Phương trình nghiệm nguyên *
(Hướng dẫn giải bài tập)

Nguyễn Chu Gia Vượng

11/2014

Các bài tập sau đây được chuẩn bị cho các bài giảng tại Trường đông Toán học 2014.

Mục tiêu của loạt các bài tập sau đây là tìm hiểu một số phương trình nghiệm nguyên cơ bản (dạng đa thức): bậc nhất, bậc 2 (Pitago, Fermat, Pell-Fermat, Markov), và bậc 3 (chủ yếu là các phương trình "elliptic"). Thông qua các ví dụ này, các bạn học sinh được làm quen với các phương pháp cơ bản trong việc giải các bài toán tìm nghiệm nguyên như: đồng dư, phân tích thành nhân tử, xuống thang, lật nghiệm Viete, sử dụng nguyên lý cực hạn (nghiên cứu tính chất của phương trình thông qua các nghiệm "cực trị"), đánh giá bất đẳng thức, qui về một số phương trình cơ bản, v.v.

1 Phương trình bậc nhất

1. Cho số nguyên dương n và số nguyên không âm k. Chứng minh rằng số các bộ số nguyên không âm $(x_1, x_2, \ldots, x_k)$ thoả mãn

$$x_1 + x_2 + \cdots + x_k = n$$

bằng $\binom{n+k-1}{k-1}$.

Giải. Đây là một phiên bản của bài toán chia kẹo Euler quen thuộc: có tất cả $\binom{n+k-1}{k-1}$ cách chia n chiếc kẹo cho k bạn học sinh. Có nhiều cách để chứng minh sự kiện này, chẳng hạn các suy luận bằng tổ hợp quen thuộc.

Ta cũng có thể suy luận như sau. Số các bộ số nguyên không âm $(x_1, \ldots, x_k)$ thoả mãn $x_1 + x_2 + \cdots + x_k$ bằng hệ số của x^n trong khai triển của

$$f(x) = (1 + x + x^2 + x^3 + \cdots) \times \cdots \times (1 + x + x^2 + x^3 + \cdots) \quad \text{(k nhân tử)}.$$

Với $|x| < 1$, $f(x)$ định nghĩa một hàm số liên tục và khả vi vô hạn (như ta sẽ thấy, thậm chí khai triển thành chuỗi Taylor). Ta suy ra hệ số của x^n trong khai triển của $f(x)$ chính là $\frac{1}{n!}f^{(n)}(0)$ (đạo hàm thứ n tại 0 chia cho $n!$).

Để có thể tính toán các đạo hàm tại 0 của f, ta sẽ tính hàm số f. Ta có, với $|x| < 1$ thì

*Đây là bản nháp, hãy sử dụng với sự thận trọng.

$$1 + x + x^2 + x^3 + \cdots = \frac{1}{1-x}.$$

Suy ra

$$f(x) = \frac{1}{(1-x)^k}.$$

Ta có

$$\begin{aligned} f'(x) &= k\frac{1}{(1-x)^{k+1}}, \\ f''(x) &= k(k+1)\frac{1}{(1-x)^{k+2}}, \\ \cdots &= \cdots \\ f^{(n)}(x) &= k(k+1)\cdots(n+k-1)\frac{1}{(1-x)^{k+n-1}}. \end{aligned}$$

Như vậy, $f^{(n)}(0) = k(k+1)\cdots(n+k-1)$ và do đó

$$\frac{f^{(n)}(0)}{n!} = \frac{k(k+1)\cdots(n+k-1)}{n!} = \frac{(n+k-1)!}{(k-1)!n!} = \binom{n+k-1}{k-1}.$$

□

2. Tìm số các bộ số nguyên không âm (x, y, z, t), với $x, y, z, t \leq 9$, sao cho

$$x + y + z + t = 10.$$

Giải. Số các bộ cần tìm chính là số các nghiệm nguyên không âm của $x + y + z + t = 10$ trừ đi 4 nghiệm tương ứng với $(10, 0, 0, 0), (0, 10, 0, 0), (0, 0, 0, 10)$. Như vậy, đáp số cần tìm là

$$\binom{10+3-1}{4} - 4.$$

□

3. Cho số nguyên dương n. Tìm số các bộ số nguyên không âm (x, y, z) với z chẵn sao cho

$$x + y + z = n.$$

Giải. Ta có một lời giải đơn giản như sau: với mỗi z nguyên không âm chẵn và $\leq n$, phương trình $x + y = n - z$ có tất cả $n - z + 1$ nghiệm nguyên không âm (ứng với các bộ $(0, n - z + 1), (1, n - z), \ldots, (n - z + 1, 0)$). Như vậy số nghiệm cần tìm được cho bởi

$$\sum_{k=0,1,\ldots,\lfloor n/2 \rfloor} (n-2k+1) = (\lfloor n/2 \rfloor + 1)(n+1) - \lfloor n/2 \rfloor(\lfloor n/2 \rfloor + 1) = (\lfloor n/2 \rfloor + 1)(n+1-\lfloor n/2 \rfloor).$$

Tuy nhiên, ta cũng có thể tiếp cận bằng hàm sinh như sau. Số các nghiệm của phương đã cho là hệ số của x^n trong khai triển của

$$f(x) = (1 + x + x^2 + \cdots)(1 + x + x^2 + \cdots)(1 + x^2 + x^4 + \cdots).$$

Ta có, nếu $|x| < 1$ thì

$$f(x) = \frac{1}{1-x}\frac{1}{1-x}\frac{1}{1-x^2} = \frac{1}{(1-x)^3(1+x)}.$$

Chú ý rằng hệ số của x^n trong $f(x)$ bằng $\frac{f^{(n)}(0)}{n!}$. Để tính giá trị của các đạo hàm của f tại 0 ta phân tích f thành các phân thức đơn. Ta biết rằng tồn tại a, b, c, d để

$$f(x) = \frac{1}{1-x}\frac{1}{1-x}\frac{1}{1-x^2} = \frac{1}{(1-x)^3(1+x)} = \frac{a}{1-x} + \frac{b}{(1-x)^2} + \frac{c}{(1-x)^3} + \frac{d}{1+x}.$$

Để xác định cụ thể các giá trị a, b, c, d ta có thể qui đồng mẫu số và cân bằng các hệ số ở hai vế. Ta cũng có thể nhận xét như sau:

$$d = \lim_{x\to -1}(x+1)f(x) = \lim_{x\to -1}\frac{1}{(1-x)^3} = \frac{1}{8}.$$

$$c = \lim_{x\to 1}(1-x)^3 f(x) = \lim_{x\to 1}\frac{1}{(1+x)} = \frac{1}{2}.$$

$$b = \lim_{x\to 1}(1-x)^2\left(f(x) - \frac{c}{(1-x)^3}\right) = \lim_{x\to 1}\frac{1}{2(1+x)} = \frac{1}{4}.$$

$$a = \lim_{x\to 1}(1-x)\left(f(x) - \frac{c}{(1-x)^3} - \frac{b}{(1-x)^2}\right) = \lim_{x\to 1}\frac{1}{4(1+x)} = \frac{1}{8}.$$

Như vậy,

$$f(x) = \frac{1}{8}\frac{1}{1-x} + \frac{1}{4}\frac{1}{(1-x)^2} + \frac{1}{2}\frac{1}{(1-x)^3} - \frac{1}{8}\frac{1}{1+x}.$$

Chú ý rằng $\frac{1}{1-x} = 1+x+x^2+\cdots$, $\frac{1}{(1-x)^2} = \left(\frac{1}{1-x}\right)' = 1+2x+3x^2+\cdots$, $\frac{1}{(1-x)^3} = \frac{1}{2}\left(\frac{1}{(1-x)^2}\right)' = 1 + 3x + \cdots + \frac{(n+2)(n+1)}{2}x^n + \cdots$.

Từ đây, không khó để suy ra rằng số các nghiệm cần tìm bằng

$$\frac{f^{(n)}(0)}{n!} = \frac{1}{n!}\left[\frac{n!}{8} + \frac{(n+1)!}{4} + \frac{(n+2)!}{4} + \frac{(-1)^n n!}{8}\right] = \frac{2(n+1)(n+3) + 1 + (-1)^n}{8}.$$

□

4. (Định lý Sylvester) Cho a, b là hai số nguyên dương nguyên tố cùng nhau.

(a) Chứng minh rằng $ab - a - b$ là số nguyên dương lớn nhất không biểu diễn được dưới dạng $ax + by$ với x, y tự nhiên.

(b) Cho n là một số nguyên không âm và $\leq ab - a - b$. Chứng minh rằng n viết được dưới dạng $n = ax + by, a, b \in \mathbb{N}$ khi và chỉ khi $ab - a - b - n$ không viết được dưới dạng như vậy.

(c) Chứng minh rằng có đúng $\frac{1}{2}(a-1)(b-1)$ số nguyên dương không viết được dưới dạng $ax + by$ với x, y là các số tự nhiên.

Giải. Ta hãy quan sát xem khi nào một số nguyên không âm n có thể biểu diễn được thành tổng của các bội không âm của a và b. Trước tiên, nhận xét rằng phương trình $ax + by = n$ luôn có nghiệm trong tập các số nguyên. Hơn nữa, nếu (r, s) là một nghiệm nguyên bất kì thì tập các nghiệm của nó có dạng $(r + bk, s - ak)$ với $k \in \mathbb{Z}$. Nói riêng, tồn tại duy nhất một nghiệm nguyên (x_0, y_0) với x_0 là nguyên không âm nhỏ nhất và đây là nghiệm nguyên được xác định bởi điều kiện $0 \leq x_0 \leq b - 1$. Nhận xét rằng

$$ax + by = n \quad \text{có nghiệm nguyên không âm} \quad \Leftrightarrow y_0 \geq 0.$$

Thật vậy, như đã nói ở trên mọi nghiệm nguyên đều có dạng $(x_0 + bk, y_0 - bk)$ với $k \in \mathbb{Z}$: để $x_0 + bk \geq 0$, vì $0 \leq x_0 \leq b - 1$, ta phải có $k \geq 0$, và như vậy để $y_0 - bk \geq 0$ thì ta phải có $y_0 \geq 0$; đảo lại nếu $y_0 \geq 0$ thì rõ ràng (x_0, y_0) là một nghiệm nguyên không âm cần tìm.

Chú ý rằng, x_0 định nghĩa như ở trên còn có thể được đặc trưng bởi tính chất:

$$x_0 \quad \text{là số nguyên duy nhất nằm trong khoảng} \quad [0, b-1] \quad \text{sao cho} \quad ax_0 \equiv n \pmod{b}.$$

(a) Ta đặt $n = ab - a - b$ và áp dụng các tính chất đã chỉ ra ở trên đây. Thế thì theo các nhận xét ở trên, nghiệm (x_0, y_0) (định nghĩa ở trên) được đặc trưng bởi: $0 \leq x_0 \leq b - 1$ và $ax_0 \equiv ab - a - b \pmod{b} \Leftrightarrow ax_0 \equiv -a \pmod{b} \Leftrightarrow a(x_0 + 1) \equiv 0 \pmod{b} \Leftrightarrow x_0 \equiv b - 1 \pmod{b}$. Rõ ràng rằng điều này chứng tỏ $x_0 = b - 1$. Khi đó, ta có $y_0 = \frac{n - ax_0}{b} = \frac{ab - a - b - a(b-1)}{b} = -1$. Điều này chứng tỏ $ab - a - b$ không thể biểu diễn được thành tổng của các bội nguyên không âm của a và b.

Bây giờ, cũng với các tính chất đã thiết lập ở trên cho $n > ab - a - b$. Ta suy ra nghiệm (x_0, y_0) (định nghĩa ở trên) phải thoả mãn $x_0 \leq b - 1$. Và khi đó ta có $y_0 = \frac{b - ax_0}{b} > \frac{ab - a - b - a(b-1)}{b} = -1$. Bởi vì y_0 nguyên bất đẳng thức $y_0 > -1$ chứng tỏ $y_0 \geq 0$ và do đó n có thể biểu diễn được thành tổng của các bội nguyên không âm của a và b.

(b) Cố định $0 \leq n \leq ab - a - b$ và kí hiệu (x_0, y_0) là nghiệm định nghĩa như ở trên ứng với n và kí hiệu (x_0^*, y_0^*) là nghiệm định nghĩa như ở trên ứng với $ab - a - b - n$. Ta cần chứng minh đúng một trong hai y_0, y_0^* là nguyên không âm. Trước hết nhận xét rằng, do $n = ax_0 + by_0, ab - a - b - n = ax_0^* + by_0^*$ ta có $ab - a - b = a(x_0 + x_0^*) + b(y_0 + y_0^*)$ và do $x_0 + x_0 \geq 0$ nên theo câu trên ta phải có $y_0 + y_0^* \leq -1$ (nếu không $ab - a - b$ biểu diễn được thành tổng của các bội nguyên không âm của a và b!). Ta sẽ chỉ ra rằng

$$y_0 + y_0^* = -1.$$

Chú ý rằng, đẳng thức này, cùng với việc y_0, y_0^* là các số nguyên chứng tỏ rằng đúng một trong các số y_0, y_0^* là ≥ 0.

Để thiết lập đẳng thức trên, ta hãy tìm hiểu mối quan hệ giữa x_0 và x_0^*. Theo định nghĩa chúng là các số nguyên nằm trong khoảng $[0, b-1]$ định nghĩa bởi $ax_0 \equiv n \pmod b$ và $ax_0^* \equiv ab - a - b - n \pmod b$. Suy ra $a(x_0 + x_0^*) \equiv ab - a - b \equiv -a \pmod b$. Như vậy, $a(x_0 + x_0 + 1) \equiv 0 \pmod b$, hay

$$x_0 + x_0^* + 1 \equiv 0 \pmod b.$$

Nhưng điều kiện $0 \leq x_0, x_0^* \leq b-1$ chứng tỏ $0 \leq x_0 + x_0^* \leq 2b-2$ và do đó đồng dư trên chỉ xảy ra với

$$x_0 + x_0^* = b - 1.$$

Bây giờ, đẳng thức $a(x_0 + x_0^*) + b(y_0 + y_0^*) = ab - a - b$ dẫn đến $y_0 + y_0^* = \frac{ab-a-b-a(b-1)}{b} = -1$, như mong muốn.

(c) Rõ ràng đây là một hệ quả trực tiếp từ câu trên.

□

5. (IMO 1983.) Cho a, b, c là các số nguyên dương đôi một nguyên tố cùng nhau. Chứng minh rằng $2abc - ab - bc - ca$ là số nguyên dương lớn nhất không biểu diễn được dưới dạng $abx + bcy + caz$ với x, y, z là các số tự nhiên.

Giải. Ta lập luận giống hệt như phần đầu ở bài tập trên. Giả sử n là một số nguyên không âm. Ta tìm cách đặc trưng khi nào n viết được thành tổng của các bội nguyên không âm của ab, bc, ca. Trước hết, do $(ab, bc, ca) = 1$ phương trình $abx + bcy + caz = n$ luôn có nghiệm nguyên. Cố định một nghiệm (r, s, t) và mô tả tập các nghiệm của nó. Ta có

$$abx + bcy + caz = n \Leftrightarrow ab(x - r) + bc(y - s) + ca(z - t) = 0.$$

Bằng rút gọn modulo a, b, c đẳng thức trên ta suy ra $x \equiv r \pmod c, y \equiv s \pmod a$ và $z \equiv t \pmod b$. Hơn nữa, nếu $x = kc + r, y = ha + s$ thì ta có $ca(z - t) = -abc(k + h)$ và như vậy $z = t - b(k+h)$. Điều này có nghĩa là, mọi nghiệm nguyên của phương trình $abx + bcy + caz = n$ được tham số bởi $(r + kc, s + ha, t - b(k + h)), k, h \in \mathbb{Z}$, trong đó (r, s, t) là một nghiệm nguyên bất kì.

Ta gọi (x_0, y_0, z_0) là nghiệm nguyên duy nhất của $abx + bcy + caz = n$ thoả mãn điều kiện $0 \leq x_0 \leq c - 1, 0 \leq y_0 \leq a - 1$. Thế thì, ta có các nhận xét đơn giản sau đây:

- phương trình $abx + bcy + caz = n$ có nghiệm nguyên không âm khi và chỉ khi $z_0 \leq 0$.
- x_0, y_0 được đặc trưng bởi các tính chất: $0 \leq x_0 \leq c - 1, abx_0 \equiv n \pmod c, 0 \leq y_0 \leq a - 1, cay_0 \equiv n \pmod a$.

Ta áp dụng các tính chất trên để chỉ ra rằng $n = 2abc - ab - bc - ca$ không biểu diễn được thành tổng các bội nguyên của ab, bc, ca. Thật vậy, nghiệm (x_0, y_0, z_0) định nghĩa như trên được đặc trưng bởi: $0 \leq x_0 \leq c - 1, abx_0 \equiv 2abc - ab - bc - ca \pmod c$ hay $ab(x_0 + 1) \equiv 0 \pmod c$, và như vậy $x_0 + 1 \equiv 0 \pmod c$, hay $x_0 = c - 1$ (vì $0 \leq x_0 \leq c - 1$). Tương tự ta có $y_0 = a - 1$. Từ đó suy ra $z_0 = \frac{2abc-ab-bc-ca-bc(a-1)-ca(b-1)}{ab} = -1$. Điều này chứng tỏ $2abc - ab - bc - ca$ không biểu diễn được dưới dạng mong muốn.

Bây giờ, giả sử $n > 2abc - ab - bc - ca$. Thế thì nghiệm (x_0, y_0, z_0) định nghĩa như trên luôn có $x_0 \leq c-1, y_0 \leq a-1$ và do đó $z_0 = \frac{n-abx_0-bcy_0}{ab} > \frac{2abc-ab-bc-ca-bc(a-1)-ca(b-1)}{ab} = -1$. Do z_0 nguyên, ta phải có $z_0 \geq 0$ và do đó n biểu diễn được dưới dạng mong muốn.

Bài toán được chứng minh.

□

6. (Theo Komal 1999, VN TST 2000.) Cho a, b, c là các số nguyên dương đôi một nguyên tố cùng nhau.

   (a) Với mọi số nguyên không âm $n \leq 2abc - ab - bc - ca$, số n biểu diễn được dưới dạng $abx + bcy + caz$, với x, y, z nguyên không âm, khi và chỉ khi $2abc - ab - bc - ca - n$ không biểu diễn được.

   (b) Chứng minh rằng có đúng $\frac{2abc-ab-bc-ac+1}{2}$ số nguyên dương không thể biểu diễn được dưới dạng $abx + bcy + caz$ với x, y, z nguyên không âm.

   Gợi ý. Suy luận giống hệt như với đjnh lý Sylvester.

□

2 Phương trình bậc hai

1. (Bộ ba Pitago.) Xét phương trình Pitago

$$x^2 + y^2 = z^2.$$

   (a) Chứng minh rằng moi nghiệm nguyên dương của phương trình trên có dạng (kx_0, ky_0, kz_0) với k nguyên dương và (x_0, y_0, z_0) là một nghiệm nguyên dương mà x_0, y_0, z_0 các số nguyên đôi một nguyên tố cùng nhau. Một nghiệm nguyên dương (x_0, y_0, z_0) của phương trình Pythagoras với x_0, y_0, z_0 đôi một nguyên tố cùng nhau được gọi là một nghiệm **nguyên thuỷ**.

   (b) Chứng minh rằng nếu (x_0, y_0, z_0) là một nghiệm nguyên thuỷ thì x_0, y_0 không cùng tính chẵn lẻ.

   (c) Chứng minh rằng mọi nghiệm nguyên thuỷ (x_0, y_0, z_0) với x_0 chẵn có dạng

$$x_0 = 2mn, y_0 = m^2 - n^2, z_0 = m^2 + n^2$$

   với $m > n$ là các số nguyên dương nguyên tố cùng nhau và khác tính chẵn lẻ.

   Giải. Đây là một kết quả kinh điển và ta có thể lập luận như sau.

   (a) Giả sử (x, y, z) là một nghiệm nguyên dương của phương trình đã cho. Đặt $k = (x, y)$ và viết $x = kx_0, y = ky_0$. Thế thì

$$k^2(x_0^2 + y_0^2) = z^2.$$

   Suy ra $k^2 \mid z^2$ và như vậy $k \mid z$. Đặt $z = kz_0$. Ta suy ra

$$x_0^2 + y_0^2 = z_0^2.$$

Dễ thấy $(x_0, z_0) = 1$: thật vậy, nếu $d = (x_0, z_0)$ thì $d \mid z_0^2 - x_0^2 = y_0^2$ nên $d^2 \mid y_0^2$ và như vậy $d \mid y_0$ và do đó $d \mid (x_0, y_0) = 1$, hay $d = 1$. Tương tự $(y_0, z_0) = 1$. Như vậy (x_0, y_0, z_0) là một bộ ba Pitago nguyên thuỷ.

(b) Bằng cách modulo 4 và với nhận xét rằng $a^2 \equiv 0 \pmod 4$ nếu a chẵn và $\equiv 1 \pmod 4$ nếu a lẻ, ta thấy rằng nếu (x_0, y_0, z_0) thoả mãn

$$x_0^2 + y_0^2 = z_0^2$$

thì x_0, y_0 không thể cùng lẻ.

(c) Giả sử (x_0, y_0, z_0) là một bộ ba Pitago nguyên thuỷ với x_0 chẵn. Đặt $x_0 = 2x'$. Thế thì

$$4x'^2 = (z_0 - y_0)(z_0 + y_0).$$

Do $z_0 - y_0, z_0 + y_0$ cùng tính chẵn lẻ (và tích là một số chẵn) ta suy ra chúng cùng chẵn. Ta viết lại đẳng thức trên dưới dạng

$$x'^2 = \frac{z_0 - y_0}{2} \frac{z_0 + y_0}{2}.$$

Nếu một số nguyên d là ước chung của $\frac{z_0+y_0}{2}, \frac{z_0-y_0}{2}$ thì nó cũng là ước của tổng và hiệu của hai số này, nghĩa là $d \mid z_0, d \mid y_0$. Giả thiết (x_0, y_0, z_0) nguyên thuỷ đảm bảo rằng $d = \pm 1$, nói cách khác $\frac{z_0+y_0}{2}, \frac{z_0-y_0}{2}$ (là các số nguyên dương) nguyên tố cùng nhau. Lại do tích của chúng là một số chính phương nên mỗi nhân tử phải là chính phương: tồn tại các số nguyên dương m, n sao cho.

$$m = \frac{z_0 + y_0}{2}, n = \frac{z_0 - y_0}{2}.$$

Từ đó suy ra $y_0 = m^2 - n^2, z_0 = m^2 + n^2$, cũng như $x = 2mn$. Chú ý rằng bất đẳng thức $m > n$ cũng như điều kiện $(m, n) = 1$ là rõ ràng. Việc m, n không cùng tính chẵn lẻ đến từ việc x_0, y_0 không cùng tính chẵn lẻ (và như vậy, z_0 là lẻ).

Thử lại, ta dễ dàng kiểm tra được rằng bộ ba $(2mn, m^2 - n^2, m^2 + n^2)$, với các điều kiện như trên, là một bộ ba Pitago nguyên dương và nguyên thủy.

□

2. Tìm tất cả các số nguyên dương x, y sao cho

$$x^2 + y^2 = 2014(x - y).$$

Giải. Trước hết, ta có thể sử dụng một số biến đổi đại số để đưa phương trình về một dạng quen biết. Ở đây, như chúng ta sẽ thấy, bài toán đưa về phương trình Pitago.

Ta có thể viết lại phương trình đã cho dưới dạng $2x^2 + 2y^2 - 2 \cdot 2014(x - y) = 0$, hay $(x + y)^2 + (x - y)^2 - 2 \cdot 2014(x - y) = 0$, nghĩa là

$$(x + y)^2 + (2014 - x + y)^2 = 2014^2.$$

Đây là phương trình Pitago quen thuộc. Nếu (x, y) là một nghiệm thì ta có $x+y, 2014-x+y$ cùng tính chẵn lẻ, do đó phải cùng chẵn (xét modulo 4). Chú ý rằng điều kiện x, y nguyên dương chứng tỏ $x + y \leq 2014$. Ta viết lại phương trình đã cho dưới dạng

$$\left(\frac{x+y}{2}\right)^2 + \left(\frac{2014-x+y}{2}\right)^2 = 1007^2 = (19 \cdot 53)^2.$$

Từ đó suy ra $d = \left(\frac{x+y}{2}, \frac{2014-x+y}{2}\right) \mid 1007 = 19 \cdot 53$. Như vậy $d = 1, 19, 53$ hoặc 1007. Ta xét các trường hợp tương ứng:

- $d = 1$, tồn tại m, n nguyên dương, nguyên tố cùng nhau để $m^2 + n^2 = 1007$ và hoặc $2mn = \frac{x+y}{2}, 1007 - \frac{x-y}{2} = m^2 - n^2$ hoặc hoặc $m^2 - n^2 = \frac{x+y}{2}, 1007 - \frac{x-y}{2} = 2mn$. Trước hết, $m, n \leq \sqrt{1007} \implies m, n \leq 31$. Hơn nữa, do $m > n$ ta suy ra $m^2 \geq 504$ và do đó $m \geq 21$.

  Mặt khác, bằng cách xét các số dư có thể của một số chính phương modulo 19. Ta suy ra $m^2, n^2 \equiv 0, 1, 4, 9, 16, 6, 7, 17, 11, 7, 5$ ta suy ra để $m^2 + n^2 = 1007$ ta phải có $19 \mid m, 19 \mid n$. Rõ ràng rằng điều này mâu thuẫn với chặn $21 \leq m \leq 31$ ở trên.
- $d = 53$. Ta viết lại phương trình dưới dạng

  $$\left(\frac{x+y}{106}\right)^2 + \left(\frac{2014-x+y}{106}\right)^2 = (19)^2.$$

  Tương tự như trên, bằng cách xét modulo 19 ta phải có $\frac{x+y}{106} \equiv \frac{2014-x+y}{106} \equiv 0 \pmod{19}$ và do đó $\frac{x+y}{106} = 19, \frac{2014-x+y}{106} = 0$ (trường hợp $\frac{x+y}{106} = 0, \frac{2014-x+y}{106} = 19$ bị loại do x, y nguyên dương). Như vậy ta có $x+y = 19 \cdot 106 = 2014, x-y = 2014$, hay $x = 2014, y = 0$ (loại).
- $d = 19$. Ta viết lại phương trình dưới dạng

  $$\left(\frac{x+y}{38}\right)^2 + \left(\frac{2014-x+y}{38}\right)^2 = (53)^2.$$

  Do $\left(\frac{x+y}{38}, \frac{2014-x+y}{38}\right) = 1$ ta suy ra tồn tại $m > n$ nguyên tố cùng nhau để $m^2+n^2 = 53$ và hoặc $\frac{x+y}{38} = m^2-n^2, \frac{2014-x+y}{38} = 2mn$ hoặc $\frac{x+y}{38} = 2mn, \frac{2014-x+y}{38} = m^2-n^2$. Dễ thấy rằng phương trình $m^2+n^2 = 53$ chỉ có nghiệm nguyên dương $m > n$ duy nhất là $m = 7, n = 2$. Nếu $\frac{x+y}{38} = 2mn = 28, \frac{2014-x+y}{38} = 7^2 - 2^2 = 45$ thì ta có $x + y = 1064, x - y = 304$, hay $x = 684, y = 380$. Nếu $\frac{x+y}{38} = 45, \frac{2014-x+y}{38} = 28$ thì ta có $x + y = 1710, x - y = 950$, hay $x = 1330, y = 380$.
- $d = 1003$. Trong trường hợp này ta phải có $x + y = 2014, x - y = 2014$ hoặc $x + y = 0, x - y - 2014$. Cả hai trường hợp đều không thể xảy ra.

Tóm lại, ta tìm được các cặp nghiệm $(684, 380)$ và $(1330, 380)$. Thử lại ta thấy các bộ này thoả mãn phương trình yêu cầu.

□

Nhận xét. Để có lời giải ngắn gọn hơn, ta cũng có thể sử dụng sự kiện: mọi ước nguyên tố lẻ của $x^2 + y^2$ hoặc đồng thời là ước của x và y hoặc $\equiv 1 \pmod 4$.

3. (Fermat.) Chứng minh rằng phương trình

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

không có nghiệm nguyên dương.

Giải. Đây là bài toán điển hình của phương pháp xuống thang. Về mặt lịch sử, lời giải mà ta trình bày sau đây là chứng minh duy nhất được Fermat công bố (tất cả các kết quả còn lại của Fermat được công bố mà không kèm theo chứng minh).

Giả sử phương trình đã cho có nghiệm nguyên dương. Ta gọi (x, y, z) là một nghiệm nguyên dương nhỏ nhất theo nghĩa z là nhỏ nhất. Điều kiện này nói riêng dẫn đến x, y, z đôi một nguyên tố cùng nhau. Thật vậy, chẳng hạn nếu x, y có một ước chung $d > 1$ thì hiển nhiên $d^4 \mid x^4 + y^4 = z^2$, do đó $d^2 \mid z$ và khi đó $(x/d, y/d, z/d^2)$ là một nghiệm nhỏ hơn của phương trình đã cho, mâu thuẫn.

Do phương trình ban đầu còn có thể viết được dưới dạng

$$(x^2)^2 + (y^2)^2 = z^2,$$

bộ (x^2, y^2, z) là một bộ ba Pi-ta-go nguyên thuỷ. Từ đó suy ra, chẳng hạn với x lẻ và y chẵn, tồn tại các số nguyên dương r, s khác tính chẵn lẻ, nguyên tố cùng nhau sao cho

$$x^2 = r^2 - s^2, y^2 = 2rs, z = r^2 + s^2.$$

Do x được giả thiết là lẻ, $r^2 - s^2 \equiv 1 \pmod 4$ ta không thể có r chẵn, s lẻ mà phải có r lẻ, s chẵn. Viết $s = 2s'$. Đẳng thức

$$y^2 = 4rs'$$

kết hợp với sự kiện $(r, s') = 1$, dẫn đến mỗi r, s' là chính phương. Chẳng hạn $r = u^2, s' = v^2$.

Bây giờ, ta sử dụng đẳng thức $x^2 = r^2 - s^2$ mà ta sẽ viết dưới dạng

$$x^2 + s^2 = r^2$$

và các điều quen biết về các bộ ba Pi-ta-go để rút ra rằng (chú ý x lẻ, nguyên tố với s) tồn tại các số nguyên dương z, t nguyên tố cùng nhau sao cho

$$x = z^2 - t^2, s = 2zt, r = z^2 + t^2.$$

Từ đó suy ra $2zt = s = 2s'$ và như vậy $s' = zt$ và (do z, t nguyên tố cùng nhau) $z = z'^2, t = t'^2$ với z', t' nguyên dương nào đó. Bây giờ, đẳng thức $r = z^2 + t^2$ có thể được viết dưới dạng

$$z'^4 + t'^4 = u^2.$$

Điều này cho thấy phương trình (**??**) nhận (z', t', u) làm nghiệm. Dễ thấy đây là một nghiệm nhỏ hơn (x, y, z) ban đầu, mâu thuẫn.

Nhận xét.

- Như là một hệ quả, phương trình Fermat $x^n + y^n = z^n$ với $n = 4$ không có nghiệm nguyên không tầm thường.
- Với cùng phương pháp suy luận ta cũng có thể chỉ ra được rằng phương trình

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

cũng không có nghiệm nguyên không tầm thường.

□

4. (Định lý Fermat về tổng 2 số chính phương.) Cho số nguyên tố $p > 2$. Chứng minh rằng phương trình

$$x^2 + y^2 = p$$

có nghiệm nguyên khi và chỉ khi $p \equiv 1 \pmod 4$.

Giải. Giả sử x, y là một nghiệm nguyên dương của phương trình $x^2 + y^2 = p$. Thế thì do p lẻ, x, y không cùng tính chẵn lẻ và do đó $x^2 + y^2 \equiv 1 \pmod 4$ ($a^2 \equiv 0 \pmod 4$ nếu a chẵn và $\equiv 1 \pmod 4$ nếu a lẻ).

Đảo lại, giả sử p là một số nguyên tố $\equiv 1 \pmod 4$. Ta sẽ chỉ ra sự tồn tại của các số nguyên dương x, y để $x^2 + y^2 = p$. Trước hết, ta chỉ ra rằng tồn tại số nguyên a để $a^2 \equiv 1 \pmod p$. Tất nhiên, ta có thể sử dụng luật thuận nghịch toàn phương để chỉ ra điều này. Tuy nhiên ta sẽ chỉ ra một số nguyên a một cách cụ thể như sau. Chú ý rằng theo định lý Wilson, nếu $p = 4k + 1$ là nguyên tố thì $(4k)! \equiv -1 \mod p$ hay $1 \cdot 2 \cdots 2k \cdot (2k + 1) \cdots 4k \equiv -1 \pmod p$, nghĩa là $1 \cdot 2 \cdots 2k \cdot (-2k) \cdot (-2k + 1) \cdots (-1) \pmod -)1$, nghĩa là $(2k!)^2 \equiv -1 \pmod p$.

Bổ đề (Thue)**.** *Cho p là một số nguyên tố. Với mọi số nguyên a không chia hết cho p, tồn tại các số nguyên $\{1, 2 \cdots, \lfloor\sqrt{p}\rfloor\}$ sao cho hoặc $ax \equiv y$ hoặc $ax \equiv -y \pmod p$.*

Đây là một ứng dụng của nguyên lý Dirichlet. Tập hợp $\{0, 1, 2 \cdots, \lfloor\sqrt{p}\rfloor\} \times \{0, 1, 2 \cdots, \lfloor\sqrt{p}\rfloor\}$ có $(\lfloor\sqrt{p}\rfloor+1)^2 > p$ phần tử. Như vậy, (x, y) chạy trên tập $\{0, 1, 2 \cdots, \lfloor\sqrt{p}\rfloor\} \times \{0, 1, 2 \cdots, \lfloor\sqrt{p}\rfloor\}$, ta thu được $> p$ giá trị $ax - y \mod p$. Do có cả thảy p lớp đồng dư modulo p, nguyên lý Dirichlet nói rằng tồn tại $(x_1, y_1) \neq (x_2, y_2), x_1, x_2, y_1, y_2 \in \{0, 1, 2 \cdots, \lfloor\sqrt{p}\rfloor\} \times \{0, 1, 2 \cdots, \lfloor\sqrt{p}\rfloor\}$ sao cho $ax_1 - y_1 \equiv ax_2 - y_2 \pmod p$. Đặt $x = |x_1 - x_2|, y = |y_1 - y_2|$ thế thì hoặc $ax \equiv y$ hoặc $ax \equiv y \pmod p$. Ta có $x, y \in \{0, 1, \ldots, \lfloor\sqrt{p}\rfloor\}$. Để kết thúc, ta cần loại trường hợp $x = 0$ (và $y = 0$). Như điều này là dễ dàng: $x = 0$ khi và chỉ khi $y \equiv 0$ và điều này chỉ xảy ra khi $x_1 \equiv x_2$ và $y_1 \equiv y_2$ đồng thời xảy ra, mâu thuẫn.

Quay trở lại bài toán. Ta chọn a là một số nguyên sao cho $a^2 + 1 \pmod p$. Theo Bổ đề trên, ta có thể tìm được các số nguyên $x, y \in \{1, 2, \ldots, \lfloor\sqrt{p}\rfloor\}$ sao cho $a^2x^2 \equiv y^2 \pmod p$. Suy ra $x^2 + y^2 \equiv 0 \pmod p$. Chú ý rằng theo xây dựng $x^2 < p, y^2 < p$. Như vậy $x^2 + y^2 < 2p$ và do đó đồng dư $x^2 + y^2 \equiv p$ chỉ xảy ra khi $x^2 + y^2 = p$. Bài toán được chứng minh.

□

Cách khác. Điều kiện đủ còn có thể được lập luận dựa vào qui nạp như sau. [1]

Ta có $5 = 1^2 + 2^2$. Cố định $p \equiv 1 \pmod 4$ và $p > 5$. Ta giả sử mọi số nguyên tố $< p$ và $\equiv 1 \pmod 4$ đều viết được thành tổng của 2 số chính phương. Ta sẽ chỉ ra rằng p cũng viết được thành tổng của 2 số chính phương.

Trước hết ta sử dụng sự kiện sau đây (xem chứng minh đầu tiên): tồn tại a để $p \mid a^2 + 1$. Nói riêng, tồn tại u_0, v_0 nguyên tố cùng nhau để $p \mid u^2 + v^2$. Nếu cần, ta có thể thay thế u (tương ứng, v) bởi phần dư của u modulo p hoặc $p-$ phần dư của u modulo p, ta có thể giả sử $0 \leq r, s < p/2$ và $p \mid r^2 + s^2$. Tuy nhiên việc thay đổi như vậy có thể khiến r, s trở nên không nguyên tố cùng nhau. Thế nhưng việc thay đổi này vẫn đảm bảo $p \nmid r, p \nmid s$. Chính vì vậy, nếu cần, ta thay r, s tương ứng bởi thương của chúng cho ước chung lớn nhất của r và s, ta vẫn có thể giả sử $p \mid r^2 + s^2, (r, s) = 1$ và $0 \leq r, s < p/2$. Như vậy $r^2 + s^2 = N$ với $N \leq p^2/2$. Điều này chứng tỏ mọi ước nguyên tố $\neq p$ của N đều $< p$. Ta biết rằng, bởi vì $(r, s) = 1$, mọi ước nguyên tố của $r^2 + s^2$ hoặc $= 2$ hoặc $\equiv 1 \pmod 4$.

Bài toán được giải quyết nếu ta thiết lập được khẳng định sau đây:

Bổ đề. *Giả sử $N = r^2 + s^2$ với $(r, s) = 1$ và q là một ước nguyên tố của N. Giả sử $q = a^2 + b^2$ với $a, b \in \mathbb{Z}$, thế thì N/q cũng là tổng của 2 số chính phương nguyên tố cùng nhau.*

Thật vậy, ta lấy một ước nguyên tố $q \neq p$ bất kì của $N = r^2 + s^2$, $q = 2$ (khi đó $2 = 1^2 + 1^2$) hoặc $q \equiv 1 \pmod 4$ và $q < p$, nên theo giả thiết qui nạp q viết được thành tổng của 2 số chính phương. Bổ đề trên cho thấy $N/q = r_1^2 + s_1^2$ với r_1, s_1 nguyên tố cùng nhau. Lập luận liên tiếp như vậy với các ước nguyên tố $\neq p$ của N cho đến khi ta nhận được một biểu diễn $p = r_k^2 + s_k^2$ như mong đợi.

Chứng minh Bổ đề. Ta có

$$Nq = (r^2 + s^2)(a^2 + b^2) = (ar + bs)^2 + (as - br)^2 = (ar - bs)^2 + (as + br)^2.$$

Ta có $q \mid (ar + bs)(ar - bs) = a^2r^2 - b^2s^2 = (r^2 + s^2)a^2 - (a^2 + b^2)s^2 = Na^2 - qs^2$. Vì vậy hoặc $ar + bs$ hoặc $ar - bs$ chia hết cho p. Chẳng hạn $q \mid ar + bs$ (hoàn toàn tương tự cho trường hợp ngược lại.) Khi đó hiển nhiên $q \mid as - br$. Thế thì bằng cách đặt $r_1 = (ar + bs)/q, s_1 = (as - br)/q$ thì bằng cách chia hai vế của đẳng thức $Nq = (ar + bs)^2 + (as - br)^2$ cho q^2 ta thu được

$$N/q = r_1^2 + s_1^2.$$

Việc chỉ ra rằng r_1, s_1 nguyên tố cùng nhau được để lại cho bạn đọc. □

□

Nhận xét.

- Trong Bổ đề trên, ta chỉ sử dụng các sự kiện $\sqrt{p}$ không nguyên và a, p nguyên tố cùng nhau.

[1] Đây là chứng minh đưa ra bởi Euler. Về mặt lịch sử, kết quả này được phát biểu (nhưng không chứng minh) lần đầu tiên bởi Fermat. Chứng minh của Euler mà ta trình bày ở đây được tin là chứng minh mà Fermat nghĩ đến. Lưu ý rằng ý tưởng cơ bản của chứng minh này là phương pháp xuống thang: nếu $p \equiv 1$ không viết được dưới dạng tổng của 2 số chính phương thì luôn tìm được số nguyên tố $p' \equiv 1 \pmod 4$ cũng không viết được dưới dạng tổng của 2 số chính phương.

- Trong lập luận của chứng minh trên đây của Định lý Fermat về tổng 2 số chính phương, tính chất mà ta cần từ a là việc $p \mid a^2+1$.
- Điều kiện cần còn có thể được chứng minh dựa vào một sự kiện quen biết và hữu ích sau đây: nếu x, y nguyên tố cùng nhau thì mọi ước nguyên tố lẻ của x^2+y^2 đều $\equiv 1 \pmod 4$.

  Thật vậy, rõ ràng $p \nmid x, p \nmid y$ (nếu không p phải đồng thời là ước của x, y!). Bằng cách nhân 2 vế với nghịch đảo y^{-1} của y modulo p, ta suy ra $p \min a^2+1$ với a là một số nguyên nào đó. Ta sẽ chỉ ra rằng mọi ước nguyên tố lẻ của a^2+1 đồng dư với 1 modulo 4. Thật vậy, ta có $a^2 \equiv -1 \pmod p$. Nói riêng $p \nmid a$. Từ đó suy ra $a^4 \equiv 1 \pmod p$. Điều này chứng tỏ $ord_p(a) \mid 4$. Nhưng $a^2 \equiv -1 \pmod p$ cũng cho thấy $ord_p(a) \neq 2$. Từ đó suy ra $ord_p(a) = 4$. Nhưng theo định lý Fermat nhỏ, $a^{p-1} \equiv 1 \pmod p$, nói cách khác $ord_p(a) \mid p-1$. Có nghĩa là $4 \mid p-1$, hay $p \equiv 1 \pmod 4$ [2].

5. (VN TST 1998.) Giả sử d là một ước dương của $5+1998^{1998}$. Chứng minh rằng d có thể biểu diễn được dưới dạng $d = 2x^2+2xy+3y^2$ khi và chỉ khi d chia 20 có số dư là 3 hoặc 7.

   Giải. **Điều kiện cần.** Một số nguyên $\equiv 3 \pmod{20}$ khi và chỉ khi đồng thời $\equiv 3 \pmod 5$ và $\equiv 3 \pmod 4$. Tương tự, một số nguyên $\equiv 7 \pmod{20}$ khi và chỉ khi đồng thời $\equiv 2 \pmod 5$ và $\equiv 3 \pmod 4$. Như vậy một số $\equiv 3$ hoặc $7 \pmod{20}$ khi và chỉ khi $\equiv 3 \pmod 4$ và $\equiv 2$ hoặc $3 \pmod 5$. Dễ thấy nếu $d \mid 5+1998^{1998}$ thì d lẻ và $d \nmid 5$.

   Tại sao $d \equiv 3 \pmod 4$? Tất nhiên điều này cần phải được suy ra từ việc d có thể biểu diễn được dưới dạng $d = 2x^2+2xy+3y^2$. Với một biểu diễn như vậy, ta có $y \equiv d \pmod 2$ nên y lẻ. Từ đó suy ra với mọi x thì $2x^2+2xy = 2x(x+y)$ chia hết cho 4, do đó $d \equiv 3y^2 \equiv 3 \mod 4$. Tại sao $d \equiv 2, 3 \pmod 5$? Ta có $2d = 4x^2+4xy+6y^2 = (2x+y)^2+5y^2 \equiv (2x+y)^2 \pmod 5$. Từ đó (bởi vì $5 \nmid 2d$) ta suy ra $2d \equiv \pm 1 \pmod 5$, điều này chứng tỏ $d \equiv 2, 3 \pmod 5$.

   Điều kiện đủ. Ta sẽ chỉ ra rằng với mọi số nguyên $d \equiv 3, 7 \pmod{20}$ đều có thể biểu diễn được dưới dạng yêu cầu. Ta lấy lại biểu diễn ở trên: ta cần tìm x, y để

   $$2d = (2x+y)^2+5y^2.$$

   Đặt $a = 1998^{999}$. Khi đó $d \mid a^2+5$. Chú ý rằng nói riêng ta có $(d, a) = 1$. Ta hãy lặp lại các suy luận của chứng minh trên của định lý Fermat về tổng của hai số chính phương.

   Theo Bổ đề Thue (hoặc lặp lại chứng minh trên, với p thay bởi d), tồn tại các số nguyên $1 \leq Y, X \leq \lfloor \sqrt{d} \rfloor$ để $a^2Y^2 \equiv X^2 \pmod d$. Thế nhưng $a^2 \equiv -5 \pmod d$, ta suy ra $X^2+5Y^2 \equiv 0 \pmod d$. Chú ý rằng $X, Y \leq \sqrt{d}$ nên $X^2+5Y^2 \leq 6d$. Như vậy $X^2+5Y^2 = d, 2d, 3d, 4d, 5d$ hoặc $6d$. Ta xét các trường hợp

   - $X^2+5Y^2 = d$. Ta suy ra $d \equiv X^2 \pmod 5$ và do đó $d \not\equiv 2, 3 \pmod 5$, vô lý.
   - $X^2+5Y^2 = 2d$. Đây là trường hợp thuận lợi nhất. Ta suy ra $X^2+Y^2 \equiv 2 \pmod 4$ (do $d \equiv 3 \pmod 4$) nên X, Y cùng lẻ. Từ đây, ta có thể tìm được x, y để $X = 2x+y, y = Y$ và như vậy $2d = (2x+y)^2+5y^2$ hay $d = 2x^2+2xy+3y^2$.
   - $X^2+5Y^2 = 3d$. Suy ra $X^2-Y^2 \equiv 0 \pmod 3$ và như vậy hoặc $X \equiv Y \pmod 3$ hoặc $X \equiv -Y \pmod 3$.

[2] Hoàn toàn tương tự, mọi ước nguyên tố lẻ của $a^{2^k}+1$ luôn đồng dư với $1 \mod 2^{k+1}$.

– Giả sử $X \equiv Y \pmod 3$. Đặt $x = (X-Y)/3, y = Y$ thì ta có

$$3d = X^2 + 5Y^2 = (3x+y)^2 + 5y^2 \implies 2x^2 + 2xy + 3y^2 = d.$$

– Giả sử $X \equiv -Y \pmod 3$. Đặt $-x = (X+Y)/3, y = Y$ thì

$$3d = X^2 + 5Y^2 = (3x+y)^2 + 5y^2 \implies 2x^2 + 2xy + 3y^2 = d.$$

- $X^2 + 5Y^2 = 4d$. Suy ra $X^2 \equiv 4d \pmod 5$ hay $X^2 \equiv 2, 3 \pmod 5$, vô lý.
- $X^2 + 5Y^2 = 5d$. Khi đó $X = 5X'$ và do đó $5X'^2 + Y^2 \equiv d \pmod 5$. Ta suy ra $Y^2 \equiv d \pmod 5$ và do đó $Y^2 \equiv 2, 3 \pmod 5$, vô lý.
- $X^2 + 5Y^2 = 6d$. Khi đó $X^2 \equiv d \pmod 5$ và như vậy $X^2 \equiv 2, 3 \pmod 5$, vô lý.

Điều kiện đủ được chứng minh hoàn toàn.

□

Nhận xét.

(a) Điều kiện cần cũng có thể được tiến hành nhờ vào luật thuận nghịch toàn phương.

(b) Điều kiện đủ là một trường hợp riêng của vấn đề biểu diễn các số nguyên thành "dạng toàn phương nhị nguyên". Chú ý rằng tam thức bậc hai $2x^2 + 2xy + 3xy$ có biệt thức bằng -20 giống như $x^2 + 5y^2$. Ta có thể chứng minh sự kiện sau đây: với mọi số nguyên tố p,
   - p biểu diễn được dưới dạng $x^2 + 5y^2$ (x, y nguyên) khi và chỉ khi $p \equiv 1, 9 \pmod{20}$;
   - p biểu diễn được dưới dạng $2x^2 + 2xy + 3y^2$ khi và chỉ khi $p \equiv 3, 7 \pmod{20}$.

(c) Các sự kiện trên cho phép một lời giải khác được phác thảo như sau:
   - Chỉ ra rằng mọi ước nguyên tố p của $5 + 1998^{1998}$ thoả mãn $p \equiv 3, 7 \pmod{20}$;
   - Chỉ ra rằng mọi số nguyên tố $\equiv 3, 7 \pmod{20}$ có thể biểu diễn được dưới dạng $2x^2 + 2xy + 3y^2$;
   - Chỉ ra rằng tích của 2 số biểu diễn được dưới dạng như yêu cầu cũng có biểu diễn tương tự.

6. (USAMO 1986.) Tìm số nguyên $n \geq 2$ nhỏ nhất sao cho $\sqrt{\frac{1^2+2^2+\cdots+n^2}{n}}$ là một số nguyên.

Giải. Ta cần tìm các số nguyên dương $n \geq 2$ và k sao cho

$$\frac{(n+1)(2n+1)}{6} = k^2 \Leftrightarrow (4n+3)^2 - 48k^2 = 1.$$

Xét phương trình Pell $x^2 - 48y^2 = 1$. Phương trình có nghiệm nhỏ nhất $(7, 1)$ và các nghiệm nguyên dương của nó được cho bởi dãy $(x_k, y_k)_{n\geq 1}$ định nghĩa bởi

$$x_k + \sqrt{48}y_k = (7 + \sqrt{48})^k.$$

Nói riêng $x_1 = 7, x_2 = 97, x_3 = 1351, \ldots$. Như vậy $k = 3$ là chỉ số nhỏ nhất > 1 sao cho $x_k \equiv 3 \pmod 4$. Giá trị này cho ta $n = \frac{1351-3}{4} = 337$.

Ta kết luận rằng $n = 337$ là giá trị cần tìm.

□

7. Cho n là một số nguyên sao cho $3n+1$ và $4n+1$ đều là các số chính phương. Chứng minh rằng $56 \mid n$.

Giải. Viết $3n+1=a^2, 4n+1=b^2$. Thế thì, $(2a)^2-3b^2=1$. Xét phương trình

$$x^2-3y^2=1.$$

Phương trình có nghiệm nhỏ nhất $(x_0,y_0)=(2,1)$. Ta cần tìm các nghiệm (x_n,y_n) với

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

sao cho x_n chẵn. Điều này xảy ra khi và chỉ khi $n=2k+1$. Như vậy ta có

$$2a=(2+\sqrt{3})^{2k+1}+(2-\sqrt{3})^{2k+1}$$

Ta suy ra $n=\frac{1}{2}(a^2-1)=\frac{1}{12}(x_{2k+1}^2-4)$. Từ đây ta thu được

$$n=\frac{7^{2k+1}-7}{24}+2\binom{2k+1}{2}7^{2k-1}+2\cdot 48\binom{2k+1}{2}7^{2k-3}+\cdots$$

Từ đây ta suy ra $7 \mid n$ và $8 \mid n$. □

8. Chứng minh rằng phương trình

$$x^4+y^3=z^2$$

có vô hạn các nghiêm nguyên dương thoả mãn $(x,z)=1$.

Giải. Ta có

$$x^4+y^3=z^2 \Leftrightarrow y^3=(z+x^2)(z-x^2).$$

Nếu z,x khác tính chẵn lẻ thì $(z+x^2,z-x^2)=1$ và khi đó mỗi nhân tử $z+x^2, x-x^2$ phải là lập phương của một số nguyên lẻ:

$$z+x^2=a^3, z-z^2=b^3.$$

Chú ý rằng nếu $(a,b)=1$ và a,b lẻ thì các hệ trên cho ta $z=\frac{a^3+b^3}{2}, x^2=\frac{a^3-b^3}{2}$. Ta sẽ chọn $a=2y+1, b=2y-1$ với y hợp lý. Chú ý rằng điều này đảm bảo a,b lẻ cũng như $(z,x)=1$ nếu x,z nguyên. Ta cần y và x sao cho

$$x^2=\frac{(2y+1)^3-(2y-1)^3}{2}=6y^2+1.$$

Nói cách khác,

$$x^2-6y^2=1.$$

Rõ ràng $(5, 2)$ là nghiệm nhỏ nhất của phương trình Pell này. Theo lý thuyết các phương trình Pell, phương trình này có vô số nghiệm nguyên dương và được cho bởi

$$x + y\sqrt{6} = (5 + 2\sqrt{6})^n, n \geq 1.$$

Bài toán được chứng minh. □

Cách khác. Bài toán còn có thể được giải quyết bằng cách sử dụng đẳng thức đáng chú ý sau đây: với mọi n nguyên dương thì

$$1^3 + 2^3 + \cdots + (n-1)^3 + n^3 = \left[\frac{(n(n+1)}{2}\right]^2.$$

Từ đó suy ra đẳng thức này còn có thể được viết dưới dạng

$$\left[\frac{(n(n-1)}{2}\right]^2 + n^3 = \left[\frac{(n(n+1)}{2}\right]^2.$$

Như vậy, ta chỉ cần tìm n, x sao cho $\frac{n(n-1)}{2} = x^2$ (và khi đó ta đặt $y = n, z = \frac{n(n+1)}{2}$. Quan hệ giữa x và n còn có thể được viết dưới dạng $4n(n-1) = 8x^2$, hay

$$(2n-1)^2 - 8x^2 = 1.$$

Bằng cách sử dụng phương trình Pell ta dễ dàng xây dựng được vô hạn bộ (n, x) thoả mãn quan hệ trên. Bài toán được giải quyết.

□

9. Chứng minh rằng tồn tại vô hạn số nguyên dương n sao cho

$$n^2 + 1 \mid n!.$$

Giải. Ta sẽ tìm các số nguyên n, m sao cho $n^2 + 1 = km^2$ với $k \geq 2$ cố định, không chính phương. Hơn nữa, ta chọn k để sao cho khi đó $k, m, 2m$ là các số nguyên $\leq n$. Chẳng hạn, ta có thể chọn $k = 5$: $n^2 + 1 = 5m^2 > (2m)^2$ đảm bảo rằng $2m < n$.

Phương trình $x^2 + 1 = 5y^2$, hay $x^2 - 5y^2 = -1$ có nghiệm nguyên nhỏ nhất $(2, 1)$. Phương trình $x^2 - 5y^2 = 1$ có vô số nghiệm. Từ đó suy ra phương trình $x^2 + 1 = 5y^2$ có vô số nghiệm nguyên dương. Trong số các nghiệm này, ta chỉ cần chọn các nghiệm với $y > 5$ khi đó $5, y, 2y$ là phân biệt và $< n$. Với các giá trị đó $x^2 + 1 = 5 \cdot y \cdot y \mid 5 \cdot y \cdot 2y \mid x!$. Từ đó ta có điều cần chứng minh.

□

10. (Phương trình Markov (1).) Cho số nguyên dương k. Chứng minh rằng nếu phương trình

$$x^2 + y^2 + z^2 = kxyz$$

có nghiệm nguyên dương thì $k = 1$ hoặc $k = 3$.

Hơn nữa, chứng minh rằng nếu x, y, z là các số nguyên dương thoả mãn

$$x^2 + y^2 + z^2 = xyz$$

thì x, y, z chia hết cho 3 và $(X, Y, Z) = (x/3, y/3/z/3)$ là các nghiệm của phương trình

$$X^2 + Y^2 + Z^2 = 3XYZ.$$

Giải. Giả sử phương trình đã cho có nghiệm nguyên dương. Hơn thế nữa, ta giả sử x, y, z là nghiệm sao cho $x \le y \le z$ với $\max\{x, y, z\}$ nhỏ nhất. Do tính đối xứng, không giảm tổng quát, giả sử $x \le y \le z$.

Chú ý rằng đẳng thức $x^2 + y^2 + z^2 = kxyz$ chứng tỏ z là nghiệm của phương trình bậc 2:

$$f(T) = T^2 - kxyT + x^2 + y^2 = 0.$$

Chú ý rằng theo định lý Viete, phương trình còn một nghiệm nữa là z' thoả mãn $z + z' = kxy$ và $zz' = x^2 + y^2$. Nói riêng, z' nguyên (vì $z + z'$ nguyên) và dương (vì $zz' = x^2 + y^2 > 0$.)

Mặt khác,

$$f(y) = y^2 - kxy^2 + x^2 + y^2 = 2y^2 - kxy^2 + x^2 = 3y^2 - kxy^2 + (x^2 - y^2) = (3 - kx)y^2 + x^2 - y^2.$$

Như vậy $f(y) < 0$ nếu $3 - kx < 0$, nói riêng nếu $k > 3$ hoặc nếu $3 - kx = 0$ nhưng $x \ne y$. Trong trường hợp này, ta có y nằm giữa các nghiệm z, z', nghĩa là $z' < y < z$. Điều này có nghĩa là bộ (x, y, z') là một nghiệm của phương trình đã cho với $\max\{x, y, z'\} < \max\{x, y, z\}$, vô lý.

Xét $3 - kx \ge 0$, khi đó $kx \le 3$. Nếu $kx = 1$ thì $k = 1 = x$. Nếu $kx = 2$ thì $k = 1, x = 2$ hoặc $k = 2, x = 1$. Nhưng trường hợp này không thể xảy ra vì khi đó $y^2 + z^2 + 1 = 2yz$ hay $(y - z)^2 = 1$. Nếu $kx = 3$ và $x \ne y$ thì ta có mâu thuẫn như đã giải thích ở trên. Ta giả sử $kx = 3$ và $x = y$. Khi đó hoặc $k = 1, x = y = 3$ hoặc $k = 3, x = y = 1$.

Các lập luận trên cho thấy: hoặc $k = 1$ hoặc $k = 3$.

Bây giờ, giả sử $x^2 + y^2 + z^2 = xyz$. Nếu x, y, z đều không chia hết cho 3 thì $x^2 + y^2 + z^2 \equiv 3 \equiv 0 \pmod z$, mâu thuẫn. Như vậy một trong các số x, y, z phải là nghiệm của 3, chẳng hạn $3 \mid x$. Thế thì $y^2 + z^2 \equiv 0 \pmod 3$. Dễ thấy đồng dư này chỉ xảy ra với $y \equiv z \equiv 0 \pmod 3$. Điều này chứng tỏ cả 3 số x, y, z đều chia hết cho 3. Bằng cách đặt $x = 3X, y = 3Y, z = 3Z$ ta suy ra $X^2 + Y^2 + Z^2 = 3XYZ$. Đảo lại, nếu X, Y, Z thoả mãn đẳng thức cuối cùng này thì x, y, z hiển nhiên thoả mãn $x^2 + y^2 + z^2$.

□

Nhận xét.

(a) Nói riêng với $z = 1$ ta suy ra phương trình $x^2 + y^2 + 1 = kxy$ có nghiệm chỉ khi $k = 3$ (chúng ta không thể có $x^2 + y^2 + 1 = xy$ vì lý do hiển nhiên).

(b) Phương pháp xây dựng một nghiệm mới bằng cách sử dụng các hệ thức Viete, đặc biệt trong trường hợp một biến xuất hiện như nghiệm của một tam thức bậc 2 khi cố định các nghiệm còn lại ở trên còn được biết tới tên gọi **bước nhảy Viete**.

11. (Phương trình Markov (2).) Chứng minh rằng có vô hạn bộ số nguyên dương (x, y, z) thoả mãn

$$x^2 + y^2 + z^2 = 3xyz.$$

Giải. Ta sử dụng các lập luận ở bài trước. Phương trình đã cho có nghiệm hiển nhiên $(1, 1, 1)$. Với mỗi nghiệm (x_n, y_n, z_n) ta xây dựng một bộ nghiệm mới như sau. Sắp thứ tự $x_n \leq y_n \leq z_n$. Theo định nghĩa, x_n là nghiệm của

$$f(T) = T^2 - 3y_n z_n T + y_n^2 + z_n^2.$$

Theo định lý Viete, ngoài x_n, phương trình còn một nghiệm x' nữa thoả mãn $x_n + x' = 3y_n z_n, x_n x' = y_n^2 + z_n^2$. Nói riêng x' nguyên dương. Hơn nữa, dễ thấy $x' > 3y_n - x_n > 2y_n > x_n$. Đặt $(x_{n+1}, y_{n+1}, z_{n+1}) = (x', y_n, z_n)$.

Dễ thấy xây dựng này cho ta một dãy vô hạn các nghiệm bởi vì nghiệm tiếp theo lớn hơn nghiệm trước nếu ta định nghĩa thứ tự (trên tập các nghiệm):

$$(x_{n+1}, y_{n+1}, z_{n+1}) > (x_n, y_n, z_n) : |x_{n+1}| + |y_{n+1}| + |z_{n+1}| > |x_n| + |y_n| + |z_n|.$$

□

Nhận xét. Ta có một số bình luận sau đây.

(a) Các nghiệm của phương trình Markov có thể được mô tả một cách tường minh: mọi nghiệm của phương trình $x^2 + y^2 + z^2 = 3xyz$ đều được sinh ra từ nghiệm $(1, 1, 1)$ (nghiệm nhỏ nhất) bằng cách áp dụng liên tiếp các "lật nghiệm Viete".

(b) Ta cũng có thể chỉ ra rằng phương trình $x^2 + y^2 + z^2 = kxyz$ chỉ có nghiệm nguyên dương khi $k = 1$ hoặc 3 như được phác thảo như sau:

- Giả sử phương trình $x^2 + y^2 + z^2 = kxyz$ có nghiệm nguyên dương (a, b, c) thế thì (ka, kb, kc) là một nghiệm của phương trình $x^2 + y^2 + z^2 = xyz$.
- Mọi nghiệm của $x^2 + y^2 + z^2 = xyz$ có dạng $(3A, 3B, 3C)$ với (A, B, C) là nghiệm của $x^2 + y^2 + z^2 = 3xyz$.
- Mọi nghiệm nguyên dương (m, n, p) của phương trình $x^2 + y^2 + z^2 = 3xyz$ đều nguyên thoả mãn: m, n, p là nguyên tố cùng nhau. Sự kiện này có thể được suy ra từ một lập luận dựa vào "bước nhảy Viete".

12. Chứng minh rằng nếu x, y, z là các số nguyên dương thoả mãn

$$x^2 - zxy + y^2 + z = 0$$

thì $z = 5$.

Giải. Ý tưởng ở đây, cũng giống như với phương trình Markov là sử dụng **bước nhảy Viete**. Giả sử phương trình đã cho có nghiệm nguyên dương (x, y, z). Điều này có nghĩa là tập hợp

$$S = \{(a, b); a, b \in \mathbb{Z}^+; a^2 - zab + b^2 + z = 0\}$$

là khác rỗng (lưu ý: ta giả sử (x, y, z) là một nghiệm, như vậy z là một số nguyên dương cố định chứ không phải là một biến!).

Ta dễ dàng kiểm tra rằng nếu $(a, b) \in S$ thì $a \neq b$. Theo giả thiết ở trên $S \neq \emptyset$. Gọi (a_0, b_0) là một phần tử của S sao cho a_0+b_0 là nhỏ nhất (một phần tử như vậy hiển nhiên tồn tại do tính sắp thứ tự tốt của tập các số nguyên dương). Do tính đối xứng của S: $(a, b) \in S \Leftrightarrow (b, a) \in S$, ta có thể giả sử $a_0 \leq b_0$ và như vậy $a_0 < b_0$ theo nhận xét ở trên.

Phương trình bậc hai

$$T^2 - za_0T + a_0^2 + z = 0$$

có một nghiệm hiển nhiên b_0. Gọi nghiệm còn lại là b_1. Theo công thức Viète, ta có

$$b_1 + b_0 = za_0 \quad \text{và} \quad b_1b_0 = a_0^2 + z.$$

Như vậy $b_1 \in \mathbb{Z}^+$. Ta suy ra $(a_0, b_1) \in S$ và do đó, theo định nghĩa của (a_0, b_0) ta phải có bất đẳng thức

$$b_1 \geq b_0.$$

Theo công thức Viete ở trên $b_1 = \frac{a_0^2}{b_0}$. Từ đó suy ra $\frac{a_0^2}{b_0} \geq b_0 \implies b_0^2 - a_0^2 \geq z \implies (b_0 - a_0)(b_0 + a_0) \geq z$. Mặt khác, $b_0 > a_0$ theo giả thiết, ta suy ra $2a_0 < z$ hay

$$z \geq 2a_0 + 1.$$

Ta quay lại phương trình bậc hai $T^2 - za_0T + a_0^2 + z = 0$ với các nghiệm nguyên dương b_0, b_1. Ta biết rằng biệt thức của nó phải là một số chính phương. Ta có

$$\Delta = z^2a_0^2 - 4(a_0^2 + z).$$

Như vậy $\Delta < z^2a_0^2$. Mặt khác do $\Delta \equiv za_0 \pmod 2$ ta cũng suy ra $\Delta \neq (za_0 - 1)^2$. Như vậy $\Delta \leq (za_0 - 2)^2$. Điều này có nghĩa là

$$4za_0 - 4 - 4(a_0^2 + z) \leq 0, \quad \text{hay} \quad z(a_0 - 1) - a_0^2 - 1 \leq 0.$$

Mặt khác ta biết rằng $z \geq 2a_0 + 1$ nên $z(a_0 - 1) - a_0^2 - 1 \geq (2a_0 + 1)(a_0 - 1) - a_0^2 - 1 = a_0^2 - a_0 - 2 = (a_0 + 1)(a_0 - 2)$. Bất đẳng thức trên chỉ có thể xảy ra khi

$$a_0 = 1 \quad \text{hoặc} \quad a_0 = 2.$$

Xét các trường hợp:

$a_0 = 1$. Ta có $z = \frac{b_0^2+1}{b_0-1} = b_0 + \frac{2}{b_0-1}$. Ta suy ra $b_0 - 1 = 1$ hoặc 2 hay $b_0 = 2$ hoặc 3. Với cả hai trường hợp ta có $z = 5$ (tuy nhiên trường hợp $b_0 = 3$ bị loại theo định nghĩa của (a_0, b_0).

$a_0 = 2$. Ta có $z = \frac{b_0^2+4}{2b_0-1} \implies 4z = \frac{4b_0^2+16}{2b_0-1} \implies 2b_0 + 1 + \frac{17}{2b_0-1} \implies 2b_0 - 1 = 1$ hoặc 17. Như vậy $b_0 = 1$ hoặc $b_0 = 9$. Với cả hai trường hợp ta đều có $z = 5$ nhưng đều bị loại, trường hợp thứ nhất vì $b_0 < a_0$, trường hợp thứ 2 vì với $z = 5$ bộ $(2, 9)$ không phải là bộ có tổng nhỏ nhất (mà là $(1, 2)$ ở trên).

Kết luận, ta có $z = 5$ và giá trị này thỏa mãn điều kiện bài toán.

□

Nhận xét. Các lập luận trên đây thực ra cho ta nhiều thông tin hơn các yêu cầu của bài toán. Chẳng hạn, với $z = 5$, phương trình trở thành

$$x^2 - 5xy + y^2 + 5.$$

Các lập luận trên chứng tỏ $(1, 2)$ là nghiệm nguyên dương nhỏ nhất theo nghĩa tổng $1 + 2$ là nhỏ nhất (và điều này có thể được kiểm tra trực tiếp). Chú ý rằng, nếu $x = 1$ thì phương trình trở thành $y^2 - 5y + 6 = 0$ và do đó $(1, 2), (1, 3)$ là các nghiệm duy nhất với $x = 1$.

13. (Việt Nam TST 1995.) Tìm tất cả các số nguyên x, y thoả mãn

$$x^2 - 5xy + y^2 + 5 = 0.$$

Giải. Một lần nữa, ý tưởng là lập luận sử dụng bước nhảy Viete: từ một nghiệm (a, b) bất kì, ta suy luận bằng "xuống thang", xây dựng một nghiệm khác nhỏ hơn, và tiếp tục xuống thang như vậy, v.v. Cho đến khi ta không thể xuống thang được nữa, có nghĩa là ta nhận được một nghiệm nhỏ nhất theo một nghĩa chính xác nào đó. Để mô tả nghiệm ban đầu, ta liệt kê tất các nghiệm nhỏ nhất có thể và "đi lên" để có nghiệm ban đầu.

Cụ thể hơn, ta tiến hành như sau. Giả sử (a, b) là một nghiệm nguyên dương của phương trình đã cho mà ta sẽ kí hiệu là $(*)$. Rõ ràng rằng nếu (a, b) là một nghiệm thì (b, a) cũng là một nghiệm. Hơn nữa, chú ý rằng ta luôn có $a \neq b$ (nếu không $a^2 - 5a^2 + a^2 + 5 = 0 \implies 3a^2 = 5$!) Ta sẽ giả sử $a < b$. Đặt $a_0 = b, a_1 = a$. Ta sẽ xây dựng một dãy các số nguyên dương (a_n) bằng qui nạp dựa vào các tính chất:

- $a_0 = b, a_1 = a$;
- (a_i, a_{i+1}) là một nghiệm của $(*)$ với mọi i;
- a_{n+2} được xây dựng từ a_{n+1}, a_n như sau: bởi vì (a_n, a_{n+1}) là một nghiệm của $(*)$, a_n là một nghiệm của

$$T^2 - 5Ta_{n+1} + a_{n+1}^2 + 5 = 0,$$

nên theo công thức Viete, phương trình còn một nghiệm nữa mà ta sẽ đặt là a_{n+2}.

Lưu ý rằng các hệ thức Viete

$$a_{n+2} + a_n = 5a_{n+1}, a_{n+2}a_n = a_{n+1}^2 + 5$$

cho thấy a_{n+2} cũng là một số nguyên dương và dĩ nhiên (a_{n+1}, a_{n+2}) cũng là một nghiệm nguyên dương của $(*)$.

Bây giờ, ta sẽ nghiên cứu dáng điệu của dãy (a_n): ta sẽ thấy rằng, nói chung, nếu $a_n > a_{n+1}$ thì gần như luôn luôn ta sẽ có $a_{n+1} > a_{n+2}$, trừ một vài trường hợp ngoại lệ.

Thật vậy, giả sử $a_n > a_{n+1}$. Ta có $a_{n+2} = \frac{a_{n+1}^2+5}{a_n} \leq \frac{a_{n+1}^2+5}{a_{n+1}+1}$. Ta xác định xem với các giá trị của a_{n+1} nào thì ta có $a_{n+2} < a_{n+1} + 1$? Lưu ý rằng điều này dẫn đến $a_{n+1} \leq a_n$ và do đó $a_{n+1} < a_n$ (bởi vì ta biết rằng nếu (A, B) là một nghiệm của $(*)$ thì $A \neq B$). Bất đẳng thức $a_{n+2} < a_{n+1} + 1$ được đảm bảo nếu ta có $a_{n+1}^2 + 5 < (a_{n+1} + 1)^2$. Nói cách khác nếu ta có $a_{n+1} > 2$.

Như vậy, dãy (a_n) xây dựng ở trên, nếu bắt đầu với $a > 2$, sẽ luôn luôn giảm ngặt cho đến khi một số hạng nào đó bằng 1 hoặc 2.

Ta quan sát kí hơn trường hợp tới hạn : nếu $a_{n+1} = 1, 2$ thì a_n, a_{n+2} bằng bao nhiêu ?

- Giả sử $a_{n+1} = 1$. Khi đó a_n, a_{n+2} là các nghiệm của phương trình $T^2 - 5T + 6 = 0$, hay $a_n, a_{n+2} \in \{2, 3\}$.
- Giả sử $a_{n+1} = 2$. Khi đó a_n, a_{n+2} là các nghiệm của $T^2 - 10T + 9$, hay $a_n, a_{n+2} \in \{1, 9\}$. Chú ý rằng nếu $a_n = 9$ thì $a_{n+2} = 1$ và ngược lại.

Các lập luận trên đây chứng tỏ hoặc $(b, a) = (2, 1), (3, 1)$ hoặc nếu không từ (b, a) (với $b > a$) sẽ sinh ra một dãy a_n định nghĩa như trên sao cho tồn tại một chỉ số N nhỏ nhất nào đó để $a_0 > a_1 > \cdots > a_N$ và $a_N = 1$ hoặc $a_N = 2$. Trong trường hợp thứ 2, ta có $a_{N-1} = 9$ và do đó $a_{N+1} = 1$. Như vậy trong mọi trường hợp, tồn tại chỉ số nguyên dương N nhỏ nhất để $a_N = 1$. Điều này hiển nhiên cũng đúng nếu ta xuất phát từ bộ nghiệm $(2, 1)$ hoặc $(3, 1)$. Hơn thế nữa, nếu $a_N = 1$ thì $a_{N-1} = 2$ hoặc $a_{N-1} = 3$.

Các lập luận trên cho thấy dãy a_n có dạng

$$a, b, \ldots, 2, 1, 2, 1, \cdots \quad \text{hoặc} \quad b, a, \ldots, 3, 1, 3, 1, \cdots .$$

Cuối cùng, để "khôi phục" lại (a, b) ta để ý rằng dãy số a_n định định nghĩa bằng quan hệ truy hồi: $a_{n+2} + a_n = 5a_{n+1}$. Từ đó suy ra, (a, b) là các số hạng liên tiếp của một trong 1 dãy:

$$\begin{cases} u_0 = 1, u_1 = 2, \\ u_n = 5u_{n+1} - u_n. \end{cases} \qquad \begin{cases} v_0 = 1, v_1 = 3, \\ v_n = 5v_{n+1} - v_n. \end{cases}$$

Các suy luận ở trên có thể đảo ngược và cho thấy các bộ (u_n, u_{n+1}) và $(v_n, v_{n+1}), (n \geq 0)$ là thoả mãn $(*)$ và do đó chúng là tập tất cả các nghiệm nguyên dương của $(*)$.

□

Nhận xét. Có lẽ lớp phương trình nghiệm nguyên bậc hai trên 2 biến có vô hạn nghiệm cơ bản nhất là lớp các phương trình Pell. Không phải ngẫu nhiên mà phương trình $(*)$ có vô hạn nghiệm nguyên dương. Thật vậy, ta có thể biến đổi $(*)$ để đưa nó về dạng "đường chéo" như sau:

$$x^2 - 5xy + 5y^2 + 5 = 0 \Leftrightarrow 4x^2 - 20xy + 4y^2 + 20 = 0 \Leftrightarrow (2x + 5y)^2 - 21y^2 = -20.$$

Từ đây, bằng việc nghiên cứu phương trình Pell: $X^2 - 21Y^2 = -20$ ta cũng có thể giải quyết được bài toán.

14. (Theo VMO 2012.) Tìm tất cả các bộ số nguyên dương (x, y, z, t) với x, y lẻ thoả mãn

$$\begin{cases} x^2 + 2 = yz \\ y^2 + 2 = xt \end{cases}$$

Giải. Ta tiếp tục sử dụng bước nhảy Viete.

Giả sử x, y, z, t là các số nguyên thoả mãn hệ phương trình đã cho với x, y lẻ. Dễ thấy nếu d là một ước chung của x và y thì $d \mid 2$. Điều kiện x, y là các số lẻ dẫn đến $d = 1$, hay x, y nguyên tố cùng nhau. Bây giờ, ta có $x \mid y^2 + 2 \implies x \mid x^2 + y^2 + 2$ và $y \mid x^2 + 2 \implies y \mid x^2 + y^2 + 2$. Như vậy, bởi vì $(x, y) = 1$ ta suy ra $xy \mid x^2 + y^2 + 2$. Viết lại quan hệ này dưới dạng

$$x^2 + y^2 + 2 = kxy \Leftrightarrow x^2 - kyx + y^2 + 2 = 0 \quad (k \in \mathbb{Z}_{\geq 0}).$$

Chú ý rằng đẳng thức $x^2 - kxy + y^2 + 2 = 0$ suy ra x, y là các số nguyên lẻ và $(x, y) = 1$. Thật vậy nếu $x^2 - kxy + y^2 + 2 = 0$ và $d = (x, y)$ thì $d^2 \mid 2 \implies (x, y) = 1$. Nói riêng x, y không thể cùng chẵn. Bằng cách xét modulo 2 đẳng thức $x^2 - kxy + y^2 + 2 = 0$ ta cũng nhận thấy x, y không thể khác tính chẵn lẻ. Từ đó suy ra $(x, y) = 1$ và cùng lẻ.

Trước hết nhận xét rằng $k \geq 3$. Thật ra, ta sẽ chỉ ra rằng $k = 4$.

Gọi (x, y) là một bộ số nguyên dương thỏa mãn điều kiện bài toán. Nếu $x = y$ thì ta dễ dàng suy ra $x = y = 1$ và $k = 4$. Ta giả sử $x \neq y$ và không mất tổng quát $x < y$. Ta xây dựng dãy số nguyên $(a_i)_{i \geq 0}$ như sau

$$\begin{cases} a_0 &= y, a_1 = x, \\ a_{i+2} &= ka_{i+1} - a_i, \ \forall i \geq 0. \end{cases}$$

Chú ý rằng với mọi do $x = a_0$ là nghiệm của phương trình

$$x^2 - ka_1 x + a_1^2 + 2 = 0$$

nên theo định nghĩa a_2 là nghiệm còn lại của phương trình này. Nói riêng ta có $a_2 = \frac{a_1^2+2}{a_0} > 0$. Như vậy a_2 là một số nguyên dương. Các lập luận tương tự cho $a_3, \ldots$ chứng tỏ dãy (a_i) là một dãy các số nguyên dương thỏa mãn: a_{i+1}, a_{i-1} là hai nghiệm của

$$x^2 - ka_i x + a_i^2 + 2 = 0, \ \forall i.$$

Lưu ý rằng các lập luận ở trên cho thấy a_i là một dãy số nguyên dương lẻ. Bây giờ, ta chứng minh

$$1 < a_i < a_{i-1} \implies a_{i+1} < a_i.$$

Thật vậy, ta có $a_{i+1} = \frac{a_i^2+2}{a_{i-1}} \leq \frac{a_i^2+2}{a_i+1} = a_i + \frac{2-a_i}{a_i} < a_i$ bởi vì $a_i \geq 3$.

Ta suy ra tồn tại một chỉ số N sao cho $a_0 > a_1 > \cdots > a_{N-2} > a_{N-1} = 1$. Lại chú ý rằng a_{N-2} là nghiệm nguyên dương của $x^2 - ka_{N-1}x + a_{N-1}^2 = 0 \Leftrightarrow x^2 - kx + 3 = 0$ nên $a_{N-2} \mid 3 \implies a_{N-2} = 3$ (bởi vì $a_{N-2} > a_{N-1}$). Ta suy ra $k = 4$. Ta cũng chú ý rằng $a_N = a_{N-1} = 1$.

Bây giờ, dãy số (a_i) thỏa mãn $a_{N-1} = a_N = 1$ và $a_{i-2} = 4a_{i-1} - a_i$ với mọi i. Như vậy, nếu ta định nghĩa $b_i = a_{N-i}$ thì ta có $n = a_0 = b_N, m = a_1 = b_{N-1}$ và $b_0 = b_1 = 1$, $b_{i+2} = 4b_{i+1} - b_i$. Nói cách khác, các số nguyên dương lẻ m, n thỏa mãn điều kiện là các số hạng liên tiếp của dãy sai phân

$$b_0 = b_1 = 1, b_{i+2} = 4b_{i+1} - b_i.$$

Ta dễ dàng tìm được công thức cụ thể của m, n bằng cách giải phương trình sai phân này.

□

Nhận xét. Tương tự như bài tập trước. Một khi ta đã chỉ ra được rằng $k = 4$ thì ta có thể xác định được các nghiệm của phương trình $x^2 + y^2 + 2 = 4xy$ bằng cách sử dụng lý thuyết các phương trình Pell dựa vào đổi đơn giản:

$$x^2 + y^2 + 2 = 4xy \Leftrightarrow (x - 2y)^2 - 3y^2 = -2.$$

3 Phương trình bậc ba

1. (Italia 94.) Tìm các bộ số nguyên x, y thỏa mãn

$$y^2 = x^3 + 16.$$

Giải. Đây là bài tập khá đơn giản. Ta có thể bắt đầu bằng phương pháp phân tích thành nhân tử và nhận xét rằng phương trình đã cho tương đương với

$$(y - 4)(y + 4) = x^3.$$

Nếu y lẻ thì $y - 4, y + 4$ là nguyên tố cùng nhau nên chúng phải là các lập phương. Từ đó suy ra hiệu của hai số lập phương này bằng 8. Bằng các lập luận quen thuộc (phân tích thành nhân tử, bất đẳng thức) ta dễ dàng chỉ ra được rằng điều này không thể xảy ra.

Như vậy, y chẵn và do đó x chẵn. Đặt $y = 2y', x = 2x'$ và phương trình ban đầu trở thành

$$(y' - 2)(y' + 2) = 2x'^3.$$

Ta suy ra y' chẵn, như vậy có dạng $y' = 2u$ và do đó x' cũng chẵn $x' = 2v$. Bây giờ, quan hệ của u và v được viết dưới dạng

$$(u - 1)(u + 1) = 4v^3.$$

Từ đây, u là lẻ, $u = 2u'$ và $u'(u' + 1) = v^3$. Việc kết thúc bài toán không còn trở ngại nào nữa: mỗi $u', u' + 1$ là lập phương của một số nguyên, do đó $u' = -1$ hoặc $u' = 0$ và $v = 0$ trong cả hai trường hợp. Quay ngược lại các giá trị, ta suy ra nghiệm các nghiệm $(x, y) = (0, \pm 4)$. □

2. Tìm các số nguyên x, y sao cho

$$y^2 = x^3 + (x + 4)^2.$$

Giải. Phương trình có các nghiệm hiển nhiên $(x, y) = (0, \pm 4)$. Ta sẽ chứng minh phương trình không có nghiệm với $x \neq 0$. Viết phương trình dưới dạng

$$x^3 = (y - x - 4)(y + x + 4).$$

Với $x \neq 0$ thì $y - x - 4$ và $y + x + 4$ khác 0, kí hiệu d là ước chung lớn nhất của chúng. Ta có

$$\begin{aligned} &d \mid x \\ d \mid y - x - 4, d \mid y + x + 4 \implies &d \mid 2x + 8 \end{aligned}$$

Từ đó suy ra $d \mid 8$. Ta phân ra các trường hợp

- $d = 1$. Thế thì $y - x - 4 = a^3, y + x + 4 = b^3$ với a, b nào đó. Ta suy ra $x = ab$ và $2x + 8 = b^3 - a^3$. Ta suy ra

  $$2ab + 8 = (b - a)(b^2 - ab + a^2) = (b - a)((b - a)^2 + 3ab).$$

  Chú ý rằng $b \neq a$ vì nếu không $x = -4$ và $y^2 = -64$! Nếu $ab > 0$ thì vế trái $\geq 3ab + 1$ và $2ab + 8 \geq 3ab + 1 \implies ab \leq 7$. Hơn nữa, các lập luận chi tiết hơn cho thấy có các trường hợp

  - $b - a = 1 \implies ab = 7$, vô lý;
  - $b - a \geq 2 \implies 2ab + 8 > 6ab \implies ab < 2 \implies ab = 1 \implies a = b$, vô lý.

  Như vậy $ab < 0$ và khi đó $b < a \implies b < 0 < a$. Khi đó $-2ab - 8 = a^3 - b^3 = a^3 - (-b)^3 \geq a^2 + (-b)^2 \geq -2ab$ vô lý.
- $d = 2$. Ta suy ra $y - x - 4 = 2a, y + x + 4 = 2b$ với $(a, b) = 1$ nào đó. Ta suy ra $x^3 = 4ab$ và do đó $2 \mid x$. Điều này hiển nhiên cho thấy $2 \mid y$. Nhưng $y = a + b$ nên $2 \mid a + b$. Do $(a, b) = 1$ ta suy ra a, b phải lẻ. Thế nhưng khi đó $x^3 = 4ab$ không thể xảy ra!
- $d = 4$. Ta suy ra $y - x - 4 = 4a, y + x + 4 = 4b$ với $(a, b) = 1$. Ta có $x^3 = 16ab$ nên $4 \mid x$, từ đó suy ra $4 \mid ab$. Do a, b nguyên tố cùng nhau nên một trong hai số a, b là lẻ và số còn lại là bội của 4. Thế nhưng ta lại có $4 \mid x, 4 \mid y - x - 4 \implies 4 \mid y$ và $y = 2(a + b) \not\equiv 0 \pmod 4$!
- $d = 8$. Ta suy ra $y - x - 4 = 8a, y + x + 4 = 8b$ với $(a, b) = 1$ nào đó. Như vậy $x^3 = 64ab \implies 4 \mid x$. Từ $(x/4)^3 = ab$ ta suy ra $a = a_0^3, b = b_0^3$. Lại do $2x + 8 = 8(b - a) = 8(b_0^3 - a_0^3)$. Ta suy ra $a_0 b_0 + 1 = b_0^3 - a_0^3$. Các lập luận tương tự (phương pháp chặn) như trên cũng cho ta điều vô lý.

□

3. (Lebesgue) Chứng minh rằng phương trình

$$y^2 = x^3 + 7$$

không có nghiệm nguyên.

Giải. Giả sử (x, y) là một nghiệm nguyên của phương trình đã nêu. Suy luận đơn giản theo modulo 4 cho thấy x không thể chẵn. Vậy x lẻ và do đó y chẵn. Ta viết lại phương trình đã cho dưới dạng

$$y^2 + 1 = x^3 + 8 = (x + 2)(x^2 - 2x + 4)$$

Vì x lẻ nên $x^2 - 2x + 4 = (x - 1)^2 + 3 \equiv 3 \pmod 4$ do đó $x^2 - 2x + 4$ có một ước nguyên tố lẻ $p \equiv 3 \pmod 4$. Nhưng ta lại có $y^2 + 1 \equiv 0 \pmod p$. Điều này chứng tỏ -1 là chính phương modulo p và như vậy $p \equiv 1 \pmod 4$, mâu thuẫn.

□

4. Chứng minh rằng phương trình

$$y^2 = x^3 - 5$$

không có nghiệm nguyên.

Giải. Ta tiến hành tương tự như với bài tập trước. Xét phương trình theo modulo 4. Nếu x chẵn thì $y^2 \equiv -1 \pmod 4$ vô lý. Vậy x lẻ và như vậy y chẵn. Vì x lẻ nên ta có $x^3 \equiv x \pmod 4$. Mặt khác, $y^2 \equiv 0 \pmod 4$ nên từ phương trình ban đầu ta suy ra $x \equiv 1 \pmod 4$. Viết lại phương trình dưới dạng

$$y^2 + 4 = x^3 - 1 = (x - 1)(x^2 + x + 1)$$

Một mặt, bởi vì $x \equiv 1 \pmod 4$ nên $x^2 + x + 1 \equiv 3 \pmod 4$. Như vậy $x^2 + x + 1 > 0$ có một ước nguyên tố $p \equiv 3 \pmod 4$. Mặt khác $y^2 + 2^2 \equiv 0 \pmod p$ kéo theo -1 là chính phương modulo p nên $p \equiv 1 \pmod 4$ và ta có điều mâu thuẫn.

□

5. Tìm các số nguyên x, y sao cho

$$y^2 = x^3 + 4x.$$

Giải. Ta có kết quả quen thuộc sau.

Bổ đề. *Phương trình*

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

không có nghiệm nguyên không tầm thường (nghĩa là $xyz \neq 0$).

Chứng minh. Đây là ứng dụng quen thuộc của phương pháp xuống thang cùng với miêu tả các bộ ba Pitago. □

Tất nhiên, với cùng phương pháp, ta chứng minh được rằng $x^4 + y^4 = z^2$ cũng không có nghiệm không tầm thường. Như là một hệ quả, Định lý Fermat đúng với $n = 4$.

Quay lại bài toán. Ta có

$$y^4 = (x^3 + 4x)^2 = x^6 + 8x^4 + 16x^2 = x^6 - 8x^4 + 16x^2 + 16x^4 = (x^3 - 4x)^2 + (2x)^4.$$

Hay

$$y^4 - (2x)^4 = (x^3 - 4x)^2.$$

Nhưng ta biết rằng phương trình $r^4 - s^4 = t^2$ không có nghiệm không tầm thường. Như vậy ta phải có $x = 0$ hoặc $y = 0$ hoặc $x^3 = 4x$, nghĩa là $y = 0$ hoặc $x = 0$ hoặc $x = \pm 2$. Thay vào phương trình đầu tiên ta thu được $(x, y) = (0, 0), (\pm 4, 2)$.

□