

THE PROOF OF FERMAT'S LAST THEOREM

Wong Chiaho (汪家诒)¹

(Received April 10, 1995)

Abstract

(i) Instead of $x^n + y^n = z^n$, we use

$$(x-b)^n + x^n = (x+a)^n \quad (0.1)$$

as the general equation of Fermat's Last Theorem (FLT), where a and b are two arbitrary natural numbers. By means of binomial expansion, (0.1) can be written as

$$x^n - \sum_{r=1}^n \binom{n}{r} x^{n-r} [a^r - (-b)^r] = 0 \quad (0.2)$$

Because $a^r - (-b)^r$ always contains $a+b$ as its factor, (0.2) can be written as

$$x^n - (a+b) \sum_{r=1}^n \binom{n}{r} x^{n-r} \phi_r = 0 \quad (0.3)$$

where $\phi_r = [a^r - (-b)^r] / (a+b)$ are integers for $r = 1, 2, 3, \dots, n$

(ii) Let s be a factor of $a+b$ and let $(a+b) = sc$. We can use $x = sy$ to transform (0.3) to the following (0.4)

$$(sy)^n - sc \left[\sum_{r=1}^{n-2} \binom{n}{r} (sy)^{n-r} \phi_r + n sy \phi_{n-1} \right] = sc \phi_n \quad (0.4)$$

(iii) Dividing (0.4) by s^2 we have

$$s^{n-2} y^n - c \left[\sum_{r=1}^{n-2} \binom{n}{r} s^{n-r-1} y^{n-r} \phi_r + n y \phi_{n-1} \right] = \frac{c \phi_n}{s} \quad (0.5)$$

On the left side of (0.5) there is a polynomial of y with integer coefficients and on the right side there is a constant $c\phi/s$. If $c\phi/s$ is not an integer, then we cannot find an integer y to satisfy (0.5), and then FLT is true for this case. If $c\phi_n/s$ is an integer, we may change a and c such the $c\phi_n/s \neq$ an integer.

Key words factorization, cofactor, relative prime, gcd, combination, algebraic division, Fermat's Last Theorem

I. Introduction

(a) The statement of Fermat's Last Theorem (FLT): The equation

$$x^n + y^n = z^n \quad (1.1)$$

where n is a natural number larger than 2, has no solution in positive integers, x, y, z all different from 0.

¹ Zhejiang University, Hangzhou 310013, P. R. China

(b) Two important restrictions

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

(ii) It will suffice to prove FLT in the case where the exponent n is a prime.

(c) Short biography of Fermat and his FLT

Pierre de Fermat (1601–1665) was a french mathematician. His assertion of FLT was made about 1637. He proved FLT only the case $n=4$ i. e. $x^4+y^4=z^4$ has no integer solution of x, y, z by principle of "infinite descent", so called by Fermat himself (Ref. [1]).

We know that any positive integer belongs among one of 4 types: $4m, 4m+1, 4m+2, 4m+3$. Fermat proved $n=4$, then $x^{4m}+y^{4m}=z^{4m}$ can be written as $(x^m)^4+(y^m)^4=(z^m)^4$, FLT is also true for $n=4m$. Then there remain only three cases: $4m+1, 4m+2, 4m+3$. But $4m+2=2(2m+1)$, so that we can prove $x^{4m+2}+y^{4m+2}=z^{4m+2}$ in terms of $(x^2)^{2m+1}+(y^2)^{2m+1}=(z^2)^{2m+1}$. Now $4m+1, 2m+1, 4m+3$, they are all odd integers. Then we need to prove n is an odd prime only.

II. Theorem 1: No Two of x, y, z Variables Can Be Equal

If $z=x$ then the equation $x^n+y^n=z^n$ becomes $y=0$. It is contradicted because they are all different from 0. If $z=y$, then $x=0$. We have the same reason as before. If $x=y$, then $2x^n=z^n$, and then $z=(2)^{1/n}x$. Therefore even if x is an integer, z is not an integer, and follows that the three integers x, y, z , are all different to each other, and therefore the equation of FLT can be written as

$$(x-b)^n+x^n=(x+a)^n \quad (0.1)$$

where a and b are two arbitrary natural numbers.

III. The Three Inspired Problems of FLT

(a) $(x-1)^3+x^3=(x+1)^3$, where $x-1, x, x+1$ are three neighboring integers. Then we have

$$x^3-3x^2+3x-1+x^3=x^3+3x^2+3x+1 \quad \text{or} \quad x^3-6x^2-2=0$$

or $x^3=2(3x^2+1)$ which shows that x must be an even integer.

$$\text{Let us take the transformation} \quad x=2y \quad (3.1)$$

$$\text{Then we have} \quad (2y)^3=2[3(2y)^2+1] \quad \text{or} \quad 8y^3-24y^2=2 \quad (3.2)$$

$$\text{Dividing (3.2) by 8, we get} \quad y^3-3y^2=1/4 \quad (3.3)$$

If y is an integer, then the left side of (3.3) is an integer, but the right side is a fraction $1/4$, then the integer y must be nonexistent. It follows that the even integer x is also nonexistent. We have proved FLT is true for this case.

$$(b) \text{ To prove FLT is true for } (x-1)^n+x^n=(x+1)^n \quad (3.4)$$

Using the binomial expansion, we find that

$$(x-1)^n=x^n+\sum_{r=1}^n \binom{n}{r} x^{n-r} (-1)^r \quad \text{and} \quad (x+1)^n=x^n+\sum_{r=1}^n \binom{n}{r} x^{n-r} (1)^r$$

Substituting then into (3.4), we get

$$x^n+\sum_{r=1}^n \binom{n}{r} x^{n-r} [(-1)^r-1]=0 \quad (3.5)$$

When r is an even integer, $(-1)^r-1=0$, and when r is an odd integer $(-1)^r-1=-2$.

Let us use the sign $\sum_{r=1}^n$ to express the summation taken over r which are odd integers only. Then we can write (3.5) as

$$x^n = 2 \sum_{r=1}^n \binom{n}{r} x^{n-r} \quad (3.6)$$

(3.6) shows z must be an even integer.

$$\text{Let } x = 2y \quad (3.7)$$

Then after substituting (3.7) into (3.6), the (3.6) becomes

$$(2y)^n - 2 \left[\sum_{r=1}^{n-4} \binom{n}{r} (2y)^{n-r} + \frac{n(n-1)}{2} (2y)^2 \right] = 2 \quad (3.8)$$

The coefficients of the polynomial on the left-side have a $\text{gcd} = 2^3$. Dividing (3.8) by 8, we get

$$2^{n-3}y^n - \sum_{r=1}^{n-4} \binom{n}{r} 2^{n-r-2}y^{n-r} - \frac{n(n-1)}{2}y^2 = \frac{1}{4} \quad (3.9)$$

On the left side of (3.9), there is a polynomial of y with integer coefficients and on right side there is a fraction $1/4$, such equation has no solution in integer of y . Then the even integer x is also nonexistent and then FLT is true for this case. Thus we have proved (3.4) has no solution in integer for any positive integer n greater than 2, no matter what it is even or odd. The above statement is our important discriminating principle.

(c) To prove $(x-a)^n + x^n = (x+a)^n$ its FLT is true

$$(x-a)^n + x^n = (x+a)^n \quad (3.10)$$

Let us take a transformation $x = aw$, then (3.10) becomes

$$(aw-a)^n + (aw)^n = (aw+a)^n \quad (3.11)$$

Cancelling a^n from both sides of (3.11), it becomes

$$(w-1)^n + w^n = (w+1)^n \quad (3.12)$$

(3.12) has the same form as (3.4), which has been proved "Its FLT is true for (3.4), then FLT is also true for (3.12)"

IV. Changing the Form of General Equation $(x-b)^n + x^n = (x+a)^n$

Using the binomial expansion of $(x-b)^n$ and $(x+a)^n$, we have

$$(x-b)^n = x^n + \sum_{r=1}^n \binom{n}{r} x^{n-r} (-b)^r \quad (4.1)$$

and

$$(x+a)^n = x^n + \sum_{r=1}^n \binom{n}{r} x^{n-r} a^r \quad (4.2)$$

Substituting $(x-b)^n$ of (4.1) and $(x+a)^n$ of (4.2) into Eq. (0.1), we have

$$x^n - \sum_{r=1}^n \binom{n}{r} x^{n-r} [a^r - (-b)^r] = 0 \quad (4.3)$$

When

$$\begin{aligned} r=2m+1, a^r - (-b)^r &= a^{2m+1} - (-b)^{2m+1} = a^{2m+1} + b^{2m+1} \\ &= (a+b)(a^{2m} - a^{2m-1}b + a^{2m-2}b^2 - \dots + a^2b^{2m-2} - ab^{2m-1} + b^{2m}) \end{aligned} \quad (4.4)$$

When

$$\begin{aligned} r=2m, a^r - (-b)^r &= a^{2m} - b^{2m} = (a+b)(a^{2m-1} - a^{2m-2}b + a^{2m-3}b^2 \\ &\quad - \dots + a^2b^{2m-4} - a^2b^{2m-3} + ab^{2m-2} - b^{2m-1}) \end{aligned} \quad (4.5)$$

Hence $a^r - (-b)^r$ is always contented $a+b$ as it's factor. We may write

$$a^r - (-b)^r = (a+b)\phi_r \quad (r=1, 2, \dots, n) \quad (4.6)$$

where $\phi_r (r=1, 2, 3 \dots n)$ are all integers.

Then Eq. (4.3) becomes

$$x^n - (a+b) \left[\sum_{r=1}^n \binom{n}{r} x^{n-r} \phi_r \right] = 0 \quad (4.7)$$

or we write it as a more useful equation as below

$$x^n - (a+b) \left[\sum_{r=1}^{n-2} \binom{n}{r} x^{n-r} \phi_r + nx\phi_{n-1} \right] = (a+b)\phi_n \quad (4.8)$$

where

$$\phi_n = \frac{a^n - (-b)^n}{a+b} = a^{n-1} - a^{n-2}b + a^{n-3}b^2 - \dots + a^2b^{n-3} - ab^{n-2} + b^{n-1} \quad (4.9)$$

Now we make a list of some ϕ_r below

$$\begin{aligned} \phi_1 &= 1, \quad \phi_2 = a-b, \quad \phi_3 = a^2 - ab + b^2 \\ \phi_4 &= a^3 - a^2b + ab^2 - b^3, \quad \phi_5 = a^4 - a^3b + a^2b^2 - ab^3 + b^4 \\ \phi_6 &= a^5 - a^4b + a^3b^2 - a^2b^3 + ab^4 - b^5 \\ \phi_n &= a^{n-1} - a^{n-2}b + a^{n-3}b^2 - a^{n-4}b^3 + \dots - a^2b^{n-4} + a^2b^{n-3} - ab^{n-2} + b^{n-1} \end{aligned}$$

The equation of FLT for $n=7$ can be written as

$$\begin{aligned} x^7 - (a+b) &[7x^6 + \binom{7}{2}x^5(a-b) + \binom{7}{3}x^4(a^2 - ab + b^2) \\ &+ \binom{7}{4}x^3(a^3 - a^2b + ab^2 - b^3) + \binom{7}{5}x^2(a^4 - a^3b + a^2b^2 - ab^3 + b^4) \\ &+ \binom{7}{6}x(a^5 - a^4b + a^3b^2 - a^2b^3 + ab^4 - b^5)] \\ &= (a+b)(a^6 - a^5b + a^4b^2 - a^3b^3 + a^2b^4 - ab^5 + b^6) \end{aligned} \quad (4.10)$$

V. Using the Condition: $\gcd(a, b)=1$ to Discard the Mediocre Solution of FLT.

When using $x^n + y^n = z^n$ as the equation of FLT, we use $\gcd(x, y, z)=1$ to discard the mediocre solution (cx, cy, cz) . If a and b have a common factor c , then we have $a = \bar{a}c$ and $b = \bar{b}c$, so that $a+b = (\bar{a} + \bar{b})c$. From (4.7), we have

$$x^n = (\bar{a} + \bar{b})c \sum_{r=1}^n \binom{n}{r} x^{n-r} \phi_r \quad (5.1)$$

then x^n contains c as its factor. But x^n is an integer so that x itself must contain c as its factor. Let $x = \bar{x}c$. Then $y = x - b = \bar{x}c - \bar{b}c = (\bar{x} - \bar{b})c$ and $z = x + a = \bar{x}c + \bar{a}c = (\bar{x} + \bar{a})c$.

Then $\gcd(x, y, z) = \gcd(\bar{x}c, \bar{y}c, \bar{z}c) = c \neq 1$, it is contradiction with the condition $\gcd(x, y, z) = 1$. Hence we must have $(a, b) = 1$. or written as $\gcd(a, b, a \neq b) = 1$. (5.2)

VI. Theorem 2: $\frac{a^n + b^n}{(a+b)^2}$ Is An Integer When and Only When $a + b = n$

$$\frac{a^n + b^n}{(a+b)^2} = \frac{a^n + b^n}{a+b} \bigg/ (a+b) = \left[\sum_{r=1}^n a^{n-r} (-b)^{r-1} \right] \bigg/ (a+b)$$

$$= (a^{n-1} - a^{n-2}b + a^{n-3}b^2 - \dots + a^2b^{n-3} - ab^{n-2} + b^{n-1}) / (a+b) \quad (6.1)$$

The division of $(a^n + b^n) / (a+b)^2$

$$\begin{array}{r} (a^{n-1} - a^{n-2}b + a^{n-3}b^2 - \dots + a^2b^{n-3} - ab^{n-2} + b^{n-1}) / (a+b) \\ a+b \overline{) a^{n-1} - a^{n-2}b + a^{n-3}b^2 - a^{n-4}b^3 + a^{n-5}b^4 - a^{n-6}b^5 + a^{n-7}b^6 - \dots} \\ \underline{a^{n-1} + a^{n-2}b} \phantom{+ a^{n-3}b^2 - a^{n-4}b^3 + a^{n-5}b^4 - a^{n-6}b^5 + a^{n-7}b^6 - \dots} \\ -2a^{n-2}b + a^{n-3}b^2 \phantom{- a^{n-4}b^3 + a^{n-5}b^4 - a^{n-6}b^5 + a^{n-7}b^6 - \dots} \\ \underline{-2a^{n-2}b - 2a^{n-3}b^2} \phantom{+ a^{n-4}b^3 + a^{n-5}b^4 - a^{n-6}b^5 + a^{n-7}b^6 - \dots} \\ 3a^{n-3}b^2 - a^{n-4}b^3 \phantom{+ a^{n-5}b^4 - a^{n-6}b^5 + a^{n-7}b^6 - \dots} \\ \underline{3a^{n-3}b^2 + 3a^{n-4}b^3} \phantom{+ a^{n-5}b^4 - a^{n-6}b^5 + a^{n-7}b^6 - \dots} \\ -4a^{n-4}b^3 + a^{n-5}b^4 \phantom{- a^{n-6}b^5 + a^{n-7}b^6 - \dots} \\ \underline{-4a^{n-4}b^3 - 4a^{n-5}b^4} \phantom{+ a^{n-6}b^5 + a^{n-7}b^6 - \dots} \\ +5a^{n-5}b^4 - a^{n-6}b^5 \phantom{+ a^{n-7}b^6 - \dots} \\ \underline{+5a^{n-5}b^4 + 5a^{n-6}b^5} \phantom{+ a^{n-7}b^6 - \dots} \\ -6a^{n-6}b^5 + a^{n-7}b^6 \\ \dots \end{array}$$

Then we have

$$\frac{a^n + b^n}{(a+b)^2} = a^{n-1} - 2a^{n-2}b + 3a^{n-3}b^2 - 4a^{n-4}b^3 + 5a^{n-5}b^4 - 6a^{n-6}b^5 + \dots \quad (6.2)$$

For $n=7$ as an example, we have

$$\frac{a^7 + b^7}{(a+b)^2} = a^5 - 2a^4b + 3a^3b^2 - 4a^2b^3 + 5ab^4 - 6b^5 + \frac{7b^6}{a+b} \quad (6.3)$$

Then the last term of (6.2) must be $nb^{n-1} / (a+b)$ (6.4)

By means of $\gcd(a, b, a+b)=1$, we know that $b^{n-1} / (a+b)$ is not an integer. Then the expression of (6.4) will be an integer only when $n=a+b$. Thus we have the following Theorem 2:

$a^n + b^n / (a+b)^2$ is an integer when and only when $a+b=n$

Let

$$\phi_n = \frac{a^n + b^n}{a+b} = a^{n-1} - a^{n-2}b + a^{n-3}b^2 - \dots + a^2b^{n-3} - ab^{n-2} + b^{n-1} \quad (6.5)$$

Then $\phi_n / (a+b)$ will be an integer only when $a+b=n$

VII. Theorem 3: $(a^n + b^n) / (a+b)^3$ Is Not an Integer

$$\begin{array}{r} a+b \overline{) a^{n-3} - 3a^{n-4}b + 6a^{n-5}b^2 - 10a^{n-6}b^3 + 15a^{n-7}b^4 - \dots} \\ \underline{a^{n-3} - 2a^{n-3}b + 3a^{n-4}b^2 - 4a^{n-5}b^3 + 5a^{n-6}b^4 - 6a^{n-7}b^5 + \dots} \\ -3a^{n-3}b + 3a^{n-4}b^2 \phantom{- 4a^{n-5}b^3 + 5a^{n-6}b^4 - 6a^{n-7}b^5 + \dots} \\ \underline{-3a^{n-3}b - 3a^{n-4}b^2} \phantom{+ 4a^{n-5}b^3 + 5a^{n-6}b^4 - 6a^{n-7}b^5 + \dots} \\ +6a^{n-4}b^2 - 4a^{n-5}b^3 \phantom{+ 5a^{n-6}b^4 - 6a^{n-7}b^5 + \dots} \\ \underline{+6a^{n-4}b^2 + 6a^{n-5}b^3} \phantom{+ 5a^{n-6}b^4 - 6a^{n-7}b^5 + \dots} \\ -10a^{n-5}b^3 + 5a^{n-6}b^4 \phantom{- 6a^{n-7}b^5 + \dots} \\ \underline{-10a^{n-5}b^3 - 10a^{n-6}b^4} \phantom{+ 5a^{n-6}b^4 - 6a^{n-7}b^5 + \dots} \\ 15a^{n-6}b^4 - 6a^{n-7}b^5 \phantom{+ 5a^{n-6}b^4 - 6a^{n-7}b^5 + \dots} \\ \underline{15a^{n-6}b^4 + 15a^{n-7}b^5} \phantom{+ 5a^{n-6}b^4 - 6a^{n-7}b^5 + \dots} \\ -21a^{n-7}b^5 \phantom{+ 5a^{n-6}b^4 - 6a^{n-7}b^5 + \dots} \\ \dots \end{array}$$

Note that let $S_m = 1 + 2 + 3 + \dots + (m-1) + m$ (7.1)

Then $S_1 = 1$, $S_2 = 1 + 2 = 3$, $S_3 = 1 + 2 + 3 = 6$, $S_4 = 1 + 2 + 3 + 4 = 10$, etc.

Thus the quotient of $\frac{\phi_n}{(a+b)^2}$ can be written as

$$\begin{aligned} \frac{\phi_n}{(a+b)^2} = & S_1 a^{n-3} - S_2 a^{n-4} b + S_3 a^{n-5} b^2 - S_4 a^{n-6} b^3 + \dots \\ & + \dots + S_m a^{n-m-2} (-b)^{m-1} + \dots \end{aligned} \quad (7.2)$$

The last some terms of the division may be found as follows

$$\begin{array}{r} (S_{n-4})a^2b^{n-5} - (S_{n-3})ab^{n-4} + (S_{n-2})b^{n-3} \\ a+b \overline{) \dots + (n-4)a^3b^{n-5} - (n-3)a^2b^{n-4} - (n-2)ab^{n-3} - (n-1)b^{n-2} + b^{n-1}} \\ \underline{-(S_{n-5})a^3b^{n-5}} \\ (S_{n-4})a^3b^{n-5} - (n-3)a^2b^{n-4} \\ \underline{-(S_{n-4})a^3b^{n-5} + (S_{n-4})a^2b^{n-4}} \\ -(S_{n-3})a^2b^{n-4} + (n-2)ab^{n-3} \\ \underline{-(S_{n-3})a^2b^{n-4} - (S_{n-3})ab^{n-3}} \\ (S_{n-2})ab^{n-3} - (n-1)b^{n-2} \\ \underline{(S_{n-2})ab^{n-3} + (S_{n-2})b^{n-2}} \\ -(S_{n-1})b^{n-2} + b^{n-1} \end{array}$$

Combining the above division expressions, we obtain

$$\begin{aligned} \frac{\phi_n}{(a+b)^2} = & a^{n-3} - S_2 a^{n-4} b + S_3 a^{n-5} b^2 - S_4 a^{n-6} b^3 + S_5 a^{n-7} b^4 \\ & + (S_{n-4})a^2b^{n-5} - (S_{n-3})ab^{n-4} + S_{n-2}b^{n-3} + \frac{-S_{n-1}b^{n-2} + b^{n-1}}{a+b} \end{aligned}$$

Now let us consider the above last fraction

$$\frac{-(S_{n-1})b^{n-2} + b^{n-1}}{a+b} = \frac{(-S_{n-1} + b)b^{n-2}}{a+b} \quad (7.3)$$

We know that $a+b$ and b^{n-2} are relative prime, so that we may consider only the part of the above fraction:

$$\frac{-S_{n-1} + b}{a+b}, \text{ where } S_{n-1} = 1 + 2 + 3 + \dots + (n-2) + (n-1) = \frac{n(n-1)}{2}$$

Because we have $a+b=n$, we have

$$\frac{-S_{n-1} + b}{a+b} = \frac{-\frac{n(n-1)}{2} + b}{n} = \frac{-n(n-1)}{2n} + \frac{b}{a+b} = \frac{-(n-1)}{2} + \frac{b}{a+b} \quad (7.4)$$

Because $n \geq 3$ and n is an odd prime, $\frac{n-1}{2}$ is an integer, but $\frac{b}{a+b}$ is not an integer, hence their sum is not an integer. Then we have proved Theorem 3 that $\frac{a^n + b^n}{(a+b)^3} = \frac{\phi_n}{(a+b)^2}$ is not an integer.

VIII. If $a+b$ Is a Prime Integer, Then FLT Is True for This Case

(A) $a+b \neq n$

When $a+b$ is a prime, we may take a transformation $x = (a+b)w$.

Substituting $x = (a+b)w$ into (4.8), we get

$$(a+b)^n w^n - (a+b) \left[\sum_{r=1}^{n-2} \binom{n}{r} (a+b)^{n-r} w^{n-r} \phi_r + n(a+b)w \phi_{n-1} \right] = (a+b) \phi_n \quad (8.1)$$

The coefficients in the left side of the above equation has a $\gcd = (a+b)^2$, we divide the above by $(a+b)^2$, we get

$$(a+b)^{n-2}w^n - \left[\sum_{r=1}^{n-2} \binom{n}{r} (a+b)^{n-r-1} w^{n-r} \phi_r + n w \phi_{n-1} \right] = \frac{\phi_n}{a+b} \quad (8.2)$$

In the left side of (8.2), there is a polynomial of w with integer coefficients, and in the right side there is a fraction $\phi_n/(a+b)$, as shown in (6.4) when $a+b \neq n$. Such equation has no solution in integer. Then FLT is true for this case.

(B) $a+b=n$

If n is a prime, besides $\binom{n}{n}=1$, all $\binom{n}{r}$ contains n as its factor. The Eq. (8.2) can be written as

$$n^n w^n - n \left[\sum_{r=1}^{n-2} \binom{n}{r} n^{n-r-1} w^{n-r} \phi_r + n^2 w \phi_{n-1} \right] = n \phi_n \quad (8.3)$$

In the left side of (8.3), the coefficients have a $\gcd = n^3$. Dividing (8.3) by n^3 , we get

$$n^{n-3} w^n - \left[\sum_{r=1}^{n-2} \binom{n}{r} n^{n-r-3} w^{n-r} \phi_r + w \phi_{n-1} \right] = \frac{\phi_n}{n^2} \quad (8.4)$$

In the left side of (8.4), there is a polynomial of w with integer coefficients, but in the right side of (8.4) is a fraction it is not an integer, then (8.4) has no solution in integer, i. e. FLT is true for this case.

IX. If $a+b$ Is an Even Integer, Then FLT is True

Let $a+b=2^m B$, where B is the cofactor of 2^m and B is an odd integer, i. e. B does not contain the factor 2 again. First of all, we must discuss the parity condition of a and b .

(A) If a and b are both even integer, then $\gcd(a, b, a+b)=2$. It is contradiction with $\gcd(a, b, a+b)=1$.

(B) If a and b have the different parity $a+b$ is not an even integer, which is out of our problem.

(C) Then a and b are both odd integers.

Let $a=2l+1$ and $b=2m+1$, then $a+b=2(l+m+1)$

where $l+m+1$ is an any integer. Then we may put

$$a+b=2^{n_0} p_1^{n_1} p_2^{n_2} \dots p_t^{n_t} = 2^{n_0} E \quad (9.1)$$

where

$$E = p_1^{n_1} p_2^{n_2} \dots p_t^{n_t} \quad (9.2)$$

p_1, p_2, \dots, p_t are odd primes, n_1, n_2, \dots, n_t are natural numbers.

Substituting (9.1) into (4.8), we get

$$x^n - 2^{n_0} E \left[\sum_{r=1}^{n-2} \binom{n}{r} x^{n-r} \phi_r + n x \phi_{n-1} \right] = 2^{n_0} E \phi_n \quad (9.3)$$

Then x must contain 2 as its factor. Let us take $x=2^m w$ as a transformation, then the transformed equation becomes

$$2^{mn} w^n - 2^{n_0} E \left[\sum_{r=1}^{n-2} \binom{n}{r} 2^{m(n-r)} w^{n-r} \phi_r + n 2^m w \phi_{n-1} \right] = 2^{n_0} E \phi_n \quad (9.4)$$

If we choose m so that $m \geq n_0 / (n-1)$, then $mn \geq n_0 + m$. Thus there is a $\gcd = 2^{m+n_0}$ in the coefficients of the left side of (9.4). Dividing (9.4) by 2^{m+n_0} , we have

$$w^n 2^{mn-m-n_0} - E \left[\sum_{r=1}^{n-2} \binom{n}{r} 2^{m(n-r)-m} w^{n-r} \phi_r + n w \phi_{n-1} \right] = \frac{E \phi_n}{2^m} \quad (9.5)$$

In the left side of (9.5), there is a polynomial of w with integer coefficients and the right side is a fraction, such equation has no integer w to satisfied (9.5), and then FLT is true for this case.

X. If $a+b$ Contains a Factor p^t , Where p Is a Prime and t Is a Natural Number, Then FLT Is True.

Proof Let $a+b = p^t B$, where B is an integer, and it is the cofactor of p^t in $a+b$, then FLT equation of this problem becomes

$$x^n - p^t B \left[\sum_{r=1}^{n-2} \binom{n}{r} x^{n-r} \phi_r + n x \phi_{n-1} \right] = p^t B \phi_n. \quad (10.1)$$

By means of (10.1), x must contain p^s as its factor, where $1 \leq s \leq t$. Let $x = p^s y$. Substituting $x = p^s y$ into (10.1), we have

$$(p^s y)^n - p^t B \left[\sum_{r=1}^{n-2} \binom{n}{r} (p^s y)^{n-r} \phi_r + n (p^s y) \phi_{n-1} \right] = p^t B \phi_n \quad (10.2)$$

Now we choose s , so that $s \geq \frac{t}{n-1}$, then $ns \geq t + s$. The coefficients in the left side of (10.2) have a $\gcd = p^{t+s}$. Dividing two sides of (10.2) by p^{t+s} , then (10.2) becomes

$$p^{s(n-t-s)} y^n - B \left[\sum_{r=1}^{n-2} \binom{n}{r} p^{s(n-r)-s} y^{n-r} \phi_r + n y \phi_{n-1} \right] = B \phi_n / p^s \quad (10.3)$$

In the left side of (10.3), there is a polynomial of y with integer coefficients, and on the right side, there is a fraction $B \phi_n / p^s$, such equation does not have an integer solution of y , then FLT is true for this problem.

XI. Conclusion

Now we have proved the problem of FLT with the cases (1) $a=b$, (2) $a+b$ is prime, (3) $a+b$ is an even integer, (4) $a+b$ contains a factor of p^t where p is an any prime and t is an any natural number, then we have proved the FLT problem completely.

Note 1 We know that Pierre de Fermat proved only the case $n=4$. L. Euler only proved the case $n=3$ with his proof having a gap. G. L. Dirichlet proved $n=5$ in 1828, etc. We know that prime number n may be very large without limit, so that if we use known value of integer n (>2), our proof of FLT cannot prove completely. In this paper we use " n is an any prime number".

Note 2 In our proof, we use " $n/(a+b)$ as a fraction, it becomes an integer only when $n=a+b$, i. e. $n/(a+b)=1$."

References

- [1] Paulo Ribenboim, 13 *Lectures on Fermat's Last Theorem*, Springer-Verlag, New York Inc. USA (1979).
- [2] M. Harold, *Fermat's Last Theorem (A genetic Introduction to Algebraic Number Theory)*, Springer-Verlag (1977)