Elementary Proof of Fermat's Last Theorem

โดย

ศตวรรษ สันติสุรัตน์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

วิศวกรรมเครื่องกล ประเทศไทย

E-mail : sattawatsuntisurat@gmail.com

23 ธันวาคม 2563

Abstract: Proof of Fermat's last theorem by using basic of algebra.

จากทฤษฎีบทสุดท้ายของแฟมาร์

$a^n + b^n \neq c^n$, ไม่มีจำนวนเต็มบวก a , b , c ใดๆ ที่ทำให้สมการเป็นจริง เมื่อ $n > 2$

เริ่มการพิสูจน์

สมมุติให้มีจำนวนเต็มบวก a , b , c ที่ทำให้ $a^n + b^n = c^n$ เป็นจริง และให้ n เป็นจำนวนเต็มบวก

และ a , b , c ไม่มีตัวประกอบใดๆร่วมกัน

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

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

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

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

โดยที่ $K = c^{n-2} + 2b\,c^{n-3} + 3b^2 c^{n-4} + \ldots + (n-1)b^{n-2}$ และ $c - b \neq 1$

สมมุติให้ a เป็นจำนวนเฉพาะ

ถ้า a เป็นจำนวนเฉพาะ ก็จะทำให้ $(c - b) = a^k$, $k \geq 1$

แต่เนื่องจาก $a + b > c$ =====> $a > c - b$ ซึ่งขัดแย้งกัน ดังนั้น a จึงไม่ใช่จำนวนเฉพาะ

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

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

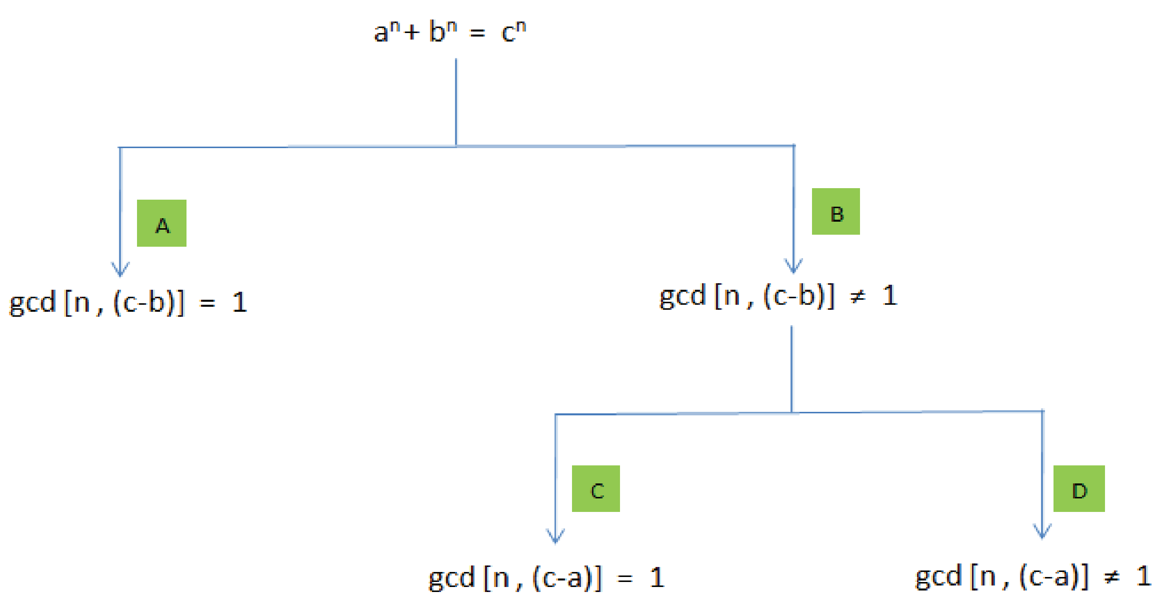
สมมุติให้ b เป็นจำนวนเฉพาะ

ถ้า b เป็นจำนวนเฉพาะ ก็จะทำให้ $(c - a) = b^k$, $k \geq 1$

แต่เนื่องจาก $a + b > c$ =====> $b > c - a$ ซึ่งขัดแย้งกัน ดังนั้น b จึงไม่ใช่จำนวนเฉพาะ

สรุปว่า ทั้ง a และ c ไม่ใช่จำนวนเฉพาะ แต่เป็นจำนวนประกอบ

ต่อไปจะเข้าสู่แนวทางการพิสูจน์ ตามรูปด้านล่างนี้



จะเริ่มพิจารณาทีละขั้นตอน โดยเริ่มจาก ขั้นตอนที่ A , B , C , D ตามลำดับ

พิจารณาที่จุด A , gcd [n, (c-b)] = 1

คือให้ n กับ (c-b) ไม่มีตัวประกอบร่วมกันเลย ถ้าเป็นอย่างนั้น จะสามารถเขียนสมการใหม่ได้ตามด้านล่างนี้

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

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

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

แล้ว b^n ต้องหารด้วย $(k^n + b - mk)$ ลงตัว

ดังนั้นจากทฤษฎีเศษเหลือ จะได้ว่า $(mk - k^n)^n = 0$

$k^{n-1} = m$ ซึ่งไม่จริง เพราะ $\gcd(m, k) = 1$

ดังนั้นที่จุด A นี้ สรุปได้ว่า $a^n + b^n \neq c^n$

พูดง่ายๆก็คือ ไม่มีจำนวนเต็มบวก a , b , c ใดๆที่ทำให้สมการเป็นจริง ถ้า n ไม่มีตัวประกอบร่วมกันกับ (c-b) เลย

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

คือให้ n กับ (c-b) มีตัวประกอบร่วมกัน ซึ่งก็อาจทำให้สมการ $a^n + b^n = c^n$ เป็นจริงได้

ดังนั้นที่จุด B นี้ สรุปได้ว่า ถ้าจะทำให้สมการเป็นจริงนั้น n ต้องมีตัวประกอบร่วมกันกับ (c-b) อย่างน้อยหนึ่งตัว

พิจารณาที่จุด C, $\gcd[n, (c-a)] = 1$

คือให้ n กับ (c-a) ไม่มีตัวประกอบร่วมกันเลย ถ้าเป็นอย่างนั้น จะสามารถเขียนสมการใหม่ได้ตามด้านล่างนี้

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

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

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

ดูแล้ว a^n ต้องหารด้วย $(p^n + a - pq)$ ลงตัว

ดังนั้นจากทฤษฎีเศษเหลือ จะได้ว่า $(pq - p^n)^n = 0$

$p^{n-1} = q$ ซึ่งไม่จริง เพราะ $\gcd(p, q) = 1$

ดังนั้นที่จุด C นี้ สรุปได้ว่า $a^n + b^n \neq c^n$

ก็คือว่า ไม่มีจำนวนเต็มบวก a , b , c ใดๆที่ทำให้สมการเป็นจริง เมื่อ n ไม่มีตัวประกอบร่วมกันกับ (c-a) เลย

จากข้อสรุปของจุด B กับจุด C เมื่อพิจารณาร่วมกันจะพบว่า ถ้าจะทำให้สมการ $a^n + b^n = c^n$ เป็นจริง

n ต้องมีตัวประกอบร่วมกันกับ (c-b) และ (c-a) อย่างน้อยอย่างละหนึ่งตัว

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

คือให้ n กับ (c-a) มีตัวประกอบร่วมกันอย่างน้อยหนึ่งตัว ซึ่งก็อาจทำให้สมการ $a^n + b^n = c^n$ เป็นจริงได้

จากข้อสรุปที่ผ่านมา เรารู้ว่า n ต้องมีตัวประกอบร่วมกันกับ (c-b) และ (c-a) อย่างน้อยอย่างละหนึ่งตัว

ทำให้ได้สมการที่เป็นไปได้คือ

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

เมื่อ f(c-a) คือตัวประกอบของ (c-a) , f(c-b) คือตัวประกอบของ (c-b) และ N คือจำนวนเต็มใดๆ

จัดรูปสมการใหม่ $(a^{f(c-a)})^{f(c-b)N} + (b^{f(c-a)})^{f(c-b)N} = (c^{f(c-a)})^{f(c-b)N}$

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

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

จากข้อสรุปที่ผ่านมา ทำให้ทราบว่า f(c-b)N ต้องมีตัวประกอบร่วมกับ C - A อย่างน้อยหนึ่งตัว

$$C - A = (c-a)(c^{f(c-a)-1} + a\,c^{f(c-a)-2} + a^2 c^{f(c-a)-3} + \dots + a^{f(c-a)-1}) \qquad \text{(2)}$$

เมื่อพิจารณาจากสมการ (2) แล้ว พบว่า f(c-b)N ไม่มีตัวประกอบใดๆร่วมกันกับ C – A เลย ทำให้สมการ (1) ไม่เกิดขึ้นจริงด้วย เพราะฉะนั้นจึงสามารถสรุปได้แล้วว่า

$a^n + b^n \neq c^n$ เมื่อ a , b , c เป็นจำนวนเต็มบวกใดๆ เมื่อ $n > 2$ เมื่อ $c - a \neq 1$ หรือ $c - b \neq 1$

ยังมีอีกหนึ่งกรณีที่ต้องนำมาพิจารณา เพื่อให้บทพิสูจน์สมบูรณ์แบบ คือ กรณีที่ $a = c - 1$ หรือ $b = c - 1$

เพราะจะทำให้พิสูจน์แบบวิธีข้างต้นไม่ได้ จำเป็นต้องพิสูจน์ด้วยวิธีที่ต่างออกไป

สมมุติให้ $a^n + b^n = c^n$ เมื่อ a , b , c เป็นจำนวนเต็มบวก และ $n > 2$

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

กำหนดให้ $a = c - k$ เมื่อ $1 < k < c$ และ k เป็นจำนวนเต็ม

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

ต้องหารด้วย $(c - k)$ แล้วลงตัวทั้งสองข้างของสมการ ถ้าหารลงตัวแล้ว k ก็คือรากของสมการทางขวามือนั่นเอง

จากทฤษฎีเศษเหลือจะได้ว่า $k^{n-1} + (k - 1)\, k^{n-2} + (k - 1)^2\, k^{n-3} + \ldots + (k - 1)^{n-1} = 0$

จะเห็นได้ว่า เมื่อ k เป็นจำนวนเต็มบวกที่มากกว่าหนึ่ง จะไม่ทำให้สมการเป็นจริงได้เลย ดังนั้น k ต้องไม่ใช่จำนวนเต็ม

เมื่อ k ไม่ใช่จำนวนเต็ม ก็ทำให้ a ไม่ใช่จำนวนเต็มไปด้วย ซึ่งขัดแย้งกับสมการ ทำให้สมการไม่เกิดขึ้นจริง

ดังนั้นสรุปได้ว่า

$a^n + b^n \neq c^n$ เมื่อ a , b , c เป็นจำนวนเต็มบวกใดๆ และ $n > 2$