Classification of Pythagorean triples and reflection on Fermat's last theorem

Kuan Peng titang78@gmail.com
19 July 2025

Abstract: Pythagorean triples are generated with Euclid's formula. But how this formula was derived by or before Euclid is a mystery. We have derived Euclid's formula directly from Pythagorean equation and classified all Pythagorean triples in a 3D table. The equation $X^2 + Y^j = Z^2$ is proven to have infinitely many integer solutions. By comparing Pythagorean equation with Fermat's equation for n=3 we were able to explain why Fermat's equation with n=2 has integer solutions while with n ≥ 3 it has not. We propose an algebraic method to work Fermat's last theorem.

1. Introduction

Fermat's last theorem is one of the most famous problems in mathematics which was conjectured in a spectacular way by Pierre de Fermat. More than three centuries later Andrew Wiles has finally proven it. However, being an algebraic problem Fermat's last theorem should be proved with algebra. Fermat's last theorem states that the Fermat's equation given below :

$$X^n + Y^n = Z^n \qquad (1)$$

does not have integer solution when n ≥ 3.

On the other hand, Fermat's equation with n=2 is the Pythagorean equation shown below :

$$X^2 + Y^2 = Z^2 \qquad (2)$$

which has infinitely many integer solutions. What is the reason that makes Fermat's equation to have integer solutions when n=2 but none when n ≥ 3? For answering this question, let's examine the Pythagorean equation and its integer solutions which are sets of three integers (X, Y, Z) called Pythagorean triples. The integers X, Y and Z are generated with Euclid's formula which is the following three equations:

$$\begin{aligned} X &= a^2 - b^2 \\ Y &= 2ab \\ Z &= a^2 + b^2 \end{aligned} \qquad (3)$$

where *a* and *b* are two positive integers with *a* > *b* > 0. See « Euclid's Elements, Book X, Proposition 29 », https://mathcs.clarku.edu/~djoyce/java/elements/bookX/propX29.html

How this formula was originally derived and how it is related to Pythagorean equation are mysterious. Also, Pythagorean triples seem to have some order, but this order is not well understood.

2. Derivation of the Euclid's formula

For deriving the Euclid's formula, we make the change of variable below in the Pythagorean equation (2) :

$$Z = X + L \quad (4)$$

where L is a positive integer.

The square of Z and $Z^2 - X^2$ are then expressed with X and L:

$$\begin{aligned} Z^2 &= (X + L)^2 \\ &= X^2 + 2XL + L^2 \quad (5) \\ Z^2 - X^2 &= 2XL + L^2 \quad (6) \end{aligned}$$

Combining Pythagorean equation (2) with equation (6) we can express Y^2 with X and L; we divide both sides of equation (7) with L^2 and obtain:

$$\begin{aligned} Y^2 &= Z^2 - X^2 \\ &= 2XL + L^2 \quad (7) \\ \left(\frac{Y}{L}\right)^2 &= 2\frac{X}{L} + 1 \quad (8) \end{aligned}$$

By expressing $\frac{Y}{L}$ as the ratio of two coprime integers a and b, $\frac{Y}{L}$ and $\left(\frac{Y}{L}\right)^2$ are expressed with a and b :

$$\frac{Y}{L} = \frac{a}{b} \quad (9)$$

$$\left(\frac{Y}{L}\right)^2 = \frac{a^2}{b^2} \quad (10)$$

By introducing equation (10) into (8) we express $\frac{X}{L}$ with a and b :

$$\frac{a^2}{b^2} = 2\frac{X}{L} + 1 \quad (11)$$

$$\frac{X}{L} = \frac{a^2 - b^2}{2b^2} \quad (12)$$

In equation (12), X equals the numerator and L the denominator :

$$X = a^2 - b^2 \quad (13)$$

$$L = 2b^2 \quad (14)$$

Using equations (9) and (14) we get the expression of Y:

$$Y = 2ab \quad (15)$$

Using equations (4), (13) and (14) we derive the expression of Z :

$$\begin{aligned} Z &= X + L \\ &= a^2 - b^2 + 2b^2 \quad (16) \\ &= a^2 + b^2 \end{aligned}$$

The equations (13), (15) and (16) are derived from the Pythagorean equation (2) and are the Euclid's formula (3) . The derivation of the Euclid's formula gives us a way to classify all Pythagorean triples in a completely new way.

Note: I have inquired around about the derivation of the Euclid's formula, nobody has been able to explain how it was derived. If this derivation was lost after Euclid, then we have solved a two thousand year mystery.

3. Classification of Pythagorean triples

The parameter L that we used above is the difference between Z and X, see (4):

$$L = Z - X \quad (17)$$

This parameter is the key to classify Pythagorean triples. Equation (14) expresses Z-X with the parameter b :

$$Z - X = 2b^2 \quad (18)$$

which allows X and Z to have many values while keeping Z-X constant. The Pythagorean triples that have the same Z-X make a series in which the value of *b* is constant. So, Pythagorean triples are classified into series with increasing *b*, that is, series of *b*=1, 2, 3, … . Because X is positive, we have *a* > *b*, see (13). In one series the Pythagorean triples are classified with increasing *a* : *a* = *b+1, b+2, b+3*… . For showing concrete examples of these series, the first 5 Pythagorean triples of the first 5 series are shown in Table 1.

b=1 *a*=2,3,4,5,6			*b*=2 *a*=3,4,5,6,7			*b*=3 *a*=4,5,6,7,8			*b*=4 *a*=5,6,7,8,9			*b*=5 *a*=6,7,8,9,10		
Z-X =2			Z-X =8			Z-X =18			Z-X =32			Z-X =50		
3	4	5	5	12	13	7	24	25	9	40	41	11	60	61
8	6	10	12	16	20	16	30	34	20	48	52	24	70	74
15	8	17	21	20	29	27	36	45	33	56	65	39	80	89
24	10	26	32	24	40	40	42	58	48	64	80	56	90	106
35	12	37	45	28	53	55	48	73	65	72	97	75	100	125

Table 1

In addition to classifying Pythagorean triples with constant Z-X, we can also classify them with constant values of Z-Y. Let's express Z-Y and X with *a* and *b* as follow, see (3):

$$\begin{aligned} Z - Y &= a^2 + b^2 - 2ab \\ &= (a - b)^2 \end{aligned} \quad (19)$$

$$\begin{aligned} X &= a^2 - b^2 \\ &= (a + b)(a - b) \end{aligned} \quad (20)$$

We see that X and Z-Y are functions of *a* + *b* and *a* - *b* . So, we pose the variables *c* and *d*:

$$c = a + b \quad (21)$$

$$d = a - b \quad (22)$$

and express *a* and *b* with *c* and *d:*

$$a = \frac{c + d}{2} \quad (23)$$

$$b = \frac{c - d}{2} \quad (24)$$

The expressions of *Y* and *Z* with *c* and *d* are :

$$\begin{aligned} Y &= 2ab \\ &= 2\frac{c + d}{2}\frac{c - d}{2} \\ &= \frac{c^2 - d^2}{2} \end{aligned} \quad (25)$$

$$\begin{aligned} Z &= d^2 + Y \\ &= d^2 + \frac{c^2 - d^2}{2} \\ &= \frac{c^2 + d^2}{2} \end{aligned} \quad (26)$$

Then, the expressions of X, Y and *Z* with *c* and *d* are:

$$\begin{aligned} X &= cd \\ Y &= \frac{c^2 - d^2}{2} \\ Z &= \frac{c^2 + d^2}{2} \end{aligned} \quad (27)$$

Then Z-Y equals:

$$Z - Y = d^2 \quad (28)$$

As Y is positive, we have $c > d$; as Y is integer, $c^2 - d^2$ must be even, see (27):

$$\begin{aligned} c &= a + b \\ &= a - b + 2b \qquad (29) \\ &= d + 2b \end{aligned}$$

Pythagorean triples are classified in series of constant Z-Y, with d =1, 2, 3, … . In each series, Pythagorean triples are classified with increasing c which are $c = d+2\cdot 1, d+2\cdot 2, d+2\cdot 3\ldots$, see (29). The first 5 Pythagorean triples of the first 5 series are shown in Table 2.

d=1 *c*=3,5,7,9,11			*d*=2 *c*=4,6,8,10,12			*d*=3 *c*=5,7,9,11,13			*d*=4 *c*=6,8,10,12,14			*d*=5 *c*=7,9,11,13,15		
Z-Y =1			Z-Y =4			Z-Y =9			Z-Y =16			Z-Y =25		
3	4	5	8	6	10	15	8	17	24	10	26	35	12	37
5	12	13	12	16	20	21	20	29	32	24	40	45	28	53
7	24	25	16	30	34	27	36	45	40	42	58	55	48	73
9	40	41	20	48	52	33	56	65	48	64	80	65	72	97
11	60	61	24	70	74	39	80	89	56	90	106	75	100	125

Table 2

Since c and d are functions of a and b, the Pythagorean triples in Table 2 should equal those in Table 1. By comparing these two tables, we find that the columns of Table 2 equal the lines of Table 1. So, Table 2 is the transposition of Table 1, which in fact arranges Pythagorean triples with constant Z-X along the columns and with constant Z-Y along the lines. We relabel the lines of Table 1 with the values of Z-Y to makes Table 3.

k=1	Z-X = 2			Z-X = 8			Z-X = 18			Z-X = 32			Z-X = 50		
Z-Y = 1	3	4	5	5	12	13	7	24	25	9	40	41	11	60	61
Z-Y = 4	8	6	10	12	16	20	16	30	34	20	48	52	24	70	74
Z-Y = 9	15	8	17	21	20	29	27	36	45	33	56	65	39	80	89
Z-Y = 16	24	10	26	32	24	40	40	42	58	48	64	80	56	90	106
Z-Y = 25	35	12	37	45	28	53	55	48	73	65	72	97	75	100	125

Table 3

Table 3 does not contain all possible Pythagorean triples because if (X_1, Y_1, Z_1) is a Pythagorean triple, the integer triple ($k\cdot X_1$, $k\cdot Y_1$, $k\cdot Z_1$) where k being positive integer, is also a Pythagorean triple. Let's call ($k\cdot X_1$, $k\cdot Y_1$, $k\cdot Z_1$) a multiple Pythagorean triple. Since most multiple Pythagorean triples are not in Table 3, we create the tables of multiple Pythagorean triples by multiplying Table 3 with k.

The Pythagorean triples in Table 3 are not primitive triples, for example, the triples in the diagonal (12, 16, 20), (27, 36, 45), (48, 64, 80), (75, 100, 125) are multiples of (3, 4, 5) while being all in Table 3. We find also multiples of (8, 6, 10) and (5, 12, 13) in Table 3. These multiples show more orders in Pythagorean triples.

So, we call Table 3 the table of basic Pythagorean triples and mark the first cell with k=1 because the multiplier k equals 1. The table that equals Table 3 multiplied by k is called page k. As example, the page k=2 is given in Table 4 .

k=2	Z-X= 4			Z-X= 16			Z-X= 36			Z-X= 64			Z-X= 100		
Z-Y= 2	6	8	10	10	24	26	14	48	50	18	80	82	22	120	122
Z-Y= 8	16	12	20	24	32	40	32	60	68	40	96	104	48	140	148
Z-Y= 18	30	16	34	42	40	58	54	72	90	66	112	130	78	160	178
Z-Y= 32	48	20	52	64	48	80	80	84	116	96	128	160	112	180	212
Z-Y= 50	70	24	74	90	56	106	110	96	146	130	144	194	150	200	250

Table 4

Finally, all possible Pythagorean triples are classified in a three-dimensional table. Along the columns, Z-X are constant, along the lines, Z-Y are constant, in the page k the multiplier k is constant.

For showing the logic of this classification we have plotted in Figure 1 the series of the second column of Table 1, with b=2 and a=3,4,5,6,7. This figure shows four functions :

1. $Z - X = 2b^2$ is the horizontal line.
2. $Y = 2ab$ is the straight increasing line.
3. $X = a^2 - b^2$ and $Z = a^2 + b^2$ are the two parabolas.

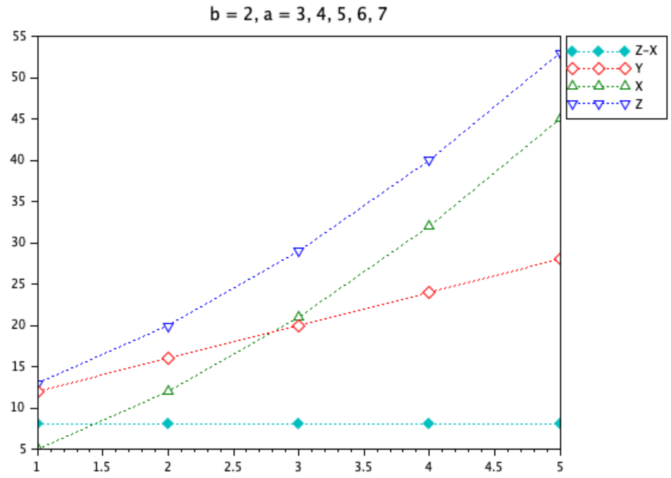

Figure 1

4. Extension of Pythagorean equation

Equation (8) is linear with respect to $\frac{X}{L}$. We take advantage of this linearity to extend Pythagorean equation. Let's apply the change of variables $p = \left(\frac{Y}{L}\right)^2$ to equation (8) and derive its reverse:

$$p = 2\frac{X}{L} + 1 \quad (30)$$
$$\frac{X}{L} = \frac{p-1}{2} \quad (31)$$

Equation (31) implies that the following equation with $j = 1, 2, 3\ldots$ has infinitely many integer solutions :

$$X^2 + Y^j = Z^2 \quad (32)$$

Let's prove this claim. First, we take Pythagorean equation and multiply the term Y^2 with a positive integer G:

$$X^2 + G \cdot Y^2 = Z^2 \quad (33)$$

By using equation (6) we get :

$$\begin{aligned} G \cdot Y^2 &= Z^2 - X^2 \\ &= 2XL + L^2 \end{aligned} \quad (34)$$

We divide both sides of this equation with L^2:

$$G \cdot \left(\frac{Y}{L}\right)^2 = 2\frac{X}{L} + 1 \quad (35)$$

By introducing $\frac{Y}{L} = \frac{a}{b}$ into (35) we get :

$$G\frac{a^2}{b^2} - 1 = 2\frac{X}{L} \quad (36)$$

From (36) we derive the expressions of X and L:

$$\frac{X}{L} = \frac{Ga^2 - b^2}{2b^2} \quad (37)$$
$$\begin{aligned} X &= Ga^2 - b^2 \\ L &= 2b^2 \end{aligned} \quad (38)$$

Since $\frac{Y}{L} = \frac{a}{b}$, we get the expressions of Y :

$$\begin{aligned} Y &= L\frac{a}{b} \\ &= 2ab \end{aligned} \qquad (39)$$

Because Z=X+L, we get the expressions of Z:

$$\begin{aligned} Z &= X + L \\ &= Ga^2 - b^2 + 2b^2 \\ &= Ga^2 + b^2 \end{aligned} \qquad (40)$$

Then, the integer solution of (33) are the following X, Y and Z:

$$\begin{aligned} X &= Ga^2 - b^2 \\ Y &= 2ab \\ Z &= Ga^2 + b^2 \end{aligned} \qquad (41)$$

When G = Y^i with *i*=1, 2, 3… , equation (33) becomes:

$$X^2 + Y^{2+i} = Z^2 \qquad (42)$$

By introducing G = Y^i into (41), we get the expressions of X, Y and Z with *a* and *b* :

$$\begin{aligned} X &= (2ab)^i a^2 - b^2 \\ Y &= 2ab \\ Z &= (2ab)^i a^2 + b^2 \end{aligned} \qquad (43)$$

These X, Y and Z are the infinitely many integer solutions of equation (42) .

The equations $X^2 + Y = Z^2$ and $X^2 + Y^2 = Z^2$ are the equation (32) with *j* = 1, 2 and have infinitely many integer solutions. Equation (42) is the equation (32) with *j*=3, 4, 5… and has infinitely many integer solutions. So, equation (32) have infinitely many integer solutions with *j* = 1, 2, 3… .

For checking the validity of this claim, we have computed four series of X, Y and Z with *j*=3 and *b*=1, 2, 3, 4. These series are solutions of the equation below:

$$X^2 + Y^3 = Z^2 \qquad (44)$$

and are computed as follow :

$$\begin{aligned} Y &= 2ab \\ X &= Ya^2 - b^2 \\ Z &= Ya^2 + b^2 \end{aligned} \qquad (45)$$

and shown in Table 5.

b=1 *a*=2, 3, 4, 5, 6			*b*=2 *a*=3, 4, 5, 6, 7			*b*=3 *a*=4, 5, 6, 7, 8			*b*=4 *a*=5, 6, 7, 8, 9		
X	Y	Z	X	Y	Z	X	Y	Z	X	Y	Z
225	64	289	2809	216	3025	16129	512	16641	62001	1000	63001
10816	1728	12544	63504	4096	67600	246016	8000	254016	739600	13824	753424
140625	13824	154449	549081	27000	576081	1656369	46656	1703025	4198401	74088	4272489
968256	64000	1032256	2930944	110592	3041536	7441984	175616	7617600	16646400	262144	16908544
4558225	216000	4774225	11594025	343000	11937025	25959025	512000	26471025	52780225	729000	53509225

Table 5

In addition, since G can be any positive integer, we claim the Theorem 1:
For G(Y) being any positive integer function of Y, the following equation has infinitely many integer solutions :

$$X^2 + G(Y) \cdot Y^2 = Z^2 \qquad (46)$$

Corollary:
With $(A_n Y^n + A_{n-1} Y^{n-1} + \cdots + A_1 Y + A_0)$ being a polynomial of Y with positive integer coefficients, the following equation has infinitely many integer solutions :

$$X^2 + (A_n Y^n + A_{n-1} Y^{n-1} + \cdots + A_1 Y + A_0) Y^2 = Z^2 \quad (47)$$

5. Fermat's equation with n=3

The study of Pythagorean triples shows that the method with the change of variable Z = X+L is efficient. Let's call this method "Z=X+L method" and apply it to the following Fermat's equation with n=3 and transform it to express Y^3 :

$$X^3 + Y^3 = Z^3 \quad (48)$$

$$\begin{aligned} Y^3 &= Z^3 - X^3 \\ &= (X+L)^3 - X^3 \end{aligned} \quad (49)$$

We divide both sides of (49) with L^3:

$$\left(\frac{Y}{L}\right)^3 = \left(\frac{X}{L} + 1\right)^3 - \left(\frac{X}{L}\right)^3 \quad (50)$$

We develop $\left(\frac{X}{L} + 1\right)^3$ and get the expression of $\left(\frac{Y}{L}\right)^3$:

$$\left(\frac{X}{L} + 1\right)^3 = \left(\frac{X}{L}\right)^3 + 3\left(\frac{X}{L}\right)^2 + 3\left(\frac{X}{L}\right) + 1 \quad (51)$$

$$\begin{aligned} \left(\frac{Y}{L}\right)^3 &= \left(\frac{X}{L} + 1\right)^3 - \left(\frac{X}{L}\right)^3 \\ &= 3\left(\frac{X}{L}\right)^2 + 3\left(\frac{X}{L}\right) + 1 \end{aligned} \quad (52)$$

Let's pose the rational variables *t* and *s* such that :

$$t = \frac{X}{L} \quad (53)$$

$$\begin{aligned} s^3 &= 3\left(\frac{X}{L}\right)^2 + 3\left(\frac{X}{L}\right) + 1 \\ &= 3t^2 + 3t + 1 \end{aligned} \quad (54)$$

If Fermat's equation with n=3 were true, *s* should be rational, see (52) and (54):

$$s = \frac{Y}{L} \quad (55)$$

We transform (54) into the following quadratic equation which we solve :

$$t^2 + t + \frac{1}{3}(1 - s^3) = 0 \quad (56)$$

The solution of this equation is :

$$t = \frac{-1 \pm \sqrt{1 - \frac{4}{3}(1 - s^3)}}{2} \quad (57)$$

The solution $t = \frac{X}{L}$ is rational, so the square root must be rational. Let's denote the square root as *r* and express *t* with *r* :

$$r = \sqrt{\frac{1}{3}(4s^3 - 1)} \quad (58)$$

$$t = \frac{-1 \pm r}{2} \quad (59)$$

The expression of r^2 is:

$$r^2 = \frac{1}{3}(4s^3 - 1) \quad (60)$$

The parentheses is factorized using the formula $a^3 - 1 = (a-1)(a^2 + a + 1)$:

$$\begin{aligned} 4s^3 - 1 &= \left(4^{\frac{1}{3}}s\right)^3 - 1 \\ &= \left(4^{\frac{1}{3}}s - 1\right)\left(4^{\frac{2}{3}}s^2 + 4^{\frac{1}{3}}s + 1\right) \end{aligned} \quad (61)$$

which we introduce into equation (60):

$$r^2 = \frac{1}{3}\left(4^{\frac{1}{3}}s - 1\right)\left(4^{\frac{2}{3}}s^2 + 4^{\frac{1}{3}}s + 1\right) \quad (62)$$

Let's write r^2 as the product $r{\cdot}r'$, with $r' = r$. So r^2 can be written in the form of 4 factorizations :

1) $r = 1 \qquad r' = \frac{1}{3}(4s^3 - 1) \quad (63)$
2) $r = \frac{1}{3} \qquad r' = 4s^3 - 1 \quad (64)$
3) $r = \frac{1}{3}\left(4^{\frac{1}{3}}s - 1\right) \qquad r' = 4^{\frac{2}{3}}s^2 + 4^{\frac{1}{3}}s + 1 \quad (65)$
4) $r = 4^{\frac{1}{3}}s - 1 \qquad r' = \frac{1}{3}\left(4^{\frac{2}{3}}s^2 + 4^{\frac{1}{3}}s + 1\right) \quad (66)$

The first factorization gives $r = 1$. Then, equation (59) gives:

$$t = 0 \text{ or } -1 \quad (67)$$

As $\frac{X}{L}$ is bigger than zero, $t = \frac{X}{L}$ does not equal 0 or -1. So, equation (67) cannot satisfy Fermat's equation.

The second factorization gives $r = \frac{1}{3}$, which makes :

$$\frac{1}{3} = 4s^3 - 1 \quad (68)$$

$$s^3 = \frac{1}{3} \quad (69)$$

$$s = \frac{1}{\sqrt[3]{3}} \quad (70)$$

As $s = \frac{Y}{L}$ is rational, see (55), it does not equal the irrational $\frac{1}{\sqrt[3]{3}}$. So, equation (70) cannot satisfy Fermat's equation.

The third and fourth factorizations, equations (65) and (66), can be analyzed together. These equations give $r = \frac{1}{3}\left(4^{\frac{1}{3}}s - 1\right)$ or $4^{\frac{1}{3}}s - 1$. Since $s = \frac{Y}{L}$ is rational and $4^{\frac{1}{3}}$ irrational, the resulting r is irrational in both cases. So, equations (65) and (66) cannot satisfy Fermat's equation.

In summary, equations (63) gives 0 or -1 to $t = \frac{X}{L}$, (64), (65) and (66) give irrational values to $s = \frac{Y}{L}$ or $t = \frac{X}{L}$. So, the four factorizations are all invalid. Since the expression of r^2 in equation (60) can be factorized only in these 4 ways which are all invalid, we conclude that Fermat's equation with n=3 does not have integer solution and the Fermat's last theorem for n=3 is true.

Of course, this is not the first proof of the case n=3, but it shows that the "Z=X+L method" can be used to work with Fermat' equation.

6. Why does Fermat's equation with n=2 have integer solutions ?

Fermat's last theorem states that Fermat's equation does not have integer solution for all n except 2. Then, proving Fermat's last theorem needs to explain why with n=2 Fermat's equation has infinitely many integer solutions. With the knowledge we have acquired in deriving the Euclid's formula, we now can explain what makes Pythagorean equation so particular within the group of Fermat's equation.

Let's introduce the change of variables $p = \frac{Y}{L}$ and $t = \frac{X}{L}$ into the equation $\left(\frac{Y}{L}\right)^2 = 2\frac{X}{L} + 1$ to obtain (71) and its reverse :

$$p^2 = 2t + 1 \quad (71)$$
$$t = \frac{p^2 - 1}{2} \quad (72)$$

Since $p^2 = \left(\frac{Y}{L}\right)^2$ is a rational number and equation (72) is linear with respect to p^2, $t = \frac{X}{L}$ is rational. Then X, L and Z=X+L are integer. In summary :

1. Integer Y and L give rational p^2 .
2. Because the function $t = \frac{p^2-1}{2}$ in (72) is linear, rational p^2 gives rational $t = \frac{X}{L}$.
3. Rational $t = \frac{X}{L}$ gives integer X, L and Z.

In consequence, Pythagorean triples exist because the function $2\frac{X}{L} + 1$ in (8) is linear with respect to X.

Above, $t = \frac{X}{L}$ is generated with integer Y. In the reverse direction, to generate Y with integer X, we take the square root of equation (8):

$$\frac{Y}{L} = \sqrt{2\frac{X}{L} + 1} \quad (73)$$

The function $2\frac{X}{L} + 1$ with integer X does not necessarily equal the square of a rational number, in which case, Y will be irrational. For example, for X=5, L=2, we have :

$$\begin{aligned} 2\frac{X}{L} + 1 &= 2\frac{5}{2} + 1 \\ &= 6 \end{aligned} \quad (74)$$

In this case, $Y = \sqrt{6}$ is irrational.

How should be the integer X to generate integer Y? Let's introduce $p = \frac{a}{b}$ into (72) to get the resulting t:

$$t = \frac{1}{2}\left(\left(\frac{a}{b}\right)^2 - 1\right) \quad (75)$$

Then we introduce this t into (71) and get:

$$\begin{aligned} p^2 &= \left(\frac{a}{b}\right)^2 + (1 - 1) \\ &= \left(\frac{a}{b}\right)^2 \end{aligned} \quad (76)$$

Here, p^2 equals the square of a rational number because 1 – 1 = 0. So, for an integer X to give integer Y, the value of $t = \frac{X}{L}$ should contain the square of a rational number $\left(\frac{a}{b}\right)^2$ in the form of equation (75). I call the rational number $\frac{1}{2}\left(\left(\frac{a}{b}\right)^2 - 1\right)$ solution "by chance" because it gives the square of a rational number $\left(\frac{a}{b}\right)^2$ while not being the square $\left(\frac{X}{L} + 1\right)^2$.

The solution "by chance" for Pythagorean equation is the following , see (3) and (27):

$$X = cd, \qquad Y = 2ab, \qquad Z = a^2 + b^2 \quad (77)$$

This solution has a particular form, that is, the X and Y are products of integers. For n = 3, we have solved equation (56) which shows that the solution $t = \frac{X}{L}$ cannot be a product of rational numbers, see (57). This is because $\left(\frac{Y}{L}\right)^3$ is nonlinear with respect to X, see (52):

$$\left(\frac{Y}{L}\right)^3 = 3\left(\frac{X}{L}\right)^2 + 3\left(\frac{X}{L}\right) + 1 \qquad (78)$$

So, for whatever integers Y and L, the solution X would be irrational, which implies that solution "by chance" does not exist for Fermat's equation with n=3.

In conclusion, Pythagorean triples exist because the function $2\frac{X}{L} + 1$ is linear with respect to X which allows solutions "by chance" to exist. Fermat's equations with n ≥ 3 is nonlinear with respect to X, which exclude integer solution.

For illustrating the difference between Pythagorean equation and the Fermat's equation with n=3, we have plotted the functions Y^2 and $Z^2 - X^2$ in Figure 2. These functions are computed with L=2. The blue parabola is Y^2, the green straight line is the function $Z^2 - X^2$. We see that $Z^2 - X^2$ is well a linear function. The markers indicate the points of $Z^2 - X^2$ where X are integer and the points of Y^2 where Y are integer. The red horizontal lines indicate where Y^2 equal $Z^2 - X^2$ when X and Y are both integers.

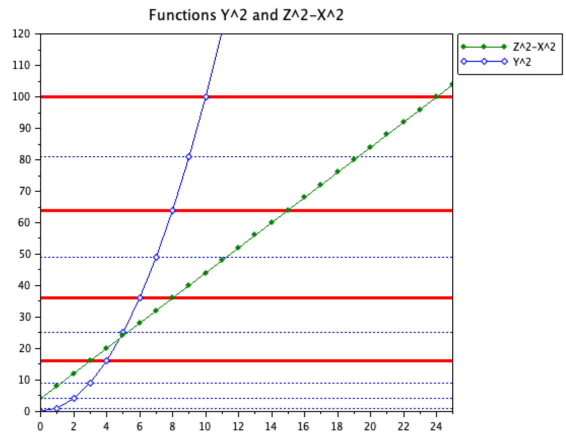

Figure 2

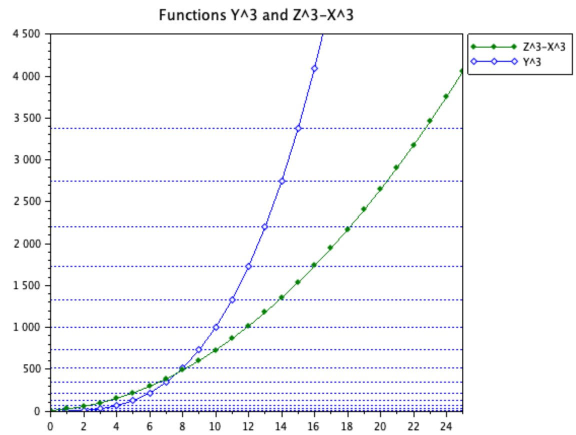

Figure 3

On the other hand, we have plotted in Figure 3 the functions $Y^3$and $Z^3 - X^3$ for the Fermat's equation with n=3. These functions are also computed with L=2. The blue curve is Y^3 and the green curve is $Z^3 - X^3$ which is well nonlinear. The markers indicate the points of Y^3 where Y are integer and the points of $Z^3 - X^3$ where X are integer. The horizontal lines hit all blue markers but none of the green markers, meaning that no integer Y^3 equals integer $Z^3 - X^3$.

Figure 2 and Figure 3 show well that the linear function $Z^2 - X^2$ makes integers X to correspond integers Y, while the nonlinear function $Z^3 - X^3$ cannot.

Figure 4 is another view of the Fermat's equation with n = 3. We have plotted the function $Z^3 - X^3$ with L=6, and two examples of Y^3: the curves of $Y^3 = (X + 2)^3$ and $Y^3 = (X + 4)^3$. These curves intersect with $Z^3 - X^3$ roughly at X=18 and X=12 respectively. The points of intersection correspond to solutions of the Fermat's equation with n = 3. Figure 5 is a close-up at X=18, which shows that the intersection does not occur at X=18 but at an irrational X. So, the solutions X's are real numbers but not integers.

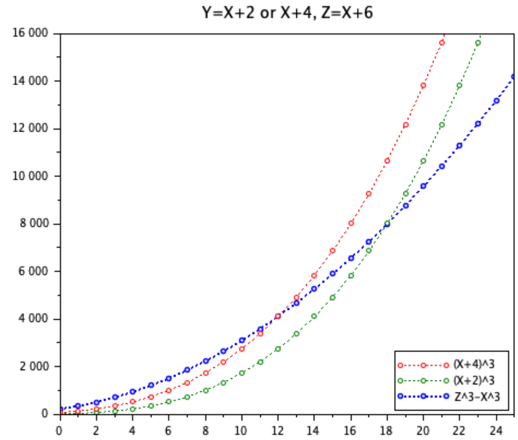

Figure 4

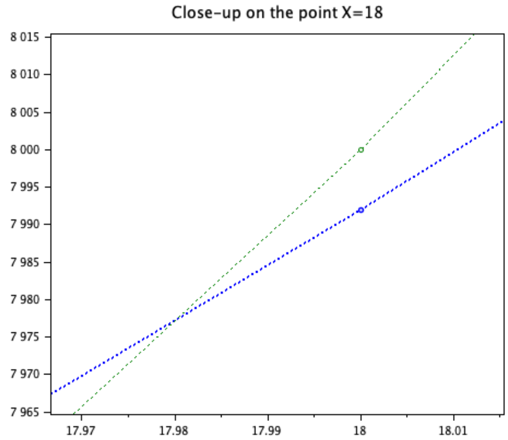

Figure 5

7. Fermat's last theorem with algebra

Below are some of my reflections about proving Fermat's last theorem with the "Z=X+L method". The advantage of the "Z=X+L method" is that it downgrades the degree of the Fermat's equation by one. For example, the degree of the function $Z^2 - X^2$ is two, after applying Z=X+L to Z^2 the function becomes:

$$(X+L)^2 - X^2 = 2XL + L^2 \quad (79)$$

which is of degree one.

Fermat's equation with n ≥ 3 is :

$$X^n + Y^n = Z^n \qquad (80)$$

to which we apply the change of variable Z=X+L to express Y^n with X and L :

$$\begin{aligned} Y^n &= Z^n - X^n \\ &= (X+L)^n - X^n \end{aligned} \qquad (81)$$

We develop $(X+L)^n$ with binomial theorem:

$$(X+L)^n = X^n + nX^{n-1}L + \binom{n}{2}X^{n-2}L^2 + \cdots + \binom{n}{n-1}XL^{n-1} + L^n \quad (82)$$

Then, the polynomial expression of $Z^n - X^n$ is :

$$\begin{aligned} Z^n - X^n &= (X+L)^n - X^n \\ &= nX^{n-1}L + \binom{n}{2}X^{n-2}L^2 + \cdots + \binom{n}{n-1}XL^{n-1} + L^n \end{aligned} \qquad (83)$$

of which the degree is n-1 instead of n.

a) Polynomial analysis

•

For proving Fermat's last theorem, we have to show that $Z^n - X^n$ equals the n^{th} power of an integer number. Let's take an arbitrary integer and express it as X+K. The binomial expansion of $(X+K)^n$ is:

$$(X+K)^n = X^n + nX^{n-1}K + \binom{n}{2}X^{n-2}K^2 + \cdots + \binom{n}{n-1}XK^{n-1} + K^n \qquad (84)$$

Comparing this polynomial with the polynomial of $Z^n - X^n$ given in (83), we find that (83) lacks the term X^n . So, $Z^n - X^n$ could not equal $(X+K)^n$. Let Y=X+K, then we have $Z^n - X^n \neq Y^n$ and then:

$$X^n + Y^n \neq Z^n \quad (85)$$

This seems to demonstrate Fermat's last theorem. However, there still is a possibility that, like with Pythagorean equation, $Z^n - X^n$ equals $(X+K)^n$ "by chance" for particular values of L and K. For excluding this possibility, we use the method of proof by contradiction and suppose that L and K satisfies the following equation "by chance":

$$(X+L)^n - X^n = (X+K)^n \quad (86)$$

Because $X^n > 0$, we have:

$$(X+L)^n > (X+K)^n \quad (87)$$

Then, L is bigger than K:

$$L > K \quad (88)$$

We choose that :

$$K > 0 \quad (89)$$

So, the integer K must be within the interval [1, L-1]:

$$1 \leq K \leq L-1 \quad (90)$$

Since L > K, L can be expressed as L=K+J which we introduce into (83):

$$Z^n - X^n = nX^{n-1}(K+J) + \binom{n}{2}X^{n-2}(K+J)^2 + \cdots + \binom{n}{n-1}X(K+J)^{n-1} + (K+J)^n \quad (91)$$

If we develop all $(K+J)^i$ and rearrange all the terms, we will get the following equation:

$$Z^n - X^n = F(X,K,J,n) + nX^{n-1}K + \binom{n}{2}X^{n-2}K^2 + \cdots + \binom{n}{n-1}XK^{n-1} + K^n \quad (92)$$

where $F(X,K,J,n)$ is a very complex expression.

Because we suppose that equation (86) is true, the function in (83) should equal that in (84) and then :

$$F(X,K,J,n) = X^n \quad (93)$$

Because $F(X,K,J,n)$ is very complex, it is very hard to prove (93) wrong and thus, to exclude solution "by chance" with polynomial analysis only.

-

Let's see equation (86) from another angle. The left hand side of (86) is the expression of $(X+L)^n - X^n$ given in (83). The right hand side is the n^{th} power of Y, Y^n. Then equation (86) can be written as:

$$nX^{n-1}L + \binom{n}{2}X^{n-2}L^2 + \cdots + \binom{n}{n-1}XL^{n-1} + L^n = Y^n \quad (94)$$

As Y^n is the n^{th} power of an integer while the left hand side is not, the solution X of this equation is surely irrational. For example, the third degree Fermat's equation with L=1 is :

$$(X+1)^3 - X^3 = Y^3 \quad (95)$$

The function $(X+1)^3 - X^3$ equals:

$$f(X) = 3X^2 + 3X + 1 \quad (96)$$

For X=1, 2, 3, 4, 5 , the value of *f(X)* are shown in the second line of the following Table :

X	1	2	3	4	5
f(X)	7	19	37	61	91

Table 6

Because none of 7,19,37,61,91 are third power of an integer, the values of Y in the following equations are irrational :

$$\begin{aligned} Y &= \sqrt[3]{7} \\ Y &= \sqrt[3]{19} \\ Y &= \sqrt[3]{37} \quad (97) \\ Y &= \sqrt[3]{61} \\ Y &= \sqrt[3]{91} \end{aligned}$$

This indicate that for equation (94), if X is an integer, Y should be irrational and vice versa. This example shows that proving the solution X is irrational for all *n* and Y is equivalent to proving Fermat's last theorem.

b) Rational number analysis

Fermat's equation has three variables: X, Y and Z. We can reduce the number of variables to two by dividing equation (86) with X^n :

$$\frac{(X+K)^n}{X^n} = \frac{(X+L)^n - X^n}{X^n} \quad (98)$$

We introduce the following change of variable into (98):

$$\alpha = \frac{K}{X}, \qquad \beta = \frac{L}{X} \quad (99)$$

and equation (98) becomes :

$$(1+\alpha)^n = (1+\beta)^n - 1 \quad (100)$$

The binomial expansion of $(1+\alpha)^n$ is:

$$(1+\alpha)^n = 1 + n\alpha + \binom{n}{2}\alpha^2 + \cdots + \binom{n}{n-1}\alpha^{n-1} + \alpha^n \quad (101)$$

The binomial expansion of $(1+\beta)^n$ is:

$$(1+\beta)^n = 1 + n\beta + \binom{n}{2}\beta^2 + \cdots + \binom{n}{n-1}\beta^{n-1} + \beta^n \quad (102)$$

We name the right hand side expression of (100) as the function $f(\beta)$:

$$\begin{aligned} f(\beta) &= (1+\beta)^n - 1 \\ &= n\beta + \binom{n}{2}\beta^2 + \cdots + \binom{n}{n-1}\beta^{n-1} + \beta^n \end{aligned} \quad (103)$$

Compared with the binomial expansion of $(1+\alpha)^n$ in (101), the function $f(\beta)$ lacks the first term which is 1. So, $f(\beta)$ does not equal $(1+\alpha)^n$. Since $1+\alpha$ is an arbitrary rational number, $f(\beta)$ would not equal any rational number to the power n, which indicates that equations (98), (86) and (80) could be wrong. However, we have to exclude the possibility of solution "by chance". For doing so, we make the change of variable $\beta=\gamma+\delta$ in equation (103):

$$f(\beta) = n(\gamma+\delta) + \binom{n}{2}(\gamma+\delta)^2 + \cdots + \binom{n}{n-1}(\gamma+\delta)^{n-1} + (\gamma+\delta)^n \quad (104)$$

If we develop all $(\gamma+\delta)^i$ and rearrange all the terms, we get the following equation:

$$f(\beta) = g(\gamma,\delta,n) + n\gamma + \binom{n}{2}\gamma^2 + \cdots + \binom{n}{n-1}\gamma^{n-1} + \gamma^n \quad (105)$$

For $f(\beta)$ to equal a rational number to the power n, that is, $f(\beta) = (1+\gamma)^n$, the term $g(\gamma,\delta,n)$ should equal 1:

$$g(\gamma,\delta,n) = 1 \quad (106)$$

I think that proving $g(\gamma,\delta,n) = 1$ wrong is very hard, even impossible.

c) Multidimensional space analysis

Let's introduce the binomial expansions of $(1+\alpha)^n$ and $(1+\beta)^n$ into (100) which then becomes:

$$1 + n\alpha + \binom{n}{2}\alpha^2 + \cdots + \binom{n}{n-1}\alpha^{n-1} + \alpha^n = n\beta + \binom{n}{2}\beta^2 + \cdots + \binom{n}{n-1}\beta^{n-1} + \beta^n \quad (107)$$

We gather all the terms on the left hand side and rearrange all the terms as below:

$$1 + n(\alpha-\beta) + \binom{n}{2}(\alpha^2-\beta^2) + \cdots + \binom{n}{n-1}(\alpha^{n-1}-\beta^{n-1}) + (\alpha^n-\beta^n) = 0 \quad (108)$$

We write (108) in the form of matrix equation :

$$\begin{bmatrix} 1 & n & \binom{n}{2} & \cdots & \binom{n}{n-1} & 1 \end{bmatrix} \begin{bmatrix} 1 \\ \alpha-\beta \\ \alpha^2-\beta^2 \\ \cdots \\ \alpha^{n-1}-\beta^{n-1} \\ \alpha^n-\beta^n \end{bmatrix} = 0 \quad (109)$$

We define the two vectors $\boldsymbol{U}$ and $\boldsymbol{V}$ as follow :

$$\boldsymbol{U} = \left[1, n, \binom{n}{2}, \dots, \binom{n}{n-1}, 1\right] \quad (110)$$

$$\boldsymbol{V} = \begin{bmatrix} 1 \\ \alpha - \beta \\ \alpha^2 - \beta^2 \\ \dots \\ \alpha^{n-1} - \beta^{n-1} \\ \alpha^n - \beta^n \end{bmatrix} \quad (111)$$

Then, equation (109) is simply the following dot product :

$$\boldsymbol{U} \cdot \boldsymbol{V} = 0 \quad (112)$$

The vector $\boldsymbol{V}$ is the solution of equation (112). This equation has integer solution because we know a trivial solution of (112) which correspond to:

$$(1-1)^n = 0 \quad (113)$$

We develop $(1-1)^n$ with binomial theorem and write it in matrix form:

$$\begin{aligned} (1-1)^n &= 1 + n(-1) + \binom{n}{2}(-1)^2 + \dots + \binom{n}{n-1}(-1)^{n-1} + (-1)^n \\ &= \begin{bmatrix} 1 & n & \binom{n}{2} & \cdots & \binom{n}{n-1} & 1 \end{bmatrix} \begin{bmatrix} 1 \\ -1 \\ 1 \\ \dots \\ (-1)^{n-1} \\ (-1)^n \end{bmatrix} \quad (114) \\ &= \boldsymbol{U} \cdot \boldsymbol{V}_0 \end{aligned}$$

where the vector $\boldsymbol{V_0}$ is :

$$\boldsymbol{V}_0 = \begin{bmatrix} 1 \\ -1 \\ 1 \\ \dots \\ (-1)^{n-1} \\ (-1)^n \end{bmatrix} \quad (115)$$

Because $(1-1)^n = 0$, the dot product $\boldsymbol{U} \cdot \boldsymbol{V}_0$ equals 0:

$$\boldsymbol{U} \cdot \boldsymbol{V}_0 = 0 \quad (116)$$

So, $\boldsymbol{V_0}$ is an integer solution of equation (112).

In fact, the dot product $\boldsymbol{U} \cdot \boldsymbol{V_0} = 0$ means that the vector $\boldsymbol{V_0}$ is orthogonal to $\boldsymbol{U}$. Let's compare the components of $\boldsymbol{V}$ with those of $\boldsymbol{V_0}$. Equation (111) shows that the components of $\boldsymbol{V}$ are:

$$1, \alpha - \beta, \alpha^2 - \beta^2, \cdots, \alpha^{n-1} - \beta^{n-1}, \alpha^n - \beta^n \quad (117)$$

which have all the same sign except the first 1, while those of $\boldsymbol{V_0}$ are alternately positive 1 and negative 1. Because the signs of the components of $\boldsymbol{V_0}$ and $\boldsymbol{V}$ do not match, $\boldsymbol{V}$ does not equal $\boldsymbol{V_0}$:

$$\begin{bmatrix} 1 \\ \alpha - \beta \\ \alpha^2 - \beta^2 \\ \dots \\ \alpha^{n-1} - \beta^{n-1} \\ \alpha^n - \beta^n \end{bmatrix} \neq \begin{bmatrix} 1 \\ -1 \\ 1 \\ \dots \\ (-1)^{n-1} \\ (-1)^n \end{bmatrix} \quad (118)$$

$$\boldsymbol{V} \neq \boldsymbol{V}_0 \quad (119)$$

However, this inequality does not prove that $\boldsymbol{U} \cdot \boldsymbol{V} \neq 0$ because there are many vectors that are orthogonal to $\boldsymbol{U}$. For showing that equation (109) is wrong we have to show that the vector $\boldsymbol{V}$ is not orthogonal to $\boldsymbol{U}$.

The vectors $\boldsymbol{U}$ and $\boldsymbol{V}$ have n+1 components, so they are objects of a space with n+1 dimensions. In this space there is a subspace that is orthogonal to $\boldsymbol{U}$. All the vectors that are orthogonal to $\boldsymbol{U}$ belong to this subspace and are defined by the following equation:

$$\boldsymbol{U}\cdot\boldsymbol{W} = 0 \quad (120)$$

where $\boldsymbol{W}$ being an arbitrary vector orthogonal to $\boldsymbol{U}$ and member of the subspace .

This subspace has n dimensions, so the vector $\boldsymbol{W}$ can be expressed as a linear combination of a set of n independent vectors $\boldsymbol{v}_1$, $\boldsymbol{v}_2$, …, $\boldsymbol{v}_{n-1}$, $\boldsymbol{v}_n$:

$$\boldsymbol{W} = b_1\boldsymbol{v}_1 + b_2\boldsymbol{v}_2 + \cdots + b_{n-1}\boldsymbol{v}_{n-1} + b_n\boldsymbol{v}_n \quad (121)$$

We set that all the vectors $\boldsymbol{v}_i$ with i=1, 2, 3, 4, … , n are orthogonal to $\boldsymbol{U}$ such that the dot product $\boldsymbol{U}\cdot\boldsymbol{W}$ equal zero:

$$\boldsymbol{U}\cdot\boldsymbol{v}_i = 0 \quad (122)$$

The vectors $\boldsymbol{v}_i$ are constructed one by one. Let's construct the first vector $\boldsymbol{v}_1$ as follow:

$$\boldsymbol{v}_1 = \begin{bmatrix} 1 \\ e_1^1 \\ e_1^2 \\ \cdots \\ e_1^{n-1} \\ e_1^n \end{bmatrix} = \begin{bmatrix} 1 \\ -\frac{1}{n}\left(1+0+\binom{n}{2}+\cdots+\binom{n}{n-1}+1\right) \\ 1 \\ \cdots \\ 1 \\ 1 \end{bmatrix} \quad (123)$$

We check that $\boldsymbol{v}_1$ is really orthogonal to $\boldsymbol{U}$ by verifying that $\boldsymbol{U}\cdot\boldsymbol{v}_1$=0, see (110):

$$\boldsymbol{U}\cdot\boldsymbol{v}_1 = 1 - n\frac{1}{n}\left(1+0+\binom{n}{2}+\cdots+\binom{n}{n-1}+1\right) + \binom{n}{2} + \cdots + \binom{n}{n-1} + 1 \\ = 0 \quad (124)$$

Then, we construct the other vectors $\boldsymbol{v}_i$ in the same way. The vectors $\boldsymbol{v}_i$ are defined with their components e_i^j:

$$\boldsymbol{v}_i = \begin{bmatrix} 1 \\ e_i^1 \\ e_i^2 \\ \cdots \\ e_i^{n-1} \\ e_i^n \end{bmatrix} \quad (125)$$

with i=1, 2, 3, 4, … , n.

We write the components of $\boldsymbol{U}$ as follow :

$$a_0 = 1, a_1 = n, a_2 = \binom{n}{2}, \dots a_{n-1} = \binom{n}{n-1}, a_n = 1 \quad (126)$$

Then, the i^{th} component of the i^{th} vector $\boldsymbol{v}_i$ equals:

$$e_i^i = -\frac{\sum a_j - a_i}{a_i} \quad (127)$$

with j=0, 1, 2, 3, 4, … , n.

The other components of $\boldsymbol{v}_i$ equal 1:

$$e_i^j = 1, \text{except } j = i \quad (128)$$

This way, all the vectors $\boldsymbol{v}_i$ are constructed and are expressed as follow :

$$\boldsymbol{v}_1 = \begin{bmatrix} 1 \\ -\frac{\sum a_j - a_1}{a_1} \\ 1 \\ \cdots \\ 1 \\ 1 \end{bmatrix}, \boldsymbol{v}_2 = \begin{bmatrix} 1 \\ 1 \\ -\frac{\sum a_j - a_2}{a_2} \\ \cdots \\ 1 \\ 1 \end{bmatrix}, \cdots, \boldsymbol{v}_{n-1} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ \cdots \\ -\frac{\sum a_j - a_{n-1}}{a_{n-1}} \\ 1 \end{bmatrix}, \boldsymbol{v}_n = \begin{bmatrix} 1 \\ 1 \\ 1 \\ \cdots \\ 1 \\ -\frac{\sum a_j - a_n}{a_n} \end{bmatrix} \quad (129)$$

By introducing (129) into (121) we get the general expression of $\boldsymbol{W}$:

$$\boldsymbol{W} = \begin{bmatrix} b_1 + b_2 + \cdots + b_{n-1} + b_n \\ -b_1 \frac{\sum a_j - a_1}{a_1} + b_2 + \cdots + b_{n-1} + b_n \\ b_1 - b_2 \frac{\sum a_j - a_2}{a_2} + \cdots + b_{n-1} + b_n \\ \cdots \\ b_1 + b_2 + \cdots - b_{n-1} \frac{\sum a_j - a_{n-1}}{a_{n-1}} + b_n \\ b_1 + b_2 + \cdots + b_{n-1} - b_n \frac{\sum a_j - a_n}{a_n} \end{bmatrix} \quad (130)$$

If a vector $\boldsymbol{V_s}$ is in the subspace orthogonal to $\boldsymbol{U}$, we can derive the coefficients b_i that give the corresponding $\boldsymbol{W}$=$\boldsymbol{V_s}$ by solving the equation below:

$$\begin{bmatrix} b_1 + b_2 + \cdots + b_{n-1} + b_n \\ -b_1 \frac{\sum a_j - a_1}{a_1} + b_2 + \cdots + b_{n-1} + b_n \\ b_1 - b_2 \frac{\sum a_j - a_2}{a_2} + \cdots + b_{n-1} + b_n \\ \cdots \\ b_1 + b_2 + \cdots - b_{n-1} \frac{\sum a_j - a_{n-1}}{a_{n-1}} + b_n \\ b_1 + b_2 + \cdots + b_{n-1} - b_n \frac{\sum a_j - a_n}{a_n} \end{bmatrix} = \boldsymbol{V}_s \quad (131)$$

For example, the coefficients b_i for the vector $\boldsymbol{V_0}$ defined in (115) is the solution of the following equation:

$$\begin{bmatrix} -b_1 \frac{\sum a_j - a_1}{a_1} + b_2 + \cdots + b_{n-1} + b_n \\ b_1 - b_2 \frac{\sum a_j - a_2}{a_2} + \cdots + b_{n-1} + b_n \\ \cdots \\ b_1 + b_2 + \cdots - b_{n-1} \frac{\sum a_j - a_{n-1}}{a_{n-1}} + b_n \\ b_1 + b_2 + \cdots + b_{n-1} - b_n \frac{\sum a_j - a_n}{a_n} \end{bmatrix} = \begin{bmatrix} -1 \\ 1 \\ \cdots \\ (-1)^{n-1} \\ (-1)^n \end{bmatrix} \quad (132)$$

We notice that the first line of equation (130) is not present in (132). This is because equation (130) has n+1 lines while the number of the unknown b_i is n. For the coefficients b_i to satisfy equation (130), the first element of the resulting $\boldsymbol{W}$ must equal that of $\boldsymbol{V_0}$, that is :

$$b_1 + b_2 + \cdots + b_{n-1} + b_n = 1 \quad (133)$$

For checking the validity of (130), we compute three examples of $\boldsymbol{V_0}$ by solving the equation (132) with n=3, 4 and 5 . The solutions for these examples are the coefficients b_i, i=1, 2, 3, 4, 5, shown in Table 7.

n=3	n=4	n=5
b_1= 0.750	b_1= 0.5	b_1= 0.313
b_2=0	b_2=0	b_2=0
b_3=0.25	b_3=0.5	b_3=0.625
	b_4=0	b_4=0
		b_5=0.063
$b_1 + b_2 + b_3$= 1	$b_1 + b_2 + b_3 + b_4 = 1$	$b_1 + b_2 + b_3 + b_4 + b_5 = 1$

Table 7

The last line of Table 7 shows that the resulting b_i respect the equation (133). So, these examples of $\boldsymbol{W}$ equal well the vector $\boldsymbol{V_0}$ for n=3, 4 and 5.

Now, let's see if the vectors $\boldsymbol{V}$ defined by (111) can be expressed using equation (121). For doing so, we compute three examples of $\boldsymbol{V}_s$ by solving the equation (131) with n=3, 4 and 5 and $\alpha = \frac{4}{7}$, $\beta = \frac{5}{7}$. The corresponding coefficients b_i are solutions of the following equation:

$$\begin{bmatrix} -b_1 \frac{\sum a_j - a_1}{a_1} + b_2 + \cdots + b_{n-1} + b_n \\ b_1 - b_2 \frac{\sum a_j - a_2}{a_2} + \cdots + b_{n-1} + b_n \\ \cdots \\ b_1 + b_2 + \cdots - b_{n-1} \frac{\sum a_j - a_{n-1}}{a_{n-1}} + b_n \\ b_1 + b_2 + \cdots + b_{n-1} - b_n \frac{\sum a_j - a_n}{a_n} \end{bmatrix} = \begin{bmatrix} \alpha - \beta \\ \alpha^2 - \beta^2 \\ \cdots \\ \alpha^{n-1} - \beta^{n-1} \\ \alpha^n - \beta^n \end{bmatrix} \quad (134)$$

The resulting b_i are shown in Table 8.

n=3		n=4		n=5	
Components of $\boldsymbol{V}_3$	b_i for $\boldsymbol{W}_3$,	Components of $\boldsymbol{V}_4$	b_i for $\boldsymbol{W}_4$	Components of $\boldsymbol{V}_5$	b_i for $\boldsymbol{W}_5$
$\alpha - \beta = -0.143$	b_1=-0.488	$\alpha - \beta = -0.143$	b_1=-0.67	$\alpha - \beta = -0.143$	b_1=-0.838
$\alpha^2 - \beta^2 = -0.184$	b_2=-0.503	$\alpha^2 - \beta^2 = -0.184$	b_2=-1.021	$\alpha^2 - \beta^2 = -0.184$	b_2=-1.69
$\alpha^3 - \beta^3 = -0.178$	b_3=-0.167	$\alpha^3 - \beta^3 = -0.178$	b_3=-0.679	$\alpha^3 - \beta^3 = -0.178$	b_3=-1.688
		$\alpha^4 - \beta^4 = -0.154$	b_4=-0.168	$\alpha^4 - \beta^4 = -0.154$	b_4=-0.84
				$\alpha^5 - \beta^5 = -0.125$	b_5=-0.167
$b_1 + b_2 + b_3$= -1.157		$b_1 + b_2 + b_3 + b_4$ = -2.539		$b_1 + b_2 + b_3 + b_4 + b_5$ = -5.223	

Table 8

The last line of Table 8 shows that equation (133) is not satisfied by the solutions because the first components of $\boldsymbol{W}_3$, $\boldsymbol{W}_4$ and $\boldsymbol{W}_5$ are -1.157, -2.539 and -5.223, see the last line of Table 8, while those of $\boldsymbol{V}_3$, $\boldsymbol{V}_4$ and $\boldsymbol{V}_5$ are all 1:

$$\boldsymbol{W}_3 = \begin{bmatrix} -1.157 \\ \alpha - \beta \\ \alpha^2 - \beta^2 \\ \alpha^3 - \beta^3 \end{bmatrix}, \boldsymbol{V}_3 = \begin{bmatrix} 1 \\ \alpha - \beta \\ \alpha^2 - \beta^2 \\ \alpha^3 - \beta^3 \end{bmatrix} \Rightarrow \boldsymbol{W_3} \neq \boldsymbol{V_3} \quad (135)$$

$$\boldsymbol{W}_4 = \begin{bmatrix} -2.539 \\ \alpha - \beta \\ \alpha^2 - \beta^2 \\ \alpha^3 - \beta^3 \\ \alpha^4 - \beta^4 \end{bmatrix}, \boldsymbol{V}_4 = \begin{bmatrix} 1 \\ \alpha - \beta \\ \alpha^2 - \beta^2 \\ \alpha^3 - \beta^3 \\ \alpha^4 - \beta^4 \end{bmatrix} \Rightarrow \boldsymbol{W}_4 \neq \boldsymbol{V}_4 \quad (136)$$

$$\boldsymbol{W}_5 = \begin{bmatrix} -5.223 \\ \alpha - \beta \\ \alpha^2 - \beta^2 \\ \alpha^3 - \beta^3 \\ \alpha^4 - \beta^4 \\ \alpha^5 - \beta^5 \end{bmatrix}, \boldsymbol{V}_5 = \begin{bmatrix} 1 \\ \alpha - \beta \\ \alpha^2 - \beta^2 \\ \alpha^3 - \beta^3 \\ \alpha^4 - \beta^4 \\ \alpha^5 - \beta^5 \end{bmatrix} \Rightarrow \boldsymbol{W}_5 \neq \boldsymbol{V}_5 \quad (137)$$

Because $\boldsymbol{U} \cdot \boldsymbol{W}_3 = 0$, $\boldsymbol{U} \cdot \boldsymbol{W}_4 = 0$ and $\boldsymbol{U} \cdot \boldsymbol{W}_5 = 0$, but $\boldsymbol{W}_3 \neq \boldsymbol{V}_3$, $\boldsymbol{W}_4 \neq \boldsymbol{V}_4$ and $\boldsymbol{W}_5 \neq \boldsymbol{V}_5$, then $\boldsymbol{U} \cdot \boldsymbol{V}_3 \neq 0$, $\boldsymbol{U} \cdot \boldsymbol{V}_4 \neq 0$ and $\boldsymbol{U} \cdot \boldsymbol{V}_5 \neq 0$ and the vectors $\boldsymbol{V}_3$, $\boldsymbol{V}_4$ and $\boldsymbol{V}_5$ are not orthogonal to $\boldsymbol{U}$.

These examples indicate that the vectors $\boldsymbol{V}$ defined with α and β in (111) could be not orthogonal to $\boldsymbol{U}$. This is the first indicator that the vectors $\boldsymbol{V}$ would not satisfy Fermat's equation.

Secondly, the number 1 to n components of $\boldsymbol{V}$ are all negative because $\alpha < \beta$, see (99), while those of $\boldsymbol{W}$ would have different sign. This is the second indicator that vectors $\boldsymbol{V}$ would not satisfy Fermat's equation. If we could prove either of these two indicators, we would have proven Fermat's last theorem.

For giving a visual sense of the orthogonality between the vectors $\boldsymbol{W}$ and $\boldsymbol{U}$, I have drawn the case of a 3D vector $\boldsymbol{U}$ in Figure 6 . All the components of $\boldsymbol{U}$ are positive. The subspace orthogonal to $\boldsymbol{U}$ is the plane, all vectors belonging to the plane are vectors $\boldsymbol{W}$ and are orthogonal to $\boldsymbol{U}$.

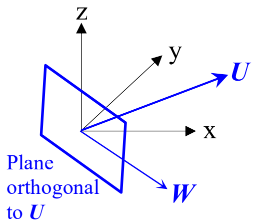

Figure 6

In the 3D space the components of the vector $\boldsymbol{V}$ defined with α and β are $1, \alpha-\beta, \alpha^2-\beta^2$. Suppose that these α and β do not correspond a solution "by chance", then the vector $\boldsymbol{W}$ corresponding to $\alpha-\beta, \alpha^2-\beta^2$ has its first component different than 1 and the vectors $\boldsymbol{V}$ are not orthogonal to $\boldsymbol{U}$, see the last line of Table 8. Figure 6 is a visualization of the equations (110) and (114) and shows a geometrical sense of Fermat's equation.

For the general case with n ≥ 3, because $\boldsymbol{W}$ is a linear combination of $\boldsymbol{v}_1$, $\boldsymbol{v}_2$, …, $\boldsymbol{v}_{n-1}$, $\boldsymbol{v}_n$, I think that proving equations (112) wrong would be much easier than proving equations (93) and (106) wrong . Because $\boldsymbol{W}$ and $\boldsymbol{U}$ are in a space with n+1 dimensions, the N-complex number system that I proposed in « N-complex number, N-dimensional polar coordinate and 4D Klein bottle with 4-complex number » https://pengkuanonmaths.blogspot.com/2024/06/n-complex-number-n-dimensional-polar.html could be useful to the demonstration.

In consequence, the proof of Fermat's last theorem with algebra could be within reach with multidimensional space analysis. However, I'm not able to prove it now. So, I hope that someone more competent than me could carry this proof out or even could take advantage of my analysis to solve other mathematical problems.

d) Where is the condition n=2?

In this chapter we have studied Fermat's last theorem with n ≥ 3 without the need of the condition n ≠ 2. This could mean that the above analyses would be valid for n=2, which would contradict Pythagorean equation. How can we solve this contradiction? Let's recall that in the section "Why does Fermat's equation with n=2 have integer solutions" we have explained that solutions to Pythagorean equation cannot be in the form $(X+K)^2$. In the same way, we have shown that with n ≥ 3 the function (83) cannot be in the form $(X+K)^n$. So, the analyses about binomial expansion apply to Pythagorean equation too.

On the other hand, solutions "by chance" exist for Pythagorean equation because it is linear with respect to X. But with n ≥ 3, the function $(X+L)^n-X^n$ is nonlinear with respect to X. So, the analysis for the case n ≥ 3 about solutions "by chance" do not apply to Pythagorean equation.

In consequence, the proof of Fermat's last theorem with algebra contains two parts:

- The function $(X+L)^n-X^n$ cannot be transformed into the form $(X+K)^n$, for n=2, 3, 4, 5… . This part applies to Pythagorean equation.
- Fermat's equation for n ≥ 3 does not have solution "by chance" because it is nonlinear with respect to X, while Pythagorean equation is linear with respect to X. This part concerns only the case for n ≥ 3.

In conclusion, there is no contradiction with Pythagorean equation because the first part is valid for Pythagorean equation, and the second part does not concern Pythagorean equation.

8. Discussion

In this article we have used the "Z=X+L method" which has allowed us to derive Euclid's formula directly from Pythagorean equation. This derivation shows that Euclid's formula and Pythagorean equation are two equivalent formulations of the same thing. I do not know if the derivation of Euclid's formula were known.

We have classified all Pythagorean triples in a 3D table. The lines of this table are series of Pythagorean triples with the same gap Z-Y, the columns are series with the same gap Z-X and the pages are 2D tables with the same multiplier k.

We have extended the Pythagorean equation and proven that the equations $X^2 + G \cdot Y^2 = Z^2$ where G being any positive integer, have infinitely many integer solutions.

We have proven Fermat's last theorem for n=3 with a new method by solving the Fermat's equation with n=3 and have shown that all the solutions of this equation contain irrational number.

We have explained why Pythagorean equation has integer solutions although being a Fermat's equation. So, the real exception of Pythagorean equation within the group of Fermat's equations is that Pythagorean equation has solutions "by chance". This is a new understanding about Fermat's equation.

Fermat's last theorem being an algebraic problem, it would be better to prove it using algebra. We have analyzed Fermat's equation with the "Z=X+L method" which is an algebraic method, although we have not proven the theorem .

Letter to readers

In this article, I have presented several results from my work. For example:

1. Derivation of the Euclid's formula
2. Classification of Pythagorean triples
3. Why does Fermat's equation with n=2 have integer solutions ?

These results are arranged in a logical order: Result 2 follows from Result 1, Result 3 builds on Results 1 and 2, and so on. However, this is not the order in which these ideas originally came to me during my research. I believe the sequence in which ideas emerge reveals something about how the mind works in the process of discovery. Additionally, I have learned some valuable lessons through this work, and I would like to share these insights with you.

At first, I set out to prove Fermat's Last Theorem using algebra—an attempt in which I ultimately failed. I'm well aware that some of the most brilliant mathematicians in history tried and did not succeed, and that taking on such a challenge might make me seem pretentious. Still, I wanted to give it a try. So, my first idea was this bold ambition: to prove Fermat's Last Theorem using algebra.

In 2015, I had already written an article titled «On Fermat's last theorem» https://pengkuanonmaths.blogspot.com/2015/07/on-fermats-last-theorem.html. Although it was ultimately a failed attempt, I received a very insightful comment from a reader: "Where is n=2?" This simple question got me thinking: "Why does Fermat's equation have integer solutions when n=2?" That remark became the true inspiration for writing this article. I would like to give credit to the reader, but unfortunately, I cannot identify who he was or which discussion forum his comment appeared on.

In exploring the question "Why does Fermat's equation have integer solutions when n=2?" I pursued many ideas—most of them unsuccessful—and produced numerous formulas along the way. Eventually, I stumbled upon the following equations for a special case:

$$\begin{aligned} X &= L(1+2I) \\ Y &= 2L(I+I^2) \\ Z &= 2L(I+I^2)+L = Y+L \end{aligned} \qquad (138)$$

I noticed that the equation Z=Y+L implies the gap between Y and Z can remain constant even as their values vary. This observation led me to suspect that I was touching on the inherent order within Pythagorean triples.

To solve the Pythagorean equation, I had the idea to introduce a change of variables: $\frac{Y}{L}=\frac{a}{b}$. At first, this substitution seemed meaningless, but I applied it to the equation $\left(\frac{Y}{L}\right)^2=2\frac{X}{L}+1$ (see (8)). To my surprise, this led directly to Euclid's formula and ultimately to a classification of Pythagorean triples.

In summary, the natural order in which the ideas developed was as follows:

1. A bold ambition: to prove Fermat's Last Theorem using algebra.
2. Posing the question: "Why does Fermat's equation have integer solutions when n=2?"
3. Accidentally discovering the hidden structure of Pythagorean triples.
4. Deriving Euclid's formula.
5. Classifying Pythagorean triples.
6. Answering the original question: "Why does Fermat's equation have integer solutions when n=2?"

The natural order of ideas reveals that research rarely follows a straight, linear path—one that would neatly proceed as: Result 1, Result 2, Result 3, and so on, leading to the final result. Instead, ideas often emerge in a zigzagging, unpredictable way. Typically, you begin by setting a final objective, then propose an idea that might help achieve it. This initial idea is often more of an intuition than a logical deduction. In the effort to prove your main objective—and to validate the initial idea itself—you are compelled to develop other intermediate ideas along the way. It is through this back-and-forth process that your thoughts evolve and eventually mature into a coherent and well-structured demonstration.

Through this work, I've learned some valuable lessons. The first is the importance of daring to take on seemingly impossible challenges. Many people shy away from topics considered unsolvable by mainstream experts, fearing they might waste their time or appear foolish. For instance, I failed to prove Fermat's Last

Theorem using algebra. However, had I not attempted it, I would never have arrived at the unexpected and meaningful results: the derivation of Euclid's formula, the classification of Pythagorean triples, and the explanation of why Fermat's equation has integer solutions when n=2. In this sense, setting bold objectives—even those that seem out of reach—can open the door to real progress.

The second lesson is that discoveries are often made by accident. My primary goal was to prove Fermat's Last Theorem. But in the process of pursuing that objective, I stumbled upon mathematical patterns and laws I hadn't anticipated. If no one had been searching for a classification of Pythagorean triples or a derivation of Euclid's formula, these results might never have been uncovered—except by chance. This experience taught me the importance of paying close attention to even the smallest unexpected outcomes and being curious about what they might reveal. Unintended results can often lead to meaningful breakthroughs. In this way, surprise can become a path to success.

The third lesson is perseverance. I spent more than nine months pursuing Fermat's Last Theorem through trial and error. Equation (138) emerged on February 4, 2025—four months after I had started this work. Had I given up earlier, I would have gained nothing. The trial-and-error method involves proposing a potentially promising idea, testing its validity, and—when it turns out to be wrong, as it often does—replacing it with another. This cycle is repeated over and over. A failed idea is not a failure, but the closure of an incorrect path, bringing you one step closer to the right one. Moreover, it is often during this process that unexpected and valuable outcomes emerge. Thus, the long and sometimes frustrating process of trial and error is not wasted effort—it is a path to discovery, including results you never initially set out to find.

In the section "Fermat's Last Theorem with Algebra," I mentioned that the system of N-dimensional complex numbers I proposed in my earlier work, «N-complex number, N-dimensional polar coordinate and 4D Klein bottle with 4-complex number»
https://pengkuanonmaths.blogspot.com/2024/06/n-complex-number-n-dimensional-polar.html ,
could potentially be used to prove Fermat's Last Theorem. Interestingly, this mathematical system was itself an unintended outcome of my research on 'Oumuamua, described in « Trajectory of 'Oumuamua and wandering Sun, alien asteroids and comets detected by SOHO »
https://pengkuanonphysics.blogspot.com/2023/04/trajectory-of-oumuamua-and-wandering.html.

'Oumuamua was the first observed interstellar object, passing by the Sun in 2017. Its trajectory had been theoretically predicted and precisely tracked, yet its final observed position deviated from predictions by about 40,000 kilometers. This discrepancy—interpreted as an unexpected "acceleration"—sparked numerous speculations about its nature and origin.

In that article, I explained that during the observation period, time had passed and the Sun had moved approximately 82,400 kilometers due to the gravitational attraction of Jupiter. If this motion of the Sun had been taken into account in the calculation of 'Oumuamua's trajectory, the predicted final position would have been about 37,000 kilometers farther than initially estimated—explaining most of the 40,000-kilometer discrepancy.

I mention 'Oumuamua because, just a few days ago—on July 1, 2025—a new interstellar object, designated 3I/ATLAS, was discovered. As with 'Oumuamua, astronomers will now predict its trajectory and monitor its motion closely. However, if the Sun's motion is not included in these calculations, they may once again observe a discrepancy between the predicted and actual positions. Depending on the relative positions of Jupiter and the Sun at this time, the gap could appear as either an "acceleration" or a "slowing down."

We now await the conclusion of 3I/ATLAS's observation period. The size and nature of any gap between prediction and observation will serve as a test of my hypothesis: that the Sun's motion, influenced by the gravity of the planets, must be included in trajectory models. A match would lend support to this explanation and cast further doubt on alternative theories—such as the outgassing hypothesis proposed for 'Oumuamua, which lacked observational evidence and remains highly improbable.

I have not submitted this article to any academic journal because I believe it would likely be rejected. In fact, my previous submissions have all been declined. For example, «Extending complex number to spaces with 3, 4 or any number of dimensions» was rejected, as was « Trajectory of Oumuamua and wandering Sun, alien asteroids and comets detected by SOHO». It would be unfortunate if ideas such as the classification of Pythagorean triples and the derivation of Euclid's formula failed to reach the mathematical community. For this reason, I have chosen to publish my work online independently, in the hope that interested readers will share it with others or build upon it in their own research.

Additionally, I would like to make a request to readers who are experienced in editing Wikipedia. I would be very grateful if you could consider adding the derivation of Euclid's formula and the classification of Pythagorean triples to the Wikipedia page on "Pythagorean triple" https://en.wikipedia.org/wiki/Pythagorean_triple, as these contributions represent new mathematical insights. Contributing this knowledge to a platform like Wikipedia would not only help preserve it for future generations, but also give the satisfaction of enriching a global resource—offering lasting value to curious minds around the world.