The Simplest Proving Method of Fermat's Last Theorem

Haofeng Zhang
Beijing, China

Abstract: In this paper the author gives the simplest proving method of **Fermat's Last Theorem** (FLT) that is just equivalent to the one that Fermat had said there were not enough spaces to write it down but of course not the same one since nobody knows what the proof of Fermat was. The purpose of this paper is not only just to demonstrate the simplest proof but also to illustrate that there are many simple proving methods of FLT that are waited to be found.

1. Some Relevant Theorems

There are some theorems for proving or need to be known. ***All symbols in this paper represent positive integers unless stated they are not.***

Theorem 1.1. In the equation of

$$\begin{cases} x^n + y^n = z^n \\ \gcd(x, y, z) = 1 \\ n > 2 \end{cases} \tag{1-1}$$

x, y, z meet $x \neq y$, $x + y > z$ and if $x > y$ then $z > x > y$.

Proof: Let

$$x = y,$$

we have

$$2x^n = z^n$$

and

$$\sqrt[n]{2}x = z$$

where $\sqrt[n]{2}$ is not an integer and x, z are all positive integers, so $x \neq y$. Since

$$(x+y)^n = x^n + C_n^1 x^{n-1} y + \ldots + C_n^{n-1} x y^{n-1} + y^n > z^n,$$

so we get

$$x + y > z.$$

Obviously since $x^n + y^n = z^n$, so we have

$$z^n > x^n, z^n > y^n$$

and get

$$z > x > y$$

when $x > y$.

Theorem 1.2. In the equation of (1-1), x, y, z meet

$$\gcd(x, y) = \gcd(y, z) = 1$$

and $z - y \geq 2$ when $x > y$.

Proof: According to equation (1-1), since

$$x^n + y^n = z^n,$$

so we have

$$x^n = z^n - y^n = (z - y)\left(z^{n-1} + z^{n-2}y + z^{n-3}y^2 + \ldots + z^2y^{n-3} + zy^{n-2} + y^{n-1}\right).$$

From **Theorem 1.1** we know $x \neq y$, so let

$$x > y,$$

we have

$$z > x > y$$

and

$$\begin{cases} z - x \geq 1 \\ x - y \geq 1 \\ z - y \geq 2 \end{cases}.$$

It is obviously that x can not be a prime number because the right side is a product of two positive numbers and $z - y \geq 2$.

If $\gcd(z, y) > 1$ then we have

$$x^n = \gcd(z, y) \times (z_1 - y_1)\left(z^{n-1} + z^{n-2}y + z^{n-3}y^2 + \ldots + z^2y^{n-3} + zy^{n-2} + y^{n-1}\right),$$

since the right side contains the factor of $\gcd(z, y) > 1$ so the left side must also contains this factor that is contradicted against (1-1) in which $\gcd(x, y, z) = 1$.

Since $x^n + y^n = z^n$, if $\gcd(x, y) > 1$ then we have $\left(x_1^n + y_1^n\right) \times [\gcd(x, y)]^n = z^n$ which causes $\gcd(x, y, z) > 1$ since the left side contains the factor of $[\gcd(x, y)]^n$ so the right side must also contains this factor but contradicts against (1-1) in which $\gcd(x, y, z) = 1$.

So we have the conclusion of $\gcd(x, y) = \gcd(y, z) = 1$ and $z - y \geq 2$ when $x > y$.

Theorem 1.3. If there is no positive integer solution for

$$x^p + y^p = z^p$$

when $p > 2$ is a prime number then there is also no positive integer solution for

$$\left(x^p\right)^k+\left(y^p\right)^k=\left(z^p\right)^k.$$

Proof: Since $x^p+y^p=z^p$ has no positive integer solution, so there still no positive integer solution for

$$\left(x^k\right)^p+\left(y^k\right)^p=\left(z^k\right)^p$$

which means there is also no positive integer solution for

$$\left(x^p\right)^k+\left(y^p\right)^k=\left(z^p\right)^k.$$

So we only need to prove there is no positive integer solution for equation (1-1) when n is a prime number.

Theorem 1.4. In the equation of (1-1), x, y, z meet

$$x^{n-i}+y^{n-i}>z^{n-i}$$

where $n>i\geq 1.$

Proof: According to equation (1-1), since

$$x^n+y^n=z^n,$$

and $\frac{x}{z}<1,\frac{y}{z}<1$, so we have

$$x^{n-i}+y^{n-i}>\left[\left(\frac{x}{z}\right)^i x^{n-i}+\left(\frac{y}{z}\right)^i y^{n-i}=z^{n-i}\right]$$

that means

$$x^{n-i}+y^{n-i}>z^{n-i}.$$

Theorem 1.5. In figure 1-1, x, y, z of equation (1-1) meet

$$\frac{x^{n-1}+y^{n-1}-z^{n-1}}{x^{n-2}+y^{n-2}-z^{n-2}}\leq 1.$$

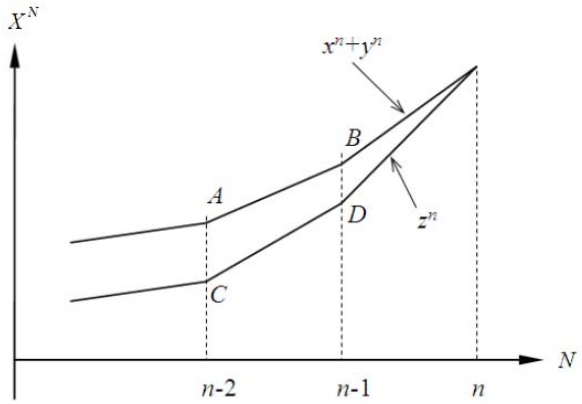

Figure 1-1 Graph for $x^n + y^n = z^n$

Proof: Obviously the meaning of $\dfrac{x^{n-1} + y^{n-1} - z^{n-1}}{x^{n-2} + y^{n-2} - z^{n-2}} \le 1$ is the slope of AB is not greater than that of CD and if $\dfrac{x^{n-1} + y^{n-1} - z^{n-1}}{x^{n-2} + y^{n-2} - z^{n-2}} = 1$ then the slope of AB equals to that of CD.

If $\dfrac{x^{n-1} + y^{n-1} - z^{n-1}}{x^{n-2} + y^{n-2} - z^{n-2}} > 1$ then there must have a positive real number $0 < r < 1$ for $n - r$ between $n-1$ and n whose slope equals to that of BE which means

$$\frac{x^n + y^n - x^{n-1} - y^{n-1}}{\dfrac{z^{n-r} - z^{n-1}}{1-r}} = 1$$

that can be explained by figure 1-2 where $BE \,//\, DF$.

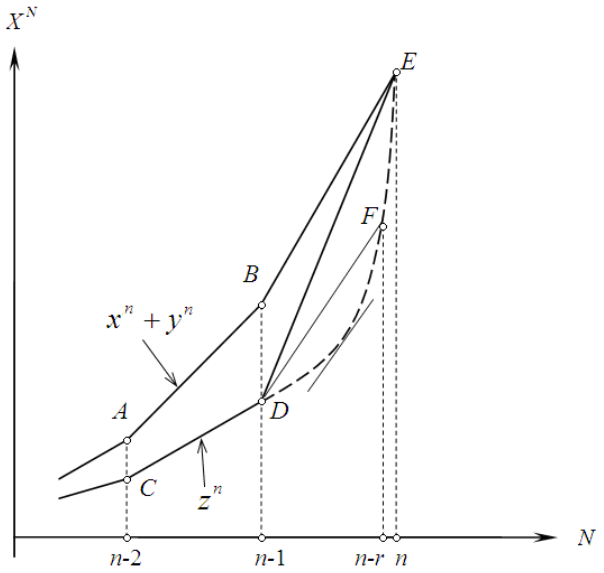

Figure 1-2 Graph for $x^n + y^n = z^n$ *when* $\dfrac{x^{n-1} + y^{n-1} - z^{n-1}}{x^{n-2} + y^{n-2} - z^{n-2}} > 1$

So we have

$$x^n + y^n - x^{n-1} - y^{n-1} = \left(\frac{z^{-r} - z^{-1}}{1-r} \right) z^n \tag{1-2}$$

If the real number of r is a irrational number then the right side is not an integer but the left side is a positive integer since if not we have

$$\begin{cases} \dfrac{z^{-r}-z^{-1}}{1-r}=\dfrac{b}{a} \\ \gcd(a,b)=1 \end{cases}$$

and

$$\frac{a}{z^r}+br=b+\frac{a}{z}$$

that is impossible since the left side is a irrational number (the sum of positive irrational numbers is still a irrational number whether they are same or not) but the right side is a rational number so (1-2) can not be sissified in this case. If the real number of r is a rational number then let

$$\begin{cases} r=\dfrac{b}{a} \\ a>b \\ \gcd(a,b)=1 \\ \end{cases}$$

and z^r have to be rational numbers to let the right side equal to the left, so we have

$$\begin{cases} z^r=z^{\frac{b}{a}}=\dfrac{d}{c} \\ \gcd(c,d)=1 \end{cases}$$

where

$$z^b=\left(\frac{c}{d}\right)^a$$

which is impossible since the left side is a positive integer but the right side is not. So we have

$$z^r=z^{\frac{b}{a}}=d$$

and

$$z^b=d^a,$$

if there are common factors for z,d then after divided by these common factors we have

$$z_1{}^b z_2=d_1{}^a d_2,$$

since $a>b$ and there are no positive integer numbers of the left side equal to that of the right sides which means it is impossible to let the left side of (1-2) equal to the right side and $\dfrac{x^{n-1}+y^{n-1}-z^{n-1}}{x^{n-2}+y^{n-2}-z^{n-2}}>1$ is not possible .

In other plain words to say is that the real number r_1 which causes the maximum value of $f(r)=x^{n-r}+y^{n-r}-z^{n-r}$ between $n-1$ and n whose slope equals to that of BE does not

exist which means $x^n + y^n$ and z^n can not meet together at point E that directly leads to the result of there are no positive integer solutions for equation (1-1) at the assumption of $\frac{x^{n-1} + y^{n-1} - z^{n-1}}{x^{n-2} + y^{n-2} - z^{n-2}} > 1$. So we have the conclusion of

$$\frac{x^{n-1} + y^{n-1} - z^{n-1}}{x^{n-2} + y^{n-2} - z^{n-2}} \le 1.$$

Theorem 1.6. There are no positive integer solutions for

$$1^n + y^n = z^n.$$

Proof: Since

$$1 = z^n - y^n = (z - y)\left(z^{n-1} + z^{n-2}y + ... + zy^{n-2} + y^{n-1}\right)$$

where

$$\begin{cases} z - y = 1 \\ \left(z^{n-1} + z^{n-2}y + ... + zy^{n-2} + y^{n-1}\right) = 1 \end{cases}$$

that causes z, y to be non positive integers, so there are no positive integer solutions for

$$1^n + y^n = z^n.$$

Theorem 1.7. There are no positive integer solutions for

$$2^n + y^n = z^n.$$

Proof: Since

$$2^n = z^n - y^n = (z - y)\left(z^{n-1} + z^{n-2}y + ... + zy^{n-2} + y^{n-1}\right),$$

if

$$\begin{cases} z - y = 1 \\ z^{n-1} + z^{n-2}y + ... + zy^{n-2} + y^{n-1} = 2^n \end{cases}$$

then taking the least value for $y = 1, z = 3$, we have

$$3^{n-1} + 3^{n-2} + ... + 1 > 2^n$$

when $n > 2$ that is impossible. If

$$\begin{cases} z - y = 2^i \\ z^{n-1} + z^{n-2}y + ... + zy^{n-2} + y^{n-1} = 2^j \\ i + j = n \\ i \ge 1 \end{cases}$$

then $z > 2$ and taking the least value of $y = 1, z = 3$, we get

$$3^{n-1} + 3^{n-2} + ... + 1 > 2^j$$

with $n > 2$ that is also impossible, so there are no positive integer solutions for

$$2^n + y^n = z^n .$$

2. Proving Method

In equation (1-1), let

$$\begin{cases} a = x^{n-2} \\ b = y^{n-2} \\ c = z^{n-2} \end{cases},$$

we have

$$\begin{cases} ax^2 + by^2 = cz^2 \\ a^{\frac{n-1}{n-2}}x + b^{\frac{n-1}{n-2}}y = c^{\frac{n-1}{n-2}}z \end{cases}. \tag{2-1}$$

If we can prove $x \neq a^{\frac{n-1}{n-2}}, y \neq a^{\frac{n-1}{n-2}}, z \neq a^{\frac{n-1}{n-2}}$ then equation (1-1) must have no positive integer solution. Since we reduce the order of equation so the method is called “Order reducing method for equations”.

Assume

$$\begin{cases} a = x^{n-2} \\ b = y^{n-2} \\ c = z^{n-2} \end{cases},$$

let

$$\begin{cases} y = x - f \\ z = x + e \end{cases}. \tag{2-2}$$

From (2-1) and (2-2) we have

$$\begin{cases} ax^2 + b(x - f)^2 = c(x + e)^2 \\ a^{\frac{n-1}{n-2}}x + b^{\frac{n-1}{n-2}}(x - f) = c^{\frac{n-1}{n-2}}(x + e) \end{cases}$$

and

$$\begin{cases} (a + b - c)x^2 - 2(bf + ce)x + (bf^2 - ce^2) = 0 \\ a^{\frac{n-1}{n-2}}x + b^{\frac{n-1}{n-2}}(x - f) - c^{\frac{n-1}{n-2}}(x + e) = 0 \end{cases},$$

the roots are

$$x=\frac{(bf+ce)\pm\sqrt{(bf+ce)^2-(a+b-c)(bf^2-ce^2)}}{x^{n-2}+y^{n-2}-z^{n-2}}, \tag{2-3}$$

and

$$x=\frac{c^{\frac{n-1}{n-2}}e+b^{\frac{n-1}{n-2}}f}{a^{\frac{n-1}{n-2}}+b^{\frac{n-1}{n-2}}-c^{\frac{n-1}{n-2}}}=\frac{bfy+cez}{x^{n-1}+y^{n-1}-z^{n-1}}. \tag{2-4}$$

There are two cases for bf^2, ce^2 when $bf^2 \geq ce^2$ and $bf^2 < ce^2$.

Case A: If $bf^2 \geq ce^2$, from (2-3) when

$$x=\frac{(bf+ce)+\sqrt{(bf+ce)^2-(a+b-c)(bf^2-ce^2)}}{x^{n-2}+y^{n-2}-z^{n-2}},$$

since $\left(a+b-c=x^{n-2}+y^{n-2}-z^{n-2}\right)>0$, so we have

$$x\leq\frac{2(bf+ce)}{x^{n-2}+y^{n-2}-z^{n-2}},$$

and also since $\left(x^{n-1}+y^{n-1}-z^{n-1}\right)>0$, compare to (2-4) we get

$$\frac{bfy+cez}{x^{n-1}+y^{n-1}-z^{n-1}}\leq\frac{2(bf+ce)}{x^{n-2}+y^{n-2}-z^{n-2}}.$$

From **Theorem 1.5** we know $\frac{x^{n-1}+y^{n-1}-z^{n-1}}{x^{n-2}+y^{n-2}-z^{n-2}}\leq 1$, so we have

$$bfy+cez\leq 2(bf+ce)$$

that is impossible since from **Theorem 1.6** we have already know $y\neq 1$ which means $y\geq 2$ and $z\geq 3$. When

$$x=\frac{(bf+ce)-\sqrt{(bf+ce)^2-(a+b-c)(bf^2-ce^2)}}{x^{n-2}+y^{n-2}-z^{n-2}}.$$

we have

$$x\leq\frac{bf+ce}{x^{n-2}+y^{n-2}-z^{n-2}},$$

compare to (2-4) we get

$$\frac{bfy+cez}{x^{n-1}+y^{n-1}-z^{n-1}}\leq\frac{bf+ce}{x^{n-2}+y^{n-2}-z^{n-2}}.$$

From **Theorem 1.5** we have

$$bfy + cez \le bf + ce$$

that is impossible since we have already know $y \ge 2$ and $z \ge 3$.

Case B: If $bf^2 < ce^2$, from (2-3) when

$$x = \frac{(bf + ce) + \sqrt{(bf + ce)^2 + (a + b - c)(ce^2 - bf^2)}}{x^{n-2} + y^{n-2} - z^{n-2}},$$

we can prove $(bf + ce)^2 > (a + b - c)(ce^2 - bf^2)$ since if not we have

$$(bf + ce)^2 \le (a + b - c)(ce^2 - bf^2)$$

and

$$[(2b + a) - c]bf^2 + 2bfce + [2c - (a + b)]ce^2 \le 0$$

that is impossible since $2c - (a + b) > 0, a + b - c > 0.$ So we have

$$x < \frac{(bf + ce)(1 + \sqrt{2})}{x^{n-2} + y^{n-2} - z^{n-2}}$$

compare to (2-4) we get

$$\frac{bfy + cez}{x^{n-1} + y^{n-1} - z^{n-1}} < \frac{(bf + ce)(1 + \sqrt{2})}{x^{n-2} + y^{n-2} - z^{n-2}}.$$

From **Theorem 1.5** we have

$$bfy + cez < (bf + ce)(1 + \sqrt{2}) < 2.5(bf + ce)$$

and

$$bf(x - f) + ce(x + e) < 2.5(bf + ce)$$

that leads to

$$x < \left[\frac{2.5(bf + ce) + bf^2 - ce^2}{bf + ce} = 2.5 - \frac{ce^2 - bf^2}{bf + ce} \right] < 2.5$$

where possible values for x are 1, 2 but according to **Theorem 1.6**, **1.7** we know there are no positive integer solutions. When

$$x = \frac{(bf + ce) - \sqrt{(bf + ce)^2 + (a + b - c)(ce^2 - bf^2)}}{x^{n-2} + y^{n-2} - z^{n-2}}$$

is not possible since $x \le 0$.

Now we have completely solved no positive integer solutions for equation (1-1) when $n > 2$

using “Order reducing method for equations”.

3. Conclusion

Through the above contents we can see clearly that the proving of *Fermat's Last Theorem* is just a problem of elementary mathematics. “Order reducing method for equations” that the author invented is a very effective method in the proving of Fermat's Last Theorem and the author’s technique in which let $y = x - f$ and $z = x + e$ is a very important step for solving.

Fermat's Last Theorem is a problem that has lasted for about 380 years. Proving methods are not important but the theorem’s correctness is very necessary because many useful inferences can be deduced that are obviously better than “conjectures”.

The author has been working on proving of *Fermat's Last Theorem* for quite some times (90 days) without any reference and many methods have been thought about, for example “Method of prime factorization” but not work. So the author has already known that there are no ways to solve except “Solving high order equations” which is also an important aspect in solving other mathematic problems.