The Elementary Proof of Fermat's Last Theorem

By

Sattawat Suntisurat

King's Mongkut Institute of Technology Ladkrabang

Mechanical Engineering Thailand

E-mail : sattawatsuntisurat@gmail.com

25 Dec 2020

Abstract : Proof of Fermat's Last Theorem by using basic of algebra.

From Fermat's Last Theorem,

$$a^n + b^n \neq c^n \quad \text{for every positive integer } a , b , c \text{ and } n > 2$$

Begin to prove…

Assume a , b , c can make $a^n + b^n = c^n$, n is positive integer

and $\gcd(a , b , c) = 1$

$$a^n + b^n = c^n$$

$$a^n = c^n - b^n$$

$$a^n = (c - b)(c^{n-1} + b\,c^{n-2} + b^2 c^{n-3} + \dots + b^{n-1})$$

$$a^n = (c - b)[\,(c - b)K + nb^{n-1}\,]$$

$$K = c^{n-2} + 2b\,c^{n-3} + 3b^2 c^{n-4} + \dots + (n - 1)b^{n-2} \quad \text{and} \quad c - b \neq 1$$

Assume a is a prime

If a is a prime , then $(c - b) = a^k$, $k \geq 1$

But $a + b > c$ =====> $a > c - b$ it is contradiction , so a isn't prime.

Rewrite again $b^n = (c - a)[(c - a)P + na^{n-1}]$

$P = c^{n-2} + 2ac^{n-3} + 3a^2 c^{n-4} + \ldots + (n-1)b^{n-2}$ and $c - a \neq 1$

Assume b is a prime

If b is a prime, then $(c - a) = b^k$, $k \geq \mathbf{1}$

But $a + b > c$ =====> $b > c - a$ it is contradiction, so a isn't prime.

Therefore a and c aren't prime but they are composite numbers.

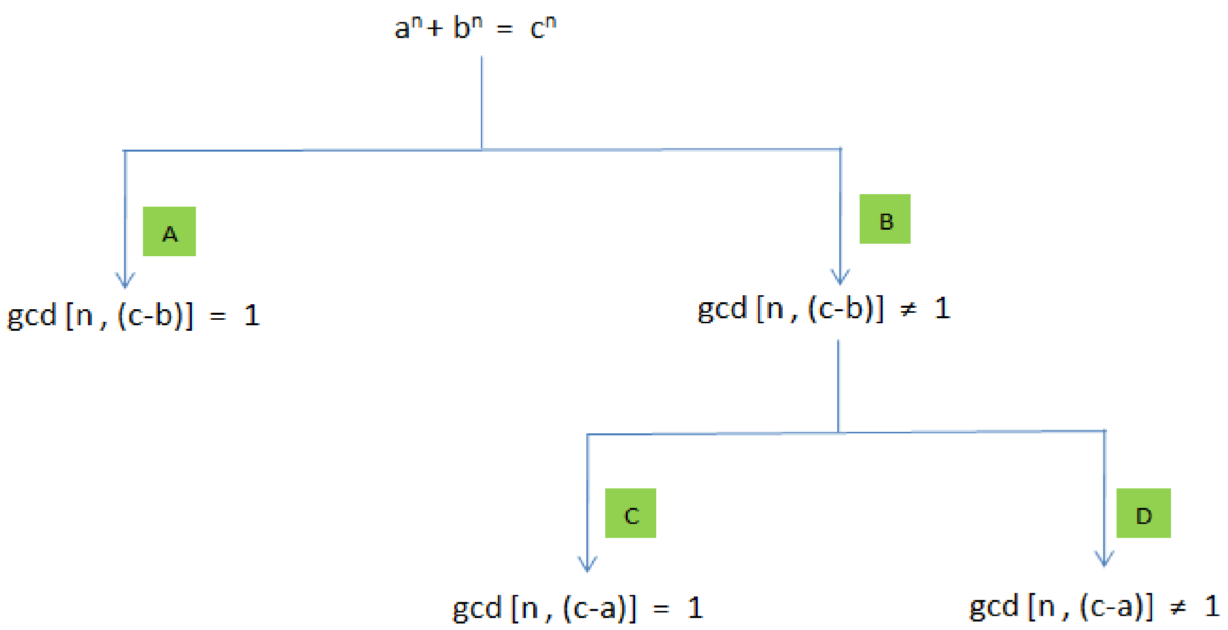
Assume $a = b$

$$2b^n = c^n$$

$$(\sqrt[n]{2}\, b)^n = c^n$$ then c is irrational.

Therefore $a \neq b$

After that, to continue by following below diagram



Consider from A → B → C → D

Consider at A , $\gcd[n, (c-b)] = 1$

I can write as below,

$$(k^n + b)^n = (mk)^n + b^n$$

Let $k^n + b = c$, $mk = a$, $\gcd(m, k) = 1$

Rewrite again, $b^n = (k^n + b - mk)[(k^n + b)^{n-1} + mk(k^n + b)^{n-2} + \dots + (mk)^{n-1}]$

Then b^n can be divided by $(k^n + b - mk)$

Ref. Remainder theorem , $(mk - k^n)^n = 0$

$k^{n-1} = m$ it isn't true because $\gcd(m, k) = 1$

Therefore $a^n + b^n \neq c^n$ at A Step

No positive integer a , b , c can make it true if n has no common factors with (c-b)

Consider at B , $\gcd[n, (c-b)] \neq 1$

The equation $a^n + b^n = c^n$ may be true if n has common factors with (c-b)

Consider at C , $\gcd[n, (c-a)] = 1$

I can write as below,

$$(p^n + a)^n = a^n + (pq)^n$$

Let $p^n + a = c$, $pq = b$, $\gcd(p, q) = 1$

Rewrite again, $a^n = (p^n + a - pq)[(p^n + a)^{n-1} + pq(p^n + a)^{n-2} + \dots + (pq)^{n-1}]$

Then a^n can be divided by $(p^n + a - pq)$

Ref. Remainder theorem , $(pq - p^n)^n = 0$

$p^{n-1} = q$ it isn't true because $\gcd(p, q) = 1$

Therefore $a^n + b^n \neq c^n$ at C Step

No positive integer a , b , c can make it true if n has no common factors with (c-a)

From Step B and C , if the equation $a^n + b^n = c^n$ will be true when...

$gcd[n , (c-a)] \neq 1$ and $gcd[n , (c-b)] \neq 1$

Consider at D , $gcd [n, (c-a)] \neq 1$

From the previous proof , then equation must be this form,

$$a^{f(c-a)f(c-b)N} + b^{f(c-a)f(c-b)N} = c^{f(c-a)f(c-b)N} \quad \text{\_\_\_\_\_\_\_\_\_\_\_\_\_\_} (1)$$

f(c-a) is factor of (c-a) , f(c-b) is factor of (c-b) and N is a positive integer

Rewrite again, $(a^{f(c-a)N})^{f(c-b)} + (b^{f(c-a)N})^{f(c-b)} = (c^{f(c-a)N})^{f(c-b)}$

Let $a^{f(c-a)N} = A$, $b^{f(c-a)N} = B$, $c^{f(c-a)N} = C$

$$A^{f(c-b)} + B^{f(c-b)} = C^{f(c-b)}$$

From the proof , must $gcd [f(c-b) , C – A] \neq 1$

$$C – A = (c-a)(c^{f(c-a)N-1} + a c^{f(c-a)N-2} + a^2 c^{f(c-a)N-3} + \dots + a^{f(c-a)N-1}) \quad \text{\_\_\_\_\_\_\_\_\_\_\_\_\_\_} (2)$$

From (2), I found that f(c-b) has no any common factors with C – A

It contradict the previous proof , So I can say...

$a^n + b^n \neq c^n$ a , b , c are the positive integers , $n > 2$, $c - a \neq 1$ and $c - b \neq 1$

There is another case, $a = c - 1$ or $b = c - 1$

I have to prove it with the different method as below,

Assume $a^n + b^n = c^n$, a , b , c are positive integers and $n > 2$

Let $b = c - 1$, $a^n = c^{n-1} + (c - 1)c^{n-2} + (c - 1)^2 c^{n-3} + \dots + (c - 1)^{n-1}$

Let $a = c - k$, $1 < k < c$ and k is positive integer

$$(c - k)^n = c^{n-1} + (c - 1)c^{n-2} + (c - 1)^2 c^{n-3} + \dots + (c - 1)^{n-1}$$

The equation must be divided by $(c - k)$ for the both sides,

k is a root of polynomial at right side.

Ref. Remainder theorem, $k^{n-1} + (k - 1)k^{n-2} + (k - 1)^2 k^{n-3} + \dots + (k - 1)^{n-1} = 0$

But $k^{n-1} + (k - 1)k^{n-2} + (k - 1)^2 k^{n-3} + \dots + (k - 1)^{n-1} > 0$ always for $1 < k < c$

So k isn't an integer, if k isn't an integer then a won't an integer too.

But a must be integer, it is contradiction. So I can say…

$a^n + b^n \neq c^n$ for every positive integer a , b , c and $n > 2$