a triangle, we derived Fermat–Pythagoras polynomials $\Xi_4$ for the smaller third side. We showed that the values of the real roots $\Xi_4$ are the lengths of this variable side satisfying the Fermat equation for $n = 4$. We used algebraic and geometric arguments to prove that $\Xi_4$ cannot have rational roots. We now extend the approach, showing the existence of Fermat–Pythagoras polynomials $\Xi_n$ for all positive integers $n$. We explicitly derive the roots of these polynomials for $\Xi_3$, and prove that their real roots cannot be rational.

We will restate definitions and terminology from [9] and extend them as relevant to the present work. First, we generalize the Fermat equation and show that the triplets satisfying the equation are all triangles. We refer only to plane triangles throughout the work. 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 $\phi$ the *Fermat index* of $(a, b, c)$. We allow $\phi$ to take values as large as required to satisfy (1). For some choices of the triplet $(a, b, c)$, $\phi$ 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 $\phi$ grows unboundedly large. For completeness of our definition of the Fermat index, we accommodate for this possibility and define $\phi$ 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 [1].

Let the positive integer values of $\phi$ 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 analyze (2) for $n = 3$

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

We will first show that (1) represents triangles, which are obtuse for $1 < n < 2$ and acute for $n > 2$.

**Theorem 1.1.** *The triplet $(a, b, c)$ satisfying (1) forms a plane triangle with c the longest side.*

*Proof.* First let $(a, b, c) \in \mathbb{R}_{>0}$, with $b > a$ and $\phi \in (1, \infty)$; and consider the expression

$$(a + b)^\phi = b^\phi[1 + (a/b)]^\phi,$$

which, on expanding $[1 + (a/b)]^\phi$ as a convergent binomial series with $k \in \mathbb{Z}_{\geq 0}$, becomes

$$b^\phi \sum_{k=0}^{\infty} \binom{\phi}{k} (a/b)^k, \text{ where} \binom{\phi}{k} := \phi(\phi - 1) \cdots (\phi - k + 1)/k!,$$

$$= b^\phi + \phi a b^{\phi-1} + b^\phi \sum_{k=2}^{\infty} \binom{\phi}{k} (a/b)^k,$$

which holds for both integer and non-integer real values of $\phi$. Since $a^{\phi-1} < \phi b^{\phi-1}$,

$$(a+b)^\phi > \; b^\phi + a^\phi + b^\phi \sum_{k=2}^{\infty} \binom{\phi}{k} (a/b)^k. \tag{4}$$

The $k$-th term of $\sum_{k=2}^{\infty} \binom{\phi}{k} (a/b)^k$ is

$$t_k = [\phi(\phi-1)\cdots(\phi-k+1)/k!](a/b)^k,$$

so that

$$t_k + t_{k+1} = t_k\{1 + [(\phi-k)/(k+1)](a/b)\}.$$

Let $n$ be the first integer that is greater than $\phi$; then $t_n = [\phi(\phi-1)\cdots(\phi-n+1)/n!](a/b)^n \geq 0$, and in fact $\forall\, i \in \mathbb{Z}_{\geq 0} \ni r = n + 2i,\ t_r \geq 0$, because $\binom{\phi}{r}$ is either $0$ (when $\phi$ is an integer), or contains the product of an even number of negative terms in the numerator (when $\phi$ is a non-integer real number). Since $1 < \phi < r$, it follows that $r - \phi < r - 1 < r + 1$. Therefore, $\phi - r < 0$ and $|(\phi - r)/(r+1)| < 1 \implies 0 < t_r + t_{r+1} \leq t_r$, with the equality applying when $\phi = n - 1$. Hence

$$\sum_{k=2}^{\infty} \binom{\phi}{k} (a/b)^k = \sum_{k=2}^{\infty} t_k = \sum_{k=2}^{n-1} t_k + (t_n + t_{n+1}) + (t_{n+2} + t_{n+3}) + \cdots,$$

which implies that

$$0 < \sum_{k=2}^{n-1} t_k < \sum_{k=2}^{\infty} \binom{\phi}{k} (a/b)^k < (1 + a/b)^n,$$

and from (4) leading to the inequality

$$(a+b)^\phi > a^\phi + b^\phi = c^\phi,$$

from which we conclude that $a + b > c$. Since $c > a$ and $c > b$, we get $b + c > a$ and $c + a > b$. Thus, for $a \neq b$ and $\phi > 1$, (2) implies the triangle inequalities, which are necessary and sufficient for the triplet $(a, b, c)$ to form a triangle [7]. When $\phi = 1$, (2) implies that $(a, b, c)$ is a degenerate triangle. For $a = b$, the triangle inequality is trivially satisfied, since in (2), $2^{1/\phi} a = c$ (taking only the positive real root), thus $2a > c$, but also $c > a$.

Conversely, consider a triangle $(a, b, c) \in \mathbb{R}_{>0}$ which is either degenerate or non-degenerate (in the former case with $c$ and at least one of $a$, $b$ non-zero), with the length of all non-zero sides greater than 1. Let $c$ be (one of) the longest side(s). We have, in the degenerate case $a + b = c, a < c, b \leq c$, and in the non-degenerate case, $a + b > c$, $a \leq c$, $b \leq c$. First we assume strict inequality, and defer the equality cases to Lemmas 1.1 and 1.3 (where they will be shown to correspond to the extreme cases $\phi \to 1$ and $\phi \to \infty$). Thus, $a + b > c$, $a < c$, $b < c$. Note also that $\ln(c) > \ln(a)$ and $\ln(c) > \ln(b)$, where $\ln(.)$ refers to the natural logarithm. For every real number $x > 1$, let $y(x) = c^x/(a^x + b^x)$. Then

$$y'(x) = c^x\{a^x[\ln(c) - \ln(a)] + b^x[\ln(c) - \ln(b)]\}/(a^x + b^x)^2$$
$$= [c^x/(a^x + b^x)]\{a^x[\ln(c) - \ln(a)] + b^x[\ln(c) - \ln(b)]\}/(a^x + b^x),$$

thus

$$y'(x) = y(x)\{a^x[\ln(c) - \ln(a)] + b^x[\ln(c) - \ln(b)]\}/(a^x + b^x). \tag{5}$$

Let $\varepsilon = \min([\ln(c) - \ln(a)], [\ln(c) - \ln(b)])$. When we take away the terms $\ln(a)$ and $\ln(b)$ in (5) we see that

$$0 < \varepsilon < \{a^x[\ln(c) - \ln(a)] + b^x[\ln(c) - \ln(b)]\}/(a^x + b^x) < \ln(c),$$

hence we have

$$0 < \varepsilon y(x) < y'(x) < \ln(c)y(x),$$

and $y$ is smooth and real analytic, so that with $z \in \mathbb{R}$, for some value of $z > 1$

$$\int_1^z \varepsilon dx < \int_1^z dy/y < \int_1^z \ln(c)dx,$$

hence

$$\varepsilon(z-1) < \ln[y(z)/y(1)] < \ln(c)(z-1) \implies y(1)e^{\varepsilon(z-1)} < y(z) < y(1)e^{[\ln(c)](z-1)}. \tag{6}$$

Therefore, it is possible to choose $z = z_1$ and $z = z_2$ such that

$$y(1) < y(1)e^{\varepsilon(z_1-1)} = 1 \implies z_1 = 1 - (1/\varepsilon)\ln[y(1)] > 1,$$
$$y(1)e^{\ln(c)(z_2-1)} = 1 \implies z_2 = 1 - [1/\ln(c)]\ln[y(1)] > 1.$$

Since $\varepsilon < \ln(c)$, $1 - (1/\varepsilon)\ln[y(1)] > 1 - [1/\ln(c)]\ln[y(1)]$. In (6), the choice of $z = z_2$ (respectively, $z = z_1$), leads to $y(z_2) < 1$ (respectively, $y(z_1) > 1$). Thus, there exist $0 < \epsilon_1, \epsilon_2 < 1$ such that $1 - \epsilon_1 \le y(z) \le 1 + \epsilon_2$ whenever $1 - [1/\ln(c)]\ln[y(1)] \le z \le 1 - (1/\varepsilon)\ln[y(1)]$. Since $y$ is continuous in this interval, from Cauchy's Intermediate Value Theorem [2], there exists $\phi \in [1 - [1/\ln(c)]\ln[y(1)], 1 - (1/\varepsilon)\ln[y(1)]]$ such that $y(\phi) = 1$, or $c^\phi = a^\phi + b^\phi$. Moreover, $y'(x) > \varepsilon y(x) > 0 \ \forall \ x$. Then, from Cauchy's Mean Value Theorem [11], there exists some $\xi$ such that $\forall \ \delta > 0$, $[y(\phi+\delta) - y(\phi)]/\delta = y'(\xi) > 0$, hence $y(\phi+\delta) > y(\phi)$, and therefore $x = \phi$ is the unique value at which $y(x) = 1$. □

For rigor and completeness, the degenerate case $a + b = c, a < c, b \le c$, and the equality cases arising from $a + b > c, a \le c, b \le c$ must also be considered. Here we will call triangles with $a = c$ or $b = c$, or both, (isoceles and equilateral triangles) *singular triangles* in the context of our approach.

**Lemma 1.1.** *The Fermat index of a degenerate triangle is* 1.

*Proof.* Let $(a, b, c) \in \mathbb{R}_{>0}$ such that for some finite $\phi > 1$, $a^\phi + b^\phi = c^\phi \implies (a^\phi + b^\phi)^2 = (c^\phi)^2$. Let $\gamma$ be the angle opposite the longest side $c$ of the corresponding triangle $(a, b, c)$ with Fermat index $\phi$. As $\phi > 1$ and $\phi \to 1$, $(a, b, c)$ exists, and $(a + b)^2 \to c^2 \implies a^2 + b^2 - c^2 \to -2ab$, therefore, $\cos\gamma = \dfrac{a^2 + b^2 - c^2}{2ab} \to \dfrac{-2ab}{2ab} = -1$. Hence,

$$\lim_{\phi \to 1}(\gamma \mid a^\phi + b^\phi = c^\phi)\gamma = \pi.$$

Clearly the converse is true since $a+b=c \implies \phi=1$, and both $a, b$ cannot be zero together. In the case of one of the sides going to zero, $\phi$ is taken as 1 by definition (and is the Fermat index of a degenerate triangle in any case). Note that if $(a, b, c)$ is a finite degenerate triangle such that there exists a finite common exponent $\phi > 1$, $a = a_1^\phi, b = b_1^\phi, c = c_1^\phi \implies a_1^\phi + b_1^\phi = c_1^\phi$ with $(a_1, b_1, c_1) \in \mathbb{R}_{>0}$, then from Theorem 1.1, $(a_1, b_1, c_1)$ is a non-degenerate, non-singular triangle with Fermat index $\phi$. □

**Lemma 1.2.** *For obtuse non-degenerate triangles,* $1 < \phi < 2$ *and for acute triangles* $\phi > 2$.

*Proof.* Let $\gamma$ be the (largest) angle opposite $c$ for a triangle $(a, b, c)$ such that $a, b, c > 1$ (all triangles can be scaled thus). For any $x \in \mathbb{R}_{>0}$, let $h(x) = c^x$ and $l(x) = a^x + b^x$. From Theorem 1.1, there is a unique finite real number $x = \phi$ such that (2) holds for non-singular triangles. Set $x = \phi + y$, so that $h(\phi + y) = c^{(\phi+y)} = c^\phi e^{y\ln(c)} = a^\phi e^{y\ln(c)} + b^\phi e^{y\ln(c)}$, and similarly $l(\phi+y) = a^\phi e^{y\ln(a)} + b^\phi e^{y\ln(b)}$. Since $\ln(c) > \ln(a)$ and $\ln(c) > \ln(b)$, for $1 \le \phi + y < \phi \implies 1 - \phi \le y < 0$, $l(\phi + y) > h(\phi + y)$ and for $\phi < \phi + y < \infty \implies 0 < y < \infty$, $l(\phi + y) < h(\phi + y)$. Hence,

$$\begin{aligned} a^{\phi+y} + b^{\phi+y} &> c^{\phi+y}, & 1-\phi \le y < 0;\\ a^{\phi+y} + b^{\phi+y} &= c^{\phi+y}, & y = 0;\\ a^{\phi+y} + b^{\phi+y} &< c^{\phi+y}, & y > 0. \end{aligned} \tag{7}$$

When the Fermat index of $(a, b, c)$ is $1 < \phi < 2$, (7) implies that $a^2 + b^2 < c^2$, and $\cos\gamma = (a^2 + b^2 - c^2)/2ab < 0$, thus $\pi/2 < \gamma < \pi$ and the triangle is obtuse. When $2 < \phi < \infty$, then from (7), $a^2 + b^2 > c^2$, and $\cos\gamma = (a^2 + b^2 - c^2)/2ab > 0$, therefore, $\gamma < \pi/2$ and the triangle is acute. Obtuse triangles transition to acute ones as $\phi$ increases, passing through the right triangle at $\phi = 2$. □

**Lemma 1.3.** *For a singular triangle with sides* $(a_s, b_s, c)$*, with one or both of* $(a_s, b_s) = c$,

$$\lim_{a,b\to a_s,b_s} \phi \to \infty. \tag{8}$$

*Proof.* First let $a_s < c, b_s = c$. Let us begin with $(a, b, c)$ such that $a^\phi + b^\phi = c^\phi$ for some finite $\phi > 1$. We first assume $b > a$. Dividing throughout by $b$, and letting $b = b_s - \epsilon = c - \epsilon \implies c = b + \epsilon$,

$$\begin{gathered} (a/b)^\phi + 1 = (1+\epsilon/b)^\phi = 1 + \phi\epsilon/b + \delta(\epsilon),\\ \text{where } \delta(\epsilon) = \sum_{k=2}^{\infty} \binom{\phi}{k} (\epsilon/b)^k, \text{ with } \binom{\phi}{k} := \phi(\phi-1)\cdots(\phi-k+1)/k!,\\ \text{thus, } (a/b)^\phi/\phi = \epsilon/b + \delta(\epsilon)/\phi. \end{gathered} \tag{9}$$

Moreover, $\phi$ is a function of $\epsilon$. Since $\lim_{\epsilon\to 0}\delta(\epsilon) \to 0$, $\lim_{\epsilon\to 0}(a/b)^\phi/\phi \to 0$; the limit on the left-hand side of the equation, assumed indeterminate, can be evaluated with the application of the L'Hôpital rule [11].We differentiate the numerator and denominator by $\phi$ in the interval $(1, \infty)$.

We thus obtain $\lim_{\epsilon\to 0}(a/b)^{\phi}\ln(a/b) \to 0 \implies (a/b)^{\phi} \to 0 \implies \lim_{\epsilon\to 0}(\phi)\ln(a/b) \to -\infty$, since $a < b$, $\ln(a/b) < 1$, and $\lim_{\epsilon\to 0}\phi \to \infty$. Conversely, $\phi \to \infty \implies \epsilon \to 0$ in (9), and $b \to b_s = c$ will satisfy the limit. Therefore, any non-singular triangle $(a, b, c) \in \mathbb{R}_{>0}$ must have a finite $\phi$, and any triangle with two equal longest sides cannot have a finite $\phi$. Now let both $a_s, b_s = c$, so that $a \to a_s = c$ and $b \to b_s = c$. Let $\epsilon_1$ and $\epsilon_2$ both be small positive real numbers, and let $a = c - \epsilon_1$ and $b = c - \epsilon_2$. The two possibilities are: a subsequence in which $\epsilon_1 > \epsilon_2$ (which is covered by our previous analysis), or a subsequence in which $\epsilon_1 = \epsilon_2 = \epsilon \to 0$, from which we get $2[c-\epsilon]^{\phi} = c^{\phi}$, which, on taking positive real $\phi$-th roots (since $c$ and $c - \epsilon \in \mathbb{R}_{>0}$), leads to the equation

$$2^{1/\phi} = c/(c-\epsilon) \implies \phi = \ln(2)/\ln[c/(c-\epsilon)], \tag{10}$$

from which we conclude that $\lim_{\epsilon\to 0}\phi \to \infty$; conversely $\lim_{\phi\to\infty}\epsilon \to 0$. □

**Lemma 1.4.** *The triplet* $(a, b, c)$ *satisfying* (3) *forms an acute triangle with* $c$ *being the longest side.*

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

**Theorem 1.2.** *There exists no rational triangle with a Fermat index of* 3*.*

In Section 2, we recall the framework used in [9], and apply it for the proof of Theorem 1.2, followed by the proof in Section 3.

We will now state some definitions and lemmas (omitting proofs of those in [9]). Degenerate triangles are ruled out by definition, and from Lemma 1.4, obtuse and right triangles are also ruled out. Therefore, for the proof of Theorem 1.2, 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 1.5** ( [9]). *For any integer triplet* $(a, b, c)$ *satisfying* (2)*,* $a^2 + b^2 - c^2$ *is even.*

# 2 Framework for the proof of Theorem 1.2

In this section, we recall the framework used in [9]. We also include a couple of results important for the analysis.

## 2.1 Construction

We consider a construction as shown in Figure 1 below.

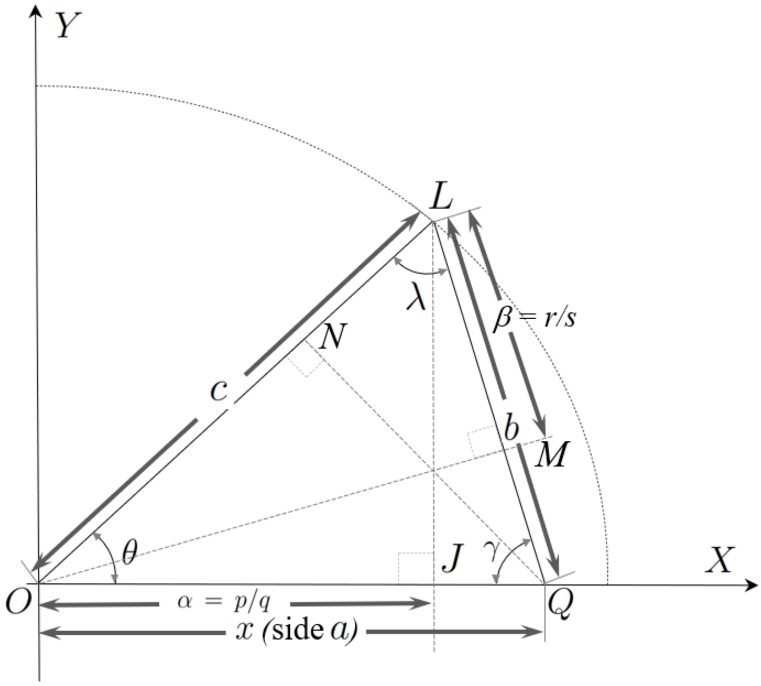



Figure 1. Construction for the proof.

At $O$, the origin of the Cartesian coordinate system in two dimensions, place a line segment $OL$ of length $c$, at an angle $\theta$ to $OX$. Along $OX$, mark a line segment $OQ$ of length $a$. This is labeled $x$ in Figure 1, and will be primarily used to indicate the variable length of side $a$. 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 $\lambda$, that opposite side $b$ be $\theta$, and that opposite side $c$ be $\gamma$. Note that, since we are looking for integer (hence rational) values of $x$ (side $a$) and $b$, we allow $\cos\theta$ to only take on rational values. The projection of $c$ on side $x$ is $\alpha = p/q$, and that on side $b$ is $\beta = r/s$, where $p, q$ (respectively $r, s$) are either $1$ or positive coprime integers ($\alpha, \beta$ 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 $(x, b, c)$, from the cosine law, $(x^2 + c^2 - b^2)/(2ac) = p/(qc)$, and from Lemma 1.5, $2 \mid (x^2 + c^2 - b^2)$, and respectively for side $b$, therefore

$$q \mid x. \tag{11}$$

Since we are looking for positive values of $x$ and $b$, it is sufficient to restrict $\theta$ 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 Figure 1, with $c$ at an angle $\lambda$ to the $X$-axis, and side $b$ swapped with side $x$, as the *transposed* triangle, indicated by the operation $(x, b, c)^T = (b, x, c)$.

Now (1) can also be written as the following (dual) trigonometric equation:

$$\sin^\phi\theta + \sin^\phi\lambda = \sin^\phi\gamma = \sin^\phi(\theta + \lambda) \tag{12}$$

Equation (12) is derived by invoking the sine rule [11]: $\sin\lambda/x = \sin\theta/b = \sin\gamma/c = 1/(2R)$ where $R$ is the circumradius of the triangle with sides $x, b$ and $c$.

Theorem 2.1 and the following Corollary 2.1.1 are needed to show that the Fermat index $\phi$ is strictly increasing with $\theta$, and has a unique value at every $\theta$. This enables us to use the construction in Section 2 to examine $\phi$ for increasing values of $x$, at every rational $\cos\theta$, thereby introducing a systematic and complete coverage of all possible rational values of the sides of the triangles, and to derive some useful properties of the Fermat–Pythagoras polynomials.

**Theorem 2.1.** *Let $\omega = \max[\theta, (\pi-\theta)/2]$. For constant $c$ and $\theta$, $\gamma$ in the interval $(\omega, \pi-\theta]$ is a continuous, strictly decreasing and bijective function of $\phi$.*

*Proof.* As shown in the proof to Theorem 1.1 and implied by (5), given a triangle $(x, b, c)$, $x^z + b^z - c^z$ is strictly decreasing for $z \geq 1$. Refer to Figure 1; let us hold $c$ and $\alpha$ constant (hence angle $\theta$ constant) while $x$ increases in the interval $[0, 2\alpha)$. From the construction, we see that $\gamma$ is strictly decreasing with respect to $x$; since $\theta$ is constant, as $x$ increases, $\lambda$ increases, and $\gamma$ decreases. This implies that, since $0 \leq \gamma \leq \pi - \theta$, $\cos\gamma$ is strictly increasing with respect to $x$. For each triangle, (2) can also be written in the trigonometric form (12). Consider two triangles at $x_1$ and $x_2$, respectively, with angles $\gamma_1 > \gamma_2$ and $\lambda_1 < \lambda_2$, sides $(x_1, b_1, c)$, $(x_2, b_2, c)$, circumradii $R_1$, $R_2$ and Fermat indices $\phi_1$, $\phi_2$. We will consider the following two cases: 1) $\gamma_1, \gamma_2 \in (\pi/2, \pi-\theta)$, and 2) $\gamma_1, \gamma_2 \in (0, \pi/2)$, with the condition that $\gamma_1 > \gamma_2$ in both cases.

Case 1 ($\pi - \theta > \gamma_1 > \gamma_2 > \pi/2$): Since we have $2R_1 \sin\gamma_1 = 2R_2 \sin\gamma_2 = c$, and $x_2 > x_1 \implies R_2 \sin\lambda_2 > R_1 \sin\lambda_1$, the relations together yield: $\sin\lambda_2/\sin\gamma_2 > \sin\lambda_1/\sin\gamma_1$. Taking the $\phi_1$-th powers and subtracting 1 from both sides then gives

$$[\sin^{\phi_1}\lambda_2 - \sin^{\phi_1}\gamma_2]/\sin^{\phi_1}\gamma_2 > [\sin^{\phi_1}\lambda_1 - \sin^{\phi_1}\gamma_1]/\sin^{\phi_1}\gamma_1$$

(note that $\phi_1 > 1$). Using $\sin\gamma_2 > \sin\gamma_1 > 0$ we further obtain

$$[\sin^{\phi_1}\lambda_2 - \sin^{\phi_1}\gamma_2]/\sin^{\phi_1}\gamma_2 > [\sin^{\phi_1}\lambda_1 - \sin^{\phi_1}\gamma_1]/\sin^{\phi_1}\gamma_2,$$

which leads to

$$\sin^{\phi_1}\lambda_2 - \sin^{\phi_1}\gamma_2 > \sin^{\phi_1}\lambda_1 - \sin^{\phi_1}\gamma_1, \tag{13}$$

in which the right-hand side, from (12), gives $\sin^{\phi_1}\lambda_1 - \sin^{\phi_1}\gamma_1 = -\sin^{\phi_1}\theta$, which upon substitution in (13) yields

$$\sin^{\phi_1}\theta + \sin^{\phi_1}\lambda_2 > \sin^{\phi_1}\gamma_2. \tag{14}$$

Now we multiply (14) throughout with the factor $(2R_2)^{\phi_1}$ and get

$$x_2^{\phi_1} + b_2^{\phi_1} > c^{\phi_1}, \tag{15}$$

which from the analysis in Lemma 1.2 and (7) leads to $\phi_2 > \phi_1$.

Case 2 ($\pi/2 > \gamma_1 > \gamma_2 > 0$): Recalling the law of cosines [11] as $\cos\gamma = (x^2 + b^2 - c^2)/2xb$,

$$x_1 < x_2 \iff \gamma_1 > \gamma_2 \iff \cos\gamma_1 < \cos\gamma_2,$$

which implies

$$(x_1^2 + b_1^2 - c^2)/2x_1b_1 < (x_2^2 + b_2^2 - c^2)/2x_2b_2,$$

because

$$x_1 < x_2 \wedge b_1 < b_2, \implies x_1^2 + b_1^2 - c^2 < x_2^2 + b_2^2 - c^2,$$

and since $2 < \phi < \infty$, this implies from (7) in Lemma 1.2, that there exists $\epsilon > 0 \wedge \phi_1 = 2+\epsilon \ni (x_1)^{\phi_1} + (b_1)^{\phi_1} - (c)^{\phi_1} = 0$, at which value of $\phi$ we also have $(x_2)^{\phi_1} + (b_2)^{\phi_1} - (c)^{\phi_1} > 0$, (because $x_1 < x_2 \wedge b_1 < b_2$). It follows from (7) that there must exist $\phi_2 > \phi_1$, such that $x_2^{\phi_2} + b_2^{\phi_2} - c_2^{\phi_2} = 0$.

From Cases 1 and 2, it holds that for fixed $c, \theta$

$$x_1 < x_2 \iff \gamma_1 > \gamma_2 \iff \phi_1 < \phi_2. \tag{16}$$

Assuming that $\theta \leq \pi/3$, a singular triangle occurs when $x = c$ (or $b = c$, if $\theta \geq \pi/3$ to begin with). For the condition $x = c$, $\gamma = (\pi - \theta)/2$, and if $b = c$, $\gamma = \theta$. When $\gamma = \omega$, from Lemma 1.3, $\phi = \infty$; however, in the limit as $\gamma \to \omega$, the geometric condition of (16) is always satisfied. Thus, the interval $(\omega, \pi - \theta]$ is a bijection of $\phi \in [1, \infty)$, with the special points $\phi(\pi - \theta) = 1$, $\phi(\pi/2) = 2$ and $\lim_{\gamma \to \omega} \phi \to \infty$ defining degenerate, right and singular triangles, respectively. □

**Corollary 2.1.1.** *For constant $c$ and $\theta$, let $\gamma^+ = \gamma \ni x = \max(b, c)$. Then, $\gamma$ in the interval $(0, \gamma^+)$ is a continuous, strictly increasing and bijective function of $\phi$.*

*Proof.* At the value of $x$ for which $x = \max(b, c)$, $(x, b, c)$ is singular, and hence is not an obtuse triangle, and $\pi/2 > \lambda_2 > \lambda_1 > 0$. Then, as $x$ increases, $\lambda \to \pi/2$. Therefore, an analysis similar to Case 1 of Theorem 2.1 applies in this case also, except that (applying the same terminology) the governing equation becomes:

$$\sin^\phi \gamma + \sin^\phi \theta = \sin^\phi \lambda. \tag{17}$$

Since $\sin \lambda_2 > \sin \lambda_1$ and $\sin \gamma_2 < \sin \gamma_1$, we have $\sin^{\phi_1} \lambda_2 - \sin^{\phi_1} \gamma_2 > \sin^{\phi_1} \lambda_1 - \sin^{\phi_1} \gamma_1 = \sin^{\phi_1} \theta$ from (17). This leads to

$$\sin^{\phi_1} \theta + \sin^{\phi_1} \gamma_2 < \sin^{\phi_1} \lambda_2. \tag{18}$$

Now we multiply (18) throughout with the factor $(2R_2)^{\phi_1}$ and get

$$b_2^{\phi_1} + c^{\phi_1} < x_2^{\phi_1}, \tag{19}$$

which from the analysis in Lemma 1.2 and (7) leads to $\phi_2 < \phi_1$.

For $\pi/2 < \lambda < \pi$, it holds that $\lambda_2 > \lambda_1 \implies \cos \lambda_2 < \cos \lambda_1 < 0 \implies -\cos \lambda_2 > -\cos \lambda_1$, hence $(x_2^2 - c^2 - b_2^2)/2b_2c > (x_1^2 - c^2 - b_1^2)/2b_1c \implies b_2^2 + c^2 - x_2^2 < b_1^2 + c^2 - x_1^2 < 0$ because $b_2 > b_1$. Then from Lemma 1.2, and (7), there exist $\epsilon > 0$ and $\phi_1 = 2 - \epsilon$ such that $b_1^{\phi_1} + c^{\phi_1} - x_1^{\phi_1} = 0$, and $0 < \delta < 1$ such that $b_1 = b_2^\delta, x_1 = x_2^\delta$, so that with $\phi_m = \delta\phi_1 < \phi_1$, $b_2^{\phi_m} + c^{\phi_1} - x_2^{\phi_m} = 0 \implies b_2^{\phi_m} + c^{\phi_m} - x_2^{\phi_m} < 0$. From Lemma 1.2, and (7), this leads to $\phi_2 < \phi_1$ such that $b_2^{\phi_2} + c^{\phi_2} - x_2^{\phi_2} = 0$. □

Theorem 1.2 is now equivalent to the following statement.

**Theorem 2.2.** *There exists no primitive triangle with Fermat index* 3.

## 2.2 Fermat–Pythagoras polynomials

Theorem 2.2 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 [6]. 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 $\alpha$, which for $n \geq 3$ is

$$\begin{aligned}\Xi_n = u_n(c,\alpha,x) &= \left(b(x)^2\right)^n - (c^n - x^n)^2 \\ &= (c^2 + x^2 - 2\alpha x)^n - (c^n - x^n)^2,\end{aligned} \tag{20}$$

$$\begin{aligned}&= nc^{2(n-1)}x(x-2\alpha) + x^n(x-2\alpha)^n \\ &\quad + \sum_{k=2}^{n-1}\binom{n}{k}c^{2(n-k)}x^k(x-2\alpha)^k + 2c^nx^n - x^{2n}\end{aligned} \tag{21}$$

Thus

$$\begin{aligned}u_n(c,\alpha,x) &= xs_n(c,\alpha,x) \\ &= x[nc^{2(n-1)}(x-2\alpha) + x^{n-1}(x-2\alpha)^n \\ &\quad + \sum_{k=2}^{n-1}\binom{n}{k}c^{2(n-k)}x^{k-1}(x-2\alpha)^k + 2c^nx^{(n-1)} - x^{(2n-1)}]\end{aligned} \tag{22}$$

where $b$ is a function of $x$, and hence is denoted by $b(x)$. Clearly, $\Xi_n = xS_n$ 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 such polynomials by equating 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. Also, $\Xi_1 = 0$ and $\Xi_2 = 0$ are degenerate cases as can be seen by inspection in (20). Further,

$$\begin{aligned}s_n(c,\alpha,x) &= nc^{2(n-1)}(x-2\alpha) + x^{n-1}(x-2\alpha)^n \\ &\quad + \sum_{k=2}^{n-1}\binom{n}{k}c^{2(n-k)}x^{k-1}(x-2\alpha)^k + 2c^nx^{n-1} - x^{2n-1},\end{aligned} \tag{23}$$

which upon some simplification becomes

$$\begin{aligned}-s_n(c,\alpha,x) &= 2n\alpha x^{2(n-1)} - 2n(n-1)\alpha^2x^{2n-3} + \cdots + 2^n\alpha^nx^{n-1} - 2c^nx^{n-1} \\ &\quad - \sum_{k=2}^{n-1}\binom{n}{k}c^{2(n-k)}x^{k-1}(x-2\alpha)^k - nc^{2(n-1)}x + 2nc^{2(n-1)}\alpha.\end{aligned} \tag{24}$$

with the $s_n(c,\alpha,x)$ being collectively represented by $S_n$.

**Theorem 2.3.** *Every Fermat–Pythagoras polynomial $\Xi_n$ has one trivial root, $x = 0$, and $S_n$ has $2(n-1)$ roots, denoted by $\rho_n = \{\rho_n^{\mathbb{R}}, \rho_n^{\mathbb{C}}\}$ comprising 2 real roots in $\rho_n^{\mathbb{R}}$ and $2(n-2)$ complex roots $\rho_n^{\mathbb{C}}$, respectively, the latter being $n-2$ pairs of complex conjugates. Let $\rho_n^{\mathbb{R}} = \{r_1, r_2\}$ and $\rho_n^{\mathbb{C}} = \{\rho_n^{c+}, \rho_n^{c-}\}$, so that $\rho_n^{c+} = \{c_1^+, c_2^+, \ldots, c_{n-2}^+\}$, and $\rho_n^{c-} = \{c_1^-, c_2^-, \ldots, c_{n-2}^-\}$. Then $r_1 r_2 = c_1^+ c_1^- = c_2^+ c_2^- = \cdots = c_{n-2}^+ c_{n-2}^- = c^2$, and the roots may also be grouped into pairs of real (respectively, complex but not conjugate) elements, the product of each pair being $c^2$.*

*Proof.* We begin by examining the zeros of $u_n(c, \alpha, x)$. Firstly, setting $u_n(c, \alpha, x) = 0$ in (20) leads to $[c^n - x^n] = \pm\sqrt{[c^2 + x^2 - 2x\alpha]^n} = \pm b^n$, the principal roots of which are always real since for all $x \in \mathbb{R}$, $c^2 + x^2 - 2x\alpha = (x-\alpha)^2 + c^2 - \alpha^2 > 0$ because $c > \alpha$. Here $b$ can be regarded as the third side of a triangle with sides $c$, $x$ and $b$, and Fermat index $n$; the side $b$ can also be seen to result from the cosine law applied to this triangle. Therefore, $u_n(c, \alpha, x) = 0$ represents two forms of the Fermat equation: $c^n = x^n + b^n$ (a triangle with $c$ as the hypotenuse), and $c^n + b^n = x^n$ (a triangle with $x$ as the hypotenuse).

Along with this observation, we see that the monotonicity and bijective nature of $\phi$ in relation to $x$ described in Theorem 2.1 ($x$ being one of the smaller sides) and Corollary 2.1.1 ($x$ being the largest side), imply that there are exactly two real solutions for $x$. Note the term $-2x\alpha$ in $u_n(c, \alpha, x)$: this term in the cosine law is sign dependent, and our assumption that $0 \leq \alpha < 1$, along with $(x, b, c)$ being acute geometrically ($n > 2$) implies that $x > 0$ is the only possibility for the non-trivial real solution. Secondly, since $u_n(c, \alpha, x) = x s_n(c, \alpha, x)$ in (22), the term $x$ is either a trivial zero, or factors out of $u_n(c, \alpha, x)$. The value $x = 0$ corresponds to one of $a = 0$ or $b = 0$ in (2). Also note that for $n = 1$ in (22), $s_1[c, \alpha, x] = 2x(c - \alpha)$, and hence there is just the trivial solution $x = 0$ (corresponding to the degenerate triangle). Hence we will assume $n \geq 2$, and there are two non-trivial real solutions to $u_n(c, \alpha, x) = 0$, both of which are necessarily triangles with Fermat index $n$. As $x$ increases from $\alpha$, the first such (identifiable) triangle will be called *primal triangle* and the second triangle, the *dual triangle*.

Refer to Figure 2; let $x = \alpha + h$. We divide the real line $x$ into three domains or cases:

(a) $h < 0$,
(b) $0 \leq h \leq \min(c - \alpha, \alpha)$; and
(c) $\min(c - \alpha, \alpha) < h < \infty$.

Consider case (a): for all values of $h < 0$, the triangle formed by line segments $x$ and $c$ is obtuse, for example $Q_2OL$ in the figure. From Lemma 1.2, the Fermat index of such triangles is not a whole number: $1 < \phi < 2$, and for $n \geq 2 \in \mathbb{Z}$, $s_n(c, \alpha, x) \neq 0$; both the cases $c^n - x^n = \pm b^n$ are not satisfied. Moreover, the Fermat index of any possible obtuse triangle can never equal $n$ (except $n = 1$, which is the degenerate case). Therefore, in case (a), $s_n(c, \alpha, x)$ cannot have a real root.

In case (b), the triangle is right or acute: all triangles including and beyond $JOL$, such as $Q_1OL$, with $x$ increasing up to the point $N$ such that $JN = \min(c - \alpha, \alpha)$. Here $\phi$ is a strictly increasing and bijective function of $h$ as shown in (16), and $2 \leq \phi < \infty$, with $\phi \to \infty$ as $h \to \min(c - \alpha, \alpha)$.

Therefore, there is exactly one value of $h$ (corresponding to $\alpha + h^* = x^*$) at which $\phi_{x^*}(c, \alpha) = n$, and $s_n(c, \alpha, x^*) = s_n(c, \alpha, \alpha + h^*) = 0$. This is the first non-trivial real solution for $u_n(c, \alpha, x) = 0$

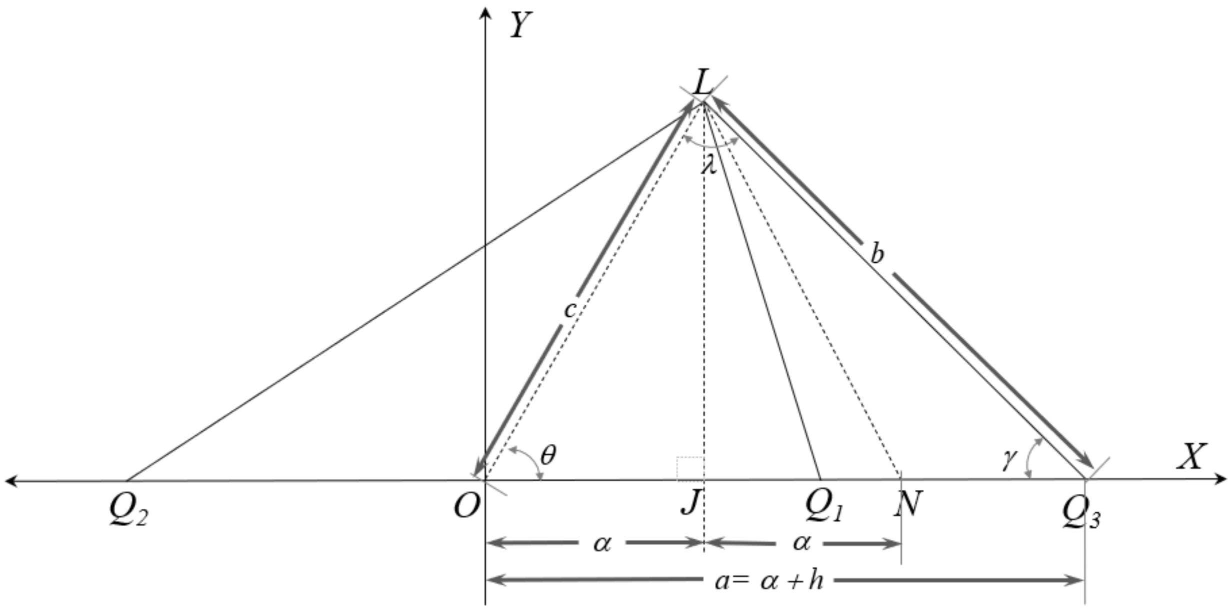



Figure 2. Geometric interpretation of (20): $x$ is the variable side of the triangle on the $x-$axis, $c$ is fixed, and $b$ is determined simultaneously by the cosine rule and the Fermat equation.

with $c$ as hypotenuse, which is the primal triangle (which corresponds to the *Type I* triangle in [9]). In this case, the corresponding Fermat equation is $(x^*)^n + b^n = c^n$. Multiplying this equation throughout by the factor $(c/x^*)^n$, we get $c^n + (bc/x^*)^n = (c^2/x^*)^n$. Since the hypotenuse of the triangle is already fixed as $c$, for increasing values of $x$, we expect a second solution, at $x = c^2/x^*$ (which can be verified by substituting $x^*$ with $c^2/x^*$ in $u_n(c, \alpha, x^*) = 0$ in (20)). Since in the second form of the equation $x$ must be the largest side of the triangle, Corollary 2.1.1 shows that there is again exactly one real solution. Given that there are only two possible real solutions, and given that the first zero of $s_n(c, \alpha, x) = 0$ at $x = x^*$, the second must occur at $x = c^2/x^*$, which is the dual triangle (such as $Q_3OL$ in Figure 2, corresponding to the *Type II* triangle in [9]). Since $x^* < c$, $c^2/x^* > c$ which means $c$ is no longer the largest side, but the smallest side, with the triangle now being $(c, cb/x^*, c^2/x^*)$.

Summarizing, $u_n(c, \alpha, x)$ has exactly one trivial zero. The corresponding $\Xi_n$ has two nontrivial real zeros of the form $x^*$ and $c^2/x^*$, the product of the roots being $c^2$. Note from (24) that $s_n(c, \alpha, x)$ is a polynomial of degree $2(n - 1)$. Therefore, from the Fundamental Theorem of Algebra [8], $\Xi_n$ must additionally have $2(n - 2)$ complex roots, which, from the Complex Conjugate Root Theorem [11], comprise $n - 2$ complex conjugate pairs. As shown earlier, there are only 2 real triangles that will geometrically satisfy $\Xi_n$ for a given $c$ and $\alpha$ (and, equivalently, only two equations of the form (2)), but the unknown in each of these equations also being an $n$-th root of a positive number, must have $n$ roots or solutions, of which we therefore expect $n - 1$ (if $n$ is odd), or $n - 2$ (if $n$ is even), complex solutions for each triangle. These complex solutions form complex triangles (with sides $a, b \in \mathbb{C}$ and (by definition) $c \in \mathbb{R}_{>0}$). Clearly therefore, for each complex root $x^* \in \mathbb{C}$, there must also exist a root of the form $c^2/x^* \in \mathbb{C}$, which must also satisfy (2) as a corresponding complex triangle, and the product of these two roots is $c^2$. Theorem 1.1 shows that $(x, b, c)$ is constrained to be a triangle, imposing a dependence between $x$ and $b$, which results in negative roots being absent for even $n$. Hence, each of the primal and dual triangles will consist of only one real root (triangle) and $n-1$ ($n$ odd), or $n-2$ ($n$ even), complex roots (triangles). The $2(n-2)$ complex conjugate roots of $\Xi_n$ can also be paired into (non-conjugate) roots whose product is $c^2$. Therefore, each complex root of the primal triangle (which we will call *primal root*) must have a corresponding complex root of the dual triangle, that we will call *dual root*. Each pair of primal and dual roots will be referred to as *complementary roots*. $\square$

In the rest of the paper, we will denote odd prime numbers by the symbol $m$.

**Corollary 2.3.1.** *Every Fermat–Pythagoras polynomial $\Xi_m$, has exactly one pair of complex roots, that are both conjugate and complementary.*

*Proof.* With an odd prime number $m$, $\Xi_m$ will have $2(m-1)$ roots, with one real root each corresponding to the primal and dual triangles respectively. Of the remaining $2(m-2)$ roots, it is necessary that both the primal and dual triangles possess an equal number of roots, since a given root in the primal triangle, say $x^*$, will necessarily correspond to a complementary root $c^2/x^*$, in the dual triangle. Hence the primal and dual triangles have $m-2$ complex roots each. Since $m$ is an odd number, $m-2$ is also odd, but this poses a problem, as the Complex Conjugate Root Theorem [11] requires that each complex root must also be associated with a complex conjugate root. Moreover, as described in the proof of Theorem 2.3, for odd $m$, (2) must have one real root and $m-1$ complex roots. Then the only possibility is that there exists exactly one pair of complex roots that satisfy both the primal and dual triangles. However, the roots of the dual triangle are complementary to those of the primal triangle. Therefore, this pair of roots must be such that they are both conjugate and complementary. Now, let one root be of the form $a_c + ib_c$. Then, it must follow that,

$$(a_c + ib_c)(a_c - ib_c) = c^2, \implies a_c^2 + b_c^2 = c^2 \tag{25}$$

Therefore, there exists one pair of complex triangles that are common to both sets of primal and dual triangles, possible because one complex side ($x$) has the modulus $c$, while the other side ($b$) is of modulus $0$. We will call roots of the form (25) *conjoint roots* of $\Xi_m$. Note that the components of the conjoint roots form a right triangle with $c^2$ as the hypotenuse. We will call such a triangle *conjoint right triangle*. Hence, every Fermat–Pythagoras polynomial with an odd prime Fermat index is associated with exactly one pair of conjoint roots, which we will denote by $(c_1, c_2)$, associated with one pair of conjoint complex degenerate triangles and a conjoint right triangle $(a_c, b_c, c)$. $\square$

**Lemma 2.1.** *At constant c and $\cos\theta$, $\Xi_3$ has exactly two positive non-zero real roots $\rho_3^{\mathbb{R}} = (r_1, r_2)$ and two conjoint roots $(c_1, c_2)$, with $r_1 r_2 = c_1 c_2 = c^2$.*

**Remark 2.1.** *For $n = 2$, $\Xi_2 = (x-\alpha)(c^2 - x\alpha)$, and a quadratic equation of the form $(\alpha+h)^2 - \alpha(\alpha+h) = 0$ is produced in result, which has two real roots $h = -\alpha$ corresponding to a degenerate triangle with zero area, the primal root being at $h = 0$ ($x = \alpha$), corresponding to a right triangle. As expected, the dual root occurs when $x = \alpha + h = c^2/\alpha$, or, $c^2 = \alpha(\alpha+h)$, which implies that $\alpha + h$ forms a right triangle with sides $c$ and $b$, which can be seen by applying the* *cosine law, $b^2 = c^2 + c^4/\alpha^2 - 2c(c^2/\alpha)(\alpha/c)$, which results in $c^2 + b^2 = (c^2/\alpha)^2$. Geometrically, the solution $x = \alpha + h = c^2/\alpha$ simply corresponds to scaling the original right triangle with sides $(\alpha, b, c)$, by the factor $c/\alpha$, to get a right triangle $(c, bc/\alpha, c^2/\alpha)$.*

We state some relevant results with proofs where needed and derive further properties related to the geometric construction and Fermat's equation. We will use the symbol $y \perp z$ to indicate integer $y$ is coprime to integer $z$.

**Lemma 2.2.** *The sides of a primitive integer triangle with an integer Fermat index are pairwise coprime.*

This is because for (2) with all variables as positive integers, $a$, $b$, and $c$ must be pairwise coprime [5]. Lemma 2.2 shows that no factor of $c$ can be a factor in an integer root of (2), and hence of $\Xi_m$, if such an integer root exists. A well-known and basic result for (2) is the basis for the following (see [5])

**Lemma 2.3.** *In a primitive integer triangle $(a, b, c)$ with integer Fermat index $n$, exactly two of the sides $a$, $b$ and $c$ are odd, and the remaining side is even.*

We restate (11) and add further results important to our analysis:

**Lemma 2.4.** *In an integer triangle $(a, b, c)$ if $\alpha = p/q \in \mathbb{Q}_{>0}$, then $q \mid a$. Furthermore, $q$ is odd, and $q \equiv 1 \mod (m)$.*

*Proof.* In triangle $(a, b, c)$, $\cos\theta = \dfrac{a^2 + c^2 - b^2}{2ac} = \dfrac{p}{qc}$. Hence $\dfrac{a^2 + c^2 - b^2}{2a} = \dfrac{p}{q}$, and $p$ and $q$ are coprime by definition. Since $a$, $b$ and $c$ are assumed integers, from the parity condition described by Lemma 2.3, two of the sides are odd while one is even, hence $a^2 + c^2 - b^2$ is even. Thus, $q$ must be a factor of $a$. Now let $a = \zeta q$. Then (2) can be written for Fermat index $m$ as $\zeta^m q^m = (c - b)(\sum_{k=1}^{m} c^{m-k} b^{k-1}) = (c - b)\kappa$. Following the method in [5] (p. 64, for example), we see that $(c - b) \perp \kappa$. Moreover, $(c + b) \perp \kappa$. Since $a^2 + c^2 - b^2 = \zeta^2 q^2 + (c - b)(c + b)$ and $p = \dfrac{\zeta^2 q^2 + (c - b)(c + b)}{2\zeta q}$, $\zeta \mid (c - b)(c + b) \implies \zeta^m = (c - b)$, and $q \nmid (c - b)(c + b) \implies q^m = \kappa \implies q \mid \kappa$, hence $q \perp \zeta$. We also know from Lemma 2.3 that at least one or both of $c$ and $b$ are odd, which means that $\kappa$ contains the sum of an odd number (1 or $m$ respectively) of odd terms, and is therefore odd. Hence $q^m$ is odd, and $q$ is odd. Let us assume that $m$ divides $c$ or $b$ (it cannot divide both, from Lemma 2.2), say $b$. From Fermat's Little Theorem [5], if $m \nmid c$, then $c^{m-1} \equiv 1 \mod (m)$. Clearly $\kappa \equiv 1 \mod (m)$. Now let $m \nmid cb$. Then $(c^m - b^m) \mod (m) \equiv (c(c^{m-1}) - b(b^{m-1})) \mod (m) \equiv (c - b) \mod (m) \equiv (c - b)\kappa \mod (m)$. Hence $\kappa = q^m \equiv 1 \mod (m) \implies q \equiv 1 \mod (m)$. □

Equating $LJ$ in Fig. 1 as $c^2 - \alpha^2 = b^2 - (x - \alpha)^2$ leads to a useful identity: $x(2\alpha - x) = c^2 - b^2$. With $\alpha = \dfrac{p}{q}$, $x = \zeta q$ and $\zeta^m = c - b$, we have $2p\zeta = \zeta^2 q^2 + \zeta^m q(c + b)$. From the arguments leading up to (11),

$$q \perp pc. \tag{26}$$

Condition (26) is by definition since $\cos\theta = \dfrac{p}{qc}$ is in its simplest form, and due to Lemmas 2.2 and 2.4.

## 3 Proof of Theorem 2.2

For $n = 3$, (24) becomes

$$- s_3(c, x, \alpha) = 6\alpha x^4 - 12\alpha^2 x^3 + 8\alpha^3 x^2 - 2c^3 x^2 \\ - \sum_{k=2}^{2} \binom{3}{2} c^{2(3-k)} x^{k-1} (x - 2\alpha)^k - 3c^4 x + 6c^4 \alpha,$$

$$- s_3(c, x, \alpha) = 6\alpha x^4 - (12\alpha^2 + 3c^2)x^3 \\ + (8\alpha^3 - 2c^3 + 12c^2\alpha)x^2 - (12c^2\alpha^2 + 3c^4)x + 6c^4\alpha, \quad (27)$$

which we will refer to also as $s_3$. From Theorem 2.3, $s_3$ has two real roots $\rho_3^{\mathbb{R}} = (r_1, r_2) = (x^*, c^2/x^*)$. It also has two complex roots, which from Theorem 2.3 and Corollary 2.3.1 must be both conjugate and complementary, and therefore conjoint. We denote them by $\rho_3^{\mathbb{C}} = (c_1, c_2) = (\eta + i\mu, \eta - i\mu)$. Therefore, $\eta^2 + \mu^2 = c^2$.

For a fourth degree polynomial, the product of the roots is expressed as

$$- s_3(c, x, \alpha) = (x - r_1)(x - r_2)(x - c_1)(x - c_2) = x^4 - (r_1 + r_2 + c_1 + c_2)x^3 \\ + (r_1 r_2 + r_1 c_1 + r_2 c_1 + r_1 c_2 + r_2 c_2 + c_1 c_2)x^2 \\ - (r_1 r_2 c_1 + r_1 r_2 c_2 + r_1 c_1 c_2 + r_2 c_1 c_2)x + r_1 r_2 c_1 c_2. \quad (28)$$

Comparing (27) termwise with (28), we get for the first two bracketed quantities,

$$x^* + c^2/x^* + 2\eta = \frac{12\alpha^2 + 3c^2}{6\alpha} \quad (29)$$

$$2\eta(x^* + c^2/x^*) = \frac{8\alpha^3 - 2c^3 + 12c^2\alpha}{6\alpha} - 2c^2. \quad (30)$$

The remaining two bracketed quantities yield equations that are equivalent to (29), so they are redundant. Now, we denote

$$z_1 = x^* + c^2/x^* \quad (31)$$

$$z_2 = 2\eta. \quad (32)$$

Upon substituting (31) in (27), we get the following quadratic equation:

$$z^2 - \frac{4\alpha^2 + c^2}{2\alpha} z + \frac{4\alpha^3 - c^3}{3\alpha} = 0. \quad (33)$$

Solving (33) leads to

$$z = (z_1, z_2) = \frac{4\alpha^2 + c^2 \pm \sqrt{D}}{4\alpha},$$

$$D = (4\alpha^2 + c^2)^2 - \frac{16\alpha(4\alpha^3 - c^3)}{3} \\ = \frac{48\alpha^4 + 3c^4 + 24\alpha^2c^2 - 64\alpha^4 + 16\alpha c^3}{3} \\ = \frac{3c^4 + 16\alpha c^3 + 24\alpha^2 c^2 - 16\alpha^4}{3}. \quad (34)$$

The real roots of $s_3(c, \alpha, x) = \rho^{\mathbb{R}} = (r_1, r_2)$ are the lengths of the sides of the triangles that represent (3). If $\sqrt{D}$ is irrational, then $(r_1, r_2)$ are irrational. To find out if $\sqrt{D}$ is irrational, we first expand (34) for $\alpha = \frac{p}{q}$, setting $qc = l$.

$$\begin{aligned} D &= \frac{1}{q^2}\sqrt{\frac{3l^4 + 16pl^3 + 24p^2l^2 - 16p^4}{3}} \\ &= \frac{1}{q^2}\sqrt{\frac{(3l-2p)(l+2p)^3}{3}}. \end{aligned} \tag{35}$$

**Lemma 3.1.** *If $p \perp c$ and $c$ is odd, then $(3l - 2p) \perp (l + 2p)$.*

*Proof.* From (26) and the assumption $p \perp c$, we have $l \perp p$. Now assume that $3l - 2p$ and $l + 2p$ have a common prime integer divisor $\zeta_p$. For some positive integers $k_1$ and $k_2$, let

$$\begin{aligned} 3l - 2p &= k_1\zeta_p, \\ l + 2p &= k_2\zeta_p \\ \therefore\ \ 4l &= (k_1 + k_2)\zeta_p. \end{aligned}$$

If $\zeta_p \mid l$, then $\zeta_p \nmid p$ because $l \perp p$, resulting in $\zeta_p \nmid (3l - 2p), (l + 2p)$. Therefore, $\zeta_p \nmid l$. Then $\zeta_p = 4$. But both $3l - 2p$ and $l + 2p$ are odd by the assumption that $c$ is odd, since Lemma 2.4 shows that $l = qc$ is odd. □

**Lemma 3.2.** $D = \frac{1}{q^2}\sqrt{\frac{(3l-2p)(l+2p)^3}{3}}$ *is irrational.*

*Proof.* $D = \frac{1}{q^2}\sqrt{\frac{(3l-2p)(l+2p)^3}{3}} = \frac{l+2p}{q^2}\sqrt{\frac{(3l-2p)(l+2p)}{3}}$. If the assumptions $p \perp c$ and $c$ is odd are true, then from Lemma 3.1, $(3l - 2p) \perp (l + 2p)$ as they do not share a common divisor. Therefore, 3 can divide only one of these expressions. For $D$ to be irrational, one or both of $(3l - 2p)$ and $(l + 2p)$ should be square-free (after the division by 3). Assume $(l + 2p)$ is square-free. If $3 \mid (3l - 2p)$, then $D$ is still irrational due to our assumption. Then 3 must divide $(l + 2p)$ completely, and this can only happen if $l + 2p = 3$. Now $D$ can be rational if $3l - 2p$ is a perfect square. Therefore, the only possibility for $D$ to be rational given these assumptions is:

$$\begin{aligned} l + 2p &= 3 \\ 3l - 2p &= k^2. \end{aligned} \tag{36}$$

Summing up, $4l = 3 + k^2$. From (36), $k$ is odd, since $l$ and $p$ are odd, but $k$ should be such that $3 + k^2$ is divisible by 4. The smallest number for which this is possible is $k = 1$, for which $l = 1$. The next number is $k = 3$, for which $l = 3$, but this means $p = 0$ which is not possible, and $p \leq 0$ for any $k \geq 3$. Therefore, $k = 1$, and $l = qc = 1$. This means $2p = 3 - 1 = 2$, and $p = 1$. However, we know from Section 2 that $\cos\theta = \alpha = \frac{p}{qc} = 1 \implies \theta = 0$, which is only admissible as a degenerate triangle. Therefore, $D$ is irrational given these assumptions.

Now we examine the situation when our assumptions do not hold: that is, $c$ is even, $p$ is not coprime to $c$, and both $(3l - 2p), (l + 2p)$ are not square-free. Then we gather all common factors of $l$ and $p$ into the integer term $\zeta_c$ so that $(3l-2p)(l+2p) = \zeta_c^2(3t-\rho)(t+\rho)$, where $(3t - \rho)$ and $(t+\rho)$ are odd, with positive integers $t \perp \rho$. Note here that $3(3t-\rho)(t+\rho) = (3t+\rho)^2 - 4\rho^2 = k^2$, for integer $k$, must form a primitive Pythagorean triple with primitives $(\zeta, \zeta_\rho)$, where $\rho \mid p = \zeta\zeta_\rho$

is even, $t$ is odd and $l = qc = 4^\iota t$, with $\iota$ some positive integer. In addition, we multiply and divide $D$ by $\sqrt{3}$ such that $D = \frac{(l+2p)\zeta_c}{3q^2}\sqrt{3(3t-\rho)(t+\rho)}$. From arguments following Lemma 3.1, $(3t-\rho) \perp (t+\rho)$. Let any one of $(3t-\rho)$ and $(t+\rho)$ be $3f^2$ and $g^2$, respectively, with $g, f$ odd integers, $g \perp f$. Thus we have $4t = 3f^2 + g^2$. Also $(3t-\rho)(t+\rho) = 3k^2$, with $k$ odd, which leads to $t(3t+2\rho) = 3k^2 + \rho^2$. From [5] (p. 49), we see that all numbers of the form $3i^2 + j^2$, with odd integers $i \perp j$, are divisible by 4, and retain this form after division. Moreover, all odd factors of numbers of this form retain the form. Therefore, we can represent $t = 3d^2 + e^2$, and since this divides $3k^2 + \rho^2$, $3t + \rho = t + 2(t+\rho) = 3i^2 + j^2$. Thus, either $(3d^2 + e^2) + 2(g^2) = 3i^2 + j^2$, or $(3d^2 + e^2) + 2(3f^2) = 3i^2 + j^2$, depending on our choice of assigning $3f^2$ and $g^2$ to $(3t-\rho)$ and $(t+\rho)$. In either case, if $t$ were even and $\rho$ odd, $3d^2 + e^2$ and $3i^2 + j^2$ are divisible by 4, whereas $2(g^2)$ and $2(3f^2)$ are only divisible by 2 and not 4, and the equation cannot have solutions in integers. With $t$ odd and $\rho$ even, $q$ and $t$ are both of the form $u^2 + 3v^2$, with $u, v$ integers. Applying Euler's device to (3) (see [5], p.40), with integers $z, w > 1, z \perp w$, and $c = \frac{4^\iota t}{q}$, we have $2z(z^2 + 3w^2) \equiv (4^\iota(u^2 + 3v^2))^3$. This shows that a smaller integer of the form $u^2 + 3v^2$ may be factored from $c$. This factor can now be multiplied with $q$, to get a smaller $4l' \equiv (u'^2 + 3v'^2)$, $8p' = 8\zeta'\zeta'_\rho = 9v'^2 - u'^2$, from which can be obtained $\zeta' \mid 3v' \pm u'$, and $a = \zeta' q$. Hence a Fermat–Pythagoras polynomial with a rational $D$ (and hence rational roots), representing a smaller integer triangle for $n = 3$, can be derived from the present triangle. As this cannot continue infinitely, $u$ and $v$, hence $l$ and $p$, cannot combine to yield a rational $D$. Lastly, $t = u^2 + 3v^2$ and $\rho = 9v^2 - u^2$ yields an integer $D$, but $t$ and $\rho$ have the same parity, which contradicts our assumptions. Thus $D$ is irrational. $\square$

From (34) and Lemma 3.2, $x^* + c^2/x^*$ is irrational when $c$ is an integer, and hence the roots of (3) cannot be rational numbers. Thus Fermat's Last Theorem for $n = 3$ is proved by the plane trigonometric approach.

A computed example is shown in the supplementary results in the Appendix. Figure 3 displays the computation of the roots. Table 1 shows the values of the roots and their conjugates in accordance with Theorem 2.3. A comparison between explicit calculation of roots using (3) and the analytical result (34) is shown in Figure 4.

# 4 Conclusions

We have generalized the definition of Fermat–Pythagoras polynomials for any positive integer $n > 2$ and explored the properties of their roots. This led to the plane trigonometric proof of the case $n = 3$ of Fermat's Last Theorem, in which we explicitly derived the form of the roots and showed that they are irrational. We believe the approach might offer further geometric and algebraic insight into the problem for other indices.


# Acknowledgements

The author is grateful to Siemens Technology for the opportunity, and to sources of invaluable learning. Special thanks are due to family.

# References


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

[2] Barany, M. J. (2013). Stuck in the Middle: Cauchy's Intermediate Value Theorem and the history of analytic rigor. *Notices of the American Mathematical Society*, 60(10), 1334–1338.

[3] Barbara, R. (2017). 101.01 Fermat's last theorem for $n = 3$ revisited. *The Mathematical Gazette*, 101(550), 90–93.

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

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

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

[7] Heath, T. L. (1925). *The Thirteen Books of Euclid's Elements* (2nd ed.). Dover Publications, New York **1**, 286–287.

[8] De Oliveira, O. R. B. (2012). The fundamental theorem of algebra: From the four basic operations. *The American Mathematical Monthly*, 119, 753–758.

[9] Prabhakar, G. (2021). A plane trigonometric proof for the case $n = 4$ of Fermat's Last Theorem. *Notes on Number Theory and Discrete Mathematics*, 27(4), 154–163.

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

[11] Sastry, S. (2004). *Engineering Mathematics*. PHI Learning.

[12] Wiles, A. (1995). Modular elliptic curves and Fermat's Last Theorem. *Annals of Mathematics*, 141(3), 443—551.

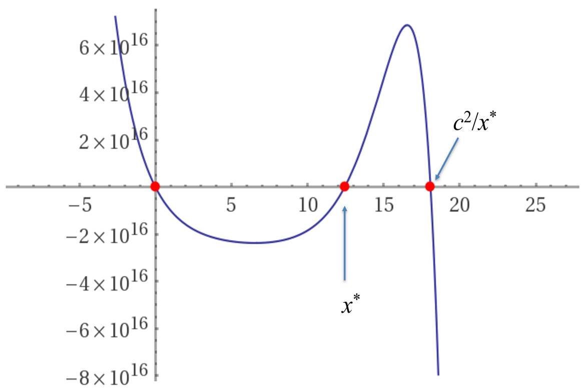
[13] Wolfram Research, Inc., Wolfram—Alpha, Champaign, IL (2024). WolframAlpha ["solve($(c^2 + x(x - 2(\alpha)))^n - (c^n - x^n)^2 = 0$), for $c = 15, \alpha = 7, n = 7$", HTTP Link for Root Plot] (access June 14, 2025).


# Appendix

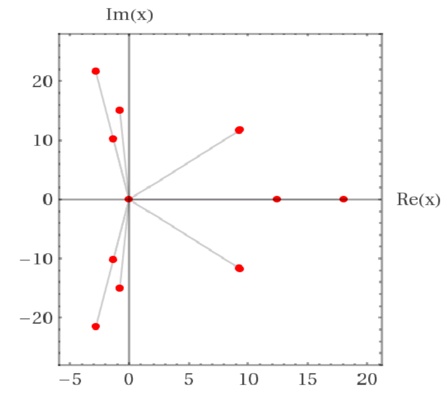
**Computed example.** Roots of $u_7(15, 7, x)$.

A plot of $u_7(15, 7, x)$ is shown in Figure 3(a), and can be expanded as [13]:

$$\begin{aligned} u_7(15,7,x) &= xs_7(15,7,x) \\ &= -x(98x^{12} - 5691x^{11} + 228340x^{10} - 7038185x^9 + 172149054x^8 - 3442681627x^7 \\ &\quad + 56343906554x^6 - 774603366075x^5 + 8715045858750x^4 - 80169326015625x^3 \\ &\quad + 585210445312500x^2 - 3281717373046875x + 12715141113281250). \end{aligned}$$




(a) Plot of $u_7(15, 7, x)$.




(b) Roots of $u_7(15, 7, x)$ in the complex plane.

Figure 3. Polynomial $u_n(c, \alpha, x) = [c^2 + x(x-2\alpha)]^n - [c^n - x^n]^2$ evaluated for $c = 15, \alpha = 7$ and $n = 7$ [13]. This is equivalent to $[q^2c^2 + x(x - 2\alpha)]^n - [q^nc^n - x^n]^2$ with $c = 5, \alpha = p/q$, $p = 7, q = 3$, and $n = 7$.

| **Root** | **Values** | | **Root** | **Values** | | **Product** | **Values** | |
|---|---|---|---|---|---|---|---|---|
| | **Real** | **Complex** | | **Real** | **Complex** | | **Real** | **Complex** |
| $r_1$ | 12.443068 | 0 | $r_2$ | 18.08236 | 0 | $r_1r_2$ | 225 | 0 |
| $c_1^+$ | $-2.8136572$ | $-21.56939602$ | $c_1^-$ | $-1.33798$ | 10.25691 | $c_1^+c_1^-$ | 225 | $8.88178E{-}14$ |
| $c_2^+$ | $-2.8136572$ | 21.56939602 | $c_2^-$ | $-1.33798$ | $-10.2569$ | $c_2^+c_2^-$ | 225 | $-8.88178E{-}14$ |
| $c_3^+$ | $-0.7776268$ | $-14.97982966$ | $c_3^-$ | $-0.77763$ | 14.97983 | $c_3^+c_3^-$ | 225 | 0 |
| $c_4^+$ | 9.3281065 | $-11.69961771$ | $c_4^-$ | 9.37416 | 11.75738 | $c_4^+c_4^-$ | 225 | $7.24754E{-}13$ |
| $c_5^+$ | 9.3281065 | 11.69961771 | $c_5^-$ | 9.37416 | $-11.7574$ | $c_5^+c_5^-$ | 225 | $-7.24754E{-}13$ |

Table 1. Values of roots of $u_7(15, 7, x)$ and their pairwise product (limited by finite (64-bit) precision arithmetic) [13]. The conjoint root is $c_3$.

Verification of (36) by explicit computation (up to the limits of finite (64-bit) precision arithmetic):

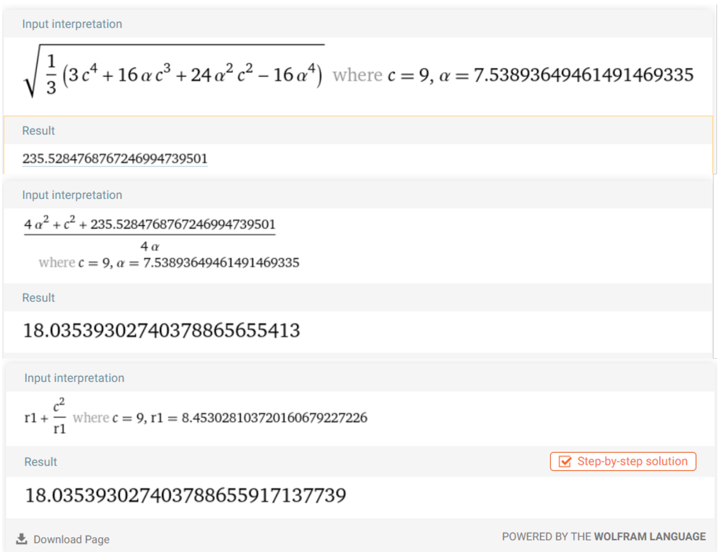



Figure 4. Comparison of roots $r_1 + r_2 = r_1 + c^2/r_1$ of polynomial $-s_3(c, \alpha, x)$ evaluated for $c = 9$, $b = 5$, $\alpha = (c^2 - b^2 + a^2)/(2a)) \approx 7.53893649461491469335$, $r_1 = a \approx 8.4530281037201606792$ computed by (35), and explicitly using $r_1 = (c^3 - b^3)^{1/3}$, $r_2 = c^2/r_1$.