

Application of the Radical Method in Solving Indeterminate Equations (Groups)

Liu Lushi

Longhu Middle School, Chao'an District, Chaozhou City, Guangdong, China, Province

ABSTRACT

Fermat's last theorem was proposed by the 17th-century French mathematician Pierre de Fermat. He asserted that when the integer $n > 2$, there was no positive integer solution for the $x^n + y^n = z^n$ equation.

However, Fermat did not write down his proof, while his other conjectures contributed greatly to mathematics. Therefore, it inspired many mathematicians' interests in this conjecture. Their corresponding work enriched number theory and promoted its development.

In 1995, Wiles proved that the theorem was valid when $n > 2$. However, his process of proof is tediously long. It is said that only a few world-class masters can understand it, which is confusing.

A Perfect cuboid, also known as a perfect box, refers to a cuboid whose edge lengths, diagonals of faces, and body diagonals are all integers. The mathematician Euler once speculated that a perfect rectangle might not exist. No one in the mathematical world has allegedly found a perfect cuboid. Meanwhile, no one has been able to prove that it does not exist.

What's a Hellen triangle? A Hellen triangle is a triangle whose sides and areas are rational numbers.

For thousands of years, triangles and their geometric properties have been studied intensively and thoroughly. With the understanding of Hellen triangles, people have found Hellen triangles with three integer heights and with three integer angle bisectors. However, Hellen triangles with three integer midlines have yet to be found.

After several years of research, the author discovered that the above three problems had commonalities and could be demonstrated using the same method. The same algebraic structure is the key to solving these three problems, such as the equations $y=x^3+ax^2+bx+c$ and $y=(x+3)^3+a(x+3)^2+b(x+3)+c$ are algebraically isomorphic. These two equations represent the same curve and are essentially indistinguishable. The above three problems can be solved with this property easily and concisely.

*Corresponding author

Liu Lushi, Longhu Middle School, Chao'an District, Chaozhou City, Guangdong, China, Province.

Received: April 04, 2024; **Accepted:** April 12, 2024; **Published:** January 04, 2025

Keywords: Fermat's Last Theorem, Perfect Rectangles, Hellen Triangles, Rational Number Solutions, Algebraic Isomorphism

Definition: If the solution sets of two equations (groups) have the same algebraic operation structure based on the equations (groups), the two equations (groups) are called isomorphic equations (groups), and their solution sets are equivalent.

Proof 1 of Fermat's Last Theorem

Fermat's last theorem

Given $x, y, z \in \mathbb{R}^+$, $n \in \mathbb{N}$, when $n \geq 3$, the equation $x^n + y^n = z^n$ has no rational solution.

Proofing

From the equation, it can be obtained

$$(x/z)^n + (y/z)^n = 1 \quad (1)$$

Let $a=x/z$, $b=y/z$, then Equation (1) is transformed into

$$a^n + b^n = 1 \quad (2)$$

When $n \geq 3$, suppose the equation $x^n + y^n = z^n$ has rational solutions, then Equation (2) must also have rational solutions $\{a, b\}$, and any equation that is isomorphic to $()^n + ()^n = 1$ must also have rational solutions. Otherwise, it conflicts with the supposition that Equation (2) has rational solutions. Let $ab=M$, it is easy to know that when a and b are both rational numbers, M must be a rational number. Solve Equation (2), and it can be obtained

$$\begin{cases} a = \sqrt[n]{\frac{1+\sqrt{1-4M^n}}{2}} \\ b = \sqrt[n]{\frac{1-\sqrt{1-4M^n}}{2}} \end{cases} \quad (\text{without loss of generality, always let } a \geq b)$$

If $(1-4M^n)=0$, then $a = \sqrt[n]{\frac{1}{2}}$, $b = \sqrt[n]{\frac{1}{2}}$, which is impossible when $n \geq 3$. Therefore $(1-4M^n) > 0$, and $(1-4M^n)$ must be the square of a rational number. Otherwise, a and b are always irrational numbers, which also conflict with the supposition. Then let $\sqrt{1-4M^n} = c^n$ (3)

(Any positive rational number can be written as then-th power of a positive number). From Equation (3), it can be obtained $(1-4M^n)=0$ must be the square of a rational number. Otherwise, a and b are always irrational numbers, which also conflict with the supposition. Then let $\sqrt[n]{1-4M^n}=c^n$ (3)
(Any positive rational number can be written as then-th power of a positive number). From Equation (3), it can be obtained

$$(c^2)^n + (\sqrt[n]{2^2} M)^n = 1 \quad (4)$$

Since Equation (4) is isomorphic to $()^n + ()^n = 1$, there must be rational number sets

$$\{(c^2)_{Q^+}, (\sqrt[n]{2^2} M)_{Q^+}\} \sim \{a_{Q^+}, b_{Q^+}\} \quad (5)$$

to make Equation (4) have rational solutions when $n \geq 3$. However, when $n \geq 3$, and a and bare both rational numbers, the (c^2) of Equation (4) traverses all rational number sets $\{a_{Q^+}\}$, then there always exists $(\sqrt[n]{2^2} M)$ not belonging to $\{b_{Q^+}\}$, which means that Equation (4) does not have rational solution sets isomorphic to Equation (2). It conflicts with the supposition that Equation (2) has rational solutions.

Therefore, when $n \geq 3$, the equation $x^n + y^n = z^n$ has no rational solution.
QED.

Graphic Solution:

$$\begin{array}{c}
 a^n + b^n = 1 \\
 \text{replaceable} \quad \text{When n is greater than 3,} \\
 \quad \quad \quad \quad \quad \quad \quad \text{If a and b are both rational numbers,} \\
 \quad \quad \quad \quad \quad \quad \quad \text{It is not replaceable on n-th expansion} \\
 (c^2)^n + (\sqrt[n]{2^2} M)^n = 1 \\
 \text{(Because the algebra is isomorphic, it's replaceable)}
 \end{array}$$

Proof 2 of Fermat's Last Theorem

Fermat's last theorem

Given $x, y, z \in R^+$, $n \in N$, when $n \geq 3$, the equation $x^n + y^n = z^n$ has no rational solution.

Proofing

From the equation, it can be obtained

$$(x/z)^n + (y/z)^n = 1 \quad (1)$$

Let $a=x/z$, $b=y/z$, then Equation (1) is transformed into

$$a^n + b^n = 1 \quad (2)$$

When $n \geq 3$, suppose the equation $x^n + y^n = z^n$ has rational solutions, then Equation (2) must also have rational solutions $\{a, b\}$, and any equation that is isomorphic to $()^n + ()^n = 1$ must also have rational solutions. Otherwise, it conflicts with the supposition that Equation (2) has rational solutions. Let $ab=M$, it is easy to know that when a and bare both rational numbers, M must be a rational number. Square the two sides of Equation (2), and it can be obtained

$$\begin{aligned}
 a^{2n} + 2a^n b^n + b^{2n} &= 1 \\
 a^{2n} - 2a^n b^n + b^{2n} &= 1 - 2a^n b^n \\
 (a^n - b^n)^2 &= 1 - 2a^n b^n \quad (3)
 \end{aligned}$$

Extract roots of the two sides of Equation (3) simultaneously, and it can be obtained:

$$\begin{aligned}
 a^n - b^n &= \sqrt{1 - 2a^n b^n} \quad (a \geq b) \\
 a^n &= b^n + \sqrt{1 - 2a^n b^n} \quad (a \geq b) \quad (4)
 \end{aligned}$$

$$\begin{aligned}
 \text{或} \quad b^n - a^n &= \sqrt{1 - 2a^n b^n} \quad (a \leq b) \\
 \text{或} \quad b^n &= a^n + \sqrt{1 - 2a^n b^n} \quad (a \leq b) \quad (5)
 \end{aligned}$$

If $(1 - 2a^n b^n) = 0$, then $1 = \sqrt[n]{2} a = \sqrt[n]{2} b$, which is impossible when $n \geq 3$.

Therefore $(1 - 2a^n b^n) > 0$, and $(1 - 2a^n b^n)$ must be the square of a rational number. Otherwise, a and b are always irrational numbers, which also conflict with the supposition. Then let $\sqrt{1 - 2a^n b^n} = c^n$ (6)

(Any positive rational number can be written as then-th power of a positive number). From Equation (6), it can be obtained

$$(c^2)^n + (\sqrt[n]{2^2} ab)^n = 1 \quad (7)$$

Since Equation (7) is isomorphic to $()^n + ()^n = 1$, there must be rational number sets

$$\{(c^2)_{Q^+}, (\sqrt[n]{2^2} ab)_{Q^+}\} \sim \{a_{Q^+}, b_{Q^+}\} \quad (8)$$

to make Equation (7) have rational solutions when $n \geq 3$. However, when $n \geq 3$, and a and b are both rational numbers, the (c^2) of Equation (7) traverses all rational number sets $\{a_{Q^+}\}$, then there always exists $(\sqrt[n]{2^2} ab)$ not belonging to $\{b_{Q^+}\}$, which means that Equation (7) does not have rational solution sets isomorphic to Equation (2). It conflicts with the supposition that Equation (2) has rational solutions.

Therefore, when $n \geq 3$, the equation $x^n + y^n = z^n$ has no rational solution.
QED.

Graphic Solution:

$$\begin{array}{c}
 a^n + b^n = 1 \\
 \text{replaceable} \quad \text{When n is greater than 3,} \\
 \quad \quad \quad \quad \quad \quad \quad \text{If a and b are both rational numbers,} \\
 \quad \quad \quad \quad \quad \quad \quad \text{It is not replaceable on n-th expansion} \\
 (c^2)^n + (\sqrt[n]{2^2} ab)^n = 1 \\
 \text{(Because the algebra is isomorphic, it's replaceable)}
 \end{array}$$

Proof 3 of Fermat's Last Theorem

Fermat's last theorem: Given $x, y, z \in R^+$, $n \in N$, when $n \geq 3$, the equation $x^n + y^n = z^n$ has no rational solution.

Proofing

From the equation, it can be obtained

$$(x/z)^n + (y/z)^n = 1 \quad (1)$$

Let $a=x/z$, $b=y/z$, then Equation (1) is transformed into

$$a^n + b^n = 1 \quad (2)$$

When $n \geq 3$, suppose the equation $x^n + y^n = z^n$ has rational solutions, then Equation (2) must also have rational solutions $\{a, b\}$, and any equation that is isomorphic to $()^n + ()^n = 1$ must also have rational solutions. Otherwise, it conflicts with the supposition that Equation (2) has rational solutions.

Suppose the following Equation Group ① is tenable.

$$\textcircled{1} \begin{cases} a^n + b^n = 1 & (3) \\ a^n - b^n = c^n & (4) \end{cases}$$

(Any positive rational number can be written as the n-th power of a positive number)

From Equation Group ①, it can be obtained

$$\textcircled{2} \begin{cases} 2a^n = 1 + c^n & (5) \\ 2b^n = 1 - c^n & (6) \end{cases}$$

Multiply equations (5) and (6), it can be obtained

$$2^2 a^n b^n = 1 - c^{2n}$$

That is,

$$(c^2)^n + (\sqrt[n]{2^2 ab})^n = 1 \quad (7)$$

Since Equation (7) is isomorphic to, there must be rational number sets

$$\{(c^2)_{Q+}, (\sqrt[n]{2^2 ab})_{Q+}\} \sim \{a_{Q+}, b_{Q+}\} \quad (8)$$

to make Equation (7) have rational solutions when $n \geq 3$. However, when $n \geq 3$, and a and b are both rational numbers, the (c^2) of Equation (7) traverses all rational number sets $\{a_{Q+}\}$, then there always exists (ab) not belonging to $\{b_{Q+}\}$, which means that Equation (7) does not have rational solution sets isomorphic to Equation (2). It conflicts with the supposition that Equation (2) has rational solutions.

Therefore, when $n \geq 3$, the equation $x^n + y^n = z^n$ has no rational solution. QED.

$$a^n + b^n = 1$$

replaceable

When n is greater than 3,
If a and b are both rational numbers,
It is not replaceable on n -th expansion

Graphic Solution:

$$(c^2)^n + (\sqrt[n]{2^2 ab})^n = 1$$

(Because the algebra is isomorphic, it's replaceable)

There is no Perfect cuboid

Euler great theorem

Given that Equation Group ① is tenable, where $a, b, c, d, l_1, l_2, l_3 \in R^+$, When l_1, l_2 and l_3 are all rational numbers, Equation (4) has no rational solution.

$$\textcircled{1} \begin{cases} a^2 + b^2 = l_1^2 & (1) \\ b^2 + c^2 = l_2^2 & (2) \\ c^2 + a^2 = l_3^2 & (3) \\ a^2 + b^2 + c^2 = d^2 & (4) \end{cases}$$

Proofing

Suppose that Equation (4) has rational solutions when l_1, l_2 and l_3 are all rational numbers. From Equation Group CD, it can be obtained

$$l_1^2 + l_2^2 + l_3^2 = (\sqrt{2} d)^2 \quad (5)$$

Multiply the two sides of Equation (5) by $(abc)^2$, it can be obtained

$$(l_1 abc)^2 + (l_2 abc)^2 + (l_3 abc)^2 = (\sqrt{2} abcd)^2 \quad (6)$$

Multiply the two sides of Equation (4) by $(l_1, l_2, l_3)^2$, it can be obtained

$$(l_1 l_2 l_3 a)^2 + (l_1 l_2 l_3 b)^2 + (l_1 l_2 l_3 c)^2 = (l_1 l_2 l_3 d)^2 \quad (7)$$

Since Equation (4) has rational solutions when l_1, l_2 and l_3 are all rational numbers, Equation (7) must also have rational solutions. Then any equation that is isomorphic to $(\)^2 + (\)^2 + (\)^2 = (\)^2$ must also have rational solutions. Otherwise, it conflicts with the supposition that Equation (7) has rational solutions.

Because Equation (6) is isomorphic to Equation (7), there must exist rational solution sets

$$\{(l_1 abc)_{Q+}, (l_2 abc)_{Q+}, (l_3 abc)_{Q+}, (\sqrt{2} abcd)_{Q+}\} \sim$$

$$\{(l_1 l_2 l_3 a)_{Q+}, (l_1 l_2 l_3 b)_{Q+}, (l_1 l_2 l_3 c)_{Q+}, (l_1 l_2 l_3 d)_{Q+}\}$$

However, the $\{(l_1 abc), (l_2 abc), (l_3 abc)\}$ of Equation (6) traverse

all rational number sets $\{(l_1 l_2 l_3 a)_{Q+}, (l_1 l_2 l_3 b)_{Q+}, (l_1 l_2 l_3 c)_{Q+}\}$, then

there always exists $\{(\sqrt{2} abcd)\}$ not belonging which means that Equation (6) does not have rational solutions isomorphic to Equation (7). It conflicts with the supposition that Equation (7) has rational solutions.

Therefore, Equation (4) has no rational solutions when l_1, l_2 and l_3 are all rational numbers.

It can be deduced from above that there is no Perfect cuboid.

Graphic Solution:

$$(l_1 l_2 l_3 a)^2 + (l_1 l_2 l_3 b)^2 + (l_1 l_2 l_3 c)^2 = (l_1 l_2 l_3 d)^2$$

replaceable

replaceable

replaceable

replaceable

When a, b, c, d, l_1, l_2 and l_3 are all rational numbers, it cannot be permuted on the quadratic extension field.

$$(l_1 abc)^2 + (l_2 abc)^2 + (l_3 abc)^2 = (\sqrt{2} abcd)^2$$

(Because the algebra is isomorphic, it's replaceable)

There is no such thing as a Hellen triangle with all three midlines being integers Hellen Great Theorem

Given that Equation Group ① is tenable, where $a, b, e, m_a, m_b, m_c, S \in R^+$.

When m_a, m_b and m_c are rational numbers simultaneously, Equation (4) has no rational solution.

Proofing

Suppose that Equation (4) has rational solutions when m_a, m_b and m_c are rational numbers simultaneously. It can be obtained from Equation Group ①:

$$\textcircled{1} \begin{cases} 2^2 m_a^2 + a^2 = 2b^2 + 2c^2 & (1) \\ 2^2 m_b^2 + b^2 = 2a^2 + 2c^2 & (2) \\ 2^2 m_c^2 + c^2 = 2a^2 + 2b^2 & (3) \\ 2^4 S^2 + (a^2 + c^2 - b^2)^2 = 2^2 a^2 c^2 & (4) \end{cases}$$

$$3^2S^2 + (m_a^2 + m_c^2 - m_b^2)^2 = 2^2m_a^2m_c^2 \quad (5)$$

Multiply the two sides of Equation (4) by $S^2m_a^4/m_b^4/m_c^4$, then it can be obtained

$$(2Sm_a m_b m_c)^4 + [(a^2 + c^2 - b^2)Sm_a^2 m_b^2 m_c^2]^2 = (2acSm_a^2 m_b^2 m_c^2)^2 \quad (6)$$

Multiply the two sides of Equation (5) by $S^2a^4b^4c^4$, then it can be obtained:

$$(\sqrt{3} Sabc)^4 + [(m_a^2 + m_c^2 - m_b^2)Sa^2b^2c^2]^2 = (2m_a m_c Sa^2b^2c^2)^2 \quad (7)$$

Because Equation (4) has rational solutions when m_a , m_b and m_c are rational numbers simultaneously, there must exist rational solution sets

$$\{(2Sm_a m_b m_c), [(a^2 + c^2 - b^2)Sm_a^2 m_b^2 m_c^2], (2acSm_a^2 m_b^2 m_c^2)\}$$

to make Equation (6) have rational solutions. Then any equation that is isomorphic to $(\quad)^4 + (\quad)^2 = (\quad)^2$ must also have rational solutions. Otherwise, it conflicts with the supposition that Equation (6) has rational solutions. Since Equation (7) is isomorphic to $(\quad)^4 + (\quad)^2 = (\quad)^2$, there must exist rational solution sets

$$\{(\sqrt{3} Sabc)_{Q+}, [(m_a^2 + m_c^2 - m_b^2)Sa^2b^2c^2]_{Q+}, (2m_a m_c Sa^2b^2c^2)_{Q+}\} \\ \sim \{(2Sm_a m_b m_c)_{Q+}, [(a^2 + c^2 - b^2)Sm_a^2 m_b^2 m_c^2]_{Q+}, (2acSm_a^2 m_b^2 m_c^2)_{Q+}\}$$

to make Equation (7) have rational solutions. However, the

$\{[(m_a^2 + m_c^2 - m_b^2)Sa^2b^2c^2], (2m_a m_c Sa^2b^2c^2)\}$ of Equation (7) traverse

all rational number sets $\{[(a^2 + c^2 - b^2)Sm_a^2 m_b^2 m_c^2]_{Q+}, (2acSm_a^2 m_b^2 m_c^2)_{Q+}\}$,

then there always exists $(\sqrt{3} Sabc)$ not belonging to $\{(2Sm_a m_b m_c)_{Q+}\}$, which means that Equation (7) does not have rational solution sets isomorphic to Equation (6). It conflicts with the supposition that Equation (6) has rational solutions.

Therefore, Equation(4) has no rational solutions when m_a , m_b and m_c are rational numbers simultaneously.

As can be seen from the above, there is no Hellen triangle with all three midlines being integers.

Graphic Solution:

