Phương trình Pell dương và phương trình Pell âm

Sự tồn tại nghiệm, cấu trúc nghiệm và tính chia hết

Trong toàn bài, D là một số nguyên dương không phải số chính phương; đặc biệt $D \geq 2$. Ta khảo sát phương trình Pell

$$x^2 - Dy^2 = 1 \tag{1}$$

và phương trình Pell âm

$$x^2 - Dy^2 = -1. \tag{2}$$

Mọi nghiệm đều được hiểu là nghiệm nguyên. Nghiệm dương là nghiệm có cả hai tọa độ dương. Hệ số D được phép có ước chính phương lớn hơn 1.

Bài viết trình bày một chứng minh sơ cấp về sự tồn tại nghiệm của (1), mô tả đầy đủ các nghiệm của hai phương trình và khai thác những tính chất số học của dãy nghiệm. Các tài liệu [1, 2, 3] cung cấp thêm nhiều ví dụ và cách tiếp cận.

1 Liên hợp, chuẩn và phép nhân nghiệm

Đặt $\mathbb{Z}[\sqrt{D}] = \{x + y\sqrt{D} : x, y \in \mathbb{Z}\}$. Do $\sqrt{D}$ vô tỉ, phần tử $x + y\sqrt{D}$ xác định duy nhất cặp (x, y). Với $\alpha = x + y\sqrt{D}$, ta gọi

$$\overline{\alpha} = x - y\sqrt{D}, \qquad \mathcal{N}(\alpha) = \alpha\overline{\alpha} = x^2 - Dy^2$$

lần lượt là liên hợp và chuẩn của α. Kiểm tra trực tiếp cho

$$\overline{\alpha\beta} = \overline{\alpha}\,\overline{\beta}, \qquad \mathcal{N}(\alpha\beta) = \mathcal{N}(\alpha)\mathcal{N}(\beta).$$

Vì vậy, nhân hai phần tử có chuẩn 1 vẫn cho một phần tử có chuẩn 1; nhân hai phần tử có chuẩn -1 cho một phần tử có chuẩn 1.

Viết cụ thể, nếu $x^2 - Dy^2 = N$ và $u^2 - Dv^2 = 1$ thì

$$(ux + Dvy)^2 - D(vx + uy)^2 = N.$$

Phép nhân này là cơ sở để sinh nghiệm mới từ nghiệm đã biết.

2 Sự tồn tại nghiệm dương

Phương trình (1) có hai nghiệm tầm thường $(\pm 1, 0)$. Để chứng minh luôn có nghiệm dương, ta bắt đầu bằng một hệ quả của nguyên lý Dirichlet. Với $t \in \mathbb{R}$, ký hiệu $\{t\} = t - \lfloor t \rfloor$ là phần lẻ của t.

Bổ đề 1 (Xấp xỉ Dirichlet)**.** Nếu $\theta > 0$ vô tỉ thì có vô hạn cặp $(p, q) \in \mathbb{Z} \times \mathbb{Z}_{>0}$ thỏa mãn

$$|p - q\theta| < \frac{1}{q}.$$

Chứng minh. Với mỗi $M \in \mathbb{Z}_{>0}$, chia $[0, 1)$ thành M nửa khoảng $[i/M, (i+1)/M)$, $0 \leq i < M$. Trong $M + 1$ số

$$\{0\theta\}, \{1\theta\}, \ldots, \{M\theta\},$$

có hai số $\{a\theta\}$, $\{b\theta\}$ cùng thuộc một nửa khoảng, với $0 \leq a < b \leq M$. Đặt

$$q = b - a, \qquad p = \lfloor b\theta \rfloor - \lfloor a\theta \rfloor.$$

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

Khi đó $1 \le q \le M$ và

$$|p - q\theta| = |\{b\theta\} - \{a\theta\}| < \frac{1}{M} \le \frac{1}{q}.$$

Nếu chỉ có hữu hạn cặp thỏa mãn yêu cầu thì các sai số $|p - q\theta|$ của chúng có một giá trị nhỏ nhất $c > 0$, do θ vô tỉ. Chọn M sao cho $1/M < c$; lập luận trên cho một cặp có sai số nhỏ hơn c, mâu thuẫn. □

Định lý 1 (Lagrange)**.** Với mọi số nguyên dương D không chính phương, phương trình $x^2 - Dy^2 = 1$ có nghiệm dương.

Chứng minh. Áp dụng Bổ đề 1 với $\theta = \sqrt{D}$, ta được vô hạn cặp (x, y), $y \ge 1$, sao cho $|x - y\sqrt{D}| < 1/y$. Với mỗi cặp, $x > \sqrt{D} - 1 > 0$ và

$$0 < |x^2 - Dy^2| < \frac{1}{y}\left(2y\sqrt{D} + \frac{1}{y}\right) \le 2\sqrt{D} + 1.$$

Vì $x^2 - Dy^2$ là số nguyên khác 0 và bị chặn, tồn tại một số nguyên $c \ne 0$ sao cho $x^2 - Dy^2 = c$ có vô hạn nghiệm dương.

Chỉ có $|c|^2$ cặp số dư của (x, y) modulo $|c|$. Do đó có hai nghiệm dương phân biệt (x_1', y_1'), (x_2', y_2') thỏa mãn

$$x_1' \equiv x_2' \pmod{|c|}, \qquad y_1' \equiv y_2' \pmod{|c|}.$$

Đổi thứ tự nếu cần để $x_1' + y_1'\sqrt{D} > x_2' + y_2'\sqrt{D}$. Xét

$$t = \frac{x_1' + y_1'\sqrt{D}}{x_2' + y_2'\sqrt{D}} = \frac{x_1'x_2' - Dy_1'y_2'}{c} + \frac{y_1'x_2' - x_1'y_2'}{c}\sqrt{D}.$$

Hai hệ số ở vế phải là số nguyên: theo các đồng dư vừa chọn, tử số thứ nhất đồng dư $x_2'^2 - Dy_2'^2 = c$ modulo $|c|$, còn tử số thứ hai đồng dư 0.

Viết $t = u + v\sqrt{D}$. Ta có $\mathcal{N}(t) = 1$, $t > 1$, nên

$$u = \frac{t + t^{-1}}{2} > 0, \qquad v = \frac{t - t^{-1}}{2\sqrt{D}} > 0.$$

Vậy (u, v) là nghiệm dương cần tìm. □

Nhận xét. Ý tưởng của chứng minh là tìm vô hạn nghiệm cho một vế phải nhỏ c, rồi chia hai nghiệm có cùng cặp số dư modulo $|c|$. Phép chia giữ các hệ số nguyên và đưa chuẩn từ c về 1. Hai lần dùng nguyên lý Dirichlet lần lượt cố định chuẩn và cố định cặp số dư.

3 Nghiệm cơ bản và cấu trúc tập nghiệm

Định nghĩa 1. Nghiệm dương (x_1, y_1) của (1) có x_1 nhỏ nhất được gọi là nghiệm cơ bản. Đặt

$$\varepsilon = x_1 + y_1\sqrt{D} > 1.$$

Do $x = \sqrt{1 + Dy^2}$, việc tối thiểu hóa x, y hay $x + y\sqrt{D}$ trên các nghiệm dương là tương đương. Ngoài ra, $\varepsilon^{-1} = x_1 - y_1\sqrt{D} \in \mathbb{Z}[\sqrt{D}]$.

Định lý 2 (Cấu trúc nghiệm Pell)**.** Mọi nghiệm của $x^2 - Dy^2 = 1$ có biểu diễn duy nhất

$$x + y\sqrt{D} = \pm\varepsilon^n, \qquad n \in \mathbb{Z}.$$

Dấu cộng tương ứng với $x > 0$. Các nghiệm dương tương ứng chính xác với dấu cộng và $n \ge 1$.

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

Chứng minh. Các số $\pm\varepsilon^n$, $n \in \mathbb{Z}$, đều thuộc $\mathbb{Z}[\sqrt{D}]$ và có chuẩn 1, nên đều cho nghiệm.

Ngược lại, từ $x^2 = 1 + Dy^2$ suy ra $|x| > |y|\sqrt{D}$, nên $x + y\sqrt{D}$ cùng dấu với x. Sau khi đổi dấu đồng thời hai tọa độ, chỉ cần xét $t = x + y\sqrt{D} > 0$. Chọn $n \in \mathbb{Z}$ sao cho $\varepsilon^n \le t < \varepsilon^{n+1}$. Khi đó

$$\beta = t\varepsilon^{-n} = u + v\sqrt{D} \in \mathbb{Z}[\sqrt{D}], \qquad 1 \le \beta < \varepsilon, \qquad \mathcal{N}(\beta) = 1.$$

Nếu $\beta > 1$ thì

$$u = \frac{\beta + \beta^{-1}}{2} > 0, \qquad v = \frac{\beta - \beta^{-1}}{2\sqrt{D}} > 0,$$

trái với tính nhỏ nhất của ε. Vậy $\beta = 1$, tức $t = \varepsilon^n$.

Dấu trong biểu diễn được xác định bởi dấu của $x + y\sqrt{D}$, còn số mũ được xác định duy nhất vì $\varepsilon > 1$. Với dấu cộng, $2y\sqrt{D} = \varepsilon^n - \varepsilon^{-n}$, nên $y > 0$ khi và chỉ khi $n \ge 1$. □

Từ đây, ta dùng ký hiệu

$$x_n + y_n\sqrt{D} = \varepsilon^n, \qquad n \in \mathbb{Z}. \tag{3}$$

Khi đó $x_0 = 1$, $y_0 = 0$, $x_{-n} = x_n$, $y_{-n} = -y_n$ và

$$x_n = \frac{\varepsilon^n + \varepsilon^{-n}}{2}, \qquad y_n = \frac{\varepsilon^n - \varepsilon^{-n}}{2\sqrt{D}}. \tag{4}$$

Cả hai dãy $(x_n)_{n\ge0}$ và $(y_n)_{n\ge0}$ đều tăng ngặt. Vì vậy, (x_n, y_n), $n \ge 1$, chính là dãy nghiệm dương được sắp theo thứ tự tăng của từng tọa độ.

3.1 Các công thức truy hồi

Định lý 3. Với mọi $m, n \in \mathbb{Z}$, ta có

$$x_{m+n} = x_m x_n + D y_m y_n, \qquad y_{m+n} = x_m y_n + y_m x_n, \tag{5}$$
$$x_{n+1} = x_1 x_n + D y_1 y_n, \qquad y_{n+1} = y_1 x_n + x_1 y_n, \tag{6}$$
$$x_{n+1} = 2x_1 x_n - x_{n-1}, \qquad y_{n+1} = 2x_1 y_n - y_{n-1}. \tag{7}$$

Đặc biệt,

$$x_{2n} = 2x_n^2 - 1 = 2Dy_n^2 + 1, \qquad y_{2n} = 2x_n y_n, \tag{8}$$
$$x_{3n} = 4x_n^3 - 3x_n, \qquad y_{3n} = (4Dy_n^2 + 3)y_n. \tag{9}$$

Chứng minh. Khai triển $\varepsilon^{m+n} = \varepsilon^m\varepsilon^n$ và so sánh hai hệ số cho (5); lấy $m = 1$ cho (6). Từ $\varepsilon + \varepsilon^{-1} = 2x_1$, nhân với ε^n cho (7). Các công thức nhân đôi và nhân ba suy ra bằng cách khai triển $(x_n + y_n\sqrt{D})^2$, $(x_n + y_n\sqrt{D})^3$ và dùng $x_n^2 - Dy_n^2 = 1$. □

3.2 Tính chia hết của hai dãy tọa độ

Định lý 4. Với mọi $m, n \in \mathbb{Z}_{>0}$, ta có:

a) $\gcd(x_n, y_n) = \gcd(x_n, D) = 1$;

b) $\gcd(y_m, y_n) = y_{\gcd(m,n)}$, và do đó

$$y_m \mid y_n \iff m \mid n;$$

c)

$$x_m \mid x_n \iff m \mid n \text{ và } n/m \text{ lẻ}.$$

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

Chứng minh. a) Cả hai đẳng thức suy ra trực tiếp từ $x_n^2 - Dy_n^2 = 1$.

b) Khai triển $(x_m + y_m\sqrt{D})^k$, $k \geq 1$, cho thấy hệ số của $\sqrt{D}$ luôn chia hết cho y_m. Vì vậy $y_m \mid y_{km}$; điều này cũng đúng với $k = 0$ do $y_0 = 0$.

Do tính đối xứng, giả sử $n \geq m$ và viết $n = qm + r$, $0 \leq r < m$. Theo (5),

$$y_n = x_{qm}y_r + y_{qm}x_r \equiv x_{qm}y_r \pmod{y_m}.$$

Vì $y_m \mid y_{qm}$ và $\gcd(x_{qm}, y_{qm}) = 1$, ta có $\gcd(x_{qm}, y_m) = 1$. Suy ra

$$\gcd(y_n, y_m) = \gcd(y_r, y_m).$$

Lặp lại theo thuật toán Euclid cho cặp chỉ số (m, n), ta được $\gcd(y_m, y_n) = y_{\gcd(m,n)}$. Tính tăng ngặt của dãy (y_n) cho phép tương đương về chia hết trong phát biểu.

c) Nếu $n = (2q + 1)m$, $q \geq 0$, phần hữu tỉ của $(x_m + y_m\sqrt{D})^{2q+1}$ gồm những số hạng có số mũ của x_m là số lẻ dương. Do đó $x_m \mid x_n$.

Ngược lại, giả sử $x_m \mid x_n$. Từ $\varepsilon^{k+2m} + \varepsilon^k = 2x_m\varepsilon^{k+m}$, ta có

$$x_{k+2m} \equiv -x_k \pmod{x_m} \qquad (k \in \mathbb{Z}). \tag{10}$$

Viết $n = 2qm + r$, $0 \leq r < 2m$. Đồng dư trên cho $x_m \mid x_r$. Nếu $r < m$ thì $0 < x_r < x_m$, vô lý. Nếu $m < r < 2m$, đặt $s = 2m - r \in \{1, \ldots, m - 1\}$; do $x_{-s} = x_s$, ta có $x_r \equiv -x_s \pmod{x_m}$, cũng vô lý vì $0 < x_s < x_m$. Vậy $r = m$, tức $n = (2q + 1)m$. □

Hệ quả 1. Nếu x_n là số nguyên tố thì n là một lũy thừa của 2, kể cả $n = 1 = 2^0$.

Chứng minh. Nếu n có một ước nguyên tố lẻ p, đặt $m = n/p < n$. Định lý 4c) cho $x_m \mid x_n$, trong khi $1 < x_m < x_n$, mâu thuẫn. □

Nhận xét. Hai tọa độ có quy luật chia hết khác nhau: với y_n, chỉ cần chỉ số chia hết; với x_n, thương hai chỉ số còn phải lẻ. Điều kiện ở Hệ quả 1 chỉ là điều kiện cần. Chẳng hạn với $D = 3$, $x_8 = 18817 = 31 \cdot 607$ là hợp số.

4 Phương trình Pell âm

Phương trình (2) có thể vô nghiệm. Chẳng hạn, với $D = 3$, xét modulo 3 cho $x^2 \equiv -1 \pmod 3$, vô lý. Khi có nghiệm, cấu trúc nghiệm của nó được xác định bởi cùng phần tử ε của phương trình Pell dương.

Định lý 5. Giả sử $x^2 - Dy^2 = -1$ có nghiệm. Gọi (a_1, b_1) là nghiệm dương nhỏ nhất và đặt $\eta = a_1 + b_1\sqrt{D}$. Khi đó:

a) $\eta^2 = \varepsilon$, hay
$$x_1 = 2a_1^2 + 1 = 2Db_1^2 - 1, \qquad y_1 = 2a_1b_1;$$

b) mọi nghiệm của (2) có biểu diễn duy nhất
$$x + y\sqrt{D} = \pm\eta^{2k+1}, \qquad k \in \mathbb{Z};$$
các nghiệm dương ứng với dấu cộng và $k \geq 0$;

c) toàn bộ nghiệm của hai phương trình $x^2 - Dy^2 = \pm 1$ gộp thành
$$x + y\sqrt{D} = \pm\eta^n, \qquad n \in \mathbb{Z}.$$
Vế phải của phương trình là 1 khi n chẵn, là -1 khi n lẻ.

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

Chứng minh. Một nghiệm của (2) không thể có tọa độ nào bằng 0, nên đổi dấu độc lập hai tọa độ cho một nghiệm dương. Trên các nghiệm dương, $x = \sqrt{Dy^2 - 1}$ tăng theo y, nên tồn tại nghiệm nhỏ nhất (a_1, b_1).

a) Phần tử η^2 có chuẩn 1 và lớn hơn 1, nên $\eta^2 = \varepsilon^m$ với một $m \geq 1$. Nếu $m = 2r$ thì $\eta = \varepsilon^r$, mâu thuẫn về chuẩn. Nếu $m \geq 3$ lẻ thì

$$\eta' = \eta\varepsilon^{-1} \in \mathbb{Z}[\sqrt{D}], \qquad \mathcal{N}(\eta') = -1, \qquad 1 < \eta' < \eta.$$

Viết $\eta' = a' + b'\sqrt{D}$, ta có

$$a' = \frac{\eta' - \eta'^{-1}}{2} > 0, \qquad b' = \frac{\eta' + \eta'^{-1}}{2\sqrt{D}} > 0,$$

trái với tính nhỏ nhất của η. Do đó $m = 1$. Khai triển η^2 cho các đẳng thức tọa độ.

b) Ta có $\eta^{-1} = -\overline{\eta} \in \mathbb{Z}[\sqrt{D}]$, nên mọi số $\pm\eta^{2k+1}$ đều có hệ số nguyên và chuẩn -1. Ngược lại, với một nghiệm $\alpha = x + y\sqrt{D}$, đổi dấu đồng thời nếu cần để $\alpha > 0$. Khi đó

$$\frac{\alpha}{\eta} = -\alpha\overline{\eta} \in \mathbb{Z}[\sqrt{D}]$$

là số dương có chuẩn 1. Vì vậy $\alpha/\eta = \varepsilon^k$, hay $\alpha = \eta^{2k+1}$. Tính duy nhất suy ra từ $\eta > 1$. Với $t = \eta^{2k+1}$, hai tọa độ là

$$x = \frac{t - t^{-1}}{2}, \qquad y = \frac{t + t^{-1}}{2\sqrt{D}}.$$

Do đó cả hai dương khi và chỉ khi $k \geq 0$.

c) Suy ra từ $\varepsilon = \eta^2$ và cấu trúc nghiệm đã chứng minh. □

Hệ quả 2. Phương trình $x^2 - Dy^2 = -1$ có nghiệm khi và chỉ khi

$$\frac{x_1 - 1}{2}, \qquad \frac{x_1 + 1}{2D}$$

đều là bình phương của các số nguyên dương. Khi ấy hai căn bậc hai tương ứng là a_1, b_1.

Chứng minh. Chiều cần là Định lý 5a). Ngược lại, nếu hai số trên là a^2, b^2 thì $Db^2 - a^2 = 1$ và $(a + b\sqrt{D})^2 = \varepsilon$; suy ra (a, b) là nghiệm dương nhỏ nhất của phương trình Pell âm. □

Nhận xét. Hệ quả trên chỉ đòi hỏi kiểm tra hai số sau khi đã biết nghiệm cơ bản của phương trình Pell dương. Một điều kiện loại nhanh là

$$x_1 < 2D - 1 \quad \Longrightarrow \quad x^2 - Dy^2 = -1 \text{ vô nghiệm},$$

vì nếu có nghiệm thì $x_1 = 2Db_1^2 - 1 \geq 2D - 1$.

5 Tìm nghiệm cơ bản và các ví dụ tính toán

5.1 Liên phân số của căn bậc hai

Định lý Lagrange bảo đảm rằng việc thử lần lượt $y = 1, 2, \ldots$ để tìm $Dy^2 + 1$ chính phương sẽ kết thúc. Tuy nhiên, nghiệm đầu tiên có thể lớn. Liên phân số cho một cách tính có hệ thống. Ta dùng kết quả kinh điển sau; xem [1, 4].

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

Định lý 6. Viết liên phân số đơn của $\sqrt{D}$ dưới dạng

$$\sqrt{D} = [c_0; \overline{c_1, \ldots, c_\ell}],$$

với ℓ là độ dài chu kỳ ngắn nhất. Gọi $p_j/q_j = [c_0; c_1, \ldots, c_j]$ là các phân số hội tụ. Khi đó

$$(x_1, y_1) = \begin{cases} (p_{\ell-1}, q_{\ell-1}), & \ell \text{ chẵn}, \\ (p_{2\ell-1}, q_{2\ell-1}), & \ell \text{ lẻ}. \end{cases}$$

Phương trình Pell âm có nghiệm khi và chỉ khi ℓ lẻ; khi ấy (a_1, b_1) trong Định lý 5 được xác định bởi $(p_{\ell-1}, q_{\ell-1})$.

Các phân số hội tụ được tính từ

$$p_j = c_j p_{j-1} + p_{j-2}, \qquad q_j = c_j q_{j-1} + q_{j-2}, \qquad j \geq 0,$$

với $p_{-2} = 0$, $p_{-1} = 1$, $q_{-2} = 1$, $q_{-1} = 0$. Để tìm các thương riêng, đặt $m_0 = 0$, $d_0 = 1$, $c_0 = \lfloor \sqrt{D} \rfloor$ và dùng

$$m_{j+1} = d_j c_j - m_j, \qquad d_{j+1} = \frac{D - m_{j+1}^2}{d_j}, \qquad c_{j+1} = \left\lfloor \frac{c_0 + m_{j+1}}{d_{j+1}} \right\rfloor.$$

Chu kỳ kết thúc ở chỉ số $\ell \geq 1$ đầu tiên có $m_\ell = c_0$, $d_\ell = 1$; khi đó $c_\ell = 2c_0$.

5.2 Tính nghiệm bằng truy hồi

Ví dụ 1. Giải hai phương trình $x^2 - 2y^2 = 1$ và $x^2 - 2y^2 = -1$.

Lời giải. Phương trình Pell dương có nghiệm cơ bản $(3, 2)$: $y = 1$ cho $x^2 = 3$, còn $y = 2$ cho $x^2 = 9$. Phương trình Pell âm có nghiệm dương nhỏ nhất $(1, 1)$. Do đó

$$\eta = 1 + \sqrt{2}, \qquad \varepsilon = \eta^2 = 3 + 2\sqrt{2}.$$

Toàn bộ nghiệm nguyên lần lượt là

$$x + y\sqrt{2} = \pm(3 + 2\sqrt{2})^n \quad (n \in \mathbb{Z}),$$

và

$$x + y\sqrt{2} = \pm(1 + \sqrt{2})^{2k+1} \quad (k \in \mathbb{Z}).$$

Với nghiệm dương, lấy dấu cộng và lần lượt $n \geq 1$, $k \geq 0$. Nhân với $3 + 2\sqrt{2}$ cho truy hồi chung

$$x' = 3x + 4y, \qquad y' = 2x + 3y.$$

Một vài nghiệm dương đầu tiên là

Vế phải	Nghiệm thứ nhất	Nghiệm thứ hai	Nghiệm thứ ba	Nghiệm thứ tư
1	$(3, 2)$	$(17, 12)$	$(99, 70)$	$(577, 408)$
-1	$(1, 1)$	$(7, 5)$	$(41, 29)$	$(239, 169)$

□

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

5.3 Nghiệm cơ bản lớn và chu kỳ lẻ

Ví dụ 2. Tìm nghiệm cơ bản của $x^2 - 29y^2 = 1$ và giải $x^2 - 29y^2 = -1$.

Lời giải. Thuật toán liên phân số cho $\sqrt{29} = [5; \overline{2, 1, 1, 2, 10}]$, có chu kỳ dài 5. Các phân số hội tụ trước khi kết thúc chu kỳ đầu là

j	0	1	2	3	4
p_j	5	11	16	27	70
q_j	1	2	3	5	13
$p_j^2 - 29q_j^2$	-4	5	-5	4	-1

Theo Định lý 6, nghiệm dương nhỏ nhất của phương trình Pell âm là $(70, 13)$. Bình phương cho

$$(70 + 13\sqrt{29})^2 = 9801 + 1820\sqrt{29}.$$

Vậy nghiệm cơ bản của phương trình Pell dương là $(9801, 1820)$. Toàn bộ nghiệm của phương trình Pell âm được cho bởi

$$x + y\sqrt{29} = \pm(70 + 13\sqrt{29})^{2k+1}, \qquad k \in \mathbb{Z}.$$

Đối với phương trình Pell dương, công thức tương ứng là

$$x + y\sqrt{29} = \pm(9801 + 1820\sqrt{29})^n, \qquad n \in \mathbb{Z}.$$

□

6 Một số điều kiện số học cho phương trình Pell âm

Tiêu chuẩn liên phân số quyết định được sự tồn tại nghiệm với mỗi D. Trong nhiều bài toán, có thể kết luận nhanh hơn bằng tính chẵn lẻ, thặng dư bậc hai hoặc phân tích hai thừa số nguyên tố cùng nhau.

Với số nguyên tố lẻ p và số nguyên a, ký hiệu Legendre được định nghĩa bởi

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & p \mid a, \\ 1, & p \nmid a \text{ và } a \text{ là thặng dư bậc hai modulo } p, \\ -1, & \text{các trường hợp còn lại.} \end{cases}$$

Ta dùng tính nhân của ký hiệu Legendre cùng các công thức cổ điển

$$a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p} \quad (p \nmid a), \qquad \left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}, \qquad \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

Định lý 7. a) Nếu $x^2 - Dy^2 = -1$ có nghiệm thì $4 \nmid D$ và D không có ước nguyên tố đồng dư 3 modulo 4.

b) Phương trình có nghiệm nếu $D = 2$, hoặc $D = p^{2r+1}$ với p nguyên tố, $p \equiv 1 \pmod 4$ và $r \in \mathbb{Z}_{\geq 0}$.

c) Phương trình có nghiệm nếu $D = 2p$, trong đó p nguyên tố và $p \equiv 5 \pmod 8$.

Chứng minh. a) Nếu $4 \mid D$ thì $x^2 \equiv -1 \pmod 4$, vô lý. Nếu một số nguyên tố lẻ $q \mid D$ thì $x^2 \equiv -1 \pmod q$, nên $q \equiv 1 \pmod 4$.

b) Với $D = 2$, ta có nghiệm $(1, 1)$. Xét $D = p^{2r+1}$ như trong phát biểu. Vì $D \equiv 1 \pmod 4$, phương trình $x_1^2 - Dy_1^2 = 1$ buộc x_1 lẻ, $y_1 = 2w$ chẵn. Do đó

$$A = \frac{x_1 - 1}{2}, \qquad B = \frac{x_1 + 1}{2}$$

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

là hai số nguyên dương liên tiếp, nguyên tố cùng nhau và $AB = Dw^2$. Mọi số nguyên tố khác p xuất hiện với số mũ chẵn, còn số mũ của p là lẻ. Bởi vậy

$$(A, B) = (Da^2, b^2) \quad \text{hoặc} \quad (b^2, Da^2)$$

với $a, b \in \mathbb{Z}_{>0}$. Khả năng đầu cho $b^2 - Da^2 = 1$ với $0 < b < x_1$, trái với tính cơ bản của (x_1, y_1). Khả năng còn lại cho $b^2 - Da^2 = -1$.

c) Với $D = 2p$, phương trình Pell dương buộc x_1 lẻ. Do $8 \mid x_1^2 - 1 = 2py_1^2$, ta có $y_1 = 2w$. Đặt A, B như trên; khi đó $AB = 2pw^2$, $\gcd(A, B) = 1$ và $B - A = 1$. Vì A, B nguyên tố cùng nhau, sau khi tách các thừa số chính phương, hai thừa số $2, p$ chỉ có thể phân bố theo bốn cách:

$$(A, B) \in \{(2pa^2, b^2), (b^2, 2pa^2), (pa^2, 2b^2), (2b^2, pa^2)\}.$$

Cách thứ nhất cho một nghiệm dương nhỏ hơn của phương trình Pell dương, nên bị loại. Cách thứ hai cho $b^2 - 2pa^2 = -1$, đúng yêu cầu. Hai cách cuối cho $2b^2 \equiv 1 \pmod p$ hoặc $-2b^2 \equiv 1 \pmod p$, đều không thể vì

$$\left(\frac{2}{p}\right) = \left(\frac{-2}{p}\right) = -1 \qquad (p \equiv 5 \pmod 8).$$

□

Ví dụ 3 (Điều kiện cần chưa đủ)**.** Chứng minh rằng $x^2 - 34y^2 = -1$ vô nghiệm nguyên.

Lời giải. Số $34 = 2 \cdot 17$ thỏa mãn điều kiện cần trong Định lý 7a). Tuy nhiên, thử $y = 1, 2, 3, 4, 5$ cho $34y^2 + 1$ lần lượt bằng $35, 137, 307, 545, 851$, đều không chính phương; còn $34 \cdot 6^2 + 1 = 35^2$. Vậy $(x_1, y_1) = (35, 6)$.

Nếu phương trình Pell âm có nghiệm thì $35 = x_1 = 2a_1^2 + 1$, suy ra $a_1^2 = 17$, vô lý. Cũng có thể dùng ngay $x_1 = 35 < 2D - 1 = 67$ để kết luận. □

7 Một số bài toán áp dụng

Trong phần này, (x_n, y_n) luôn được đánh chỉ số theo (3); đặc biệt, chỉ số 1 ứng với nghiệm cơ bản của phương trình Pell dương.

Bài 1. Cho $D \in \mathbb{Z}_{>0}$ không chính phương và dãy nghiệm (x_n, y_n) của $x^2 - Dy^2 = 1$.

a) Với mỗi số nguyên tố lẻ $p \nmid D$, đặt $\delta = \left(\frac{D}{p}\right)$. Chứng minh rằng

$$p \mid y_{(p-\delta)/2}.$$

b) Với mỗi $M \in \mathbb{Z}_{>0}$, chứng minh rằng có vô hạn $n \in \mathbb{Z}_{>0}$ sao cho $M \mid y_n$.

Lời giải. a) Khai triển $\varepsilon^p = (x_1 + y_1\sqrt{D})^p$. Các hệ số nhị thức ở giữa chia hết cho p; dùng định lý Fermat nhỏ và tiêu chuẩn Euler, ta được

$$x_p \equiv x_1 \pmod p, \qquad y_p \equiv \delta y_1 \pmod p.$$

Vì $x_{-\delta} = x_1$, $y_{-\delta} = -\delta y_1$, công thức cộng cho

$$\begin{aligned} x_{p-\delta} &= x_p x_1 - \delta D y_p y_1 \equiv x_1^2 - Dy_1^2 = 1 \pmod p, \\ y_{p-\delta} &= y_p x_1 - \delta x_p y_1 \equiv 0 \pmod p. \end{aligned}$$

Đặt $m = (p - \delta)/2$. Công thức nhân đôi cho

$$2x_m^2 - 1 = x_{2m} \equiv 1 \pmod p, \qquad 2x_m y_m = y_{2m} \equiv 0 \pmod p.$$

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

Vì p lẻ, đồng dư đầu cho $x_m^2 \equiv 1 \pmod p$; suy ra $p \nmid 2x_m$. Đồng dư sau cho $p \mid y_m$.

b) Xét M^2+1 cặp số dư

$$(x_n \bmod M, y_n \bmod M), \qquad 0 \le n \le M^2.$$

Theo nguyên lý Dirichlet, có $0 \le i < j \le M^2$ sao cho $x_j \equiv x_i$, $y_j \equiv y_i \pmod M$. Công thức cộng với chỉ số $-i$ cho

$$x_{j-i} = x_j x_i - D y_j y_i \equiv 1 \pmod M, \qquad y_{j-i} = y_j x_i - x_j y_i \equiv 0 \pmod M.$$

Đặt $t = j - i \ge 1$. Khi đó $M \mid y_t$, và $y_t \mid y_{kt}$ với mọi $k \ge 1$. Vậy mọi chỉ số $n = kt$ đều thỏa mãn yêu cầu. □

Nhận xét. Câu b) còn cho một chỉ số $t \le M^2$ với $M \mid y_t$. Lập luận dựa trên tính hữu hạn của tập cặp số dư và khả năng nhân ngược bằng ε^{-i}; nó không cần phân tích M thành thừa số nguyên tố.

Nếu cần xây dựng chỉ số từ các lũy thừa nguyên tố, có thể dùng tính chất

$$p^e \mid y_t \quad \Longrightarrow \quad p^{e+1} \mid y_{pt} \qquad (e \ge 1).$$

Với $p = 2$, điều này suy ra từ $y_{2t} = 2x_t y_t$. Với p lẻ, khai triển $(x_t + y_t\sqrt{D})^p$ cho số hạng đầu của y_{pt} là $p x_t^{p-1} y_t$, còn các số hạng sau đều chứa y_t^3, nên đều chia hết cho p^{e+1}. Kết hợp câu a), trường hợp $p = 2$ và trường hợp $p \mid D$ (khi ấy $p \mid y_p$), ta thu được cách xây dựng chỉ số theo từng thừa số nguyên tố.

Bài 2. a) Với mỗi $k \in \mathbb{Z}_{\ge 1}$, tìm nghiệm cơ bản của $x^2 - (k^2+2)y^2 = 1$ và chứng minh rằng $x^2 - (k^2+2)y^2 = -1$ vô nghiệm nguyên.

b) Với mỗi $k \in \mathbb{Z}_{\ge 3}$, tìm nghiệm cơ bản của $x^2 - (k^2-2)y^2 = 1$ và chứng minh rằng $x^2 - (k^2-2)y^2 = -1$ vô nghiệm nguyên.

Lời giải. a) Ta có $k^2 < k^2 + 2 < (k+1)^2$, nên $D = k^2 + 2$ không chính phương. Mặt khác,

$$(k^2+1)^2 - (k^2+2)k^2 = 1.$$

Nếu có nghiệm dương (x, y) với $y < k$ thì

$$(ky)^2 < x^2 = (ky)^2 + 2y^2 + 1 < (ky+1)^2,$$

vô lý. Vậy nghiệm cơ bản là $(x_1, y_1) = (k^2+1, k)$. Do $x_1 = k^2 + 1 < 2D - 1 = 2k^2 + 3$, phương trình Pell âm vô nghiệm.

b) Với $k \ge 3$, ta có $(k-1)^2 < k^2 - 2 < k^2$, và

$$(k^2-1)^2 - (k^2-2)k^2 = 1.$$

Nếu một nghiệm dương có $y < k$ thì

$$(ky-1)^2 < x^2 = (ky)^2 - 2y^2 + 1 < (ky)^2,$$

cũng vô lý. Vậy nghiệm cơ bản là $(x_1, y_1) = (k^2-1, k)$. Với $k \ge 3$, ta có $x_1 = k^2 - 1 < 2D - 1 = 2k^2 - 5$, nên phương trình Pell âm vô nghiệm. □

Nhận xét. Điều kiện $k \ge 3$ ở câu b) có vai trò loại $k = 2$: khi ấy $D = 2$ và phương trình Pell âm có nghiệm $(1, 1)$. Ví dụ 3 ứng với $k = 6$ của câu b). Chọn $k = 12$ trong câu a) cho $D = 146 = 2 \cdot 73$, một ví dụ khác thỏa điều kiện cần trong Định lý 7a) nhưng phương trình Pell âm vẫn vô nghiệm.

Bài 3 (Một tiêu chuẩn của Dirichlet)**.** Cho p, q là hai số nguyên tố phân biệt, $p \equiv q \equiv 1 \pmod 4$ và $\left(\frac{p}{q}\right) = -1$. Chứng minh rằng $x^2 - pqy^2 = -1$ có nghiệm nguyên.

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

Lời giải. Gọi (x_1, y_1) là nghiệm cơ bản của $x^2 - pqy^2 = 1$. Vì $pq \equiv 1 \pmod 4$, ta có x_1 lẻ, $y_1 = 2w$ chẵn. Đặt

$$A = \frac{x_1 - 1}{2}, \qquad B = \frac{x_1 + 1}{2}.$$

Khi đó $AB = pqw^2$, $\gcd(A, B) = 1$, $B - A = 1$. Do đó có bốn khả năng:

$$(A, B) \in \{(pqa^2, b^2), (b^2, pqa^2), (pa^2, qb^2), (qb^2, pa^2)\},$$

với $a, b \in \mathbb{Z}_{>0}$. Khả năng đầu cho $b^2 - pqa^2 = 1$ với $0 < b < x_1$, trái với tính cơ bản. Hai khả năng cuối cho $pa^2 - qb^2 = \pm 1$. Xét modulo q, vì $q \equiv 1 \pmod 4$ nên cả 1 và -1 đều là thặng dư bậc hai, dẫn tới $\left(\frac{p}{q}\right) = 1$, mâu thuẫn.

Vậy chỉ còn $(A, B) = (b^2, pqa^2)$, cho $b^2 - pqa^2 = -1$. □

Nhận xét. Các chứng minh ở Định lý 7 và Bài 3 có chung cách tổ chức: tách $(x_1 - 1)/2$ và $(x_1 + 1)/2$ thành hai thừa số nguyên tố cùng nhau, phân bố các thừa số nguyên tố có số mũ lẻ, rồi loại các khả năng. Tính nhỏ nhất của nghiệm cơ bản loại nghiệm Pell dương nhỏ hơn; thặng dư bậc hai loại những cách phân bố không phù hợp.

Bài 4 (Tính chia hết kiểu Matiyasevich)**.** Với dãy nghiệm (x_n, y_n) của phương trình $x^2 - Dy^2 = 1$, chứng minh rằng:

a) với mọi $m, n \in \mathbb{Z}_{>0}$,

$$y_m^2 \mid y_n \iff m y_m \mid n, \qquad y_m^3 \mid y_n \iff m y_m^2 \mid n;$$

b) không có $m, n \in \mathbb{Z}_{>0}$, $m < n$, sao cho $y_n = y_m^2$ hoặc $y_n = y_m^3$.

Lời giải. a) Với $k \geq 1$, khai triển $(x_m + y_m\sqrt{D})^k$ và chia hệ số của $\sqrt{D}$ cho y_m, ta có

$$\frac{y_{km}}{y_m} = \sum_{j=0}^{\lfloor (k-1)/2 \rfloor} \binom{k}{2j+1} x_m^{k-2j-1} y_m^{2j} D^j.$$

Các số hạng với $j \geq 1$ đều chia hết cho y_m^2, nên

$$\frac{y_{km}}{y_m} \equiv k x_m^{k-1} \pmod{y_m^2}. \tag{11}$$

Do $\gcd(x_m, y_m) = 1$, với $r \in \{1, 2\}$ ta được

$$y_m^r \mid \frac{y_{km}}{y_m} \iff y_m^r \mid k.$$

Nếu $y_m^{r+1} \mid y_n$ thì $y_m \mid y_n$, nên $m \mid n$ theo Định lý 4b). Viết $n = km$ và dùng phép tương đương trên cho

$$y_m^{r+1} \mid y_n \iff y_m^r \mid k \iff m y_m^r \mid n.$$

Chiều ngược lại cũng theo đúng phép biến đổi ấy. Lấy $r = 1, 2$ thu được hai khẳng định cần chứng minh.

b) Nếu $y_m = 1$ thì tính tăng ngặt cho $y_n > 1 = y_m^2 = y_m^3$ với $n > m$. Do đó chỉ cần xét $y_m \geq 2$.

Nếu $y_n = y_m^2$, câu a) cho $n \geq m y_m \geq 2m$. Vì $x_m = \sqrt{D y_m^2 + 1} > y_m$, ta có

$$y_n \geq y_{2m} = 2 x_m y_m > y_m^2,$$

mâu thuẫn.

Nếu $y_n = y_m^3$, câu a) cho $n \geq m y_m^2 \geq 4m > 3m$. Công thức nhân ba (9) cho

$$y_n \geq y_{3m} = (4D y_m^2 + 3) y_m > y_m^3,$$

cũng mâu thuẫn. □

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

Nhận xét. Điểm chính là đồng dư (11): tính chia hết của một tọa độ được chuyển thành tính chia hết của chỉ số. Sau đó tốc độ tăng của dãy nghiệm tạo ra mâu thuẫn về kích thước. Các đồng dư kiểu này xuất hiện trong việc dùng phương trình Pell để biểu diễn quan hệ Diophantine; có thể đọc thêm [5].

Tài liệu tham khảo

[1] T. Nagell, *Introduction to Number Theory*, John Wiley & Sons, New York, 1951, Chương VI.

[2] K. Conrad, *Pell's Equation, I*, tài liệu bài giảng.
https://kconrad.math.uconn.edu/blurbs/ugradnumthy/pelleqn1.pdf

[3] K. Conrad, *Pell's Equation, II*, đặc biệt mục 2 về sự tồn tại nghiệm Pell.
https://kconrad.math.uconn.edu/blurbs/ugradnumthy/pelleqn2.pdf

[4] B. Lynn, *Pell Equations*, ghi chép về liên phân số và phương trình Pell.
https://crypto.stanford.edu/pbc/notes/ep/pell.html

[5] K. Pak, *The Matiyasevich Theorem. Preliminaries*, Formalized Mathematics **25** (2017), no. 4, 315–322. DOI: 10.1515/forma-2017-0029.
https://mizar.uwb.edu.pl/fm/2017-25/pdf25-4/hilb10_1.pdf

https://nttuan.org/

T's Lab

Nguyễn Trung Tuân, 0915011235