Một số lớp phương trình Diophant cơ bản

Đặng Hùng Thắng

Trường Đại học KHTN, DHQGHN

1 Mở đầu

Phương trình Diophant là phương trình đại số có dạng

$$P(x_1, x_2, \ldots, x_n) = 0$$

ở đó $P(x_1, x_2, \ldots, x_n)$ là một đa thức hệ số nguyên và ta chỉ yêu cầu tìm các nghiệm nguyên (hoặc nguyên dương) mà thôi.

Người đầu tiên nghiên cứu về các phương trình loại này là nhà toán học Hylap Diophantus sống ở thành phố Alexandria vào khoảng năm 250 sau công nguyên. Toàn bộ sự nghiệp của ông dành cho việc thu thập những bài toán loại này,sáng tạo thêm những bài toán mới rồi sau đó biên soạn thành một bộ sách tên là *Arithmetica* (Số học) gồm 13 tập. Trải qua những biến loạn thời Trung cổ, đến thời Phục hưng bảy tập đã bị thất lạc chỉ còn sáu tập là còn lưu giữ được và đã truyền cảm hứng và trở thành Kinh thánh cho các nhà Toán học thời Phục hưng trong đó có Ferma. Ông đã xem xét kỹ lưỡng sự trình bày của Diophante về bộ ba các số Pitago (x, y, z) là nghiệm nguyên dương của phương trình $x^2 + y^2 = z^2$. Ông đã ghi lại bên lề cuốn sách nhận xét sau đây của mình

Một số lập phương không thể viết dược dưới dạng tổng của hai lập phương. Một lũy thừa bậc bốn không thể viết dược dưới dạng tổng của hai lũy thừa bậc bốn. Một cách tổng quát, một số là lũy thừa bậc lớn hơn hai không thể viết dưới dạng tổng của hai lũy thừa cùng bậc. Tôi đã có một chứng minh thực sự tuyệt vời mệnh đề này nhưng do lề quá hẹp nên không thể viết hết ra được.

Như vậy vào năm 1637 Fermar đã phát biểu và tin rằng ông đã chứng minh được định lý sau đây, mà sau này thường được gọi là *Định lý cuối cùng của Ferma* (mà đúng ra phải gọi là Giả thuyết cuối cùng của Ferma).

Với $n > 2$ thì phương trình Diophant

$$x^n + y^n = z^n$$

không có nghiệm nguyên dương.

Trong hơn ba thế kỷ, những nỗ lực tìm kiếm chứng minh định lý này đều thất bại và Định lý cuối cùng của Ferma đã trở thành một bài toán khó giải nhất của toán học.Nhiều nhà toán học xuất sắc đã thất bại ê chề khi cố gắng tấn công bài toán này. Mấy dòng ghi chú bên lề của Ferma như một lời thách thức nhiều thế hệ các nhà toán học.

Mãi đến năm 1994 (tức là 350 năm sau) Định lý cuối cùng của Ferma này mới chính thức được chứng minh bởi nhà toán học Mỹ Andrew Wiles. Chứng minh của ông dài 130 trang, là một tuyệt phẩm của toán học hiện đại, sử dụng những kỹ thuật toán học mới nhất và tinh tế nhất của toán học thế kỷ 20 như phương trình cliptic,dạng modular, nhóm Galoir, phương pháp Kolyvagin-Flax, giả thuyết Taniyama-Shimura..

Như vậy hai khả năng có thể xảy ra : Hoặc là chứng minh tuyệt vời của ông thực ra là một chứng minh sai. Hoặc là ông đã có một chứng minh thiên tài chỉ dựa trên những kỹ thuật sơ cấp toán học của thế kỷ 17 với một suy

luận cực kỳ độc đáo tới mức từ Ole dến đến Wiles không ai nghĩ ra được. Hiện nay một số người vẫn tin vào khả năng này và họ vẫn đang tìm cách phát minh lại chứng minh của Ferma.

2 Phương trình bậc nhất

2.1 Phương trình bậc nhất hai ẩn

Phương trình Diophant đơn giản nhất là phương trình bậc nhất hai ẩn

$$Ax + By = C \quad (1)$$

trong đó $A, B, C \in Z$.

Định lý 1 a) Phương trình (1) có nghiệm nguyên khi và chỉ khi $d = (A, B)$ là ước của C.

b) Nếu (x_0, y_0) là một nghiệm của (1) thì mọi nghiệm của (1) được cho bởi

$$\begin{cases} x &= x_0 + \frac{B}{d}t \\ y &= y_0 - \frac{A}{d}t \end{cases}$$

ở đó $t \in Z$

Chứng minh a) Nếu (1) có nghiệm (x_0, y_0) thì $Ax_0 + By_0 = C \rightarrow d|C$.

Đảo lại giả sử $d|C$. Không giảm tổng quát giả sử $B > 0$. Ta có $A = da, B = db, C = dc$ với $(a, b) = 1$. Khi đó (1) tương đương với

$$ax + by = c \quad (2)$$

Vì $(a, b) = 1$ nên tập $\{a, 2a, ..., ab\}$ là hệ đầy đủ mod b. Vậy tồn tại $x \in \{1, 2, ...a_1\}$ sao cho $ax \equiv c \pmod{b} \rightarrow c - ax = by$ với $y \in Z$.

b)Nếu (x, y) cho bởi công thức trên thì $Ax+By = Ax_0+By_0 = C$. Đảo lại giả sử (x, y) là một nghiệm của (1) tức là thỏa mãn (2). Khi đó $ax+by = ax_0+by_0 \rightarrow a(x-x_0) = b(y_0-y) \rightarrow b|a(x-x_0)$. Vì $(a, b) = 1$ nên $b|x-x_0 \rightarrow x-x_0 = bt \rightarrow x = x_0+bt = x_0+\frac{B}{d}t, t \in Z$. Từ $x-x_0 = bt$ suy ra $at = y_0-y \rightarrow y = y_0-at = y_0-\frac{A}{d}t$. Dịnh lý được chứng minh.

Hệ quả Nếu $a, b \in N^*, (a, b) = 1$ thì tồn tại $u, v \in N^*$ để $au - bv = 1$.

Chứng minh Theo định lý trên phương trình $ax + by = 1$ có nghiệm

$$\begin{cases} x = x_0 + bt \\ y = y_0 - at, t \in Z \end{cases}$$

do đó phương trình $au - bv = 1$ có nghiệm

$$u = bt + x_0, \quad v = at - y_0, t \in Z$$

Chọn $t \in Z : t > -x_0/b, t > y_0/a$ ta có $u, v \in N^*$.

Từ định lý trên ta thấy việc tìm nghiệm của (1) quy về việc tìm UCLN $d = (A, B)$ và tìm một nghiệm riêng (x_0, y_0). Sau đây ta sẽ trình bày một thuật toán sử dụng liên phân số để tìm một nghiệm riêng (x_0, y_0).

Ta nhắc lại một số kiến thức về liên phân số. 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 $a_0, a_1, ..., a_n \in R$ và $a_1, ..., a_n \neq 0$ được ký hiệu là $[a_0; a_1, ..., a_n]$. Từ định nghĩa suy ra

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

Nếu $a_0 \in Z$ và $a_1, ..., a_n \in N^*$ 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 số hữu tỷ. Ngược lại ta có

Bổ đề 1Mỗi số hữu tỷ là một liên phân số hữu hạn

Chứng minh Giả sử $x = a/b$ trong đó $a, b \in Z$ và $b > 0$. Đặt $r_0 = a, r_1 = b$. Thực hiện thuật toán O-cơ -lit

$$r_0 = r_1 q_1 + r_2 \qquad 0 < r_2 < r_1$$

$$r_1 = r_2 q_2 + r_3 \qquad 0 < r_3 < r_2$$

.....

$$r_{n-2} = r_{n-1} q_{n-1} + r_n \qquad 0 < r_n < r_{n-1}$$

$$r_{n-1} = r_n q_n$$

Từ đó

$$x = \frac{r_0}{r_1} = [q_1; q_2, ..., q_n]$$

Ví dụ1 Biểu diễn số $x = 62/23$ thành giản phân. Ta có

$$62 = 2.23 + 16$$

$$23 = 1.16 + 7$$

$$16 = 2.7 + 2$$

$$7 = 3.2 + 1$$

$$2 = 2.1$$

Do đó

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

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

Ta có định lý cơ bản sau của liên phân số

Định lý Cho liên phân số $[a_0; a_1, ..., a_n]$. Xét dãy số $p_0, p_1, ...p_n$ và $q_0, q_1, ..., q_n$ xác định truy hồi theo cách sau

$$p_0 = a_0 \qquad q_0 = 1$$

$$p_1 = a_0a_1 + 1 \qquad q_1 = a_1$$

....

$$p_k = a_kp_{k-1} + p_{k-2} \qquad q_k = a_kq_{k-1} + q_{k-2}$$

Khi đó

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

$$p_kq_{k\ \ 1} - p_{k\ \ 1}q_k = (-1)^{k=1}$$

Để giải phương trình

$$Ax + By = C \quad (1)$$

ta thực hiên theo các bước sau

- Dùng thuật toán O-cơ-lit tìm $d = (A, B)$. Nếu d không là ước của C phương trình vô nghiệm. Nếu $d|C$ viết $A = da, B = db, C = dc$ và (1) tương đương với

$$ax + by = c \quad (2)$$

ở đó $(a_1, b_1) = 1$

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

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

Giả sử p_{n-1}/q_{n-1} và p_n/q_n là hai giản phân cấp $n-1$ và cấp n. 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 ta

có

$$p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1} \rightarrow$$

$$aq_{n-1} - |b| p_{n-1} = (-1)^{n-1} \rightarrow$$

$$a(-1)^{n-1} q_{n-1} + |b|(-1)^n p_{n-1} = 1$$

$$a(-1)^{n-1} cq_{n-1} + |b|(-1)^n cp_{n-1} = c$$

- Vậy nếu $b > 0$ thì phương trình (1) có nghiệm riêng là

$$x_0 = (-1)^n \ ^1 cq_{n-1}; y = (-1)^n cp_{n-1}$$

Nếu $b < 0$ thì phương trình (1) có nghiệm riêng là

$$x_0 = (-1)^{n-1} cq_{n-1}; y = (-1)^{n-1} cp_{n-1}$$

Ví dụ Giải phương trình $342x - 123y = 15 \quad (1')$.

Giải

- Ta có $(342, 123) = 3$ do đó $a = 114, b = -41$. Do đó (1') tương đương với

$$114x - 41y = 5 \quad (2')$$

- Biểu diễn 114/41 thành liên phân số

$$114 = 2.41 + 32$$

$$41 = 1.32 + 9$$

$$32 = 3.9 + 5$$

$$9 = 1.5 + 4$$

$$5 = 1.4 + 1$$

$$4 = 4.1$$

Do vậy

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

Ta có $n = 5, p_4/q_4 = [2,1,3,1,1] = 25/9 \rightarrow p_4 = 25, q_4 = 9.$

- Vì $b = -41 < 0$ nên (1') có nghiệm riêng là $x_0 = (-1)^4 5.9 = 45, y_0 = (-1)^4 5(25) = 125$. Vậy nghiệm của (1') là

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

với $t \in Z$.

2.2 Phương trình bậc nhất nhiều ẩn

Phương trình bậc nhất k ẩn ($k \geq 2$) là phương trình dạng

$$A_1x_1 + A_2x_2 + \cdots + A_kx_k = C \quad (4)$$

trong đó $a, b, c \in Z$.

Định lý 2 i) Phương trình (4) có nghiệm nguyên khi và chỉ khi $d = (A_1, A_2, ..., A_k)$ là ước của C.

ii) Nếu (4) có nghiệm nó sẽ có vô số nghiêm.

Chứng minh i) Diều kiện cần hiển nhiên .Chứng minh điều kiện đủ bằng quy nạp: Với $k = 2$ khẳng định đúng. Giả sử đúng với k. Xét phương trình với $d = (A_1, ..., A_k, A_{k+1})|C$. Dặt $H = (A_1, ..., A_k) \rightarrow d = (H, A_{k+1})|C$. Theo định lý 1 tồn tại $t, x_{k+1} \in Z$ sao cho $Ht + A_{k+1}x_{k+1} = C$. Vì $H|Ht$ nên theo giả thiết quy nạp tồn tại $x_1, ..., x_k$ sao cho

$$\sum_{i=1}^{k} A_ix_i = Ht$$

Vậy

$$\sum_{i=1}^{k+1} A_i x_i = \sum_{i=1}^{k} A_i x_i + A_{k+1} x_{k+1} = Ht + A_{k+1} x_{k+1} = C$$

ii) Chứng minh bằng quy nạp.Giả sử đúng với k. Tồn tại $t_1, ..., t_k, t_{k+1} \in Z$ sao cho

$$\sum_{i=1}^{k+1} A_i t_i = C$$

Xét phương trình

$$\sum_{i=1}^{k} A_i x_i = C - A_{k+1} t_{k+1} \quad (5)$$

Phương trình này có nghiệm $(t_1, ..., t_k)$. Theo quy nạp (5) có vô số nghiệm. Với mỗi nghiệm $(x_1, ... x_k)$ của (5) thì $((x_1, ..., x_k, t_{k+1})$ là nghiệm của phương trình

$$\sum_{i=1}^{k+1} A_i x_i = C \quad (6)$$

Do đó (6) có vô số nghiệm.

Có thể chứng minh được nghiệm tổng quát của (4) có dạng

$$\begin{cases} x_1 & = \alpha_1 + \sum_{i=1}^{k-1} L_{i1} t_i \\ x_2 & = \alpha_2 + \sum_{i=1}^{k-1} L_{i2} t_i \\ \cdots & \\ x_k & = \alpha_k + \sum_{i=1}^{k-1} L_{ik} t_i \end{cases}$$

trong đó $(\alpha_1 \ldots, \alpha_k)$ là một nghiệm riêng. $(L_{ij}), i = 1, ..., k-1; j = 1, 2, \ldots, k$ là các hệ số nguyên và $t_1, ..., t_{k\ 1}$ là các số nguyên tùy ý.

Tuy nhiên không có công thức tường minh của các hệ số (L_{ij}).

Ví dụ Giải phương trình

$$6x + 15y + 10x = 3 \quad (7)$$

Giải Ta có (7) $\Leftrightarrow 6(x+z)+15y+4z=3$. Đặt $u=x+z$ ta có $15y+4z=3-6u$. Cố định u.Ta thấy $(-1,4)$ là nghiệm riêng của $15y+4z=1$ do đó $(-3+6u,12-24u)$ là nghiệm riêng của $15y+4z=3-6u$. Từ đó

$$y=-3+6u+4t; z=12-24u-15t, \rightarrow x=u-z=-12+25u+15t$$

Dễ kiểm tra mỗi bộ (x,y,z) có dạng trên là nghiệm. Vậy phương trình có nghiệm

$$\begin{cases} x &= -12+25u+15t \\ y &= -3+6u+4t \\ z &= 12-24u-15t \end{cases}$$

C. Một số bài toán chon lọc

Bài toán 1 Cho $a>1$. Chứng minh rằng

$$(a^m-1,a^n-1)=a^{(m,n)}-1$$

Giải Xét trường hợp $(m,n)=1$. Ta phải chứng minh

$$(a^m-1,a^n-1)=a-1$$

Dặt $d=(a^m-1,a^n-1)$. Vì $a-1|a^m-1, a-1|a^n-1$ nên $a-1|d$. Dảo lại giả sử $m>n$. Theo hệ quả tồn tại $u,v\in N^*$ để $mu-nv=1$. Vì $a^m\equiv 1 \pmod d, a^n\equiv 1 \pmod d \rightarrow a^{mu}\equiv 1 \pmod d, a^{nv}\equiv 1 \pmod d \rightarrow a^{mu}-a^{nv}\equiv 0 \pmod d$ Khi đó

$$d|(a^{mu}-a^{nv}=a^{nv}(a^{mu-nv}-1)=a^{nv}(a-1)$$

Vì $a-1|d$ nên $(d,a)=1$ do đó $d|a-1$.Vậy $d=a-1$ Với (m,n) bất kỳ đặt $g=(m,n)$ ta có $m=gm_1, n=gn_1$. Đặt $b=a^g$. Khi đó

$$(a^m-1,a^n-1)=(b^{m_1}-1,b^{n_1}-1)=b-1=a^{(m,n)}-1$$

Bài toán 2 Cho $a > 1$ và $m, n \in N^*$. Giả sử $m = 2^i r, n = 2^j s$ với r, s là các số lẻ.Chứng minh rằng

$$(a^m + 1, a^n + 1) = \begin{cases} a^{(m,n)} + 1 & \text{nếu } i = j \\ 2 & \text{nếu } i \neq j \text{ , } a \text{ lẻ} \\ 1 & \text{nếu } i \neq j \text{ , } a \text{ chẵn} \end{cases}$$

Giải

- Nếu m, n lẻ , $(m, n) = 1$ .Ta chứng minh

$$(a^m + 1, a^n + 1) = a + 1$$

Đặt $d = (a^m+1, a^n+1)$. Vì $a+1|a^m = 1, a = 1|a^n+1$ nên $a+1|d$. Dảo lại giả sử $m > n$.Theo hệ quả tồn tại $u, v \in N^*$ để $mu-nv = 1$. Do m, n lẻ nên u, v khác tính chẵn lẻ. Giả sử u lẻ, v chẵn. Ta có $a^m \equiv -1 \pmod d, a^n \equiv -1 \pmod d \rightarrow a^{mu} \equiv -1 \pmod d, a^{nv} \equiv 1 \pmod d a^{mu} + a^{nv} \equiv 0 \pmod d$.Khi đó

$$d|(a^{mu} + a^{nv} = a^{nv}(a^{mu-nv} + 1) = a^{nv}(a + 1)$$

Vì $a + 1|d$ nên $(d, a) = 1$ do đó $d|a + 1$.Vậy $d = a + 1$

- Nếu m, n lẽ . Đặt $g = (m, n)$ ta có $m = gm_1, n = gn_1$. Đặt $b = a^{(m,n)} = a^g$. Khi đó

$$(a^m + 1, a^n + 1) = (b^{m_1} + 1, b^{n_1} + 1) = b + 1 = a^{(m,n)} + 1$$

- Nếu $m = 2^i r, n = 2^i s$ với r, s là các số lẻ. Dặt $b = a^{2^i}$. Khi đó $(a^m + 1, a^n + 1) = (b^r + 1, b^s + 1) = b^{(r,s)} + 1 = a^{2^i(r,s)} + 1 = a^{(m,n)} + 1$

- Nếu m, n khác tính chẵn lẻ, chẳng hạn m chẵn, n lẻ. Ta có $a^m \equiv -1 \pmod d, a^n \equiv -1 \pmod d \rightarrow a^{mn} \equiv -1 \pmod d, a^{nm} \equiv 1 \pmod d \rightarrow -1 \equiv$

$1 \pmod d \to 2 \equiv 0 \pmod d$. Vậy $d = 1$ hoặc $d = 2$. Nếu a lẻ thì $2|d \to d = 2$. Nếu a chẵn thì $d \neq 2 \to d = 1$.

- Nếu $m = 2^i r, n = 2^j s$ với r, s là các số lẻ và $i \neq j$, chẳng hạn $i > j$. Đặt $b = a^{2^j} \to a^n = b^s, a^m = b^{2^{i-j}r} = b^t$, ở đó $t = 2^{i-j}r$ chẵn. Khi đó nếu a lẻ thì b lẻ do đó $(a^m + 1, a^n + 1) = (b^t + 1, b^s + 1) = 2$.Nếu a chẵn thì b chẵn do đó $(a^m + 1, a^n + 1) = (b^t + 1, b^s + 1) = 1$

Bài toán 3 Cho $A, B \in N^*, (A, B) = 1$. Ký hiệu $\mathcal{A}$ là tập các số $n \in N^*$ sao cho phương trình

$$Ax + By = n$$

không có nghiệm nguyên dương.Chứng minh rằng

i) $\max \mathcal{A} = ab$.

ii) Tìm $|\mathcal{A}|$

Giải

i) Chứng minh $AB \in \mathcal{A}$: Giả sử trái lại $AB \notin \mathcal{A}$. Tồn tại $x, y \in N^*$ sao cho $Ax + By = AB \to By = A(x - B) \to A|By \to A|y \to y \geq A$. Tương tự $x \geq B$. Vậy $AB = Ax + By \geq 2AB$. Mâu thuẫn. Tiếp theo ta chứng minh nếu $n > AB$ thì $n \notin \mathcal{A}$. Phương trình $Ax + By = n$ có nghiệm là $x = x_0 + Bt, y = y_0 - At$. Ta chứng minh tồn tại $t \in Z$ sao cho $x > 0, y > 0 \to -x_0/B < t < y_0/A \Leftrightarrow t \in (-x_0/B; y_0/A)$. Vì khoảng $(-x_0/B; y_0/A)$ có độ dài $y_0/A + x_0/B = (Ax_0 + By_0)/AB = n/AB > 1$ nên tồn tại $t \in Z, t \in (-x_0/B; y_0/A)$.

ii) Xét $n \leqslant AB$. Ta chứng minh $n \in \mathcal{A}$ nếu và chỉ nếu $m = AB + A + B - n \notin \mathcal{A}$. Tồn tại $1 \leqslant x \leqslant B$ sao cho $Ax \equiv n \pmod B \to n = Ax + By$. Thành thử với mỗi $n \in N^*$ ta luôn có biểu diễn

$$n = Ax + By, 1 \leqslant x \leqslant B, y \in n^*$$

Nếu $n \in \mathcal{A}$ thì $y \leq 0$. Vậy $m = AB + A + B - Ax - By = A(B + 1 - x) + B(1 - y) = Ax_1 + By_1$ ở đó $x_1 = B + 1 - x \geq 1, y_1 = 1 - y \geq 1$. Vậy $m \notin \mathcal{A}$. Đảo lại giả sử $m \notin \mathcal{A} \rightarrow m = Ax_1 + By_1, x_1, y_1 \in N^*$. Nếu trái lại $n \notin A \rightarrow n = Ax_2 + By_2, x_2, y_2 \in N^* \rightarrow AB = m - A - B + n = Ax_1 + By_1 - A - B + Ax_2 + By_2 = A(x_1 + x_2 - 1) + B(y_1 + y_2 - 1) \rightarrow AB \notin \mathcal{A}$. Mâu thuẫn với i). Ta có với $1 \leqslant n \leqslant A + B - 1 \rightarrow n \in \mathcal{A}$. Xét $n \in I = [A + B; AB]$. Ánh xạ $f : I \rightarrow I$ cho bởi $f(n) = AB + A + B - n$ là một song ánh và $n \in \mathcal{A} \Leftrightarrow f(n) \notin \mathcal{A}$ .Vậy $|I \cap \mathcal{A}| = |I|/2 = (AB - A - B + 1)/2$. Thành thử

$$|\mathcal{A}| = A + B - 1 + \frac{AB - A - B + 1}{2} = \frac{AB + A + B - 1}{2}$$

Bài toán 4 Cho $A_1, ..., A_k \in N^*, (A_1, ..., A_k) = 1$. Ký hiệu $\mathcal{A}$ là tập các số $n \in N^*$ sao cho phương trình

$$\sum_{i=1}^{k} A_k x_k = n$$

không có nghiệm nguyên dương.Chứng minh rằng $\mathcal{A}$ là tập hữu hạn và

$$|\mathcal{A}| \leqslant (k - 1)A_1...A_k$$

Giải Ta chứng minh quy nạp rằng:

Nếu $n > (k - 1)A_1...A_k$ *thì* $n \notin \mathcal{A}$

Với $k = 2$ khẳng định đúng (bài toán 3). Giả sử đúng với k. Không giảm tổng quát giả sử $A_1 \leqslant A_2 \leqslant ... \leqslant A_{k+1}$. Đặt $d = (A_1, ..., A_k), B_i = A_i/d$. Khi đó $(d, A_{k+1}) = 1, (B_1, \ldots, B_k) = 1$. Do $(d, A_{k+1}) = 1$ nên tồn tại $x_{k+1}, y \in Z$ với $1 \leqslant x_{k+1} \leqslant d$ sao cho

$$dy + A_{k+1}x_{k+1} = n$$

Ta chứng minh

$$y > (k - 1)B_1...B_k \quad (7)$$

Ta có $y > (k-1)B_1...B_k \Leftrightarrow dy > (k-1)dB_1...B_k \Leftrightarrow n > (k-1)dB_1...B_k + A_{k+1}x_{k+1}$.
Vì $x_{k+1} \leqslant d$ nên chỉ cần chứng minh

$$n > (k-1)B_1...B_k d + A_{k+1}d \quad (8)$$

Thật vậy do $A_i = dB_i \rightarrow A_{k+1} \geq A_i \geq d, A_i \geq B_i (i = 1, 2, ..k)$ nên

$$A_1...A_kA_{k+1} \geq A_1...A_kd \geq B_1...B_kd$$

$$A_1...A_kA_{k+1} \geq A_kA_{k+1} \geq dA_{k+1}$$

$$\rightarrow kA_1...A_kA_{k+1} = (k-1)A_1...A_kA_{k+1} + A_1...A_kA_{k+1}$$

$$\geq (k-1)B_1...B_kd + A_{k+1}d$$

$$\rightarrow n > kA_1...A_kA_{k+1} \geq (k-1)B_1...B_kd + A_{k+1}d$$

Vậy (8) do đó (7) được chứng minh. Theo quy nạp tồn tại $x_1, ..., x_k \in N^*$ sao cho

$$\sum_{i=1}^{k} B_kx_k = y \rightarrow \sum_{i=1}^{k} A_kx_k = dy$$

$$\rightarrow \sum_{i=1}^{k} A_kx_k + A_{k+1}x_{k+1} = dy + A_{k+1}x_{k+1} = n$$

$$\rightarrow \sum_{i=1}^{k+1} A_kx_k = n$$

Đặt

$$M(A_1, \ldots, A_k) = \max \mathcal{A}$$

$$G(A_1, \ldots, A_k) = |\mathcal{A}|$$

Ở bài toán 3 ta có

$$M(A_1, A_2) = A_1A_2$$

$$G(A_1, A_2) = \frac{A_1A_2 + A_1 + A_2 - 1}{2}$$

Từ bài toán 3 và 4 suy ra $M(A_1,\ldots,A_k) \leqslant (k-1)A_1...A_k$ và dấu bằng xảy ra với $k=2$. Tuy nhiên với $k>2$ dấu bằng không xẩy ra . Biểu thức tưởng minh biểu diễn $M(A_1,\ldots,A_k)$ và $G(A_1,\ldots,A_k)$ theo $A_1,...,A_k$ vẫn chưa biết trong trường hợp tổng quát.

Bài toán 5 Giả sử $A=bc, B=ca, C=ab$ trong đó $a,b,c \in N^*$ đôi một nguyên tố cùng nhau. Chứng minh rằng

$$i) M(A,B,C) = 2\sqrt{ABC}$$

$$ii) G(A,B,C) = \frac{2\sqrt{ABC}+A+B+C-1}{2}$$

Giải i) Chứng minh $2\sqrt{ABC} \in \mathcal{A}$: Giả sử trái lại $2\sqrt{ABC} \notin \mathcal{A}$. Tồn tại $x,y,z \in N^*$ sao cho $Ax+By+Bz = 2\sqrt{ABC} \Leftrightarrow bcx+acy+abz = 2abc \rightarrow abz = 2abc-c(bx+ay) \rightarrow c|abz \rightarrow c|z \rightarrow z \geq c$. Tương tự $y \geq b; x \geq a$. Vậy $2abc = bcx+cay+abz \geq 3abc$. Mâu thuẫn. Tiếp theo ta chứng minh nếu $n > 2\sqrt{ABC} = 2abc$ thì $n \notin \mathcal{A}$. Do $n > abc, (ab,c) = 1$ nên theo bài toán 3 tồn tại $1 \leqslant z \leqslant c, t \in N^*$ sao cho $ct+abz = n$. Ta có $ct = n-abz > 2abc-abc = abc \rightarrow t > ab$. Theo bài toán 3 tồn tại $x,y \in N^*$ sao cho $t = bx+ay$. Từ đó $n = ct+abz = c(bx+ay)+abz = bcx+acy+abz \rightarrow n \notin \mathcal{A}$.

ii) Xét $n \leqslant 2\sqrt{ABC} = 2abc$. Ta chứng minh $n \in \mathcal{A}$ nếu và chỉ nếu $m = 2abc+bc+ca+ab-n \notin \mathcal{A}$. Vì $\{bcx\}_{x=1}^{a}$ là hệ đầy đủ (mod a) nên tồn tại $1 \leqslant x \leqslant a$ sao cho $bcx \equiv n \pmod{a} \rightarrow n = bcx+at, t \in Z$.Vì $\{cy\}_{y=1}^{b}$ là hệ đầy đủ (mod b) nên tồn tại $1 \leqslant y \leqslant b$ sao cho $cy \equiv t \pmod{b} \rightarrow t = cy+bz, z \in Z$. Thành thử với mỗi $n \in N^*$ có biểu diễn

$$n = bcx+acy+abz \quad 1 \leqslant x \leqslant a, 1 \leqslant x \leqslant b, z \in Z$$

Nếu $n \in \mathcal{A}$ thì $z \leq 0$. Vậy $m = 2abc+bc+ca+ab-n = 2abc+bc+ca+ab-bcz-acy-abz = bc(a+1-x)+ac(b+1-y)+ab(1-z) = Ax_1+By_1+Cz_1$ ở đó $x_1 = a+1-x \geq 1, y_1 = b = 1-1 \geq 1, z_1 = 1-z \geq 1$. Vậy $m \notin \mathcal{A}$.

Đảo lại giả sử $m \notin \mathcal{A} \to m = bcx_1 + acy_1 + abz_1, x_1, y_1, z_1 \in N^*$. Nếu trái lại $n \notin A \to n = bcx_2 + acy_2 + abz_2, x_2, y_2, z_2 \in N^* \to 2abc = m - bc - ca - ab + n = bcx_1 + acy_1 + abz_1 - bc - ca - ab + bcx_2 + cay_2 + abz_2 = bc(x_1 + x_2 - 1) + ca(y_1 + y_2 - 1) + ab(z_1 + z_2 - 1) \to 2abc \notin \mathcal{A}$. Mâu thuẫn với i).

Ta có với $1 \leqslant n \leqslant bc + ca + ab - 1 \to n \in \mathcal{A}$. Xét $n \in I = [bc + ca + ab; 2abc]$. Ánh xạ $f : I \to I$ cho bởi $f(n) = 2abc + bc + ca + ab - n - n$ là một song ánh và $n \in \mathcal{A} \Leftrightarrow f(n) \notin \mathcal{A}$ .Vậy $|I \cap \mathcal{A}| = |I|/2 = (2abc - bc - ca - ab + 1)/2$. Thành thử

$$\begin{aligned} |\mathcal{A}| &= bc + ca + ab - 1 + \frac{2abc - bc - ca - ab + 1}{2} \\ &= \frac{2abc + bc + ca + ab - 1}{2} \\ &= \frac{2\sqrt{ABC} + A + B + C - 1}{2} \end{aligned}$$

2.3 Bài tập

1. Cho $a, b \in N^*$ với $(a, b) = 1$. Chứng minh rằng phương trình $ax + by = 1$ có vô số nghiệm (x, y) với $(x, a) = (y, b) = 1$

2. Tìm tất cả nghiệm nguyên của phương trình

$$6x + 45y + 6z - 10t = 13$$

3. Cho các số nguyên dương a, b thỏa mãn điều kiện $5a \geq 7b$. Chứng tinh rằng tồn tại các số tự nhiên x, y, z, t sao cho $x + 2y + 3z + 7t = a$ và $y + 2z + 5t = b$.

4. Chứng minh rằng

   i) $M(2, 4, 5) = 14$

   ii) $M(7, 8, 9) = 44$

5. Chứng minh rằng nếu $A \leqslant B \leqslant C$ thì

$$M(A,B,C) \leqslant AC + B$$

6. Cho $a_1, a_2, ..., a_k$ là các số nguyên dương đôi một nguyên tố cùng nhau. Đặt $A = a_1...a_k$ và

$$A_i = \frac{A}{a_i}$$

Chứng minh rằng

$$M(A_1, ..., A_k) = (k-1)\sqrt[k-1]{A_1 A_2 ... A_k}$$

3 Phương trình Pell

3.1 Phương trình Pell loại 1

Phương trình Pell loại 1 là phương trình có dạng

$$x^2 - Dy^2 = 1 \qquad \text{(I)}$$

trong đó $D \in N^*$ và ta yêu cầu tìm nghiệm $x, y \in N^*$. Trong tiết này khi nói đến nghiệm của (I) ta hiểu là nghiệm nguyên dương

Định lý 1(Điều kiện tồn tại nghiệm). Phương trình (I) có nghiệm nguyên dương khi và chỉ khi D là số không chính phương.

Chứng minh Giả sử $D = m^2$. Khi đó

$$x^2 - Dy^2 = x^2 - m^2y^2 = 1 \to (x - my)(x + my) = 1$$

$$\to x - my = x + my = 1 \to x = 1, y = 0$$

Vậy (I) không có nghiệm nguyên dương.

Ngược lại giả sử Dlà số không chính phương. Ta có các bổ đề sau

Bổ đề 1 Cho $\alpha \notin Q$. Khi đó tồn tại vô số cặp số nguyên (h, k) với$k > 0$ sao cho

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

Chứng minh Ta sử dụng nhận xét đã biết sau: Với mỗi$q \in N^*$ tồn tại cặp số nguyên (h, k) với $1 \leqslant k \leqslant q$ sao cho

$$\left|a - \frac{h}{k}\right| < \frac{1}{kq}$$

Ký hiệu

$$A = \{(h, k) : \left|\alpha - \frac{h}{k}\right| < \frac{1}{k^2}\}.$$

Ta phải chứng minh $|A| = \infty$. Giả sử trái lại $|A| < \infty$. Khi đó tồn tại ϵ sao cho $\left|\alpha - \frac{h}{k}\right| > \epsilon$ với mọi $(h, k) \in A$. Chọn $q \in N^*$ sao cho

$$\frac{1}{q} < \epsilon. \tag{1}$$

Theo nhận xét trên tồn tại cặp số nguyên (h_0, k_0) với $1 \leqslant k_0 \leqslant q$ sao cho

$$\left|\alpha - \frac{h_0}{k_0}\right| < \frac{1}{k_0 q} \leqslant \frac{1}{k_0^2} \tag{2}$$

Từ (2) ta có $(h_0, k_0) \in A \rightarrow \left|\alpha - \frac{h_0}{k_0}\right| > \epsilon$. Nhưng $\frac{1}{q} \geq \frac{1}{k_0 q} > \left|\alpha - \frac{h_0}{k_0}\right| > \epsilon$. Mâu thuẫn với (1).

Bổ đề 2 Tồn tại vô số cặp số nguyên dương (x, y) sao cho

$$|x^2 - Dy^2| < 1 + 2\sqrt{D}$$

Chứng minh. Theo bổ đề 1 tồn tại vô số cặp số nguyên (x, y) sao cho

$$0 < \left|\sqrt{D} - \frac{x}{y}\right| < \frac{1}{y^2}.$$

Suy ra

$$\left|\frac{x}{y} + \sqrt{D}\right| = \left|\frac{x}{y} - \sqrt{D} + 2\sqrt{D}\right| < \frac{1}{y^2} + 2\sqrt{D}$$

Vậy

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

Chứng minh định lý Từ bổ đề 2 (x, y) tồn tại vô số cặp số nguyên dương (x, y) sao cho

$$|x^2 - Dy^2| < 1 + 2\sqrt{D}$$

Đặt $I = [-1 - 2\sqrt{d}; 1 + 2\sqrt{d}]$. Với mỗi $k \in I$ ký hiệu

$$A_k = \{(x, y) \in N^* : x^2 - Dy^2 = k\}$$

Do đó tồn tại $k \in I$ để $|A_k| = \infty$. Suy ra tồn tại $(x_1, y_1) \neq (x_1, y_1) \in A_k$ để

$$x_1 \equiv x_2 \pmod{|k|} \quad y_1 \equiv y_2 \pmod{|k|}$$
$$x_1^2 - Dy_1^2 = x_2^2 - Dy_2^2 = k$$

Xét tích

$$(x_1 - y_1\sqrt{D})(x_2 + y_2\sqrt{D}) = x_1x_2 - Dy_1y_2 + \sqrt{D}(x_1y_2 - x_2y_1) \tag{3}$$

Vì

$$x_1x_2 - Dy_1y_2 \equiv x_1^2 - Dy_1^2 \equiv 0 \pmod{|k|}$$
$$x_1y_2 - x_2y_1 \equiv x_1y_1 - x_1y_1 \equiv 0 \pmod{|k|}$$

Vậy tồn tại $u, v \in Z$ sao cho

$$x_1x_2 - Dy_1y_2 = ku \tag{4}$$
$$x_1y_2 - Dy_1x_2 = kv \tag{5}$$

Từ (3), (4), (5) suy ra

$$(x_1 - y_1\sqrt{D})(x_2 + y_2\sqrt{D}) = k(u + v\sqrt{D})$$
$$(x_1 + y_1\sqrt{D})(x_2 - y_2\sqrt{D}) = k(u - v\sqrt{D})$$

Nhân hai đẳng thức trên với nhau và chú ý rằng $(x_1, y_1), (x_2, y_2) \in A_k \rightarrow$ $x_1^2 - dy_1^2 = x_2^2 - dy_2^2 = k$ ta được

$$k^2 = k^2(u^2 - Dv^2) \longrightarrow \quad u^2 - Dv^2 = 1$$

Ta chứng minh $u, v > 0$. Rõ ràng $u > 0$. Nếu trái lại $v = 0$ thì $u = \pm 1 \rightarrow$ $(x_1 - y_1\sqrt{D})(x_2 + y_2\sqrt{D}) = \pm k = \pm(x_1^2 - Dy_1^2) = \pm(x_1 - y_1\sqrt{D})(x_1 + y_1\sqrt{D}) \rightarrow$ $x_2 + y_2\sqrt{D} = x_1 + y_1\sqrt{D} \longrightarrow x_1 = x_2, y_1 = y_2$ Ta có mâu thuẫn. Vậy (u, v) là nghiệm nguyên dương của phương trình (I)

Định lý 2(Công thức nghiệm) Ký hiệu (a, b) là nghiệm nhỏ nhất của phương trình

$$x^2 - Dy^2 = 1$$

Khi đó dãy (x_n, y_n) cho bởi

$$x_n = \frac{(a + b\sqrt{D})^n + (a - b\sqrt{D})^n}{2}$$
$$y_n = \frac{(a + b\sqrt{D})^n - (a - b\sqrt{D})^n}{2\sqrt{D}}$$

cho ta tất cả các nghiệm của (I).

Dãy nghiệm (x_n, y_n) cũng có thể xác định theo công thức truy hồi sau

$$x_0 = 1, x_1 = a, x_{n+2} = 2ax_{n+1} - x_n \tag{6}$$
$$y_0 = 0, y_1 = b, y_{n+2} = 2ay_{n+1} - y_n \tag{7}$$

Chứng minh. Ta có

$$x_n + y_n\sqrt{D} = (a + b\sqrt{d})^n, x_n - y_n\sqrt{D} = (a - b\sqrt{D})^n. \tag{8}$$

Suy ra $(x_n^2 - Dy_n^2) = (a^2 - Db^2)^n = 1$.

Đảo lại giả sử (x, y) là nghiệm bất kỳ của (I). Ta chứng minh tồn tại $n \in N^*$ để $x = x_n; y = y_n$. Vì D không chính phương nên điều này tương đương

Tồn tại $n \in N^*$ để

$$x + y\sqrt{D} = x_n + y_n\sqrt{D} = (a + b\sqrt{D})^n$$

Chứng minh bằng phản chứng. Giả sử trái lại

$$x + y\sqrt{D} \neq (a + b\sqrt{D})^n \quad \forall n \in N^*$$

Khi đó tồn tại $m \in N^*$ sao cho

$$(a + b\sqrt{D})^m < x + y\sqrt{D} < (a + b\sqrt{D})^{m+1}$$

Nhân hai vế với $(a - b\sqrt{D})^m$ ta được

$$1 < (x + y\sqrt{D})(a - b\sqrt{D})^m < a + b\sqrt{D}$$

Do (8) ta có

$$\begin{aligned}(x + y\sqrt{D})(a - b\sqrt{D})^m &= (x + y\sqrt{D})(x_m - y_m\sqrt{D}) \\ &= (xx_m - Dyy_m) + (x_my - y_mx)\sqrt{D} \\ &= u + v\sqrt{D}\end{aligned}$$

ở đó $u = xx_m - Dyy_m, v = x_my - y_mx$. Vậy

$$1 < u + v\sqrt{d} < a + b\sqrt{d}. \tag{9}$$

Ta có

$$\begin{aligned}u^2 - Dv^2 &= (xx_m - Dyy_m)^2 - D(x_my - y_mx)^2 \\ &= (x^2 - Dy^2)(x_m^2 - Dy_m^2) = 1\end{aligned}$$

Lại có $x > y\sqrt{d}, x_m > y_m\sqrt{d}$ nên $u > 0$. Lại có $(u - v\sqrt{D})(u + v\sqrt{D}) = 1$ và $1 < u + v\sqrt{d}$ nên $0 < u - v\sqrt{d} < 1 < u + v\sqrt{d} \to v > 0$. Vậy (u, v) là nghiệm của (I) do đó $a \leqslant u, b \leqslant v \to a + b\sqrt{d} \leqslant u + v\sqrt{d}$ trái với (9).Định lý được chứng minh.

Từ định lý trên ta thấy việc tìm nghiệm của phương trình Pell (I) quy về tìm nghiệm nhỏ nhất (a, b) của nó. Cách đơn giản nhất là thử bằng tay: Thay lần lượt $y = 1, 2, ..$ vào biểu thức $1 + Dy^2$ cho tới khi nào được số chính phương thì dừng lại. Vì phương trình (I) có nghiệm nên chắc chắn quá trình này sẽ dừng lại sau b phép thử. Khi đó nghiệm nhỏ nhất là (a, b) với $a = \sqrt{1 + Db^2}$. Nếu nghiệm nhỏ nhất b này lớn thì cách thử này không khả thi. Thí dụ với phương trình $x^2 - 61y^2$ thì cặp nghiệm nhỏ nhất là

$$a = 1766319049$$

$$b = 226153980$$

Sau đây ta sẽ trình bày một thuật toán sử dụng liên phân số để tìm một nghiệm nhỏ nhất (a, b) của (I).

Định nghĩa Cho $a_0, a_1, a_2, ...$ là dãy số nguyên trong đó $a_i > 0, i \geq 1$. Đặt

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

Khi đó tồn tại giới hạn

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

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

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

Định lý $\alpha = [a_0; a_1, a_2, ...]$ là một số vô tỷ . Ngược lại mỗi số vô tỷ đều biểu diễn duy nhất dưới dạng một liên phân số vô hạn.

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

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

Nếu D là số không chính phương, biểu diễn liên phân số của $\sqrt{D}$ được cho bởi

Định lý Biểu diễn liên phân số của $\sqrt{D}$ là tuần hoàn và có dạng

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

với $a = [\sqrt{D}]$. Hơn nữa có công thức tường minh để xác định dãy $(a_1, \ldots, a_n)$. Chú ý rằng dãy $(a_1, \ldots, a_n)$ là đối xứng tức là

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

Ví dụ

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

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

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

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

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

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

Định lý 3 Cho phương trình Pell

$$x^2 - Dy^2 = 1. \quad (I)$$

- Biểu diễn $\sqrt{D}$ thành liên phân số

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

- Nếu chu kỳ n là số chẵn ta tính giản phân thứ $n-1$

$$C_{n-1} = \frac{p_{n-1}}{q_{n-1}}$$

Khi đó (p_{n-1}, q_{n-1}) là nghiệm nhỏ nhất của (I)

- Nếu chu kỳ n là số lẻ ta tính giản phân thứ $2n-1$.

$$C_{2n-1} = \frac{p_{2n-1}}{q_{2n-1}}$$

Khi đó (p_{2n-1}, q_{2n-1}) là nghiệm nhỏ nhất của (I)

Ví dụ Tìm nghiệm nhỏ nhất của phương trình $x^2 - 14y^2 = 1$. Ta có $\sqrt{14} = [3; \overline{1, 2, 1, 6}]$. Chu kỳ $n = 4$ là số chẵn. Vậy ta tính giản phân

$$C_3 = [3, 1, 2, 1] = 3 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1}}} = \frac{15}{4}$$

Vậy nghiệm nhỏ nhất là $(15, 4)$

Ví dụ Tìm nghiệm nhỏ nhất của phương trình $x^2 - 13y^2 = 1$. Ta có $\sqrt{13} = [3; \overline{1, 1, 1, 1, 6}] = [3, 1, 1, 1, 1, 6, 1, 1, 1, 1, 6, ...$ Chu kỳ $n = 5$ là số lẻ. Vậy ta tính

giản phân

$$C_9 = [3, 1, 1, 1, 1, 6, 1, 1, 1, 1]$$

$$= 3 + \cfrac{1}{1 + \cfrac{1}{1 + \ddots + \cfrac{1}{1 + \cfrac{1}{1}}}}$$

$$= \frac{649}{180}$$

Vậy nghiệm nhỏ nhất là $(649, 180)$

Trở lại phương trình $x^2 - 61y^2 = 1$. Ta có

$$\sqrt{76} = [7; \overline{1, 4, 3, 1, 2, 2, 1, 3, 4, 1, 14}]$$

Chu kỳ $n = 11$ là số lẻ. Ta tính giản phân

$$C_{21} = [7, 1, 4, 3, 1, 2, 2, 1, 3, 4, 1, 14, 1, 4, 3, 1, 2, 2, 1, 3, 4, 1]$$

$$= 7 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{3 + \ddots + \cfrac{1}{4 + \cfrac{1}{1}}}}}$$

$$= \frac{1766319049}{226153980}$$

Vậy nghiệm nhỏ nhất là $(1766319049, 226153980)$

3.2 Phương trình Pell loại 2

Phương trình Pell loại 2 là phương trình

$$x^2 - Dy^2 = -1 \qquad \text{(II)}$$

ở đó $D \in N^*$. Nghiệm của (II) luôn được hiểu là nghiệm nguyên dương.

Định lý 1 Điều kiện cần để (II) có nghiệm là D không là số chính phương và D không có ước nguyên tố dạng $4k+3$.

Chứng minh i)) Nếu $D = m^2$ thì (II) trở thành $(my-x)(my+x) = 1 \to my-x = my+x = 1 \to x = 0$ Vậy (II) vô nghiệm.

ii) Nếu D có ước nguyên tố $p = 4k+3$: Giả sử (x, y) là nghiệm. Khi đó $x^2+1 = Dy^2 \to p|x^2+1$. Vì$p = 4k+3$ nên$p|1$. Mâu thuẫn.

Tuy nhiên , đây không là điều kiện đủ.

Định lý 2 Nếu $D = p$ là số nguyên tố thì (II) có nghiệm khi và chỉ khi $p = 2$ hoặc $p \neq 4k+3$.

Chứng minh. Nếu (II) có nghiệm thì từ Định lý 1 suy ra $p = 2$ hoặc $p \neq 4k+3$. Dảo lại nếu $p = 2$ thì phương trình $x^2 - 2y^2 = -1$ có nghiệm $(x, y) = (1; 1)$. Xét $p \equiv 1 \pmod 4$. Xét phương trình Pell loại I

$$x^2 - Dy^2 = 1 \qquad (10)$$

Gọi (a, b) là nghiệm nhỏ nhất của (10). Ta có $a^2 - 1 = pb^2$. Nếu a chẵn thì b lẻ do đó $b^2 \equiv 1 \pmod 4 \to a^2 \equiv 1+p \equiv 2 \pmod 4$. Mâu thuẫn . Vậy a lẻ, b chẵn. Đặt $a = 2a_1+1, b = 2b_1$. Ta có $(a-1)(a+1) = pb^2 \Leftrightarrow a_1(a_1+1) = pb_1^2$. Do p nguyên tố và $(a_1, a_1+1) = 1$ nên $a_1 = u^2, a_1+1 = pv^2$ hoặc $a_1 = pu^2, a_1+1 = v^2$. Nếu $a_1 = u^2, a_1+1 = pv^2 \to u^2 - pv^2 = -1$. Vậy (II) có nghiệm (u, v).

Nếu $a_1 = pu^2, a_1+1 = v^2 \to v^2 - pu^2 = 1$. Vậy (v, u) là nghiệm của (10)). Suy ra $v \geq a \to a_1+1 = v^2 \geq v \geq a = 2a_1+1$. Mâu thuẫn .

Định lý 3 Gọi (a, b) là nghiệm nhỏ nhất của (10) . Khi đó (II) có nghiệm khi và chỉ khi

$$\begin{cases} a = x^2 + Dy^2 \\ b = 2xy \end{cases} \tag{11}$$

có nghiệm nguyên dương.

Hơn nữa nếu (11) hệ có nghiệm nó sẽ có nghiệm duy nhất.Nghiệm duy nhất (x_1, y_1) này chính là nghiệm nhỏ nhất của (II)

Chứng minh. 1) Giả sử (II) có nghiệm. Gọi (x_1, y_1) là nghiệm nhỏ nhất của (II). Đặt $u = x_1^2 + Dy_1^2, v = 2x_1, y_1$. Ta chứng minh $u = a, v = b$ do đó (x_1, y_1) chính là nghiệm của (11). Ta có $u^2 - Dv^2 = (x_1^2 - Dy_1^2)^2 = 1$ Vậy (u, v) là nghiệm của (10) . Suy ra $u \geq a; v \geq b$. Ta có

$$(a^2 - Db^2)(x_1 - Dy_1^2) = 1(-1) = -1$$

$$\Leftrightarrow (ax_1 - Dby_1)^2 - D(ay_1 - bx_1)^2 = -1.$$

Dễ thấy $(ax_1 - Dby_1)^2 > 0, (ay_1 - bx_1)^2 > 0$. Do (x_1, y_1) là nghiệm của (II) nên

$$(ax_1 - Dby_1)^2 \geq x_1^2 \Leftrightarrow a^2x_1^2 + D^2b^2y_1^2 - x_1^2 \geq 2abDx_1y_1$$

$$\rightarrow x_1^2(a^2 - 1) + D^2b^2y_1^2 \geq 2abDx_1y_1$$

$$\rightarrow x_1^2Db^2 + D^2b^2y_1^2 \geq 2abDx_1y_1$$

$$\rightarrow b(x_1^2 + Dy_1^2) \geq 2ax_1y_1 \rightarrow bu \geq av$$

$$\rightarrow b^2u^2 \geq a^2v^2 \rightarrow b^2(Dv^2 + 1) \geq v^2(Db^2 + 1)$$

$$\rightarrow b \geq v \rightarrow b = v \rightarrow u = a$$

2) Đảo lại giả sử (u, v) là nghiệm của (11). Ta có $a^2 - Db^2 = 1 \Leftrightarrow (u^2 + Dv^2)^2 - D(2uv)^2 = (u^2 - Dv^2)^2 = 1$. Vậy $u^2 - Dv^2 = 1$ hoặc $u^2 - Dv^2 = -1$. Nếu $u^2 - Dv^2 = 1$ thì (u, v) là nghiệm của (10) do đó $u \geq a = u^2 + Dv^2$. Mâu thuẫn. Vậy $u^2 - Dv^2 = -1$ do đó (II) có nghiệm (u, v)

Tiếp theo ta chứng minh (u, v) là nghiệm nhỏ nhất của (II).Giả sử (x_1, y_1) là nghiệm nhỏ nhất của (II). Theo chứng minh ở 1) ta có $a = u^2 + Dv^2 = x_1^2 + Dy_1^2; b = 2uv = 2x_1y_1 \to u^2 + Dv^2 + 2uv = x_1^2 + Dy_1^2 + 2x_1y_1 \to (u + v\sqrt{D})^2 = (x_1 + y_1\sqrt{D})^2 \to u = x_1; v = y_1$. Định lý được chứng minh.

Ví dụ là một áp dụng của định lý 2. Nó cũng chỉ ra rằng điều kiện của định lý 1 chỉ là điều kiện cần.

Ví dụ Chứng minh rằng phương trình $x^2 - 34y^2 = -1$ vô nghiệm (Ở đây $34 = 2.17$ không là số chính phương và cũng không có ước nguyên tố dạng $4k + 3$).

Giải Phương trình $x^2 - 34y^2 = 1$ có nghiệm nhỏ nhất là$(a; b) = (35; 6)$. Xét hệ

$$\begin{cases} 35 = x^2 + 34y^2 \\ 6 = 2xy \end{cases}$$

Từ phương trình thứ nhất của hệ suy ra $(x; y) = (1; 1)$. Tuy nhiên $(1; 1)$ không thỏa mãn phương trình thứ hai. Vậy hệ vô nghiệm do đó theo định lý 2 phương trình $x^2 - 34y^2 = -1$ vô nghiệm.

Ta thừa nhận định lý sau

Định lý 3 Phương trình Pell loại 2

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

có nghiệm khi và chỉ khi trong biểu diễn $\sqrt{D}$ thành liên phân số

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

chu kỳ n là số lẻ. Trong trường hợp đó (p_{n-1}, q_{n-1}) là nghiệm nhỏ nhất của phương trình,ở đó

$$C_{n-1} = \frac{p_{n-1}}{q_{n-1}}$$

là giản phân thứ $n-1$.

Ví dụ

i)Xét phương trình $x^2 - 13y^2 = -1$. Ta có $\sqrt{13} = [3; \overline{1, 1, 1, 1, 6}]$. Chu kỳ $n = 5$ là số lẻ. Vậy phương trình có nghiệm. Ta tính giản phân

$$C_4 = [3, 1, 1, 1, 1]$$

$$= 3 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1}}}}$$

$$= 3 + \frac{3}{5} = \frac{18}{5}$$

Vậy nghiệm nhỏ nhất là $(18, 5)$

ii)Xét phương trình $x^2 - 34y^2 = -1$. Ta có $\sqrt{34} = [5; \overline{1, 4, 1, 10}]$. Chu kỳ $n = 4$ là số chẵn. Vậy phương trình vô nghiệm.

Định lý 4 (Công thức nghiệm) Giả sử phương trình Pell loại 2

$$x^2 - Dy^2 = -1 \quad (II)$$

có nghiệm. Gọi (α, β) là nghiệm nhỏ nhất của nó. Khi đó dãy $(x_n, y_n)_{n=1}^{\infty}$ cho bởi

$$x_n = \frac{(\alpha + \beta\sqrt{D})^{2n-1} + (\alpha - \beta\sqrt{D})^{2n-1}}{2}$$

$$y_n = \frac{(\alpha + \beta\sqrt{D})^{2n-1} - (\alpha - \beta\sqrt{D})^{2n-1}}{2\sqrt{D}}$$

cho ta tất cả các nghiệm của (II).

*Chứng minh*Giả sử (x_n, y_n) cho bởi công thức trên. Khi đó

$$x_n + y_n\sqrt{D} = (\alpha + \beta\sqrt{D})^{2n-1}$$

$$x_n - y_n\sqrt{D} = (\alpha - \beta\sqrt{D})^{2n-1}$$

$$\rightarrow x_n^2 - Dy_n^2 = (\alpha^2 - D\beta^2)^{2n-1} = -1$$

Ngược lại giả sử (x, y) là một nghiệm của (II). Ta có

$$(x + y\sqrt{D})(\alpha + \beta\sqrt{D}) = (x\alpha + Dy\beta) + (y\alpha + x\beta)\sqrt{D}$$

$$= s + t\sqrt{D}$$

$$\text{ở đó } s = x\alpha + Dy\beta, t = y\alpha + x\beta$$

$$\rightarrow s^2 - Dt^2 = (x\alpha + Dy\beta)^2 - D(y\alpha + x\beta)^2$$

$$= (x^2 - Dy^2)(\alpha^2 - D\beta^2) = (-1)(-1) = 1$$

Vậy (s, t) là nghiệm của phương trình Pell loại 1 $s^2 - Dt^2 = 1$. Goi (a, b) là nghiệm nhỏ nhất của nó.Theo công thức nghiệm của phương trình Pell loại 1 và định lý 3 tồn tại $n \in N^*$ sao cho

$$(x + y\sqrt{D})(\alpha + \beta\sqrt{D}) = s + t\sqrt{D} = (a + b\sqrt{D})^n$$

$$= (\alpha^2 + D\beta^2 + 2\alpha\beta\sqrt{D})^n = (\alpha + \beta\sqrt{D})^2)^n$$

$$= (\alpha + \beta\sqrt{D})^{2n}$$

$$\rightarrow x + y\sqrt{D} = (\alpha + \beta\sqrt{D})^{2n-1} = x_n + y_n\sqrt{D}$$

$$\rightarrow x = x_n, y = y_n$$

3.3 Một số bài toán chọn lọc

Bài toán 6 Số nguyên dương S được gọi là số Heron nếu nó là diện tích của một tam giác có ba cạnh là ba số nguyên liên tiếp. Chứng minh rằng S

là số Heron khi và chỉ khi S khi là số hạng của dãy $(S_n), n \geq 1$ xác định bởi

$$S_0 = 0, S_1 = 6, S_2 = 84, S_{n+2} = 14S_{n+1} - S_n$$

Giải Gọi S là diện tích của tam giác có ba cạnh là $x-1, x, x+1$ với $x > 2, x \in N^*$. Theo công thức Heron

$$S = \frac{1}{4}x\sqrt{3(x^2-4)} \longrightarrow 16S^2 = 3x^2(x^2-4). \tag{12}$$

Vậy S là số Heron khi và chỉ khi phương trình (12) có nghiệm nguyên dương (S, x). Dễ thấy x phải chẵn . Đặt $x = 2y$ ta có

$$16S^2 = 3x^2(x^2-4) \Leftrightarrow S^2 = 3y^2(y^2-1)$$

$$\longrightarrow S = y\sqrt{3(y^2-1)} \longrightarrow 3(y^2-1) = h^2$$

$$\longrightarrow h = 3z \longrightarrow 3(y^2-1) = 9z^2$$

$$\longrightarrow y^2 - 3z^2 = 1, S = 3yz$$

Ngược lại nếu (y, z) là nghiệm của phương trình Pell

$$y^2 - 3z^2 = 1 \tag{13}$$

thì $x = 2y, y > 1, S = 3yz$ là nghiệm của (12)(12) Nghiệm nhỏ nhất của (13) là $(2, 1)$ Vậy tất cả nghiệm của $(13)(y_n, z_n)$ cho bởi

$$y_n = \frac{(2+\sqrt{3})^n + (2-\sqrt{3})^n}{2}$$

$$z_n = \frac{(2+\sqrt{3})^n - (2-\sqrt{3})^n}{2\sqrt{3}}$$

Do đó

$$S_n = 3y_n z_n = \frac{\sqrt{3}}{4}((7+4\sqrt{3})^n - (7-4\sqrt{3})^n)$$

$$\rightarrow S_{n+2} = 14S_{n+1} - S_n, S_0 = 0, S_1 = 6, S_2 = 84$$

Bài toán 7 Tìm tất cả các số nguyên dương n sao cho $2n+1$ và $3n+1$ đều là số chính phương.

Giải Vì $(2n+1, 3n+1) = 1$ nên $2n+1$ và $3n+1$ đều là số chính phương khi và chỉ khi $(2n+1)(3n+1) = y^2, y \in N^*$ Suy ra $(12n+5)^2 - 24y^2 = 1$. Đặt $x = 12n+5$ ta có $x^2 - 24y^2 = 1$. Gọi (x_k, y_k) là nghiệm của nó. Nghiệm nhỏ nhất của phương trình Pell này là $(5, 1)$. Do đó (x_k) cho bởi hệ thức

$$x_0 = 1, x_1 = 5, x_{k+2} = 10x_{k+1} - x_k.$$

Dễ chứng minh $x_k \equiv 5 \pmod{12}$ khi và chỉ khi k lẻ. Vậy $n = n_k, k \geq 1$ ở đó

$$n_k = \frac{x_{2k+1} - 5}{12}.$$

Ta xác định hệ thức truy hồi của dãy (n_k)

Đặt $u_k = x_{2k+1} = 12n_k + 5$. Ta có

$$x_{2k+3} = 10x_{2k+2} - x_{2k+1} = 10(10x_{2k+1} - x_{2k}) - x_{2k+1}$$

$$= 100x_{2k+1} - 10x_{2k} - x_{2k+1} = 99x_{2k+1} - x_{2k+1} - x_{2k-1}$$

$$= 98x_{2k+1} - x_{2k-1}$$

$$\rightarrow u_{k+2} = 98u_{k+1} - u_k$$

$$\Leftrightarrow 12n_{k+2} + 5 = 98(12n_{k+1} + 5) - 12n_k - 5$$

$$n_{k+2} = 98n_{k+1} - n_k + 40$$

với $n_1 = 40, n_2 = 3960$

Bài toán 8 Cho dãy (x_n, y_n) xác định như sau $(x_0, y_0) = (0, 1), (x_1, y_1) = (3, 5)$ và

$$\begin{cases} x_{n+1} &= 3x_n + 2y_n + 1 \\ y_{n+1} &= 4x_n + 3y_n + 2 \end{cases} \tag{14}$$

Chứng minh rằng (x_n, y_n) là tất cả các nghiệm nguyên dương của phương trình

$$x^2 + (x+1)^2 = y^2$$

Giải Phương trình đã cho tương đương với

$$(2x+1)^2 - 2y^2 = -1 \tag{15}$$

Đặt $u = 2x+1, \to u^2 - 2y^2 = -1$. Nghiệm nhỏ nhất của phương trình này là $(1,1)$. Do vậy dãy nghiệm (u_n, y_n) cho bởi

$$u_n = \frac{(1+\sqrt{2})^{2n+1} + (1-\sqrt{2})^{2n+1}}{2}$$
$$y_n = \frac{(1+\sqrt{2})^{2n+1} - (1-\sqrt{2})^{2n+1}}{2\sqrt{2}}$$

Từ đó

$$u_0 = 1, u_1 = 7, u_{k+2} = 6u_{k+1} - u_k$$
$$y_0 = 1, y_1 = 5, y_{k+2} = 6y_{k+1} - y_k$$

Ta có $u_n = 2x_n + 1 \to 2x_{k+2} + 1 = 6(2n_{k+1} + 1) - 2n_k - 1 \to x_0 = 0, x_1 = 3, x_{k+2} = 6x_{k+1} - x_k + 2$. Thành thử dãy nghiệm (x_n, y_n) của (15) cho bởi

$$x_0 = 0, x_1 = 3, x_{n+2} = 6x_{n+1} - x_n + 2$$
$$y_0 = 1, y_1 = 5, y_{n+2} = 6y_{n+1} - y_k$$

Thành thử ta chỉ cần chứng minh dãy (14) thỏa mãn quan hệ

$$x_{n+2} = 6x_{n+1} - x_n + 2$$
$$y_{n+2} = 6y_{n+1} - y_k$$

Thật vậy đặt $z_n = 2x_n + 1$. Khi đó dễ kiểm tra

$$z_{n+1} = 3z_n + 4y_n$$

$$y_{n+1} = 2z_n + 3y_n$$

$$\rightarrow z_{n+2} = 3z_{n+1} + 4y_{n+1} = 3z_{n+1} + 8z_n + 12y_n$$

$$= 3z_{n+1} + 8z_n + 3z_{n+1} - 9z_n = 6z_{n+1} - z_n$$

$$\rightarrow 2x_{n+2} + 1 = 6(2x_{n+1} + 1) - 2x_n - 1$$

$$\rightarrow x_{n+2} = 6x_{n+1} - x_n + 2$$

Tương tự $y_{n+2} = 6y_{n+1} - y_k$

3.4 Bài tập

1. Tìm tất cả các số nguyên dương n sao cho $\frac{n(n+1)}{2}$ là số chính phương.

2. Tìm tất cả các số nguyên dương n sao cho

$$\frac{1^2 + 2^2 + 3^2 + \cdots + n^2}{n}$$

là số chính phương

3. Cho $n \in N^*$ thỏa mãn: $3n + 1$ và $4n + 1$ đều là số chính phương. Chứng minh rằng n chia hết cho 56 .

4. Tìm cặp số nguyên dương (m, n) thỏa mãn $1+2+\cdots+m = (m+1)+\cdots+n$

4 Phương trình Pitago

4.1 Phương trình Pitago

Phương trình Pitago là phương trình sau

$$x^2 + y^2 = z^2 \tag{16}$$

Bộ ba số nguyên dương (x, y, z) thỏa mãn (16) được gọi là bộ ba Pitago. Bộ ba Pitago (x, y, z) được gọi là nguyên thủy nếu $(x, y, z) = 1$.

Bổ đề Nếu (x, y, z) là bộ ba Pitago nguyên thủy thì $(x, y) = (x, z) = (y, z) = 1$ và x, y không cùng tính chẵn lẻ .

Chứng minh Giả sử $(x, y) > 1$ và p là ước nguyên tố chung của x, y thì $p^2|x^2 + y^2 = z^2 \to p|z \to p|(x, y, z)$. Mâu thuẫn .Vậy $(x, y) = 1$. Tương tự $(x, z) = 1, (y, z) = 1$.

Vì $(x, y) = 1$ nên x, y không cùng chẵn. Nếu x, y cùng lẻ thì $x^2 \equiv y^2 \equiv 1 \pmod 4 \to z^2 \equiv 2 \pmod 4$. Mâu thuẫn. Vậy x, y không cùng tính chẵn lẻ.

Định lý Tập hợp tất cả các bộ ba Pitago (x, y, z) được cho bởi công thức

$$x = t(m^2 - n^2)$$

$$y = 2tmn$$

$$z = t(m^2 + n^2)$$

hoặc

$$x = 2tmn$$

$$y = t(m^2 - n^2)$$

$$z = t(m^2 + n^2)$$

trong đó $t, m, n \in N^*, m > n, (m, n) = 1$ và m, n khác tính chẵn lẻ.

Chứng minh Dễ kiểm tra nếu (x, y, z) cho bởi công thức trên thì $x^2 + y^2 = z^2$. Ngược lại giả sử (x, y, z) là bộ ba Pitago.

i) Trường hợp $(x, y, z) = 1$: Theo bổ đề x, y khác tính chẵn lẻ. Không giảm tổng quát giả sử x lẻ, y chẵn do đó z lẻ. Ta có $y^2 = z^2 - x^2 = (z + x)(z - x)$. Vì x, z lẻ nên $z + x = 2k, z - x = 2t, y = 2h, k, h \in N^*$. Thay vào (16) ta được$h^2 = kt$.Ta có $z = k + t, x = k - t$. Theo bổ đề $(x, z) = 1 \to (k, t) = 1$. Vậy tồn tại m, n sao cho $k = m^2, t = n^2 \to h = mn$. Vậy $x = k - t = m^2 - n^2, y = 2h = 2mn, z = k + h = m^2 + n^2$. Giả sử $(m, n) > 1$ và p là ước nguyên tố chung của m, n $p|m, p|n$ thì $p^2|m^2, p^2|n^2 \to p|x, p|z$. Mâu thuẫn. Vậy $(m, n) = 1$. Vì z lẻ nên m, n khác tính chẵn lẻ.

ii) Trường hợp (x, y, z) là bộ ba Pitago bất kỳ: Đặt $t = (x, y, z) \to x = tx_1, y = ty_1, z = tz_1, (x_1, y_1, z_1) = 1, x_1^2 + y_1^2 = z_1^2$. Vậy (x_1, y_1, z_1) là bộ ba Pitago nguyên thủy. Áp dụng i) ta có $x = tx_1 = t(m^2 - n^2); y = ty_1 = 2tmn; z = tz_1 = t(m^2 + n^2)$.Định lý được chứng minh

4.2 Một số bài toán chọn lọc

Bài toán 9 Chứng minh rằng phương trình

$$x^4 + y^4 = z^2 \tag{17}$$

Giải. Giả sử (17) có nghiệm. Gọi (x_0, y_0, z_0) là nghiệm sao cho z_0 nhỏ nhất. Ta có

i) $(x_0, y_0) = 1$.Thật vậy gọi p là ước nguyên tố chung của x_0, y_0. Ta có $p^4|x_0^4 + y_0^4 = z_0^2 \to p^2|z_0 \to x_0 = px_1, y_0 = py_1, z_0 = p^2z_1 \to x_1^4 + y_1^4 = z_1^2$. Vậy (x_1, y_1, z_1) là nghiệm của (17) với $z_1 < z_0$. Mâu thuẫn

ii) Vậy $(x_0^2, y_0^2, z_0) = 1$. Giả sử y_0 chẵn, x_0 lẻ. Theo định lý ta có

$$\begin{aligned} x_0^2 &= m^2 - n^2 \\ y_0^2 &= 2mn \\ z_0 &= m^2 + n^2 \end{aligned} \tag{18}$$

trong đó $t, m, n \in N^*, m > n, (m, n) = 1$ Từ (19)suy ra (x_0, n, m) là bộ ba Pitago nguyên thủy.Theo định lý ta có

$$\begin{aligned} x_0 &= a^2 - b^2 \\ n &= 2ab \\ m &= a^2 + b^2 \end{aligned} \tag{19}$$

trong đó $a, b \in N^* a > b, (a, b) = 1$.

Đặt $y_0 = 2y_1$. Từ (19)ta có $y_0^2 = 4y_1^2 = 2mn = 4ab(a^2 + b^2) \rightarrow y_1^2 = ab(a^2 + b^2) = abm$. Lại có $(a, b) = 1 \rightarrow (a, m) = (b, m) = 1 \rightarrow a = a_1^2, b = b_1^2, m = m_1^2$. Thay vào (19) ta có$m_1^2 = a_1^4 + b_1^4$. Vậy (a_1, b_1, m_1) là nghiệm của (17) với $m_1 \leqslant m_1^2 = m < m^2 + n^2 = z_0$. Mâu thuẫn với cách chọn (x_0, y_0, z_0) .

Bài toán 10 Chứng minh rằng không tồn tại hai số nguyên dương x, y mà tổng bình phương của chúng và hiệu bình phương của chúng đề là số chính phương.

Giải Giả sử trái lại hệ

$$\begin{cases} x^2 + y^2 &= z^2 \\ x^2 - y^2 &= t^2 \end{cases} \tag{20}$$

có nghiệm nguyên dương (x, y, z, t) và gọi (x_0, y_0, z_o, t_0) là nghiệm mà $x_0^2 + y_0^2$ bé nhất.

+)Ta có $(x_0, y_0) = 1$. Thật vậy giả sử trái lại gọi p là ước nguyên tố chung của x_0, y_0. Ta có $x_0 = px_1, y_0 = py_1 \rightarrow z_0 = pz_1, t_0 = pt_1$ và (x_1, y_1, z_1, t_1) là nghiệm

của (20). Mà $x_0^2 + y_0^2 = p^2(x_1^2 + y_1^2) > x_1^2 + y_1^2$.Mâu thuẫn .

+)Từ (20) suy ra $z_0^2 + y_0^2 = 2x_0^2$. Vậy z_0, t_0 có cùng tính chẵn lẻ. Đặt

$$u = \frac{z_0 + t_0}{2}, \quad v = \frac{z_0 - t_0}{2}$$

Suy ra

$$u^2 + v^2 = x_0^2 \tag{21}$$

Ta có $(u, v) = 1$. Thật vậy giả sử trái lại gọi p là ước nguyên tố chung của u, v. Khi đó $p^2|x_0^2 \to p|x_0, p|u + v = z_0 \to p^2|z_0^2 - x_0^2 = y_0^2 \to p|y_0 \to (x_0, y_0) > 1$. Mâu thuẫn.

+) Từ (21) và định lý ta suy ra

$$u = (m^2 - n^2)$$

$$v = 2mn$$

$$x_0 = (m^2 + n^2)$$

hoặc

$$u = 2mn$$

$$v = (m^2 - n^2)$$

$$x_0 = (m^2 + n^2)$$

trong đó $t, m, n \in N^*, m > n, (m, n) = 1$, m, n khác tính chẵn lẻ. Trong cả hai trường hợp ta đều có $uv = 2mn(m^2 - n^2)$. Ta có

$$2y_0^2 = z_0^2 - t_0^2 = (u + v)^2 - (u - v)^2 = 4uv$$

$$= 8mn(m^2 - n^2)$$

$$\to y_0^2 = 4mn(m^2 - n^2) \to y_0 = 2k$$

$$k^2 = mn(m^2 - n^2) \quad (22)$$

Vì $(m,n)=1$ nên dễ thấy $(m,n)=(m,m^2-n^2)=(n,m^2-n^2)=1$. Từ (22) suy ra tồn tại $a,b,c\in N^*$ để $m=a^2,n=b^2,m^2-n^2=c^2$. Vì $(m,n)=1$, m,n khác tính chẵn lẻ nên $(m+n,m-n)=1$. Mà $(m+n)(m-n)=c^2$ nên tồn tại $r,s\in N^*$ để

$$\begin{cases} m+n &= s^2 \\ m-n &= r^2 \end{cases}$$

Suy ra

$$\begin{cases} a^2+b^2 &= s^2 \\ a^2-b^2 &= r^2 \end{cases}$$

Vậy (a,b,s,r) là nghiệm của (20). Mặt khác

$$a^2+b^2=m+n\leqslant 2m\leqslant 2mn=u=\frac{z_0+t_0}{2}<z_0\leqslant z_0^2=x_0^2+y_0^2$$

Ta có mâu thuẫn.

4.3 Bài tập

1. Chứng minh rằng phương trình

$$x^4-y^4=z^2$$

không có nghiệm nguyên dương

2. Giải phương trình $x^4-2y^4=14$

3. Giải phương trình $x^4-2y^4=-1$

4. Hỏi có tồn tại hay không hình chóp tứ giác đều mà các cạnh,diện tích toàn phần và thể tích của nó đều là các số nguyên.