A Short and Plain Proof of Fermat's Last Theorem

[Jae Yul Lee and Yul Jin Lee]

Abstract

In this paper, we show the Pythagorean triples and a short and plain Fermat's Last Theorem proof. Fermat's Last Theorem asserts what there do not exist none-zero integers, X, Y and Z such that $X^n + Y^n = Z^n$, where $n > 2$. The Theorem was first stated by Fermat in the early 1600s. He claimed what he had found a short proof, but left no evidence of what it was. Finding a proof became the most famous unsolved problem in the mathematics until Andrew Wiles, in the late 1990s, found one. The original version of his proof was about 200 pages long, and so the question remains if a much shorter proof exists.

1. Preface

The Pythagorean triples are the positive integer solutions to the Pythagorean Theorem, $X^2 + Y^2 = Z^2$.

The Fermat's Last Theorem states what $X^n + Y^n = Z^n$ has no none-zero integer solutions for X, Y and Z when $n > 2$. This theorem means what $X^n + Y^n = Z^n$ cannot have the positive integer solutions. Because we can get $W^n + U^n = V^n$ from $(-U)^n + V^n = W^n$ in the odd n.

Without loss of generality, we assume what X, Y and Z are relatively prime, i.e., $(X, Y) = 1$, $(Y, Z) = 1$ and $(X, Z) = 1$. Because we can get $X^n + Y^n = Z^n$ from $U^n + V^n = W^n$, $U = QX$, $V = QY$, $(QX)^n + (QY)^n = W^n$ and $W/Q = Z$ in relatively prime, X, Y and Z.

2. Introduction

Let $A = Z - Y$, $B = Z - X$ and $X + B = Y + A = Z$ in the Diophantine equation, $X^n + Y^n = Z^n$.

....

Key Words and Phrases

$X^n = \{(2ab)^{1/2} + a\}^2$, $Y^n = \{(2ab)^{1/2} + b\}^2$ and $Z^n = \{(2ab)^{1/2} + a + b\}^2$.
$X = 2cd + c^2$, $Y = 2cd + 2d^2$ and $Z = 2cd + c^2 + 2d^2$.
Pythagorean triples cannot be the mth power numbers like x^m, y^m and z^m.

MSC : 11D41 Fermat's equation.

Then $X - A = Y - B = Z - A - B = X + Y - Z$. Here, assume what X, Y and Z are the positive integers and relatively prime, then A and B are also the positive integers and relatively prime.

Let

$$\begin{aligned} G &= (X-A)/(AB)^{1/n} = (Y-B)/(AB)^{1/n} \\ &= (Z-A-B)/(AB)^{1/n} = (X+Y-Z)/(AB)^{1/n}. \end{aligned}$$

Then

$$\begin{aligned} X &= G(AB)^{1/n} + A, \\ Y &= G(AB)^{1/n} + B, \\ Z &= G(AB)^{1/n} + A + B \end{aligned}$$

and

$$X + Y - Z = G(AB)^{1/n}.$$

Therefore,

$$\{G(AB)^{1/n} + A\}^n + \{G(AB)^{1/n} + B\}^n = \{G(AB)^{1/n} + A + B\}^n.$$

Let $\{G(AB)+A\}+\{G(AB)+B\} = \{G(AB)+A+B\}$ when $n = 1$. Then $G(AB) = 0$ and $G = 0$.

Therefore,
$X = A$, $Y = B$, $Z = A + B$ and $X + Y - Z = 0$ in the odd $n = 1$.

3. $X^n + Y^n = Z^n$ cannot have the positive integer solutions in the odd $n > 2$

Let $a = Z^{n/2} - Y^{n/2}$ and $b = Z^{n/2} - X^{n/2}$ in $(X^{n/2})^2 + (Y^{n/2})^2 = (Z^{n/2})^2$ from $X^n + Y^n = Z^n$.

Then $X^{n/2} - a = Y^{n/2} - b = Z^{n/2} - a - b = X^{n/2} + Y^{n/2} - Z^{n/2}$. Here, assume what X, Y and Z are the positive integers and relatively prime, then a and b can be the positive real numbers.

Let

$$\begin{aligned} G &= (X^{n/2} - a)/(ab)^{1/2} = (Y^{n/2} - b)/(ab)^{1/2} \\ &= (Z^{n/2} - a - b)/(ab)^{1/2} = (X^{n/2} + Y^{n/2} - Z^{n/2})/(ab)^{1/2}. \end{aligned}$$

Then

$$X^{n/2} = G(ab)^{1/2} + a, \;\; Y^{n/2} = G(ab)^{1/2} + b, \;\; Z^{n/2} = G(ab)^{1/2} + a + b$$

and

$$X^{n/2} + Y^{n/2} - Z^{n/2} = G(ab)^{1/2}.$$

Let

$$\{G(ab)^{1/2} + a\}^2 + \{G(ab)^{1/2} + b\}^2 = \{G(ab)^{1/2} + a + b\}^2.$$

Then $G = 2^{1/2} > 0$. Here, $X^{n/2} + Y^{n/2} - Z^{n/2} = G(ab)^{1/2} > 0$. Because $(X^{n/2} + Y^{n/2})^2 > (Z^{n/2})^2$ in the positive real numbers, $X^{n/2}$, $Y^{n/2}$ and $Z^{n/2}$.

So,

$$X^{n/2} = (2ab)^{1/2} + a, Y^{n/2} = (2ab)^{1/2} + b \text{ and } Z^{n/2} = (2ab)^{1/2} + a + b.$$

Therefore,

$$X^n = \{(2ab)^{1/2} + a\}^2 = [\{2(Z^{n/2} - Y^{n/2})(Z^{n/2} - X^{n/2})\}^{1/2} + (Z^{n/2} - Y^{n/2})]^2,$$
$$Y^n = \{(2ab)^{1/2} + b\}^2 = [\{2(Z^{n/2} - Y^{n/2})(Z^{n/2} - X^{n/2})\}^{1/2} + (Z^{n/2} - X^{n/2})]^2$$

and

$$Z^n = \{(2ab)^{1/2} + a + b\}^2 = [\{2(Z^{n/2} - Y^{n/2})(Z^{n/2} - X^{n/2})\}^{1/2} + (Z^{n/2} - Y^{n/2}) + (Z^{n/2} - X^{n/2})]^2.$$

Let n be the odd number, then one or two factors of $X^{n/2}$, $Y^{n/2}$ and $Z^{n/2}$ can be the positive integers but at least one factor of $X^{n/2}$, $Y^{n/2}$ and $Z^{n/2}$ cannot be the integer, i.e., the assumption that all three factors of $X^{n/2}$, $Y^{n/2}$ and $Z^{n/2}$ can be the positive integers means what n is the even number. So, at least one factor of $X^{n/2}$, $Y^{n/2}$ and $Z^{n/2}$ cannot be the integer in the odd n. [ex.; $\{(x^{2r+1})^{2k+1}, (y^{2s})^{2k+1}, (z^{2t})^{2k+1}\}$].

In the odd n, X^n, Y^n and Z^n are the positive integers but $\{(2ab)^{1/2}+a\}^2$, $\{(2ab)^{1/2}+b\}^2$ and $\{(2ab)^{1/2} + a + b\}^2$ cannot be the integers like these 7 cases.

(Case 1). Let $X^{n/2}$, $Y^{n/2}$ and $Z^{n/2}$ are not the integers, then

$$\{(2ab)^{1/2} + a\}^2 = [\{2(Z^{n/2} - Y^{n/2})(Z^{n/2} - X^{n/2})\}^{1/2} + (Z^{n/2} - Y^{n/2})]^2,$$
$$\{(2ab)^{1/2} + b\}^2 = [\{2(Z^{n/2} - Y^{n/2})(Z^{n/2} - X^{n/2})\}^{1/2} + (Z^{n/2} - X^{n/2})]^2$$

and

$$\{(2ab)^{1/2}+a+b\}^2 = [\{2(Z^{n/2}-Y^{n/2})(Z^{n/2}-X^{n/2})\}^{1/2}+(Z^{n/2}-Y^{n/2})+(Z^{n/2}-X^{n/2})]^2$$

cannot be the integers.

(Case 2). Let $X^{n/2}$ and $Z^{n/2}$ are not the integers but $Y^{n/2} = y$ is the positive integer, then

$$\{(2ab)^{1/2} + a\}^2 = [\{2(Z^{n/2} - y)(Z^{n/2} - X^{n/2})\}^{1/2} + (Z^{n/2} - y)]^2,$$
$$\{(2ab)^{1/2} + b\}^2 = [\{2(Z^{n/2} - y)(Z^{n/2} - X^{n/2})\}^{1/2} + (Z^{n/2} - X^{n/2})]^2$$

and

$$\{(2ab)^{1/2} + a + b\}^2 = [\{2(Z^{n/2} - y)(Z^{n/2} - X^{n/2})\}^{1/2} + (Z^{n/2} - y) + (Z^{n/2} - X^{n/2})]^2$$

cannot be the integers.

(Case 3). Let $Y^{n/2}$ and $Z^{n/2}$ are not the integers but $X^{n/2} = x$ is the positive integer, then

$$\{(2ab)^{1/2} + a\}^2 = [\{2(Z^{n/2} - Y^{n/2})(Z^{n/2} - x)\}^{1/2} + (Z^{n/2} - Y^{n/2})]^2,$$
$$\{(2ab)^{1/2} + b\}^2 = [\{2(Z^{n/2} - Y^{n/2})(Z^{n/2} - x)\}^{1/2} + (Z^{n/2} - x)]^2$$

and

$$\{(2ab)^{1/2} + a + b\}^2 = [\{2(Z^{n/2} - Y^{n/2})(Z^{n/2} - x)\}^{1/2} + (Z^{n/2} - Y^{n/2}) + (Z^{n/2} - x)]^2$$

cannot be the integers.

(Case 4). Let $X^{n/2}$ and $Y^{n/2}$ are not the integers but $Z^{n/2} = z$ is the positive integer, then

$$\{(2ab)^{1/2} + a\}^2 = [\{2(z - Y^{n/2})(z - X^{n/2})\}^{1/2} + (z - Y^{n/2})]^2,$$
$$\{(2ab)^{1/2} + b\}^2 = [\{2(z - Y^{n/2})(z - X^{n/2})\}^{1/2} + (z - X^{n/2})]^2$$

and

$$\{(2ab)^{1/2} + a + b\}^2 = [\{2(z - Y^{n/2})(z - X^{n/2})\}^{1/2} + (z - Y^{n/2}) + (z - X^{n/2})]^2$$

cannot be the integers.

(Case 5). Let $X^{n/2}$ is not the integer but $Y^{n/2} = y$ and $Z^{n/2} = z$ are the positive integers, then

$$\{(2ab)^{1/2} + a\}^2 = [\{2(z - y)(z - X^{n/2})\}^{1/2} + (z - y)]^2,$$
$$\{(2ab)^{1/2} + b\}^2 = [\{2(z - y)(z - X^{n/2})\}^{1/2} + (z - X^{n/2})]^2$$

and

$$\{(2ab)^{1/2} + a + b\}^2 = [\{2(z - y)(z - X^{n/2})\}^{1/2} + (z - y) + (z - X^{n/2})]^2$$

cannot be the integers.

(Case 6). Let $Y^{n/2}$ is not the integer but $X^{n/2} = x$ and $Z^{n/2} = z$ are the positive integers, then

$$\{(2ab)^{1/2} + a\}^2 = [\{2(z - Y^{n/2})(z - x)\}^{1/2} + (z - Y^{n/2})]^2$$
$$\{(2ab)^{1/2} + b\}^2 = [\{2(z - Y^{n/2})(z - x)\}^{1/2} + (z - x)]^2$$

and

$$\{(2ab)^{1/2} + a + b\}^2 = [\{2(z - Y^{n/2})(z - x)\}^{1/2} + (z - Y^{n/2}) + (z - x)]^2$$

cannot be the integers.

(Case 7). Let $Z^{n/2}$ is not the integer but $X^{n/2} = x$ and $Y^{n/2} = y$ are the positive integers, then

$$\{(2ab)^{1/2} + a\}^2 = [\{2(Z^{n/2} - y)(Z^{n/2} - x)\}^{1/2} + (Z^{n/2} - y)]^2,$$
$$\{(2ab)^{1/2} + b\}^2 = [\{2(Z^{n/2} - y)(Z^{n/2} - x)\}^{1/2} + (Z^{n/2} - x)]^2$$

and

$$\{(2ab)^{1/2}+a+b\}^2 = [\{2(Z^{n/2}-y)(Z^{n/2}-x)\}^{1/2}+(Z^{n/2}-y)+(Z^{n/2}-x)]^2$$

cannot be the integers.

In those 7 cases, $\{(2ab)^{1/2}+a\}^2$, $\{(2ab)^{1/2}+b\}^2$ and $\{(2ab)^{1/2}+a+b\}^2$ cannot be the integers but X^n, Y^n and Z^n are the positive integers.

It is an apparent contradiction because of the odd n. So, $X^n+Y^n=Z^n$ cannot have the positive integer solutions in the odd n. I.e., the contradiction appears in the odd n but the contradiction does not appear in the even n.

Therefore,
$X^n+Y^n=Z^n$ cannot have the positive integer solutions in the odd n.

But $X^n+Y^n=Z^n$ may have some positive integer solutions in the even n.

4. $X^n+Y^n=Z^n$ cannot have the positive integer solutions in the even $n>2$

4-1. The Pythagorean triples, X, Y and Z in the positive integers, A and B.

Let $A=Z-Y$ and $B=Z-X$ in the Pythagorean Theorem, $X^2+Y^2=Z^2$.

Then $X-A=Y-B=Z-A-B=X+Y-Z$. Here, assume what X, Y and Z are the positive integers and relatively prime, then A and B are also the positive integers and relatively prime.

Let

$$\begin{aligned} G &= (X-A)/(AB)^{1/2} = (Y-B)/(AB)^{1/2} \\ &= (Z-A-B)/(AB)^{1/2} = (X+Y-Z)/(AB)^{1/2}. \end{aligned}$$

Then

$$X=G(AB)^{1/2}+A, \quad Y=G(AB)^{1/2}+B, \quad Z=G(AB)^{1/2}+A+B$$

and

$$X+Y-Z=G(AB)^{1/2}.$$

Let

$$\{G(AB)^{1/2}+A\}^2+\{G(AB)^{1/2}+B\}^2=\{G(AB)^{1/2}+A+B\}^2.$$

Then $G=2^{1/2}>0$. Here, $X+Y-Z=G(AB)^{1/2}>0$. Because $(X+Y)^2>Z^2$ in the positive integers, X, Y and Z.

So,
$X=(2AB)^{1/2}+A$, $Y=(2AB)^{1/2}+B$ and $Z=(2AB)^{1/2}+A+B$.

Let X, Y and Z are the positive integers, then A and B are always the positive integers. So, the positive integers, X, Y and Z are all Pythagorean triples in the positive integers, A and B.

Let $c^2=A=Z-Y$ and $2d^2=B=Z-X$ in $X=(2AB)^{1/2}+A$, $Y=(2AB)^{1/2}+B$ and $Z=(2AB)^{1/2}+A+B$.

Then
$X = 2cd + c^2$, $Y = 2cd + 2d^2$ and $Z = 2cd + c^2 + 2d^2$.
And let $c + d = r$.
Then
$X = r^2 - d^2$, $Y = 2rd$ and $Z = r^2 + d^2$.
Therefore, X and Z are always the odd numbers and Y is always the even number in relatively prime, X, Y and Z.

4-2. The Pythagorean triples, X, Y and Z cannot be the mth power numbers like x^m, y^m and z^m.

Let $c^2 = Z - Y$ and $2d^2 = Z - X$ in the Pythagorean Theorem, $X^2 + Y^2 = Z^2$.
Then $X = 2cd + c^2$, $Y = 2cd + 2d^2$ and $Z = 2cd + c^2 + 2d^2$.
Here, assume what some Pythagorean triples, X, Y and Z can be the mth power numbers like these $X = (et)^m = x^m$, $Y = (2fs)^m = y^m$ and $XY = 2cd(c+d)(c+2d) = (2efst)^m = (xy)^m$ when $c = e^m$, $d = 2^{(m-1)}f^m$, $c + d = e^m + 2^{(m-1)}f = s^m$ and $c + 2d = e^m + (2f)^m = t^m$ in the positive integers and relatively prime, e, $2f$ and t. Then this is an illogical assumption when $m > 1$.
Let $g^2 = t^{m/2} - (2f)^{m/2}$ and $2h^2 = t^{m/2} - e^{m/2}$ in $(e^{m/2})^2 + \{(2f)^{m/2}\}^2 = (t^{m/2})^2$ from $e^m + (2f)^m = t^m$.
Then

$$e^{m/2} - g^2 = (2f)^{m/2} - 2h^2 = t^{m/2} - g^2 - 2h^2 = e^{m/2} + (2f)^{m/2} - t^{m/2}.$$

Here, remember what e, $(2f)$ and t were assumed to be the positive integers and relatively prime. Then g^2 and $2h^2$ are also the positive integers and relatively prime.
Let

$$G = (e^{m/2} - g^2)/2gh = \{(2f)^{m/2} - 2h^2\}/2gh$$
$$= (t^{m/2} - g^2 - 2h^2)/2gh = \{e^{m/2} + (2f)^{m/2} - t^{m/2}\}/2gh.$$

Then

$$e^{m/2} = 2ghG + g^2, \quad (2f)^{m/2} = 2ghG + 2h^2, \quad t^{m/2} = 2ghG + g^2 + 2h^2$$

and

$$e^{m/2} + (2f)^{m/2} - t^{m/2} = 2ghG.$$

Let

$$\{2ghG + g^2\}^2 + \{2ghG + 2h^2\}^2 = \{2ghG + g^2 + 2h^2\}^2.$$

Then $G = 1 > 0$. Here, $e^{m/2} + (2f)^{m/2} - t^{m/2} = 2ghG > 0$. Because $\{e^{m/2} + (2f)^{m/2}\}^2 > (t^{m/2})^2$ in the positive real numbers, $e^{m/2}$, $(2f)^{m/2}$ and $t^{m/2}$.
So,

$$e^{m/2} = 2gh + g^2,\ (2f)^{m/2} = 2gh + 2h^2 \text{ and } t^{m/2} = 2gh + g^2 + 2h^2.$$

Therefore,

$$e^m = \{2gh + g^2\}^2,\ (2f)^m = \{2gh + 2h^2\}^2 \text{ and } t^m = \{2gh + g^2 + 2h^2\}^2 \text{ and}$$
$$e^{1/2} = \{2gh + g^2\}^{1/m},\ (2f)^{1/2} = \{2gh + 2h^2\}^{1/m} \text{ and } t^{1/2} = \{2gh + g^2 + 2h^2\}^{1/m}$$

Here, remember what e, $2f$ and t were assumed to be the positive integers and relatively prime. Then g and h are needed to be the positive integers and relatively prime. So, the mth power Pythagorean triples like $(e^{1/2})^m$, $\{(2f)^{1/2}\}^m$ and $(t^{1/2})^m$ are needed in the Pythagorean Theorem, $(e^{m/2})^2 + \{(2f)^{m/2}\}^2 = (t^{m/2})^2$.

The assumption that the Pythagorean triples, X, Y and Z can be the mth power numbers like x^m, y^m and z^m means what the smaller mth power Pythagorean triples like $(e^{1/2})^m$, $\{(2f)^{1/2}\}^m$ and $(t^{1/2})^m$ must be needed.

It is an illogical assumption when $m > 1$.

So, $m = 1$.

4-3. $X^n + Y^n = Z^n$ cannot have the positive integer solutions in the even $n > 2$.

The assumption of the mth power Pythagorean triples like $X = x^m$, $Y = y^m$ and $Z = z^m$ is illogical when $m > 1$.

So, $m = 1$.

Therefore,

$X^n + Y^n = Z^n$ cannot have the positive integer solutions in the even $n > 2$.

5. Conclusion

We have got $X = (2AB)^{1/2} + A$, $Y = (2AB)^{1/2} + B$ and $Z = (2AB)^{1/2} + A + B$, where $A = Z - Y$ and $B = Z - X$ in the Pythagorean Theorem, $X^2 + Y^2 = Z^2$. And all Pythagorean triples, X, Y and Z cannot be the mth power numbers like x^m, y^m and z^m.

When $n > 2$, $X^n + Y^n = Z^n$ cannot have the positive integer solutions. It means what $X^n + Y^n = Z^n$ has no none-zero integer solutions.

Acknowledgment

We believe what the space and the matters come into existence when the numbers come into existence. And we also believe what all cosmic materials and lives change but the number theory cannot change now and forever.

Thanks.

References

[1] **BarryCipra.** (1994). "Straightening out nonlinear codes." What's happening in Mathematical Sciences. pp. 37-40, vol. 2.

Author1
Jae Yul Lee(Corresponding Author)
e-mail: leejaeyul5@yahoo.co.kr
Gyeonggi Safety Company
010-3723-5244

Author2
You Jin Lee
e-mail: jgyoujin@hanmail.net
College of Veterinary Medicine Seoul National University
042-621-4848