Tổng của hai và bốn bình phương

Một số nguyên dương được biểu diễn thành tổng hai bình phương khi nào? Nếu thay hai bình phương bằng bốn bình phương, câu trả lời thay đổi ra sao? Hai câu hỏi gần nhau ấy dẫn đến hai kết quả có bản chất khác biệt: trong trường hợp thứ nhất, các ước nguyên tố đồng dư 3 modulo 4 tạo ra trở ngại; trong trường hợp thứ hai, mọi số nguyên không âm đều biểu diễn được.

Bài viết trình bày các tiêu chuẩn biểu diễn, tính duy nhất trong trường hợp số nguyên tố và điều kiện để hai số trong biểu diễn nguyên tố cùng nhau. Các định lý chính được chứng minh bằng công cụ số học sơ cấp. Bên cạnh phương pháp xuống thang, ta giới thiệu chứng minh tổ hợp của Don Zagier cho định lý hai bình phương và một cách chứng minh định lý bốn bình phương thông qua việc hạ mẫu của biểu diễn hữu tỉ.

1 Các khái niệm và bổ đề cơ sở

Định nghĩa 1. Cho số nguyên tố p và số nguyên $n \neq 0$. Số nguyên không âm lớn nhất k sao cho $p^k \mid n$ được gọi là *số mũ của p trong n*, ký hiệu là $v_p(n)$. Như vậy,

$$v_p(n) = k \quad \Longleftrightarrow \quad p^k \mid n \text{ và } p^{k+1} \nmid n.$$

Với mọi số nguyên $a, b \neq 0$, ta có

$$v_p(ab) = v_p(a) + v_p(b), \qquad v_p(a^2) = 2v_p(a).$$

Định nghĩa 2. Cho số nguyên dương m. Một tập gồm m số nguyên đôi một không đồng dư modulo m được gọi là một *hệ thặng dư đầy đủ modulo m*. Mỗi số nguyên đồng dư với đúng một phần tử của hệ này. Đặc biệt, nếu m lẻ thì

$$-\frac{m-1}{2}, -\frac{m-3}{2}, \ldots, -1, 0, 1, \ldots, \frac{m-1}{2}$$

là một hệ thặng dư đầy đủ; mọi phần tử r trong hệ đều thỏa mãn $|r| < m/2$.

Định nghĩa 3. Cho số nguyên dương k. Một số nguyên không âm n được gọi là *biểu diễn được thành tổng k bình phương* nếu tồn tại $x_1, \ldots, x_k \in \mathbb{Z}$ sao cho

$$n = x_1^2 + \cdots + x_k^2.$$

Các x_i được phép bằng 0. Nếu yêu cầu mọi $x_i \neq 0$, ta nói rõ n là tổng bình phương của k số nguyên khác 0; điều này tương đương với việc n là tổng bình phương của k số nguyên dương.

Ta sử dụng định lý nhỏ Fermat: nếu p là số nguyên tố và $p \nmid a$ thì $a^{p-1} \equiv 1 \pmod p$.

Bổ đề 1 (Định lý Wilson)**.** Với mọi số nguyên tố p, ta có $(p-1)! \equiv -1 \pmod p$.

Chứng minh. Trường hợp $p = 2$ là hiển nhiên. Với p lẻ, mỗi phần tử khác 0 modulo p có duy nhất một nghịch đảo. Một phần tử trùng với nghịch đảo của nó khi và chỉ khi

$$a^2 \equiv 1 \pmod p \quad \Longleftrightarrow \quad a \equiv 1 \text{ hoặc } -1 \pmod p.$$

Vì thế, ngoài 1 và $p-1$, các số $1, 2, \ldots, p-1$ được ghép thành từng cặp có tích đồng dư 1 modulo p. Suy ra

$$(p-1)! \equiv 1 \cdot (p-1) \equiv -1 \pmod p. \qquad \square$$

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

Bổ đề 2. Với số nguyên tố lẻ p, phương trình đồng dư $a^2 \equiv -1 \pmod{p}$ có nghiệm khi và chỉ khi $p \equiv 1 \pmod{4}$.

Chứng minh. Nếu $a^2 \equiv -1 \pmod{p}$ thì $p \nmid a$. Theo định lý nhỏ Fermat,

$$1 \equiv a^{p-1} \equiv (-1)^{(p-1)/2} \pmod{p}.$$

Do p lẻ, số $(p-1)/2$ phải chẵn, tức là $p \equiv 1 \pmod{4}$.
Ngược lại, giả sử $p \equiv 1 \pmod{4}$ và đặt $h = (p-1)/2$. Khi đó h chẵn và theo Bổ đề 1,

$$-1 \equiv (p-1)! = \prod_{j=1}^{h} j(p-j) \equiv (-1)^h (h!)^2 = (h!)^2 \pmod{p}.$$

Vậy $a = h!$ là một nghiệm. □

Bổ đề 3 (Bổ đề Thue)**.** Cho số nguyên dương n và số nguyên a. Tồn tại các số nguyên x, y không đồng thời bằng 0 sao cho

$$|x|, |y| \le \lfloor \sqrt{n} \rfloor, \qquad ax \equiv y \pmod{n}.$$

Chứng minh. Đặt $h = \lfloor \sqrt{n} \rfloor$. Xét $(h+1)^2$ cặp số nguyên (u, v) với $0 \le u, v \le h$ và gán cho mỗi cặp số dư của $au - v$ modulo n. Vì $(h+1)^2 > n$, nguyên lý Dirichlet cho hai cặp phân biệt (u_1, v_1) và (u_2, v_2) có cùng số dư. Khi đó $x = u_1 - u_2$, $y = v_1 - v_2$ thỏa mãn các yêu cầu. □

Bổ đề 4 (Các hằng đẳng thức nhân)**.** Với các biến thực, ta có:

(i) Hằng đẳng thức Brahmagupta–Fibonacci:

$$\begin{aligned}(a^2+b^2)(c^2+d^2) &= (ac-bd)^2 + (ad+bc)^2 \\ &= (ac+bd)^2 + (ad-bc)^2.\end{aligned}$$

(ii) Hằng đẳng thức bốn bình phương Euler:

$$\left(\sum_{i=1}^{4} a_i^2\right)\left(\sum_{i=1}^{4} b_i^2\right) = A^2 + B^2 + C^2 + D^2,$$

trong đó

$$\begin{aligned}A &= a_1b_1 + a_2b_2 + a_3b_3 + a_4b_4, \\ B &= a_1b_2 - a_2b_1 + a_3b_4 - a_4b_3, \\ C &= a_1b_3 - a_3b_1 + a_4b_2 - a_2b_4, \\ D &= a_1b_4 - a_4b_1 + a_2b_3 - a_3b_2.\end{aligned}$$

Chứng minh. Khai triển các vế phải. Các tích chéo triệt tiêu từng đôi một, còn lại lần lượt là các số hạng trong khai triển các vế trái. □

Nhận xét. Tích của hai số biểu diễn được thành tổng hai bình phương vẫn biểu diễn được thành tổng hai bình phương. Điều tương tự đúng với bốn bình phương. Tính chất này cho phép chuyển từ các số nguyên tố sang mọi số nguyên dương.

2 Tổng của hai bình phương

Định lý 1 (Fermat)**.** Một số nguyên tố lẻ p biểu diễn được thành tổng hai bình phương khi và chỉ khi $p \equiv 1 \pmod{4}$. Khi biểu diễn tồn tại, nó là duy nhất nếu không kể thứ tự và dấu của hai số trong biểu diễn.

https://nttuan.org/
Ti's Lab
Nguyễn Trung Tuân, 0915011235

Chứng minh 1 (dùng bổ đề Thue). Nếu $p = x^2 + y^2$ thì, do một số chính phương chỉ đồng dư 0 hoặc 1 modulo 4 và p lẻ, ta có $p \equiv 1 \pmod 4$.

Ngược lại, giả sử $p \equiv 1 \pmod 4$. Theo Bổ đề 2, tồn tại $a \in \mathbb{Z}$ sao cho $a^2 \equiv -1 \pmod p$. Bổ đề 3 cho các số nguyên x, y không đồng thời bằng 0 thỏa mãn $|x|, |y| \le \lfloor \sqrt{p} \rfloor$ và $ax \equiv y \pmod p$. Khi đó

$$x^2 + y^2 \equiv x^2 + (ax)^2 = x^2(1 + a^2) \equiv 0 \pmod p.$$

Vì p không là số chính phương,

$$0 < x^2 + y^2 \le 2\lfloor \sqrt{p} \rfloor^2 < 2p.$$

Do đó $x^2 + y^2 = p$.

Để chứng minh tính duy nhất, giả sử

$$p = a^2 + b^2 = c^2 + d^2, \qquad 0 < a < b, \quad 0 < c < d.$$

Ta có

$$(ac + bd)(ad + bc) = ab(c^2 + d^2) + cd(a^2 + b^2) = p(ab + cd).$$

Suy ra $p \mid ac + bd$ hoặc $p \mid ad + bc$. Mặt khác,

$$p^2 = (ac + bd)^2 + (ad - bc)^2 = (ad + bc)^2 + (ac - bd)^2.$$

Trong khả năng thứ nhất, $0 < ac + bd \le p$ nên $ac + bd = p$ và $ad = bc$; kết hợp với $a^2 + b^2 = c^2 + d^2$, suy ra $(a, b) = (c, d)$. Trong khả năng thứ hai, tương tự ta được $ad + bc = p$, $ac = bd$ và $(a, b) = (d, c)$, trái với $a < b$, $c < d$. Vậy biểu diễn là duy nhất. □

Chứng minh tiếp theo của Don Zagier giải quyết phần tồn tại bằng một phép đếm chẵn lẻ trên tập hữu hạn; tính duy nhất đã được chứng minh ở trên.

Chứng minh 2 (Don Zagier). Một ánh xạ $\varphi : S \to S$ được gọi là *phép đối hợp* nếu $\varphi(\varphi(s)) = s$ với mọi $s \in S$. Phần tử s thỏa mãn $\varphi(s) = s$ được gọi là một *điểm bất động*. Các phần tử không bất động được ghép thành những cặp $\{s, \varphi(s)\}$, nên nếu S hữu hạn thì

$$|S| \equiv |\{s \in S : \varphi(s) = s\}| \pmod 2. \tag{1}$$

Cho $p = 4k + 1$ là số nguyên tố. Xét tập hữu hạn

$$S = \{(x, y, z) \in \mathbb{Z}^3_{>0} : x^2 + 4yz = p\}.$$

Tập này khác rỗng vì $(1, 1, k) \in S$. Ánh xạ $\tau(x, y, z) = (x, z, y)$ là một phép đối hợp trên S. Nếu τ có điểm bất động thì $y = z$, từ đó $p = x^2 + (2y)^2$. Vì vậy, theo (1), chỉ cần chứng minh $|S|$ lẻ.

Để làm điều đó, xét ánh xạ

$$\sigma(x, y, z) = \begin{cases} (x + 2z,\ z,\ y - x - z), & x < y - z, \\ (2y - x,\ y,\ x - y + z), & y - z < x < 2y, \\ (x - 2y,\ x - y + z,\ y), & x > 2y. \end{cases}$$

Hai trường hợp biên không xuất hiện: nếu $x = y - z$ thì $p = (y + z)^2$; nếu $x = 2y$ thì $p = 4y(y + z)$. Cả hai đều trái với tính nguyên tố của p. Do đó công thức trên xác định σ trên toàn bộ S.

Ở mỗi nhánh, ba tọa độ của ảnh đều dương. Các đẳng thức

$$\begin{aligned} (x + 2z)^2 + 4z(y - x - z) &= x^2 + 4yz, \\ (2y - x)^2 + 4y(x - y + z) &= x^2 + 4yz, \\ (x - 2y)^2 + 4y(x - y + z) &= x^2 + 4yz \end{aligned}$$

cho thấy $\sigma(S) \subseteq S$.

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

Ta kiểm tra tính đối hợp. Nếu $x < y - z$ và $(X, Y, Z) = (x + 2z, z, y - x - z)$ thì $X > 2Y$; áp dụng nhánh thứ ba cho (X, Y, Z) thu lại (x, y, z). Ngược lại, nhánh thứ ba đưa một bộ về miền của nhánh thứ nhất và hai công thức cũng khử nhau. Nếu $y - z < x < 2y$ thì ảnh $(X, Y, Z) = (2y - x, y, x - y + z)$ vẫn thỏa mãn $Y - Z < X < 2Y$; áp dụng nhánh thứ hai một lần nữa cũng thu lại (x, y, z). Vậy σ là một phép đối hợp.

Nhánh thứ nhất và thứ ba không có điểm bất động vì tọa độ thứ nhất thay đổi. Ở nhánh thứ hai, điều kiện bất động tương đương với $x = y$. Khi đó

$$p = x^2 + 4xz = x(x + 4z).$$

Tính nguyên tố của p buộc $x = y = 1$, $z = k$. Như vậy, σ có đúng một điểm bất động là $(1, 1, k)$.

Theo (1), $|S|$ lẻ. Bởi vậy τ có ít nhất một điểm bất động và p là tổng hai bình phương. □

Nhận xét. Hai phép đối hợp trong chứng minh Zagier đảm nhiệm hai vai trò khác nhau. Điểm bất động của τ cho ngay biểu diễn cần tìm; điểm bất động của σ lại dễ xác định nhờ tính nguyên tố của p. Công thức (1) nối hai phép đếm ấy với nhau. Với số nguyên tố chẵn, ta có $2 = 1^2 + 1^2$, cũng là biểu diễn duy nhất.

Để chuyển từ số nguyên tố sang số nguyên dương bất kỳ, ta cần xác định vai trò của các số nguyên tố đồng dư 3 modulo 4.

Bổ đề 5. Cho số nguyên tố $q \equiv 3 \pmod 4$ và $x, y \in \mathbb{Z}$. Nếu $q \mid x^2 + y^2$ thì $q \mid x$ và $q \mid y$.

Chứng minh. Nếu $q \nmid y$ thì y có nghịch đảo modulo q. Từ $x^2 + y^2 \equiv 0 \pmod q$, suy ra $(xy^{-1})^2 \equiv -1 \pmod q$, trái với Bổ đề 2. Vậy $q \mid y$, rồi $q \mid x$. □

Định lý 2 (Fermat–Euler)**.** Một số nguyên dương n biểu diễn được thành tổng hai bình phương khi và chỉ khi $v_q(n)$ chẵn với mọi ước nguyên tố $q \equiv 3 \pmod 4$ của n.

Chứng minh. Giả sử $n = x^2 + y^2$. Nếu một trong hai số x, y bằng 0 thì n là số chính phương, nên mọi số mũ trong phân tích nguyên tố của n đều chẵn. Nếu $xy \neq 0$, với mỗi số nguyên tố $q \equiv 3 \pmod 4$, đặt $h = \min\{v_q(x), v_q(y)\}$ và viết $x = q^h u$, $y = q^h v$. Khi đó u, v không đồng thời chia hết cho q. Bổ đề 5 cho $q \nmid u^2 + v^2$, nên từ

$$n = q^{2h}(u^2 + v^2)$$

suy ra $v_q(n) = 2h$ chẵn.

Ngược lại, giả sử các số mũ nêu trong định lý đều chẵn. Tách phần chính phương ra khỏi n, ta viết được

$$n = m^2\, 2^\alpha p_1 \cdots p_s,$$

trong đó $m \geq 1$, $\alpha \in \{0, 1\}$ và $p_1, \ldots, p_s$ là các số nguyên tố phân biệt đồng dư 1 modulo 4; cho phép $s = 0$. Ta có $1 = 1^2 + 0^2$, $2 = 1^2 + 1^2$ và mỗi p_i là tổng hai bình phương theo Định lý 1. Dùng liên tiếp Bổ đề 4(i), rồi nhân hai số trong biểu diễn với m, ta thu được biểu diễn của n. □

Điều kiện để cả hai số trong biểu diễn đều khác 0 được mô tả như sau.

Định lý 3. Một số nguyên dương n là tổng bình phương của hai số nguyên khác 0 khi và chỉ khi hai điều kiện sau đồng thời được thỏa mãn:

(i) $v_q(n)$ chẵn với mọi ước nguyên tố $q \equiv 3 \pmod 4$ của n;

(ii) $v_2(n)$ lẻ hoặc n có một ước nguyên tố $p \equiv 1 \pmod 4$.

Chứng minh. Giả sử $n = x^2 + y^2$ với $xy \neq 0$. Điều kiện (i) suy ra từ Định lý 2. Đặt $d = \gcd(x, y)$, $x = du$, $y = dv$ và $N = u^2 + v^2$, trong đó $\gcd(u, v) = 1$. Vì $uv \neq 0$ nên $N \geq 2$. Theo Bổ đề 5, N không có ước nguyên tố đồng dư 3 modulo 4. Nếu N có ước nguyên tố đồng dư 1 modulo 4 thì n cũng có ước ấy. Nếu không, N là một lũy thừa của 2. Do $\gcd(u, v) = 1$, hai số u, v không cùng chẵn; vì N chẵn nên cả hai cùng lẻ và $N \equiv 2 \pmod 4$. Suy ra $N = 2$ và $v_2(n) = 2v_2(d) + 1$ lẻ. Vậy (ii) luôn đúng.

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

Ngược lại, giả sử (i) và (ii) được thỏa mãn. Theo Định lý 2, n là tổng hai bình phương. Nếu n không là số chính phương thì mọi biểu diễn như vậy đều có hai số khác 0. Nếu $n = m^2$ thì $v_2(n)$ chẵn, nên (ii) cho một ước nguyên tố $p \equiv 1 \pmod 4$ của n; khi đó $p \mid m$. Theo Định lý 1, viết $p = a^2 + b^2$ với $a, b > 0$. Vì p lẻ nên $a \neq b$. Từ

$$p^2 = (a^2 - b^2)^2 + (2ab)^2$$

suy ra

$$n = \left(\frac{m}{p}(a^2 - b^2)\right)^2 + \left(\frac{2mab}{p}\right)^2,$$

là biểu diễn cần tìm. □

Hệ quả 1. Một số nguyên dương n biểu diễn được dưới dạng $n = x^2 + y^2$ với $x, y \in \mathbb{Z}$ và $\gcd(x, y) = 1$ khi và chỉ khi $4 \nmid n$ và n không có ước nguyên tố đồng dư 3 modulo 4.

Chứng minh. Chiều cần suy ra từ Bổ đề 5 và nhận xét rằng $4 \mid x^2 + y^2$ buộc x, y cùng chẵn.

Xét chiều đủ. Trước hết, cho $p \equiv 1 \pmod 4$ là số nguyên tố và viết $p = a^2 + b^2$ với $a, b > 0$. Đặt

$$(x_1, y_1) = (a, b), \qquad x_{k+1} = ax_k - by_k, \quad y_{k+1} = bx_k + ay_k.$$

Hằng đẳng thức nhân cho $x_k^2 + y_k^2 = p^k$. Từ $b^2 \equiv -a^2 \pmod p$, quy nạp theo k còn cho

$$x_k \equiv 2^{k-1}a^k \pmod p, \qquad y_k \equiv 2^{k-1}a^{k-1}b \pmod p.$$

Thật vậy, thay hai đồng dư ở chỉ số k vào công thức truy hồi, ta lần lượt được $x_{k+1} \equiv 2^k a^{k+1}$ và $y_{k+1} \equiv 2^k a^k b \pmod p$. Do p lẻ và $p \nmid a$, suy ra $p \nmid x_k$. Mọi ước nguyên tố chung của x_k, y_k phải chia p^k, nên phải bằng p; do đó $\gcd(x_k, y_k) = 1$.

Tiếp theo, giả sử

$$M = x^2 + y^2, \quad N = u^2 + v^2, \qquad \gcd(x, y) = \gcd(u, v) = \gcd(M, N) = 1.$$

Đặt $A = xu - yv$, $B = xv + yu$. Ta có $A^2 + B^2 = MN$. Nếu số nguyên tố r chia cả A và B thì $r \mid MN$. Do M, N nguyên tố cùng nhau, xét trước khả năng $r \mid M$, $r \nmid N$. Các đẳng thức

$$uA + vB = xN, \qquad uB - vA = yN$$

buộc $r \mid x, y$, vô lý. Khả năng $r \mid N$, $r \nmid M$ cũng bị loại bởi

$$xA + yB = uM, \qquad xB - yA = vM.$$

Vậy $\gcd(A, B) = 1$.

Cuối cùng, số n thỏa mãn giả thiết có dạng

$$n = 2^\alpha \prod_{i=1}^{s} p_i^{\beta_i}, \qquad \alpha \in \{0, 1\}, \quad \beta_i \geq 1,$$

với các $p_i \equiv 1 \pmod 4$ đôi một phân biệt. Mỗi lũy thừa $p_i^{\beta_i}$ có biểu diễn nguyên tố cùng nhau như trên; $2 = 1^2 + 1^2$ cũng có tính chất ấy. Ghép lần lượt các thừa số đôi một nguyên tố cùng nhau, ta được biểu diễn cần tìm. Trường hợp $n = 1$ được xử lý bởi $1 = 1^2 + 0^2$. □

3 Tổng của bốn bình phương

Hằng đẳng thức Euler cho phép quy bài toán về các số nguyên tố. Với một số nguyên tố lẻ p, trước hết ta tìm một bội dương nhỏ của p là tổng bốn bình phương, rồi tìm cách loại bỏ hệ số của bội ấy.

Bổ đề 6. Với mọi số nguyên tố lẻ p, tồn tại các số nguyên x, y và số nguyên dương $m < p$ sao cho $x^2 + y^2 + 1 = mp$.

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

Chứng minh. Xét hai tập số dư modulo p:

$$A = \left\{ x^2 \bmod p : 0 \le x \le \frac{p-1}{2} \right\}, \qquad B = \left\{ -1 - y^2 \bmod p : 0 \le y \le \frac{p-1}{2} \right\}.$$

Nếu $x_1^2 \equiv x_2^2 \pmod p$ với $0 \le x_1, x_2 \le (p-1)/2$ thì $p \mid (x_1 - x_2)(x_1 + x_2)$, suy ra $x_1 = x_2$. Vì vậy $|A| = |B| = (p+1)/2$. Do $|A| + |B| > p$, hai tập này có phần tử chung, tức là tồn tại $0 \le x, y \le (p-1)/2$ sao cho $p \mid x^2 + y^2 + 1$. Mặt khác,

$$0 < x^2 + y^2 + 1 \le \frac{(p-1)^2}{2} + 1 < p^2.$$

Do đó $x^2 + y^2 + 1 = mp$ với $1 \le m < p$. □

Định lý 4. Mọi số nguyên tố đều biểu diễn được thành tổng bốn bình phương.

Chứng minh 1 (xuống thang theo hệ số của bội). Với $p = 2$, ta có $2 = 1^2 + 1^2 + 0^2 + 0^2$. Cho p là số nguyên tố lẻ. Theo Bổ đề 6, tồn tại bội mp với $1 \le m < p$ là tổng bốn bình phương. Chọn m nhỏ nhất có tính chất này và viết

$$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2.$$

Giả sử $m > 1$.

Nếu m chẵn thì trong bốn số x_i có một số chẵn các số lẻ. Sau khi đổi thứ tự, có thể giả sử $x_1 \equiv x_2 \pmod 2$ và $x_3 \equiv x_4 \pmod 2$. Khi đó

$$\frac{m}{2} p = \left(\frac{x_1 + x_2}{2}\right)^2 + \left(\frac{x_1 - x_2}{2}\right)^2 + \left(\frac{x_3 + x_4}{2}\right)^2 + \left(\frac{x_3 - x_4}{2}\right)^2$$

là tổng bốn bình phương nguyên, trái với tính nhỏ nhất của m.

Vậy m lẻ. Chọn các số nguyên y_i sao cho

$$y_i \equiv x_i \pmod m, \qquad |y_i| < \frac{m}{2} \quad (i = 1, 2, 3, 4).$$

Ta có $m \mid \sum y_i^2$, nên $\sum y_i^2 = mr$ với $r \ge 0$. Nếu $r = 0$ thì mọi $y_i = 0$, do đó $m \mid x_i$ với mọi i và $m^2 \mid mp$, suy ra $m \mid p$. Điều này không thể xảy ra vì $1 < m < p$. Mặt khác,

$$mr = \sum_{i=1}^{4} y_i^2 < 4 \left(\frac{m}{2}\right)^2 = m^2.$$

Bởi vậy $1 \le r < m$.

Áp dụng Bổ đề 4(ii) cho hai bộ (x_i) và (y_i), ta được

$$m^2 pr = A^2 + B^2 + C^2 + D^2,$$

trong đó

$$\begin{aligned} A &= x_1 y_1 + x_2 y_2 + x_3 y_3 + x_4 y_4, \\ B &= x_1 y_2 - x_2 y_1 + x_3 y_4 - x_4 y_3, \\ C &= x_1 y_3 - x_3 y_1 + x_4 y_2 - x_2 y_4, \\ D &= x_1 y_4 - x_4 y_1 + x_2 y_3 - x_3 y_2. \end{aligned}$$

Vì $y_i \equiv x_i \pmod m$, ta có

$$A \equiv \sum_{i=1}^{4} x_i^2 = mp \equiv 0 \pmod m, \qquad B \equiv C \equiv D \equiv 0 \pmod m.$$

Chia đẳng thức trên cho m^2, suy ra

$$pr = \left(\frac{A}{m}\right)^2 + \left(\frac{B}{m}\right)^2 + \left(\frac{C}{m}\right)^2 + \left(\frac{D}{m}\right)^2,$$

lại trái với tính nhỏ nhất của m. Do đó $m = 1$. □

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

Một cách chứng minh khác là xây dựng trước một biểu diễn hữu tỉ, rồi chuyển nó thành biểu diễn nguyên. Công cụ cần thiết là bổ đề sau.

Bổ đề 7 (Hạ mẫu cho tổng bốn bình phương)**.** Nếu một số nguyên dương N là tổng bình phương của bốn số hữu tỉ thì N cũng là tổng bình phương của bốn số nguyên.

Chứng minh. Trong các biểu diễn

$$N = \left(\frac{a_1}{q}\right)^2 + \cdots + \left(\frac{a_4}{q}\right)^2, \qquad a_i \in \mathbb{Z}, \quad q \in \mathbb{Z}_{>0},$$

chọn một biểu diễn có mẫu chung q nhỏ nhất. Nếu $q = 1$ thì xong. Giả sử $q > 1$. Với mỗi i, chọn số nguyên b_i gần a_i/q nhất và đặt $c_i = a_i - qb_i$. Khi đó $|c_i| \le q/2$.

Xét trước trường hợp $|c_i| = q/2$ với mọi i. Khi ấy $a_i/q = h_i/2$ với các h_i đều lẻ, và

$$N = \frac{h_1^2 + h_2^2 + h_3^2 + h_4^2}{4}.$$

Đổi dấu một h_i nếu cần, ta có thể giả sử $h_1 + h_2 + h_3 + h_4 \equiv 0 \pmod 4$. Do đó bốn số

$$\frac{h_1 + h_2 + h_3 + h_4}{4}, \quad \frac{h_1 + h_2 - h_3 - h_4}{4}, \quad \frac{h_1 - h_2 + h_3 - h_4}{4}, \quad \frac{h_1 - h_2 - h_3 + h_4}{4}$$

đều nguyên. Tổng bình phương của chúng bằng $(h_1^2 + h_2^2 + h_3^2 + h_4^2)/4 = N$, nên đã có biểu diễn cần tìm.

Bây giờ giả sử ít nhất một bất đẳng thức $|c_i| \le q/2$ là nghiêm. Không thể có mọi $c_i = 0$, vì khi đó $N = \sum b_i^2$, trái với tính nhỏ nhất của $q > 1$. Mặt khác,

$$\sum_{i=1}^4 c_i^2 \equiv \sum_{i=1}^4 a_i^2 = Nq^2 \equiv 0 \pmod q, \qquad 0 < \sum_{i=1}^4 c_i^2 < q^2.$$

Vì thế có số nguyên r thỏa mãn

$$\sum_{i=1}^4 c_i^2 = qr, \qquad 1 \le r < q.$$

Đặt $k = N - \sum b_i^2 \in \mathbb{Z}$. Thay $a_i = qb_i + c_i$ vào $\sum a_i^2 = Nq^2$ và rút gọn, ta được

$$qk = 2\sum_{i=1}^4 b_i c_i + r. \tag{2}$$

Để bảo toàn tổng bình phương, xét phương trình $\sum (b_i + tc_i)^2 = N$ theo t. Phương trình này đã có nghiệm $t = 1/q$; theo hệ thức Viète, nghiệm còn lại là $t = -k/r$. Vì vậy, đặt $y_i = b_i - (k/r)c_i$. Dùng (2), ta có

$$\begin{aligned}\sum_{i=1}^4 y_i^2 &= \sum_{i=1}^4 b_i^2 - \frac{2k}{r}\sum_{i=1}^4 b_i c_i + \frac{k^2}{r^2}\sum_{i=1}^4 c_i^2 \\ &= \sum_{i=1}^4 b_i^2 + \frac{k}{r}\left(qk - 2\sum_{i=1}^4 b_i c_i\right) \\ &= \sum_{i=1}^4 b_i^2 + k = N.\end{aligned}$$

Đây là một biểu diễn hữu tỉ của N với mẫu chung $r < q$, mâu thuẫn. Bổ đề được chứng minh. □

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

Chứng minh 2 của Định lý 4 (dùng hạ mẫu). Giả sử có số nguyên tố không biểu diễn được thành tổng bốn bình phương và chọn p là số nhỏ nhất như vậy. Vì $2 = 1^2 + 1^2 + 0^2 + 0^2$, ta có p lẻ.

Theo Bổ đề 6, tồn tại $1 \le m < p$ sao cho mp là tổng bốn bình phương. Mọi ước nguyên tố của m đều nhỏ hơn p, nên theo cách chọn p, mỗi ước ấy là tổng bốn bình phương. Bổ đề 4(ii) cho thấy m cũng là tổng bốn bình phương; nếu $m = 1$ thì dùng $1 = 1^2 + 0^2 + 0^2 + 0^2$.

Áp dụng tiếp hằng đẳng thức Euler cho mp và m, ta được

$$m^2 p = A^2 + B^2 + C^2 + D^2$$

với $A, B, C, D \in \mathbb{Z}$. Suy ra

$$p = \left(\frac{A}{m}\right)^2 + \left(\frac{B}{m}\right)^2 + \left(\frac{C}{m}\right)^2 + \left(\frac{D}{m}\right)^2.$$

Theo Bổ đề 7, p là tổng bốn bình phương nguyên, trái với cách chọn p. □

Nhận xét. Chứng minh thứ nhất giảm hệ số m trong biểu diễn của mp. Chứng minh thứ hai giảm mẫu chung của một biểu diễn hữu tỉ. Điểm cần chú ý ở bổ đề hạ mẫu là dấu nghiêm $\sum c_i^2 < q^2$: khi cả bốn sai số làm tròn cùng có trị tuyệt đối bằng $1/2$, phải dùng phép đổi biến riêng đã nêu trong chứng minh.

Định lý 5 (Bốn bình phương Lagrange)**.** Mọi số nguyên không âm n đều biểu diễn được dưới dạng

$$n = a^2 + b^2 + c^2 + d^2, \qquad a, b, c, d \in \mathbb{Z}.$$

Chứng minh. Ta có $0 = 0^2 + 0^2 + 0^2 + 0^2$ và $1 = 1^2 + 0^2 + 0^2 + 0^2$. Với $n \ge 2$, phân tích $n = p_1 \cdots p_s$ thành tích các số nguyên tố, cho phép các thừa số lặp lại. Theo Định lý 4, mỗi p_i là tổng bốn bình phương. Dùng liên tiếp hằng đẳng thức Euler, suy ra n cũng có tính chất ấy. □

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

Tài liệu tham khảo

[1] D. Zagier, *A One-Sentence Proof That Every Prime $p \equiv 1 \pmod 4$ Is a Sum of Two Squares*, The American Mathematical Monthly **97** (1990), no. 2, p. 144. doi:10.2307/2323918.

[2] E. Dubouis, kết quả về biểu diễn thành tổng các bình phương khác 0 (1911); xem phát biểu trong P. S. Park, *Multiplicative Functions Which Are Additive on Sums of Two Nonzero Squares*, Integers **22** (2022), Paper A87, Lemma 1. `https://math.colgate.edu/~integers/w87/w87.pdf`.

https://nttuan.org/

T's Lab

Nguyễn Trung Tuân, 0915011235