

Một số định lý dùng cho chứng minh FLT

Định lý 2.1 Nếu a, b, m và n là những số nguyên, và nếu $c|a$ và $c|b$ thì $c|ma + nb$

Định lý 2.2 Nếu a, b và k là những số nguyên thì $GDC(a + kb, b) = GDC(a, b)$.

Hệ quả 2.2.1 Nếu $GDC(a, b) = 1$ thì $GDC(a + b, b) = GDC(a - b, b) = 1$.

Định lý 2.3 Nếu $GDC(a, b) = 1$ và $c|a$ thì $GDC(c, b) = 1$.

Định lý 2.4 Nếu a, b và c là những số nguyên sao cho $GCD(a, b) = 1$ và $a|bc$, thì $a|c$.

Định lý 2.5 Nếu a, b và c là những số nguyên sao cho $GDC(a, b) = GCD(a, c) = 1$ thì $GDC(a, bc) = 1$.

Hệ quả 2.5.1 Nếu $GDC(a, b) = 1$ và n, m là những số nguyên tự nhiên thì $GDC(a^n, b^m) = 1$.

Định lý 2.6 Nếu a, b là những số nguyên dương sao cho $a|b$ và $b|a$ thì $a = b$.

Định lý 2.7 Nếu a, b là 2 số chẵn lẻ khác nhau và $GDC(a, b) = 1$ thì $GDC(a + b, a - b) = 1$.

Định lý 2.8 Nếu a, b đều lẻ và $GDC(a, b) = 1$ thì $GDC(\frac{a+b}{2}, \frac{a-b}{2}) = 1$.

Định lý 2.9 Nếu a, b đều lẻ và $GDC(\frac{a+b}{2}, \frac{a-b}{2}) = 1$ thì $GDC(a, b) = 1$.

Định lý 2.10 Nếu a, b đều lẻ và $GDC(a, b) = 1$ thì $GDC(ab, \frac{a^2 + b^2}{2}) = 1$.

Định lý 2.11 Nếu $GCD(a, b) = 1$ và n, m là những số nguyên tự nhiên thì $GCD((a + b)^n, b^m) = 1$ and $GCD((a - b)^n, b^m) = 1$.

Định lý 2.12. Nếu a, b chẵn lẻ khác nhau và $GDC(a, b) = 1$ và n là một số nguyên tự nhiên thì $GDC(a^n + b^n, a^n - b^n) = 1$.

Định lý 2.13 Nếu k là một số nguyên tự nhiên lẻ và m là một số nguyên tự nhiên thì $a^m + b^m$ là một ước số của $a^{km} + b^{km}$

Định lý 2.14 Nếu k là một số nguyên tự nhiên chẵn và m là một số nguyên tự nhiên thì $a^m + b^m$ là một ước số của $a^{km} - b^{km}$.

Định lý 2.15 Cho phương trình $a_0x^m + a_1x^{m-1} + \dots + a_{m-1}x + a_m = 0$ (1), trong đó m là một số nguyên tự nhiên và $a_0, a_1, \dots, a_m$ là những số nguyên với $a_0 \neq 0$ và $a_m \neq 0$.

Nếu $\frac{k}{s}$ là một nghiệm hữu tỷ của phương trình (1), trong đó s là một số nguyên tự nhiên, k là một số nguyên và $GCD(k, s) = 1$ thì k và s lần lượt là ước số của a_m và a_0

Định lý 2.16 Cho $x^2 + y^2 + z^2 = m^2$ với z lẻ và $GCD(x, y, z) = 1$, tồn tại các số nguyên u, v, w và t sao cho

$$\begin{aligned} x &= 2(uw - vt) \\ y &= 2(ut + vw) \\ z^2 &= u^2 + v^2 - w^2 - t^2 \\ m^2 &= u^2 + v^2 + w^2 + t^2 \end{aligned} \quad (2.1)$$

Fermat's Last Theorem

Không có điểm hữu tỷ khác zero trên đường cong $x^n + y^n - 1 = 0$ với bất kỳ số nguyên $n > 2$.

Chứng minh

Rõ ràng nếu FLT đúng với n nào đó thì nó cũng sẽ đúng với mọi số mũ là bội số của n . Bởi vì mọi số nguyên n lớn hơn 2 đều chia hết cho 4 hay cho một số lẻ nào đó cho nên chúng ta chỉ cần chứng minh định lý khi n là một số lẻ bất kỳ lớn hơn 2 và khi $n = 4$.

Chúng ta sẽ chứng minh FLT bằng phản chứng, nghĩa là chúng ta sẽ giả định tồn tại một điểm hữu tỷ khác zero nào đó trên đường cong $x^n + y^n - 1 = 0$ sau đó chỉ ra rằng điều này dẫn đến một phương trình bậc 2 mà cả hai nghiệm của nó đều bị loại bởi tính vô lý của chúng.

Giả sử rằng với n là một số lẻ bất kỳ lớn hơn 2 hay $n = 4$, tồn tại một điểm hữu tỷ khác zero nào đó $M_0(x_0, y_0)$ trên đường cong $(L): x^n + y^n - 1 = 0$. Không mất tính tổng quát, giả sử $x_0 = \frac{a}{c}$, $y_0 = \frac{b}{c}$, với a, b, c là những số nguyên khác zero và nguyên tố cùng nhau.

Vì $GCD(a, b) = 1$ nên chỉ có thể tồn tại hai trường hợp:

Trường hợp 1: Hai số a, b chẵn lẻ khác nhau.

Trường hợp 2: Cả hai số a, b đều lẻ.

Chúng ta nhận xét trường hợp 2 như sau:

Với n là một số lẻ bất kỳ lớn hơn 2, nếu $a^n + b^n = c^n$ thì ta có $a^n = c^n + (-b)^n$. Đặt $A = c$, $B = -b$, $C = a$ thì $A^n + B^n = C^n$, trong đó A, B là chẵn lẻ khác nhau. Đây là trường hợp 1.

Nếu $a^4 + b^4 = c^4$ thì c chẵn. Đặt $c = 2u$, trong đó u là một số nguyên khác zero thì $a^4 + b^4 = (2u)^4$ hay $\frac{a^4 + b^4}{2} = 8u^4$. Điều này vô lý bởi vì $\frac{a^4 + b^4}{2}$ là một số lẻ trong khi $8u^4$ là một số chẵn.

Vì vậy, chúng ta chỉ quan tâm trường hợp 1. Từ đây về sau chúng ta giả sử rằng a, b là hai số chẵn lẻ khác nhau và nguyên tố sánh đôi.

Đặt $m = \frac{x_0}{y_0} = \frac{a}{b}$ thì dễ thấy $m \neq 0, m \neq 1$ and $m \neq -1$.

Trong mặt phẳng Oxy , nếu gọi (Δ) là tiếp tuyến với (L) tại $M_0(x_0, y_0)$, (C) là vòng tròn tâm O đi qua $M_0(x_0, y_0)$, (δ) là tiếp tuyến với (C) tại $M_0(x_0, y_0)$ thì phương trình của (Δ) và (δ) lần lượt là $y = -m^{n-1}(x - x_0) + y_0$, $y = -m(x - x_0) + y_0$. Chúng ta sẽ khảo sát sự tương giao của đường thẳng (Δ) và vòng tròn (C) .

Nếu đường thẳng (Δ) trùng với đường thẳng (δ) thì

$$-m^{n-1} = -m \quad (3.1)$$

hay

$$m^{n-2} - 1 = 0 \quad (3.2)$$

Bởi định lý 2.15, nghiệm hữu tỷ của phương trình (3.2), nếu tồn tại, chỉ có thể là $m = 1$ hay $m = -1$ nên đường thẳng (Δ) phải cắt vòng tròn (C) tại hai điểm phân biệt $M_0(x_0, y_0)$ và $M_1(x_1, y_1)$ sao cho

$$x_1 = \frac{(m^{2n-2} - 1)x_0 + 2m^{n-1}y_0}{m^{2n-2} + 1} \quad (3.3)$$

$$y_1 = \frac{2m^{n-1}x_0 + (1 - m^{2n-2})y_0}{m^{2n-2} + 1} \quad (3.4)$$

Từ (3.3), (3.4) và $y_0 \neq 0$,

$$\frac{x_1}{y_0} = \frac{m^{2n-1} + 2m^{n-1} - m}{m^{2n-2} + 1} \quad (3.5)$$

$$\frac{y_1}{y_0} = \frac{-m^{2n-2} + 2m^n + 1}{m^{2n-2} + 1} \quad (3.6)$$

Nếu $x_1 = 0$ thì $m^{2n-2} + 2m^{n-1} - 1 = 0$.

Nếu $y_1 = 0$ thì $m^{2n-2} - 2m^n - 1 = 0$.

Hai phương trình này không có nghiệm hữu tỷ. Vì vậy $x_1 \neq 0$ và $y_1 \neq 0$.

Đặt $\frac{x_1}{y_0} = \frac{d}{e}$ và $\frac{y_1}{y_0} = \frac{r}{s}$, trong đó d, e, r, s là những số nguyên khác zero sao cho $GCD(d, e) = 1$ và $GCD(r, s) = 1$. Từ (3.5) và (3.6), chúng ta có hệ phương trình sau:

$$em^{2n-1} - dm^{2n-2} + 2em^{n-1} - em - d = 0 \quad (3.7)$$

$$(r+s)m^{2n-2} - 2sm^n + r - s = 0 \quad (3.8)$$

Vì $m = \frac{a}{b}$ là một nghiệm hữu tỷ của phương trình (3.7), bởi định lý 2.15, ta có $d = pa$ và $e = qb$, trong đó p, q là những số nguyên khác zero và $GCD(p, q) = 1$. Do đó,

$$\frac{d}{e} = \frac{pa}{qb} = \frac{p}{q} m = \frac{m^{2n-1} + 2m^{n-1} - m}{m^{2n-2} + 1} \quad (3.9)$$

Khử $m \neq 0$ ở hai vế phương trình (3.9) ta được

$$\frac{p}{q} = \frac{m^{2n-2} + 2m^{n-2} - 1}{m^{2n-2} + 1} \quad (3.10)$$

hay

$$(p-q)m^{2n-2} - 2qm^{n-2} + p + q = 0 \quad (3.11)$$

Nếu $r+s=0$ thì từ (3.8) ta có

$$m^n + 1 = 0 \quad (3.12)$$

Nếu $r-s=0$ thì từ (3.8) ta có

$$m^{n-2} - 1 = 0 \quad (3.13)$$

Nếu $p+q=0$ thì từ (3.11) ta có

$$m^n + 1 = 0 \quad (3.14)$$

Nếu $p-q=0$ thì từ (3.11) ta có

$$m^{n-2} - 1 = 0 \quad (3.15)$$

Nghiệm hữu tỷ của bốn phương trình này, nếu tồn tại, chỉ có thể là $m=1$ hay $m=-1$. Do đó $r+s, r-s, p+q$ và $p-q$ phải là những số nguyên khác zero.

Từ (3.8) và (3.11),

$$2sm^n = (r+s)m^{2n-2} + r - s \quad (3.16)$$

$$2qm^{n-2} = (p-q)m^{2n-2} + p + q \quad (3.17)$$

Nhân vế với vế của hai phương trình (3.16), (3.17),

$$4sqm^{2n-2} = \{(r+s)m^{2n-2} + r - s\} \{(p-q)m^{2n-2} + p + q\} \quad (3.18)$$

Đặt $m^{2n-2} = t$ thì do $(p-q)(r+s) \neq 0$, phương trình (3.18) có thể được viết lại như là một phương trình bậc hai của ẩn t

$$(p-q)(r+s)t^2 + 2(pr-qs)t + (p+q)(r-s) = 0 \quad (3.19)$$

Hai nghiệm của phương trình (3.19) là

$$t_1 = -1 \quad (3.20)$$

và

$$t_2 = \frac{(p+q)(s-r)}{(p-q)(s+r)} \quad (3.21)$$

Nếu $t = t_1$, điều này dẫn đến $m^{2n-2} + 1 = 0$. Do phương trình này không có nghiệm hữu tỷ nên nghiệm thứ nhất bị loại bỏ. Kế tiếp, chúng ta sẽ chỉ ra rằng nghiệm thứ hai cũng bị loại bỏ bằng cách chứng minh rằng nó sẽ dẫn đến sự kiện $4a^{n-1}b^{n-1}(a^{n-2} - b^{n-2})(a^n + b^n)$ không phải là một số nguyên. Thực vậy, nếu $t = t_2$ thì từ (3.16) và (3.17) ta thu được

$$m^n = \frac{q(s-r)}{s(p-q)} \quad (3.22)$$

$$m^{n-2} = \frac{s(p+q)}{q(s+r)} \quad (3.23)$$

Chia vế với vế của hai phương trình (3.22), (3.23),

$$m^2 = \frac{q^2(s^2 - r^2)}{s^2(p^2 - q^2)} \quad (3.24)$$

Nâng cả hai vế của phương trình (3.24) đến lũy thừa $2(n-1)$,

$$m^{2(n-1)} = \frac{q^{2(n-1)}(s+r)^{n-1}(s-r)^{n-1}}{s^{2(n-1)}(p+q)^{n-1}(p-q)^{n-1}} \quad (3.25)$$

Từ (3.21) và (3.25),

$$\frac{(p+q)(s-r)}{(p-q)(s+r)} = \frac{q^{2(n-1)}(s+r)^{n-1}(s-r)^{n-1}}{s^{2(n-1)}(p+q)^{n-1}(p-q)^{n-1}} \quad (3.26)$$

hay

$$s^{2(n-1)}(p+q)^n(p-q)^{n-2} = q^{2(n-1)}(s+r)^n(s-r)^{n-2} \quad (3.27)$$

Từ $GCD(p, q) = 1$, bởi định lý 2.11, ta có $GCD((p+q)^n, q^{2n-2}) = 1$ và $GCD((p-q)^{n-2}, q^{2n-2}) = 1$. Vì thế từ (3.27), bởi định lý 2.4, suy ra $q^{2(n-1)}$ là một ước số của $s^{2(n-1)}$. Hơn nữa, từ $GCD(s, r) = 1$, ta có $GCD((s+r)^n, s^{2n-2}) = 1$ và $GCD((s-r)^{n-2}, s^{2n-2}) = 1$. Vì thế từ (3.27), bởi định lý 2.4, suy ra $s^{2(n-1)}$ là một ước số của $q^{2(n-1)}$. Từ những kết quả này, bởi định lý 2.6, $s^{2(n-1)} = q^{2(n-1)}$. Chú ý rằng đối với các phân số $\frac{p}{q}$ và $\frac{r}{s}$ chúng ta luôn

luôn có thể giả sử rằng p, r là những số nguyên khác zero và q, s là những số nguyên dương vì vai trò của $-p, -r$ là tương tự như vai trò của p, r . Vì vậy từ $s^{2(n-1)} = q^{2(n-1)}$ ta có $s = q$.

Do đó từ $t = m^{2n-2} = \frac{a^{2n-2}}{b^{2n-2}}$, biểu thức (3.21) trở thành

$$-a^{2n-2}(p-q)(q+r) + b^{2n-2}(p+q)(q-r) = 0 \quad (3.28)$$

Đặt $b^{n-1} = a^{n-1} + f$, trong đó f là một số nguyên khác zero thì phương trình (3.28) trở thành

$$(p+q)(q-r)f^2 + 2a^{n-1}(p+q)(q-r)f + a^{2n-2}\{(p+q)(q-r) - (p-q)(q+r)\} = 0 \quad (3.29)$$

Vì $(p+q)(q-r) \neq 0$, biểu thức (3.29) có thể được xem như là một phương trình bậc hai của ẩn f . Vì f là một số nguyên khác zero, biệt thức của phương trình (3.29) phải là bình phương của một số nguyên khác zero (do $p \neq q, q \neq r$). Điều này có nghĩa là

$$(p^2 - q^2)(q^2 - r^2) = g^2 \quad (3.30)$$

trong đó g là một số nguyên khác zero nào đó.

Mặt khác, thay $m = \frac{a}{b}$ vào (3.10) và (3.6) ta được

$$\frac{p}{q} = \frac{m^{2n-2} + 2m^{n-2} - 1}{m^{2n-2} + 1} = \frac{a^{2n-2} + 2a^{n-2}b^n - b^{2n-2}}{a^{2n-2} + b^{2n-2}} \quad (3.31)$$

$$\frac{r}{q} = \frac{-m^{2n-2} + 2m^n + 1}{m^{2n-2} + 1} = \frac{-a^{2n-2} + 2a^n b^{n-2} + b^{2n-2}}{a^{2n-2} + b^{2n-2}} \quad (3.32)$$

Từ đây suy ra,

$$p+r = \frac{2a^{n-2}b^{n-2}(a^2 + b^2)q}{a^{2n-2} + b^{2n-2}} \quad (3.33)$$

$$p-r = \frac{2(a^{n-2} - b^{n-2})(a^n + b^n)q}{a^{2n-2} + b^{2n-2}} \quad (3.34)$$

Rõ ràng $p+r$ and $p-r$ là những số nguyên khác zero.

Với n là một số lẻ lớn hơn 2, vì $GCD(a^{2n-2} - b^{2n-2}, a^{2n-2} + b^{2n-2}) = 1$ và, bởi định lý 2.14, $a^2 + b^2$ là một ước số của $a^{2n-2} - b^{2n-2}$, ta có $GCD(a^2 + b^2, a^{2n-2} + b^{2n-2}) = 1$ bởi định lý 2.3. Từ (3.33) suy ra $a^{2n-2} + b^{2n-2}$ là một ước số của q . Hơn nữa, từ (3.31) và $GCD(p, q) = 1$ ta có q là một ước số của $a^{2n-2} + b^{2n-2}$. Vì thế, bởi định lý 2.6

$$q = a^{2n-2} + b^{2n-2} \quad (3.35)$$

Từ (3.33), (3.34) và (3.35) ta tìm được

$$p+r = 2a^{n-2}b^{n-2}(a^2 + b^2) \quad (3.36)$$

$$p-r = 2(a^{n-2} - b^{n-2})(a^n + b^n) \quad (3.37)$$

Rõ ràng tất cả các số p, q, r và $\frac{p^2+r^2}{2}$ đều lẻ.

Mặt khác nếu xem (3.28) và (3.35) như là một hệ hai phương trình tuyến tính hai ẩn a^{2n-2} , b^{2n-2} và giải ra ta được

$$a^{2n-2} = \frac{(p+q)(q-r)}{2(p-r)} \quad (3.38)$$

$$b^{2n-2} = \frac{(p-q)(q+r)}{2(p-r)} \quad (3.39)$$

Nhân vế với vế hai biểu thức (3.38), (3.39),

$$a^{2n-2}b^{2n-2} = \frac{(p^2-q^2)(q^2-r^2)}{4(p-r)^2} \quad (3.40)$$

rồi nhân cả hai vế của biểu thức (3.40) với $4(p-r)^2 \neq 0$ ta được

$$(p^2-q^2)(q^2-r^2) = \{2(p-r)a^{n-1}b^{n-1}\}^2 \quad (3.41)$$

Thay giá trị của $p-r$ ở trên vào (3.41),

$$(p^2-q^2)(q^2-r^2) = \{4a^{n-1}b^{n-1}(a^{n-2}-b^{n-2})(a^n+b^n)\}^2 \quad (3.42)$$

Bây giờ chúng ta hãy viết lại điều kiện (3.30) như là

$$g^2 + (q^2 - \frac{p^2+r^2}{2})^2 + (pr)^2 = (\frac{p^2+r^2}{2})^2 \quad (3.43)$$

Nếu $q^2 - \frac{p^2+r^2}{2} = 0$, nghĩa là $p^2 - q^2 = q^2 - r^2$, thì từ (3.24) suy ra $m^2 = 1$. Điều này trái với giả thiết ở trên.

Nếu $q^2 - \frac{p^2+r^2}{2} \neq 0$ thì bộ bốn $\left[g, q^2 - \frac{p^2+r^2}{2}, pr, \frac{p^2+r^2}{2} \right]$ sẽ là một bộ nghiệm nguyên của phương trình $x^2 + y^2 + z^2 = w^2$.

Vì $a^2 + b^2$, $a^{n-2} - b^{n-2}$ lần lượt là các ước số của $a^{2n-4} + b^{2n-4}$, $a^{2n-4} - b^{2n-4}$ và $GCD(a^{2n-4} + b^{2n-4}, a^{2n-4} - b^{2n-4}) = 1$, ta có $GCD(a^2 + b^2, a^{n-2} - b^{n-2}) = 1$. Hơn nữa, vì $a^2 + b^2$, $a^n + b^n$ lần lượt là các ước số của $a^{2n} + b^{2n}$, $a^{2n} - b^{2n}$ và $GCD(a^{2n} + b^{2n}, a^{2n} - b^{2n}) = 1$, ta có $GCD(a^2 + b^2, a^n + b^n) = 1$. Vì vậy, ta có $GCD(\frac{p+r}{2}, \frac{p-r}{2}) = 1$. Điều này dẫn đến $GCD(p, r) = 1$. Bởi định lý 2.10, ta có $GCD(pr, \frac{p^2+r^2}{2}) = 1$. Vì vậy, bởi định lý 2.16, tồn tại các số nguyên i, j, k, l sao cho

$$g = 2(jk + il) \quad (3.44)$$

$$q^2 - \frac{p^2 + r^2}{2} = 2(ik - jl) \quad (3.45)$$

$$pr = i^2 + j^2 - k^2 - l^2 \quad (3.46)$$

$$\frac{p^2 + r^2}{2} = i^2 + j^2 + k^2 + l^2 \quad (3.47)$$

Cộng vế với vế hai biểu thức (3.46), (3.47) rồi chia cả hai vế của phương trình nhận được cho 2,

$$\left(\frac{p+r}{2}\right)^2 = i^2 + j^2 \quad (3.48)$$

Xem (3.44) và (3.45) như là một hệ hai phương trình tuyến tính của hai ẩn k, l và giải ra ta được

$$k = \frac{\frac{2q^2 - p^2 - r^2}{4}i + \frac{g}{2}j}{i^2 + j^2} \quad (3.49)$$

$$l = \frac{\frac{g}{2}i - \frac{2q^2 - p^2 - r^2}{4}j}{i^2 + j^2} \quad (3.50)$$

Từ (3.36) và (3.37) ta tìm được

$$\left(\frac{p+r}{2}\right)^2 = a^{2n-4}b^{2n-4}(a^2 + b^2)^2 \quad (3.51)$$

$$\frac{2q^2 - p^2 - r^2}{4} = \frac{2q^2 - \left\{\frac{(p+r)^2 + (p-r)^2}{2}\right\}}{4} = a^{n-2}b^{n-2}(a^{n-2} - b^{n-2})(a^n + b^n)(a^2 - b^2) \quad (3.52)$$

Từ (3.30) và (3.42), ta thu được

$$\left\{4a^{n-1}b^{n-1}(a^{n-2} - b^{n-2})(a^n + b^n) - g\right\}\left\{4a^{n-1}b^{n-1}(a^{n-2} - b^{n-2})(a^n + b^n) + g\right\} = 0 \quad (3.53)$$

Nếu $4a^{n-1}b^{n-1}(a^{n-2} - b^{n-2})(a^n + b^n) = g$ thì từ (3.48), (3.49), (3.50) (3.51) and (3.52) ta tìm được

$$k = \frac{(a^{n-2} - b^{n-2})(a^n + b^n)\{(a^2 - b^2)i + 2abj\}}{a^{n-2}b^{n-2}(a^2 + b^2)^2} \quad (3.54)$$

$$l = \frac{(a^{n-2} - b^{n-2})(a^n + b^n)\{2abi - (a^2 - b^2)j\}}{a^{n-2}b^{n-2}(a^2 + b^2)^2} \quad (3.55)$$

Vì $GCD((a^{n-2} - b^{n-2})(a^n + b^n), a^{n-2}b^{n-2}(a^2 + b^2)^2) = 1$, từ (3.54), (3.55) bởi định lý 2.4 ta có

$$(a^2 - b^2)i + 2abj = h_1 a^{n-2} b^{n-2} (a^2 + b^2)^2 \quad (3.56)$$

$$2abi - (a^2 - b^2)j = h_2 a^{n-2} b^{n-2} (a^2 + b^2)^2 \quad (3.57)$$

trong đó h_1 và h_2 là những số nguyên khác zero.

Bình phương cả hai vế của biểu thức (3.56),

$$\{(a^2 - b^2)i\}^2 + 2(2abj)\{(a^2 - b^2)i\} + (2abj)^2 = h_1^2 a^{2n-4} b^{2n-4} (a^2 + b^2)^4 \quad (3.58)$$

Bình phương cả hai vế của biểu thức (3.57),

$$(2abi)^2 - 2(2abi)\{(a^2 - b^2)j\} + \{(a^2 - b^2)j\}^2 = h_2^2 a^{2n-4} b^{2n-4} (a^2 + b^2)^4 \quad (3.59)$$

Cộng vế với vế hai biểu thức (3.58), (3.59),

$$\{(2ab)^2 + (a^2 - b^2)^2\}(i^2 + j^2) = (h_1^2 + h_2^2) a^{2n-4} b^{2n-4} (a^2 + b^2)^4 \quad (3.60)$$

Từ (3.48), (3.51) and (3.60), chúng ta dễ tìm ra

$$h_1^2 + h_2^2 = 1 \quad (3.61)$$

Điều này vô lý !!!

Nếu $4a^{n-1}b^{n-1}(a^{n-2} - b^{n-2})(a^n + b^n) = -g$ thì từ (3.48), (3.49), (3.50) (3.51) and (3.52) ta tìm được

$$k = \frac{(a^{n-2} - b^{n-2})(a^n + b^n)\{(a^2 - b^2)i - 2abj\}}{a^{n-2}b^{n-2}(a^2 + b^2)^2} \quad (3.62)$$

$$l = \frac{-(a^{n-2} - b^{n-2})(a^n + b^n)\{2abi + (a^2 - b^2)j\}}{a^{n-2}b^{n-2}(a^2 + b^2)^2} \quad (3.63)$$

Vì $GCD((a^{n-2} - b^{n-2})(a^n + b^n), a^{n-2}b^{n-2}(a^2 + b^2)^2) = 1$, từ (3.62), (3.63) bởi định lý 2.4 ta có

$$(a^2 - b^2)i - 2abj = h_3 a^{n-2} b^{n-2} (a^2 + b^2)^2 \quad (3.64)$$

$$2abi + (a^2 - b^2)j = h_4 a^{n-2} b^{n-2} (a^2 + b^2)^2 \quad (3.65)$$

trong đó h_3 và h_4 là những số nguyên khác zero.

Bình phương cả hai vế của biểu thức (3.64),

$$\{(a^2 - b^2)i\}^2 - 2(2abj)\{(a^2 - b^2)i\} + (2abj)^2 = h_3^2 a^{2n-4} b^{2n-4} (a^2 + b^2)^4 \quad (3.66)$$

Bình phương cả hai vế của biểu thức (3.65),

$$(2abi)^2 + 2(2abi)\{(a^2 - b^2)j\} + \{(a^2 - b^2)j\}^2 = h_4^2 a^{2n-4} b^{2n-4} (a^2 + b^2)^4 \quad (3.67)$$

Cộng về với về hai biểu thức, (3.66), (3.67),

$$\{(2ab)^2 + (a^2 - b^2)^2\}(i^2 + j^2) = (h_3^2 + h_4^2) a^{2n-4} b^{2n-4} (a^2 + b^2)^4 \quad (3.68)$$

Từ (3.48), (3.51) and (3.68), chúng ta dễ tìm ra

$$h_3^2 + h_4^2 = 1 \quad (3.69)$$

Điều này vô lý !!!

Với $n = 4$, (3.31), (3.33) và (3.34) trở thành,

$$\frac{p}{q} = \frac{a^6 + 2a^2b^4 - b^6}{a^6 + b^6} \quad (3.70)$$

$$p + r = \frac{2a^2b^2(a^2 + b^2)q}{a^6 + b^6} \quad (3.71)$$

$$p - r = \frac{2(a^2 - b^2)(a^4 + b^4)q}{a^6 + b^6} \quad (3.72)$$

Vì $a^2 - b^2$ là một ước số của $a^6 - b^6$ và $GCD(a^6 - b^6, a^6 + b^6) = 1$, ta có $GCD(a^2 - b^2, a^6 + b^6) = 1$. Hơn nữa, vì $a^4 + b^4$, $a^6 + b^6$ lần lượt là các ước số của $a^{12} + b^{12}$, $a^{12} - b^{12}$ và $GCD(a^{12} - b^{12}, a^{12} + b^{12}) = 1$, ta có $GCD(a^4 + b^4, a^6 + b^6) = 1$. Từ (3.72) suy ra $a^6 + b^6$ là một ước số của q . Hơn nữa, từ (3.70) và $GCD(p, q) = 1$, ta thấy q là một ước số của $a^6 + b^6$. Vì vậy, bởi định lý 2.6 ta có

$$q = a^6 + b^6 \quad (3.73)$$

Từ (3.71), (3.72) và (3.73) chúng ta tìm ra

$$p + r = 2a^2b^2(a^2 + b^2) \quad (3.74)$$

$$p - r = 2(a^2 - b^2)(a^4 + b^4) \quad (3.75)$$

Rõ ràng $GCD(\frac{p+r}{2}, \frac{p-r}{2}) = 1$. Điều này dẫn đến $GCD(p, r) = 1$. Bởi định lý 2.10, ta có

$GCD(pr, \frac{p^2 + r^2}{2}) = 1$. Tương tự, trường hợp này cũng dẫn đến mâu thuẫn bởi những lập luận đã được dùng trong chứng minh của trường hợp trước.

Định lý đã được chứng minh $\square$