6.3.2 Ứng dụng

Trong Lý thuyết số

Ví dụ 6.13. *Chứng minh rằng với mỗi số tự nhiên n, tồn tại n số tự nhiên liên tiếp mà mỗi số trong n số đó đều là hợp số.* △

Lời giải. Ý tưởng: ta sẽ tạo ra một hệ phương trình đồng dư gồm n phương trình đồng dư. Dựa vào định lí thặng dư Trung Hoa, ta kết luận được sự tồn tại nghiệm của hệ đó.
Giả sử $p_1, p_2, ..., p_n$ là n số nguyên tố khác nhau từng đôi một.
Xét hệ phương trình đồng dư $x \equiv -k \pmod{p_k^2} (k = 1, 2, ..., n)$.
Theo định lí thặng dư Trung Hoa, tồn tại $x_0 \in \mathbb{N}^*$ sao cho $x_0 \equiv -k \pmod{p_k^2}, \forall k = 1, 2, ..., n$.
Khi đó các số $x_0 + 1; x_0 + 2, ...; x_0 + n$ đều là hợp số.(đpcm) ■

Ví dụ 6.14. *Chứng minh rằng với mọi số tự nhiên n, tồn tại n số tự nhiên liên tiếp sao cho bất kì số nào trong các số đó cũng đều không phải lũy thừa (với số mũ nguyên dương) của một số nguyên tố.* △

Nhận xét. Bài này cũng gần tương tự với ý tưởng của bài toán ở ví dụ củng cố. Tuy nhiên việc tìm ra hệ phương trình đồng dư khó hơn một chút.

Lời giải. Với mỗi số tự nhiên n, xét n số nguyên tố khác nhau từng đôi một $p_1, p_2, ..., p_n$.
Theo định lí Thặng dư Trung Hoa, tồn tại $a \in \mathbb{N}^*$ sao cho $a \equiv p_k - k \pmod{p_k^2}$ $(k = 1, 2, ..., n)$.
Khi đó dễ thấy rằng các số $a + 1, a + 2, ..., a + n$ đều không phải lũy thừa với số mũ nguyên dương của một số nguyên tố (đpcm). ■

Ví dụ 6.15. *Cho trước các số nguyên dương n, s. Chứng minh rằng tồn tại n số nguyên dương liên tiếp mà mỗi số đều có ước là lũy thừa bậc s của một số nguyên dương lớn hơn 1.* △

Lời giải. Xét dãy $F_n = 2^{2^n} + 1, (n = 0, 1, 2, ...)$. Dễ chứng minh bổ đề sau:

Bổ đề 6.4– *Nếu $n \neq m$ thì* $(F_n, F_m) = 1$. □

Áp dụng định lí Thặng dư Trung Hoa cho n số nguyên tố cùng nhau $F_1^s, F_2^s, ..., F_n^s$ và n số $r_i = -i (i = 1, 2, .., n)$ ta có tồn tại số nguyên c sao cho $c + i \vdots F_i^s$.
Vậy dãy $\{c+i\}_{i=1}^n$ là n số nguyên dương liên tiếp, số hạng thứ i chia hết cho F_i^s. ■

Ví dụ 6.16. *Chứng minh rằng tồn tại một đa thức $P(x) \in \mathbb{Z}[x]$, không có nghiệm nguyên sao cho với mọi số nguyên dương n, tồn tại số nguyên x sao cho $P(x)$ chia hết cho n.* △

Lời giải. Ta có thể xét đa thức $P(x) = (3x+1)(2x+1)$.
Với mỗi số nguyên dương n, ta biểu diễn n dưới dạng $n = 2^k(2m+1)$.
Vì $GCD(2^k, 3) = 1$ nên tồn tại a sao cho $3a \equiv 1 \pmod{2^k}$. Từ đó

$$3x \equiv -1 \pmod{2^k} \Leftrightarrow x \equiv -a \pmod{2^k}$$

Tương tự $GCD\ (2, 2m+1) = 1$ nên tồn tại b sao cho $2b \equiv 1 \pmod{(2m+1)}$. Từ đó

$$2x \equiv -1 \pmod{(2m+1)} \Leftrightarrow x \equiv -b \pmod{(2m+1)}$$

Cuối cùng, do $GCD\ (2^k, 2m+1) = 1$ nên theo định lý Thặng dư Trung Hoa, tồn tại số nguyên x là nghiệm của hệ:

$$\begin{cases} x \equiv -a \pmod{2^k} \\ x \equiv -b \pmod{(2m+1)} \end{cases}$$

Và theo lý luận trên, $P(x) = (3x+1)(2x+1) \vdots n$. ■

Ví dụ 6.17. *Trong lưới điểm nguyên của mặt phẳng tọa độ Oxy, một điểm A với tọa độ $(x_0, y_0) \in \mathbb{Z}^2$ được gọi là nhìn thấy từ O nếu đoạn thẳng OA không chứa điểm nguyên nào khác ngoài A, O. Chứng minh rằng với mọi n nguyên dương lớn tùy ý, tồn tại hình vuông $n \times n$ có các đỉnh nguyên, hơn nữa tất cả các điểm nguyên nằm bên trong và trên biên của hình vuông đều không nhìn thấy được từ O.* △

[13] Nguyễn Trọng Nam, *Lý thuyết đồng dư và ứng dụng trong mã sửa sai*

Lời giải. Dễ thấy điều kiện cần và đủ để điểm $A(x_0, y_0)$ nhìn thấy được từ O là $\gcd(x_0, y_0) = 1$.
Để giải quyết bài toán, ta sẽ xây dựng một hình vuông $n \times n$ với n nguyên dương lớn tùy ý sao cho với mọi điểm nguyên (x, y) nằm trong hoặc trên hình vuông đều không thể nhìn thấy được từ O.
Thật vậy, chọn p_{i_j} là các số nguyên tố đôi một khác nhau với $0 \le i, j \le n$. Xét hai hệ đồng dư sau:

$$\begin{cases} x \equiv 0 \pmod{p_{0_1}p_{0_2}...p_{0_n}} \\ x+1 \equiv 0 \pmod{p_{1_1}p_{1_2}...p_{1_n}} \\ x+2 \equiv 0 \pmod{p_{2_1}p_{2_2}...p_{2_n}} \\ ... \\ x+n \equiv 0 \pmod{p_{n_1}p_{n_2}...p_{n_n}} \end{cases}$$

và

$$\begin{cases} y \equiv 0 \pmod{p_{0_1}p_{0_2}...p_{0_n}} \\ y+1 \equiv 0 \pmod{p_{1_1}p_{1_2}...p_{1_n}} \\ y+2 \equiv 0 \pmod{p_{2_1}p_{2_2}...p_{2_n}} \\ ... \\ y+n \equiv 0 \pmod{p_{n_1}p_{n_2}...p_{n_n}} \end{cases}$$

Theo định lý Thặng dư Trung Hoa thì tồn tại (x_0, y_0) thỏa mãn hai hệ đồng dư trên.
Khi đó, rõ ràng $\gcd(x_0 + i, y_0 + i) > 1, \ \forall i, j = 0, 1, 2, ..., n$.
Điều đó có nghĩa là mọi điểm nằm bên trong hoặc trên biên hình vuông $n \times n$ xác định bởi điểm phía dưới bên trái là (x_0, y_0) đều không thể nhìn thấy được từ O. Bài toán được chứng minh. ■

Trong tìm số lượng nghiệm nguyên của một phương trình nghiệm nguyên

Ví dụ 6.18. *Cho số nguyên dương $n = p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha_k}$, trong đó $p_1, p_2, ..., p_k$ là các số nguyên tố đôi một khác nhau. Tìm số nghiệm của phương trình:*

$$x^2 + x \equiv 0 \pmod{n}$$

Lời giải. Ta có:

$$x^2+x\equiv 0 \pmod n \Leftrightarrow \begin{cases} x(x+1)\equiv 0 \pmod{p_i^{\alpha_i}} \\ i=\overline{1,k} \end{cases}$$
$$\Leftrightarrow \begin{cases} \left[\begin{array}{rcl} x &\equiv& 0 \pmod{p_i^{\alpha^i}} \\ x &\equiv& -1 \pmod{p_i^{\alpha^i}} \end{array}\right. \\ i=\overline{1,k} \end{cases} \quad (6.14)$$

Theo định lí Thặng dư Trung Hoa, mỗi hệ phương trình $x^2+x\equiv 0 \pmod n \Leftrightarrow \begin{cases} x\equiv a_i \pmod{p_i^{\alpha_i}} \\ a_i\in\{-1;0\} \\ i=\overline{1,k} \end{cases}$ có duy nhất một nghiệm và ta có 2^k hệ (bằng số bộ $(a_1,a_2,...,a_k)$, $a_i\in\{-1;0\}$), nghiệm của các hệ khác nhau. Suy ra phương trình đã cho có đúng 2^k nghiệm. ■

Ví dụ 6.19. *Cho $m=2007^{2008}$. Hỏi có tất cả bao nhiêu số tự nhiên $n<m$ sao cho $m|n(2n+1)(5n+2)$.* △

Lời giải. Dễ thấy $GCD\ (m;10)=1$. Do đó:

$$\begin{array}{rcl} n(2n+1)(5n+2) &\equiv& 0 \pmod m \\ \Leftrightarrow 10n(10n+5)(10n+4) &\equiv& 0 \pmod m \end{array} \quad (6.15)$$

Ta có: $m=3^{4016}.223^{2008}$. Để cho thuận tiện, đặt $10n=x$; $3^{4016}=q_1$; $223^{2008}=q_2$.
Khi đó $GCD\ (q_1,q_2)=1$ nên (6.15) tương đương với:

$$x(x+5)(x+4)\equiv 0 \pmod{q_1} \quad (6.16)$$
$$x(x+5)(x+4)\equiv 0 \pmod{q_2} \quad (6.17)$$

Dễ thấy:

- (6.16) xảy ra khi và chỉ khi $x\equiv 0 \pmod{q_1}$ hoặc $x\equiv -5 \pmod{q_1}$ hoặc $x\equiv -4 \pmod{q_1}$.
- (6.17) xảy ra khi và chỉ khi $x\equiv 0 \pmod{q_2}$ hoặc $x\equiv -5 \pmod{q_2}$ hoặc $x\equiv -4 \pmod{q_2}$.

Tài liệu tham khảo

[1] Vũ Hữu Bình,*Phương trình nghiệm nguyên và kinh nghiệm giải*

[2] Phan Huy Khải, *Các chuyên đề bồi dưỡng học sinh giỏi toán trung học. Chuyên đề 5: Phương trình nghiệm nguyên*

[3] Phạm Minh Phương và nhóm tác giả chuyên toán Đại học Sư phạm Hà Nội, *Các chuyên đề Số học bồi dưỡng học sinh giỏi Trung học cơ sở*

[4] Titu Andreescu, Dorin Andrica, *Number Theory: Structures, Examples and Problems*

[5] Tạp chí Toán Tuổi Thơ, Toán học và Tuổi trẻ, Mathematical Reflections, v.v

[6] Các đề thi học sinh giỏi, tuyển sinh vào THPT, TST, IMO,v.v

[7] Tài nguyên Internet, đặc biệt: HTTP://DIENDANTOANHOC.NET/FORUM/, HTTP://WWW.ARTOFPROBLEMSOLVING.COM/, HTTP://BOXMATH.VN

[8] Gv THPT chuyên ĐHKHTN Hà Nội,*Bài giảng Số học*

[9] Đặng Hùng Thắng, *Đồng dư và phương trình đồng dư*

[10] Phan Huy Khải, *Các bài toán cơ bản của Số học*

[11] Hà Huy Khoái, *Chuyên đề bồi dưỡng HSG THPT Số Học*

[12] Kỷ yếu của các hội thảo Toán học, Tạp chí Toán học và Tuổi trẻ, tạp chí Crux,v.v

Do đó từ (6.16) và (6.17), với lưu ý rằng $x \equiv 0 \pmod{10}$, suy ra n là số tự nhiên thỏa mãn các điều kiện đề bài khi và chỉ khi $n = \dfrac{x}{10}$, với x là số nguyên thỏa mãn hệ điều kiện sau:

$$\begin{cases} x \equiv 0 \pmod{10} \\ x \equiv 1 \pmod{q_1} \\ x \equiv r_2 \pmod{q_2} \\ 0 \le x < 10q_1q_2 \\ r_1, r_2 \in \{0; -4; -5\} \end{cases} \tag{6.18}$$

Vì 10; q_1; q_2 đôi một nguyên tố cùng nhau nên theo định lí Thặng dư Trung Hoa, hệ (6.18) có nghiệm duy nhất.
Dễ thấy sẽ có 9 số x là nghiệm của 9 hệ (6.18) tương ứng. Vì mỗi số x cho ta một số n và hai số x cho hai số n khác nhau nên có 9 số n thỏa mãn các điều kiện đề bài. ■

Nhận xét. Ví dụ 6.19 chính là trường hợp đặc biệt của bài toán tổng quát sau:

Ví dụ 6.20. *Cho số nguyên dương n có phân tích tiêu chuẩn $n = p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha_k}$. Xét đa thức $P(x)$ có hệ số nguyên. Nghiệm x_0 của phương trình đồng dư $P(x) \equiv 0 \pmod{n}$ là lớp đồng dư $\overline{x_0} \in \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{n-1}\}$ thỏa mãn $P(x_0) \equiv 0 \pmod{n}$. Khi đó, điều kiện cần và đủ để phương trình $P(x) \equiv 0 \pmod{n}$ có nghiệm là với mỗi $i = 1, 2, ..., s$, phương trình $P(x) \equiv 0 \pmod{p_i^{\alpha_i}}$ có nghiệm. Hơn nữa, nếu với mỗi $i = 1, 2, ..., s$, phương trình $P(x) \equiv 0 \pmod{p_i^{\alpha_i}}$ có r_i nghiệm module $p_i^{\alpha_i}$ thì phương trình có $r = r_1r_2...r_s$ nghiệm module n.* △

6.4 Bài tập đề nghị & gợi ý – đáp số

Bài tập đề nghị

Bài 1. a. Chứng minh rằng: Nếu $(a, m) = 1$ và x chạy qua một hệ thặng dư đầy đủ modulo m thì $ax + b$, với b là một số nguyên tùy ý, cũng chạy qua một hệ thặng dư đầy đủ module m.

b. Chứng minh rằng: Nếu $(a,m)=1$ và x chạy qua một hệ thặng dư thu gọn modulo m thì ax cũng chạy qua một hệ thặng dư thu gọn module m.

Bài 2. Mỗi số nguyên dương T được gọi là số tam giác nếu nó có dạng $T=\dfrac{k(k+1)}{2}$, trong đó k là một số nguyên dương. Chứng minh rằng tồn tại một HĐĐ module n gồm n số tam giác.

Bài 3. a. Cho m_1,m_2 là hai số nguyên dương nguyên tố cùng nhau. Chứng minh rằng:

$$\Phi(m_1m_2)=\Phi(m_1).\Phi(m_2)$$

b. Giả sử số nguyên dương m có phân tích chính tắc thành tích các thừa số nguyên tố $m=p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha_k}$. Chứng minh rằng:

$$\Phi(m)=p_1^{\alpha_1-1}p_2^{\alpha_2-1}...p_k^{\alpha_k-1}(p_1-1)(p_2-2)...(p_k-1)$$

Bài 4. Tính tổng sau:

$$S=\sum_{k=6}^{2012}\left[\frac{17^k}{11}\right]$$

Bài 5. Cho số nguyên dương n và số nguyên tố p lớn hơn $n+1$. Chứng minh rằng đa thức $P(x)=1+\dfrac{x}{n+1}+\dfrac{x^2}{2n+1}+...+\dfrac{x^p}{pn+1}$ không có nghiệm nguyên.

Bài 6. Cho p là số nguyên tố có dạng $3k+2$ (k nguyên dương). Tìm số dư khi chia $S=\sum\limits_{k=1}^{p}(k^2+k+1)$ cho p.

Bài 7. Cho các số nguyên dương a,b thỏa mãn $(a,b)=1$. Chứng minh rằng phương trình $ax+by=1$ có vô số nghiệm nguyên (x,y) và $(x,a)=(y,b)=1$.

$$(5d+2n;2d+n)=(d;2d+n)=(d;n)=1$$
$$\Rightarrow\left\{\begin{array}{l}5d+2n=x^2\\2d+n=y^2\end{array}\right.\left(\begin{array}{l}x;y\in\mathbb{N}^*\\(x;y)=1\end{array}\right)\Rightarrow\left\{\begin{array}{l}d=x^2-2y^2\\n=5y^2-2x^2\end{array}\right.$$

Nếu $x=2z$ với $z\in\mathbb{N}^*\Rightarrow\left\{\begin{array}{l}d=4z^2-2y^2\\n=5y^2-8z^2\end{array}\right.$

$$(7.8)\Leftrightarrow\left(ad^2+1\right)^2=4z^2y^2\Leftrightarrow a\left(4z^2-2y^2\right)^2+1=2zy$$

Phương trình cuối cùng vô nghiệm nguyên do 2 vế khác tính chẵn lẻ.
Suy ra, x lẻ $\Rightarrow d$ lẻ $\Rightarrow c$ lẻ. (ii)
Kết luận: $(i),(ii)\Rightarrow c$ là số chính phương lẻ. ■

Không ngừng tìm kiếm, ta sẽ tìm một lời giải khác súc tích hơn. Nếu ta biết đến công cụ $v_p(n)$ thì sẽ thấy nó sẽ rất hiệu quả cho bài toán này, ta có cách chứng minh thú vị sau.

Chứng minh (Chứng minh 3). Giả sử c chẵn khi đó ta có:

$$v_2(c)=v_2(5c+2b)+v_2(2c+b)$$

Nếu b lẻ thì ta có $v_2(c)=v_2(5c+2b)=v_2(5c)\Rightarrow v_2(5c)<v_2(2b)=1$.
Điều này vô lí!
Do đó c lẻ. Xét $p|c$ là một ước nguyên tố của c.
Ta có $v_p(c)=v_p(5c+2b)+v_p(2c+b)$.
Ta thấy rằng $v_p(c)>v_p(5c+2b),v_p(2c+b)>0$.
Do đó $v_p(5c+2b)=min[v_p(c);v_p(4c+2b)]$
$\Rightarrow v_p(5c+2b)=v_p(4c+2b)=v_p(2c+b)$
$\Rightarrow v_p(c)=2v_p(5c+2b)$: số chẵn nên suy ra c là số chính phương. ■

Và hi vọng còn những lời giải khác hay hơn, sáng tạo hơn từ các bạn. Mong bạn đọc thảo luận thêm và đóng góp ý kiến cho bài toán.

Lời cảm ơn

Rất cảm ơn Karl Heinrich Marx,nguyenta98, Vương Nguyễn Thùy Dương và perfectstrong đã đóng góp ý kiến cho bài viết này.

Khi đó

$$\begin{aligned}
&(7.7)\Leftrightarrow m\left(dam+1\right)^2=d\left(5m+2n\right)\left(2m+n\right)\\
&\left.\begin{array}{l}\Rightarrow d|m\left(dam+1\right)^2\\(d;dam+1)=1\end{array}\right\}\Rightarrow d|m\Rightarrow m=dp\Rightarrow(p;n)=(d;n)=1\\
&(7.7)\Leftrightarrow p\left(d^2ap+1\right)^2=\left(5dp+2n\right)\left(2dp+n\right)\\
&\left.\begin{array}{l}\Rightarrow p|\left(5dp+2n\right)\left(2dp+n\right)\\(p;2dp+n)=1\end{array}\right\}\Rightarrow p|5dp+2n\Rightarrow p|2n\\
&(p;n)=1\Rightarrow p|2\Rightarrow p\in\{1;2\}
\end{aligned}$$

• Trường hợp 1: p=2, khi đó $2\left(2ad^2+1\right)^2=\left(10d+2n\right)\left(4d+n\right)$, suy ra $\left(2ad^2+1\right)^2=\left(5d+n\right)\left(4d+n\right)$. Nhưng vì $(5d+n;4d+n)=(d;4d+n)=(d;n)=1$ Cho nên ta phải có

$$\left\{\begin{array}{l}5d+n=x^2\\4d+n=y^2\end{array}\right.\qquad(x;y\in\mathbb{N}^*,(x;y)=1)$$

Suy ra $d=x^2-y^2$. Mặt khác

$$2ad^2+1=xy\Leftrightarrow a=\frac{xy-1}{2d^2}=\frac{xy-1}{2\left(x^2-y^2\right)^2}$$

Ta chứng minh $2\left(x^2-y^2\right)^2>(x+y)^2>xy-1$
Thật vậy

$$\begin{aligned}
&(x+y)^2\geq 4xy>xy-1\\
&2\left(x^2-y^2\right)^2-(x+y)^2=(x+y)^2\left(2\left(x-y\right)^2-1\right)>0\\
&\Rightarrow 2\left(x^2-y^2\right)^2>xy-1\Rightarrow a<1:\text{ Trái gt}
\end{aligned}$$

Vậy $p=2$ bị loại.
• Trường hợp 2: p=1

$$\begin{aligned}
&\Rightarrow d=m\Rightarrow\left\{\begin{array}{l}c=d^2,(i)\\b=dn\end{array}\right.\\
&(7.7)\Leftrightarrow d^2\left(ad^2+1\right)^2=\left(5d^2+2dn\right)\left(2d^2+dn\right)\\
&\qquad\Leftrightarrow\left(ad^2+1\right)^2=\left(5d+2n\right)\left(2d+n\right)\qquad(7.8)
\end{aligned}$$

Bài 8. Tìm số nguyên dương nhỏ nhất có tính chất: chia 7 dư 5, chia 11 dư 7, chia 13 dư 3.

Bài 9. Chứng minh rằng tồn tại một dãy tăng $\{a_n\}_{n=1}^{\infty}$ các số tự nhiên sao cho với mọi số tự nhiên k, dãy $\{k+a_n\}$ chỉ chứa hữu hạn các số nguyên tố.

Bài 10. Số nguyên dương n được gọi là có tính chất P nếu như với các số nguyên dương a,b mà $a^3b+1\vdots n$ thì $a^3+b\vdots n$. Chứng minh rằng số các số nguyên dương có tính chất P không vượt quá 24.

Bài 11. Tìm tất cả các số tự nhiên n thỏa mãn 2^n-1 chia hết cho 3 và có một số nguyên m mà $\frac{2^n-1}{3}|4m^2+1$.

Bài 12. Chứng minh rằng tồn tại số tự nhiên k sao cho tất cả các số $k.2^n+1$ $(n=1,2,...)$ đều là hợp số.

Gợi ý – đáp số

Bài 1. Chứng minh trực tiếp dựa vào định nghĩa.

Bài 2. Ta chứng minh n phải có dạng $n=2^k$. Phản chứng, giả sử $n=2^k.m$ với m lẻ và $m>1$. Sử dụng tính chất hệ thặng dư đầy đủ.

Bài 3. Ta có thể chứng minh dựa vào kiến thức về hệ thặng dư đầy đủ, cũng có thể chứng minh dựa vào định lí Thặng dư trung Hoa.

Bài 4. Sử dụng HTG.

Bài 5. Biểu diễn $P(x)$ dưới dạng $P(x)=a_px^p+a_{p-1}x^{p-1}+...+a_2x^2+a_1x+a_0$. Phản chứng, giả sử $P(x)$ có nghiệm nguyên $x=u$. Suy ra mâu thuẫn.

Bài 6. Tiến hành tương tự Ví dụ 6.7.

Bài 7. Sử dụng kiến thức HDD.

Bài 8. Đáp số: 887.

Bài 9. Gọi p_k là số nguyên tố thứ k, $k > 0$. Theo định lí Thặng dư Trung Hoa, tồn tại dãy số $\{a_n\}_{n=1}^{\infty}$ thỏa mãn $a_1 = 2; a_n = -k(\mathrm{mod} p_{k+1}), \forall k \leq n$.

Bài 10. Định lý Thặng dư Trung Hoa.

Bài 11. Chứng minh n có dạng 2^k. Sử dụng tính chất của số Fecma (xem lại Ví dụ 6.15).

Bài 12. Ví dụ 6.15 và Bài 3.

Do đó, $d = 8$ bị loại.

• Trường hợp 2: $\boxed{\text{d=4}} \Rightarrow \left(\frac{c}{4}; \frac{c}{4} + 2(ac+1)^2\right) = 1$

$\Rightarrow \frac{c}{4}; \frac{c}{4} + 2(ac+1)^2$ là những số chính phương (*)

Nếu $\frac{c}{4}$ là số chẵn $\Rightarrow \frac{c}{4} + 2(ac+1)^2 \vdots 2$

$\Rightarrow \left(\frac{c}{4}; \frac{c}{4} + 2(ac+1)^2\right) = 2$: mâu thuẫn.

Do đó, $\frac{c}{4}$ là số lẻ. Mà $\frac{c}{4}$ là số chính phương $\Rightarrow \frac{c}{4} \equiv 1 \pmod 4$

Mặt khác, do c chẵn nên $ac+1$ là số lẻ $\Rightarrow (ac+1)^2 \equiv 1 \pmod 4$

$\Rightarrow \frac{c}{4} + 2(ac+1)^2 \equiv 1 + 2.1 \equiv 3 \pmod 4$: vô lý do (*).

Do đó, $d = 4$ bị loại.

• Trường hợp 3: $\boxed{\text{d=2}}$.

Tương tự tự Trường hợp 2, ta có $\frac{c}{2}$ lẻ $\Rightarrow \frac{c}{2} \equiv 1 \pmod 8$

c chẵn nên $ac+1$ lẻ $\Rightarrow (ac+1)^2 \equiv 1 \pmod 8$

$$\Rightarrow \frac{c}{2} + 4(ac+1)^2 \equiv 1 + 4.1 \equiv 5 \pmod 8 : \text{ vô lý}$$

Do đó, $d = 2$ bị loại.

• Trường hợp 4: $\boxed{\text{d=1}}$

Tương tự trường hợp 2, ta có ngay c lẻ và do $(c; c + 8(ac+1)^2) = 1$ nên c là số chính phương.

Vậy ta có đpcm. ■

Nhận xét. Ta thấy trong bài này, b và c có 1 mối liên quan khá chặt chẽ với nhau nên ta thử giải theo b, c sử dụng kĩ thuật GCD tức là đặt $d = GCD(b; c)$ ta có cách chứng minh thứ 2.

Chứng minh (Chứng minh 2). Đặt $d = (b; c) \Rightarrow \begin{cases} c = dm \\ b = dn \end{cases} \left(\begin{array}{c} m; n \in \mathbb{N}^* \\ (m; n) = 1 \end{array} \right)$

7.2 $c(ac+1)^2=(5c+2)(2c+b)$

Bài toán 7.2. *Cho 3 số nguyên dương $a;b;c$ thoả mãn đẳng thức:*

$$c(ac+1)^2=(5c+2b)(2c+b) \tag{7.7}$$

Chứng minh rằng : c là số chính phương lẻ. △

Nhận xét. Thoạt nhìn vào bài toán, thật khó để tìm 1 phương pháp cho loại này. Nhận xét trong giả thiết ở VP (7.7), thì b xuất hiện với bậc là 2. Thế là ta có 1 hướng nghĩ là dùng tam thức bậc 2 cho bài toán này. Ta không nên chọn c vì bậc của c là 3, không chọn a vì phương trình mới theo a hiển nhiên trở lại (7.7)

Chứng minh (Chứng minh 1).

$$\begin{aligned}&c\left(ac+1\right)^2=\left(5c+2b\right)\left(2c+b\right)\\&\Leftrightarrow 2b^2+9bc+10c^2-c\left(ac+1\right)^2=0\\&\Delta_b=81c^2-4.2.\left(10c^2-c\left(ac+1\right)^2\right)=c^2+8c\left(ac+1\right)^2\\&\Rightarrow\Delta_b=c\left[c+8\left(ac+1\right)^2\right]=x^2,(x\in\mathbb{N}^*)\end{aligned}$$

Đặt $\left.\begin{array}{l}d=GCD(c;c+8(ac+1)^2)\Rightarrow d|8\left(ac+1\right)^2\\d|c\Rightarrow\left(\left(ac+1\right)^2;d\right)=1\end{array}\right\}\Rightarrow d|8$

• Trường hợp 1: $\boxed{\text{d=8}}\Rightarrow\left(\frac{c}{8};\frac{c}{8}+\left(ac+1\right)^2\right)=1$

$$\begin{aligned}&c\left[c+8\left(ac+1\right)^2\right]=x^2(x\in\mathbb{N})\Leftrightarrow\frac{c}{8}.\left(\frac{c}{8}+\left(ac+1\right)^2\right)=\left(\frac{x}{8}\right)^2\\&\Rightarrow 8|x\Rightarrow x=8x_2\,(x_2\in\mathbb{N}^*)\Rightarrow\frac{c}{8}.\left(\frac{c}{8}+\left(ac+1\right)^2\right)=x_2^2\\&\Rightarrow\left\{\begin{array}{l}\frac{c}{8}=t^2\\\frac{c}{8}+\left(ac+1\right)^2=p^2\end{array}\right.\left(\begin{array}{l}t;p\in\mathbb{N}^*\\(t;p)=1\end{array}\right)\\&\Rightarrow\left\{\begin{array}{l}c=8t^2\\t^2+\left(8t^2a+1\right)^2=p^2\end{array}\right.\end{aligned}$$

Mà dễ chứng minh

$$\begin{aligned}&\left(8t^2a+1\right)^2<t^2+\left(8t^2a+1\right)^2<\left(8t^2a+2\right)^2\\&\Rightarrow\left(8t^2a+1\right)^2<p^2<\left(8t^2a+2\right)^2:\text{ mâu thuẫn}\end{aligned}$$

Chương

7 Một số bài toán số học hay trên VMF

Phần này gồm một số bài toán hay được thảo luận nhiều trên Diễn đàn Toán học. Bạn đọc có thể vào trực tiếp topic của bài toán đó trên Diễn đàn Toán học, bằng cách click vào tiêu đề của bài toán đó.

7.1 $m^3+17\vdots 3^n$

Bài toán 7.1. *Chứng minh rằng với mọi số nguyên dương n, tồn tại một số tự nhiên m sao cho*

$$\left(m^3+17\right)\vdots 3^n$$

. △

Đầu tiên, chúng ta đến với chứng minh đề xuất cho bài toán đầu bài.

Chứng minh. Ta sẽ chứng minh bài toán bằng quy nạp.

Với $n=1$, ta chọn $m=4$.

Với $n=2$, ta chọn $m=1$.

Giả sử bài toán đúng đến $n=k$, hay $\exists m\in\mathbb{N}:m^3+17\vdots 3^k$

Ta chứng minh rằng đối với trường hợp $n=k+1$ cũng đúng tức là tồn tại một số m' sao cho $m'^3+17\vdots 3^{k+1}$.

Đặt $m^3+17=3^k.n\Rightarrow n\not\vdots 3$.

$$\Rightarrow \left[\begin{array}{l} n \equiv 2 \\ n \equiv 1 \end{array}\right. (\text{mod} 3) \Rightarrow \left[\begin{array}{l} m^3+17 \equiv 2.3^k \\ m^3+17 \equiv 3^k \end{array}\right. \left(\text{mod} 3^{k+1}\right)$$

• ***Trường hợp 1:*** $m^3+17 \equiv 2.3^k \pmod{3^{k+1}}$
Xét:

$$(m+3^{k-1})^3 = m^3+m^2 3^k+m3^{2k-1}+3^{3k-3} \equiv m^3+m^2 3^k \pmod{3^{k+1}}$$

(Do $k \geq 2 \Rightarrow 3^{2k-1} \vdots 3^{k+1}$ và $3^{3k-3} \vdots 3^{k+1}$).
Suy ra:

$$\left(m+3^{k-1}\right)^3+17 \equiv m^3+m^2.3^k+17 \equiv 2.3^k+m^2.3^k \equiv 0 \pmod{3^{k+1}}$$

(vì $m \not\vdots 3 \Rightarrow m^2 \equiv 1 \pmod 3 \Rightarrow 2+m^2 \vdots 3 \Rightarrow (2+m^2).3^k \vdots 3^{k+1}$).

Như vậy, ở trường hợp 1, ta có: $\left(m+3^{k-1}\right)^3+17 \vdots 3^{k+1}$.

• ***Trường hợp 2:*** $m^3+17 \equiv 3^k \pmod{3^{k+1}}$.
Xét:

$$\left(m-3^{k-1}\right)^3 = m^3-m^2 3^k+m3^{2k-1}-3^{3k-3} \equiv m^3-m^2 3^k \pmod{3^{k+1}}$$

(Do $k \geq 2 \Rightarrow 3^{2k-1} \vdots 3^{k+1}$ và $3^{3k-3} \vdots 3^{k+1}$).
Suy ra:

$$\left(m-3^{k-1}\right)^3+17 \equiv m^3-m^2 3^k+17 \equiv 3^k-m^2 3^k \equiv 0 \pmod{3^{k+1}}$$

(vì $m \not\vdots 3 \Rightarrow m^2 \equiv 1 \pmod 3 \Rightarrow 1-m^2 \vdots 3 \Rightarrow \left(1-m^2\right).3^k \vdots 3^{k+1}$).

Như vậy, ở trường hợp 2 ta có: $\left(m-3^{k-1}\right)^3+17 \vdots 3^{k+1}$.

Tóm lại, ta đều tìm được số nguyên $t \not\vdots 3$ mà $t^3+17 \vdots 3^{k+1}$.
Ta đã chứng minh được vấn đề đúng trong trường hợp $n=k+1$.
Theo nguyên lý quy nạp, ta có đpcm.

Mấu chốt bài toán này là bổ đề sau:

Mặt khác $X^{x_0} \equiv {x_n}^{x_0} \pmod{p^n}$ (do cách chọn trong hệ (II)).

$$\Rightarrow X^X+y \equiv {x_n}^{x_0}+y \equiv 0 \pmod{p^n}$$

Theo nguyên lý quy nạp, bài toán đã được chứng minh. ■

Mở rộng của bài toán đầu đề vẫn còn nhiều, như tăng thêm điều kiện để chặn như $(m^3+17 \vdots 3^n) \wedge (m^3+17 \not\vdots 3^{n+1})$, v.v. Rất mong nhận được ý kiến đóng góp cho việc mở rộng.

Lời cảm ơn

Rất cảm ơn Nguyen Lam Thinh, Karl Heinrich Marx,nguyenta98, The Gunner đã đóng góp ý kiến và mở rộng cho bài viết này.

Chưa dừng lại ở đây, nếu trong (7.3), ta thay k bởi x, ta sẽ được 1 bài toán khác:

ĐỊNH LÝ 7.2– *Cho p nguyên tố lẻ. $y \in \mathbb{N}$ và y cố định. Biết rằng $gcd(y, p) = 1$. Khi đó:*

$$\forall n \in \mathbb{N}, \exists x \in \mathbb{N} : x^x + y \vdots p^n \tag{7.6}$$

Chứng minh. Ta chứng minh bài toán này bằng phương pháp quy nạp. Ta coi định lý 7.1 như 1 bổ đề. Dễ thấy nếu x thỏa (7.6) thì $gcd(x; p) = 1$.
Khi đó, với $n = 1$, ta xét hệ đồng dư (I)

$$\begin{cases} x \equiv k \pmod{(p-1)} \\ x \equiv x_0 \pmod{p} \end{cases}$$

trong đó, $x_0; k \in \mathbb{N}$ thỏa $x_0^k + y \vdots p$.
Do $gcd(p-1; p) = 1$ nên theo định lý Thặng dư Trung Hoa thì hệ (I) luôn có nghiệm x'.
Chọn $x = x'$, ta chứng minh x thỏa (7.6) khi $n = 1$. Thật vậy

$$\begin{aligned} gcd(x; p) = 1 \Rightarrow x^{p-1} \equiv 1 \pmod{p} \Rightarrow x^k \equiv x^x \pmod{p} \\ \Rightarrow x^x + y \equiv x^k + y \equiv x_0^k + y \equiv 0 \pmod{p} \end{aligned}$$

Vậy $\exists x \in \mathbb{N} : x^x + y \vdots p$.

Giả sử (7.6) đúng đến $n-1$, tức là tồn tại x_0 để ${x_0}^{x_0} + y \vdots p^{n-1}$.
Theo cách chứng minh quy nạp ở (7.6), ta chọn được $x_n = ap^n + x_0$ thỏa $x_n^{x_0} + y \vdots p^n$.
Khi đó, dễ nhận thấy $x_n \equiv x_0 \pmod{p^{n-1}}$. Ta xét hệ đồng dư (II)

$$\begin{cases} X \equiv x_0 \pmod{(p^{n-1}(p-1))} \\ X \equiv x_n \pmod{p^n} \end{cases}$$

Do $gcd(p^{n-1}(p-1); p^n) = 1$ nên theo định lý Thặ ng dư Trung hoa, hệ (II) có nghiệm X. Ta chứng minh $x = X$ thỏa (7.6). Thật vậy
Do $(p-1)p^{n-1} = \phi(p^n) \Rightarrow X^X \equiv X^{x_0} \pmod{p^n}$ (định lý Euler).

BỔ ĐỀ 7.1– *Cho a, b, q là các số nguyên thỏa $(a; q) = 1$ và $q > 0$.*
Khi ấy, luôn tồn tại $k \in \mathbb{Z}$ sao cho $ak \pm b \vdots q$. □

Chứng minh. Ta chứng minh đại diện cho trường hợp $ak + b \vdots q$. Trường hợp còn lại tương tự.
Xét $A = \{1; 2; 3; ...; q\}$ là 1 hệ đầy đủ HĐD mod q.
Theo tính chất của Hệ thặng dư, ta có tập $B = \{a; 2a; 3a; ...; qa\}$ cũng là HĐD mod q.
$\Rightarrow C = \{a + b; 2a + b; 3a + b; ...; qa + b\}$ cũng là HĐD mod q.
Do đó, tồn tại $k \in [1; q]$ sao cho $ak + b \vdots q$. ■

Nhận xét. Bài toán đã cho thực chất là yêu cầu tìm 1 số x nguyên sao cho $x + 17 \vdots 3^n$ và x là lập phương 1 số nguyên. Bổ đề trên đã cho thấy sự tồn tại của x nguyên để $x + 17 \vdots 3^n$. Còn việc tìm x để là x là lập phương 1 số nguyên thì ta sẽ dùng phương pháp quy nạp như trên.
Đối với 1 người yêu toán, ta phải không ngừng sáng tạo. Ta hãy thử tổng quát bài toán đã cho:

- thay vì m^3, ta thử thay m^k với k là số nguyên dương cố định.
- thay vì 3^n, ta thử thay p^n với p là 1 số nguyên tố.
- thay số 17 bởi $y \in \mathbb{N}$ với y cố định.

Kết hợp các thay đổi trên, ta có 1 bài toán "tổng quát" hơn

DỰ ĐOÁN 7.1– *Cho p là số nguyên tố. $y, k \in \mathbb{N}$ và y, k cố định. Khẳng định hoặc phủ định mệnh đề sau*

$$\forall n \in \mathbb{N}, \exists x \in \mathbb{N} : x^k + y \vdots p^n \tag{7.1}$$

Ta thử thay một vài giá trị p, k, y vào để thử xem (7.1) có đúng không.

Khi thay $k = 2, y = 1, p = 3$ thì mệnh đề (7.1) trở thành

$$\forall n \in \mathbb{N}, \exists x \in \mathbb{N} : x^2 + 1 \vdots 3^n \tag{7.2}$$

Rất tiếc, khi này, (7.2) lại sai!!!. Ta sẽ chứng minh (7.2) sai khi $n \geq 1$.

Thật vậy, để chứng minh dự đoán 7.1 sai, ta cần có bổ đề sau

Bổ đề 7.2– *Cho p là số nguyên tố dạng $4k+3$ và $a, b \in \mathbb{Z}$. Khi đó*

$$a^2 + b^2 \vdots p \Leftrightarrow (a \vdots p) \wedge (b \vdots p)$$

Từ (7.2), suy ra $x^2 + 1 \vdots 3$. Áp dụng bổ đề 7.2 với $p = 3$, ta suy ra $1 \vdots 3$: vô lý.

Vậy khi $n \geq 1$ thì $\nexists x \in \mathbb{Z} : x^2 + 1 \vdots 3^n$.

Không nản lòng, ta thử thêm một vài điều kiện để (7.1) trở nên chặt hơn và đúng. Nếu bạn đọc có ý kiến nào hay, xin hãy gửi vào topic này để thảo luận. Sau khi thêm một số điều kiện, ta có 1 bài toán hẹp hơn nhưng luôn đúng.

Định lý 7.1– *Cho p nguyên tố lẻ. $y, k \in \mathbb{N}$ và y, k cố định.*
Biết rằng $gcd(k, p) = gcd(k, p-1) = gcd(y, p) = 1$.
Chứng minh rằng:

$$\forall n \in \mathbb{N}, \exists x \in \mathbb{N} : x^k + y \vdots p^n \tag{7.3}$$

Chứng minh. Trước hết, để chứng minh (7.3), ta cần có bổ đề sau

Bổ đề 7.3– *Cho p là số nguyên tố lẻ. k nguyên dương thỏa*

$$(k; p) = (k-1; p) = 1$$

Khi đó, $\{1^k; 2^k; ...; (p-1)^k\}$ là HTG mod$p$. □

Chứng minh. Gọi g là căn nguyên thủy của p tức là $ord_p(g) = p-1$.
Khi đấy thì $g^1, g^2, ..., g^{p-1}$ lập thành 1 HTG mod$p$ và rõ ràng $g^{a_1}, g^{a_2}, ..., g^{a_{p-1}}$ là HTG mod$p \Leftrightarrow a_1, a_2, .., a_{p-1}$ là HĐĐ của $p-1$.
Với $1 \leq i \leq p-1$ thì tồn tại a_i để mà $i \equiv g^{a_i} \pmod p$ và rõ ràng a_i lập thành 1 HTG mod$p$ nên hệ $1^k, 2^k, .., (p-1)^k$ có thể viết lại là $g^k, g^{2k}, ..., g^{(p-1)k}$, nó là HTG mod$p$ khi và chỉ khi $k, 2k, ..., (p-1)k$ là hệ thặng dư đầy đủ của $p-1$, tức là k nguyên tố cùng nhau với $p-1$.
Bổ đề được chứng minh. ■

Quay lại bài toán. Ta chứng minh (7.3) bằng phương pháp quy nạp.
Với $n = 1$, theo bổ đề 7.3 thì

$$\exists x_0 \in \{1; 2; ...; p-1\} : x_0^k \equiv -y \pmod p \Rightarrow x_0^k + y \vdots p$$

Giả sử bài toán đúng đếnn hay tồn tại $x^k + y \vdots p^n$

Ta sẽ chứng minh $n+1$ cũng đúng hay tồn tại $x_0^k + y \vdots p^{n+1}$
Thật vậy, từ giả thiết quy nạp suy ra $x^k + y = p^n.q$

- Trường hợp 1: $q \vdots p \Rightarrow$ đpcm
- Trường hợp 2:

$$gcd(q, p) = 1 \tag{7.4}$$

Khi đó ta chọn $x_0 = v.p^n + x$
Do đó

$$\begin{aligned} &x_0^k + y = (v.p^n + x)^k + y \\ &= v^k.p^{nk} + \binom{1}{k}.v^{k-1}.p^{n(k-1)}.x + ... + \binom{k-1}{k}.v.p^n.x^{k-1} + (x^k + y) \end{aligned} \tag{7.5}$$

Dễ dàng chứng minh

$$p^{n+1} \mid v^k.p^{nk} + \binom{1}{k}.v^{k-1}.p^{n(k-1)}.x + ... \binom{k-2}{k}.v^2.p^{2n}.x^{k-2}$$

Do vậy ta xét

$$\binom{k-1}{k}.v.p^n.x^{k-1} + (x^k + y) = k.v.p^n.x^{k-1} + p^n.q = p^n(k.v.x^{k-1} + q)$$

Nhận thấy giả sử $k.x^{k-1} \equiv t \pmod p$ mà $gcd(k, p) = 1$ và $x^k + y \vdots p \Rightarrow gcd(x, p) = 1$ (do $gcd(y, p) = 1$) suy ra $gcd(t, p) = 1$
Do đó $(k.v.x^{k-1} + q) \equiv tv + q \pmod p$ mà từ (7.4) ta đã có $gcd(q, p) = 1$

Cho nên luôn tồn tại v thỏa mãn $tv + q \vdots p$. Do đó bài toán được khẳng định với $n+1$.
Theo nguyên lý quy nạp, bài toán đã được chứng minh.