Application of root number method in indefinite equation (group)

Lushi Liu

Abstract

Fermat's great theorem, also known as the "Fermat's last theorem", was proposed by the 17th-century French mathematicians Pierre De Fermat. He asserts that when the integer is $n > 2$, the equation $x^n + y^n = z^n$, about x, y and n, has no positive integer solution.

After all, Fermat did not write down the proof, and his other conjectures contributed much to mathematics, thus inspiring many mathematicians. The relevant work of mathematicians has enriched the content of number theory and promoted the development of number theory.

Although in 1995, Wiles proved that the $n > 2$ theorem holds. But the proof process is lengthy, and it is said that only a few world-class masters can understand it, which is really puzzling.

Perfect cuboid, also known as perfect box, refers to the cube with long edges, face diagonal and body diagonal are integers. Mathematician Euler has speculated that a perfect cuboid may not exist. It is said that no one in mathematics has ever found a perfect cuboid, nor can anyone prove that a perfect cuboid does not exist.

What is the Helen triangle? A Helen triangle is a triangle whose side length and area are both rational numbers.

For thousands of years, triangles have been very thoroughly studied, almost knowing the geometry of triangles. People's understanding of Helen triangle, basically can find three high Helen triangles are integers, three angular bisection lines are integer Helen triangles, but has not found three medians are integer Helen triangles. The author found that the above three problems are all in common, which can be demonstrated by the same-species method. The same algebraic structure is the key to solving these three problems, such as:

The function $\mathrm{y} = x^3 + ax^2 + b^x + \mathrm{c}$ and $y = (x+3)^3 + a(x+3)^3 + b(x+3) + c$ are algebraically isomorphism, and the two functions represent the same curves that are indistinguishable in nature. With this property to solve the above three problems, you can do easy, concise and powerful.

Key words: Fermat's great theorem, perfect cuboid, Helen triangle, rational number solution, algebra isomorphism

Definition: If the solution set of two equations (group) has the same algebraic operation structure based on equations (group), the two equations (group) are called isomorphic equations (group), and the solution set of these two equations (group) is the equivalent solution set.

Fermat's Last Theorem (Proof 1)

Fermat's great theorem: It is known that $x, y, z \in R^{+}$, when the integer is $n \geq 3$, the equation $x^n + y^n = z^n$ has no rational number solution.

Proof: From the equation $x^n + y^n = z^n$ we can be obtained that

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

Let $a = x/z, b = y/z$, then the formula (1) can be transformed into

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

When the integer is $n \geq 3$, let the equation $x^n + y^n = z^n$ has rational number solution, then formula (2) must have rational number solution $\{a, b\}$, then any isomorphic equation $(\ )^n + (\ )^n = 1$ must have a rational solution, otherwise it contradicts the formula (2). Let $ab = M$, it is easy to know that when a and b are both rational numbers, M is a rational number, so solve the equation (2) to get

$$(when\ a \geq b)\begin{cases} a = \sqrt[n]{\dfrac{1+\sqrt{1-4M^n}}{2}} \\ b = \sqrt[n]{\dfrac{1-\sqrt{1-4M^n}}{2}} \end{cases} \quad \text{or} \quad (when\ a \leq b)\begin{cases} a = \sqrt[n]{\dfrac{1-\sqrt{1-4M^n}}{2}} \\ b = \sqrt[n]{\dfrac{1+\sqrt{1-4M^n}}{2}} \end{cases}$$

If $(1-4M^n) = 0$, when the integer is $n \geq 3$,it is impossible $1 = \sqrt[n]{2}a = \sqrt[n]{2}b$. So $(1-4M^n) > 0$ and $(1-4M^n)$ must be the square of a rational number. If $(1-4M^n)$ is not the square of a rational number, and then a and b are always irrational numbers, which will contradict the assumption. Then let

(3) $$\sqrt{1-4M^n} = c^n$$

(Any positive rational number can be written as a positive number raised to the nth power)

It can be obtained from formula (3)

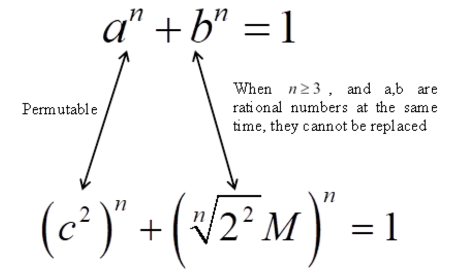
(4) $$\left(c^2\right)^n + \left(\sqrt[n]{2^2}M\right)^n = 1$$

Since equation (4) is isomorphic to the equation $(\ \ )^n + (\ \ )^n = 1$, there must be a set of rational numbers

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

which make formula (4) have a rational solution when $n \geq 3$. But when $n \geq 3$,and a, b are rational number, $\left\{\left(c^2\right)_{Q+}\right\}$ from formula (4) iterates over all rational numbers $\left\{a_{Q+}\right\}$, there has always been $\left(\sqrt[n]{2^2}M\right)_{Q+}$ that does not belong to $\left\{b_{Q+}\right\}$, which means that formula (4) does not exist in the set of rational numbers isomorphic to equation (2), so this contradicts the rational numbers of equation (2).

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



(Permutable because of algebraic isomorphism)

Fermat's Last Theorem (Proof 2)

Fermat's great theorem: It is known that $x, y, z \in R^+$, when the integer is $n \geq 3$, the equation $x^n + y^n = z^n$, has no rational number solution.

Proof: From the equation $x^n + y^n = z^n$ we can be obtained that

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

Let $a = x/z, b = y/z$, then the formula (1) can be transformed into

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

When the integer is $n \geq 3$, let the equation $x^n + y^n = z^n$ has rational number solution, then formula (2) must have rational number solution $\{a, b\}$, then any isomorphic equation $(\ )^n + (\ )^n = 1$ must have a rational solution, otherwise it contradicts the formula (2). Taking the square of both sides of Equation 2, we can get

$$a^{2n} + 2a^n b^n + b^{2n} = 1$$

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

(3) $$(a^n - b^n)^2 = 1 - 2^2 a^n b^n$$

Taking both sides of Equation (3) at the same time, we can get

$$a^n - b^n = \sqrt{1 - 2^2 a^n b^n} \ (a \geq b) \quad \text{or} \quad b^n - a^n = \sqrt{1 - 2^2 a^n b^n} \ (a \leq b)$$

Which is $a^n = b^n + \sqrt{1 - 2^2 a^n b^n}$ $(a \geq b)$ or $b^n = a^n + \sqrt{1 - 2^2 a^n b^n}$ $(a \leq b)$

If $(1 - 2^2 a^n b^n) = 0$, when the integer is $n \geq 3$,it is impossible $1 = \sqrt[n]{2}a = \sqrt[n]{2}b$. So $(1 - 2^2 a^n b^n) > 0$ and $(1 - 2^2 a^n b^n)$ must be the square of a rational number. If $(1 - 2^2 a^n b^n)$ is not the square of a rational number, and then a and b are always irrational numbers , which will contradict the assumption.

Then let

(4) $$\sqrt{1 - 2^2 a^n b^n} = c^n$$

(Any positive rational number can be written as a positive number raised to the nth power)

It can be obtained from formula (4)

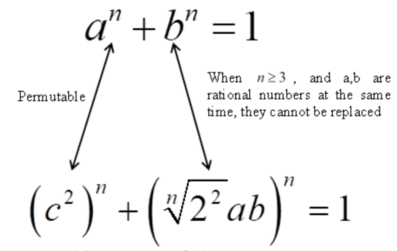
(5) $$\left(c^2\right)^n + \left(\sqrt[n]{2^2}ab\right)^n = 1$$

Since equation (5) is isomorphic to the equation $(\ )^n + (\ )^n = 1$, there must be a set of rational numbers

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

which make formula (5) have a rational solution when $n \geq 3$. But when $n \geq 3$,and a, b are rational number, $\left\{\left(c^2\right)_{Q+}\right\}$ from formula (5) iterates over all rational numbers $\{a_{Q+}\}$, and there has always been $\left(\sqrt[n]{2^2}ab\right)_{Q+}$ that does not belong to $\{b_{Q+}\}$, which means that formula (5) does not exist in the set of rational numbers isomorphic to equation (2), so this contradicts the rational numbers of equation (2).

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



(Permutable because of algebraic isomorphism)

Fermat's Last Theorem (Proof 3)

Fermat's great theorem: It is known that $x, y, z \in R^+$, when the integer is $n \ge 3$, the equation $x^n + y^n = z^n$, has no rational number solution.

Proof: From the equation $x^n + y^n = z^n$ we can be obtained that

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

Let $a = x/z, b = y/z$, then the formula (1) can be transformed into

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

When the integer is $n \ge 3$, let the equation $x^n + y^n = z^n$ has rational number solution, then formula (2) must have rational number solution $\{a, b\}$, then any isomorphic equation $(\ \ )^n + (\ \ )^n = 1$ must have a rational solution, otherwise there is a contradiction with the rational number solution of formula (2).

Without loss of generality, when a>b is set, the system of equations (3) holds

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

From system of equations (3) we can know that

(4) $$\begin{cases} 2a^n = 1 + c^n & ③ \\ 2b^n = 1 - c^n & ④ \end{cases}$$

From ③×④ we can get

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

which is

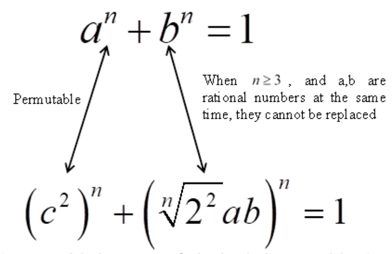
(5) $$(c^2)^n + (2^{2/n} ab)^n = 1$$

Since equation (5) is isomorphic to the equation $(\ \ )^n + (\ \ )^n = 1$, there must be a set of rational numbers

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

which make formula (5) have a rational solution when $n \ge 3$. But when $n \ge 3$,and a, b are rational number, $\left\{ \left(c^2\right)_{Q+} \right\}$ from formula (5) iterates over all rational numbers $\left\{ a_{Q+} \right\}$, and there has always been $\left(\sqrt[n]{2^2} ab\right)_{Q+}$ that does not belong to $\left\{ b_{Q+} \right\}$, which means that formula (5) does not exist in the set of rational numbers isomorphic to equation (2), so this contradicts the rational numbers of equation (2).

So when $n \ge 3$, the equation $x^n + y^n = z^n$ has no rational number solution.



(Permutable because of algebraic isomorphism)

There is no Heron's triangle that three sides are all integers
(Proof 1)

Heron's last theorem: It is known that the system of equations holds, where $a,b,c,m_a,m_b,m_c,S\in R^+$, and when m_a,m_b,m_c are rational numbers at the same time, the equation (4) has no rational number solution.

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

Proof: Assuming that when m_a,m_b,m_c are rational numbers at the same time, the equation (4) has a rational number solution. We can know from equation (4)

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

Multiply both sides of equation (4) by S^2 to get

$$2^4S^4+(a^2-c^2+b^2)^2S^2=2^2a^2c^2S^2$$

Which is

(6) $$(2S)^4+(a^2-c^2+b^2)^2S^2=(2acS)^2$$

Multiply both sides of equation (5) by S^2 to get

$$3^2S^4+(m_a^2+m_c^2-m_b^2)^2S^2=2^2m_a^2m_c^2S^2$$

Which is

(7) $$(\sqrt{3}S)^4+[(m_a^2+m_c^2-m_b^2)S]^2=(2m_am_cS)^2$$

Because when m_a,m_b,m_c are rational numbers at the same time, the equation (4) has a rational number solution, so there must be rational numbers $(2S)$, $[(a^2+c^2-b^2)S]$ and $(2acS)$ which make the formula have a rational number solution, and then any equation isomorphic to $(\ )^4+(\ )^2=(\ )^2$ must also have a rational number solution, otherwise there is a contradiction with that formula (6) has rational number solution.

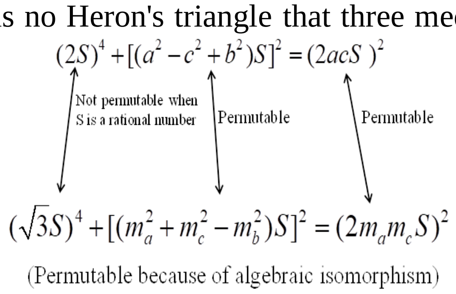
Since equation (7) is isomorphic to the equation $(\ )^4+(\ )^2=(\ )^2$, there must be a set of rational numbers

$$\left\{(\sqrt{3}S)_{Q+},[(m_a^2+m_c^2-m_b^2)S]_{Q+},(2m_am_cS)_{Q+}\right\} \sim \left\{(2S)_{Q+},[(a^2+c^2-b^2)S]_{Q+},(2acS)_{Q+}\right\}$$

which make formula (7) have a rational solution. But when S is a rational number, $\left\{[(m_a^2+m_c^2-m_b^2)S]_{Q+},(2m_am_cS)_{Q+}\right\}$ from formula (7) iterates over all rational numbers $\left\{[(a^2+c^2-b^2)S]_{Q+},(2acS)_{Q+}\right\}$, and there has always been $\left(\sqrt{3}S\right)$ that does not belong to $\left\{(2S)_{Q+}\right\}$, which means that formula (7) does not exist in the set of rational numbers isomorphic to equation (6), so this contradicts with that the equation (6) has rational number solution.

So when m_a,m_b,m_c are rational numbers at the same time, the equation (4) has no rational number solution.

It can be seen from the above that there is no Heron's triangle that three medians are all integers.



There is no Heron's triangle that three sides are all integers
(Proof 2)

Heron's last theorem: It is known that the system of equations holds, where $a,b,c,m_a,m_b,m_c,S \in R^+$, and when m_a,m_b,m_c are rational numbers at the same time, the equation (4) has no rational number solution.

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

Proof: Assuming that when m_a,m_b,m_c are rational numbers at the same time, the equation (4) has a rational number solution. We can know from equation (4)

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

Multiply both sides of equation (4) by S^2 to get

$$2^4 S^4 + (a^2 - c^2 + b^2)^2 S^2 = 2^2 a^2 c^2 S^2$$

Which is

$$(6) \qquad [(m_a^2 + m_c^2 - m_b^2)S]$$

Multiply both sides of equation (5) by S^2 to get

$$3^2 S^4 + (m_a^2 + m_c^2 - m_b^2)^2 S^2 = 2^2 m_a^2 m_c^2 S^2$$

Which is

$$(7) \qquad (\sqrt{3}S)^4 + [(m_a^2 + m_c^2 - m_b^2)S]^2 = (2m_a m_c S)^2$$

Because when m_a,m_b,m_c are rational numbers at the same time, the equation (4) has a rational number solution, so there must be rational numbers $(2S)$, $(2acS)$ and $[(a^2+c^2-b^2)S]$ which make the equation ② have a rational number solution

$$
② \begin{cases}
2^2 m_a^2 + a^2 = 2b^2 + 2c^2 \\
2^2 m_b^2 + b^2 = 2a^2 + 2c^2 \\
2^2 m_c^2 + c^2 = 2a^2 + 2b^2 \\
(2S)^4 + [(a^2 - c^2 + b^2)S]^2 = (2acS\ )^2 & (6)
\end{cases}
$$

Therefore, any system of equations ③ isomorphic to the system of equations must also have a rational number solution, otherwise it contradicts with that the system of equations ② has the rational number solution.

$$
③ \begin{cases}
2^2(\quad)_{m_a}^2 + (\quad)_a^2 = 2(\quad)_b^2 + 2(\quad)_c^2 \\
2^2(\quad)_{m_b}^2 + (\quad)_b^2 = 2(\quad)_a^2 + 2(\quad)_c^2 \\
2^2(\quad)_{m_c}^2 + (\quad)_c^2 = 2(\quad)_a^2 + 2(\quad)_b^2 \\
(\quad)_{kS}^4 + \{[(\quad)_a^2 - (\quad)_c^2 + (\quad)_b^2](\quad)_S\}^2 = (2acS\ )^2
\end{cases}
$$

Suppose the system of equations ③ holds

$$④\quad \begin{cases} 2^2 {A_m}^2 + {m_a}^2 = 2{m_b}^2 + 2{m_c}^2 \\ 2^2 {B_m}^2 + {m_b}^2 = 2{m_a}^2 + 2{m_c}^2 \\ 2^2 {C_m}^2 + {m_c}^2 = 2{m_a}^2 + 2{m_b}^2 \\ (\sqrt{3}S)^4 + [(m_a^2 + m_c^2 - m_b^2)S]^2 = (2m_a m_c S)^2 \qquad (7) \end{cases}$$

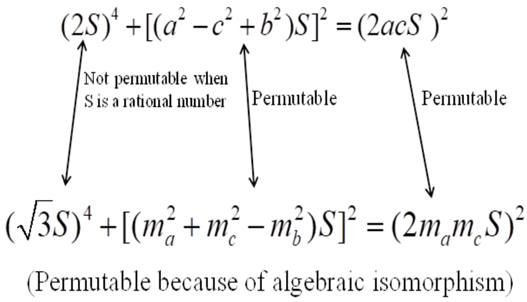
Because equation ④ is a system of equations isomorphic to equation ③, there must be a set of rational numbers

$$\left\{(\sqrt{3}S)_{Q+}, [(m_a^2 + m_c^2 - m_b^2)S]_{Q+}, (2m_a m_c S)_{Q+}\right\} \sim \left\{(2S)_{Q+}, [(a^2 + c^2 - b^2)S]_{Q+}, (2acS)_{Q+}\right\}$$

which make formula (7) have a rational solution. But when S is a rational number, $\left\{[(m_a^2 + m_c^2 - m_b^2)S]_{Q+}, (2m_a m_c S)_{Q+}\right\}$ from formula (7) iterates over all rational numbers $\left\{[(a^2 + c^2 - b^2)S]_{Q+}, (2acS)_{Q+}\right\}$, and there has always been $\left(\sqrt{3}S\right)$ that does not belong to $\left\{(2S)_{Q+}\right\}$, which means that equation ④ does not exist in the set of rational numbers isomorphic to equation ③, so this contradicts with that the equation ② has rational number solution.

So when m_a, m_b, m_c are rational numbers at the same time, the equation (4) has no rational number solution.

It can be seen from the above that there is no Heron's triangle that three medians are all integers.



There is no perfect cuboid (Proof 1)

Euler's Last Theorem: It is known that the system of equations ① is established, where $a,b,c,d,l_1,l_2,l_3 \in R^+$. When l_1,l_2 and l_3 are rational numbers, the equation (4) has no rational number solution.

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

Proof: Assuming that when l_1,l_2 and l_3 are rational numbers at the same time, the equation (4) has a rational number solution. We can know from the system of equations ①

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

Because when l_1,l_2 and l_3 are rational numbers at the same time, the equation (4) has a rational number solution, so any equation isomorphic to $(\ )^2+(\ )^2+(\ )^2=(\ )^2$ must also have a rational number solution, otherwise there is a contradiction with that formula (4) has rational number solution.

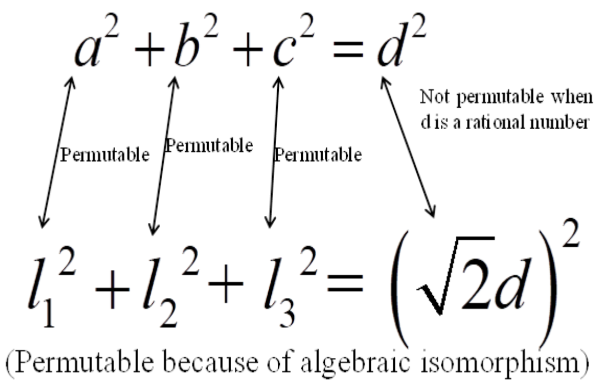
Since equation (7) is isomorphic to the equation $(\ )^2+(\ )^2+(\ )^2=(\ )^2$, there must be a set of rational numbers

$$\left\{(l_1)_{Q+},(l_2)_{Q+},(l_3)_{Q+},\left(\sqrt{2}d\right)_{Q+}\right\} \sim \left\{a_{Q+},b_{Q+},c_{Q+},d_{Q+}\right\}$$

which make formula (5) have a rational solution. But when d is a rational number, $\left\{(l_1)_{Q+},(l_2)_{Q+},(l_3)_{Q+}\right\}$ from formula (5) iterates over all rational numbers $\left\{a_{Q+},b_{Q+},c_{Q+}\right\}$, and there has always been $\left(\sqrt{2}d\right)$ that does not belong to $\left\{d_{Q+}\right\}$, which means that formula (5) does not exist in the set of rational numbers isomorphic to equation (4), so this contradicts with that the equation (4) has rational number solution.

So when l_1,l_2 and l_3 are rational numbers at the same time, the equation (4) has no rational number solution.

It can be seen from the above that a perfect cuboid does not exist.



There is no perfect cuboid (Proof 2)

Euler's Last Theorem: It is known that the system of equations ① is established, where $a,b,c,d,l_1,l_2,l_3 \in R^+$. When l_1,l_2 and l_3 are rational numbers, the equation (4) has no rational number solution.

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

Proof: Assuming that when l_1,l_2 and l_3 are rational numbers at the same time, the equation (4) has a rational number solution. We can know from the system of equations ①

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

Because when l_1,l_2 and l_3 are rational numbers at the same time, the equation (4) has a rational number solution, so equation set ① must have a rational number solution, and then any equation set isomorphic to ② must also have a rational number solution, otherwise there is a contradiction with that formula set ① has rational number solution.

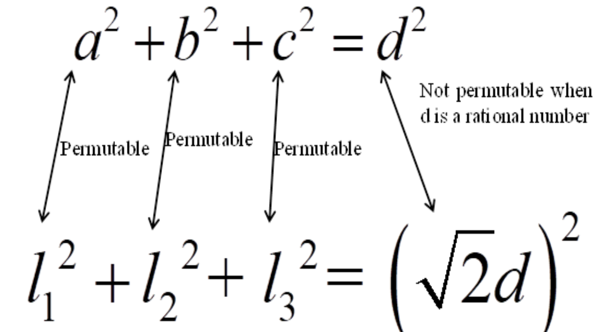
$$
② \begin{cases} (\ )_a^2+(\ )_b^2=(\ )_{l_1}^2 \\ (\ )_b^2+(\ )_c^2=(\ )_{l_2}^2 \\ (\ )_c^2+(\ )_a^2=(\ )_{l_3}^2 \\ (\ )_a^2+(\ )_b^2+(\ )_c^2=(\ )_d^2 \end{cases}
$$

$$
③ \begin{cases} l_1^2+l_2^2=k_1^2 \\ l_2^2+l_3^2=k_2^2 \\ l_3^2+l_1^2=k_3^2 \\ l_1^2+l_2^2+l_3^2=\left(\sqrt{2}d\right)^2 \end{cases}
$$

Let equation set ③ holds, because the system of equations ③ is isomorphic to the equation set ②, so there must be a set of positive rational numbers $\left\{(l_1)_{Q+},(l_2)_{Q+},(l_3)_{Q+},(k_1)_{Q+},(k_2)_{Q+},(k_3)_{Q+},\left(\sqrt{2}d\right)_{Q+}\right\} \sim \left\{a_{Q+},b_{Q+},c_{Q+},(l_1)_{Q+},(l_2)_{Q+},(l_3)_{Q+},d_{Q+}\right\}$ which make formula set ③ have a rational solution that is isomorphic to the equation set ②. But when d is a rational number, $\left\{(l_1)_{Q+},(l_2)_{Q+},(l_3)_{Q+},(k_1)_{Q+},(k_2)_{Q+},(k_3)_{Q+}\right\}$ from formula set ③ iterates over all rational numbers $\left\{a_{Q+},b_{Q+},c_{Q+},(l_1)_{Q+},(l_2)_{Q+},(l_3)_{Q+}\right\}$, and there has always been $\left(\sqrt{2}d\right)$ that does not belong to $\{d_{Q+}\}$, which means that formula set ③ does not exist in the set of rational numbers isomorphic to equation set ②, so this contradicts with that the equation set ① has rational number solution.

So when l_1, l_2 and l_3 are rational numbers at the same time, the equation (4) has no rational number solution.

It can be seen from the above that a perfect cuboid does not exist.



(Permutable because of algebraic isomorphism)

References

The Chinese version of this article has been published on Mathematics Learning and Research, No.34,2021.

Longhu Middle School, Chaoan District, Chaozhou City, Guangdong Province

E-mail address: 4432445l4@qq.com