

ỨNG DỤNG MỘT MỆNH ĐỀ VÀO GIẢI CÁC BÀI TOÁN SỐ HỌC

Phạm Quang Toàn
Trần Quốc Nhật Hân - perfectstrong

Bài viết cho trang chủ VMF - diendantoanhoc.net
Kỉ niệm 8 năm thành lập diễn đàn toán học.

1. Mở đầu

Trước hết ta đến với bài toán nhỏ sau.

Bài toán gốc. Giả sử $p = k \cdot 2^t + 1$ là số nguyên tố lẻ, t là số nguyên dương và k là số tự nhiên lẻ. Giả thiết x và y là các số tự nhiên mà $(x^{2^t} + y^{2^t}) \vdots p$. Chứng minh rằng khi đó x và y đồng thời chia hết cho p .

Chứng minh. Giả sử trái lại $x \not\vdots p$, suy ra $y \not\vdots p$.
Do p là số nguyên tố nên theo định lý Fermat nhỏ ta có

$$\begin{cases} x^{p-1} \equiv 1 \pmod{p} \\ y^{p-1} \equiv 1 \pmod{p} \end{cases}$$

Theo giả thiết thì $p - 1 = k \cdot 2^t$, do đó

$$\begin{cases} x^{k \cdot 2^t} \equiv 1 \pmod{p} \\ y^{k \cdot 2^t} \equiv 1 \pmod{p} \end{cases}$$

Từ đó ta có

$$x^{k \cdot 2^t} + y^{k \cdot 2^t} \equiv 2 \pmod{p}. \quad (1)$$

Theo giả thiết thì

$$x^{2^t} + y^{2^t} \equiv 0 \pmod{p}.$$

Do k lẻ nên

$$x^{k \cdot 2^t} + y^{k \cdot 2^t} = (x^{2^t})^k + (y^{2^t})^k \vdots (x^{2^t} + y^{2^t}) \Rightarrow (x^{k \cdot 2^t} + y^{k \cdot 2^t}) \equiv 0 \pmod{p} \quad (2)$$

Từ (1) và (2) suy ra điều mâu thuẫn. Vậy giả thiết phản chứng sai. Do đó x, y đồng thời chia hết cho p . $\square$

Từ bài toán trên, áp dụng với $t = 1$ ta có mệnh đề sau:

Mệnh đề 1. Cho p là số nguyên tố dạng $4k + 3$. Khi đó nếu $x^2 + y^2$ chia hết cho p thì x và y đều chia hết cho p .

Chứng minh. Ta dùng phản chứng. Giả sử a và b không đồng thời chia hết cho p . Ta có các trường hợp sau:

- **Trường hợp 1.** Nếu $a \vdots p, b \not\vdots p$.

$$\Rightarrow a^2 \vdots p; b^2 \not\vdots p \Rightarrow a^2 + b^2 \not\vdots p.$$

Mâu thuẫn với giả thiết ban đầu.

- **Trường hợp 2.** Nếu $a \not\equiv p, b \equiv p$. Tương tự trường hợp 1, trường hợp này cũng mâu thuẫn với giả thiết.
- **Trường hợp 3.** Nếu $a \not\equiv p, b \not\equiv p$. Vì p nguyên tố nên theo định lý Fermat nhỏ ta có:

$$\begin{aligned} a^{p-1} &\equiv 1 \pmod{p} \\ b^{p-1} &\equiv 1 \pmod{p} \\ \Leftrightarrow a^{4k+2} &\equiv 1 \pmod{p}, b^{4k+2} \equiv 1 \pmod{p} \\ \Leftrightarrow (a^2)^{2k+1} &\equiv 1 \pmod{p}, (b^2)^{2k+1} \equiv 1 \pmod{p} \\ \Rightarrow (a^2)^{2k+1} + (b^2)^{2k+1} &\equiv 2 \pmod{p} \end{aligned}$$

Do p là số nguyên tố có dạng $4k+3$ nên $p \geq 3$, nên

$$(a^2)^{2k+1} + (b^2)^{2k+1} \not\equiv p \pmod{p} \quad (1)$$

Lại có

$$(a^2)^{2k+1} + (b^2)^{2k+1} \equiv a^2 + b^2 \pmod{p}$$

Điều này mâu thuẫn với (1).

Vậy giả thiết phản chứng sai. $\square$

Mệnh đề 2. Giả sử a, b là hai số tự nhiên khác 0 và nguyên tố cùng nhau. Khi đó các ước nguyên tố lẻ của $a^2 + b^2$ chỉ có thể có dạng $4m+1$, $m \in \mathbb{Z}$.

Chứng minh. Giả sử tồn tại số nguyên tố p dạng $4m+3$ sao cho $(a^2 + b^2) \equiv p$. Theo mệnh đề 1 suy ra $a \equiv p, b \equiv p$. Do đó $(a, b) = p > 1$, mâu thuẫn với điều kiện a, b nguyên tố cùng nhau. Ta có đpcm. $\square$

2. Một số ứng dụng

Ta xét đến bài toán tổng quát cho mệnh đề 1 trên:

Bài 1. Tìm tất cả các số nguyên tố p sao cho với mọi a, b nguyên thì $(a+b) \equiv p$ khi và chỉ khi a và b đồng thời chia hết cho p .

Chứng minh. Xét các khả năng sau:

1. Nếu $p = 2$. Rõ ràng với mọi a, b lẻ thì $(a+b) \equiv 2$, mà a, b đều không chia hết cho 2. Vậy $p = 2$ không thỏa mãn.
2. Nếu $p \geq 3$ thì p lẻ, nên p có dạng $4k+1$ hoặc $4k+3$, $k \in \mathbb{N}$.
Xét tiếp hai trường hợp sau:

- Nếu p có dạng $4k+1$. Theo định lý Willson, ta có:

$$(p-1)! + 1 \equiv 0 \pmod{p} \Rightarrow (4k)! + 1 \equiv 0 \pmod{p}. \quad (2)$$

Do $p = 4k+1$ nên suy ra:

$$4k \equiv -1 \pmod{p} \Rightarrow 4k-1 \equiv -2 \pmod{p} \Rightarrow \dots \Rightarrow 2k+1 \equiv -2k \pmod{p}.$$

Ta suy ra

$$((4k)! + 1) \equiv [(2k!)^2 + 1] \pmod{p}. \quad (3)$$

Từ (1) và (2) ta có:

$$[(2k!)^2 + 1^2] \equiv 0 \pmod{p}. \quad (4)$$

Rõ ràng khi $p = 4k+1$, thì không thể có kết luận trên. Thật vậy, nếu kết luận ấy đúng thì từ (3) suy ra $1 \equiv p$, vô lý vì $p = 4k+1 \geq 3$.

Vậy với mọi số nguyên tố lớn hơn 3 có dạng $4k+1$ không thỏa mãn yêu cầu đề bài.

- Nếu p có dạng $4k + 3$. Giả sử bài toán không đúng với $p = 4k + 3$, điều đó có nghĩa là tồn tại cặp số nguyên a, b sao cho $(a + b) \vdots p$ nhưng $a \not\vdots p, b \not\vdots p$. Theo định lý Fermat nhỏ, ta có:

$$a^{p-1} - 1 \equiv 0 \pmod{p}.$$

Tương tự ta có

$$b^{p-1} - 1 \equiv 0 \pmod{p}.$$

Do đó

$$a^{p-1} + b^{p-1} - 2 \equiv 0 \pmod{p} \Rightarrow a^{4k+2} + b^{4k+2} - 2 \equiv 0 \pmod{p} \quad (5)$$

$$\Rightarrow (a^2)^{2k+1} + (b^2)^{2k+1} - 2 \equiv 0 \pmod{p}. \quad (6)$$

Áp dụng hằng đẳng thức suy ra:

$$(a^2)^{2k+1} + (b^2)^{2k+1} = (a^2 + b^2)q, \quad q \in \mathbb{N}^*$$

Do $(a^2 + b^2) \vdots p$, nên từ (5) đi đến:

$$-2 \equiv 0 \pmod{p} \Rightarrow 2 \vdots p.$$

Điều này vô lý vì $p \geq 3$. Vậy giả thiết ban đầu là sai.

Bài toán được chứng minh. □

Một số bài toán dưới đây đòi hỏi phải ứng dụng mệnh đề 1.

Bài 2.

Tìm các số nguyên dương x, y, z, t thỏa mãn hệ phương trình

$$\begin{cases} x^2 + 13y^2 = z^2 \\ 13x^2 + y^2 = t^2 \end{cases}$$

Chứng minh. Đặt $(x, y) = d \Rightarrow z \vdots d$.

$$x = d_1$$

$$\text{Đặt } y = dy_1.$$

$$z = dz_1$$

(x_1, y_1, z_1) nguyên dương, $(x_1, y_1) = 1$

Từ hệ trên dễ dàng suy ra

$$14(x^2 + y^2) = z^2 + t^2$$

$$\Rightarrow 14(x_1^2 + y_1^2) = z_1^2 + t_1^2 \Rightarrow z_1^2 + t_1^2 \vdots 7.$$

Áp dụng mệnh đề ta có $x_1 \vdots 7, y_1 \vdots 7$.

Mâu thuẫn với giả thiết $(x_1, y_1) = 1$.

Vậy phương trình không có nghiệm nguyên dương. □

Bài 3. (Đấu trường VMF - Trận thứ 4 vòng bảng Alpha, Gama - Câu 1 đội Alpha)

Tìm nghiệm nguyên của phương trình:

$$x^{1994} + y^{1994} = 4691^{4691} (x + y) \quad (7)$$

Chứng minh. (perfectstrong) Nhận thấy 4691 là số nguyên tố dạng $4k + 3$.

$$(7) \Leftrightarrow (x^{997})^2 + (y^{997})^2 = 4691^{4691} (x + y).$$

Áp dụng mệnh đề 1 ta có:

$$\begin{cases} x^{997} : 4691 \\ y^{997} : 4691 \end{cases} \Rightarrow \begin{cases} x = 4691x_1 \\ y = 4691y_1 \end{cases}$$

với $x_1, y_1 \in \mathbb{N}^*$. Thay vào (7) ta có:

$$x_1^{4691} + y_1^{4691} = 4691^{2698} (x_1 + y_1). \quad (8)$$

Áp dụng mệnh đề lần nữa ta có:

$$\begin{cases} x_1 = 4691x_2 \\ y_1 = 4691y_2 \end{cases}$$

với $x_2, y_2 \in \mathbb{N}^*$. Thay vào (8) ta có:

$$x_2^{4691} + y_2^{4691} = 4691^{705} (x_2 + y_2) \quad (9)$$

Tiếp tục áp dụng mệnh đề lần nữa, ta có:

$$\begin{cases} x_2 = 4691x_3 \\ y_2 = 4691y_3 \end{cases}$$

với $x_3, y_3 \in \mathbb{N}^*$. Thay vào (9) ta có

$$4691^{1228} (x_3^{1994} + y_3^{1994}) = x_3 + y_3 \quad (10)$$

Rõ ràng phương trình (10) không có nghiệm nguyên dương vì hiển nhiên $VT > VP$. Vậy phương trình (7) không có nghiệm nguyên dương. $\square$

Ta có bài toán tương tự sau:

Bài 4. Cho k là số nguyên dương cho trước. Tìm nghiệm nguyên dương của phương trình

$$x^2 + y^2 = 2011^{2003^k+1} (10 - z).$$

Tiếp tục đến với bài toán sau:

Bài 5.

Cho m, n là các số nguyên dương thỏa

$$m^2 + 9 : 2^n - 1.$$

Chứng minh rằng n là lũy thừa của 2.

Chứng minh. Đặt $n = 2^k \cdot l$ với $k, l \in \mathbb{N}$ và l lẻ.

Nếu $l \geq 3$ thì

$$\begin{aligned} m^2 + 9 : 2^n - 1 \\ 2^n - 1 = 2^{2^k \cdot l} - 1 = (2^l)^{2^k} - 1^{2^k} : 2^l - 1 \Rightarrow m^2 + 9 : 2^l - 1 \end{aligned}$$

Mà $l \geq 3 \Rightarrow 2^l : 4 \Rightarrow 2^l - 1 \equiv 3 \pmod{4}$ nên $2^l - 1$ có 1 ước nguyên tố p dạng $4k + 3$.

$$\left. \begin{aligned} l \geq 3 \Rightarrow 2^l : 4 \Rightarrow 2^l - 1 &\equiv 3 \pmod{4} \\ \Rightarrow m^2 + 9 : p &\Rightarrow 3 : p \Rightarrow p = 3 \\ 2^l - 1 = (3 - 1)^l - 1 &\equiv -2 \pmod{3} \end{aligned} \right\} \text{ vô lí}$$

Do đó $l = 1 \Rightarrow n = 2^k$. $\square$

Sau đây là một số bài toán áp dụng mệnh đề 2.

Bài 6. (*Bài toán Lebesgue*)

Chứng minh rằng phương trình

$$x^2 - y^3 = 7$$

không có nghiệm nguyên.

Chứng minh. Giả sử trái lại, tồn tại số nguyên x, y thỏa mãn

$$x^2 - y^3 = 7 \quad (11)$$

Chỉ có hai khả năng sau:

1. Nếu y chẵn, tức $y = 2k$. Thay vào (11) ta có

$$x^2 = 8k^3 + 7 \quad (12)$$

Nhận thấy một số chính phương chia 8 dư 0, 1, 4. Điều này mâu thuẫn với (11), vậy y không thể chẵn.

2. Nếu y lẻ. Viết lại (11) dưới dạng

$$x^2 + 1 = y^3 + 8 \Leftrightarrow x^2 + 1^2 = (y + 2)(y^2 - 2y + 4).$$

Do y lẻ, nên lại có các khả năng sau:

- Nếu y chia 4 dư 1. Khi đó

$$y + 2 = 4k + 3$$

- Nếu y chia 4 dư 3. Khi đó

$$y^2 - 2y + 4 = (4m + 3)^2 - 2(4m + 3) + 4 = 4t + 3.$$

Vậy trong mọi trường hợp $x^2 + 1$ đều có ước dạng $4k + 3$, vì thế nó phải có ước nguyên tố dạng $4k + 3$. Rõ ràng điều này mâu thuẫn với mệnh đề 2 đã nêu.

Ta suy ra giả thiết phản chứng sai. □

Bài 7. Chứng minh rằng phương trình

$$4xy - x - y = z^2 \quad (13)$$

vô nghiệm nguyên.

Chứng minh. Viết phương trình đã cho dưới dạng

$$\begin{aligned} 16xy - 4x - 4y &= 4z^2 \Leftrightarrow 16xy - 4x - 4y + 1 = 4z^2 + 1 \\ &\Leftrightarrow (4x - 1)(4y - 1) = (2z)^2 + 1. \end{aligned} \quad (14)$$

Giả sử (14) có nghiệm nguyên (x, y) thì từ (14) ta có:

$$(4x - 1)(4y - 1) = (2z)^2 + 1 \Leftrightarrow [4(x - 1) + 3][4(y - 1) + 3] = (2z)^2 + 1^2.$$

Lập luận như bài 6 ta suy ra $(2z)^2 + 1$ có ước nguyên tố dạng $4k + 3$. Điều này mâu thuẫn với mệnh đề 2. Vậy phương trình $4xy - x - y = z^2$ không có nghiệm nguyên. □

Nhận xét. Dưới đây là lời giải bài 7 của Euler:

Giả sử phương trình có nghiệm $(x, y, z) = (m, n, c)$ và giả sử c là giá trị nhỏ nhất của z .

$$\begin{aligned} &\Rightarrow 4mn - m - n = c^2 \\ &\Rightarrow (4m - 1)(4n - 1) - 1 = c^2. \quad (15) \end{aligned}$$

Cộng vào hai vế $4(4n - 1)^2 - 8a(4n - 1)$ vào hai vế của (16) ta có

$$[4m - 1 - 8c + 4(4n - 1)](4n - 1) - 1 = 4(c - 4n + 1)^2. \quad (16)$$

Như vậy phương trình có nghiệm $z = |c - 4n + 1|$.

Vì c là giá trị nhỏ nhất của z nên

$$\begin{aligned} &\Rightarrow |c - 4n + 1| > c \\ &\Rightarrow (c - 4n + 1)^2 > c^2 \\ &\Rightarrow [4m - 1 - 8a + 4(4n - 1)](4n - 1) > (4n - 1)(4m - 1) \\ &\Rightarrow 4n - 1 > 2c. \end{aligned}$$

Chúng minh tương tự ta cũng có $4m - 1 > 2c$.

Đặt $4m - 2 = p, 4n - 1 = 2a + q$ với p, q nguyên. Như vậy

$$(4m - 1)(4n - 1) = 4c^2 + 2c(p + q) + pq \quad (17)$$

Do đó từ (15) và (17) suy ra $2c = (p + q) + pq$. Điều này vô lí. Vậy phương trình không có nghiệm nguyên. $\square$

Tuy nhiên, cũng có thể thấy, rõ ràng cách chứng minh bằng mệnh đề trên nhanh và tiện lợi hơn cách chứng minh của Euler.

3. Bài tập

Một số bài cho mọi người luyện tập thêm về việc sử dụng mệnh đề này trong giải toán số học.

Bài 8. (Trần Quốc Nhật Hân – perfectstrong)

Cho n là số nguyên dương thỏa mãn:

(i) $3|2^n - 1$

(ii) $\exists m \in \mathbb{N} : 4m^2 + 1 \vdots \frac{2^n - 1}{3}$

Chúng minh rằng n là lũy thừa của 2.

Bài 9.

Giải phương trình nghiệm nguyên sau:

$$x^2 + 5 = y^3$$

Bài 10.

Tìm các nghiệm nguyên dương của phương trình

a) $x^2 + y^2 = 585$

b) $x^2 + y^2 = 2010$

c) $19x^2 + 18y^2 = 729$

d) $x^2 + y^2 = 3z^2$

Bài 11. Giả sử x, y là các số nguyên khác 0 sao cho $\frac{x^2 + y^2}{x + y}$ là số nguyên và là ước của 1978.

Chúng minh $x = y$.

(Chọn đội tuyển quốc gia CHLB Đức 1979)

Bài 12. Tìm tất cả các cặp số nguyên dương (x, y) sao cho $\frac{x^2 + y^2}{x - y}$ là số nguyên dương và là ước số của 1995.

Bài 13. Tìm số nhỏ nhất trong tập hợp các số chính phương dạng $15a + 16b$ và $16a - 15b$ với a, b là các số nguyên dương nào đó.

Bài 14. (Phạm Quang Toàn) Giải phương trình nghiệm nguyên

$$x^{2010} - 2006 = 4y^{2009} + 4y^{2008} + 2007y.$$