LIÊN PHÂN SỐ VÀ ỨNG DỤNG

Đặng Hùng Thắng

I. Liên phân số hữu hạn

Biểu thức có dạng

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}$$

trong đó $a_0, a_1, ..., a_n$ là các số thực $a_1, ..., a_n \neq 0$ được ký hiệu là $[a_0; a_1, ..., a_n]$ Từ định nghĩa dễ thấy

$$[a_0; a_1, ..., a_{k+1}] = a_0 + \frac{1}{[a_1; .a_2, ..., a_{k+1}]}$$

Nếu $a_0 \in \mathbb{Z}$ và $a_1, ..., a_n$ là các số nguyên dương thì ta nói $[a_0; a_1, ..., a_n]$ là một liên phân số hữu hạn có độ dài n. Rõ ràng một liên phân số hữu hạn là một số hữu tỷ. Ngược lại ta có

Định lý 1.1 Mỗi số hữu tỷ có thể biểu diễn dưới dạng một liên phân số hữu hạn.

Chứng minh Giả sử $x = a/b$ trong đó $a, b \in \mathbb{Z}$ và $b > 0$. Đặt $r_0 = a, r_1 = b$. Thuật chia Ô cơ lit cho ta

$$\begin{aligned}
r_0 &= r_1 q_1 + r_2 && 0 < r_2 < r_1 \\
r_1 &= r_2 q_2 + r_3 && 0 < r_3 < r_2 \\
&\cdots\cdots \\
r_{n-2} &= r_{n-1} q_{n-1} + r_n && 0 < r_n < r_{n-1} \\
r_{n-1} &= r_n q_n
\end{aligned}$$

Từ đó dễ thấy

$$\frac{a}{b} = [q_1; q_2, ..., q_n]$$

Ví dụ 1.1 Biểu diễn số $62/23$ thành liên phân số Ta có

$$\begin{aligned}
62 &= 2.23 + 16 \\
23 &= 1.16 + 7 \\
16 &= 2.7 + 2 \\
7 &= 3.2 + 1 \\
2 &= 2.1
\end{aligned}$$

Do vậy

$$\frac{62}{23} = [2; 1, 2, 3, 2]$$

Chú ý: Biểu diễn không duy nhất. Chẳng hạn

$$\frac{7}{11} = [0; 1, 1, 1, 3] = [0; 1, 1, 1, 2, 1]$$

Có thể chứng minh được một số hữu tỷư biểu diễn được theo đúng hai cách, một cách có độ dài là số chẵn , một cách có độ dài là số lẻ.

Cho liên phân số hữu hạn $[a_0; a_1, ..., a_n]$. Với mỗi $k \leqslant n$ liên phân số $C_k = [a_0; a_1, ..., a_k]$ gọi là giản phân thứ k của $[a_0; a_1, ..., a_n]$.

Công thức tính các giản phân được cho bởi định lý sau

Định lý 1.2 Cho liên phân số hữu hạn$[a_0; a_1, ..., a_n]$. Giả sữ dãy số nguyên dương $p_0, p_1, ...p_n$ và $q_0, q_1, ..., q_n$ được xác định truy hồi như sau

$$\begin{aligned} &p_0 = a_0 && q_0 = 1 \\ &p_1 = a_0a_1 + 1 && q_1 = a_1 \\ &\quad .... \\ &p_k = a_kp_{k-1} + p_{k-2} && q_k = a_kq_{k-1} + q_{k-2} \end{aligned}$$

Khi đó giản phân thứ k $C_k = [a_0; a_1, ..., a_k]$ được cho bởi

$$C_k = \frac{p_k}{q_k}$$

Chứng minh Ta chứng minh bằng quy nạp. Với $k = 0$ ta có

$$C_0 = [a_0] = p_0/q_0$$

Với $k = 1$ ta có

$$C_1 = [a_0; a_1] = a_0 + \frac{1}{a_1} = \frac{a_0a_1 + 1}{a_1} = p_1/q_1$$

Giả sử định lý đúng cho mọi $0 \leqslant k < n$. Khi đó (với $2 \leqslant k < n$)

$$C_k = [a_0; a_1, ..., a_k] = \frac{p_k}{q_k} = \frac{a_kp_{k-1} + p_{k-2}}{a_kq_{k-1} + q_{k-2}}$$

Vậy

$$\begin{aligned} C_{k+1} = [a_0; a_1, ..., a_k, a_{k+1}] &= [a_0; a_1, ..., a_{k-1}, a_k + \frac{1}{a_{k+1}}] \\ &= \frac{\left(a_k + \frac{1}{a_{k+1}}\right) p_{k-1} + p_{k-2}}{\left(a_k + \frac{1}{a_{k+1}}\right) q_{k-1} + q_{k-2}} \\ &= \frac{a_{k+1}(a_kp_{k-1} + p_{k-2}) + p_{k-1}}{a_{k+1}(a_kq_{k-1} + q_{k-2}) + q_{k-1}} \\ &= \frac{a_{k+1}p_k + p_{k-1}}{a_{k+1}q_k + q_{k-1}} \\ &= \frac{p_{k+1}}{q_{k+1}} \end{aligned}$$

Định lý được chứng minh.

Ví dụ 1.2 Ta có $173/55 = [3; 6, 1, 7]$. Theo định lý 1.2 ta tính được $(p_0, p_1, p_2, p_3) = (3, 19, 22, 173)$ và $(q_0, q_1, q_2, q_3) = (1, 6, 7, 55)$. Các giản phân là $C_0 = 3/1 = 3; C_1 = 19/6, C_2 = 22/7, C_3 = 173/55$

Bằng phương pháp quy nạp ta dễ dàng chứng minh được đẳng thức quan trọngsau giữa các (p_k) và (q_k)

Định lý 1.3

$$p_k q_{k-1} - p_{k-1} q_k = (-1)^{k=1} \tag{65}$$

Từ đó suy ra $(p_k, q_k) = 1$

Định lý1.4 Giả sử (C_k) là dãy giản phân của liên phân số hữu hạn$[a_0; a_1, ..., a_n]$.Ta có

$$C_k - C_{k-1} = \frac{(-1)^{k-1}}{q_k q_{k-1}}, \qquad (1 \leqslant k \leqslant n)$$
$$C_k - C_{k-2} = \frac{a_k(-1)^k}{q_k q_{k-2}}, \qquad (2 \leqslant k \leqslant n)$$

Chứng minh Với đẳng thức thứ nhất ta có

$$C_k - C_{k-1} = \frac{p_k q_{k-1} - p_{k-1} q_k}{q_k q_{k-1}} = \frac{(-1)^{k-1}}{q_k q_{k-1}}$$

Với đẳng thức thứ hai ta có

$$C_k - C_{k-2} = \frac{p_k q_{k-2} - p_{k-2} q_k}{q_k q_{k-2}}$$

Thay $p_k = a_k p_{k-1} + p_{k-2}, q_k = a_k q_{k-1} + q_{k-2}$ vào tử số và áp dụng (1) ta thu được điều phải chứng minh.

Từ định lý trên ta thu được kết quả quan trọng sau

Định lý 1.5 Ta có

$$C_1 > C_3 > C_5 > \cdots$$
$$C_0 < C_2 < C_4 < \cdots$$

Hơn nữa mỗi giản phân lẻ C_{2j-1} đều lớn hơn mỗi giản phân chẵn C_{2i}

Chứng minh Từ định lý trên ta thấy nếu k lẻ thì $C_k < C_{k-2}$ và nếu k chẵn thì $C_k > C_{k-2}$. Ta lại có (cũng theo định lý trên)

$$C_{2m} - C_{2m-1} = \frac{(-1)^{2m-1}}{q_{2m} q_{2m-1}} < 0 \to C_{2m} < C_{2m-1}$$

Vậy $C_{2j-1} > C_{2j-1+2i} > C_{2j+2i} > C_{2i}$

II. Liên phân số vô hạn

Định lý 2.1 Cho $a_0, a_1, a_2, ...$ là dãy vô hạn các số nguyên với $a_i > 0, i \geq 1$. Đặt

$$C_k = [a_0; a_1, ..., a_k]$$

Khi đó tồn tại giới hạn

$$\lim_{k\to\infty} C_k = \alpha$$

Ta gọi α là giá trị của liên phân số vô hạn $[a_0; a_1, a_2..,]$ và viết

$$\alpha = [a_0; a_1, a_2, ...]$$

Chứng minh Theo định lý trên ta có

$$C_1 > C_3 > C_5 > \cdots > C_{2n-1} > C_{2n+1} > \cdots$$
$$C_0 < C_2 < C_4 < \cdots < C_{2n-2} < C_{2n} < \cdots$$

Hơn nữa dãy (C_{2k+1}) là dãy giảm và bị chặn dưới bởi C_0 còn dãy (C_{2k}) tăng và bị chặn trên bởi C_1 . Vậy tồn tại

$$\lim_{k\to\infty} C_{2k+1} = \alpha_1, \quad \lim_{k\to\infty} C_{2k} = \alpha_2$$

Ta cần chứng minh $\alpha_1 = \alpha_2$. Thật vậy theo định lý trên

$$C_{2k+1} - C_{2k} = \frac{1}{q_{2k+1}q_{2k}}$$

Dễ thấy (bằng quy nạp) $q_k \geq k$. Do đó

$$\lim_{k\to\infty} C_{2k+1} - C_{2k} = 0 \to \alpha_1 = \alpha_2$$

Định lý được chứng minh.

Định lý 2.2 $\alpha = [a_0; a_1, a_2, ...]$ là một số vô tỷ,

Chứng minh Phản chứng : Giả sử trái lại $\alpha = a/b \in Q$.Theo định lý trên $C_{2n} < \alpha < C_{2n+1}$. Vậy

$$0 < \alpha - C_{2n} < C_{2n+1} - C_{2n} = \frac{1}{q_{2n+1}q_{2n}} \Leftrightarrow$$
$$0 < \alpha - \frac{p_{2n}}{q_{2n}} < \frac{1}{q_{2n+1}q_{2n}} \Leftrightarrow$$
$$0 < \alpha q_{2n} - p_{2n} < \frac{1}{q_{2n+1}} \Leftrightarrow$$
$$0 < aq_{2n} - bp_{2n} < \frac{1}{q_{2n+1}} \Leftrightarrow$$
$$1 \leqslant aq_{2n} - bp_{2n} < \frac{1}{q_{2n+1}}$$

Cho $k \to \infty$ ta có mâu thuẫn.

Ngược lại ta có

Định lý 2.3 Mỗi số vô tỷ đều biểu diễn một cách duy nhất dưới dạng một liên phân số vô hạn.

Chứng minh a) Sự tồn tại: Giả sử $\alpha = \alpha_0$ là số vô tỷ. Ta xây dựng dãy $a_0, a_1, a_2, ...$ một cách truy hồi như sau

$$a_k = [\alpha_k], \quad \alpha_{k+1} = \frac{1}{\alpha_k - a_k}$$

Trước hết ta thấy $\alpha = \alpha_0$ là số vô tỷ do đó $\alpha_0 \neq a_0$. Vậy a_1 tồn tại. Giả sử α_k vô tỷ. Suy ra α_{k+1} tồn tại và là số vô tỷ. Ta có $0 < \alpha_k - a_k < 1$ Do đó $\alpha_{k+1} = \frac{1}{\alpha_k - a_k} > 1$. Vậy $a_{k+1} = [\alpha_{k+1} \geqslant 1$. Như vậy tất cả các sô $a_1, a_2, ...$ đều là số nguyên dương. Dễ kiểm tra được

$$\alpha = [a_0; a_1, a_2, ..., a_k, \alpha_{k+1}]$$

Từ đó

$$\begin{aligned}\alpha - C_k &= \frac{\alpha_{k+1}p_k + p_{k+1}}{(\alpha_{k+1}q_k + q_{k+1})q_k} \\ &= \frac{-(p_kq_{k+1} - p_{k-1}q_k)}{(\alpha_{k+1}q_k + q_{k+1})q_k} \\ &= \frac{(-1)^{k-1}}{(\alpha_{k+1}q_k + q_{k+1})q_k}\end{aligned}$$

Vì $\alpha_{k+1}q_k + q_{k+1})q_k > a_{k+1}q_k + q_{k-1} = q_{k+1}$ suy ra

$$|\alpha - C_k| < \frac{1}{q_kq_{k+1}} \tag{66}$$

Vậy $\alpha = [a_0; a_1, a_2, ...]$.

Tiếp theo ta chứng minh biểu diễn là duy nhất. Giả sử $\alpha = [a_0; a_1, a_2, ...] = [b_0; b_1, b_2, ...]$. Vì $C_0 = a_0, C_1 = a_0 + 1/a_1$ và giản phân lẻ lớn hơn mọi giản phân chẵn nên

$$a_0 < \alpha < a_0 + 1/a_1 \to a_0 = [\alpha]$$

Chú ý rằng

$$\begin{aligned}\alpha = [a_0; a_1, a_2, ...] &= \lim_{k\to\infty}[a_0; a_1, a_2, .., a_k] \\ &= \lim_{k\to\infty}(a_0 + \frac{1}{[a_1, a_2, .., a_k]}) \\ &= a_0 + \frac{1}{[a_1, a_2, ...]} = b_0 + \frac{1}{[b_1, b_2, ...]})\end{aligned}$$

Vì $a_0 = b_0 = [\alpha]$ nên từ suy ra

$$[a_1, a_2, ...] = [b_1, b_2, ...]$$

Giả sử ta có $a_k = b_k$ và $[a_{k+1}, a_{k+2}, ...] = [b_{k+1}, b_{k+2}, ...]$. Bằng lý luận như trên ta thu được $a_{k+1} = b_{k+1}$ và

$$a_{k+1} + \frac{1}{[a_{k+2}, a_{k+3}, ...]} = b_{k+1} + \frac{1}{[b_{k+2}, b_{k+3}, ...]}$$

Suy ra $[a_{k+2}, a_{k+3}, ...] = [b_{k+2}, b_{k+3}, ...]$. Do đó bằng quy nạp suy ra $a_k = b_k \quad \forall k$.

Ví dụ 2.1 Biểu diễn $\sqrt{6}$ thành liên phân số vô hạn. Ta có

$$a_0 = [\sqrt{6}] = 2, \quad \alpha_1 = \frac{1}{\sqrt{6} - 2} = \frac{\sqrt{6} + 2}{2}$$

$$a_1 = [\frac{\sqrt{6} + 2}{2}] = 2, \quad \alpha_2 = \frac{1}{\alpha_1 - a_1} = \sqrt{6} + 2$$

$$\alpha_2 = [\sqrt{6} + 2] = 4, \quad \alpha_3 = \frac{1}{\alpha_2 - a_2} = \frac{\sqrt{6} + 2}{2} = \alpha_1$$

Vậy $\alpha_3 = \alpha_1$ do đó $a_3 = a_1, a_4 = a_2, ...,$ Vậy

$$\sqrt{6} = [2; 2, 4, 2, 4, 2, 4, ...].$$

Chú ý: Từ lý thuyết liên phân số ta tìm lại một chứng minh khác của bổ đề 1 (Xem chuyên đề 2 : Phương trình Pell).

Cho α là một số vô tỷ. Khi đó có tồn tại vô số cặp số nguyên dương(h, m) thỏa mãn

$$\left|a - \frac{h}{m}\right| < \frac{1}{m^2}$$

Thật vậy Theo (66) ta có $|\alpha - C_k| = |\alpha - p_k/q_k| < 1/q_k q_{k+1}$. Vì $q_k < q_{k+1}$ nên suy ra

$$|\alpha - p_k/q_k| < \frac{1}{q_k^2}$$

Vậy có vô số cặp số nguyên dương (h, m) mà $|\alpha - h/k| < 1/m^2$

III. Liên phân số vô hạn tuần hoàn

Ta gọi liên phân số vô hạn $[a_0; a_1, a_2, ...]$ là tuần hoàn nếu dãy (a_n) là tuần hoàn kể từ một chỉ số nào đó tức là: tồn tại số nguyên dương m và k với mọi $n \geq m$ ta có $a_n = a_{n+k}$. Số nguyên dương k được gọi là chu kỳ. Trong trường hợp đó ta viết

$$[a_0; a_1, a_2, ..., a_{m-1}, \overline{a_m, a_{m+1}, ..., a_{m+k-1}}]$$

Bài toán đặt ra là đặc trưng tất cả các số vô tỷ có biểu diễn liên phân số vô hạn tuần hoàn. Ta có khái niệm sau

Định nghĩa Số vô tỷ α gọi là số vô tỷ bậc hai nếu nó là nghiệm của một tam thức bậc hai với hệ số nguyên.

Ví dụ 3.1 Số vô tỷ $\alpha = 2 + \sqrt{3}$ là số vô tỷ bậc hai vì nó là nghiệm của $x^2 - 4x + 1 = 0$

Bổ đề 3.1 Số thực α nếu và chỉ nếu có tồn tại các số nguyên a, b, c với $b > 0$ và không chính phương,$c \neq 0$ sao cho

$$\alpha = \frac{a + \sqrt{b}}{c}$$

Chứng minh Giả sử α là số vô tỷ bậc hai. Khi đó tồn tại các số nguyên A, B, C sao cho α là nghiệm của phương trình $Ax^2 + Bx + C = 0$. Vậy

$$\alpha - \frac{-B \pm \sqrt{B^2 - AC}}{2A}$$

Đặt $a = -B, b = B^2 - 4AC, c = 2A$ hoặc $a = B, b = B^2 - 4AC, c = -2A$ Ngược lại nếu

$$\alpha = \frac{a + \sqrt{b}}{c}$$

thì α là số vô tỷ và nó là nghiệm của phương trình bậc hai $c^2x^2 - 2acx + a^2 - b = 0$

Bổ đề 3.2 Nếu α là số vô tỷ bậc hai thì $(r\alpha + s)/(t\alpha + u)$ cũng là số vô tỷ bậc hai nếu r, s, t, u là các số nguyên.

Chứng minh Giả sử

$$\alpha = \frac{a+\sqrt{b}}{c}$$

Tính toán cho ta

$$\frac{r\alpha+s}{t\alpha+u} = \frac{(ar+cs)(at+cu)-rtb+(r(at+cu)-t(ar+cs))\sqrt{b}}{(at+cu)^2-tb^2}$$

Định nghĩa Số vô tỷ

$$\alpha = \frac{a-\sqrt{b}}{c}$$

được gọi là liên hợp của α và ký hiệu là α'

Bổ đề 3.3 Nếu số vô tỷ bậc hai α là nghiệm của phương trình $Ax^2+Bx+C=0$ thì liên hợp của nó cũng là nghiệm của phương trình đó.

Thật vậy $\alpha_+\alpha' = 2a/c = -B/A, (\alpha)(\alpha') = a^2 - b/c^2 = C/A$

Bằng phép tính ta dễ thấy

Bổ đề 3.4 Ta có các hệ thức sau

$$(\alpha \pm \beta)' = \alpha' \pm \beta'$$
$$(\alpha\beta)' = \alpha'\beta'$$
$$\left(\frac{\alpha}{\beta}\right) = \frac{\alpha'}{\beta'}$$

Ta có định lý cơ bản sau đây do Lagrange tìm ra

Định lý 3.1 Số vô tỷ α có biểu diễn liên phân số tuần hoàn khi và chỉ khi nó là số vô tỷư bậc hai

Chứng minh Trước hết ta chứng minh rằng nếu α có biểu diễn liên phân số tuần hoàn thì nó là số vô tỷ bậc hai.

Giả sử

$$\alpha = [a_0; a_1, a_2, ..., a_{m-1}, \overline{a_m, a_{m+1}, ..., a_{m+k}}]$$

Đặt

$$\beta = [\overline{a_m, a_{m+1}, ..., a_{m+k}}]$$

Khi đó $\beta = [a_m, a_{m+1}, ..., a_{m+k}.\beta]$ do đó

$$\beta = \frac{\beta p_k + p_{k-1}}{\beta p_k + p_{k-1}} \qquad (1)$$

trong đó p_k/q_k và p_{k-1}/q_{k-1} là hai giản phân cuối của $[a_m, a_{m+1}, ..., a_{m+k}]$ Từ công thức (1) suy ra

$$q_k\beta^2 + (q_{k-1} - p_k)\beta - p_{k-1} = 0$$

Vậy β là số vô tỷ bậc hai. Ta lại có $\alpha = [a_0; a_1, a_2, ..., a_{m-1}, \beta]$ do đó

$$\alpha = \frac{\beta p_{m-1} + p_{m-2}}{\beta q_{m-1} + q_{m-2}}$$

do đó theo bổ đề ta có α là số vô tỷ bậc hai.

Ví dụ sau đây minh họa cách tìm số vô tỷ bậc hai từ biểu diễn liên phân số tuần hoàn của nó.

Ví dụ 3.1 Tìm x biết rằng $x = [3; \overline{1,2}]$.

Ta có $x = [3; y]$ với $y = [\overline{1,2}]$. Ta có $y = [1; 2, y]$ do đó

$$y = 1 + \frac{1}{2 + \frac{1}{y}} = \frac{3y+1}{2y+1}$$

Suy ra $2y^2 - 2y - 1 = 0$. Vì $y > 0$ nên $y = (1+\sqrt{3})/2$. Vì $x = 3 + 1/y$ nên ta tìm được

$$x = 3 + \frac{2}{1+\sqrt{2}} = \frac{4+\sqrt{2}}{2}$$

Để chứng minh phần ngược lại ta cần bổ đề sau

Bổ đề 3.5 Nếu α là số vô tỷ bậc hai thì nó có thể biểu diễn dưới dạng

$$\alpha = \frac{P + \sqrt{d}}{Q}$$

trong đó P, Q, d là các số nguyên sao cho $Q|(d - P^2)$.

Chứng minh Ta có $\alpha = (a + \sqrt{b})/c$. Nhân cả tử và mẫu với $|c|$ ta được $\alpha = (a|c| + \sqrt{bc^2})/c|c|$. Đặt $P = a|c|, d = bc^2, Q = c|c| = \pm c^2$. Khi đó $d - P^2 = c^2(b - a^2)$ chia hết $Q = \pm c^2$.

Giả sử $\alpha = \alpha_0$ là số vô tỷ bậc hai. Ta xây dựng dãy $(a_0, a_1, a_2, ...)$ như sau

Theo bổ đề trên ta có các số nguyên P_0, Q_0 và d sao cho $\alpha_0 = (P_0 + \sqrt{d})/Q_0$. $Q_0|(d - P_0^2)$. Ta đặt $a_0 = [\alpha_0]$ và xác định $P_1 = a_0 Q_0 - P_0, Q_1 = (d - P_0^2)/Q_0, \alpha_1 = (P_1 + \sqrt{d})/Q_1$. Tiếp đó đặt $a_1 = [\alpha_1]$. Một cách tổng quát nếu có

$$P_k \in \mathbb{Z}, Q_k \in \mathbb{Z}, Q_k|(d - P_k^2)$$
$$\alpha_k = \frac{(P_k + \sqrt{d})}{Q_k} \quad a_k = [\alpha_k]$$

Ta sẽ đặt

$$P_{k+1} = a_k Q_k - P_k, \quad Q_{k+1} = (d - P_{k+1}^2)/Q_k,$$
$$\alpha_{k+1} = \frac{(P_{k+1} + \sqrt{d})}{Q_{k+1}} \quad a_{k+1} = [\alpha_{k+1}]$$

Khi đó tính toán cho thấy

$$Q_{k+1} = (d - P_k^2)/Q_k + (2a_k P_k - a_k^2 Q_k)$$

do đó $Q_{k+1} \in \mathbb{Z}$ và vì $Q_{k+1} Q_k = (d - P_{k+1}^2)$ nên $Q_{k+1}|(d - P_{k+1}^2)$.

Có thể chứng minh được rằng

$$\alpha = [a_0; a_1, a_2, ...]$$

và hơn nữa dãy (a_n) xác định như trên là tuần hoàn.

Ví dụ 3.2 Khai triển liên phân số của số $\alpha = (6 + \sqrt{28})/4$

Ta có $P_0 = 6, Q_0 = 4, d = 28, 4|(28 - 6^2) = -8, \alpha_0 = (6 + \sqrt{28})/4, a_0 = [\alpha_0] = 2$ và

$P_1 = 2.4 - 6 = 2, Q_1 = (28 - 2^2)/4 = 6, \alpha_1 = (2 + \sqrt{28})/6, a_1 = [\alpha_1] = 1$

$P_2 = 1.6 - 2 - 4 = 4, Q_2 = (28 - 4^2)/6 = 2, \alpha_2 = (4 + \sqrt{28})/2, a_2 = [\alpha_2] = 4$

$P_3 = 4.2 - 4 = 4, Q_3 = (28 - 4^2)/2 = 6, \alpha_3 = (4 + \sqrt{28})/6, a_3 = [\alpha_3] = 1$

$P_4 = 1.6 - 4 = 2, Q_4 = (28 - 2^2)/6 = 4, \alpha_4 = (2 + \sqrt{28})/4, a_4 = [\alpha_4] = 1$

$P_5 = 1.4 - 2 = 2, Q_5 = (28 - 2^2)/6 = 4, \alpha_5 = (2 + \sqrt{28})/4, a_4 = [\alpha_4] = 1$

Ta thấy $P_1 = P_5, Q_1 = Q_5$ do đó $a_1 = a_5$ và dãy tuần hoàn chu kỳ 4. Ta có

$$\frac{6 + \sqrt{28}}{4} = [2; \overline{1, 4, 1, 1, 1}]$$

Tiếp theo ta muốn tìm điều kiện để số vô tỷ bậc hai có biểu diễn liên phân số tuần hoàn ngay từ đầu , tức là điều kiện để tồn tại số nguyên dương k sao cho $a_n = a_{n+k}$ với mọi $n \geq 0$. Ta có định lý sau

Định lý 3.3 Số vô tỷ bậc hai α có biểu diễn tuần hoàn ngay từ đầu nếu và chỉ nếu $\alpha > 1$ và $-1 < \alpha' < 0$.

Chứng minh định lý này khá phức tạp nên ta bỏ qua.

Bây giờ ta sẽ xác định biểu diễn liên phân số của $\sqrt{d}$.

Xét số $\alpha = \sqrt{d} + [\sqrt{d}]$. Ta có $\alpha' = [\sqrt{d}] - \sqrt{d}$ do đó $\alpha > 1$ và $-1 < \alpha' < 0$. Vậy α có biểu diễn tuần hoàn ngay từ đầu. Số hạng đầu tiên $a_0 = [\sqrt{d} + [\sqrt{d}]] = 2[\sqrt{d}] = 2a$ với $a = [\sqrt{d}]$. Ta có

$$\begin{aligned} \sqrt{d} + a = \sqrt{d} + [\sqrt{d}] &= \overline{[2a; a_1, a_2, ..., a_n]} \\ &= [2a; a_1, a_2, ..., a_n, \overline{2a; a_1, a_2, ..., a_n}] \end{aligned}$$

Suy ra

$$\sqrt{d} = [a; \overline{a_1, a_2, ..., a_n, 2a}]$$

Phân tích cẩn thận hơn ta còn có thể chứng minh được

$$a_1 = a_n, a_2 = a_{n-1}, ...$$

tức là dãy $(a_1, .., a_n)$ đối xứng,tức là nó có dạng

$$\sqrt{d} = [a; \overline{a_1, a_2, ..., a_2, a_1, 2a}]$$

ở đó $a = [\sqrt{d}]$

Ví dụ 3.3

$$\sqrt{23} = [4; \overline{1, 3, 1, 8}]$$

$$\sqrt{29} = [5; \overline{2, 1, 1, 2, 10}]$$

$$\sqrt{31} = [5; \overline{1, 1, 3, 5, 3, 1, 1, 10}]$$

$$\sqrt{46} = [6; \overline{1, 2, 1, 1, 2, 6, 2, 1, 1, 2, 1, 12}]$$

$$\sqrt{76} = [8; \overline{1, 2, 1, 1, 5, 4, 5, 1, 1, 2, 1, 16}]$$

$$\sqrt{97} = [9; \overline{1, 5, 1, 1, 1, 1, 1, 1, 5, 1, 18}]$$

IV. Ap dụng vào vấn đề tính gần đúng.

Bổ đề 4.1 Cho $\alpha = [a_1, a_2, ...]$ là một số vô tỷ. Gọi $p_j/q_j (j = 1, 2, ...$ là các giản phân của α. Khi đó nếu r, s là các số nguyên với $s > 0$ thỏa mãn

$$|s\alpha - r| < |q_k\alpha - p_k|$$

thì $s \geq q_{k+1}$.

Chứng minh Giả sử trái lại $1 \leqslant s < q_{k+1}$. Xét hệ phương trình

$$p_k x + p_{k+1} y = r$$
$$q_k x + q_{k+1} y = s$$

Suy ra

$$(p_{k+1}q_k - p_k q_{k+1})y = rq_k - sp_k$$

Vì $p_{k+1}q_k - p_k q_{k+1} = (-1)^k$ nên

$$y = (-1)^k(rq_k - sp_k)$$

Tương tự ta có

$$x = (-1)^k(sp_{k+1} - rq_{k+1})$$

Ta nhận xét rằng $x \neq 0, y \neq 0$. Thật vậy nếu $x = 0$ thì $sp_{k+1} = rq_{k+1}$. Vì $(p_{k+1}, q_{k+1}) = 1$ nên $q_{k+1}|s \to s \geq q_{k+1}$ trái giả thiết. Nếu $y = 0$ thì $r = p_k x, s = q_k x$ do đó

$$|s\alpha - r| = |x||q_k\alpha - p_k| \geqslant |q_k\alpha - p_k|$$

Mâu thuẫn.

Tiếp theo ta chứng minh $xy < 0$. Thật vậy $y < 0 \to q_k x = s - q_{k+1}y > 0 \to x > 0$. Nếu $y > 0$ thì vì $q_{k+1}y \geq q_{k+1} > s$ ta có $q_k x = s - q_{k+1}y < 0 \to x < 0$.

Mặt khác ta luôn có $p_k/q_k < \alpha < p_{k+1}/q_{k+1}$ hoặc $p_{k+1}/q_{k+1} < \alpha < p_k/q_k$ nên $q_k\alpha - p_k$ và $q_{k+1}\alpha - p_{k+1}$ có dấu trái nhau. Từ hệ phương trình trên ta có

$$\begin{aligned} |s\alpha - r| &= |(q_k x + q_{k+1}y)\alpha - (p_k x + p_{k+1}y)| \\ &= |x(q_k\alpha - p_k) + y(q_{k+1}\alpha - p_{k+1})| \end{aligned}$$

Vì $x(q_k\alpha - p_k)y(q_{k+1}\alpha - p_{k+1}) > 0$ nên $x(q_k\alpha - p_k)$ và $y(q_{k+1}\alpha - p_{k+1})$ có cùng dấu vậy

$$\begin{aligned} |s\alpha - r| &= |x||q_k\alpha - p_k| + |y||q_{k+1}\alpha - p_{k+1}| \\ &\geqslant |x||q_k\alpha - p_k| \\ &\geqslant |q_k\alpha - p_k| \end{aligned}$$

Điều này mâu thuẫn với giả thiết.Bổ đề được chứng minh.

Định lý 4.1 Trong số các số hữu tỷ r/s xấp xỉ số vô tỷ α với mẫu số $s \leqslant q_k$ thì số hữu tỷ p_k/q_k là xấp xỉ tốt nhất.

Chứng minh Giả sử $s \leqslant q_k$ và ta lại có

$$|\alpha - r/s| < |\alpha - p_k/q_k|$$

Suy ra $|s\alpha - r| < |q_k\alpha - p_k|$

$P_1 = 2.4 - 6 = 2, Q_1 = (28 - 2^2)/4 = 6, \alpha_1 = (2 + \sqrt{28})/6, a_1 = [\alpha_1] = 1$

$P_2 = 1.6 - 2 - 4 = 4, Q_2 = (28 - 4^2)/6 = 2, \alpha_2 = (4 + \sqrt{28})/2, a_2 = [\alpha_2] = 4$

$P_3 = 4.2 - 4 = 4, Q_3 = (28 - 4^2)/2 = 6, \alpha_3 = (4 + \sqrt{28})/6, a_3 = [\alpha_3] = 1$

$P_4 = 1.6 - 4 = 2, Q_4 = (28 - 2^2)/6 = 4, \alpha_4 = (2 + \sqrt{28})/4, a_4 = [\alpha_4] = 1$

$P_5 = 1.4 - 2 = 2, Q_5 = (28 - 2^2)/6 = 4, \alpha_5 = (2 + \sqrt{28})/4, a_4 = [\alpha_4] = 1$

Ta thấy $P_1 = P_5, Q_1 = Q_5$ do đó $a_1 = a_5$ và dãy tuần hoàn chu kỳ 4. Ta có

$$\frac{6 + \sqrt{28}}{4} = [2; \overline{1, 4, 1, 1, 1}]$$

Tiếp theo ta muốn tìm điều kiện để số vô tỷ bậc hai có biểu diễn liên phân số tuần hoàn ngay từ đầu , tức là điều kiện để tồn tại số nguyên dương k sao cho $a_n = a_{n+k}$ với mọi $n \geq 0$. Ta có định lý sau

Định lý 3.3 Số vô tỷ bậc hai α có biểu diễn tuần hoàn ngay từ đầu nếu và chỉ nếu $\alpha > 1$ và $-1 < \alpha' < 0$.

Chứng minh định lý này khá phức tạp nên ta bỏ qua.

Bây giờ ta sẽ xác định biểu diễn liên phân số của $\sqrt{d}$.

Xét số $\alpha = \sqrt{d} + [\sqrt{d}]$. Ta có $\alpha' = [\sqrt{d}] - \sqrt{d}$ do đó $\alpha > 1$ và $-1 < \alpha' < 0$. Vậy α có biểu diễn tuần hoàn ngay từ đầu. Số hạng đầu tiên $a_0 = [\sqrt{d} + [\sqrt{d}]] = 2[\sqrt{d}] = 2a$ với $a = [\sqrt{d}]$. Ta có

$$\begin{aligned} \sqrt{d} + a = \sqrt{d} + [\sqrt{d}] &= \overline{[2a; a_1, a_2, ..., a_n]} \\ &= [2a; a_1, a_2, ..., a_n, \overline{2a; a_1, a_2, ..., a_n}] \end{aligned}$$

Suy ra

$$\sqrt{d} = [a; \overline{a_1, a_2, ..., a_n, 2a}]$$

Phân tích cẩn thận hơn ta còn có thể chứng minh được

$$a_1 = a_n, a_2 = a_{n-1}, ...$$

tức là dãy $(a_1, .., a_n)$ đối xứng,tức là nó có dạng

$$\sqrt{d} = [a; \overline{a_1, a_2, ..., a_2, a_1, 2a}]$$

ở đó $a = [\sqrt{d}]$

Ví dụ 3.3

$$\sqrt{23} = [4; \overline{1, 3, 1, 8}]$$

$$\sqrt{29} = [5; \overline{2, 1, 1, 2, 10}]$$

$$\sqrt{31} = [5; \overline{1, 1, 3, 5, 3, 1, 1, 10}]$$

$$\sqrt{46} = [6; \overline{1, 2, 1, 1, 2, 6, 2, 1, 1, 2, 1, 12}]$$

$$\sqrt{76} = [8; \overline{1, 2, 1, 1, 5, 4, 5, 1, 1, 2, 1, 16}]$$

$$\sqrt{97} = [9; \overline{1, 5, 1, 1, 1, 1, 1, 1, 5, 1, 18}]$$

IV. Ap dụng vào vấn đề tính gần đúng.

Bổ đề 4.1 Cho $\alpha = [a_1, a_2, ...]$ là một số vô tỷ. Gọi $p_j/q_j (j = 1, 2, ...$ là các giản phân của α. Khi đó nếu r, s là các số nguyên với $s > 0$ thỏa mãn

$$|s\alpha - r| < |q_k\alpha - p_k|$$

thì $s \geq q_{k+1}$.

Chứng minh Giả sử trái lại $1 \leqslant s < q_{k+1}$. Xét hệ phương trình

$$p_k x + p_{k+1} y = r$$
$$q_k x + q_{k+1} y = s$$

Suy ra

$$(p_{k+1}q_k - p_k q_{k+1})y = rq_k - sp_k$$

Vì $p_{k+1}q_k - p_k q_{k+1} = (-1)^k$ nên

$$y = (-1)^k(rq_k - sp_k)$$

Tương tự ta có

$$x = (-1)^k(sp_{k+1} - rq_{k+1})$$

Ta nhận xét rằng $x \neq 0, y \neq 0$. Thật vậy nếu $x = 0$ thì $sp_{k+1} = rq_{k+1}$. Vì $(p_{k+1}, q_{k+1}) = 1$ nên $q_{k+1}|s \to s \geq q_{k+1}$ trái giả thiết. Nếu $y = 0$ thì $r = p_k x, s = q_k x$ do đó

$$|s\alpha - r| = |x||q_k\alpha - p_k| \geqslant |q_k\alpha - p_k|$$

Mâu thuẫn.

Tiếp theo ta chứng minh $xy < 0$. Thật vậy $y < 0 \to q_k x = s - q_{k+1}y > 0 \to x > 0$. Nếu $y > 0$ thì vì $q_{k+1}y \geq q_{k+1} > s$ ta có $q_k x = s - q_{k+1}y < 0 \to x < 0$.

Mặt khác ta luôn có $p_k/q_k < \alpha < p_{k+1}/q_{k+1}$ hoặc $p_{k+1}/q_{k+1} < \alpha < p_k/q_k$ nên $q_k\alpha - p_k$ và $q_{k+1}\alpha - p_{k+1}$ có dấu trái nhau. Từ hệ phương trình trên ta có

$$\begin{aligned} |s\alpha - r| &= |(q_k x + q_{k+1}y)\alpha - (p_k x + p_{k+1}y)| \\ &= |x(q_k\alpha - p_k) + y(q_{k+1}\alpha - p_{k+1})| \end{aligned}$$

Vì $x(q_k\alpha - p_k)y(q_{k+1}\alpha - p_{k+1}) > 0$ nên $x(q_k\alpha - p_k)$ và $y(q_{k+1}\alpha - p_{k+1})$ có cùng dấu vậy

$$\begin{aligned} |s\alpha - r| &= |x||q_k\alpha - p_k| + |y||q_{k+1}\alpha - p_{k+1}| \\ &\geqslant |x||q_k\alpha - p_k| \\ &\geqslant |q_k\alpha - p_k| \end{aligned}$$

Điều này mâu thuẫn với giả thiết.Bổ đề được chứng minh.

Định lý 4.1 Trong số các số hữu tỷ r/s xấp xỉ số vô tỷ α với mẫu số $s \leqslant q_k$ thì số hữu tỷ p_k/q_k là xấp xỉ tốt nhất.

Chứng minh Giả sử $s \leqslant q_k$ và ta lại có

$$|\alpha - r/s| < |\alpha - p_k/q_k|$$

Suy ra $|s\alpha - r| < |q_k\alpha - p_k|$

Trái với bổ đề.

Ví dụ 4.1 Ta có biểu diễn của π là

$$\pi = [3; 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, ...]$$

Các giản phân là $3, 22/7, 333/106, 335/113, 103993/33102$. Vậy chẳng hạn trong số các số hữu tỷ xấp xỉ π với mẫu số không lớn hơn 113, thì $335/113$ là xấp xỉ tốt nhất .

V. Ap dụng vào phương trình Diophant

a) Phương trình bậc nhất hai ẩn $Ax + By = C$

Chúng ta biết rằng phương trình có nghiệm nếu và chỉ nếu $d = (A, B)$ là ước của C. Trong trường hợp này giả sử $A = ad, B = bd, C = cd$ thì $(a, b) = 1$ và phương trình đã cho tương đương với

$$ax + by = c \tag{67}$$

Nếu (x_0, y_0) là một nghiệm của (67) thì tất cả các nghiệm (x, y) của (67) được cho bởi công thức $x = x_0 + bt; y = y_0 - at$. Như vậy việc giải phương trình(67) quy về tìm một nghiệm (x_0, y_0) của nó.

Xét phương trình

$$ax + by = 1 \tag{68}$$

Nếu (x_0, y_0) là một nghiệm của (68) thì (cx_0, cy_0) là nghiệm của (67). Thành thử ta quy về bài toán :

Cho $(a, b) = 1$. Hãy tìm một nghiệm của phương trình (68).

Ta biểu diễn số $a/|b|$ thành liên phân số hữu hạn

$$\frac{a}{|b|} = [a_0; a_1, a_2, ..., a_n]$$

Gọi p_{n-1}/q_{n-1} và p_n/q_n là hai giản phân cuối cùng của liên phân số này. Ta có $a/|b| = p_n/q_n, (a, b) = 1, (p_n, q_n) = 1$ nên $a = p_n, |b| = q_n$. Theo định lý 1.3 ta có

$$\begin{aligned} p_n q_{n-1} - p_{n-1} q_n &= (-1)^{n-1} \rightarrow \\ a q_{n-1} - |b| p_{n-1} &= (-1)^{n-1} \rightarrow \\ a(-1)^{n-1} q_{n-1} + |b|(-1)^n p_{n-1} &= 1 \end{aligned}$$

Vậy: Nếu $b > 0$ thì phương trình (68) có một nghiệm là

$$x = (-1)^{n-1} q_{n-1}; y = (-1)^n p_{n-1}$$

Nếu $b < 0$ thì phương trình (68) có một nghiệm là

$$x = (-1)^{n-1} q_{n-1}; y = (-1)^{n-1} p_{n-1}$$

Ví dụ 5.1 Giải phương trình $342x - 123y = 15$

Giải Vì $(342, 123) = 5$ nên phương trình đã cho tương đương với $114x - 41y = 5$. Ta biểu diễn số $114/41$ thành liên phân số

Ta có

$$\begin{aligned} 114 &= 2.41 + 32 \\ 41 &= 1.32 + 9 \\ 32 &= 3.9 + 5 \\ 9 &= 1.5 + 4 \\ 5 &= 1.4 + 1 \\ 4 &= 4.1 \end{aligned}$$

Do vậy

$$\frac{62}{23} = [2; 1, 3, 1, 1, 4]$$

Ta có $n = 5, p_4/q_4 = [2, 1, 3, 1, 1] = 25/9$. Vì $b = -41 < 0$ nên một nghiệm của phương trình $114x - 41y = 1$ là $x = q_4 = 9, y = 25$. Suy ra một nghiệm của phương trình $114x - 41y = 5$ là $x = 5.9 = 45, y = 5(25) = 125$. Nghiệm tổng quát của phương trình đã cho là

$$\begin{cases} x &= 45 + 41t \\ y &= 125 + 114t \end{cases}$$

với $t \in \mathbb{Z}$.

b) Phương trình $x^2 - dy^2 = \pm 1$

Bổ đề 5.1 Cho d là số không chính phương. Giả sử P_k, Q_k, α_k, a_k là các số xác định trong việc tìm khai triển liên phân số của $\sqrt{d}$ (xem bổ đề 3.5).

$$\begin{aligned} \alpha_k &= \frac{(P_k + \sqrt{d})}{Q_k} \quad a_k = [\alpha_k] \\ P_{k+1} &= a_k Q_k - P_k, \quad Q_{k+1} = (d - P_{k+1}^2)/Q_k, \\ \alpha_{k+1} &= \frac{(P_{k+1} + \sqrt{d})}{Q_{k+1}} \quad a_{k+1} = [\alpha_{k+1}] \end{aligned}$$

Giả sử p_k/q_k là giản phân thứ k của $\sqrt{d}$. Khi đó

$$p_k^2 - dq_k^2 = (-1)^{k-1} Q_{k+1}$$

Chứng minh Vì $\sqrt{d} = \alpha_0 = [a_0; a_1, a_2.;;;.a_k.\alpha_{k+1}]$ nên theo định lý ta có

$$\sqrt{d} = \alpha_0 = \frac{\alpha_{k+1} p_k + p_{k-1}}{\alpha_{k+1} q_k + q_{k-1}}$$

Vì $\alpha_{k+1} = (P_{k+1} + \sqrt{d})/Q_{k+1}$ ta có

$$\sqrt{d} = \frac{(P_{k+1} + \sqrt{d}) p_k + Q_{k+1} p_{k-1}}{(P_{k+1} + \sqrt{d} p_k + Q_{k+1} q_{k-1}}$$

Do đó

$$nq_k = (P_{k+1} q_k + Q_{k+1} q_{k-1})\sqrt{d} = (P_{k+1} p_k + Q_{k+1} p_{k-1}) + p_k \sqrt{d}$$

Từ đó suy ra (do$\sqrt{d} \notin Q$)

$$nq_k = P_{k+1}p_k + Q_{k+1}p_{k-1}, P_{k+1}q_k + Q_{k+1}q_{k-1} = p_k.$$

Từ đó (nhân phương trình đầu với q_k, phương trình thứ hai với p_k, rồi trừ cho nhau ta được

$$p_k^2 - dq_k^2 = (p_kq_{k-1} - p_{k-1}q_k)Q_{k+1} = (-1)^{k-1}Q_{k+1}$$

Định lý 5.1 Giả sử chu kỳ của biểu diễn liên phân số của $\sqrt{d}$ là r. Gọi p_k/q_k là giản phân thứ k của$\sqrt{d}$. Nếu r chẵn thì $x = p_{tr-1}, y = q_{tr-1}, (t = 1, 2, ...,)$ là nghiệm của phương trình Pell $x^2 - dy^2 = 1$. Nếu r lẻ thì $x = p_{2tr-1}, y = q_{2tr-1}, (t = 1, 2, ...)$ là nghiệm của phương trình Pell $x^2 - dy^2 = 1$.

Chứng minh Vì $\sqrt{d} = 0 + \sqrt{d}/1$ nên $Q_0 = 1 \to Q_{kr} = Q_0 = 1 \quad \forall k$. Theo bổ đề 1 ta có

$$p_{kr-1}^2 - dq_{kr-1}^2 = (-1)^{kr-2}Q_{kr} = (-1)^{kr}$$

Thành thử nếu r chẵn thì $p_{kr-1}^2 - dq_{kr-1}^2 = 1 \quad \forall k \in \mathbb{N}$ nếu r lẻ thì thì $p_{2tr-1}^2 - dq_{2tr-1}^2 = 1, (t = 1, 2, ...)4$

Bổ đề 5.2 $Q_i \neq 1$ với mọi i=1,2,.... và $Q_k = 1$ khi và chỉ khi k chia hết cho r

Chứng minh Giả sử tồn tại i để $Q_i = -1$. Suy ra $\alpha_i = -P_i - \sqrt{d}$. Vì α_i có biểu diễn liên phân số tuần hoàn ngay từ đầu nên $-1 < (\alpha_i)' = -P_i + \sqrt{d} < 0$ và $\alpha_i = -P_i - \sqrt{d} > 1$. Suy ra

$$\sqrt{d} < P_i < -1 - \sqrt{d}$$

Mâu thuẫn.

Giả sử $k = tr$.Với $a_0 = [\sqrt{d}]$ ta có

$$\sqrt{d} = [a_0; a_1, ..., a_{k-1}, \alpha_k] == [a_0; \overline{a_1, ..., a_r, 2a_0}]$$

Suy ra $\alpha_k = \overline{[2a_0, a_1, ..., a_r]} = a_0 + [a_0; \overline{a_1, ..., a_r, 2a_0}] = a_0 + \sqrt{d} = (P_k + \sqrt{d})/Q_k \Leftrightarrow Q_ka_0 + Q_k\sqrt{d} = P_k + \sqrt{d} \Leftrightarrow Q_k = 1, a_0 = P_k$

Đảo lại nếu $Q_k = 1$. Ta có $\alpha_k = P_k + \sqrt{d} > P_k$ Vì $\alpha_k = [a_k, a_{k+1}, ...]$ là tuần hoàn ngay từ đầu nên $-1 < (\alpha_k)' = P_k - \sqrt{d} < 0 \to \sqrt{d} - 1 < P_k < \sqrt{d}$ Thành thử $[\sqrt{d}] = P_k = a_0$. Suy ra $\alpha_k = P_k + \sqrt{d} = [\sqrt{d}] + \sqrt{d} = \overline{[2a_0, a_1, ..., a_r]}$

. Ta có

$$\sqrt{d} = \alpha = [a_0; a_1, ..., a_{k-1}, \alpha_k] = [a_0; a_1, ..., a_{k-1}, \overline{2a_0, a_1, ..., a_r}] = [a_0; \overline{a_1, ..., a_r, 2a_0}]$$

Vậy k phải là bội của chu kỳ r.

Để chứng minh đây là tất cả các nghiệm của phương trình Pell ta cần các bổ đề sau

Bổ đề 5.3 Cho α là một số vô tỷ và r/s là số hữu tỷ tối giản với $r > 0$ và

$$|\alpha - r/s| < 1/(2s^2)$$

Khi đó r/s phải là một giản phân của α.

Chứng minh Giả sử r/s không là giản phân khi đó tồn tại k sao cho

$$q_k \leqslant s < q_{k+1} \tag{69}$$

. Theo bổ đề 1 ta có

$$|q_k\alpha - p_k| \leqslant |s\alpha - r| = s|\alpha - r/s| < 1/(2s)$$

Suy ra

$$|\alpha - p_k/q_k| < 1/(2sq_k)$$

Vì rằng $|sp_k - rq_k| \geqslant 1$ nên ta có

$$\begin{aligned}\frac{1}{sq_k} &\leqslant \frac{|sp_k - rq_k|}{sq_k} \\ &= \left|\frac{p_k}{q_k} - \frac{r}{s}\right| \\ &\leqslant \left|\alpha - \frac{p_k}{q_k}\right| + \left|\alpha - \frac{r}{s}\right| \\ &< \frac{1}{2sq_k} + \frac{1}{2s^2}\end{aligned}$$

Vậy $1/2sq_k < 1/2s^2 \to 2sq_k > 2s^2 \to q_k > s$ trái với (5).

Bổ đề 5.4 Giả sử x, y là các số nguyên dương sao cho $x^2 - dy^2 = n$ và $|n| < \sqrt{d}$. Khi đó x/y là một giản phân của $\sqrt{d}$.

Chứng minh Xét trường hợp $n > 0$ Ta có $(x + y\sqrt{d})(x - y\sqrt{d}) = n \to x > y\sqrt{d} \Leftrightarrow 0 < x/y - \sqrt{d}$. Lại có

$$\begin{aligned}\frac{x}{y} - \sqrt{d} &= \frac{x - \sqrt{d}}{y} \\ &= \frac{x^2 - dy^2}{y(x + y\sqrt{d})} \\ &< \frac{n}{y(2y\sqrt{d})} \\ &< \frac{\sqrt{d}}{2y^2\sqrt{d}} = \frac{1}{2y^2}\end{aligned}$$

Theo bổ đề 5.3 thì x/y là một giản phân của $\sqrt{d}$

Giả sử $n < 0$. Khi đó

$$y^2 - (1/d)x^2 = -n/d$$

Ta có $-n/d > 0, -|n|/d < 1/\sqrt{d}$ Vậy theo bước trước y/x là một giản phân của $1/\sqrt{d}$. Nhưng khi đó $x/y = 1/(y/x)$ là một giản phân của $1/(1/(\sqrt{d}) = \sqrt{d}$

Định lý 5.2 Cho phương trình Pell

$$x^2 - dy^2 = 1.$$

Gọi r là chu kỳ của biểu diễn liên phân số của $\sqrt{d}$.

Nếu r chẵn thì tất cả các nghiệm của phương trình Pell là

$$x = p_{kr-1}, y = q_{kr-1}$$

. Nếu r lẻ thì tất cả các nghiệm của phương trình Pell là $x = p_{2tr-1}, y = q_{2tr-1}, \quad t \in \mathbb{N}^*$

Chứng minh Giả sử (x, y) là nghiệm của phương trình Pell.Theo bổ đề 5.4 tồn tại i để $x = p_i, y = q_i$. Từ đó

$$p_i^2 - dq_i^2 = 1.$$

Từ bổ đề 5.1 rút ra $(-1)^{i-1}Q_{i+1} = 1 \to Q_{i+1} = \pm 1$. Vì $Q_{k+1} \neq -1$ nên $Q_{i+1} = 1$ và i lẻ. Theo bổ đề 5.2 ta rút ra tồn tại ki $+ 1 = kr \to i = kr - 1$ và kr chẵn. Thành thửu nếu r lẻ thì k chẵn, k=2t.

Xét phương trình

$$x^2 - dy^2 = -1 \qquad (5.1)$$

Ta có kết quả sau.

Định lý 5.3 Phương trình $x^2 - dy^2 = -1$ có nghiệm khi và chỉ khi chu kỳ r của biểu diễn liên phân số của $\sqrt{d}$ là số lẻ. Trong trường hợp ấy các nghiệm của nó là $x = p_{(2tr-r-1)}, y = q_{(2tr-r-1)}$ với t=1,2,...

Chứng minh: Từ bổ đề 5.1 dễ thấy nếu chu kỳ r của biểu diễn liên phân số của $\sqrt{d}$ là số lẻ thì $x = p_{(2tr-r-1)}, y = q_{(2tr-r-1)}$ với t=1,2,... là nghiệm.

Giả sử (x, y) là nghiệm của phương trình (5.1). Theo bổ đề 5.4 tồn tại i để $x = p_i, y = q_i$. Từ đó

$$p_i^2 - dq_i^2 = -1.$$

Từ bổ đề 1 rút ra $(-1)^{i-1}Q_{i+1} = -1 \to Q_{i+1} = \pm 1$. Vì $Q_{i+1} \neq -1$ nên $Q_{i+1} = 1$ và i chẵn.Theo bổ đề 5.1 tồn tại $k \in \mathbb{N}$ sao cho $i + 1 = kr \to i = kr - 1$ và kr lẻ. Thành thửu nếu r chẵn thì kr luôn chẵn do đó phưuơng trình vô nghiêm.

Trong trường hợp r lẻ lý luận tương tự nhưu trong trường hợp phương trình Pell $x^2 - dy^2 - 1$ tất cả các nghiệm phải có dạng$x = p_{kr-1}, y = q_{kr-1}$ trong đó kr lẻ tức là khi k lẻ hay $x = p_{(2tr-r-1)}, y = q_{(2tr-r-1)}$ với t=1,2,...

V.I Phân tích một số ra thừa số Cho số nguyên dương n.Ta có nhận xét sau : Nếu tìm được hai số nguyên dương thỏa mãn $x^2 \equiv y^2 \pmod{n}$ với $x - y$ và $x + y$ không chia hết cho n. Khi đó $u = (x - y, n)$ và $v = (x + y, n)$ là các ước không tầm thường (tức là không bằng 1 hoặc n của n). Thật vậy ta có $(x - y)(x + y)$ chia hết cho n. Vì x-y không chia hết cho n nên $u \neq n$, Nếu $u = 1$ suy ra $x + y$ chia hết cho n, trái giả thiết. Tương tự $v \neq 1$.

. Giả sử p_k, q_k, P_k, Q_k là các số có được khi tính các giản phân của $\sqrt{d}$. Theo định lý ta có

$$p_k^2 \equiv (-1)^{k-1}Q_{k+1} \pmod{n}$$

Nếu ta tìm được k lẻ và $Q_{k+1} = s^2$ là số chính phương thì ta có thể dùng hai số $u = (p_k - s, n), v = (p_k + s, n)$ là các ước của n nếu chúng khác 1 nà chính n. Như vậy thuật toán như sau:

- Trong dãy Q_k với k chẵn ta nhặt ra các số chính phương.

- Giả sưt $Q_k = s^2$, k chẵn : xét các số $p_{k-1} \pm s$. Kiểm tra xem có số nào chia hết cho n không

-Nếu chúng không chia hết cho n thì ta dùng thuật toán O co lit để tìm $u = (p_k + s, n), v = ((p_k - s, n)$. Khi đó u, v chính là các thừa số của n

Ví dụ 6.1 Phân tích 1047 ra thừa số . Ta có $Q_1 = 13, Q_2 = 49 = 7^2$Ta có $p_1 \equiv (-1)^2 Q_2 \pmod{n}$, $p_1 = 129$ Vậy $(129 - 7, 1037) = (122, 1037) = 61, (129 + 7, 1037) = (136, 1037) = 17$Ta có 61.17=1037.

Ví dụ 6.2 Phân tích ra thừa số 1000009. Ta có $Q_1 = 9, Q_2 = 445, Q_3 = 873, Q_4 = 81 = 9^2$Tuy nhiên $p_3 + 9 = 2000009 + 9$ chia hết cho 1000009. Ta lại tiếp

tục tìm các số Q_k chính phương mà k chẵn. Ta tìm được $Q_{18} = 16 = 4^2$. Khi đó $p_{17} = 494881$. và $(494881 - 4, 1000009) = 293, (494881 + 4, 1000009) = 3413$. Thành thử 1000009 có hai ước phân biệt là 293 và 3413. Ta cũng thấy (293)(3413)=1000009.