A Short Proof of Fermat`s Last Theorem

Author1

Jae Yul Lee (Corresponding Author)
leejaeyul5@yahoo.co.kr
leejaeyul5@hanmail.net
Gyeonggi Safety Company
010-3723-5244

Author2

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

Abstract

This paper briefly presents all Pythagorean triples and a very short and plain FLT proof. Let A=Z-Y and B=Z-X in the Diophantine equation, $X^n+Y^n=Z^n$. Then X-A=Y-B=Z-A-B=X+Y-Z. Fermat's Last Theorem asserts that 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 that he had found a short proof, but left no evidence of what it was. Finding a proof became the most famous unsolved problem in 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.

Key Words and Phrases

X-A=Y-B=Z-A-B=X+Y-Z.
$X=2cd+c^2$, $Y=2cd+2d^2$ 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

A Short Proof of Fermat`s Last Theorem

A Short Proof of Fermat`s Last Theorem

Sentence

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 that $X^n+Y^n=Z^n$ has no non-zero integer solutions for X, Y and Z, when n>2. This theorem means that $X^n+Y^n=Z^n$ 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 number, n.

Without loss of generality we assume that X, Y and Z are relatively prime, i.e., that (X,Y)=1 and (Y,Z)=(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 and Y, Y and Z and X and Z.

2. Introduction

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

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

Then X-A=Y-B=Z-A-B=X+Y-Z.

We define that $G=(X-A)/(AB)^{1/n}=(Y-B)/(AB)^{1/n}=(Z-A-B)/(AB)^{1/n}=(X+Y-Z)/(AB)^{1/n}$.

So,

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

Therefore,

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

Now, G=0 when n=1 and $G=2^{1/2}$ when n=2.

2-2. G=0 when n=1.

Let {G(AB)+A}+{G(AB)+B}={G(AB)+A+B}.

Then G=0. Where X+Y-Z=G(AB)=0.

So, X=A, Y=B and Z=A+B.

2-3. $G=2^{1/2}$ when n=2.

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

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

Therefore,

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

2-4. G=Function(A,B) when n>2.

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

Then we can only see that G=Function(A,B) when n>2.

3. $X^n+Y^n=Z^n$ cannot have the positive integer solutions in the odd number, 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 $X^{n/2}-a=Y^{n/2}-b=Z^{n/2}-a-b=X^{n/2}+Y^{n/2}-Z^{n/2}$.

We define that $G=(X^{n/2}-a)/(ab)^{1/2}=(Y^{n/2}-b)/(ab)^{1/2}=(Z^{n/2}-a-b)/(ab)^{1/2}=(X^{n/2}+Y^{n/2}-Z^{n/2})/(ab)^{1/2}$.

So,

$X^{n/2}=G(ab)^{1/2}+a$, $Y^{n/2}=G(ab)^{1/2}+b$, $Z^{n/2}=G(ab)^{1/2}+a+b$ 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 $G=2^{1/2}>0$. Where, $X^{n/2}+Y^{n/2}-Z^{n/2}=G(ab)^{1/2}>0$. 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,

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

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

When X, Y and Z are relatively prime in the odd number, n>2, 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., if all three factors of $X^{n/2}$, $Y^{n/2}$ and $Z^{n/2}$ can be the positive integers, it means that n>2 is the even number. So, at least one factor of $X^{n/2}$, $Y^{n/2}$ and $Z^{n/2}$ cannot be the integer when X, Y and Z are relatively prime in the odd number, n>2. [ex.; $\{(x^{2r+1})^{2k+1}, (y^{2s})^{2k+1}, (z^{2t})^{2k+1}\}$].

Now, when X, Y and Z are relatively prime in the odd number, n>2, X^n, Y^n and Z^n are the positive integers, but $\{(2ab)^{1/2}+a\}^2=[\{2(Z^{n/2}-Y^{n/2})(Z^{n/2}-X^{n/2})\}^{1/2}+(Z^{n/2}-Y^{n/2})]^2$,

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

It is an apparent contradiction because of relatively prime, X, Y and Z in the odd number, n>2. So, $X^n+Y^n=Z^n$ cannot have the positive integer solutions in the odd number, n>2. I.e., the contradiction appears in the odd number, n, but the contradiction does not appear in the even number, n.

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

But $X^n+Y^n=Z^n$ may have some positive integer solutions in the even number, n>2.

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

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

We have got $X=(2AB)^{1/2}+A$, $Y=(2AB)^{1/2}+B$ and $Z=(2AB)^{1/2}+A+B$, when A=Z-Y and B=Z-X in the Pythagorean Theorem, $X^2+Y^2=Z^2$.

When X, Y and Z are the positive integers, 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.

We have got the Pythagorean triples, $X=2cd+c^2$, $Y=2cd+2d^2$ and $Z=2cd+c^2+2d^2$ when $c^2=Z-Y$ and $2d^2=Z-X$ in the Pythagorean Theorem, $X^2+Y^2=Z^2$.

If someone suppose that 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 relatively prime, e, 2f and t, he is wrong 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 $e^{m/2}-g^2=(2f)^{m/2}-2h^2= t^{m/2}-g^2-2h^2=e^{m/2}+(2f)^{m/2}-t^{m/2}$.

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

So,

$e^{m/2}=2ghG+g^2$, $(2f)^{m/2}=2ghG+2h^2$, $t^{m/2}=2ghG+g^2+2h^2$ 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. Where, $e^{m/2}+(2f)^{m/2}-t^{m/2}=2ghG>0$. 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,

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

Here, e^m, $(2f)^m$ and t^m are supposed to be the positive integers by someone. Therefore, g, h, $e^{m/2}$, $(2f)^{m/2}$ and $t^{m/2}$ are all needed to be the positive integers in

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

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

So, $e^{1/2}$, $(2f)^{1/2}$ and $t^{1/2}$ are also needed to be the positive integers in

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

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

So, $(e^{1/2})^m$, $\{(2f)^{1/2}\}^m$ and $(t^{1/2})^m$ are also needed to be the mth power Pythagorean triples in the Pythagorean Theorem, $(e^{m/2})^2+\{(2f)^{m/2}\}^2=(t^{m/2})^2$.

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

It is an illogical assumption, when m>1.

So, m=1.

4-3. Therefore, $X^n+Y^n=Z^n$ cannot have the positive integer solutions in the even number, 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 that $X^n+Y^n=Z^n$ has no non-zero integer solutions.

Acknowledgment

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

Thanks.

References

BarryCipra. (1994). "Straightening out nonlinear codes." What`s happening in Mathematical Sciences. pp. 37-40, vol. 2.