Chuyên đề 2:
Vận dụng phương pháp LTE
vào giải các bài toán số học

Phạm Quang Toàn [1]

Bổ đề về số mũ đúng (Lifting The Exponent Lemma) là một bổ đề rất hữu dụng trong việc giải các bài toán số học và rất được biết đến trong lịch sử Olympiad. Thực chất là nó được mở rộng ra từ bổ đề Hensel. Ta thường viết tắt tên của bổ đề là **LTE**, tên Tiếng Việt thì có thể gọi là *bổ đề về số mũ đúng*. Bài viết này xin được giới thiệu với bạn đọc về bổ đề và những ứng dụng đặc sắc của nó vào các bài toán lý thuyết số.

Bài viết chủ yếu dựa vào tài liệu của thành viên Amir Hossein bên trang mathlinks.ro (về mặt lý thuyết thì mình giữ nguyên bản bài viết của Amir Hossein sang bài viết này) và có kèm theo một số ví dụ được lấy từ các kì thi Olympic toán trên thế giới.

Một số khái niệm

Ở đây, thay vì kí hiệu $a \vdots b$ nghĩa là a chia hết cho b, ta sẽ kí hiệu $b|a$. Và $a \not\vdots b$ sẽ được thay bằng $b \nmid a$.

Định nghĩa 1. Cho p là số nguyên tố, a là số nguyên và α là số tự nhiên. Ta có p^α là lũy thừa đúng (exact power) của a và α là số mũ đúng (exact exponent) của p trong khai triển của α nếu $p^\alpha | a$ và $p^{\alpha+1} \nmid a$. Khi đó ta viết $p^\alpha \parallel a$ hay $v_p(a) = \alpha$.

Ví dụ. Ta có $v_5(5400) = 3$ hay $5^3 \parallel 5400$ vì $5400 = 5^3 \cdot 3^2 \cdot 2^2$.

Sau đây là một số tính chất. Chứng minh tính chất này không khó, xin dành cho bạn đọc.

Tính chất 1. Cho a, b, c là các số nguyên. Ta có

1. $v_p(ab) = v_p(a) + v_p(b)$
2. $v_p(a^n) = n \cdot v_p(a)$
3. $\min\{v_p(a), v_p(b)\} \leqslant v_p(a+b)$
   Dấu đẳng thức xảy ra khi $v_p(a) \neq v_p(b)$.
4. $v_p\left(\gcd(|a|, |b|, |c|)\right) = \min\{v_p(a), v_p(b), v_p(c)\}$
5. $v_p\left(\operatorname{lcm}(|a|, |b|, |c|)\right) = \max\{v_p(a), v_p(b), v_p(c)\}$

Chú ý. $v_p(0) = \infty$ với mọi số nguyên tố p.

[1]Lớp 9C THCS Đặng Thai Mai, Tp Vinh

Hai bổ đề

Đầu tiên, xin giới thiệu với bạn đọc hai bổ đề. Và hai bổ đề này sẽ giúp ta tìm cách chứng minh được các định lí khác của LTE.

Bổ đề 1. Cho x, y là hai số nguyên và cho n là số nguyên dương. Cho số nguyên tố p bất kì sao cho $p|x-y$ và $p \nmid x, p \nmid y$. Ta có

$$v_p(x^n - y^n) = v_p(x-y).$$

Chứng minh. Ta có $p|x-y$ nên

$$x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1} \equiv nx^{n-1} \not\equiv 0 \pmod{p}$$

Mà $x^n - y^n = (x-y)\left(x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1}\right)$ nên ta suy ra điều phải chứng minh. ❐

Bổ đề 2. Cho x, y là hai số nguyên và n là số nguyên dương lẻ. Cho số nguyên tố p bất kì thỏa mãn $p|x+y$ và $p \nmid x, p \nmid y$. Khi đó

$$v_p(x^n + y^n) = x_p(x+y).$$

Chứng minh. Áp dụng bổ đề 1 ta có $v_p(x^n - (-y)^n) = v_p(x-(-y))$ nên $v_p(x^n+y^n) = v_p(x+y)$. (vì n lẻ). Bổ đề được chứng minh. ❐

Lifting The Exponent Lemma (LTE)

Định lý 1. Cho x và y là các số nguyên (không nhất thiết phải nguyên dương), n là một số nguyên dương và p là một số nguyên tố lẻ thỏa mãn $p|x-y$ và $p \nmid x, p \nmid y$. Ta có

$$v_p\left(a^n - b^n\right) = v_p(a-b) + v_p(n)$$

Chứng minh. Ta sẽ đi chứng minh quy nạp theo $v_p(n)$. Trước hết, ta sẽ đi chứng minh khẳng định sau:

$$v_p(x^p - y^p) = v_p(x-y) + 1$$

Để chứng minh điều đó thì ta cần chỉ ra rằng

$$p|x^{p-1} + x^{p-2}y + \cdots + xy^{p-2} + y^{p-1} \tag{1}$$

và

$$p^2 \nmid x^{p-1} + x^{p-2}y + \cdots + xy^{p-2} + y^{p-1} \tag{2}$$

Với **(1)**, nhờ áp dụng $x \equiv y \pmod{p}$ ta suy ra

$$x^{p-1} + \cdots + y^{p-1} \equiv px^{p-1} \equiv 0 \pmod{p}$$

Với **(2)**, ta đặt $y = x + kp$ với $k \in \mathbb{N}^*$. Khi đó với $1 \leqslant i \leqslant p-1$ $(i \in \mathbb{N})$ thì

$$\begin{aligned} y^i x^{p-1-i} &\equiv (x+kp)^i x^{p-1-i} \\ &\equiv x^{p-1-i}\left(x^i + i(kp)x^{i-1} + \frac{i(i-1)}{2}(kp)^2 x^{i-2} + \cdots\right) \\ &\equiv x^{p-1-i}\left(x^i + i(kp)x^{i-1}\right) \\ &\equiv x^{p-1} + ikpx^{p-2} \pmod{p^2}. \end{aligned}$$

Do đó,

$$\begin{aligned} x^{p-1} + x^{p-2}y + \cdots + y^{p-1} &\equiv x^{p-1} + (x^{p-1} + kpx^{p-2}) + (x^{p-1} + 2kpx^{p-2}) + \cdots + (x^{p-1} + (p-1)kpx^{p-2}) \\ &\equiv px^{p-1} + \frac{p-1}{2} \cdot kp^2 x^{p-2} \\ &\equiv px^{p-1} \not\equiv 0 \pmod{p^2} \end{aligned}$$

Như vậy $v_p(x^p - y^p) = v_P(x-y) + 1$.
Quay lại bài toán, đặt $n = p^k \cdot h$ với $b, k \in \mathbb{N},\ b \geqslant 1$ $\gcd(b,p) = 1$. Khi đó thì

$$\begin{aligned} v_p(a^n - b^n) &= v_p((a^{p^k})^h - (b^{p^k})^h) \\ &= v_p\left(a^{p^k} - b^{p^k}\right) = v_p((a^{p^{k-1}})^p - (b^{p^{k-1}})^p) \\ &= v_p(a^{p^{k-1}} - b^{p^{k-1}}) + 1 = v_p((a^{p^{k-2}})^p - (b^{p^{k-2}})^p)) \\ &\ \ \vdots \\ &= v_p(x-y) + k = v_p(x-y) + v_p(n) \end{aligned}$$

Định lý được chứng minh. ❐

Định lý 2. Cho hai số nguyên x, y, n là số nguyên dương lẻ, và p là ước nguyên tố lẻ sao cho $p|x+y$ và $p \nmid x, p \nmid y$. Khi đó

$$v_p(x^n + y^n) = v_p(x+y) + v_p(n).$$

Chứng minh. Áp dụng định lý 1 ta có

$$v_p(x^n - (-y)^n) = v_p(x - (-y)) + v_p(n)$$

hay

$$v_p(x^n + y^n) = v_p(x+y) + v_p(n)$$

❐

Định lý 3. *(cho trường hợp $p = 2$)* Cho x, y là hai số nguyên lẻ thỏa mãn $4|x-y$. Khi đó

$$v_2(x^n - y^n) = v_2(x-y) + v_2(n).$$

Chứng minh. Theo bổ đề 1 thì nếu p nguyên tố, $\gcd(p,n) = 1, p|x-y$ và $p \nmid x, p \nmid y$ thì

$$v_p(x^n - y^n) = v_p(x-y)$$

Do đó ta chỉ cần xét tới trường hợp n là lũy thừa của 2, tức cần chứng minh

$$v_2(x^{2^n} - y^{2^n}) = v_2(x - y) + n$$

Thật vậy, ta có

$$x^{2^n} - y^{2^n} = (x^{2^{n-1}} + y^{2^{n-1}})(x^{2^{n-2}} + y^{2^{n-2}}) \cdots (x^2 + y^2)(x + y)(x - y)$$

Vì $x \equiv y \equiv \pm 1 \pmod 4$ nên $x^{2^k} \equiv y^{2^k} \equiv 1 \pmod 4$. Do đó

$$v_2(x^{2^{n-1}} + y^{2^{n-1}}) = v_2(x^{2^{n-2}} + y^{2^{n-2}}) = \cdots = v_2(x + y) = 1$$

Như vậy $v_2(x^{2^n} + y^{2^n}) = n + v_p(x - y)$, ta có điều phải chứng minh. ❒

Định lý 4. *(cho trường hợp $p = 2$)* Cho hai số nguyên lẻ x, y, n là số nguyên dương chẵn và $2|x - y$. Khi đó

$$v_2(x^n - y^n) = v_2(x - y) + v_2(x + y) + v_2(n) - 1.$$

Chứng minh. Ta có $4|x^2 - y^2$ nên đặt $n = 2^k \cdot h$ với $k, h \in \mathbb{N}^*$, $\gcd(h, 2) = 1$. Khi đó ta có

$$\begin{aligned} v_2(x^n - y^n) &= v_2(x^{h \cdot 2^k} - y^{h \cdot 2^k}) \\ &= v_2((x^2)^{2^{k-1}} - (y^2)^{2^{k-1}}) \\ &\vdots \\ &= v_2(x^2 - y^2) + k - 1 \\ &= v_2(x - y) + v_2(x + y) + v_2(n) - 1 \end{aligned}$$

❒

Ta có hệ quả sau:

Hệ quả. Cho a, n là hai số nguyên dương:

i) p là hai số nguyên tố lẻ sao cho $v_p(a - 1) = \alpha \in \mathbb{N}^*$, khi đó với mọi số tự nhiên β ta có $v_(a^n - 1) = \alpha + \beta \Leftrightarrow v_p(n) = \beta$.

ii) n chẵn sao cho $v_2(a^2 - 1) = \alpha \in \mathbb{N}^*$, khi đó với mọi số nguyên dương β thì $v_2(a^n - 1) = \alpha + \beta \Leftrightarrow v_2(n) = \beta + 1$.

Chú ý.

a) Nếu trong các bài toán đòi hỏi vận dụng phương pháp LTE, ta nên để ý tới các điều kiện đặt ra của n, x, y, lựa chọn định lý phù hợp đưa vào lời giải bài toán.

b) Nếu dữ liệu bài toán cho $a|b$ với $a, b \in \mathbb{N}$ thì với mọi p là ước nguyên tố của b, ta luôn có $v_p(b) \geqslant v_p(a)$. Ngược lại, nếu $v_p(b) \geqslant v_p(a)$ thì $a|b$. Như vậy

$$a|b \Leftrightarrow v_p(b) \geqslant v_p(a)$$

Đây là một tính chất rất thường được dùng trong các bài toán sử dụng phương pháp LTE.

Một số ví dụ

Sau đây mình xin đưa ra một số ví dụ về các ứng dụng của phương pháp này.
Ví dụ . Tìm số nguyên dương n nhỏ nhất thỏa mãn $2^{2013}|1999^n - 1$.
Lời giải. Áp dụng **Định lý 4** ta có

$$v_2(1999^n - 1) = v_2(n) + v_2(2000) + v_2(1998) = v_2(n) + 5$$

Để thỏa mãn $2^{2013}|1999^n - 1$ thì $v_2(n) + 5 \geqslant 2013$ hay $v_2(n) \geqslant 2008$.
Vậy số nguyên dương n nhỏ nhất thỏa mãn đề ra là 2^{2008}.
Ví dụ . *(IMO Shortlist 1991)* Tìm số nguyên dương k lớn nhất thỏa mãn 1991^k là ước của

$$1990^{1991^{1992}} + 1992^{1991^{1990}}.$$

Lời giải. Đặt $a = 1991$ thì a là số nguyên tố lẻ. Do đó theo **Định lý 2** thì

$$\begin{aligned} v_a\left((a-1)^{a^{a+1}} + (a+1)^{a^{a-1}}\right) &= v_a\left((a-1)^{a^2})^{a^{a-1}} + (a+1)^{a^{a-1}}\right) \\ &= v_a\left((a-1)^{a^2} + a + 1\right) + v_a(a^{a-1}) \\ &= a - 1 + v_a\left((a-1)^{a^2} + a + 1\right) \end{aligned}$$

Cũng theo Định lý 2 thì $v_a\left((a-1)^{a^2} + 1\right) = v_a(a) + v_a(a^2) = 3$ nên $v_a\left((a-1)^{a^2} + a + 1\right) = 1$.
Vậy, $v_a\left((a-1)^{a^{a+1}} + (a+1)^{a^{a-1}}\right) = a$. Ta thu được $\max k = a = \boxed{1991}$.
Ví dụ 1. *(Italy TST 2003)* Tìm bộ số nguyên nguyên (a, b, p) sao cho a, b là số nguyên dương, p là số nguyên tố thỏa mãn $2^a + p^b = 19^a$.
Lời giải. Vì a nguyên dương nên $17|19^a - 2^a$. Vậy $p = 17$. Áp dụng **Định lý 1** ta có

$$\begin{aligned} &v_{17}(19^a - 2^a) = v_{17}(17) + v_{17}(a) \\ &\Leftrightarrow b = 1 + v_{17}(a) \leqslant 1 + a \end{aligned}$$

1. Nếu $b < 1 + a$ hay $1 \leqslant b \leqslant a$. Dễ dàng chứng minh quy nạp rằng $19^a - 2^a \geqslant 17^a$ với $a \geqslant 1$. Mà $17^a \geqslant 17^b$. Vậy $a = b = 1$ ở trường hợp này.

2. Nếu $b = 1 + a$ thì dễ dàng chứng minh quy nạp $19^a - 2^a < 17^{a+1} = 17^b$, mâu thuẫn.

Vậy $(a, b, p) = (1, 1, 17)$ là đáp án duy nhất bài toán.
Ví dụ . *(IMO 1990)* Tìm số nguyên dương n sao cho $n^2|2^n + 1$.
Lời giải. Với $n = 1$ thỏa mãn. Với $n \geqslant 2$, nhận thấy n lẻ.
Gọi p là ước nguyên tố lẻ nhỏ nhất của n. Khi đó ta suy ra $2^{2n} \equiv 1 \pmod{p}$. Gọi k là số nguyên dương nhỏ nhất thỏa mãn $2^k \equiv 1 \pmod{p}$. Khi đó $k|2n$. Theo định lý Fermat nhỏ thì $2^{p-1} \equiv 1 \pmod{p}$ nên $k|p - 1$. Như vậy ta suy ra $\gcd(n, k) = 1$ nên $k|2$. Với $k = 1$ thì $p|1$, mâu thuẫn. Vậy $k = 2$. Do đó $p = 3$ hay $3|n$.
Đặt $v_3(n) = k$ ($k \in \mathbb{N}^*$). Áp dụng **Định lý 2** thì ta có

$$v_3(2^n + 1) = v_3(3) + v_3(n) = 1 + k$$

Lại có vì $n^2|2^n+1$ nên $v_3(2^n+1) \geqslant v_3(n^2) \Leftrightarrow k+1 \geqslant 2k$. Vậy $k=1$. Đặt $n=3m$ với $m \in \mathbb{N}^*$ và $\gcd(m,3)=1$.

Gọi p_1 là ước nguyên tố nhỏ nhất của m. Khi đó ta có $2^{6m} \equiv 1 \pmod{p_1}$. Gọi k_1 là số nguyên dương nhỏ nhất thỏa mãn $2^k \equiv 1 \pmod{p_1}$. Tương tự thì ta dễ dàng suy ra $k|6$. Vì $p_1 \geqslant 5$ nên $k=3$ hoặc $k=6$.

Với $k=3$ thì $p_1|7$ nên $p_1=7$. Với $k=6$ thì $p_1|63$ mà $p_1 \geqslant 5$ nên $p_1=7$. Tuy nhiên $2^n+1=2^{3m}+1=8^m+1 \equiv 2 \pmod 7$ mà $7|n^2$, mâu thuẫn.

Vậy ước nguyên tố duy nhất của n là 3 mà $3 \parallel n$ nên $n=3$.

Số nguyên dương n thỏa mãn đề bài là $n \in \{1;3\}$.

Ví dụ 2. *(European Mathematical Cup 2012, Senior Division)* Tìm số nguyên dương a,b,n và số nguyên tố p thỏa mãn

$$a^{2013}+b^{2013}=p^n$$

Lời giải. Đặt $a=p^x \cdot y, b=p^z \cdot t$ với $x,y,z,t \in \mathbb{N};\ t,y \geqslant 1$ và $\gcd(y,p)=1, \gcd(t,p)=1$.

Không làm mất tính tổng quát, giả sử rằng $x \geqslant z$. Dễ nhận thấy rằng $n \geqslant 2013x \geqslant 2013z$. Khi đó phương trình ban đầu tương đương với

$$t^{2013}+p^{2013(x-z)} \cdot y^{2013}=p^{n-2013z}$$

Nếu $x>z$ thì $p \nmid VT$. Do đó $p \nmid p^{n-2013z}$ suy ra $n=2013z$. Vậy ta được phương trình

$$t^{2013}+p^{2013(x-z)} \cdot y^{2013}=1,$$

mâu thuẫn vì $VT \geqslant 2$ (do $,ty \geqslant 1$). Vậy $x=z$. Phương trình trở thành

$$t^{2013}+y^{2013}=p^{n-2013z}=p^k\ (k=n-2013z \in \mathbb{N}^*) \tag{3}$$

Nếu $p|2013$ thì theo định lý Fermat nhỏ ta suy ra $t^{2013}+y^{2013} \equiv 2 \pmod p$, mâu thuẫn vì $p|p^k$. Vậy $\gcd(p,2013)=1$.

Dễ thấy theo (3) thì $p|t+y$. Do đó bằng việc áp dụng **Định lý 2** ta có

$$v_p\left(t^{2013}+y^{2013}\right)=v_p(t+y)$$

Ta lại có $t+y|t^{2013}+y^{2013}$ và (3) nên ta suy ra

$$\begin{aligned} p^k=t+y&=t^{2013}+y^{2013}\\ t^{2012}(t-1)+y^{2012}(y-1)&=0 \end{aligned}$$

Vì $t,y \geqslant 1$ nên từ phương trình ta suy ra $t=y=1$. Do đó $p=2$, từ đó suy ra $a=b=2^h, n=2013h+1$ với $h \in \mathbb{N}$.

Nhận xét. Ta có thể tổng quát bài toán lên thành: Giải phương trình nghiệm nguyên dương

$$a^n+b^n=p^k$$

với p nguyên tố.

Ví dụ 3. *(Romanian IMO TST 2005)* Giải phương trình nghiệm nguyên dương

$$3^x=2^x \cdot y+1$$

Lời giải. Ta xét hai trường hợp:

1. Nếu x lẻ thì áp dụng **Định lý 1** ta có $v_2(3^x-1)=v_2(3-1)=1$ hay $v_2(2^x\cdot y)=1$. Do đó $x=1$. Từ phương trình ta suy ra $y=1$.

2. Nếu x chẵn thì áp dụng **Định lý 1** ta có

$$\begin{aligned} &v_2(3^x-1)=v_2(3-1)+v_2(3+1)+v_2(x)-1=2+v_2(x)\\ \Leftrightarrow &v_2(2^x\cdot y)=2+v_2(x)\Leftrightarrow x+v_2(y)=v_2(x)+2 \qquad (1)\end{aligned}$$

   Đặt $x=2^m\cdot k$ với $m,n\in\mathbb{N}^*$. Ta dễ dàng chứng minh bằng quy nạp rằng $2^m\cdot k>m+2$ với $m\in\mathbb{N},\ m\geqslant 3$. Do đó $x>v_2(x)+2$ với $v_2(x)\geqslant 3$ hay với $x\geqslant 2^{v_2(x)}=8$. Như vậy $x\geqslant 8$ thì (1) không xảy ra. Vậy $x\leqslant 8$, x chẵn nên $x\in\{2;4;6\}$. Từ đây ta tìm được $(x,y)=(2;2),(4;5)$.

Vậy phương trình có nghiệm nguyên dương $(x,y)=(1;1),(2;2),(4;5)$.
Nhận xét. Qua bài toán trên, ta lưu ý một số ý tưởng được dùng trong phương pháp này: Với p là một ước nguyên tố của $a=p^m\cdot k$ với $m,k\in\mathbb{N}^*$ thì:

i) $a\geqslant p^{v_p(a)}$.

ii) $p^m\cdot k\geqslant m+\alpha$ với $m\geqslant\beta$. Từ đây suy ra $a\geqslant v_p(a)+\alpha$ với $v_p(a)\geqslant\beta$ hay $a\geqslant p^\beta$.

Các bài trên chủ yếu là các bài không khó để vận dụng bổ đề LTE vì ta đã xác định được các yếu tố p,a,b một cách dễ dàng. Tuy nhiên, vẫn có một số bài toán đòi hỏi ta phải đi tìm ra các yếu tố p,a,b ...
Ví dụ 4. *(IMO 1999)* Tìm tất cả các cặp (n,p) nguyên dương sao cho p là số nguyên tố và $(p-1)^n+1$ chia hết cho n^{p-1}.
Lời giải. Dễ thấy với $n=1$ thì p là số nguyên tố bất kì đều thỏa mãn đề ra. Với $n\geqslant 2$, ta có các trường hợp:
Trường hợp 1. Nếu $p=2$ thì $n|2$. Do đó $n=2$.
Trường hợp 2. Nếu p lẻ. Lấy q là ước nguyên tố nhỏ nhất của n, khi đó $(p-1)^n\equiv -1 \pmod q$ hay $(p-1)^{2n}\equiv 1 \pmod q$ và $\gcd(p-1,q)=1$. Ta lấy o là số nguyên dương nhỏ nhất thỏa mãn $(p-1)^o\equiv 1 \pmod q$. Khi đó thì ta suy ra $o|2n$. Áp dụng định lý Fermat nhỏ ta có $(p-1)^{q-1}\equiv 1 \pmod q$. Do đó $o|q-1$.
Như vậy, $o|2n$ và $o|q-1$. Nếu $\gcd(o,n)>1$ hay o,n chia hết cho số nguyên tố r, khi đó ta suy ra $r|n$ và $r\leqslant o$. Mà $o|q-1$ nên $o<q$, do đó $r<q$. Mà r và q đều là ước nguyên tố của n, mâu thuẫn với điều kiện nhỏ nhất của q. Vậy $\gcd(n,o)=1$. Do đó $2|o$. Vậy $(p-1)^2\equiv 1 \pmod q$ hay $q|p(p-2)$.

1. Nếu $q|p-2$ thì ta có $(p-1)^n+1\equiv 1^n+1\equiv 2 \pmod q$. Vậy $q=2$. Ta có $(p-1)^n+1$ chia hết cho 2 nên $p=2$, mâu thuẫn vì p lẻ.

2. Nếu $q|p$. Dễ nhận thấy n phải lẻ (vì nếu n chẵn thì $(p-1)^n+1\equiv 0 \pmod 4$, mâu thuẫn vì p lẻ). Ta áp dụng **Định lý 2** ta có

$$v_q\left((p-1)^n+1\right)=v_q(n)+v_q(p)\geqslant v_q(n)\cdot(p-1) \qquad (4)$$

Đặt $p = q^a \cdot b$ với $a, b \in \mathbb{N}^*$. Dễ dàng chứng minh bằng quy nạp $q^a \cdot b \geqslant a + 2$ (chú ý vì $q|p$ nên $q \geqslant 3$), dấu bằng xảy ra khi $a = b = 1, q = 3$. Do đó $p \geqslant v_q(p) + 2$. Kết hợp với (3) ta suy ra

$$p - 2 \geqslant v_q(p) \geqslant v_q(n)(p-2)$$

Vậy $q = p = 3$ và $v_3(n) = 1$. Đặt $n = 3k$ với $k \in \mathbb{N}^*,\ \gcd(k,3) = 1,\ \gcd(k,2) = 1$. Như vậy từ đề bài ta sẽ có $9k^2 | 8^k + 1$.

Hiển nhiên $9|8^k + 1$. Ta chỉ cần đi tìm k sao cho $k^2|8^k + 1$. Với $k = 1$ thì $n = 3$, thỏa mãn. Với $k \geqslant 2$, hoàn toàn tương tự, lấy r là ước nguyên tố nhỏ nhất của k và s là số nguyên dương nhỏ nhất sao cho $8^s \equiv 1 \pmod r$. Ta suy ra $s|2$ nên $s = 2$. Khi đó $r|8^2 - 1$ hay $r|7$, điều này mâu thuẫn vì $8^k + 1 \equiv 2 \pmod 7$.

Vậy, cặp số (n, p) thỏa mãn đề bài là $(1, p), (2, 2), (3, 3)$.

Ví dụ 5. *(Brazil XII Olympic Revenge 2013)* Tìm các bộ ba số (p, n, k) nguyên dương thỏa mãn p là số nguyên tố Fermat và

$$p^n + n = (n+1)^k \tag{5}$$

Số nguyên tố Fermat là số nguyên tố có dạng $2^{2^x} + 1$ với x tự nhiên.

Lời giải. Đặt $\alpha = 2^x$. Nếu $n = 1$ thì $(5) \Leftrightarrow p = 2^k - 1 = 2^\alpha + 1$. Do đó $k = 2, \alpha = 1$ nên $p = 3$. Nếu $n \geqslant 2$. Ta gọi r là một ước nguyên tố của n. Từ phương trình ta suy ra $p^n \equiv 1 \pmod n$ hay $p^n \equiv 1 \pmod r$. Do đó $\gcd(p, r) = 1$. Đặt k là số nguyên dương nhỏ nhất thỏa mãn $p^k \equiv 1 \pmod r$. Ta cũng có theo định lý Fermat nhỏ thì $p^{r-1} \equiv 1 \pmod r$. Vậy ta suy ra $k|r - 1$ và $k|n$. Vì $\gcd(r - 1, n) = 1$ nên $k = 1$. Ta có $r|p - 1$ hay $r|2^\alpha$. Vậy $r = 2$ hay $2|n$. Ta có

$$(5) \Leftrightarrow p^n - 1 = (n+1)\left[(n+1)^{k-1} - 1\right]$$

Từ phương trình dẫn đến $v_2(p^n - 1) = v_2\left((n+1)^{k-1} - 1\right)$.
Nếu $k - 1$ lẻ thì

$$v_2\left((n+1)^{k-1} - 1\right) = v_2(n) < v_2\left(p^2 - 1\right) + v_2(n) - 1 = v_2(p^n - 1),$$

mâu thuẫn. Vậy $k - 1$ chẵn. Áp dụng **Định lý 4** ta có

$$\begin{aligned} & v_2(p^n - 1) = v_2\left((n+1)^{k-1} - 1\right) \\ \Leftrightarrow & v_2(p^2 - 1) + v_2(n) - 1 = v_2(n) + v_2(n+2) + v_2(k-1) - 1 \\ \Leftrightarrow & v_2(p-1) + v_2(p+1) = v_2(n+2) + v_2(k-1) \end{aligned}$$

Nếu $v_2(k-1) \geqslant v_2(p-1)$ thì $p - 1|k$. Do đó $(n+1)^k \equiv n + 1 \pmod p$ theo định lý Fermat nhỏ. Tuy nhiên theo (5) thì $n \equiv (n+1)^k \pmod p$ nên $n \equiv n + 1 \pmod p$, mâu thuẫn. Vậy $v_2(k-1) < v_2(p-1)$. Khi đó theo phương trình ta có

$$1 \leqslant v_2(p+1) = v_2(2^\alpha + 2) < v_2(n+2)$$

Do đó $v_2(n+2) \geqslant 2$. Ta suy ra $n \equiv 2 \pmod 4$.

1. Nếu $p > 5$ thì $2^{2^x} + 1 > 5$ nên $x \geqslant 2$. Do đó $p \equiv 2 \pmod 5$. Áp dụng $n \equiv 2 \pmod 4$ thì ta suy ra $p^n \equiv 4 \pmod 5$. Do đó $4 + n \equiv (n+1)^k \pmod 5$. Vì $n + 4 \not\equiv n + 1 \pmod 5$ nên $k \not\equiv 1 \pmod 4$. Vì k lẻ nên $k \equiv 3 \pmod 4$. Vậy $4 + n \equiv (n+1)^3 \pmod 5$.

- Nếu $n \equiv 0 \pmod 5$ thì $4 + n - (n+1)^3 \equiv 3 \pmod 5$, mâu thuẫn.
- Nếu $n \equiv 1 \pmod 5$ thì $4 + n - (n+1)^3 \equiv 2 \pmod 5$, mâu thuẫn.
- Nếu $n \equiv 2 \pmod 5$ thì $4 + n - (n+1)^3 \equiv 4 \pmod 5$, mâu thuẫn.
- Nếu $n \equiv 3 \pmod 5$ thì $4 + n - (n+1)^3 \equiv 3 \pmod 5$, mâu thuẫn.
- Nếu $n \equiv 4 \pmod 5$ thì $4 + n - (n+1)^3 \equiv 3 \pmod 5$, mâu thuẫn.

Vậy với mọi $n \in \mathbb{N}^*$ thì $n + 4 \not\equiv (n+1)^3 \pmod 5$. Ta loại trường hợp $p > 5$.

2. Nếu $p = 5$ thì $\alpha = 2$. Khi đó thì $3 = v_2(n+2) + v_2(k-1)$. Vì $v_2(n+2) \geqslant 2$ nên ta suy ra $v_2(n+2) = 2, v_2(k-1) = 1$. Ta cũng có $5^n + n = (n+1)^k$.

   - Với $n = 2$ thì $k = 3$.
   - Với $n \geqslant 3$. Gọi q là ước nguyên tố lẻ của n thì $q | 5^{(n,q-1)} - 1 = 5^2 - 1 = 24$. Vậy $q|3$ nên $q = 3$. Do đó $n \equiv 0 \pmod 6$. Kết hợp với $n \equiv 2 \pmod 4$ ta suy ra $5^n \equiv -1 \pmod{13}$ nên $n - 1 \equiv (n+1)^k \pmod{13}$. Áp dụng **Định lý 1** ta có

   $$v_3(5^n - 1) = v_3\left((n+1)^{k-1} - 1\right) \Leftrightarrow 1 + v_3\left(\frac{n}{2}\right) = v_3(k-1) + v_3(n)$$

   Vậy $3|k-1$. Ta cũng có $k \equiv 3 \pmod 4$ nên $k \equiv 7 \pmod{12}$. Theo định lý Fermat nhỏ ta suy ra $(n+1)^k \equiv (n+1)^7 \equiv \pm(n+1) \pmod{13}$. Như vậy $n - 1 \equiv -n - 1 \pmod{13}$ dẫn đến $n \equiv 0 \pmod{13}$, vô lý. (vì với $13|n$ thì $5^n \equiv 1 \pmod{13}$, mâu thuẫn do $5^n \equiv 5 \pmod{13}$).

Vậy $(p, n, k) = (3, 1, 2), (5, 2, 3)$.

Ví dụ . Tìm bộ ba số nguyên dương (a, b, c) sao cho $a^b + 1 = (a+1)^c$.

Lời giải. Gọi p là một ước nguyên tố lẻ của a. Khi đó thì theo **Định lý 1** ta có

$$\begin{aligned} & v_p((a+1)^c - 1) = v_p(a) + v_p(c) \geqslant v_p(a) \cdot b \\ \Leftrightarrow & v_p(c) \geqslant v_p(a)(b-1) \qquad (6) \end{aligned}$$

1. Nếu c lẻ thì ta có $v_2\left((a+1)^c - 1\right) = v_2(a)$. Do đó $b = 1$. Như vậy thì ta có $a+1 = (a+1)^c$ suy ra $c = 1$.

2. Nếu c chẵn thì $v_2(c) \geqslant 1$ và $b \geqslant 2$. Theo **Định lý 4** thì

   $$v_2((a+1)^c - 1) = v_2(a) + v_2(a+2) + v_2(c) - 1 = v_2(a) \cdot b \qquad (7)$$

   - Nếu $v_2(a) = 1$ thì ta luôn có $v_2(c) \geqslant v_2(a)$. Kết hợp với (6) ta suy ra $c \geqslant a(b-1) > b$, mâu thuẫn vì lúc đó thì $(a+1)^c > a^b + 1$.
   - Nếu $v_2(a) \geqslant 2$ thì $(7) \Leftrightarrow v_2(c) = v_2(a) \cdot (b-1)$. Kết hợp với (6) ta dẫn đến $c \geqslant a(b-1) > b$, mâu thuẫn

Vậy phương trình có nghiệm $(a, b, c) = (k, 1, 1)$ với k là số nguyên dương tùy ý.

Nhận xét. Từ bài toán trên, ta có thêm một số mở rộng sau:

Mở rộng 1. Tìm các số nguyên dương m, l, n, k thỏa mãn $(1 + m^n)^l = 1 + m^k$.

Mở rộng 2. (IMO Shortlist 2000) Tìm bộ ba số nguyên dương (a, m, n) thỏa mãn $a^m+1|(a+1)^n$.

Ngoài việc phương pháp LTE được ứng dụng trực tiếp vào lời giải thì phương pháp này còn được dùng để tìm dạng vô hạn của bài toán chia hết.

Ví dụ 6. Chứng minh tồn tại vô hạn số tự nhiên n thỏa mãn $n|3^n + 1$.

Phân tích và định hướng lời giải. Điều bây giờ ta cần làm và đi tìm một trong các dạng của n thỏa mãn $n|3^n + 1$.

Trước hết, nhận thấy $5|3^2 + 1^2$. Bây giờ ta để ý đến các điều kiện a, b, p trong **Định lý 2**, áp dụng và ta sẽ được $5^{k+1}|3^{2\cdot 5^k} + 1^{2\cdot 5^k}$. Do đó $2 \cdot 5^k|3^{2\cdot 5^k} + 1$. Vậy ta chỉ cần chứng minh $n = 2 \cdot 5^k$ với $k \in \mathbb{N}$ thì $n|3^n + 1$.

Lời giải. Trước hết, ta sẽ đi chứng minh $3^{4\cdot 5^{k-1}} \equiv 1 \pmod{5^k}$. Áp dụng **Định lý 1** ta có

$$v_5\left(3^{4\cdot 5^{k-1}} - 1\right) = v_5(3^4 - 1) + v_5(5^{k-1}) = k$$

Vậy $3^{4\cdot 5^{k-1}} \equiv 1 \pmod{5^k}$ hay $5^k|\left(3^{2\cdot 5^k} - 1\right)\left(3^{2\cdot 5^k} + 1\right)$. Do đó $5^k|3^{2\cdot 5^k} + 1$. Lại có $2|3^{2\cdot 5^k} + 1$ nên $2 \cdot 5^k|3^{2\cdot 5^k} + 1$.

Vì $k \in \mathbb{N}^*$ nên tồn tại vô hạn số tự nhiên $n = 2 \cdot 5^k$ sao cho $n|3^n + 1$.

Ví dụ 7. *(Romanian Master of Mathematics Competition 2012)* Chứng minh tồn tại vô hạn số nguyên dương n thỏa mãn $2^{2^n+1} + 1$ chia hết cho n.

Phân tích và định hướng lời giải. Ta sẽ tìm một số n thỏa mãn điều kiện trên. Dễ thấy $n = 3$ thỏa mãn. Ta mạnh dạn thử với $n = 9, 27 \cdots$ cũng đều thỏa mãn. Từ đây ta dễ dàng tìm được một dạng của nn là $n = 3^k$. Ở đây mình xin giới thiệu hai lời giải:

Lời giải 1. Ta sẽ đi chứng minh số nguyên dương $a_n = 3^n$ thỏa mãn yêu cầu bài toán. Thật vậy, theo **Định lý 2** ta có

$$v_3(2^{a_n} + 1) = v_3(3) + v_3(a_n) = k + 1$$

Và

$$v_3(2^{2^{a_n}+1} + 1) = v_3(3) + v_2(2^{a_n} + 1) = k + 2$$

Vậy $a_n|2^{2^{a_n}+1} + 1$.

Lời giải 2. Ta sẽ đi chứng minh số nguyên dương $a_n = \frac{2^{3^n}+1}{9}$ thỏa mãn yêu cầu đề ra.

Áp dụng **Định lý 2** ta có

$$v_3(a_n) = v_3(3) + v_3(3^n) - 2 = n - 1$$

Đặt $a_n = 3^{n-1}m$ với $m \in \mathbb{N}^*,\ \gcd(3, m) = 1$. Ta có

$$v_3(2^{2^{a_n}+1} + 1) > v_3(2^{a_n} + 1) > v_3(a_n) = n - 1.$$

Vậy $3^{n-1}|2^{2^{a_n}+1} + 1$. Mặt khác, tiếp tục áp dụng **Định lý 2** thì

$$v_3(2^{a_n} + 1) = v_3(3) + v_3(a_n) = n$$

Do đó $3^n|2^{a_n} + 1$. Vậy ta suy ra $2^{3^n} + 1|2^{2^{a_n}+1} + 1$. Mà $m|2^{a_n} + 1$ nên $m|2^{2^{a_n}+1} + 1$.

Vì $\gcd(m, 3) = 1$ nên $a_n|2^{2^{a_n}+1} + 1$.

Bài tập vận dụng

1. Chứng minh phương trình $x^7 + y^7 = 1998^z$ không có nghiệm nguyên dương.

2. Tìm tất cả số nguyên dương n thỏa mãn $7^{2013} | 5^n + 1$.

3. Tìm số nguyên dương n lớn nhất sao cho $2^n | 2011^{2013^{2016}-1} - 1$.

4. Chứng minh tồn tại vô hạn số nguyên dương $n \in \mathbb{N}$ thỏa mãn $n^2 | 2^n + 3^n + 6^n + 1$.

5. *(Japan MO Finals 2012)* Cho p là số nguyên tố. Tìm mọi số nguyên n thỏa mãn với mọi số nguyên x, nếu $p | x^n - 1$ thì $p^2 | x^n - 1$.

6. Cho $a > b > 1$, b là một số lẻ, n là một số nguyên dương. Nếu $b^n | a^n - 1$. Chứng minh $a^b > \frac{3^n}{n}$.

7. Tìm số nguyên dương n thỏa mãn $9^n - 1$ chia hết cho 7^n.

8. *(IMO Shortlist 2007)* Tìm mọi hàm số toàn ánh $f : \mathbb{N} \to \mathbb{N}$ sao cho với mỗi $m, n \in \mathbb{N}$ và với mỗi p nguyên thố, $f(m+n)$ chia hết cho p khi và chỉ khi $f(m) + f(n)$ chia hết cho p.

9. *(IMO 2000)* Tồn tại hay không số nguyên n thỏa mãn n có đúng 2000 ước nguyên tố và $2^n + 1$ chia hết cho n ?

10. Với một số tự nhiên n, cho a là số tự nhiên lớn nhất thỏa mãn $5^n - 3^n$ chia hết cho 2^a. Lấy b là số tự nhiên lớn nhất thỏa mãn $2^b \leqslant n$. Chứng minh rằng $a \leqslant b + 3$.

11. Chứng minh rằng nếu $n \geqslant 2$ sao cho $n | 7^n - 3^n$ thì n chẵn.

12. Tìm số nguyên dương n thỏa mãn

    i) $n | 5^n + 1$.

    ii) $n^2 | 5^n + 1$.

    iii) $n^3 | 5^n + 1$.

13. Tìm mọi số nguyên dương k sao cho k số nguyên tố lẻ đầu tiên $p_1, p_2 \cdots, p_k$ đều tồn tại hai số nguyên dương a, n thỏa mãn

$$p_1 \cdot p_2 \cdots p_k - 1 = a^n$$

14. *(MOSP 2001)* Tìm các số nguyên dương (x, r, p, n) thỏa mãn $x^r - 1 = p^n$.

15. Tìm tất cả các bộ số (m, p, q) với p, q nguyên tố và m nguyên dương sao cho $2^m p^2 + 1 = q^5$.

16. *(Iran TST 2009)* Cho n là một số nguyên dương. Chứng minh rằng

$$3^{\frac{5^{2^n}-1}{2^{n+2}}} \equiv (-5)^{\frac{3^{2^n}-1}{2^{n+2}}} \pmod{2^{n+4}}$$

17. *(IMO Shortlist 2010)* Tìm các cặp số nguyên không âm (m, n) thỏa mãn

$$m^2 + 2 \cdot 3^n = m\left(2^{n+1} - 1\right).$$

18. *(Iran Third Round 2011)* Cho số tự nhiên $k \geqslant 7$. Có bao nhiêu cặp nguyên dương (x, y) thỏa mãn

$$73^{73^x} \equiv 9^{9^y} \pmod{2^k}?$$

19. Giải phương trình nghiệm nguyên dương trong đó p là số nguyên tố:

$$p^a - 1 = 2^n(p - 1)$$

Tài liệu tham khảo

[1] Amir Hossein Parvardi, Lifting The Exponent Lemma: (tài liệu pdf)
[2] Các diễn đàn toán:
diendantoanhoc.net/forum
forum.mathscope.org
mathlinks.ro