

CHỨNG MINH ĐỊNH LÝ LỚN FERMAT

Tôn Thất Hiệp, g/v THPT Phan Đăng Lưu, Phú Vang, Thừa Thiên Huế. Email: tonthathiep.pdlhue@gmail.com

Nhà toán học Pháp Pierre de Fermat (1601–1665) đã đưa ra một định lý nổi tiếng: **“phương trình $x^n + y^n = z^n$, trong đó số nguyên n lớn hơn 2 không thể tìm được nghiệm (nguyên khác không) nào”**. Đó là định lý Fermat cuối cùng. Ông ghi bên lề một cuốn sách mà không chứng minh nhưng có kèm theo dòng chữ: “Tôi có một phương pháp rất hay để chứng minh cho trường hợp tổng quát, nhưng không thể viết ra đây vì lề sách quá hẹp.”!!

Các nhà toán học sau đó đã cố gắng giải bài toán này trong suốt gần bốn thế kỷ. Và cuối cùng nhà toán học Andrew Wiles (người Anh, định cư ở Mỹ, sinh 1953) đã công bố lời giải độc nhất vô nhị vào mùa hè năm 1993 và sửa lại năm 1995, với lời giải dài 200 trang.

Trong một thời gian dài tôi tìm cách chứng minh định lý này bằng toán học sơ cấp và tôi đã thành công. Dưới đây là toàn văn chứng minh định lý lớn Fermat.

Để chứng minh định lý lớn Fermat tôi đưa ra năm bổ đề và hai hệ quả sau đây.

Bổ đề 1:

Cho $n \in \mathbb{N}, n \geq 3$, nếu phương trình (PT) $x^n + y^n = z^n$ (1) có nghiệm nguyên khác không thì bao giờ cũng tồn tại nghiệm $x = u, y = v, z = t$ sao cho $u, v, t \in \mathbb{Z}^*$ và $(u, v) = (u, t) = (v, t) = 1$.

Bổ đề 2:

Nếu có $n \in \mathbb{N}, n \geq 3$, PT $x^n + y^n = z^n$ vô nghiệm nguyên khác không thì với mọi $k \in \mathbb{N}^*$, PT $x^{nk} + y^{nk} = z^{nk}$ cũng vô nghiệm nguyên khác không.

Bổ đề 3:

Cho $a.b = c^n$, n là số nguyên dương lẻ; $a, b, c \in \mathbb{Z}^*$ sao cho $(a, b) = 1$, khi đó tồn tại hai số nguyên khác không c_1, c_2 sao cho $(c_1, c_2) = 1, c = c_1.c_2, a = c_1^n$ và $b = c_2^n$.

Bổ đề 4:

Cho $a.b = c^n$, n là số nguyên dương lẻ, $a, b, c, m \in \mathbb{Z}^*$, sao cho $|a| \geq 2, |b| \geq 2, |c| \geq 2, m$ là số nguyên tố, $(a, b) = m, b \nmid m^2$, khi đó tồn tại số nguyên dương s sao cho $ns \geq 2$ và hai số nguyên khác không c_1, c_2 sao cho $(c_1, c_2) = 1$ đồng thời $c_1 \nmid m, c_2 \nmid m, c = m^s.c_1.c_2, a = m^{ns-1}.c_1^n$ và $b = m.c_2^n$.

Bổ đề 5:

Cho n là số nguyên tố lẻ và hai số nguyên u, v sao cho $(u, v) = 1$, khi đó:

a) Nếu $(u + v) \nmid n$ thì $\left(u + v, \sum_{i=0}^{n-1} (-1)^i u^{n-1-i} v^i\right) = 1$ và $\left(\sum_{i=0}^{n-1} (-1)^i u^{n-1-i} v^i\right) \nmid n$.

b) Nếu $(u - v) \nmid n$ thì $\left(u - v, \sum_{i=0}^{n-1} u^{n-i-1} v^i\right) = 1$ và $\left(\sum_{i=0}^{n-1} u^{n-i-1} v^i\right) \nmid n$.

c) Nếu $(u + v) : n$ thì $\left(u + v, \sum_{i=0}^{n-1} (-1)^i u^{n-1-i} v^i\right) = n$ và $\left(\sum_{i=0}^{n-1} (-1)^i u^{n-1-i} v^i\right) \nmid n^2$.

Hệ quả 1:

Cho $a.b.c = d^n$ với $n, a, b, c, d \in \mathbb{N}^*$ sao cho $(a, b) = (a, c) = (c, b) = 1$.

Khi đó bao giờ cũng tồn tại ba số nguyên dương c_1, c_2, c_3 sao cho $(c_1, c_2) = (c_1, c_3) = (c_3, c_2) = 1, d = c_1.c_2.c_3, a = c_1^n, b = c_2^n$ và $c = c_3^n$.

Hệ quả 2:

Cho $a.b.c = d^n$ với $a, b, c, d, m \in \mathbb{N}^*$, sao cho $a \geq 2, b \geq 2, c \geq 2, d \geq 2, (a, b, c) = (ab, c) = m$ và m là số nguyên tố.

Khi đó tồn tại các số nguyên dương s, k, c_1, c_2, c_3 sao cho $ns - k \geq 2, (c_1, c_2) = (c_3, c_2) = (c_1, c_3) = 1$, đồng thời $c_1 \nmid m, c_2 \nmid m, c_3 \nmid m, c = mc_2^n, d = m^s c_1 c_2 c_3, a = m^k c_1^n, b = m^{ns-k-1} c_2^n$.

1. CHỨNG MINH CÁC BỔ ĐỀ

1.1. Chứng minh bổ đề 1

Giả sử $x = u_0, y = v_0, z = t_0$ là một nghiệm nguyên khác không của PT(1) và $(u_0, v_0, t_0) = d$.

+ Nếu $u_0 = v_0$ thì $2u_0^n = t_0^n$, đẳng thức này không tồn tại với u_0, v_0, t_0 là số nguyên khác không n là số nguyên dương lớn hơn 2.

+ Nếu $u_0 \neq v_0$ Khi đó tồn tại ba số $u, v, t \in \mathbb{Z}^*$ sao cho $(u, v, t) = 1, u_0 = ud, v_0 = vd, t_0 = td$ và $u_0^n + v_0^n = t_0^n$, suy ra $u^n + v^n = t^n$ (1'') và thì $u \neq v$, suy ra $x = u, y = v, z = t$ là một nghiệm nguyên khác không của PT(1).

Giả sử $(u, v) = d'$, từ (1'') suy ra t^n chia hết cho d'^n , suy ra t chia hết cho d' , mà $(u, v, t) = 1$ nên $d' = 1$.

Vậy $(u, v) = 1$.

Chứng minh tương tự ta cũng có $(u, t) = (t, v) = 1$. Bổ đề 1 đã được chứng minh.

1.2. Chứng minh bổ đề 2

Giả sử tồn tại số nguyên dương k_0 sao cho PT $x^{nk} + y^{nk} = z^{nk}$ có nghiệm nguyên khác không $x = u, y = v, z = t$, khi đó ta có $u^{nk_0} + v^{nk_0} = t^{nk_0} \Leftrightarrow (u^{k_0})^n + (v^{k_0})^n = (t^{k_0})^n$ suy ra PT $x^n + y^n = z^n$ có nghiệm nguyên khác không $x = u^{k_0}, y = v^{k_0}, z = t^{k_0}$, điều này trái với giả thiết. Bổ đề 2 đã được chứng minh.

1.3. Chứng minh bổ đề 3

Giả sử $(a, c) = c'_1$, khi đó tồn tại hai số nguyên a_1, c'_2 sao cho $(a_1, c'_2) = 1$ và $a = c'_1 a_1, c = c'_1 c'_2$. Vì $ab = c^n$, nên $c_1 a_1 b = c_1^n c_2^n$, suy ra $a_1 b = c_1^{n-1} c_2^n$, suy ra $b \mid c_1^{n-1} c_2^n$. Vì $(c'_1, b) = 1$ (do $(a, b) = 1$) nên $c'_2^n = kb$, với k là số nguyên khác không, từ đẳng thức $a_1 b = c_1^{n-1} c'_2^n$, ta suy ra $a_1 = k c_1^{n-1}$, suy ra $a_1^n = k^n c_1^{n(n-1)}$, suy ra $k \mid a_1^n$ và $k \mid c_2^n$; vì $(a_1, c'_2) = 1$ nên $(a_1^n, c_2^n) = 1$, từ đó suy ra $|k| = 1$.

Vậy $b = k c'_2^n = (k c'_2)^n = c_2^n, a = k c_1^n = (k c_1)^n = c_1^n, c = c_1 c_2$, với $c_1 = k c'_1, c_2 = k c'_2$ nguyên tố cùng nhau. Bổ đề 3 đã được chứng minh.

1.4. Chứng minh bổ đề 4

Vì $a : m, b : m$ và $ab = c^n$, suy ra $c^n : m^2$, suy ra $c : m$ (do m là số nguyên tố).

Giả sử $c = m^s r$, với $s \in \mathbb{N}^*, r \in \mathbb{Z}^*$ và $r \nmid m$, mà $c^n = m^{ns} r^n : m^2$, nên $ns \geq 2$.

Do $(a, b) = m$ và $b \nmid m^2$, nên có thể giả sử $b = mh$ và $a = m^k l$, với $k \in \mathbb{N}^*; h, l \in \mathbb{Z}^*$ sao cho $(h, l) = 1, h \nmid m, l \nmid m$.

Vì $ab = c^n$ nên $m^{k+1} hl = m^{ns} r^n$, suy ra $k+1 = ns$, suy ra $k = ns-1$ và $hl = r^n$; áp dụng bổ đề 3, ta có $r = c_1 c_2, h = c_1^n, l = c_2^n$, trong đó hai số c_1, c_2 là hai số nguyên sao cho $(c_1, c_2) = 1$. Từ đó ta có $c = m^s c_1 c_2, a = m^{ns-1} c_1^n$ và $b = m c_2^n$. Bổ đề 4 đã được chứng minh.

1.5. Chứng minh bổ đề 5

a) Đặt $A = \sum_{i=0}^{n-1} (-1)^i u^{n-1-i} v^i$.

Ta có $u^n + v^n = [(u+v) - v]^n + v^n = (u+v) \sum_{k=0}^{n-1} (-1)^k C_n^k (u+v)^{n-k-1} v^k$ mà $u^n + v^n = (u+v)A$ và $u+v \neq 0$, nên $A = \sum_{k=0}^{n-1} (-1)^k C_n^k (u+v)^{n-k-1} v^k$. Ta có $A = (u+v) \sum_{k=0}^{n-2} (-1)^k C_n^k (u+v)^{n-k-2} v^k + n v^{n-1}$, $(u, v) = 1$ và $(u+v) \nmid n$ nên

$(u+v, nv^{n-1})=1$, suy ra $(A, u+v)=1$ (đpcm).

b) Vì n là số nguyên tố lẻ, nên từ a) ta thay v bởi $-v$ ta có điều phải chứng minh.

c) Ta có
$$A = n(u+v) \left[\sum_{k=0}^{n-3} (-1)^k \frac{C_n^k}{n} (u+v)^{n-k-2} v^k - \frac{(n-1)v^{n-2}}{2} \right] + nv^{n-1} = n(u+v)A_1 + nv^{n-1},$$
 với
$$\sum_{k=0}^{n-2} (-1)^k \frac{C_n^k}{n} (u+v)^{n-k-2} v^k - \frac{(n-1)v^{n-2}}{2} = A_1.$$
 Với $k=\overline{1, n}$ thì $C_n^k : n$ (vì n là số nguyên tố), mà $(u+v):n$ nên $n(u+v)A_1 : n^2$; mặt khác $nv^{n-1} : n$ và $nv^{n-1} \not\equiv n^2$ (do $v \not\equiv n$), từ đó suy ra $n(u+v)A_1 + nv^{n-1} = A : n$ và $A \not\equiv n^2$, hơn nữa $(u+v, A) = n$ (đpcm).

1.6. Chứng minh hệ quả 1

Vì $(a, b) = (a, c) = (c, b) = 1$, nên $(a, bc) = 1$ mà $a.(bc) = d^n$, áp dụng **bổ đề 3**, ta có $a = c_1^n$ và $bc = e^n$, với $c_1, e \in \mathbb{N}^*$ sao cho $(c_1, e) = 1$ và $c_1 e = d$

Ta có $bc = e^n$ với $(c, b) = 1$, lại áp dụng **bổ đề 3**, ta có $b = c_2^n$, $c = c_3^n$, với $c_2, c_3 \in \mathbb{N}^*$ sao cho $(c_2, c_3) = 1$ và $e = c_2 \cdot c_3$, suy ra $d = c_1 \cdot c_2 \cdot c_3$.

Như vậy $a = c_1^n$, $b = c_2^n$, $c = c_3^n$, $d = c_1 \cdot c_2 \cdot c_3$. Ta có $(c_1^n, c_2^n) = (c_1^n, c_3^n) = (c_3^n, c_2^n) = 1$, nên $(c_1, c_2) = (c_1, c_3) = (c_3, c_2) = 1$. Hệ quả 1 đã được chứng minh.

1.7. Chứng minh hệ quả 2

Vì $(ab, c) = m$ và $c \not\equiv m^2$ mà $(ab).c = d^n$, áp dụng **bổ đề 4**, ta có $ab = m^{ns-1}e^n$ và $c = mc_3^n$ với $c_3, e, s \in \mathbb{N}^*$ sao cho $(c_3, e) = 1$, $c_3 \not\equiv m$, $e \not\equiv m$ và $d = m^s c_3 e$.

Vì $a : m$, $b : m$ nên $a = m^k c'_1$, $b = m^g c'_2$, trong đó $k, g, c'_1, c'_2 \in \mathbb{N}^*$ sao cho $(c'_1, c'_2) = 1$, $c'_1 \not\equiv m$, $c'_2 \not\equiv m$.

Từ $ab = m^{ns-1}e^n$ ta suy ra $m^{k+g} c'_1 c'_2 = m^{ns-1}e^n$, suy ra $k+g = ns-1$ và $c'_1 c'_2 = e^n$, suy ra $g = ns - k - 1$, suy ra $ns - k \geq 2$.

Ta có $c'_1 c'_2 = e^n$ và $(c'_1, c'_2) = 1$, áp dụng **bổ đề 3**, ta có $c'_1 = c_1^n$, $c'_2 = c_2^n$, với $c_1, c_2 \in \mathbb{N}^*$ sao cho $(c_2, c_1) = 1$ và $e = c_1 \cdot c_2$.

Như vậy $a = m^k c_1^n$, $b = m^{ns-k-1} c_2^n$, $c = m c_3^n$ và $d = m^s c_1 \cdot c_2 \cdot c_3$. Vì $(c_3, e) = 1$ ($(c_2, c_1) = 1$ và $e = c_1 \cdot c_2$ nên $(c_1, c_2) = (c_1, c_3) = (c_3, c_2) = 1$). Hệ quả 2 đã được chứng minh.

2. CHỨNG MINH ĐỊNH LÝ LỚN FERMAT

2.1. Khi $n = 4$

Với $n = 4$ ta có PT: $x^4 + y^4 = z^4$ (2).

Giả sử PT (2) có nghiệm nguyên khác không $x = u$, $y = v$, $z = t$, trong đó $(u, v) = (u, t) = (v, t) = 1$ (theo **bổ đề 1**). Ta có $u^4 + v^4 = t^4$ (2'), suy ra $|t| > |u|, |t| > |v|$. Từ (2') suy ra trong ba số u, v, t có duy nhất một số chẵn và u, v có vai trò như nhau, cho nên ta chỉ cần xét hai trường hợp.

2.1.1. Khi t chẵn

Suy ra u, v đều lẻ, suy ra: $u^4 \equiv 1(\text{mod } 8)$ và $v^4 \equiv 1(\text{mod } 8) \Rightarrow t^4 = u^4 + v^4 \equiv 2(\text{mod } 8) \Rightarrow t^4 \not\equiv 16$, vô lý, vì $t^4 \equiv 16$

2.1.2. Khi u chẵn

Suy ra t và v đều lẻ. Ta có $(2') \Leftrightarrow |u|^4 = (|t| - |v|)(|t| + |v|)(|t|^2 + |v|^2)$. Vì t, v lẻ và $(u, v) = (u, t) = (v, t) = 1$ nên $(|t| + |v|, |t| - |v|, |t|^2 + |v|^2) = (|t|^2 - |v|^2, |t|^2 + |v|^2) = 2$ và $(|t|^2 + |v|^2) \not\equiv 2^2$. Áp dụng **hệ quả 2**, ta có $|t| - |v| = 2^k u_1^4$, $|t| + |v| = 2^{4s-k-1} v_1^4$, $t^2 + v^2 = 2t_1^4$, với $|u| = 2^s u_1 v_1 t_1$; trong đó s, k là hai số nguyên dương, u_1, v_1, t_1 là ba số nguyên dương lẻ đôi một nguyên tố cùng nhau, với $2^{4s-k-1} u_1^4 < 2^k v_1^4 < 2t_1^4$.

Suy ra: $|t| = 2^{k-1} u_1^4 + 2^{4s-k-2} v_1^4$ và $|v| = 2^{4s-k-2} v_1^4 - 2^{k-1} u_1^4$, suy ra $4^{4s-k-2} v_1^8 + 4^{k-1} u_1^8 = t_1^4$ (20). Vì t, v, u_1, v_1 là các số lẻ nên $(k-1=0$ và $4s-k-2 \geq 1)$ hoặc $(4s-k-2=0$ và $k-1 \geq 1)$ suy ra $(4s-k-2=4s-3 \geq 1$ hoặc $k-1=4s-3 \geq 1)$

Như vậy đẳng thức (20) luôn có dạng $4^{h_1} v_1^8 + (u_1^2)^4 = t_1^4$ (21) hoặc $(v_1^2)^4 + 4^{h_1} u_1^8 = t_1^4$ (21') với $h_1 \in \mathbb{N}, h_1 = 4s-3$. Do vậy ta chỉ cần xét một trong hai dạng của đẳng thức (20).

Từ (21) suy ra: $t_1 > u_1, t_1 > v_1$ và $t_1^4 - (u_1^2)^4 = 4^{h_1} v_1^8 \Rightarrow (t_1 + u_1^2)(t_1 - u_1^2)(t_1^2 + u_1^4) = 2^{2h_1} v_1^8$ (21''). Vì u_1, v_1, t_1 là các số nguyên dương lẻ và đôi một nguyên tố cùng nhau nên $t_1^2 + u_1^4 = 2t_2$, $t_1 + u_1^2 = 2^h v_2$, $t_1 - u_1^2 = 2^l u_2$; trong đó h, l là hai số nguyên dương, u_2, v_2, t_2 với $2^l u_2 < 2^h v_2 < 2t_2$ là ba số nguyên dương lẻ đôi một nguyên tố cùng nhau, suy ra $t_1 = 2^{2h_1-h-2} v_2 + 2^{h-1} u_2$, $u_1^2 = 2^{h-1} v_2 - 2^{2h_1-h-2} u_2$ và $4^{h-1} v_2^2 + 4^{2h_1-h-2} u_2^2 = t_2$ (22), suy ra $t_2 > u_2$, $t_2 > v_2$. Vì u_1, t_1, u_2, v_2 là các số lẻ nên $(h-1=0$ và $2h_1-h-2 \geq 1)$ hoặc $(2h_1-h-2=0$ và $h-1 \geq 1)$ suy ra $(2h_1-h-2=2h_1-3=h_2 \geq 1$ hoặc $h-1=2h_1-3=h_2)$, với $h_1 \in \mathbb{N}, h_1 \geq 2$.

Từ (21') suy ra: $2^{l+h+1} u_2 v_2 t_2 = 2^{2h_1} v_1^8 \Rightarrow l = 2h_1 - h - 1$ và $u_2 v_2 t_2 = v_1^8$. Áp dụng **hệ quả 1**, ta có $u_2 = u_3^8, v_2 = v_3^8, t_2 = t_3^8$, với $v_2 = u_3 v_3 t_3$; với u_3, v_3, t_3 là ba số nguyên dương lẻ đôi một nguyên tố cùng nhau.

Như vậy đẳng thức (22) luôn có dạng $(u_3^{2^2})^4 + 4^{h_2} v_3^{16} = (t_3^2)^4$ (22') hoặc $(v_3^{2^2})^4 + 4^{h_2} u_3^{16} = (t_3^2)^4$ (22'')

Ta có nhận xét: Nếu có u_3, v_3, t_3 thỏa mãn (22') hoặc (22'') thì $u_3 v_3 t_3 = v_2$ hoặc $u_3 v_3 t_3 = u_2$ với $t_3 > u_3, t_3 > v_3$.

Cứ như thế, với lập luận như trên với mỗi $k \in \mathbb{N}, k \geq 3$ ta có u_k, v_k, t_k là ba nguyên dương lẻ đôi một nguyên tố cùng nhau thỏa mãn đẳng thức $(u_k^{2^{k-1}})^4 + 4^{h_{k-1}} v_k^{2^{k+1}} = (t_k^{2^{k-2}})^4$ (22'_{k-1}) hoặc $(v_k^{2^{k-1}})^4 + 4^{h_{k-1}} u_k^{2^{k+1}} = (t_k^{2^{k-2}})^4$ (22''_{k-1}) và $u_k v_k t_k = v_{k-1}$ hoặc $u_k v_k t_k = u_{k-1}$ ($h_k = 2h_{k-1} - 3, h_1 = 4s-3, k \in \mathbb{N}, k \geq 3$).

Vì $u_k v_k t_k = v_{k-1}$ hoặc $u_k v_k t_k = u_{k-1}$, $t_k > u_k, t_k > v_k, \forall k \in \mathbb{N}, k \geq 3$, cho nên chỉ xảy ra hai khả năng sau.

a) Tồn tại $k_0 \in \mathbb{N}, k_0 \geq 3$ để cho $u_{k_0} v_{k_0} t_{k_0} = u_{k_0-1} = 1$ hoặc $u_{k_0} v_{k_0} t_{k_0} = u_{k_0-1} = 1$ thì $u_{k_0} = v_{k_0} = t_{k_0} = 1$, không thỏa mãn đẳng thức $(u_{k_0}^{2^{k_0-1}})^4 + 4^{h_{k_0-1}} v_{k_0}^{2^{k_0+1}} = (t_{k_0}^{2^{k_0-2}})^4$ (22'_{k_0-1}) và $(v_{k_0}^{2^{k_0-1}})^4 + 4^{h_{k_0-1}} u_{k_0}^{2^{k_0+1}} = (t_{k_0}^{2^{k_0-2}})^4$ (22''_{k_0-1})

Vậy PT(2) vô nghiệm nguyên khác không trong trường hợp này.

b) Tồn tại $k_0 \in \mathbb{N}, k_0 \geq 3$ để cho $u_{k_0} v_{k_0} t_{k_0} = u_{k_0-1} = p$ hoặc $u_{k_0} v_{k_0} t_{k_0} = u_{k_0-1} = q$, với p, q là các số nguyên tố lẻ. Vì $t_{k_0} > u_{k_0}, t_{k_0} > v_{k_0}$ nên $(t_{k_0} = p, u_{k_0} = v_{k_0} = 1)$ hoặc $(t_{k_0} = q, u_{k_0} = v_{k_0} = 1)$ khi đó có $u_{k_0+1}, v_{k_0+1}, t_{k_0+1}$ là các số nguyên dương lẻ đôi một nguyên tố cùng nhau thỏa mãn đẳng thức $(u_{k_0+1}^{2^{k_0}})^4 + 4^{h_{k_0}} v_{k_0+1}^{2^{k_0+2}} = (t_{k_0+1}^{2^{k_0-1}})^4$ (22'_{k_0}) hoặc

$\left(v_{k_0+1}^{2^{k_0}}\right)^4 + 4^{h_{k_0}} u_{k_0+1}^{2^{k_0+2}} = \left(t_{k_0+1}^{2^{k_0-1}}\right)^4 (2_{k_0}^{//})$, với $u_{k_0+1} \cdot v_{k_0+1} \cdot t_{k_0+1} = u_{k_0} = 1$ hoặc $u_{k_0+1} \cdot v_{k_0+1} \cdot t_{k_0+1} = v_{k_0} = 1$, suy ra $u_{k_0+1} = v_{k_0+1} = t_{k_0+1} = 1$, không thỏa mãn đẳng thức $(2_{k_0}^{//})$ và $(2_{k_0}^{//})$.

Vậy PT(2) vô nghiệm nguyên khác không trong trường hợp này.

Tóm lại, khi $n = 4$, PT(1) vô nghiệm nguyên khác không.

2.2 Khi n là số nguyên tố lớn hơn 3

Giả sử PT (1) có nghiệm nguyên khác không $x = u, y = v, z = t$, trong đó

$$(u, v) = (u, t) = (v, t) = 1 \text{ (áp dụng bổ đề 1), khi đó } u^n + v^n = t^n \text{ (3)}$$

$$\text{Suy ra: } (u+v) \sum_{i=0}^{n-1} (-1)^i u^{n-i-1} v^i = t^n \text{ (4), } (t-v) \sum_{i=0}^{n-1} t^{n-i-1} v^i = u^n \text{ (5), } (t-u) \sum_{i=0}^{n-1} t^{n-i-1} u^i = v^n \text{ (6)}$$

2.2.1. Ba số u, v, t đều không chia hết cho n .

Vì $(u, v) = (u, t) = (v, t) = 1$ và từ (4), (5), (6) ta suy ra $(u+v) \nmid n, (t-v) \nmid n$ và $(t-u) \nmid n$; áp dụng **bổ đề 5a) và 5b)** ta có $\left(u+v, \sum_{i=0}^{n-1} (-1)^i u^{n-i-1} v^i\right) = \left(t-v, \sum_{i=0}^{n-1} t^{n-i-1} v^i\right) = \left(t-u, \sum_{i=0}^{n-1} t^{n-i-1} u^i\right) = 1, \left(\sum_{i=0}^{n-1} (-1)^i u^{n-i-1} v^i\right) \nmid n, \left(\sum_{i=0}^{n-1} t^{n-i-1} v^i\right) \nmid n, \left(\sum_{i=0}^{n-1} t^{n-i-1} u^i\right) \nmid n$, kết hợp với (4), (5), (6) và áp dụng **bổ đề 3**, ta có: $u+v = c^n$ (4') và $\sum_{i=0}^{n-1} (-1)^i u^{n-i-1} v^i = c'^n$, với $t = c.c', c, c' \in \mathbb{Z}^*, (c, c') = 1$ và $c \nmid n, c' \nmid n$; $t-v = b^n$ (5') và $\sum_{i=0}^{n-1} t^{n-i-1} v^i = b'^n$, với $u = b.b', b, b' \in \mathbb{Z}^*, (b, b') = 1$ và $b \nmid n, b' \nmid n$; $t-u = a^n$ (6') và $\sum_{i=0}^{n-1} t^{n-i-1} u^i = a'^n$, với $v = a.a', a, a' \in \mathbb{Z}^*, (a, a') = 1$ và $a \nmid n, a' \nmid n$; $(a, b) = (a, c) = (c, b) = 1$.

$$\begin{aligned} \text{Ta có: } c^n &= A = \sum_{i=0}^{n-1} (-1)^i u^{n-i-1} v^i = \sum_{k=0}^{n-1} (-1)^k C_n^k (u+v)^{n-k-1} v^k = \sum_{k=1}^{n-1} (-1)^k C_n^k (u+v)^{n-k-1} v^k + (u+v)^{n-1} \\ \Rightarrow c'^n - 1 &= \sum_{k=1}^{n-1} (-1)^k C_n^k (u+v)^{n-k-1} v^k + \left[(u+v)^{n-1} - 1\right]. \end{aligned}$$

Vì n là số nguyên tố và $(u+v) \nmid n$, nên với $k = \overline{1, n}$ thì $C_n^k : n$ và $\left[(u+v)^{n-1} - 1\right] : n$ (định lý nhỏ Fermat). Do đó $(c'^n - 1) : n$, mà $c' \nmid n$ nên $(c'^{n-1} - 1) : n$, suy ra $c'^n - 1 - (c'^{n-1} - 1) = c'^{n-1} (c' - 1) : n$, suy ra $(c' - 1) : n$, suy ra $c' = 1 + nk_3$, với $k_3 \in \mathbb{Z}$.

Chứng minh tương tự ta cũng có $a' = 1 + nk_1, b' = 1 + nk_2$, với $k_1, k_2 \in \mathbb{Z}$. Ta có (3) $\Leftrightarrow t^n - u - v = u^n + v^n - u - v \Rightarrow t^n - u - v = (c.c')^n - c^n = c^n \left[(1 + nk_3)^n - 1\right] : n^2$. Chứng minh tương tự ta

cũng có $(u^n - t + v) : n^2$ và $(v^n - t + u) : n^2$ suy ra $(u^n - t + v) + (v^n - t + u) - (t^n - u - v) = 2(u + v - t) : n^2 \Rightarrow (u + v - t) : n^2$. Từ (3'), (4'), (5') suy ra $u + v - t = c(c^{n-1} - c') = a(a' - a^{n-1}) = b(b' - b^{n-1}) = n^s abck$, với $k \in \mathbb{Z}, s \in \mathbb{Z}, s \geq 2, (k, a) = (k, b) = (k, c) = 1$ và $k \nmid n$, nếu $k \neq 0$. Suy ra $u = b^n + n^s abck, v = a^n + n^s abck, t = c^n - n^s abck$ và $a^n + b^n - c^n = -2n^s abck$.

2.2.2. Ba số u, v, t chỉ có một số chia hết cho n.

Vì $v^n + u^n = t^n \Leftrightarrow u^n + v^n = t^n \Leftrightarrow v^n + (-t)^n = (-v)^n \Leftrightarrow u^n + (-t)^n = (-u)^n$, nên tính chất số học và vai trò của u, v, t là như nhau. Do đó không mất tính tổng quát ta giả sử $t:n$ và $u \nmid n, v \nmid n$; từ (6) suy ra $(u+v):n$, áp dụng **bổ đề 5c** ta có $\left(u+v, \sum_{i=0}^{n-1} (-1)^i u^{n-1-i} v^i\right) = n$ và $\left(\sum_{i=0}^{n-1} (-1)^i u^{n-1-i} v^i\right) \nmid n^2$, kết hợp với (6) và áp dụng **bổ đề 4** ta có $u+v = n^{s-1} c^n$ (4'') và $\sum_{i=0}^{n-1} (-1)^i u^{n-1-i} v^i = n c'^n$ với $t = n^s c c'$, $s \in \mathbb{N}^*$; $c, c' \in \mathbb{Z}^*$, $(c, c') = 1, c \nmid n, c' \nmid n$. Từ (4), (5) suy ra $(t-v) \nmid n$ và $(t-v) \nmid n$, áp dụng **bổ đề 5b** ta có $\left(t-v, \sum_{i=0}^{n-1} t^{n-i-1} v^i\right) = \left(t-u, \sum_{i=0}^{n-1} t^{n-i-1} u^i\right) = 1$, $\left(\sum_{i=0}^{n-1} t^{n-i-1} v^i\right) \nmid n$, $\left(\sum_{i=0}^{n-1} t^{n-i-1} u^i\right) \nmid n$, kết hợp với (4), (5) và áp dụng **bổ đề 3** ta có $t-v = b^n$ (5'') và $\sum_{i=0}^{n-1} t^{n-i-1} v^i = b'^n$, với $u = b b'$, $b, b' \in \mathbb{Z}^*$, $(b, b') = 1, b \nmid n, b' \nmid n$; $t-u = a^n$ (6''), với $v = a a'$, $a, a' \in \mathbb{Z}^*$, $(a, a') = 1, a \nmid n, a' \nmid n$; $(a, b) = (a, c) = (c, b) = 1$.

Lập luận như 2.2.1 (trang 5) ta có $b' = 1 + n k_2$, $a' = 1 + n k_1$; và $(u+v-t):n^2$, mà $u+v-t = n^s c (n^{ns-1-s} c^{n-1} - c') = a (a' - a^{n-1}) = b (b' - b^{n-1}) = n^s a b c k$ nên $s \geq 2$; $(k, a) = (k, b) = (k, c) = 1$ và $k \nmid n$, nếu $k \neq 0$. Suy ra $v = n^{ns-1} a^n + n^s a b c k$, $u = b^n + n^s a b c k$, $t = c^n - n^s a b c k$ và $n^{ns-1} a^n + b^n = c^n - 2 n^s a b c k$.

2.2.3. Nhận xét

Để dàng nhận ra trong ba số u, v, t thỏa (3) thì ít có hai số không chia hết cho n. Không mất tính tổng quát ta giả sử u, v không chia hết cho n, thì theo 2.2.1 và 2.2.2 ta có $v = a^n + n^s a b c k$, $u = b^n + n^s a b c k$, $t = h - n^s a b c k$ và $a^n + b^n = h - 2 n^s a b c k$; với $(h = c^n, \text{ khi } t \nmid n) \text{ hoặc } (h = n^{ns-1} c^n, \text{ khi } t:n)$; trong đó a, b, c, k đôi một nguyên tố cùng nhau và không chia hết cho n (nếu $k \neq 0$).

2.2.3.1. Khi k = 0

Ta nhận thấy khi $k = 0$ thì $t-u=v, t-v=u$, hay $a^n = a.a', b^n = b.b'$, suy ra $|a| = |a'| = |b| = |b'| = 1 \Rightarrow |u| = |v| = 1 \Rightarrow t = 0$ hoặc $|t|^n = 2$, vô lý.

Vậy PT (1) vô nghiệm nguyên khác không trong trường hợp này.

2.2.3.2 Khi k ≠ 0

+ Theo chứng minh trên ta có $v = a^n + n^s a b c k$, $u = b^n + n^s a b c k$, $t = h - n^s a b c k$ và $a^n + b^n = h - 2 n^s a b c k$; với $h = c^n$, khi $t \nmid n$ hoặc $h = n^{ns-1} c^n$, khi $t:n$; trong đó a, b, c, k đôi một nguyên tố cùng nhau ($k \neq 0$).

Thay vào (3) ta có: $(a^n + n^s a b c k)^n + (b^n + n^s a b c k)^n = (h - n^s a b c k)^n$
 $\Leftrightarrow h^n - a^{n^2} - b^{n^2} - n [a^{n(n-1)} + b^{n(n-1)} + h^{n-1}] n^s a b c k - \frac{n(n-1)}{2} [a^{n(n-2)} + b^{n(n-2)} - h^{n-2}] (n^s a b c k)^2 - \dots -$
 $-\frac{n(n-1)(n-2)}{6} [a^{n(n-3)} + b^{n(n-3)} + h^{n-3}] (n^s a b c k)^3 - \dots - \frac{n(n-1)}{2} (a^{2n} + b^{2n} + h^2) (n^s a b c k)^{n-2} - n(a^n + b^n - h) (n^s a b c k)^{n-1} -$
 $-3(n^s a b c k)^n = 0$ suy ra

$$h^n - a^{n^2} - b^{n^2} - n [a^{n(n-1)} + b^{n(n-1)} + h^{n-1}] n^s a b c k \equiv \frac{n(n-1)}{2} [b^{n(n-2)} + a^{n(n-2)} - h^{n-2}] (n^s a b c k)^2 \pmod{n^{3s+1}} \quad (7)$$

$$h^n - a^{n^2} - b^{n^2} \equiv n [a^{n(n-1)} + b^{n(n-1)} + h^{n-1}] n^s a b c k \pmod{n^{2s+1}} \quad (8) \quad \text{và} \quad h^n - b^{n^2} - a^{n^2} \equiv 0 \pmod{n^{s+1}} \quad (9)$$

$$\begin{aligned}
& + \text{ Mặt khác ta có } t^n - u^n = v^n \Leftrightarrow (t-u) \sum_{i=0}^{n-1} t^{n-1-i} u^i = v^n \Leftrightarrow a^n \sum_{i=0}^{n-1} (h - n^s abck)^{n-1-i} (b^n + n^s abck)^i = (a^n + n^s abck)^n \\
& \Leftrightarrow \sum_{i=0}^{n-1} (h - n^s abck)^{n-1-i} (b^n + n^s abck)^i = (a^{n-1} + n^s bck)^n \\
& \Leftrightarrow \sum_{i=0}^{n-1} \sum_{j=0}^{n-1-i} \sum_{l=0}^i (-1)^j C_{n-1-i}^j C_i^l h^{n-1-i-j} b^{n(i-l)} (n^s abck)^{l+j} = \sum_{i=1}^n C_n^i a^{(n-1)(n-i)} (n^s bck)^i \\
& \Leftrightarrow \sum_{i=0}^{n-1} \sum_{j=0}^{n-1-i} \sum_{l=0}^i (-1)^j C_{n-1-i}^j C_i^l h^{n-1-i-j} b^{n(i-l)} (n^s abck)^{l+j} + \frac{1}{2} \sum_{i=2}^{n-1} i(i-1) b^{n(i-2)} h^{n-1-i} (n^s abck)^2 + \frac{1}{2} \sum_{i=0}^{n-3} (n-1-i)(n-2-i) b^{ni} h^{n-3-i} (n^s abck)^2 - \\
& - \sum_{i=1}^{n-2} i(n-1-i) b^{n(i-1)} h^{n-2-i} (n^s abck)^2 + \sum_{i=0}^{n-1} h^{n-1-i} b^{ni} + \sum_{i=1}^{n-1} i b^{n(i-1)} h^{n-1-i} n^s abck - \sum_{i=0}^{n-2} (n-1-i) b^{ni} h^{n-2-i} n^s abck = \\
& = \sum_{i=2}^n C_n^i a^{n(n-1-i)} (n^s abck)^i + a^{n(n-1)} + na^{n(n-2)} (n^s abck) \\
& \Rightarrow \frac{1}{2} \sum_{i=2}^{n-1} i(i-1) b^{n(i-2)} h^{n-1-i} (n^s abck)^2 + \frac{1}{2} \sum_{i=0}^{n-3} (n-1-i)(n-2-i) b^{ni} h^{n-3-i} (n^s abck)^2 - \sum_{i=1}^{n-2} i(n-1-i) b^{n(i-1)} h^{n-2-i} (n^s abck)^2 + \\
& + \sum_{i=0}^{n-1} h^{n-1-i} b^{ni} + \sum_{i=1}^{n-1} i b^{n(i-1)} h^{n-1-i} n^s abck - \sum_{i=0}^{n-2} (n-1-i) b^{ni} h^{n-2-i} n^s abck \equiv a^{n(n-1)} + na^{n(n-2)} n^s abck \pmod{n^{2s+1}} \\
& \Rightarrow \frac{1}{2} \sum_{i=2}^{n-1} i(i-1) b^{n(i-2)} h^{n-1-i} (n^s abck)^2 + \frac{1}{2} \sum_{i=0}^{n-3} (1+i)(2+i) b^{ni} h^{n-3-i} (n^s abck)^2 + \sum_{i=1}^{n-2} i(1+i) b^{n(i-1)} h^{n-2-i} (n^s abck)^2 + \sum_{i=0}^{n-1} h^{n-1-i} b^{ni} + \\
& + \sum_{i=1}^{n-1} i b^{n(i-1)} h^{n-1-i} n^s abck - \sum_{i=0}^{n-2} (n-1-i) b^{ni} h^{n-2-i} n^s abck \equiv a^{n(n-1)} + na^{n(n-2)} n^s abck \pmod{n^{2s+1}} \\
& \Rightarrow \frac{1}{2} \sum_{i=2}^{n-1} i(i-1) b^{n(i-2)} h^{n-1-i} (n^s abck)^2 + \frac{1}{2} \sum_{i=2}^{n-1} i(i-1) b^{n(i-2)} h^{n-1-i} (n^s abck)^2 + \sum_{i=2}^{n-1} i(i-1) b^{n(i-2)} h^{n-1-i} (n^s abck)^2 + \sum_{i=0}^{n-1} h^{n-1-i} b^{ni} + \\
& + \sum_{i=1}^{n-1} i b^{n(i-1)} h^{n-1-i} n^s abck - \sum_{i=0}^{n-2} (n-1-i) b^{ni} h^{n-2-i} n^s abck \equiv a^{n(n-1)} + na^{n(n-2)} n^s abck \pmod{n^{2s+1}} \\
& \Rightarrow 2 \sum_{i=2}^{n-1} i(i-1) b^{n(i-2)} h^{n-1-i} (n^s abck)^2 + \sum_{i=0}^{n-1} h^{n-1-i} b^{ni} + \sum_{i=1}^{n-1} i b^{n(i-1)} h^{n-1-i} n^s abck - \sum_{i=0}^{n-2} (n-1-i) b^{ni} h^{n-2-i} n^s abck \equiv a^{n(n-1)} + na^{n(n-2)} n^s abck \pmod{n^{2s+1}} \\
& \Rightarrow 2 f''(b^n) (n^s abck)^2 + \frac{h^n - b^{n^2}}{h - b^n} + f'(b^n) n^s abck - g'(h) n^s abck \equiv a^{n(n-1)} + na^{n(n-2)} n^s abck \pmod{n^{2s+1}} \\
& (\text{Với } f(x) = \frac{x^n - h^n}{x - h}, f'(x) = \frac{(n-1)x^{n-1} - nhx^{n-1} + h^n}{(x-h)^2}, f''(x) = \frac{[n(n-1)x^{n-1} - n(n-1)hx^{n-2}](x-h) - 2[(n-1)x^n - nhx^{n-1} + h^n]}{(x-h)^3} \\
& g(x) = \frac{x^n - b^{n^2}}{x - b^n}, g'(x) = \frac{(n-1)x^n - nb^n x^{n-1} + b^{n^2}}{(x-b^n)^2}) \\
& \Rightarrow \frac{2[n(n-1)b^{n(n-1)} - n(n-1)hb^{n(n-2)}](b^n - h) - 4[(n-1)b^{n^2} - nhb^{n(n-1)} + h^n]}{(b^n - h)^3} (n^s abck)^2 + \frac{(n-1)b^{n^2} - nhb^{n(n-1)} + h^n}{(h-b^n)^2} n^s abck + \\
& + \frac{h^n - b^{n^2}}{h - b^n} - \frac{(n-1)h^n - nb^n h^{n-1} + b^{n^2}}{(h-b^n)^2} n^s abck \equiv a^{n(n-1)} + na^{n(n-2)} n^s abck \pmod{n^{2s+1}} \\
& \Rightarrow \frac{4(h^n - b^{n^2})}{(h-b^n)^3} (n^s abck)^2 + \frac{h^n - b^{n^2}}{h - b^n} - \frac{n(h^n - b^{n^2}) - nb^n h[h^{n-2} - b^{n(n-2)}]}{(h-b^n)^2} n^s abck + \frac{2(h^n - b^{n^2}) n^s abck}{(b^n - h)^2} \equiv \\
& \equiv a^{n(n-1)} + na^{n(n-2)} n^s abck \pmod{n^{2s+1}}
\end{aligned}$$

$$\begin{aligned}
&\Rightarrow \frac{4(h^n - b^{n^2})}{(h-b^n)^3} (n^s abck)^2 + \frac{h^n - b^{n^2}}{h-b^n} - \frac{n[h^{n-1} + b^{n(n-1)}]}{(h-b^n)^2} (h-b^n) n^s abck + \frac{2(h^n - b^{n^2}) n^s abck}{(b^n - h)^2} \equiv a^{n(n-1)} + na^{n(n-2)} n^s abck \pmod{n^{2s+1}} \\
&\Rightarrow \frac{4(h^n - b^{n^2})}{(h-b^n)^3} (n^s abck)^2 + \frac{h^n - b^{n^2}}{h-b^n} - \frac{n[h^{n-1} + b^{n(n-1)}]}{h-b^n} n^s abck + \frac{2(h^n - b^{n^2}) n^s abck}{(b^n - h)^2} \equiv a^{n(n-1)} + na^{n(n-2)} n^s abck \pmod{n^{2s+1}} \\
&\Rightarrow \frac{4(h^n - b^{n^2})}{(h-b^n)^3} (n^s abck)^2 + \frac{h^n - b^{n^2}}{h-b^n} - \frac{n[h^{n-1} + b^{n(n-1)}]}{h-b^n} n^s abck + \frac{2(h^n - b^{n^2}) n^s abck}{(b^n - h)^2} \equiv \\
&\equiv \frac{a^{n(n-1)} (a^n + 2n^s abck) + na^{n(n-2)} (a^n + 2n^s abck) n^s abck}{h-b^n} \pmod{n^{2s+1}} \text{ (vì } h-b^n = a^n + 2n^s abck \text{)} \\
&\Rightarrow \frac{4(h^n - b^{n^2})}{(h-b^n)^3} (n^s abck)^2 + \frac{h^n - b^{n^2}}{h-b^n} - \frac{n[h^{n-1} + b^{n(n-1)}]}{h-b^n} n^s abck + \frac{2(h^n - b^{n^2}) n^s abck}{(b^n - h)^2} \equiv \frac{2a^{n(n-1)} n^s abck}{h-b^n} + \frac{a^{n^2} + na^{n(n-1)} n^s abck}{h-b^n} \pmod{n^{2s+1}} \\
&\Rightarrow \frac{4(h^n - b^{n^2})}{(h-b^n)^3} (n^s abck)^2 + \frac{h^n - b^{n^2} - a^{n^2} - n[h^{n-1} + b^{n(n-1)} + a^{n(n-1)}] n^s abck}{h-b^n} + \frac{2(h^n - b^{n^2}) n^s abck}{(b^n - h)^2} \equiv \frac{2a^{n(n-1)} n^s abck (a^n + 2n^s abck)}{(h-b^n)^2} \pmod{n^{2s+1}} \\
&\Rightarrow \frac{4(h^n - b^{n^2})}{(h-b^n)^3} (n^s abck)^2 + \frac{h^n - b^{n^2} - a^{n^2} - n[h^{n-1} + b^{n(n-1)} + a^{n(n-1)}] n^s abck}{h-b^n} + \frac{2(h^n - b^{n^2} - a^{n^2}) n^s abck}{(b^n - h)^2} \equiv \frac{2na^{n^2} n^s abck + 4a^{n(n-1)} (n^s abck)^2}{(h-b^n)^2} \pmod{n^{2s+1}} \\
&\Rightarrow \frac{4(h^n - b^{n^2})}{(h-b^n)^3} (n^s abck)^2 + \frac{\frac{n(n-1)}{2} [b^{n(n-2)} + a^{n(n-2)} - h^{n-2}] (n^s abck)^2}{h-b^n} + \frac{2n[h^{n-1} + b^{n(n-1)} + a^{n(n-1)}] (n^s abck)^2}{(h-b^n)^2} \equiv \\
&\equiv \frac{[2na^{n^2} n^s abck + 4a^{n(n-1)} (n^s abck)^2] (a^n + 2n^s abck)}{(h-b^n)^3} \pmod{n^{2s+1}} \text{ (vì } h^n - a^{n^2} - b^{n^2} - n[a^{n(n-1)} + b^{n(n-1)} + h^{n-1}] n^s abck \equiv \\
&\equiv \frac{n(n-1)}{2} [b^{n(n-2)} + a^{n(n-2)} - h^{n-2}] (n^s abck)^2 \pmod{n^{3s+1}}, h^n - a^{n^2} - b^{n^2} \equiv n[a^{n(n-1)} + b^{n(n-1)} + h^{n-1}] n^s abck \pmod{n^{2s+1}} \\
&\text{(theo (7) và (8)))} \\
&\Rightarrow \frac{4(h^n - b^{n^2})}{(h-b^n)^3} (n^s abck)^2 \equiv \frac{2na^{n^2+n} n^s abck + 4a^{n^2} (n^s abck)^2}{(h-b^n)^3} \pmod{n^{2s+1}} \\
&\Rightarrow \frac{4(h^n - b^{n^2} - a^{n^2})}{(h-b^n)^3} (n^s abck)^2 \equiv \frac{2na^{n^2+n} n^s abck}{(h-b^n)^3} \pmod{n^{2s+1}} \text{ (Vì } h^n - b^{n^2} - a^{n^2} \equiv 0 \pmod{n^{s+1}} \text{) (theo (9))} \\
&\Rightarrow 2na^{n^2+n} n^s abck \equiv 0 \pmod{n^{2s+1}} \\
&\Rightarrow a^{n^2+n+1} bck \equiv 0 \pmod{n^s}, \text{ vô lý, vì } a^{n^2+n+1} bck \not\equiv 0 \pmod{n}.
\end{aligned}$$

Vậy PT (1) vô nghiệm nguyên khác không trong trường hợp này.

Lưu ý: Trong các phương trình đồng dư ở trên, tác giả đề mẫu số (không quy đồng, bỏ mẫu) để tiện biến đổi theo hướng sử dụng (7), (8), (9) mà không mất bản chất phương trình đồng dư (vì mẫu $(h-b^n)^r \not\equiv 0 \pmod{n}, r=1,2,3$).

2.3. Khi $n = 3$

Giả sử PT: $x^3 + y^3 = z^3$ (3') có nghiệm nguyên $(x; y; z) = (u; v; t)$ trong đó u, v, t là ba số nguyên khác 0 và chúng đôi một nguyên tố cùng nhau, khi đó $u^3 + v^3 = t^3$ (2₁).

Do $n = 3$ là số lẻ và u, v, t là các số nguyên, nên có thể xem vai trò của các số này trong đẳng thức dạng (2₁) là như nhau. Vì vậy, các lập luận dưới đây đối với một trường hợp nào đó liên quan đến u, v, t thì hiểu rằng

các trường hợp còn lại được xét tương tự.

Ta có $u^3 + v^3 = t^3 \Leftrightarrow (u^3 - u) + (v^3 - v) - (t^3 - t) = -u - v + t$. Vì $(u^3 - u), (v^3 - v), (t^3 - t)$ đều chia hết cho 3 nên $(-u - v + t) : 3$, suy ra $u + v \equiv t \pmod{3} \Rightarrow (u + v)^3 \equiv t^3 \pmod{9} \Rightarrow (u + v)^3 - t^3 \equiv 0 \pmod{9}$. Mặt khác $u^3 + v^3 = t^3 \Leftrightarrow (u + v)^3 - t^3 = 3uv(u + v) \Rightarrow u : 3$ hoặc $v : 3$ hoặc $(u + v) : 3$

Dễ dàng nhận ra nếu $(u + v)$ chia hết cho 3 thì t chia hết cho 3. Như vậy trong ba số u, v, t luôn có duy nhất một số chia hết cho 3. Giả sử u và v không chia hết cho 3, từ kết quả của 2.2.2 ở trang 6 (vẫn còn đúng khi $n = 3$), ta có $u = b^3 + 3^s abck$, $v = a^3 + 3^s abck$, $t = 3^{3s-1}c^3 - 3^s abck$, suy ra, $a^3 + b^3 = 3^{3s-1}c^3 - 2 \cdot 3^s abck$, với $a, b, c, c' \in \mathbb{Z}^*$ đôi một nguyên tố cùng nhau và không chia hết cho 3; $k \in \mathbb{Z}, s \in \mathbb{N}^*, s \geq 2$, k không chia hết cho 3 và đi một nguyên tố cùng nhau với a, b, c , (nếu $k \neq 0$).

+ Khi $k = 0$ thì $t - u = v$, $t - v = u$, $a^3 = a \cdot a', b^3 = b \cdot b' \Rightarrow |a| = |a'| = |b| = |b'| = 1 \Rightarrow |u| = |v| = 1 \Rightarrow t = 0$ hoặc $|t| = 2$, vô lý.

+ Khi $k \neq 0$: Ta có $u^3 + v^3 = t^3 \Leftrightarrow t^3 - u^3 = v^3$, suy ra

$$\begin{aligned} & (3^{3s-1}c^3 - 3^s abck)^2 + (3^{3s-1}c^3 - 3^s abck)(b^3 + 3^s abck) + (b^3 + 3^s abck)^2 = (a^2 + 3^s bck)^3 \\ & \Rightarrow 3^{6s-2}c^6 - 2 \cdot 3^{4s-1}c^3(abck) + 3^{3s-1}c^3b^3 + b^6 + b^33^s abck + (3^s abck)^2 = a^6 + 3a^3(3^s abck) + 3(3^s abck)^2 + (3^s bck)^3 \\ & \Rightarrow 3^{6s-2}c^6 + 3^{3s-1}c^3b^3 + b^33^s abck - 2 \cdot 3^{4s-1}c^3(abck) = a^6 - b^6 + 3a^3(3^s abck) + 2(3^s abck)^2 + (3^s bck)^3 \\ & \Rightarrow 3^{6s-2}c^6 + 3^{3s-1}c^3b^3 + b^33^s abck - 2 \cdot 3^{4s-1}c^3(abck) = (a^3 - b^3)(a^3 + b^3) + 3a^3(3^s abck) + 2(3^s abck)^2 + (3^s bck)^3 \\ & \Rightarrow 3^{6s-2}c^6 + 3^{3s-1}c^3b^3 + b^33^s abck - 2 \cdot 3^{4s-1}c^3(abck) = (a^3 - b^3)(3^{3s-1}c^3 - 2 \cdot 3^s abck) + 3a^3(3^s abck) + 2(3^s abck)^2 + (3^s bck)^3 \\ & \text{(vì } a^3 + b^3 = 3^{3s-1}c^3 - 2 \cdot 3^s abck) \\ & \Rightarrow 3^{6s-2}c^6 + 3^{3s-1}c^3b^3 + b^33^s abck - 2 \cdot 3^{4s-1}c^3(abck) = 3^{3s-1}c^3a^3 - 3^{3s-1}b^3c^3 - 2a^3(3^s abck) + 2b^3(3^s abck) + 3a^3(3^s abck) + 2(3^s abck)^2 + (3^s bck)^3 \\ & \Rightarrow 3^{6s-2}c^6 + 3^{3s-1}c^3b^3 - 2 \cdot 3^{4s-1}c^3(abck) = 3^{3s-1}c^3a^3 - 3^{3s-1}b^3c^3 + b^3(3^s abck) + a^3(3^s abck) + 2(3^s abck)^2 + (3^s bck)^3 \\ & \Rightarrow -3^{6s-2}c^6 + 3^{3s-1}c^3a^3 - 2 \cdot 3^{3s-1}b^3c^3 + 2 \cdot 3^{4s-1}c^3(abck) + (b^3 + a^3)(3^s abck) + 2(3^s abck)^2 + (3^s bck)^3 = 0 \\ & \Rightarrow -3^{6s-2}c^6 + 3^{3s-1}c^3a^3 - 2 \cdot 3^{3s-1}b^3c^3 + 2 \cdot 3^{4s-1}c^3(abck) + (3^{3s-1}c^3 - 2 \cdot 3^s abck)(3^s abck) + 2(3^s abck)^2 + (3^s bck)^3 = 0 \\ & \Rightarrow -3^{6s-2}c^6 + 3^{3s-1}c^3a^3 - 2 \cdot 3^{3s-1}b^3c^3 + 3^{4s}c^3(abck) + (3^s bck)^3 = 0 \\ & \Rightarrow -3^{6s-2}c^6 + 3^{3s-1}c^3(a^3 - 2b^3 + 3^{s+1}abck + 3b^3k^3) = 0 \\ & \Rightarrow -3^{3s-1}c^3 + a^3 - 2b^3 + 3^{s+1}abck + 3b^3k^3 = 0 \\ & \Rightarrow (-3^{3s-1}c^3 + a^3 + b^3) + 3^{s+1}abck + 3b^3k^3 - 3b^3 = 0 \\ & \Rightarrow -2 \cdot 3^s abck + 3^{s+1}abck + 3b^3k^3 - 3b^3 = 0 \text{ (vì } a^3 + b^3 = 3^{3s-1}c^3 - 2 \cdot 3^s abck) \\ & \Rightarrow 3^s abck + 3b^3k^3 - 3b^3 = 0 \\ & \Rightarrow 3^{s-1}ac + b^2k^2 - \frac{b^2}{k} = 0(*) \\ & \Rightarrow k = 1 \vee k = -1 \end{aligned}$$

i) Khi $k = -1$: $(*) \Rightarrow 3^{s-1}ac + 2b^2 = 0(**) \Rightarrow |b| = 1$. Từ $(**)$ suy ra $3^{s-1}ac + 2 = 0 \Rightarrow 2 : 3^{s-1}$, vô lý, vì $s \geq 2, s \in \mathbb{N}^*$.

ii) Khi $k = 1$: $(*) \Rightarrow 3^{s-1}ac = 0$, vô lý, vì $ac \neq 0$.

2.4. Khi $n = pk$, p là số nguyên tố lẻ hoặc $p = 4$ ($k \in \mathbb{N}^*$)

Từ kết quả chứng minh ở 2.1, 2.2, 2.3 áp dụng bổ đề 2, suy ra PT (1) vô nghiệm nguyên khác không trong trường hợp này.

Tóm lại, với mọi số nguyên $n \geq 3$, PT(1) vô nghiệm nguyên khác không.

Vậy định lý lớn Fermat đã được chứng minh.

Phú Vang, ngày 13/12/2018

Tác giả: Tôn Thất Hiệp