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.

Khi nhà toán học Andrew Wiles chứng minh định lý này bằng cách quay cả hai guồng máy khổng lồ của đại số và hình học thì tôi có cảm nhận: có thể giải định lý đó bằng công cụ toán học sơ cấp.

Tôi nổ lực hết mình trong một thời gian rất dài và tôi đã thành công.

Cho tới thời điểm này, tôi xin báo tin với mọi người rằng, tôi đã hoàn tất chứng minh định lý lớn Fermat bằng cách sử dụng *phép chia hết của các số nguyên* cùng với khai triển *nhị thức Newton*.

Dưới đây là toàn văn chứng minh định lý lớn Fermat.

Tôi đề xuất năm bổ đề 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,* $(a,b) = m, b \not\vdots\, m^2$, *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* $c_1 \not\vdots\, m$, $c_2 \not\vdots\, m$, $c = m^s c_1.c_2$, $a = m^{ns-1} c_1^n$ *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 $(u+v) \not\vdots\, n$ *thì* $\left(u+v, \sum_{i=0}^{n-1} (-1)^i u^{n-1-i} v^i\right) = 1$ *và* $\left(\sum_{i=0}^{n-1} (-1)^i u^{n-1-i} v^i\right) \not\vdots\, n$.

b) Nếu $(u-v) \not\vdots\, n$ *thì* $\left(u-v, \sum_{i=0}^{n-1} u^{n-i-1} v^i\right) = 1$ *và* $\left(\sum_{i=0}^{n-1} u^{n-i-1} v^i\right) \not\vdots\, n$.

c) Nếu $(u+v)\vdots n$ *thì* $\left(u+v,\sum_{i=0}^{n-1}(-1)^i u^{n-1-i}v^i\right)=n$ *và* $\left(\sum_{i=0}^{n-1}(-1)^i u^{n-1-i}v^i\right)\not\vdots\, n^2$.

d) Nếu $(u-v)\vdots n$ *thì* $\left(u-v,\sum_{i=0}^{n-1}u^{n-1-i}v^i\right)=n$ *và* $\left(\sum_{i=0}^{n-1}u^{n-1-i}v^i\right)\not\vdots\, n^2$.

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 $(u_0,v_0,t_0) = d$.

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 $u^n + v^n = t^n$ ($1''$), 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 $a = c'_1a_1$, $c = c'_1c'_2$.

Vì $ab = c^n$, nên $c_1a_1b = c_1^nc_2^n$, suy ra $a_1b = c_1^{n-1}c_2^n$, suy ra $b \mid c_1^{n-1}c_2^n$. Vì $(c'_1,b) = 1$ (do (a,b) = 1) nên $c'^n_2 = kb$, với k là số nguyên khác không, từ đẳng thức $a_1b = c'^{n-1}_1c'^n_2$, ta suy ra $a_1 = kc'^{n-1}_1$, suy ra $a_1^n = k^nc'^{n(n-1)}_1$, suy ra $k \mid a_1^n$ và $k \mid c'^n_2$; vì $(a_1,c'_2) = 1$ nên $(a_1^n,c'^n_2) = 1$, từ đó suy ra $|k| = 1$.

Vậy $b = kc'^n_2 = (kc'_2)^n = c_2^n$, $a = kc'^n_1 = (kc'_1)^n = c_1^n$, $c = c_1c_2$, với $c_1 = kc'_1$, $c_2 = kc'_2$ nguyên tố cùng nhau.

Bổ đề 3 đã được chứng minh.

1.4. Chứng minh bổ đề 4

Vì $a\vdots m$, $b\vdots m$ và $a.b = c^n$, suy ra $c^n\vdots m^2$, mặt khác $b\not\vdots\, m^2$.

Giả sử $c = m^sr$ với $s\in\mathbb{N}^*$, $r\in\mathbb{Z}^*$ và $r\not\vdots\, m$, mà $c^n = m^{ns}r^n\vdots\, m^2$, nên $ns \geq 2$.

Do (a,b) = m và $b\not\vdots\, m^2$, nên có thể giả sử b = mh và $a = m^kl$, với $k\in\mathbb{N}^*$; $h,l\in\mathbb{Z}^*$ sao cho $(h,l) = 1$, $h\not\vdots\, m$, $l\not\vdots\, m$.

Vì $a.b = c^n$ 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 là hai số nguyên sao cho $(c_1,c_2) = 1$. Từ đó ta có $c = m^sc_1.c_2$, $a = m^{ns-1}c_1^n$ và $b = mc_2^n$

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 $u^n+v^n=\left[(u+v)-v\right]^n+v^n=(u+v)\sum_{k=0}^{n-1}(-1)^k C_n^k (u+v)^{n-k-1}v^k$ 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 $A=(u+v)\sum_{k=0}^{n-2}(-1)^k C_n^k (u+v)^{n-k-2}v^k+nv^{n-1}$, (u,v) =1 và $(u+v)\not\vdots\, n$ nên $(u+v,nv^{n-1})=1$, suy ra $(A,u+v)=1$(đpcm).

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

c) Ta có $A=n(u+v)\left[\sum_{k=1}^{n-2}(-1)^k\frac{C_n^k}{n}(u+v)^{n-k-2}v^k+\frac{(u+v)^{n-2}}{n}\right]+nv^{n-1}=n(u+v)A_1+nv^{n-1}$, với

$\sum_{k=1}^{n-2}(-1)^k\frac{C_n^k}{n}(u+v)^{n-k-2}v^k+\frac{(u+v)^{n-2}}{n}=A_1$.

Với $k=\overline{1,n}$ thì $C_n^k\,\vdots\, n$ (vì n là số nguyên tố), mà $(u+v)\,\vdots\, n$ nên $n(u+v)A_1\,\vdots\, n^2$; mặt khác $nv^{n-1}\,\vdots\, n$ và $nv^{n-1}\not\vdots\, n^2$ (do $v\not\vdots\, n$), từ đó suy ra $n(u+v)A_1+nv^{n-1}=A\,\vdots\, n$ và $A\not\vdots\, n^2$, hơn nữa (u + v, A) = n (đpcm).

d) Vì n là số nguyên tố lẻ, nên từ c) ta thay v bởi –v ta có điều phải chứng minh.

2. Chứng minh định lý lớn Fermat

Ta cần xét bốn trường hợp của n.

2.1. 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 (áp dụng **bổ đề 1**), khi đó $u^n + v^n = t^n$ (3)

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

Do n lẻ và u, v, t là các số nguyên, nên có thể xem vai trò của các số này trong đẳng thức dạng (3) 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.

2.1.1. 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 $(u+v)\not\vdots\, n$, $(t-v)\not\vdots\, n$ và $(t-u)\not\vdots\, n$; áp dụng **bổ đề 5a) và 5b)** ta có $\left(u+v,\sum_{i=0}^{n-1}(-1)^i u^{n-i-1}v^i\right)=\left(t-v,\sum_{i=0}^{n-1}t^{n-i-1}v^i\right)=\left(t-u,\sum_{i=0}^{n-1}t^{n-i-1}u^i\right)=1$, $\left(\sum_{i=0}^{n-1}(-1)^i u^{n-i-1}v^i\right)\not\vdots\, n$, $\left(\sum_{i=0}^{n-1}t^{n-i-1}v^i\right)\not\vdots\, n$, $\left(\sum_{i=0}^{n-1}t^{n-i-1}u^i\right)\not\vdots\, n$, kết hợp với (4), (5), (6) và áp dụng **bổ đề 3** , ta có: u + v = c^n (3') 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 $c\not\vdots\, n$, $c'\not\vdots\, n$; 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 $b\not\vdots\, n$, $b'\not\vdots\, n$; 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 $a\not\vdots\, n$, $a'\not\vdots\, n$; (a,b) = (a,c) = (c,b) = 1.

Ta có: $c'^n = A = \sum_{i=0}^{n-1}(-1)^i u^{n-i-1}v^i = \sum_{k=0}^{n-1}(-1)^k C_n^k (u+v)^{n-k-1} v^k = \sum_{k=1}^{n-1}(-1)^k C_n^k (u+v)^{n-k-1} v^k + (u+v)^{n-1}$

$\Rightarrow c'^n - 1 = \sum_{k=1}^{n-1}(-1)^k C_n^k (u+v)^{n-k-1} v^k + \left[(u+v)^{n-1} - 1\right]$.

Vì n là số nguyên tố và $(u+v) \not\vdots\, n$, nên với $k = \overline{1,n}$ thì $C_n^k \vdots\, n$ và $\left[(u+v)^{n-1} - 1\right] \vdots\, n$ (định lý nhỏ Fermat). Do đó $(c'^n - 1) \vdots\, n$, mà $c' \not\vdots\, n$ nên $(c'^{n-1} - 1) \vdots\, n$, suy ra $c'^n - 1 - (c'^{n-1} - 1) = c'^{n-1}(c'-1) \vdots\, n$, suy ra $(c'-1) \vdots\, n$, 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) $\Leftrightarrow t^n - u - v = u^n + v^n - u - v \Rightarrow t^n - u - v = (c.c')^n - c^n = c^n\left[(1+nk_3)^n - 1\right] \vdots\, n^2$. Chứng minh tương tự ta cũng có $(u^n - t + v) \vdots\, n^2$ và $(v^n - t + u) \vdots\, n^2$ suy ra $(u^n - t + v) + (v^n - t + u) - (t^n - u - v) = 2(u + v - t) \vdots\, n^2 \Rightarrow (u + v - t) \vdots\, n^2$.

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 $k \not\vdots\, n$, 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 $a^n + b^n - c^n = -2n^s abck$.

Thay vào (3) ta có: $(a^n + n^s abck)^n + (b^n + n^s abck)^n = (c^n - n^s abck)^n$

$$\Leftrightarrow 3(n^s abck)^n + C_n^1(a^n + b^n - c^n)(n^s abck)^{n-1} - \sum_{i=0}^{n-2}(-1)^i C_n^i (n^s abck)^i c^{n(n-i)} + \sum_{i=0}^{n-2} C_n^i (n^s abck)^i b^{n(n-i)} + \sum_{i=0}^{n-2} C_n^i (n^s abck)^i a^{n(n-i)} = 0$$

$$\Leftrightarrow (3-2n)(n^s abck)^n - \sum_{i=0}^{n-2}(-1)^i C_n^i (n^s abck)^i c^{n(n-i)} + \sum_{i=0}^{n-2} C_n^i (n^s abck)^i b^{n(n-i)} + \sum_{i=0}^{n-2} C_n^i (n^s abck)^i a^{n(n-i)} = 0$$

$$\Leftrightarrow (3-2n)(n^s abck)^n + B + C + D = 0 \quad (7)$$

Với $B = \sum_{i=0}^{n-2} C_n^i (n^s abck)^i b^{n(n-i)}$, $C = -\sum_{i=0}^{n-2}(-1)^i C_n^i (n^s abck)^i c^{n(n-i)}$, $D = \sum_{i=0}^{n-2} C_n^i (n^s abck)^i a^{n(n-i)}$.

* Ta có:

$$D = \sum_{i=0}^{n-2} C_n^i (n^s abck)^i a^{n(n-i)} = \sum_{i=0}^{n-2} C_n^i (n^s abck)^i \sum_{l=0}^{n-i}(-1)^{n-i-l} C_{n-i}^l (a^n + b^n)^l b^{n(n-i-l)}$$

$$= \sum_{i=0}^{n-2} C_n^i (n^s abck)^i \sum_{l=0}^{n-i}(-1)^{n-i-l} C_{n-i}^l (c^n - 2n^s abck)^l b^{n(n-i-l)} \text{ (vì } a^n + b^n = c^n - 2n^s abck\text{)}$$

$$= \sum_{i=0}^{n-2} C_n^i (n^s abck)^i \sum_{l=0}^{n-i}(-1)^{n-i-l} C_{n-i}^l b^{n(n-i-l)} \sum_{p=0}^{l} C_l^p (-2)^p (n^s abck)^p c^{n(l-p)}$$

$$= \sum_{i=0}^{n-2}\sum_{l=0}^{n-i}\sum_{p=0}^{l} C_n^i C_{n-i}^l C_l^p (-1)^{n-i-l}(-2)^p b^{n(n-i-l)} c^{n(l-p)} (n^s abck)^{p+i} = E_{\left(b^{n(n-i-l)}, c^{n(l-p)}, (n^s abck)^{p+i}\right)} \quad (8)$$

1) Với mỗi m sao cho $m = \overline{0; n-2}$ ta nhận thấy: các số hạng của biểu thức D trong khai triển (8) chỉ chứa $b^{n(n-m)}(n^s abck)^m$ khi và chỉ khi p = l và l + i = m. Khi đó:

$E_{\left(b^{n(n-m)},\left(c^n\right)^0\left(n^s abck\right)^m\right)} = \sum_{i=0}^{n-2}\sum_{l=0}^{n-i} C_n^i C_{n-i}^l (-1)^{n-m}(-2)^l b^{n(n-m)}\left(n^s abck\right)^m$, suy ra

$E_{\left(b^{n(n-m)},\left(c^n\right)^0\left(n^s abck\right)^m\right)} = (-1)^{n-m}\sum_{i=0}^{m} C_n^i C_{n-i}^{m-i}(-2)^{m-i} b^{n(n-m)}\left(n^s abck\right)^m$. Do đó hệ số của số hạng chứa $b^{n(n-m)}\left(n^s abck\right)^m$ của biểu thức B + D là

$$E^1_{\left(b^{n(n-m)},\left(c^n\right)^0\left(n^s abck\right)^m\right)} = (-1)^{n-m}\sum_{i=0}^{m} C_n^i C_{n-i}^{m-i}(-2)^{m-i} + C_n^m = \frac{n!(-1)^{n-m}}{m!(n-m)!}\sum_{i=0}^{m}\frac{m!}{(m-i)!i!}(-2)^{m-i} + C_n^m =$$

$$= C_n^m(-1)^{n-m}\sum_{i=0}^{m} C_m^i(-2)^{m-i}.1^i + C_n^m = C_n^m\left[(-1)^{n-m}(1-2)^m + 1\right] = C_n^m\left[(-1)^{n-m}.(-1)^m + 1\right] = C_n^m\left[(-1)^n + 1\right] = 0.$$

2) Các số hạng của biểu thức D trong khai triển (8) chứa c^n nhưng không chứa c^{nh} và c^{n+r} ($h, r \in \mathbb{N}^*, h \geq 2$) khi và chỉ khi l = p + 1 và p + i = 0, suy ra p = i = 0, l = 1. Khi đó số hạng này là:

$$E_{\left(b^{n(n-1)},c^n,\left(n^s abck\right)^0\right)} = C_n^0 C_n^1 C_1^0(-1)^{n-1}(-2)^0 b^{n(n-1)}c^n = C_n^1 b^{n(n-1)}c^n.$$

3) Các số hạng của biểu thức D trong khai triển (8) chỉ chứa $b^n\left(n^s abck\right)^{n-1}$ khi và chỉ khi p = l và l + i = $n-1$. Khi đó: $E_{\left(b^n,\left(c^n\right)^0,\left(n^s abck\right)^{n-1}\right)} = -\sum_{i=0}^{n-2}\sum_{l=0}^{n-i} C_n^i C_{n-i}^l(-2)^l b^n\left(n^s abck\right)^{n-1} = -\sum_{i=0}^{n-2}(n-i)C_n^i(-2)^{n-1-i} b^n\left(n^s abck\right)^{n-1}$.

Do đó hệ số của số hạng chứa $b^n\left(n^s abck\right)^{n-1}$ của biểu thức D là

$$E^1_{\left(b^n,\left(c^n\right)^0,\left(n^s abck\right)^{n-1}\right)} = -\sum_{i=0}^{n-2}(n-i)C_n^i(-2)^{n-1-i} = C_n^{n-1}(-2)^0 - \boldsymbol{\sum_{i=0}^{n-1}(n-i)C_n^i(-2)^{n-1-i}.1^i} = n - n(-2+1)^{n-1} = 0.$$

Lưu ý:

Để tính tổng $\boldsymbol{\sum_{i=0}^{n-1}(n-i)C_n^i(-2)^{n-1-i}.1^i}$, ta xét đa thức xác định trên $\mathbb{R}$ là $f(x) = (x+1)^n = \sum_{i=0}^{n} C_n^i x^{n-i}$ suy ra $f'(x) = \sum_{i=0}^{n-1}(n-i)C_n^i x^{n-1-i}.1^i = n(x+1)^{n-1}$. Cho x = –2, ta có: $\sum_{i=0}^{n-1}(n-i)C_n^i(-2)^{n-1-i}.1^i = \boldsymbol{n(-2+1)^{n-1} = n}$.

4) Các số hạng của biểu thức D trong khai triển (8) chỉ chứa $\left(n^s abck\right)^n$ khi và chỉ khi p = l và l + i = n.

Khi đó: $E_{\left(\left(b^n\right)^0,\left(c^n\right)^0,\left(n^s abck\right)^n\right)} = \sum_{i=0}^{n-2}\sum_{l=0}^{n-i} C_n^i C_{n-i}^l(-2)^l\left(n^s abck\right)^n = \sum_{i=0}^{n-2} C_n^i(-2)^{n-i}\left(n^s abck\right)^n$, suy ra hệ số của số hạng chứa $\left(n^s abck\right)^n$ của biểu thức D là

$$E^1_{\left(\left(b^n\right)^0,\left(c^n\right)^0,\left(n^s abck\right)^n\right)} = \sum_{i=0}^{n-2} C_n^i(-2)^{n-i} = -C_n^{n-1}(-2) - C_n^n(-2)^0 + \sum_{i=0}^{n} C_n^i(-2)^{n-i}.1^i = 2n - 1 + (-2+1)^n = 2n-2.$$

Vậy số hạng chứa $\left(n^s abck\right)^n$ của biểu thức D là $E_{\left(\left(b^n\right)^0,\left(c^n\right)^0,\left(n^s abck\right)^n\right)} = (2n-2)\left(n^s abck\right)^n$

5) Với mỗi m sao cho $m = \overline{0; n-2}$, ta nhận thấy: các số hạng của biểu thức D trong khai triển (8) chỉ chứa $c^{n(n-m)}\left(n^s abck\right)^m$ khi và chỉ khi p + i = m và l + i = n. Khi đó:

$E_{\left(\left(b^n\right)^0, c^{n(n-m)}, \left(n^s abck\right)^m\right)} = \sum_{i=0}^{n-2} C_n^i \left(-2\right)^{m-i} c^{n(n-m)} \left(n^s abck\right)^m$. Do đó hệ số của số hạng chứa $c^{n(n-m)}\left(n^s abck\right)^m$ của biểu thức C + D là

$$E^1_{\left(\left(b^n\right)^0, c^{n(n-m)}, \left(n^s abck\right)^m\right)} = \sum_{i=0}^{m} C_n^i C_{n-i}^{m-i} \left(-2\right)^{m-i} - \left(-1\right)^m C_n^m = \frac{n!}{m!\left(n-m\right)!} \sum_{i=0}^{m} \frac{m!}{\left(m-i\right)!i!} \left(-2\right)^{m-i} - \left(-1\right)^m C_n^m =$$

$$= C_n^m \sum_{i=0}^{m} C_m^i \left(-2\right)^{m-i}.1^i - \left(-1\right)^m C_n^m = C_n^m \left[\left(1-2\right)^m - \left(-1\right)^m\right] = C_n^m \left[\left(-1\right)^m - \left(-1\right)^m\right] = 0.$$

6) Các số hạng của biểu thức D trong khai triển (8) chứa b^n nhưng không chứa b^{nh} và b^{n+r} ($h, r \in \mathbb{N}^*, h \geq 2$) khi và chỉ khi l + i = n – 1 và p + i = 0 suy ra p = i = 0, l = n – 1. Khi đó số hạng này là: $E_{\left(b^n, c^{n(n-1)}, \left(n^s abck\right)^0\right)} = C_n^0 C_n^{n-1} C_1^0 \left(-1\right)^1 \left(-2\right)^0 c^{n(n-1)} b^n = -C_n^1 c^{n(n-1)} b^n$.

7) Các số hạng của biểu thức D trong khai triển (8) chỉ chứa $c^n\left(n^s abck\right)^{n-1}$ khi và chỉ khi p + i = $n-1$, l = p + 1 và l + i = n. Khi đó: $E_{\left(\left(b^n\right)^0, c^n, \left(n^s abck\right)^{n-1}\right)} = -\sum_{i=0}^{n-2}\sum_{l=0}^{n-i} C_n^i C_{n-i}^{n-1-i} \left(-2\right)^{n-1-i} c^n \left(n^s abck\right)^{n-1} = -\sum_{i=0}^{n-2} \left(n-i\right) C_n^i \left(-2\right)^{n-1-i} c^n \left(n^s abck\right)^{n-1}$, do đó hệ số của số hạng chứa $c^n\left(n^s abck\right)^{n-1}$ của biểu thức D là

$$E^1_{\left(\left(b^n\right)^0, c^n, \left(n^s abck\right)^{n-1}\right)} = -\sum_{i=0}^{n-2} \left(n-i\right) C_n^i \left(-2\right)^{n-1-i} = C_n^{n-1}\left(-2\right)^0 - \sum_{i=0}^{n-1} \left(n-i\right) C_n^i \left(-2\right)^{n-1-i}.1^i = n - n\left(-2+1\right)^{n-1} = 0.$$

8) Các số hạng của biểu thức D trong khai triển (8) chứa $b^{n(n-i-l)} c^{n(l-p)} \left(n^s abck\right)$ khi và chỉ khi (p = 0 và i = 1 và $l \neq 0$ và $l \neq$ n – 1) hoặc (p = 1 và i = 0 và $l \neq 1$ và $l \neq$ n). Khi đó:

$$E^{l \neq p, l \neq n-i}_{\left(b^{n(n-i-l)}, c^{n(l-p)}, n^s abck\right)} = \left[\sum_{l=0}^{n-1} C_n^1 C_{n-1}^l C_l^0 \left(-1\right)^{n-1-l} \left(-2\right)^0 b^{n(n-1-l)} c^{nl} \left(n^s abck\right) - n\left(b^{n(n-1)} + c^{n(n-1)}\right)\left(n^s abck\right)\right] +$$

$$+\left[\sum_{l=1}^{n} C_n^0 C_n^l C_l^1 \left(-1\right)^{n-l} \left(-2\right)^1 b^{n(n-l)} c^{n(l-1)} \left(n^s abck\right) + 2n\left(b^{n(n-1)} + c^{n(n-1)}\right)\left(n^s abck\right)\right]$$

$$= n\sum_{l=0}^{n-1} C_{n-1}^l \left(-b^n\right)^{n-1-l} c^{nl} \left(n^s abck\right) - 2\sum_{l=1}^{n} \boldsymbol{l C_n^l \left(-b^n\right)^{n-l} c^{n(l-1)} \left(n^s abck\right)} + n\left(b^{n(n-1)} + c^{n(n-1)}\right)\left(n^s abck\right)$$

$$= n\left(b^n - c^n\right)^{n-1}\left(n^s abck\right) - 2n\left(c^n - b^n\right)^{n-1}\left(n^s abck\right) + n\left(b^{n(n-1)} + c^{n(n-1)}\right)\left(n^s abck\right)$$

$$= -n\left(b^n - c^n\right)^{n-1}\left(n^s abck\right) + n\left(b^{n(n-1)} + c^{n(n-1)}\right)\left(n^s abck\right).$$

Lưu ý:

Để tính tổng $\boldsymbol{\sum_{l=1}^{n} l C_n^l \left(-b^n\right)^{n-l} c^{n(l-1)} \left(n^s abck\right)}$, ta xét đa thức xác định trên $\mathbb{R}$ là $f(x) = \left(x - b^n\right)^n = \sum_{l=0}^{n} C_n^l \left(-b^n\right)^{n-l} x^l$, suy ra $f'(x) = \sum_{l=1}^{n} l C_n^l \left(-b^n\right)^{n-l} x^{l-1} = n\left(x - b^n\right)^{n-1}$. Cho x = c^n, ta có:

$$\sum_{l=1}^{n} l C_n^l \left(-b^n\right)^{n-l} c^{n(l-1)} \left(n^s abck\right) = \boldsymbol{n\left(c^n - b^n\right)^{n-1}\left(n^s abck\right)}.$$

9) Vì ta đã xác định được các số hạng trong khai triển dạng (8) của biểu thức D ứng với (p = l và p + i = m,

với $m=\overline{0;n-2}$), (p = i = 0 và l = 1), (p + i = n – 1 và $p = l$), (p = l và p + i = n), (l + i = n và p + i = m, với $m=\overline{0;n-2}$), (p = i = 0 và l = n – 1), (p + i = n – 1 và l = p + 1 và l + i = n), [(p = 0 và i = 1 và $l \neq 0$ và $l \neq$ n – 1) hoặc (p = 1 và i = 0 và $l \neq 1$ và $l \neq$ n)] nên ta có:

$$B+C+D=\sum_{i=0}^{n-2}\sum_{l=0}^{n-i}\sum_{n-3\geq p+i\geq 2,\,p=0}^{l} C_n^i C_{n-i}^l C_l^p (-1)^{n-i-l}(-2)^p b^{n(n-i-l)}c^{n(l-p)}\left(n^s abck\right)^{p+i}+E_{\left(\left(b^n\right)^0,\left(c^n\right)^0,\left(n^s abck\right)^n\right)}+E^{l\neq p,l\neq n-i}_{\left(b^{n(n-i-l)},c^{n(l-p)},\left(n^s abck\right)\right)}+$$

$$+E_{\left(b^{n(n-1)},c^n,\left(n^s abck\right)^0\right)}-E_{\left(b^n,c^{n(n-1)},\left(n^s abck\right)^0\right)}=\sum_{i=0}^{n-2}\sum_{l=0}^{n-i}\sum_{n-3\geq p+i\geq 2,\,p=0}^{l} C_n^i C_{n-i}^l C_l^p (-1)^{n-i-l}(-2)^p b^{n(n-i-l)}c^{n(l-p)}\left(n^s abck\right)^{p+i}+$$

$$+(2n-2)\left(n^s abck\right)^n-n\left(b^n-c^n\right)^{n-1}\left(n^s abck\right)+n\left(b^{n(n-1)}+c^{n(n-1)}\right)\left(n^s abck\right)+C_n^1 b^{n(n-1)}c^n-C_n^1 c^{n(n-1)}b^n.$$

Từ đẳng thức (7) ta suy ra

$$\sum_{i=0}^{n-2}\sum_{l=0}^{n-i}\sum_{n-3\geq p+i\geq 2,\,p=0}^{l} C_n^i C_{n-i}^l C_l^p (-1)^{n-i-l}(-2)^p b^{n(n-i-l)}c^{n(l-p)}\left(n^s abck\right)^{p+i}+\left(n^s abck\right)^n-n\left(b^n-c^n\right)^{n-1}\left(n^s abck\right)+$$

$$+n\left(b^{n(n-1)}+c^{n(n-1)}\right)\left(n^s abck\right)+C_n^1 b^{n(n-1)}c^n-C_n^1 c^{n(n-1)}b^n=0.$$

$$\Leftrightarrow \sum_{i=0}^{n-2}\sum_{l=0}^{n-i}\sum_{n-3\geq p+i\geq 2,\,p=0}^{l} C_n^i C_{n-i}^l C_l^p (-1)^{n-i-l}(-2)^p b^{n(n-i-l)}c^{n(l-p)}\left(n^s abck\right)^{p+i}+\left(n^s abck\right)^n-na^n\left(a^{n-1}+2n^s bck\right)^{n-1}\left(n^s bck\right)+$$

$$+C_n^1 b^{n(n-1)}c^n-C_n^1 c^{n(n-1)}b^n+n\left(b^{n(n-1)}+c^{n(n-1)}\right)\left(n^s abck\right)=0 \text{ (vì } b^n-c^n=-a^n-2n^s abck\text{)}$$

$\Leftrightarrow F+L=0$ (9).

Với $F=\sum_{i=0}^{n-2}\sum_{l=0}^{n-i}\sum_{n-3\geq p+i\geq 2,\,p=0}^{l} C_n^i C_{n-i}^l C_l^p (-1)^{n-i-l}(-2)^p b^{n(n-i-l)}c^{n(l-p)}\left(n^s abck\right)^{p+i}+\left(n^s abck\right)^n-na^n\left(a^{n-1}+2n^s bck\right)^{n-1}\left(n^s bck\right)$

$L=C_n^1 b^{n(n-1)}c^n-C_n^1 c^{n(n-1)}b^n+n\left(b^{n(n-1)}+c^{n(n-1)}\right)\left(n^s abck\right)$.

Ta có $F \vdots a^2$ (vì n ≥ 5), vì vậy từ đẳng thức (9) ta suy ra $L \vdots a^2$.

* Ta có:

$$L=n\left(n^s abck\right)\left[\sum_{i=0}^{n-1}C_{n-1}^i\left(b^n-c^n\right)^{n-1-i}c^{ni}+c^{n(n-1)}\right]+nb^nc^n\left[\sum_{i=0}^{n-2}C_{n-2}^i\left(b^n-c^n\right)^{n-2-i}c^{ni}-c^{n(n-2)}\right]$$

$$=n\left(n^s abck\right)\left[\sum_{i=0}^{n-2}C_{n-1}^i\left(b^n-c^n\right)^{n-1-i}c^{ni}+2c^{n(n-1)}\right]+nb^nc^n\left[\sum_{i=0}^{n-4}C_{n-2}^i\left(b^n-c^n\right)^{n-2-i}c^{ni}+(n-2)\left(b^n-c^n\right)c^{n(n-3)}\right]$$

$$=\left[n\left(n^s abck\right)\sum_{i=0}^{n-2}C_{n-1}^i\left(b^n-c^n\right)^{n-1-i}c^{ni}+nb^nc^n\sum_{i=0}^{n-4}C_{n-2}^i\left(b^n-c^n\right)^{n-2-i}c^{ni}\right]+$$

$$+\left[2nc^{n(n-1)}\left(n^s abck\right)+n(n-2)\left(b^n-c^n\right)b^nc^{n(n-2)}\right]=M+N.$$

Với $M=n\left(n^s abck\right)\sum_{i=0}^{n-2}C_{n-1}^i\left(b^n-c^n\right)^{n-1-i}c^{ni}+nb^nc^n\sum_{i=0}^{n-4}C_{n-2}^i\left(b^n-c^n\right)^{n-2-i}c^{ni}$ và

$N=2nc^{n(n-1)}\left(n^s abck\right)+n(n-2)\left(b^n-c^n\right)b^nc^{n(n-2)}$.

* Vì $b^n-c^n=a\left(-a^{n-1}-2n^s bck\right)\vdots a$ nên $M \vdots a^2$, mà $L \vdots a^2$, nên $L-M=N \vdots a^2$.

Ta có:

$$N=2nc^{n(n-1)}\left(n^s abck\right)+n(n-2)\left(-a^n-2n^s abck\right)b^nc^{n(n-2)}$$

$$=2nc^{n(n-1)}\left(n^s abck\right)-n(n-2)a^nb^nc^{n(n-2)}-2n(n-2)\left(n^s abck\right)b^nc^{n(n-2)}$$

$$= -n(n-2)a^n b^n c^{n(n-2)} + 2nc^{n(n-2)}\left(n^s abck\right)\left[c^n - (n-2)b^n\right].$$

$$= -n(n-2)a^n b^n c^{n(n-2)} + 2nc^{n(n-2)}\left(n^s abck\right)\left[c^n - b^n - (n-3)b^n\right]$$

$$= -n(n-2)a^n b^n c^{n(n-2)} + 2nc^{n(n-2)}\left(n^s abck\right)\left[a^n + 2\left(n^s abck\right) - (n-3)b^n\right]$$

$$= \left[-n(n-2)a^n b^n c^{n(n-2)} + 2na^n c^{n(n-2)}\left(n^s abck\right) + 4nc^{n(n-2)}\left(n^s abck\right)^2\right] - \left[2n\left(n^s abck\right)(n-3)c^{n(n-2)}b^n\right]$$

$$= P - Q.$$

Với $P = -n(n-2)a^n b^n c^{n(n-2)} + 2na^n c^{n(n-2)}\left(n^s abck\right) + 4nc^{n(n-2)}\left(n^s abck\right)^2$ và $Q = 2n\left(n^s abck\right)(n-3)c^{n(n-2)}b^n$

Vì $N \vdots a^2$ và $P \vdots a^2$ nên $P - N = Q \vdots a^2$, suy ra $k = 0$ hoặc $2(n-3) \vdots a$ (nếu k $\neq$ 0).

Chứng minh tương tự ta cũng có:

$$* \; B+C+D = \sum_{i=0}^{n-2}\sum_{l=0}^{n-i}\sum_{n-3\geq p+i\geq 2,\, p=0}^{l} C_n^i C_{n-i}^l C_l^p (-1)^{n-i-l}(-2)^p a^{n(n-i-l)} c^{n(l-p)}\left(n^s abck\right)^{p+i} + E_{\left(\left(a^n\right)^0,\left(c^n\right)^0,\left(n^s abck\right)^n\right)} + E^{l\neq p, l\neq n-i}_{\left(a^{n(n-i-l)},c^{n(l-p)},\left(n^s abck\right)\right)} +$$

$$+E_{\left(a^{n(n-1)},c^n,\left(n^s abck\right)^0\right)} - E_{\left(a^n,c^{n(n-1)},\left(n^s abck\right)^0\right)} = \sum_{i=0}^{n-2}\sum_{l=0}^{n-i}\sum_{n-3\geq p+i\geq 2,\, p=0}^{l} C_n^i C_{n-i}^l C_l^p (-1)^{n-i-l}(-2)^p a^{n(n-i-l)} c^{n(l-p)}\left(n^s abck\right)^{p+i} +$$

$+(2n-2)\left(n^s abck\right)^n - n\left(a^n - c^n\right)^{n-1}\left(n^s abck\right) + n\left(a^{n(n-1)} + c^{n(n-1)}\right)\left(n^s abck\right) + C_n^1 a^{n(n-1)}c^n - C_n^1 c^{n(n-1)}a^n$. Từ đó suy ra $C_n^1 a^{n(n-1)}c^n - C_n^1 c^{n(n-1)}a^n + n\left(a^{n(n-1)} + c^{n(n-1)}\right)\left(n^s abck\right) = R \vdots b^2$, suy ra $\left[2n\left(n^s abck\right)(n-3)c^{n(n-2)}a^n\right] \vdots b^2$ suy ra k = 0 hoặc $2(n-3) \vdots b$ (nếu k $\neq$ 0).

$$* B+C+D = \sum_{i=0}^{n-2}\sum_{l=0}^{n-i}\sum_{n-3\geq p+i\geq 2,\, p=0}^{l} C_n^i C_{n-i}^l C_l^p (-1)^{n-i} 2^p b^{n(n-i-l)} a^{n(l-p)}\left(n^s abck\right)^{p+i} + E'_{\left(\left(b^n\right)^0,\left(a^n\right)^0,\left(n^s abck\right)^n\right)} + E'^{l\neq p, l\neq n-i}_{\left(b^{n(n-i-l)},a^{n(l-p)},\left(n^s abck\right)\right)} -$$

$$-E'_{\left(b^{n(n-1)},a^n,\left(n^s abck\right)^0\right)} - E'_{\left(b^n,a^{n(n-1)},\left(n^s abck\right)^0\right)} = \sum_{i=0}^{n-2}\sum_{l=0}^{n-i}\sum_{n-3\geq p+i\geq 2,\, p=0}^{l} C_n^i C_{n-i}^l C_l^p (-1)^{n-i} 2^p b^{n(n-i-l)} a^{n(l-p)}\left(n^s abck\right)^{p+i}$$

$+(2n-2)\left(n^s abck\right)^n - n\left(a^n + b^n\right)^{n-1}\left(n^s abck\right) + n\left(a^{n(n-1)} + b^{n(n-1)}\right)\left(n^s abck\right) - \left(C_n^1 a^{n(n-1)}b^n + C_n^1 b^{n(n-1)}a^n\right)$. Với $E'_{\left(\left(b^n\right)^{n-i-l},\left(a^n\right)^{l-p},\left(n^s abck\right)^{p+i}\right)} = \sum_{i=0}^{n-2}\sum_{l=0}^{n-i}\sum_{p=0}^{l} C_n^i C_{n-i}^l C_l^p (-1)^{n-i} 2^p b^{n(n-i-l)} a^{n(l-p)}\left(n^s abck\right)^{p+i}$.

Từ đó suy ra $-\left(C_n^1 a^{n(n-1)}b^n + C_n^1 b^{n(n-1)}a^n\right) + n\left(a^{n(n-1)} + b^{n(n-1)}\right)\left(n^s abck\right) = S \vdots c^2$, suy ra $\left[2n\left(n^s abck\right)(n-3)a^{n(n-2)}b^n\right] \vdots c^2$ suy ra k = 0 hoặc $2(n-3) \vdots c$ (nếu k $\neq$ 0).

Đến đây ta tóm tắt những điều đã chứng minh ở **2.1.1** bởi định lý sau:

Định lý 1:

Cho n là số nguyên tố lớn hơn 3.

Giả sử x = u, y = v, z = t là một nghiệm nguyên khác không của PT: $x^n + y^n = z^n$, với (u, v) = (u, t) = = (v, t) = 1 và u, v, t đều không chia hết cho n.

Khi đó tồn tại số nguyên s với s ≥ 2 và tồn tại bốn số nguyên khác không a, b, c, k và đều không chia hết

cho n, sao cho (a,b) = (a,c) = (a,k) = (b,c) = (b,k) = (c,k) = 1, đồng thời a | 2(n – 3), b | 2(n – 3), c | 2(n – 3), v = $a^n + n^s abck$, u = $b^n + n^s abck$, t = $c^n - n^s abck$ và u + v – t = $n^s abck$.

Nhận thấy:

Từ đẳng thức (3) và do n lẻ nên ta có thể giả sử u, v, t đều dương, suy ra t > u, t > v, suy ra u + v = $c^n > 0$, t – v = $b^n > 0$, t – u = $a^n > 0$, suy ra ***a, b, c đều dương***.

Do tính chẵn, lẻ của các số u, v, t trong đẳng thức (3) là bình đẳng và trong chúng có duy nhất một số chẵn và hai số còn lại là lẻ, cho nên, không mất tính tổng quát ta giả sử thêm: ***c chẵn, còn a và b đều lẻ***.

Xét hai trường hợp.

2.1.1.1. Khi k ≠ 0

Theo chứng minh trên, với k ≠ 0, ta có: a | 2(n – 3), b | 2(n – 3) và c | 2(n – 3), suy ra abc | 2(n – 3) (vì (c,a) = (c,b) = (b,a) =1), từ đó: $2(n-3) = rabc, r \in \mathbb{N}^*$.

Ta lại có: $n^s abck = u + v - t = b(1+nk_2) + a(1+nk_1) - c(1+nk_3) \Rightarrow a + b - c = n\left(n^{s-1}abck - ak_1 - bk_2 + ck_3\right)$

$\Rightarrow a + b - c = nm, m \in \mathbb{Z}$.

Ta có $a + b - c = nm = 2(n-3)\dfrac{m}{2} + 3m = \dfrac{rabcm}{2} + 3m \Leftrightarrow 2(a+b) = (rabm+2)c + 6m$ (10)

1) Với m ≥ 1

Vì c chẵn và $a, b, c, m, r \in \mathbb{N}^*$, nên $c \geq 2$ và $rabm + 2 > ab + 1 \geq a + b$, suy ra $2(a+b) < (rabm+2)c + 6m$, trái với (10).

2) Với $m \leq -1$

Vì ab ≥ 1, nên xét hai trường hợp.

a) Nếu $ab = 1$

Suy ra a = b =1, khi đó $c^n = u + v = 2 + 2.n^s ck = 2(1 + n^s ck) \Rightarrow c = 2$ *và* $n = 1$, vô lý.

b) Nếu ab ≥ 2

Suy ra $(rabm+2)c + 6m < 0 < 2(a+b)$, trái với (10).

3) Với m = 0

Ta có a + b = c. Vì $c^n = a^n + b^n + 2n^s abck$ nên

$$(a+b)^n = a^n + b^n + 2n^s ab(a+b)k \Rightarrow (a+b)^{n-1} - \sum_{i=0}^{n-1}(-1)^i a^{n-1-i}b^i = 2n^s abk \Rightarrow (a+b)^{n-1} - \sum_{i=0}^{n-1}(-1)^i a^{n-1-i}b^i = R \vdots 2$$

Vì a, b là hai số lẻ nên a + b là số chẵn và $\sum_{i=0}^{n-1}(-1)^i a^{n-1-i}b^i$ là số lẻ, suy ra R là số lẻ, suy ra $R \not\vdots 2$, mâu thuẫn.

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

2.1.1.2. Khi k = 0

Ta nhận thấy khi k = 0 thì $\begin{cases} u+v=t \\ t-u=v \\ t-v=u \end{cases} \Rightarrow \begin{cases} c^n = c.c' \\ a^n = a.a' \\ b^n = b.b' \end{cases} \Rightarrow \begin{cases} c = c' = 1 \\ a = a' = 1 \\ b = b' = 1 \end{cases}$ (vì (c,c') = (a, a') = (c, c') = 1 và a, b, c > 0)

$\Rightarrow u = v = t = 1$, không thỏa (3).

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

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

Không mất tính tổng quát ta giả sử $t \vdots n$,từ (4) suy ra $(u+v) \vdots n$, 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* $\left(\sum_{i=0}^{n-1}(-1)^i u^{n-1-i}v^i\right) \not\vdots\, n^2$, kết hợp với (4) và áp dụng **bổ đề 4** ta có u + v = $n^{sn-1}c^n$ và $\sum_{i=0}^{n-1}(-1)^i u^{n-1-i}v^i = nc'^n$ với t = n^sc.c', $s \in \mathbb{N}^*$; $c, c' \in \mathbb{Z}^*$ (c, c') = 1, $c \not\vdots\, n,\ c' \not\vdots\, n$.

Từ (5), (6) suy ra $(t-v) \not\vdots\, n$ *và* $(t-u) \not\vdots\, n$, áp dụng **bổ đề 5b)** ta có $\left(t-v, \sum_{i=0}^{n-1}t^{n-i-1}v^i\right) = \left(t-u, \sum_{i=0}^{n-1}t^{n-i-1}u^i\right) = 1$, $\left(\sum_{i=0}^{n-1}t^{n-i-1}v^i\right) \not\vdots\, n$, $\left(\sum_{i=0}^{n-1}t^{n-i-1}u^i\right) \not\vdots\, n$, kết hợp với (5), (6) và áp dụng **bổ đề 3** ta có t – v = b^n 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, $b \not\vdots\, n,\ b' \not\vdots\, n$; t – u = a^n, 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, $a \not\vdots\, n,\ a' \not\vdots\, n$; (a,b) = (a,c) = (c,b) = 1.

Lập luận như **2.1.1** (trang 3, 4) ta có b' = 1 + nk_2, a' = 1 + nk_1; và $(u+v-t) \vdots n^2$, mà $u+v-t = n^s c\left(n^{ns-1-s}c^{n-1} - c'\right) = a\left(a' - a^{n-1}\right) = b\left(b' - b^{n-1}\right) = n^s abck$ nên $s \geq 2$; (k,a) = (k,b) = (k,c) =1 và $k \not\vdots\, n$, nếu k ≠ 0.

Suy ra $v = a^n + n^s abck$, $v = b^n + n^s abck$, $t = n^{ns-1}c^n - n^s abck$ và $a^n + b^n = n^{ns-1}c^n - 2n^s abck$.

Thay vào (3), ta có: $\left(a^n + n^s abck\right)^n + \left(b^n + n^s abck\right)^n = \left(n^{ns-1}c^n - n^s abck\right)^n$

$$\Leftrightarrow 3\left(n^s abck\right)^n + C_n^1\left(a^n + b^n - n^{ns-1}c^n\right)\left(n^s abck\right)^{n-1} - \sum_{i=0}^{n-2}(-1)^i C_n^i\left(n^s abck\right)^i\left(n^{ns-1}c^n\right)^{n-i} + \sum_{i=0}^{n-2}C_n^i\left(n^s abck\right)^i b^{n(n-i)} + \sum_{i=0}^{n-2}C_n^i\left(n^r abck\right)^i a^{n(n-i)} = 0$$

$$\Leftrightarrow (3-2n)\left(n^s abck\right)^n - \sum_{i=0}^{n-2}(-1)^i C_n^i\left(n^s abck\right)^i\left(n^{ns-1}c^n\right)^{n-i} + \sum_{i=0}^{n-2}C_n^i\left(n^s abck\right)^i b^{n(n-i)} + \sum_{i=0}^{n-2}C_n^i\left(n^s abck\right)^i a^{n(n-i)} = 0$$

$$\Leftrightarrow (3-2n)\left(n^s abck\right)^n + B_1 + C_1 + D_1 = 0 \ (11).$$

Với $B_1 = \sum_{i=0}^{n-2}C_n^i\left(n^s abck\right)^i b^{n(n-i)}$, $C_1 = -\sum_{i=0}^{n-2}(-1)^i C_n^i\left(n^s abck\right)^i\left(n^{ns-1}c^n\right)^{n-i}$, $D_1 = \sum_{i=0}^{n-2}C_n^i\left(n^s abck\right)^i a^{n(n-i)}$.

* Ta có:

$$D_1 = \sum_{i=0}^{n-2}C_n^i\left(n^s abck\right)^i a^{n(n-i)} = \sum_{i=0}^{n-2}C_n^i\left(n^s abck\right)^i\sum_{l=0}^{n-i}C_{n-i}^l\left(a^n + b^n\right)^l b^{n(n-i-l)}$$

$$= \sum_{i=0}^{n-2}C_n^i\left(n^s abck\right)^i\sum_{l=0}^{n-i}C_{n-i}^l b^{n(n-i-l)}\left(n^{ns-1}c^n - 2n^s abck\right)^l$$

$$= \sum_{i=0}^{n-2}C_n^i\left(n^s abck\right)^i\sum_{l=0}^{n-i}C_{n-i}^l b^{n(n-i-l)}\sum_{p=0}^{l}C_l^p(-2)^p\left(n^s abck\right)^p\left(n^{ns-1}c^n\right)^{l-p}$$

$$= \sum_{i=0}^{n-2}\sum_{l=0}^{n-i}\sum_{p=0}^{l}C_n^i C_{n-i}^l C_l^p(-2)^p b^{n(n-i-l)}\left(n^{ns-1}c^n\right)^{l-p}\left(n^s abck\right)^{p+i} = E_{\left(b^{n(n-i-l)},\left(n^{ns-1}c^n\right)^{l-p},\left(n^s abck\right)^{p+i}\right)} \ (12)$$

Xác định các số hạng của biểu thức D_1 trong khai triển (12) hoàn toàn tương tự như cách xác định các số hạng của biểu thức D trong khai triển (8) (xem **2.1.1** trang 4, 5, 6, 7), ta được

$$B_1+C_1+D_1=\sum_{i=0}^{n-2}\sum_{l=0}^{n-i}\sum_{n-3\geq p+i\geq 2,p=0}^{l} C_n^i C_{n-i}^l C_l^p (-1)^{n-i-l}(-2)^p b^{n(n-i-l)}\left(n^{ns-1}c^n\right)^{l-p}\left(n^s abck\right)^{p+i}+E_{\left(\left(b^n\right)^0,\left(n^{ns-1}c^n\right)^n,\left(n^s abck\right)^n\right)}+E^{l\neq p,l\neq n-i}_{\left(b^{n(n-i-l)},\left(n^{ns-1}c^n\right)^{l-p},\left(n^s abck\right)\right)}+$$

$$+E_{\left(b^{n(n-1)},n^{ns-1}c^n,\left(n^s abck\right)^0\right)}-E_{\left(b^n,\left(n^{ns-1}c^n\right)^{n-1},\left(n^s abck\right)^0\right)}=\sum_{i=0}^{n-2}\sum_{l=0}^{n-i}\sum_{n-3\geq p+i\geq 2,p=0}^{l} C_n^i C_{n-i}^l C_l^p (-1)^{n-i-l}(-2)^p b^{n(n-i-l)}\left(n^{ns-1}c^n\right)^{l-p}\left(n^s abck\right)^{p+i}+$$

$$+(2n-2)\left(n^s abck\right)^n-n\left(b^n-n^{ns-1}c^n\right)^{n-1}\left(n^s abck\right)+n\left[b^{n(n-1)}+\left(n^{ns-1}c^n\right)^{n-1}\right]\left(n^s abck\right)+C_n^1 b^{n(n-1)}n^{ns-1}c^n-$$

$-C_n^1\left(n^{ns-1}c^n\right)^{n-1}b^n$. Vì vậy, từ đẳng thức (12) ta suy ra

$$\sum_{i=0}^{n-2}\sum_{l=0}^{n-i}\sum_{n-3\geq p+i\geq 2,p=0}^{l} C_n^i C_{n-i}^l C_l^p (-1)^{n-i-l}(-2)^p b^{n(n-i-l)}\left(n^{ns-1}c^n\right)^{l-p}\left(n^s abck\right)^{p+i}+\left(n^s abck\right)^n-n\left(b^n-n^{ns-1}c^n\right)^{n-1}\left(n^s abck\right)+$$

$$+n\left[b^{n(n-1)}+\left(n^{ns-1}c^n\right)^{n-1}\right]\left(n^s abck\right)+C_n^1 b^{n(n-1)}n^{ns-1}c^n-C_n^1\left(n^{ns-1}c\right)^{n-1}b^n=0.$$

Lập luận chứng minh tương tự như **2.1.1** (trang 7, 8) ta suy ra được $C_n^1 b^{n(n-1)}n^{ns-1}c^n-C_n^1\left(n^{ns-1}c^n\right)^{n-1}b^n+n\left[b^{n(n-1)}+\left(n^{ns-1}c^n\right)^{n-1}\right]\left(n^s abck\right)=L_1\vdots a^2$, suy ra

$\left[2n\left(n^s abck\right)(n-3)\left(n^{ns-1}c^n\right)^{n-2}b^n\right]\vdots a^2$ suy ra k = 0 hoặc $2(n-3)\vdots a$ (nếu k $\neq$ 0).

Biến đổi tương tự ta cũng có:

$$*\,B_1+C_1+D_1=\sum_{i=0}^{n-2}\sum_{l=0}^{n-i}\sum_{n-3\geq p+i\geq 2,p=0}^{l} C_n^i C_{n-i}^l C_l^p (-1)^{n-i-l}(-2)^p a^{n(n-i-l)}\left(n^{ns-1}c^n\right)^{l-p}\left(n^s abck\right)^{p+i}+E_{\left(\left(a^n\right)^0,\left(n^{ns-1}c^n\right)^n,\left(n^s abck\right)^n\right)}+E^{l\neq p,l\neq n-i}_{\left(a^{n(n-i-l)},\left(n^{ns-1}c^n\right)^{l-p},\left(n^s abck\right)\right)}+$$

$$+E_{\left(a^{n(n-1)},n^{ns-1}c^n,\left(n^s abck\right)^0\right)}-E_{\left(a^n,\left(n^{ns-1}c^n\right)^{n-1},\left(n^s abck\right)^0\right)}=\sum_{i=0}^{n-2}\sum_{l=0}^{n-i}\sum_{n-3\geq p+i\geq 2,p=0}^{l} C_n^i C_{n-i}^l C_l^p (-1)^{n-i-l}(-2)^p a^{n(n-i-l)}\left(n^{ns-1}c^n\right)^{l-p}\left(n^s abck\right)^{p+i}+$$

$$+(2n-2)\left(n^s abck\right)^n-n\left(a^n-n^{ns-1}c^n\right)^{n-1}\left(n^s abck\right)+n\left[a^{n(n-1)}+\left(n^{ns-1}c^n\right)^{n-1}\right]\left(n^s abck\right)+C_n^1 a^{n(n-1)}n^{ns-1}c^n-$$

$-C_n^1\left(n^{ns-1}c^n\right)^{n-1}a^n$. Từ đó suy ra $C_n^1 a^{n(n-1)}n^{ns-1}c^n-C_n^1\left(n^{ns-1}c^n\right)^{n-1}a^n+n\left[a^{n(n-1)}+\left(n^{ns-1}c^n\right)^{n-1}\right]\left(n^s abck\right)=P_1\vdots b^2$,

suy ra $\left[2n\left(n^s abck\right)(n-3)\left(n^{ns-1}c^n\right)^{n-2}a^n\right]\vdots b^2$ suy ra k = 0 hoặc $2(n-3)\vdots b$ (nếu k $\neq$ 0).

$$*\,B_1+C_1+D_1=\sum_{i=0}^{n-2}\sum_{l=0}^{n-i}\sum_{n-3\geq p+i\geq 2,p=0}^{l} C_n^i C_{n-i}^l C_l^p (-1)^{n-i}2^p b^{n(n-i-l)}a^{n(l-p)}\left(n^s abck\right)^{p+i}+E'_{\left(\left(b^n\right)^0,\left(a^n\right)^0,\left(n^s abck\right)^n\right)}+E'^{l\neq p,l\neq n-i}_{\left(b^{n(n-i-l)},a^{n(l-p)},\left(n^s abck\right)\right)}-$$

$$-E'_{\left(b^{n(n-1)},a^n,\left(n^s abck\right)^0\right)}-E'_{\left(b^n,a^{n(n-1)},\left(n^s abck\right)^0\right)}=\sum_{i=0}^{n-2}\sum_{l=0}^{n-i}\sum_{n-3\geq p+i\geq 2,p=0}^{l} C_n^i C_{n-i}^l C_l^p (-1)^{n-i}2^p b^{n(n-i-l)}a^{n(l-p)}\left(n^s abck\right)^{p+i}$$

$$+(2n-2)\left(n^s abck\right)^n-n\left(a^n+b^n\right)^{n-1}\left(n^s abck\right)+n\left(a^{n(n-1)}+b^{n(n-1)}\right)\left(n^s abck\right)-\left(C_n^1 a^{n(n-1)}b^n+C_n^1 b^{n(n-1)}a^n\right).$$

Với $E'_{\left(\left(b^n\right)^{n-i-l},\left(a^n\right)^{l-p},\left(n^s abck\right)^{p+i}\right)}=\sum_{i=0}^{n-2}\sum_{l=0}^{n-i}\sum_{p=0}^{l} C_n^i C_{n-i}^l C_l^p (-1)^{n-i}2^p b^{n(n-i-l)}a^{n(l-p)}\left(n^s abck\right)^{p+i}$. Từ đó suy ra $-\left(C_n^1 a^{n(n-1)}b^n+C_n^1 b^{n(n-1)}a^n\right)+n\left(a^{n(n-1)}+b^{n(n-1)}\right)\left(n^s abck\right)=S\vdots c^2$, suy ra $\left[2n\left(n^s abck\right)(n-3)a^{n(n-2)}b^n\right]\vdots c^2$ suy ra k = 0 hoặc $2(n-3)\vdots c$ (nếu k $\neq$ 0).

Đến đây ta tóm tắt những điều đã chứng minh ở **2.1.2** bởi định lý sau:

Định lý 2:

Cho n là số nguyên tố lớn hơn 3.

Giả sử x = u, y = v, z = t là một nghiệm nguyên khác không của PT: $x^n + y^n = z^n$, với (u, v) = (u, t) = = (v, t) = 1 và t chia hết cho n.

Khi đó tồn tại số nguyên s với s ≥ 2 và tồn tại bốn số nguyên khác không a, b, c, k đều không chia hết cho n, sao cho (a,b) = (a,c) = (a,k) = (b,c) = (b,k) = (c,k) = 1, đồng thời a | 2(n – 3), b | 2(n – 3), c | 2(n – 3), $v = a^n + n^s abck$, $u = b^n + n^s abck$, $t = n^{ns-1}c^n - n^s abck$ và $u + v - t = n^s abck$.

Xét hai trường hợp.

2.1.2.1. ***Khi k ≠ 0***

Theo chứng minh trên, với k ≠ 0, ta có a | 2(n – 3), b | 2(n – 3), mà (a,b) =1 nên ab | 2(n – 3), suy ra $2(n-3) = r|ab|, r \in \mathbb{N}^* \Rightarrow |ab| \le 2(n-3)$.

Vì $t \vdots n$ nên $(u+v) \vdots n$, mà u + v = a + b + n(ak$_1$ + bk$_2$), từ đó $(a+b) \vdots n$, suy ra $a+b = nm$, $m \in \mathbb{Z}^*$.

Với $a, b \in \mathbb{Z}^*$, ta có $2n-5 \ge |ab|+1 \ge |a|+|b| \ge |a+b| = |m|n \Rightarrow |m| \in \{0;1\}$.

Ta có $a+b = nm = \dfrac{2(n-3)m}{2} + 3m = \dfrac{r|ab|m}{2} + 3m \Rightarrow 2(a+b) = r|ab|m + 6m$ (13)

1) Với m = 0

Ta có: $a+b = 0 \Rightarrow a^n + b^n = 0 \Rightarrow n^{ns-1}c^n = u+v = 2n^s abck \Rightarrow n^{ns-1-s}c^{n-1} = 2abk \Rightarrow ab \vdots n$, vô lý.

2) Với $m = 1$

Ta có a + b = n (14) suy ra $2n = 2(a+b) = r|ab| + 6 = r(|ab|+1) + 6 - r \ge r(|a|+|b|) + 6 - r \ge r(|a+b|) + 6 - r \ge r(a+b) + 6 - r = nr + 6 - r$

$\Rightarrow 2n \ge nr + 6 - r \Rightarrow (n-1)(2-r) \ge 4 \Rightarrow r = 1 \Rightarrow 2(a+b) = |ab| + 6$ (15), suy ra ab là số chẵn, suy ra $|ab| \ge 2$.

Từ (14) suy ra a + b là số lẻ, vì vậy không mất tính tổng quát ta giả sử *a chẵn* và *b lẻ*

a) Nếu ab ≥ 2

Ta có: $(15) \Rightarrow a = 2 + \dfrac{2}{2-b} \Rightarrow \begin{cases} a = 4 \\ b = 1 \end{cases}$ (vì $ab \ge 2$; $a, b \in \mathbb{Z}^*$ và $a \vdots 2$) $\Rightarrow n = 5$ (do (14)).

Vì (a,b) = (a,c) = (b,c) = 1 và $2(n-3) = 4 \vdots c$ nên $c = \pm 1$.

i) Với c = 1

Ta có $5^{5s-1} = 1^5 + 4^5 + 8.5^s k \Rightarrow 5^{5s-2} = 205 + 8.5^{s-1}k$ (16).

. Khi s = 2

Từ (16) suy ra: $5^7 = 41 + 8k \Rightarrow 19521 = 2k \Rightarrow 19521 \vdots 2$, vô lý.

. Khi s ≥ 3

Từ (16) suy ra $5^{5s-3} = 41 + 8.5^{s-2}k \Rightarrow 41 \vdots 5$, vô lý.

ii) Với c = –1

Ta có $-5^{5s-1} = 1^5 + 4^5 - 8.5^s k \Rightarrow -5^{5s-2} = 205 - 8.5^{s-1}k$ (17).

. Khi s = 2

Từ (17) suy ra: $-5^7 = 41 - 8k \Rightarrow 39083 = 4k \Rightarrow 39083 \vdots 4$, vô lý.

. Khi s ≥ 3

Từ (17) suy ra $-5^{5s-3} = 41 - 8.5^{s-2}k \Rightarrow 41 \vdots 5$, vô lý.

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

b) Nếu $ab \le -2$

Ta có: $(15) \Rightarrow a = -2 + \dfrac{10}{2+b} \Rightarrow \begin{cases} b = -1 \\ a = 8 \end{cases} (vì\ ab \le -2;\ a,b \in \mathbb{Z}^*\ và\ a \vdots 2) \Rightarrow n = 7\ (do\ (14))$.

Vì (c,a) = (c,b) = (b,a) =1 và $2(n-3) = 8 \vdots c$ nên $c = \pm 1$.

i) Với c = 1

Ta có $7^{7s-1} = (-1)^7 + 8^7 - 16.7^s k \Rightarrow 7^{7s} + 7 = 7.8^7 - 16.7^{s+1}k \Rightarrow 7^s + 7 \equiv 0 \pmod{16} \Rightarrow (7^s + 7) \vdots 16$ (18).

+ Khi s chẵn

Vì $7^s + 7 = 7(7^{s-1} + 1) = 8\sum_{i=0}^{s-2}(-1)^i 7^{s-1-i}$, nên $(7^s + 7) \not\vdots 16$, trái với (18).

+ Khi s lẻ

Vì $7^s + 7 = (7^s + 1) + 6 = 8\sum_{i=0}^{s-1}(-1)^i 7^{s-1-i} + 6 = 2\left[4\sum_{i=0}^{s-1}(-1)^i 7^{s-1-i} + 3\right]$ nên $(7^s + 7) \not\vdots 16$, trái với (18).

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

ii) Với c = –1

Ta có $-7^{7s-1} = -1 + 8^7 + 16.7^s k$ (19)

+ Khi s = 2

Từ (19) ta có $-7^{13} = -1 + 8^7 + 16.7^2 k \Rightarrow (1 - 7^{13}) = 8^7 + 16.7^2 k \Rightarrow 2\left(-3\sum_{i=0}^{12} 7^{12-i}\right) = 8^7 + 16.7^2 k$

$\Rightarrow 2\left(-3\sum_{i=0}^{12} 7^{12-i}\right) \vdots 16$, vô lý.

+ Khi s ≥ 3

Từ (19) suy ra $-7^{7s-3} = 42799 + 16.7^{s-2}k \Rightarrow 42799 \vdots 7^{s-2} \Rightarrow 42799 \vdots 7$, vô lý.

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

3) Với m = –1

Ta có $(-a) + (-b) = n$, cho nên, nếu xem –a như a và –b như b thì ta cũng tìm được a, b, c và n. Lập luận tương tự như trường hợp m = 1, ta suy ra PT(1) vô nghiệm trong khác không trường hợp này.

2.1.2.2. *Khi k = 0*

Ta có $t = u + v \Rightarrow n^s c.c' = n^{ns-1}c^n \Rightarrow c' = n^{ns-1-s}c^{n-1} \Rightarrow c' \vdots n$, vô lý (vì $c' \not\vdots n$).

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

2.2. Khi n = 3

Nhà toán học Leonhard Euler (1707 – 1783) đã chứng minh PT(1) vô nghiệm nguyên khác không trong trường hợp này.

2.3. Khi n = 4

Nhà toán học Pierre de Fermat (1601–1665) đã chứng minh PT(1) vô nghiệm nguyên khác không trong trường hợp này.

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

Từ kết quả chứng minh ở **2.1**, **2.2**, **2.3**, áp dụng **bổ đề 2** ta 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, 30/04/2013
Tác giả
Tôn Thất Hiệp