Bộ ba Pythagore

Bài toán tìm các tam giác vuông có ba cạnh nguyên dẫn đến phương trình $x^2 + y^2 = z^2$. Từ phân tích $x^2 = (z-y)(z+y)$, ta sẽ suy ra công thức Euclid mô tả tất cả các bộ ba Pythagore nguyên thủy. Công thức này còn cho phép dùng phương pháp xuống thang của Fermat để chứng minh rằng hai phương trình $x^4 + y^4 = z^2$ và $x^4 - y^4 = z^2$ đều không có nghiệm nguyên dương.

1 Định nghĩa và phân loại bộ ba Pythagore

Định nghĩa 1. Bộ ba số nguyên dương (x, y, z) được gọi là một *bộ ba Pythagore* nếu

$$x^2 + y^2 = z^2. \tag{1}$$

Bộ ba ấy được gọi là *nguyên thủy* nếu $\gcd(x, y, z) = 1$.

Cho một bộ ba Pythagore (x, y, z) và đặt $d = \gcd(x, y, z)$. Khi đó $(x/d, y/d, z/d)$ là một bộ ba Pythagore nguyên thủy. Vì thế, mọi bộ ba Pythagore đều là bội nguyên dương của duy nhất một bộ ba nguyên thủy.

Trong một bộ ba Pythagore nguyên thủy, ba số x, y, z đôi một nguyên tố cùng nhau. Thật vậy, nếu một số nguyên tố là ước của hai trong ba số ấy thì theo (1), nó cũng là ước của bình phương số còn lại, do đó là ước của cả ba số.

Định lý 1. Trong một bộ ba Pythagore nguyên thủy (x, y, z), hai số x, y khác tính chẵn lẻ và z là số lẻ.

Chứng minh. Vì $\gcd(x, y) = 1$, hai số x, y không thể cùng chẵn. Nếu chúng cùng lẻ thì $z^2 \equiv 1 + 1 \equiv 2 \pmod 4$, trong khi một số chính phương chỉ có thể dư 0 hoặc 1 khi chia cho 4. Vậy x, y khác tính chẵn lẻ. Do đó z^2 lẻ, suy ra z lẻ. □

Định lý 2 (Công thức Euclid)**.** Cho x, y, z là các số nguyên dương, với x chẵn. Bộ ba (x, y, z) là một bộ ba Pythagore nguyên thủy khi và chỉ khi tồn tại hai số nguyên $m > n > 0$, nguyên tố cùng nhau và khác tính chẵn lẻ, sao cho

$$x = 2mn, \qquad y = m^2 - n^2, \qquad z = m^2 + n^2.$$

Khi đó, cặp (m, n) được xác định duy nhất.

Chứng minh. Giả sử (x, y, z) là một bộ ba Pythagore nguyên thủy. Theo Định lý 1, y, z đều lẻ. Đặt

$$U = \frac{z+y}{2}, \qquad V = \frac{z-y}{2}.$$

Vì $z > y > 0$, ta có $U > V > 0$. Mọi ước chung của U, V đều chia $U + V = z$ và $U - V = y$. Do $\gcd(y, z) = 1$, suy ra $\gcd(U, V) = 1$. Mặt khác,

$$UV = \frac{z^2 - y^2}{4} = \left(\frac{x}{2}\right)^2.$$

Mỗi ước nguyên tố của UV chỉ xuất hiện trong một trong hai thừa số U, V, với số mũ chẵn. Vì thế $U = m^2$ và $V = n^2$ với hai số nguyên dương $m > n$. Ta được

$$x = 2mn, \qquad y = U - V = m^2 - n^2, \qquad z = U + V = m^2 + n^2.$$

https://nttuan.org/
Nguyễn Trung Tuấn, 0915011235

Từ $\gcd(U,V)=1$ suy ra $\gcd(m,n)=1$. Vì $m^2+n^2=z$ lẻ nên m,n khác tính chẵn lẻ. Hai đẳng thức $m^2=U$ và $n^2=V$ cũng cho thấy m,n được xác định duy nhất.

Ngược lại, cho m,n thỏa mãn các điều kiện trên. Đẳng thức

$$(2mn)^2+(m^2-n^2)^2=(m^2+n^2)^2$$

cho thấy (x,y,z) là một bộ ba Pythagore. Nếu một số nguyên tố p chia cả y và z thì p lẻ, vì y,z đều lẻ. Khi đó, từ

$$p \mid z+y=2m^2, \qquad p \mid z-y=2n^2$$

suy ra p chia cả m và n, trái với $\gcd(m,n)=1$. Vậy $\gcd(y,z)=1$ và bộ ba thu được là nguyên thủy. □

Chẳng hạn, để liệt kê các bộ ba nguyên thủy có cạnh huyền không vượt quá 100, ta chỉ cần xét $2 \le m \le 9$, vì $m^2+n^2 \le 100$ và $n \ge 1$. Bảng dưới đây liệt kê đủ 16 bộ ba. Trong mỗi bộ, cạnh góc vuông nhỏ hơn được viết trước.

m	Các giá trị của n	Các bộ ba tương ứng
2	1	$(3,4,5)$
3	2	$(5,12,13)$
4	1, 3	$(8,15,17)$, $(7,24,25)$
5	2, 4	$(20,21,29)$, $(9,40,41)$
6	1, 5	$(12,35,37)$, $(11,60,61)$
7	2, 4, 6	$(28,45,53)$, $(33,56,65)$, $(13,84,85)$
8	1, 3, 5	$(16,63,65)$, $(48,55,73)$, $(39,80,89)$
9	2, 4	$(36,77,85)$, $(65,72,97)$

2 Phương pháp xuống thang của Fermat

Trong một phép xuống thang, ta giả sử có nghiệm và chọn một nghiệm làm nhỏ nhất một đại lượng nguyên dương. Từ nghiệm này, ta dựng một nghiệm khác có giá trị của đại lượng ấy nhỏ hơn. Bổ đề bốn số dưới đây sẽ giúp ta thực hiện bước dựng nghiệm trong Hệ quả 1.

Bổ đề 1. Cho m,n,α,β là các số nguyên dương thỏa mãn $mn=\alpha\beta$. Khi đó tồn tại các số nguyên dương p,q,r,s sao cho

$$m=pq, \qquad n=rs, \qquad \alpha=pr, \qquad \beta=qs, \qquad \gcd(q,r)=1.$$

Nếu $\gcd(m,n)=1$ thì còn có $\gcd(p,s)=1$.

Chứng minh. Đặt $p=\gcd(m,\alpha)$ và viết $m=pq,\ \alpha=pr$. Ta có $\gcd(q,r)=1$ và $qn=r\beta$, nên $r \mid n$. Viết $n=rs$ rồi thay vào $qn=r\beta$, ta được $\beta=qs$. Cuối cùng, $p \mid m$ và $s \mid n$, nên nếu $\gcd(m,n)=1$ thì $\gcd(p,s)=1$. □

Hệ quả 1. Không tồn tại hai số nguyên dương a,b sao cho a^2+b^2 và a^2-b^2 đều là số chính phương.

Chứng minh. Giả sử có một cặp như vậy. Chọn một cặp (a,b) có a nhỏ nhất. Đặt $c=\sqrt{a^2+b^2}$ và $h=\sqrt{a^2-b^2}$. Với $d=\gcd(a,b)$, cả c^2 và h^2 đều chia hết cho d^2, nên d chia cả c và h. Do đó $(a/d,b/d)$ cũng thỏa mãn giả thiết. Tính nhỏ nhất của a cho $d=1$.

https://nttuan.org/
Nguyễn Trung Tuấn, 0915011235

Bộ ba (a, b, c) nguyên thủy, nên a, b khác tính chẵn lẻ. Nếu a chẵn thì $h^2 = a^2 - b^2 \equiv 3 \pmod 4$, vô lý. Vậy a lẻ và b chẵn. Vì $a^2 - b^2 \geq 0$ và $a \neq b$, ta có $a > b$. Theo Định lý 2, tồn tại hai số nguyên $m > n > 0$, nguyên tố cùng nhau, sao cho

$$a = m^2 - n^2, \qquad b = 2mn.$$

Hai số $a - b, a + b$ đều lẻ. Mọi ước chung của chúng đều chia $2a$ và $2b$, nên $\gcd(a - b, a + b) = 1$. Vì tích của chúng bằng h^2, tồn tại hai số nguyên dương lẻ $u < v$ sao cho

$$a - b = u^2, \qquad a + b = v^2.$$

Đặt $\alpha = (v + u)/2$ và $\beta = (v - u)/2$. Khi đó

$$\alpha\beta = \frac{v^2 - u^2}{4} = \frac{b}{2} = mn, \qquad \alpha^2 + \beta^2 = \frac{v^2 + u^2}{2} = a = m^2 - n^2.$$

Theo Bổ đề 1, ta có thể viết

$$m = pq, \qquad n = rs, \qquad \alpha = pr, \qquad \beta = qs,$$

với $\gcd(p, s) = \gcd(q, r) = 1$. Thay vào đẳng thức $m^2 - n^2 = \alpha^2 + \beta^2$ rồi thu gọn, ta được

$$p^2(q^2 - r^2) = s^2(q^2 + r^2).$$

Vế phải dương nên $q > r$. Vì $\gcd(p, s) = 1$, ta có $s^2 \mid q^2 - r^2$. Do đó tồn tại số nguyên dương k sao cho

$$q^2 - r^2 = ks^2, \qquad q^2 + r^2 = kp^2.$$

Số k chia cả tổng $2q^2$ và hiệu $2r^2$ của hai số $q^2 + r^2,\ q^2 - r^2$. Vì $\gcd(q, r) = 1$, suy ra $k \mid 2$.

Nếu $k = 1$ thì $q^2 + r^2 = p^2$ và $q^2 - r^2 = s^2$, nên (q, r) là một cặp nghiệm mới. Nếu $k = 2$ thì

$$p^2 = \frac{q^2 + r^2}{2}, \qquad s^2 = \frac{q^2 - r^2}{2}.$$

Do đó $p^2 + s^2 = q^2$ và $p^2 - s^2 = r^2$, nên (p, s) là một cặp nghiệm mới. Trong cả hai trường hợp, thành phần thứ nhất của cặp mới đều nhỏ hơn a, vì

$$\max\{p, q\} \leq pq = m < m + n \leq (m - n)(m + n) = a.$$

Điều này mâu thuẫn với cách chọn a. □

Hai phương trình bậc bốn dưới đây có cùng phép rút gọn. Nếu $x^4 \pm y^4 = z^2$ và $d = \gcd(x, y)$ thì $d^4 \mid z^2$, nên $d^2 \mid z$. Do đó $(x/d, y/d, z/d^2)$ cũng là một nghiệm của phương trình với cùng dấu đã chọn.

Hệ quả 2. Phương trình $x^4 + y^4 = z^2$ không có nghiệm nguyên dương.

Chứng minh. Giả sử có nghiệm và chọn một nghiệm (x, y, z) có z nhỏ nhất. Theo phép rút gọn trên, $\gcd(x, y) = 1$. Bộ ba (x^2, y^2, z) nguyên thủy nên sau khi đổi chỗ x, y nếu cần, ta có thể giả sử x lẻ, y chẵn. Theo Định lý 2, tồn tại hai số nguyên $m > n > 0$, nguyên tố cùng nhau, sao cho

$$x^2 = m^2 - n^2, \qquad y^2 = 2mn, \qquad z = m^2 + n^2.$$

Từ $x^2 + n^2 = m^2$ và $\gcd(m, n) = 1$, ta thấy (x, n, m) cũng là một bộ ba Pythagore nguyên thủy. Vì x lẻ nên n chẵn. Áp dụng công thức Euclid cho bộ ba này, ta được hai số nguyên $u > v > 0$, nguyên tố cùng nhau, sao cho

$$x = u^2 - v^2, \qquad n = 2uv, \qquad m = u^2 + v^2.$$

https://nttuan.org/
T's Lab
Nguyễn Trung Tuấn, 0915011235

Thay vào $y^2 = 2mn$, ta được

$$\left(\frac{y}{2}\right)^2 = uvm.$$

Vì $\gcd(u, v) = 1$ và $m = u^2 + v^2$, ba số u, v, m đôi một nguyên tố cùng nhau. Tích của chúng là số chính phương, nên $u = A^2,\ v = B^2,\ m = C^2$ với A, B, C nguyên dương. Khi đó

$$A^4 + B^4 = u^2 + v^2 = m = C^2.$$

Như vậy (A, B, C) là một nghiệm mới, trong khi

$$C \le C^2 = m < m^2 + n^2 = z.$$

Điều này trái với tính nhỏ nhất của z. □

Hệ quả 3. Phương trình $x^4 - y^4 = z^2$ không có nghiệm nguyên dương.

Chứng minh. Giả sử có nghiệm. Sau khi rút gọn, ta có thể chọn một nghiệm (x, y, z) với $\gcd(x, y) = 1$. Đặt

$$A = x^2 - y^2, \qquad B = x^2 + y^2, \qquad g = \gcd(A, B).$$

Ta có $0 < A < B$ và $AB = z^2$. Vì g chia cả $A + B = 2x^2$ và $B - A = 2y^2$, suy ra $g \mid 2$. Mặt khác, $g^2 \mid z^2$ nên $g \mid z$. Hai số $A/g, B/g$ nguyên tố cùng nhau và có tích bằng $(z/g)^2$. Do đó

$$A = gu^2, \qquad B = gv^2$$

với hai số nguyên $0 < u < v$.

Nếu $g = 1$ thì $x^2 + y^2 = v^2$ và $x^2 - y^2 = u^2$, trái với Hệ quả 1. Nếu $g = 2$ thì

$$v^2 + u^2 = \frac{B + A}{2} = x^2, \qquad v^2 - u^2 = \frac{B - A}{2} = y^2.$$

Áp dụng Hệ quả 1 cho cặp (v, u), ta lại được mâu thuẫn. □

Nhận xét. Hệ quả 2 cho ngay định lý cuối cùng của Fermat với số mũ 4. Thật vậy, nếu $x^4 + y^4 = z^4$ với x, y, z nguyên dương thì (x, y, z^2) là một nghiệm nguyên dương của phương trình $X^4 + Y^4 = Z^2$.

https://nttuan.org/
Nguyễn Trung Tuân, 0915011235
T's Lab