BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN, ĐHQGHN

* * *

Nguyễn Văn Mậu, Bùi Công Huấn,
Đặng Hùng Thắng, Trần Nam Dũng, Đặng Huy Ruận

MỘT SỐ CHUYÊN ĐỀ TOÁN HỌC CHỌN LỌC BỒI DƯỠNG HỌC SINH GIỎI

HÀ NỘI - 2004

MỤC LỤC

Lời nói đầu

Chương trình đào tạo và bồi học sinh năng khiếu toán bậc phổ thông hiện sang năm thứ 39. Gắn với việc đổi mới phương pháp dạy và học chương trình năm nay, năm 2004, chúng ta đang tích cực chuẩn bị cho việc tổ chức Kỳ thi (Toán quốc tế năm 2007 tại Việt Nam, kỷ niệm 40 năm Tạp chí Toán học và ' 30 năm các đội tuyển nước ta tham dự các kỳ thi Olympic Toán quốc tế.

Có thể nói, giáo dục mũi nhọn phổ thông đã thu được những thành tựu rực Nhà nước đầu tư có hiệu quả, xã hội thừa nhận và bạn bè quốc tế khâm ph đội tuyển Toán quốc gia tham dự các kỳ thi Olympic Toán quốc tế có bề dà tích mang tính ổn định và có tính kế thừa. Đặc biệt, năm nay, Đội tuyển To gia tham dự thi Olympic Toán quốc tế đã đạt được thành tích rực rỡ: 4 huy vàng và 2 huy chương bạc, đứng thứ 4 thế giới. Nhiều năm các đội tuyển To gia tham dự các kỳ thi Olympic Toán quốc tế giữ vững được vị trí từ thứ 4 đến (Top Ten) trên tổng số gần 100 đội tuyển quốc gia tham gia.

Từ nhiều năm nay, Các Hệ và các Trường THPT Chuyên thường sử dụng sc các sách giáo khoa đại trà kết hợp với sách giáo khoa cho Hệ THPT Chuyê Học sinh các lớp năng khiếu đã tiếp thu tốt các kiến thức cơ bản theo thời lượ hành do Bộ GD và ĐT ban hành.

Hiện nay, chương trình cải cách giáo dục đang bước vào giai đoạn hoàn c SGK mới. Thời lượng kiến thức cũng như trật tự kiến thức cơ bản có những đáng kể. Các kiến thức này đang được cân nhắc để nó vẫn nằm trong khuôn k hành của các kiến thức nâng cao đối với các lớp chuyên toán. Vì lẽ đó, việc ti viết các SGK cho các lớp năng khiếu toán chưa thể tiến hành cấp bách trong t ngắn, đòi hỏi có sự suy ngẫm và xem xét toàn diện của các chuyên gia giác các cô giáo, thầy giáo đang trực tiếp giảng dạy các lớp chuyên.

Được sự cho phép của Bộ GD và ĐT, Trường Đại Học Khoa Học Tự ĐHQGHN phối hợp cùng với các chuyên gia, các nhà khoa học, các cô gi giáo thuộc ĐHSPHN, ĐHQG TpHCM, ĐH Vinh, Viện Toán Học, Hội Toán Nội, NXBGD, Tạp Chí Toán Học và Tuổi Trẻ, các Trường THPT Chuyên, Các và ĐT,... tổ chức Chương trình bồi dưỡng nghiệp vụ sau đại học về các chuyê dưỡng học sinh giỏi toán.

Nội dung chính của chuyên đề gồm hai phần: Phương trình, bất phương trì trong hình học và Một số vấn đề chọn lọc của số học.

Để đáp ứng cho nhu cầu bồi dưỡng giáo viên và bồi dưỡng học sinh giỏi tôi in cuốn Kỷ yếu này nhằm cung cấp một số kiến thức cơ bản và ứng dụng chuyên đề Toán Phổ Thông.

Đây cũng là chuyên đề và bài giảng mà các tác giả đã giảng dạy cho h và sinh viên các đội tuyển thi olympíc toán quốc gia và quốc tế và là chuyên dưỡng nghiệp vụ sau đại học cho các giáo viên dạy các lớp chuyên toán.

Chúng tôi cũng xin chân thành cảm ơn các bạn đọc cho những ý kiến đ để cuốn sách ngày càng hoàn chỉnh.

T/M Ban Tổ Chức

GS TSKH Nguyễn Văn Mậu

MỘT SỐ ĐẶC TRƯNG CƠ BẢN CỦA HÀM SỐ

Nguyễn Văn Mậu

1.1. Đặc trưng hàm của một số hàm số sơ cấp

Trong phần này ta nêu những đặc trưng hàm của một số hàm số sơ cấp, t
gặp trong chương trình phổ thông. Nhờ các đặc trưng hàm này mà ta có thể d
đáp số của các phương trình hàm tương ứng cũng như có thể đề xuất dạng h
tương tự ứng với các đặc trưng hàm đó.

Các hàm số được xét trong phần này thoả mãn điều kiện liên tục trên toàn
xác định của hàm số. Nếu hàm số thoả mãn các đặc trưng hàm đã cho mà khô
tính liên tục hoặc được xác định trên các tập rời rạc thì nghiệm của phương trìn
có thể là một biểu thức hoàn toàn khác.

1. Hàm bậc nhất: $f(x) = ax + b$ (với $a, b \neq 0$).
   Đặc trưng hàm:
$$f(\frac{x+y}{2}) = \frac{f(x)+f(y)}{2} \quad \text{với mọi } x, y \in \mathbb{R}.$$

2. Hàm tuyến tính: $f(x) = ax$ (với $a \neq 0$).
   Đặc trưng hàm:
$$f(x+y) = f(x) + f(y) \quad \text{với mọi } x, y \in \mathbb{R}.$$

3. Hàm mũ: $f(x) = a^x$ (với $a > 0$; $\neq 1$).
   Đặc trưng hàm:
$$f(x+y) = f(x).f(y) \quad \text{với mọi } x, y \in \mathbb{R}.$$

4. Hàm logarit: $f(x) = log_a|x|$ (với $a > 0$; $\neq 1$).
   Đặc trưng hàm:
$$f(x.y) = f(x) + f(y) \quad \text{với mọi } x, y \in \mathbb{R}^*.$$

5. Hàm sin : $f(x) = \sin x$.
   Đặc trưng hàm:
$$f(3x) = 3f(x) - 4f^3(x) \quad \text{với mọi } x \in \mathbb{R}.$$

6. Hàm cos : $f(x) = \cos x$.
Đặc trưng hàm:

$$f(x) = 2f^2(x) - 1 \quad \text{với mọi } x \in \mathbb{R}.$$

hoặc $f(x+y) + f(x-y) = 2f(x)f(y)$ với mọi $x, y \in \mathbb{R}$.

7. Hàm tang: $f(x) = \operatorname{tg} x$.
Đặc trưng hàm:

$$f(x+y) = \frac{f(x)+f(y)}{1-f(x)f(y)} \quad \text{với mọi } x, y \in \mathbb{R}, x+y \neq \frac{(2k+1)\pi}{2}, k \in \mathbb{Z}.$$

8. Hàm cotang: $f(x) = \operatorname{cotg} x$.
Đặc trưng hàm:

$$f(x+y) = \frac{f(x)f(y)-1}{f(x)+f(y)} \quad \text{với mọi } x, y \in \mathbb{R}, x+y \neq k\pi, k \in \mathbb{Z}.$$

9. Hàm luỹ thừa: $f(x) = x^a$ (với $a \in \mathbb{R}$; $x \in \mathbb{R}^+$).
Đặc trưng hàm:

$$f(xy) = f(x)f(y) \quad \text{với mọi } x, y \in \mathbb{R}^+.$$

10. Hàm lượng giác ngược: $f(x) = \arcsin x$.
Đặc trưng hàm:

$$f(x) + f(y) = f(x\sqrt{1-y^2} + y\sqrt{1-x^2}) \quad \text{với mọi } x, y \in [-1;1].$$

11. Hàm lượng giác ngược: $f(x) = \arccos x$.
Đặc trưng hàm:

$$f(x) + f(y) = f(xy - \sqrt{(1-x^2)(1-y^2)}) \quad \text{với mọi } x, y \in [-1;1].$$

12. Hàm lượng giác ngược: $f(x) = arctgx$.
Đặc trưng hàm:

$$f(x) + f(y) = f\left(\frac{x+y}{1-xy}\right) \quad \text{với mọi } x, y \in \mathbb{R} \text{ ; } xy \neq 1.$$

13. Hàm lượng giác ngược: $f(x) = arccotgx$.
Đặc trưng hàm:

$$f(x) + f(y) = f\left(\frac{xy-1}{x+y}\right) \quad \text{với mọi } x, y \in \mathbb{R} \text{ ; } x+y \neq 0.$$

14. Hàm sin hyperbolic: $f(x) = \frac{1}{2}(e^x - e^{-x}) := shx$.
Đặc trưng hàm:

$$f(3x) = 3f(x) + 4f^3(x) \quad \text{với mọi } x \in \mathbb{R}.$$

15. Hàm cos hyperbolic: $f(x) = \dfrac{1}{2}(e^x + e^{-x}) := \operatorname{ch} x$.
Đặc trưng hàm:

$$f(x+y) + f(x-y) = 2f(x)f(y) \quad \text{với mọi } x, y \in \mathbb{R}.$$

16. Hàm tang hyperbolic: $f(x) = \dfrac{e^x - e^{-x}}{e^x + e^{-x}} := thx$.
Đặc trưng hàm:

$$f(x+y) = \frac{1 + f(x)f(y)}{f(x) + f(y)} \quad \text{với mọi } x, y \in \mathbb{R}.$$

17. Hàm cotangenchyperbolic: $f(x) = \dfrac{e^x + e^{-x}}{e^x - e^{-x}} := cothx = \dfrac{1}{thx}$.
Đặc trưng hàm:

$$f(x+y) = \frac{1 + f(x)f(y)}{f(x) + f(y)} \quad \text{với mọi } x, y \in \mathbb{R}.$$

Tương tự, ta cũng có các đặc trưng hàm của các hàm số sau đây.

18. $f(x) = \operatorname{tg} cx$, thì $f(x+y) = \dfrac{f(x) + f(y)}{1 - f(x)f(y)}$,

19. $f(x) = \operatorname{cotg} cx$, thì $f(x+y) = \dfrac{f(x)f(y) - 1}{f(x) + f(y)}$,

20. $f(x) = c \operatorname{th} cx$, thì $f(x+y) = \dfrac{f(x) + f(y)}{1 + \dfrac{f(x)f(y)}{c^2}}$,

21. $f(x) = \dfrac{c}{x}$, thì $f(x+y) = \dfrac{f(x)f(y)}{f(x) + f(y)}$,

22. $f(x) = \dfrac{1}{1 + \operatorname{cotg} cx}$, thì $f(x+y) = \dfrac{f(x) + f(y) - 2f(x)f(y)}{1 - 2f(x)f(y)}$,

23. $f(x) = \dfrac{1}{1 + \operatorname{tg} cx}$, thì $f(x+y) = \dfrac{f(x) + f(y) - 1}{2f(x) + 2f(y) - 2f(x)f(y) - 1}$,

24. $f(x) = \dfrac{cx}{1 - cx}$, thì $f(x+y) = \dfrac{f(x) + f(y) + 2f(x)f(y)}{1 - f(x)f(y)}$,

25. $f(x) = -\dfrac{cx}{1 - cx}$, thì $f(x+y) = \dfrac{f(x) + f(y) - 2f(x)f(y)}{1 - f(x)f(y)}$,

26. $f(x) = \dfrac{\sin cx}{\sin(cx + a)}$, thì $f(x+y) = \dfrac{f(x) + f(y) - 2f(x)f(y)\cos a}{1 - f(x)f(y)}$,

27. $f(x) = \dfrac{\operatorname{sh} cx}{\operatorname{sh}(cx + a)}$, thì $f(x+y) = \dfrac{f(x) + f(y) - 2f(x)f(y)\operatorname{ch} a}{1 - f(x)f(y)}$,

28. $f(x) = -\dfrac{\operatorname{sh} cx}{\operatorname{sh}(cx + a)}$, thì $f(x+y) = \dfrac{f(x) + f(y) + 2f(x)f(y)\operatorname{ch} a}{1 - f(x)f(y)}$,

29. $f(x) = ae^{cx^2}$, thì $af(\sqrt{x^2 + y^2}) = f(x)f(y)$,

30. $f(x) = \left(\dfrac{c + x}{c - x}\right)^d$, thì $f\left(\dfrac{x+y}{1 + \dfrac{xy}{c^2}}\right) = f(x)f(y)$,

31. $f(x) = (1+cx)^a$, thì $f(x+y+cxy) = f(x)f(y)$,
32. $f(x) = cx^n$, thì $f\left(\sqrt[n]{x^n+y^n}\right) = f(x)+f(y)$, $x, y \geqslant 0$,
33. $f(x) = c(x^2+1)$, thì $f\left(\sqrt{x^2+y^2+1}\right) = f(x)+f(y)$,
34. $f(x) = cx^2$, thì $f(x+y)-f(x-y) = 4\sqrt{f(x)f(y)}$,
35. $f(x) = cx^2$, thì $f(x+y)+f(x-y) = 2[f(x)+f(y)]$,
36. $f(x) = cx+a$, thì $f(x+y)+f(x-y) = 2f(x)$,
37. $f(x) = cx$, thì $f(x+y)-f(x-y) = 2f(y)$.

⋮

1.2. Hàm số chuyển đổi phép tính số học và đại số

Trong mục này, ta khảo sát một số tính chất cơ bản của một số dạng hàm số thông qua các hệ thức hàm đơn giản. Ta cũng khảo sát một số dạng hàm bảo toàn và chuyển đổi các tính chất cơ bản của phép tính đại số như giao hoán, phân bố và kết hợp.

Bài toán 1. Xác định các hàm số $f(x)$ xác định và liên tục trên $\mathbb{R}$ thoả mãn điều kiện

$$f(x+y) = f(x)+f(y)+f(x)f(y), \quad \forall x, y \in \mathbb{R}. \tag{1}$$

Giải.

Đặt $f(x) = g(x)-1$, ta thu được

$$g(x+y)-1 = g(x)-1+g(y)-1+[g(x)-1][g(y)-1], \quad \forall x, y \in \mathbb{R}$$

hay

$$g(x+y) = g(x)g(y), \quad \forall x, y \in \mathbb{R}. \tag{2}$$

Do $f(x)$ liên tục trên $\mathbb{R}$ nên $g(x)$ cũng là hàm liên tục trên $\mathbb{R}$. Suy ra (2) có nghiệm $g(x) = e^{ax}, a \in \mathbb{R}$ và (1) có nghiệm

$$f(x) = e^{ax}-1, \ a \in \mathbb{R}.$$

Bài toán 2. Cho hàm số $F(u,v)$ $(u, v \in \mathbb{R})$. Giả sử phương trình hàm:

$$f(x+y) = F[f(x), f(y)], \quad \forall x, y \in \mathbb{R} \tag{3}$$

có nghiệm $f(x)$ xác định và liên tục trên $\mathbb{R}$. Chứng minh rằng $F(u,v)$ là hàm đối xứng ($F(u,v) = F(v,u)$ và có tính kết hợp

$$F[F(u,v), w] = F[u, F(v,w)], \quad \forall u, v, w \in \Im f. \tag{4}$$

Giải.

Nhận xét rằng tính đối xứng của $F(u,v)$ được suy trực tiếp từ (3). Mặt khác, theo (3), ta có

$$f(x+y+z) = f[(x+y)+z] = F\{F[f(x), f(y)], f(z)\}, \quad \forall x, y, z \in \mathbb{R} \tag{5}$$

và

$$f(x+y+z) = f[x+(y+z)] = f[(y+z)+x] = F\{F[f(y), f(z)], f(x)$$
$$= F\{f(x), F[f(y), f(z)]\}, \ \forall x, y, z \in \mathbb{R}.$$

Từ (5) và (6) suy ra (4):

$$F[F(u,v), w] = F[u, F(v,w)], \ \forall u, v, w \in \Im f.$$

Bài toán 3. Giả sử phương trình hàm:

$$f(x+y) = F[f(x), f(y)], \ \forall x, y \in \mathbb{R}$$

với hàm số $F(u,v)$ $(u, v \in \mathbb{R})$ là một đa thức (khác hằng), có nghiệm $f(x)$ xác và liên tục (khác hằng) trên $\mathbb{R}$. Chứng minh rằng $F(u,v)$ có dạng

$$F(u,v) = auv + bu + bv + c.$$

Giải.

Giả sử $F(u,v)$ là đa thức bậc m theo u và bậc n theo v. Khi đó, do $F(u,v$ xứng nên $m = n$. Theo (4) thì

$$F[F(u,v), w] = F[u, F(v,w)], \ \forall u, v, w \in \Im f$$

nên vế trái là một đa thức bậc n theo w còn vế phải là đa thức bậc n^2 theo w. S $n^2 = n$ hay $n = 1$. Vậy $F(u,v)$ có dạng

$$F(u,v) = auv + b_1 u + b_2 v + c.$$

Do $F(u,v)$ là đa thức đối xứng nên $b_1 = b_2$ và

$$F(u,v) = auv + bu + bv + c.$$

Nhận xét rằng, với $F(u,v) = auv + bu + bv + c$ và $F(u,v)$ thoả mãn điều (4) thì

$$ac = b^2 - b.$$

Vậy với $a \neq 0$ thì

$$ac = b^2 - b \Leftrightarrow c = \frac{b^2 - b}{a}, \ a \neq 0.$$

Bây giờ, ta chuyển sang xét các dạng đặc biệt của (7).

Bài toán 4. Cho đa thức $F(u,v) = bu + bv + c$, $b \neq 0$. Xác định các hàm số xác định và liên tục trên $\mathbb{R}$ thoả mãn điều kiện

$$f(x+y) = F[f(x), f(y)], \ \forall x, y \in \mathbb{R}$$

tức là

$$f(x+y) = bf(x) + bf(y) + c, \ \forall x, y \in \mathbb{R}.$$

Giải.

Nhận xét rằng, nếu $b \neq 1$ thì từ (9) với $y = 0$, ta có ngay $f(x) = \text{const}$. Khi $b = \frac{1}{2}$ và $c = 0$ thì mọi hàm hằng đều thoả mãn (8). Khi $b = \frac{1}{2}$ và $c \neq 0$ thì (9) vô nghiệm. Các trường hợp khác ($b \neq 1$, $b \neq \frac{1}{2}$ thì nghiệm của (9) là $f(x) = \frac{c}{1-2b}$.

Xét trường hợp $b = 1$. Khi đó (9) có dạng

$$f(x+y) = f(x) + f(y) + c, \ \forall x, y \in \mathbb{R}$$

và phương trình hàm này có nghiệm $f(x) = \alpha x - c$.

Bài toán 5. Cho đa thức $F(u,v) = auv + bu + bv + \frac{b^2 - b}{a}$, $a \neq 0$. Xác định các hàm số $f(x)$ xác định và liên tục trên $\mathbb{R}$ thoả mãn điều kiện

$$f(x+y) = F[f(x), f(y)], \ \forall x, y \in \mathbb{R}$$

tức là

$$f(x+y) = af(x)f(y) + bf(x) + bf(y) + \frac{b^2 - b}{a}, \ \forall x, y \in \mathbb{R}. \tag{10}$$

Giải.

Nhận xét rằng, nếu đặt

$$f(x) = \frac{h(x) - b}{a}$$

thì thì từ (10) ta nhận được

$$h(x+y) = h(x)h(y), \ \forall x, y \in \mathbb{R}$$

và phương trình hàm này có nghiệm $h(x) = e^{\alpha x}$. Suy ra nghiệm của (10) có dạng

$$f(x) = \frac{e^{\alpha x} - b}{a}.$$

Bài toán 6. Giả sử $f(x)$ là nghiệm của phương trình hàm:

$$f(ax + by + c) = Af(x) + Bf(y) + C \, (abAB \neq 0), \ \forall x, y \in \mathbb{R} \tag{11}$$

Chứng minh rằng hàm số $g(x) = f(x) - f(0)$ thoả mãn phương trình Cauchy

$$g(x+y) = g(x) + g(y), \ \forall x, y \in \mathbb{R}.$$

Giải.

Lần lượt đặt $x = \frac{u}{a}$, $y = \frac{v-c}{b}$; $x = \frac{u}{a}$, $y = -\frac{c}{b}$; $x = 0$, $y = \frac{v-c}{b}$; $x = 0$ $y = -\frac{c}{b}$ vào (11), ta thu được các đẳng thức

$$f(u+v) = Af\Big(\frac{u}{a}\Big) + Bf\Big(-\frac{v-c}{b}\Big) + C,$$

$$f(u) = Af\Big(\frac{u}{a}\Big) + Bf\Big(-\frac{c}{b}\Big) + C,$$

$$f(v) = Af(0) + Bf\Big(\frac{v-c}{b}\Big) + C,$$

$$f(0) = Af(0) + Bf\Big(-\frac{c}{b}\Big) + C.$$

Suy ra

$$f(u+v) = f(u) + f(v) - f(0).$$

Từ đây suy ra điều phải chứng minh.

Bài toán 7. Giả sử hàm số $f(x)$ liên tục trên $\mathbb{R}$ là nghiệm của phương trình l

$$f(ax+by+c) = Af(x) + Bf(y) + C\,(abAB \neq 0),\ \ \forall x, y \in \mathbb{R}.$$

Chứng minh rằng khi đó $A = a$, $B = b$.

Giải.

Thật vậy, nghiệm của

$$g(x+y) = g(x) + g(y),\ \ \forall x, y \in \mathbb{R}$$

trong lớp các hàm liên tục là hàm tuyến tính $g(x) = \alpha x$. Do vậy, nghiệm $f($ dạng $f(x) = \alpha x + \beta$. Thế vào (11), ta thu được $A = a$, $B = b$ và

$$\alpha c - C = (a + b - 1)\beta.$$

Bài toán 8. Giải và biện luận phương trình hàm sau trong lớp các hàm số $f(x$ tục trên $\mathbb{R}$:

$$f(ax+by+c) = Af(x) + Bf(y) + C\,(abAB \neq 0),\ \ \forall x, y \in \mathbb{R}.$$

Giải.

Theo Bài toán 7, thì điều kiện cần để phương trình hàm (11) có nghiệm là a $b = B$.

Giả sử điều kiện này được thoả mãn. Theo (12), ta chia các trường hợp riê khảo sát.

Xét các trường hợp sau:

Trường hợp $b + a = 1,\ c = 0.$

Khi đó, (11) có dạng

$$f(ax + (1-a)y) = af(x) + (1-a)f(y)\,(abAB \neq 0),\ \ \forall x, y \in \mathbb{R}.$$

Ta thu được (13) thuộc lớp hàm chuyển tiếp các đại lượng trung bình cộng. V (13) có nghiệm $f(x) = \alpha x + \beta$, $\alpha, \beta \in \mathbb{R}$.

Trường hợp $b + a = 1,\ c \neq 0.$

Khi đó, (11) có dạng

$$f(ax + (1-a)y + c) = af(x) + (1-a)f(y) + C\,(abAB \neq 0),\ \ \forall x, y \in \mathbb{R}.$$

Đặt $f(x) = \dfrac{C}{c}x + h(x)$. Ta thu được (13) dưới dạng

$$h(ax + (1-a)y + c) = ah(x) + (1-a)h(y),\ \ \forall x, y \in \mathbb{R}.$$

Dễ kiểm tra, phương trình (14) chỉ có nghiệm hằng tuỳ ý (xem (12)) và vì vậy, (13) có nghiệm $f(x) = \dfrac{C}{c}x + \beta$, $\beta \in \mathbb{R}$.

Trường hợp $b+a \neq 1$. Theo Bài toán 6 thì nghiệm của (13) có dạng $f(x) = \alpha x + \beta$. Theo (12) thì $\alpha c - C = (a+b-1)\beta$. Vậy nếu cho $\alpha \in \mathbb{R}$ giá trị tuỳ ý thì $\beta = \dfrac{\alpha c - C}{a+b-1}$.

Chú ý

Nếu không đòi hỏi nghiệm của (11) là hàm số liên tục trên $\mathbb{R}$ thì các đẳng thức $a = A$, $b = B$ và (12) có thể không thoả mãn. Tuy nhiên, ta vẫn có các tính chất đại số sau đây.

Bài toán 9. Giả sử phương trình hàm

$$f(ax + y) = Af(x) + f(y) \ \ (aA \neq 0), \ \ \forall x, y \in \mathbb{R} \tag{15}$$

có nghiệm khác hằng. Chứng minh rằng nếu a (hoặc A) là số đại số với đa thức tối tiểu $P_a(t)$(tương ứng $P_A(t)$) thì A (tương ứng a) là số đại số và

$$P_a(t) \equiv P_A(t). \tag{16}$$

Giải.

Ta thấy $f(0) = 0$ nên $f(ax) = af(x)$ và bằng quy nạp toán học, dễ dàng chứng minh

$$f(a^k x) = A^k f(x), \ \ k \in \mathbb{N}. \tag{17}$$

Giả sử

$$P_a(t) = t^n + \sum_{i=0}^{n-1} r_i t^i, \ \ r_0, \ldots, r_{n-1} \in \mathbb{Q}.$$

Khi đó, theo (17) thì

$$f\Big[(a^n + \sum_{i=0}^{n-1} r_a^i)x\Big] = f(a^n x) + \sum_{i=0}^{n-1} r_i f(a^i x)$$

$$\Big(A^n + \sum_{i=0}^{n-1} r_A^i\Big) f(x).$$

Vì $f(x)$ khác hằng nên

$$A^n + \sum_{i=0}^{n-1} r_A^i = 0 \tag{18}$$

và vì vậy A là số đại số. Suy ra $P_a(t)$ là ước của $P_A(t)$ và do $P_A(t)$ là đa thức tối tiểu nên có (16).

Ngược lại, nếu A là số đại số thoả mãn (18) thì thực hiện quy trình ngược lại, ta thu được

$$a^n + \sum_{i=0}^{n-1} r_a^i = 0 \tag{19}$$

và từ đó suy ra (16).

Bài toán 10. Giả sử phương trình hàm

$$f(ax+y) = Af(x) + f(y) \ \ (aA \neq 0,\ a \in \mathbb{Q}),\ \ \forall x, y \in \mathbb{R}$$

có nghiệm khác hằng. Chứng minh rằng khi đó $a = A$.

Giải.

Thật vậy, theo Bài toán 9 thì $P_a(t)$ là đa thức bậc nhất và vì vậy $P_A(t)$ cũng thức bậc nhất (với hệ số bậc cao nhất đều bằng 1) nên $a = A$.

Bài toán 11. Giải phương trình hàm sau trong lớp các hàm số $f(x)$ liên tục tr

$$f(x+y) = a^{xy} f(x) f(y)\,(a > 0),\ \ \forall x, y \in \mathbb{R}.$$

Giải.

Dễ thấy $f(1) \geqslant 0$. Nếu $f(1) = 0$ thì từ (21) ta có ngay $f(x) \equiv 0$. Xét trườn $f(1) > 0$. Bằng quy nạp, dễ dàng kiểm chứng hệ thức

$$f(nx) = a^{\frac{(n^2-n)x^2}{2}} [f(x)]^n,\ \ \forall n \in \mathbb{N}^*.$$

Vậy với $x = 1$ thì

$$f(n) = a^{\frac{n^2-n}{2}} [f(1)]^n,\ \ \forall n \in \mathbb{N}^*.$$

Với $x = \dfrac{m}{n}$, ta thu được

$$f(m) = a^{\frac{(n^2-n)(\frac{m}{n})^2}{2}} \left[f(\frac{m}{n})\right]^n,\ \ \forall m, n \in \mathbb{N}^*.$$

và

$$f(m) = a^{\frac{m^2-m}{2}} [f(1)]^m,\ \ \forall m \in \mathbb{N}^*.$$

Suy ra

$$f\left(\frac{m}{n}\right) = a^{\frac{1}{2}(\frac{m}{n})^2} \left[a^{-\frac{1}{2}} f(1)\right]^{\frac{m}{n}}.$$

Do $f(1) > 0$ nên có thể viết

$$c = -\frac{1}{2} + \log_a f(1).$$

Từ (21) suy ra

$$f(x) = a^{\frac{1}{2}x^2+cx},\ \ \forall x \in \mathbb{Q}^+.$$

Do $f(x)$ liên tục nên (16) thoả mãn với mọi $x \in \mathbb{R}^+$. Với $x < 0$, ta đặt $-x =$ do $f(0) = 1$ nên từ giả thiết (21) ta nhận được

$$1 = a^{-x^2} f(x) a^{(x^2/2)-cx},$$

hay

$$f(x) = a^{\frac{1}{2}x^2+cx},\ \ \forall x \in \mathbb{R}.$$

Nhận xét.

Bằng cách đặt

$$f(x) = a^{x^2/2} g(x)$$

ta đưa (15) về dạng quen biết

$$g(x+y) = g(x)g(y), \ \ \forall x \in \mathbb{R}.$$

Bài toán 12. Xác định các hàm số f xác định và liên tục trên $\mathbb{R}$ thoả mãn điều kiện

$$f(x+y) + f(z) = f(x) + f(y+z), \ \ \forall x, y, z \in \mathbb{R}. \tag{1}$$

Giải.

Đặt $f(0) = a$ thì với $z = 0$ trong (1) ta thu được

$$f(x+y) + a = f(x) + f(y), \ \ \forall x, y \in \mathbb{R}. \tag{2}$$

Đặt $f(x) = g(x) + a$. Từ (2) ta nhận được

$$g(x+y) = g(x) + g(y), \ \ \forall x, y \in \mathbb{R}. \tag{3}$$

Phương trình (3) có nghiệm $g(x) = \alpha x$, $\alpha \in \mathbb{R}$.

Suy ra phương trình (1) có nghiệm

$$f(x) = \alpha x + \beta, \ \ \alpha, \beta \in \mathbb{R}.$$

Thử lại, ta thấy hàm $f(x) = \alpha x + \beta$ thoả mãn điều kiện bài ra.

Bài toán 13. Xác định các hàm số f xác định và liên tục trên $\mathbb{R}$ thoả mãn điều kiện

$$f(x+y)f(z) = f(x)[f(y) + f(z)], \ \ \forall x, y, z \in \mathbb{R}. \tag{4}$$

Giải.

Thay $y = z = 0$ trong (4), ta thu được $f(0)f(x) = 0$. Vậy $f(0) = 0$. Với $z = 0$ thì

$$f(x+y)f(0) = f(x)[f(y) + f(0)], \ \ \forall x, y \in \mathbb{R}$$

hay

$$f(x)f(y) = 0, \ \ \forall x, y \in \mathbb{R}.$$

Suy ra $f(x) \equiv 0$.

Bài tập

Bài 1. Xác định hàm số $f(x)$ xác định và liên tục trong miền xác định và thoả mãn điều kiện:

$$f(x+y) = \frac{f(x)f(y) - 1}{f(x) + f(y)}.$$

Bài 2. Xác định hàm số $f(x)$ xác định và liên tục trong miền xác định và thoả mãn điều kiện:

$$f(x+y) = \frac{f(x) + f(y)}{1 + \dfrac{f(x)f(y)}{c^2}}.$$

Bài 3. Xác định hàm số $f(x)$ xác định và liên tục trong miền xác định và th
điều kiện:

$$f(x+y) = \frac{f(x)f(y)}{f(x)+f(y)}.$$

Bài 4. Xác định hàm số $f(x)$ xác định và liên tục trong miền xác định và th
điều kiện:

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

Bài 5. Xác định hàm số $f(x)$ xác định và liên tục trong miền xác định và th
điều kiện:

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

Bài 6. Xác định hàm số $f(x)$ xác định và liên tục trong miền xác định và th
điều kiện:

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

Bài 7. Xác định hàm số $f(x)$ xác định và liên tục trong miền xác định và th
điều kiện:

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

Bài 8. Xác định hàm số $f(x)$ xác định và liên tục trong miền xác định và th
điều kiện:

$$f(x+y) = \frac{f(x)+f(y)-2f(x)f(y)\cos a}{1-f(x)f(y)}.$$

Bài 9. Xác định hàm số $f(x)$ xác định và liên tục trong miền xác định và th
điều kiện:

$$f(x+y) = \frac{f(x)+f(y)-2f(x)f(y)\mathrm{ch\,a}}{1-\mathrm{f(x)f(y)}}.$$

Bài 10. Xác định hàm số $f(x)$ xác định và liên tục trong miền xác định và th
điều kiện:

$$f(x+y) = \frac{f(x)+f(y)+2f(x)f(y)\mathrm{ch\,a}}{1-\mathrm{f(x)f(y)}}.$$

Bài 11. Xác định hàm số $f(x)$ xác định và liên tục trong miền xác định và th
điều kiện:

$$af(\sqrt{x^2+y^2}) = f(x)f(y).$$

Bài 12. Xác định hàm số $f(x)$ xác định và liên tục trong miền xác định và th
điều kiện:

$$f\Big(\frac{x+y}{1+\frac{xy}{c^2}}\Big) = f(x)f(y).$$

Bài 13. Xác định hàm số $f(x)$ xác định và liên tục trong miền xác định và th
điều kiện:

$$f(x+y+cxy) = f(x)f(y).$$

Bài 14. Xác định hàm số $f(x)$ xác định và liên tục trong miền xác định và thoả mãn điều kiện:

$$f\left(\sqrt[n]{x^n + y^n}\right) = f(x) + f(y), \quad x, y \geqslant 0.$$

Bài 15. Xác định hàm số $f(x)$ xác định và liên tục trong miền xác định và thoả mãn điều kiện:

$$f\left(\sqrt{x^2 + y^2 + 1}\right) = f(x) + f(y).$$

Bài 16. Xác định hàm số $f(x)$ xác định và liên tục trong miền xác định và thoả mãn điều kiện:

$$f(x + y) - f(x - y) = 4\sqrt{f(x)f(y)}.$$

Bài 17. Xác định hàm số $f(x)$ xác định và liên tục trong miền xác định và thoả mãn điều kiện:

$$f(x + y) + f(x - y) = 2[f(x) + f(y)].$$

Bài 18. Xác định hàm số $f(x)$ xác định và liên tục trong miền xác định và thoả mãn điều kiện:

$$f(x + y) + f(x - y) = 2f(x).$$

Bài 19. Xác định hàm số $f(x)$ xác định và liên tục trong miền xác định và thoả mãn điều kiện:

$$f(x + y) - f(x - y) = 2f(y).$$

BẤT PHƯƠNG TRÌNH HÀM CƠ BẢN

Nguyễn Văn Mậu

2.1 Bất phương trình hàm với cặp biến tự do

Bài toán 1. Xác định các hàm số $f(x)$ thoả mãn đồng thời các điều kiện sa

(i) $f(x) \geqslant 0, \ \forall x \in \mathbb{R},$

(ii) $f(x+y) \geqslant f(x) + f(y), \ \forall x, y \in \mathbb{R}.$

Bài giải. Thay $x = 0$ vào điều kiện đầu bài, ta thu được

$$\begin{cases} f(0) \geqslant 0 \\ f(0) \geqslant 2f(0) \end{cases} \quad \text{hay} \quad f(0) = 0.$$

Vậy nên

$$f(0) = f(x + (-x)) \geqslant f(x) + f(-x) \geqslant 0.$$

Suy ra $f(x) \equiv 0$. Thử lại, ta thấy hàm số $f(x) \equiv 0$ thoả mãn điều kiện bài ra.

Bài toán 2. Cho trước hàm số $h(x) = ax$, $a \in \mathbb{R}$. Xác định các hàm số $f($ mãn đồng thời các điều kiện sau:

(i) $f(x) \geqslant ax, \ \forall x \in \mathbb{R},$

(ii) $f(x+y) \geqslant f(x) + f(y), \ \forall x, y \in \mathbb{R}.$

Bài giải. Để ý rằng $h(x+y) = h(x) + h(y)$. Đặt $f(x) = h(x) + g(x)$. Kh thu được các điều kiện (i) $g(x) \geqslant 0, \ \forall x \in \mathbb{R},$

(ii) $g(x+y) \geqslant g(x) + g(y), \ \forall x, y \in \mathbb{R}.$

Lặp lại cách giải Bài toán 1. Thay $x = 0$ vào điều kiện đầu bài, ta thu đư

$$\begin{cases} g(0) \geqslant 0 \\ g(0) \leqslant 0 \end{cases} \quad \text{hay} \quad g(0) = 0.$$

Vậy nên

$$g(0) = g(x + (-x)) \geqslant g(x) + g(-x) \geqslant 0.$$

Điều này kéo theo $g(x) \equiv 0$ hay $f(x) = ax$. Thử lại, ta thấy hàm số $f(x) = ax$ thoả mãn điều kiện bài ra.

Bài toán 3. Cho số dương a. Xác định các hàm số $f(x)$ thoả mãn đồng thời các điều kiện sau:

(i) $f(x) \geqslant a^x, \ \forall x \in \mathbb{R}$,

(ii) $f(x+y) \geqslant f(x)f(y), \ \forall x, y \in \mathbb{R}$.

Bài giải. Để ý rằng $f(x) > 0$ với mọi $x \in \mathbb{R}$. Vậy ta có thể logarit hoá hai vế các bất đẳng thức của điều kiện đã cho.

(i) $\ln f(x) \geqslant (\ln a)x, \ \forall x \in \mathbb{R}$,

(ii) $\ln f(x+y) \geqslant \ln f(x) \ln f(y), \ \forall x, y \in \mathbb{R}$.

Đặt $\ln f(x) = \varphi(x)$, ta thu được

(i) $\varphi(x) \geqslant (\ln a)x, \ \forall x \in \mathbb{R}$,

(ii) $\varphi(x+y) \geqslant \varphi(x)\varphi(y), \ \forall x, y \in \mathbb{R}$.

Ta nhận được Bài toán 2. Bằng cách đặt $\varphi(x) = g(x) + (\ln a)x$, ta thu được các điều kiện

(i) $g(x) \geqslant 0, \ \forall x \in \mathbb{R}$,

(ii) $g(x+y) \geqslant g(x) + g(y), \ \forall x, y \in \mathbb{R}$

và $g(x) \equiv 0$ hay $\varphi(x) = (\ln a)x$. Suy ra $f(x) = a^x$ Thử lại, ta thấy hàm số $f(x) = a^x$ thoả mãn điều kiện bài ra.

Bài toán 4. Xác định các hàm số $f(x)$ thoả mãn các điều kiện sau:

$$f(x) \geqslant f(0), \ f\Big(\frac{x+y}{2}\Big) \geqslant \frac{f(x)+f(y)}{2}, \ \forall x, y \in \mathbb{R}. \tag{1}$$

Bài giải. Đặt $f(0) = a$ và $f(x) - a = g(x)$. Khi đó (1) có dạng

$$g(x) \geqslant 0, \ g\Big(\frac{x+y}{2}\Big) \geqslant \frac{g(x)+g(y)}{2}, \ \forall x, y \in \mathbb{R} \tag{2}$$

với $g(0) = 0$.

Thay $y = 0$ vào (2), ta thu được

$$g\Big(\frac{x}{2}\Big) \geqslant \frac{g(x)}{2} \text{ hay } g(x) \geqslant 2g\Big(\frac{x}{2}\Big), \ \forall x \in \mathbb{R}. \tag{3}$$

Từ (2) và (3), ta suy ra

$$g\Big(\frac{x+y}{2}\Big) \geqslant g\Big(\frac{x}{2}\Big) + g\Big(\frac{y}{2}\Big), \ \forall x, y \in \mathbb{R}$$

hay

$$g(0) = 0, \ g(x) \geqslant 0, \ g(x+y) \geqslant g(x) + g(y), \ \forall x, y \in \mathbb{R}. \tag{4}$$

Tiếp theo, ta nhận được Bài toán 1. Suy ra $g(x) \equiv 0$ và $f(x) = \text{const}$.

Thử lại, ta thấy hàm số $f(x) \equiv c$ thoả mãn điều kiện bài ra.

2.2. Biểu diễn hàm số

Trong mục này, ta mô tả một số công thức biểu diễn hàm cơ bản. Các bi này thường gắn với các mục đích mô tả các đặc trưng hàm, các tính chất c thức dưới dạng tường minh và đơn giản hơn. Đây là những hệ thức rất quan trọ quan đến những ràng buộc dạng bất đẳng thức cho trước. Trong mục tiếp the xét riêng cho trường hợp biểu diễn đa thức dương trên một tập.

Bài toán 1. Xác định các hàm số $f(t)$ thỏa mãn điều kiện:

$$f(x) = \max_{y \in \mathbb{R}} \{2xy - f(y)\}, \ \forall x \in \mathbb{R}.$$

Giải.

Trước hết, từ (1) ta suy ra

$$f(x) \geqslant 2xy - f(y), \ \forall x, y \in \mathbb{R}.$$

Thay $x = y = t$ vào (2), ta thu được bất đẳng thức

$$f(t) \geqslant x^2, \ \forall x \in \mathbb{R}.$$

Ta có

$$2xy - f(y) \leqslant 2xy - y^2 = x^2 - (x-y)^2, \ \forall x, y \in \mathbb{R}.$$

Mà

$$\max_{y \in \mathbb{R}} \{x^2 - (x-y)^2\} = x^2.$$

Suy ra $f(x) \leqslant x^2$. Kết hợp với (3), ta được $f(x) = x^2$.

Thử lại, ta thấy hàm số $f(x) = x^2$ thoả mãn điều kiện bài ra.

Bài toán 2. Xác định các hàm số $f(t)$ thỏa mãn điều kiện:

$$f(x) = \max_{y \in \mathbb{R}^+} \{x^2 y + xy^2 - f(y)\}, \ \forall x \in \mathbb{R}^+.$$

Giải.

Tương tự như Bài toán 1, ta suy ra

$$f(x) \geqslant x^2 y + xy^2 - f(y), \ \forall x, y \in \mathbb{R}^+.$$

Thay $x = y = t$ vào (4), ta thu được bất đẳng thức

$$f(t) \geqslant x^3, \ \forall x \in \mathbb{R}^+.$$

Từ (4) và (5), suy ra

$$x^2y + xy^2 - f(y) \leqslant x^2y + xy^2 - y^3 = x^3 - (x+y)(x-y)^2 \leqslant x^3, \ \forall x, y \in \mathbb{R}^+$$

nên

$$\max_{y \in \mathbb{R}^+} \{x^3 - (x+y)(x-y)^2\} = x^3.$$

Suy ra $f(x) \leqslant x^3$. Kết hợp với (5), ta được $f(x) = x^3$.

Thử lại, ta thấy hàm số $f(x) = x^3$ thoả mãn điều kiện bài ra.

Nhận xét 1. Điều khẳng định trên cho ta một kết luận tương đương sau đây:

Nếu có một bất đẳng thức cổ điển cho cặp số x, y, chẳng hạn

$$x^3 + y^3 \geqslant x^2y + xy^2 \ \forall x, y \in \mathbb{R}^+$$

hay

$$x^3 \geqslant x^2y + xy^2 - y^3 \ \forall x, y \in \mathbb{R}^+$$

thì từ điều kiện

$$f(x) = \max_{y \in \mathbb{R}^+} \{x^2y + xy^2 - f(y)\}, \ \forall x \in \mathbb{R}^+$$

ta có ngay hàm cần tìm $f(x)$ có dạng $f(x) = x^3$.

Bài toán 3. Chứng minh rằng nếu:
+) Hoặc $f'(x) > 0$ và $h(x) \geqslant 0$ với mọi $x \in \Omega \subseteq D_f$
+) Hoặc $f'(x) \geqslant 0$ và $h(x) > 0$ với mọi $x \in \Omega \subseteq D_f$
thì trong Ω ta có:

$$f(g(x)) + g(x).h(x) \geqslant f(0) \Leftrightarrow g(x) \geqslant 0. \tag{1}$$

Giải.

Sử dụng định lý Lagrange, ta có

$$\begin{aligned} f(g(x)) + g(x).h(x) \geqslant f(0) &\Leftrightarrow f(g(x)) - f(0) + g(x).h(x) \geqslant 0 \\ &\Leftrightarrow [f'(c) + h(x)]g(x) \geqslant 0 \quad (c \text{ nằm giữa } 0 \text{ và } g(x)) \\ &\Leftrightarrow g(x) \geqslant 0 \quad (\text{do } [f'(c) + h(x)] > 0) \text{ (đpcm).} \end{aligned}$$

Bài toán 4. Giải bất phương trình:

$$3^{x^2-4} + (x^2 - 4)3^{x-2} \geqslant 1.$$

Giải.

Xét hàm số $f(x) = 3^x$. Hàm số $f(x)$ xác định, liên tục, khả vi với mọi $x \in \mathbb{R}$ và $f'(x) = 3^x.ln3$. Ta có

$$\begin{aligned} &(3) f(x^2 - 4) - f(0) + (x^2 - 4)3^{x-2} \geqslant 0 \quad (\text{do } f(0) = 1) \\ &f'(c)[x^2 - 4 - 0] + (x^2 - 4)3^{x-2} \geqslant 0 \\ &(c \text{ nằm giữa } 0 \text{ và } x^2 - 4, \text{ theo định lý Lagrange}) \\ &[x^2 - 4].[3^c.ln3 + 3^{x-2}] \geqslant 0 \\ &x^2 - 4 \geqslant 0 \quad (\text{do } 3^c.ln3 + 3^{x-2} > 0, \quad x \in \mathbb{R}) \\ &x \leqslant -2 \ \vee \ 2 \leqslant x. \end{aligned}$$

Vậy bất phương trình có nghiệm

$$x \leqslant -2 \ \vee \ x \geqslant 2.$$

Bài toán 5. Cho các số dương $M,\ a.$ Tìm các hàm số $f(x); g(x) : \mathbb{R} \to$ mãn điều kiện

$$|f(y) - f(x) - g(x)(x-y)| \leqslant M.|x-y|^{2+a},\ \forall x; y \in \mathbb{R}.$$

Giải.

Giả sử tồn tại các hàm số $f(x),\ g(x)$ thoả mãn yêu cầu bài ra. Đổi chỗ $x;$ (2), ta được

$$|f(x) - f(y) - g(y)(y-x)| \leqslant M.|y-x|^{2+a} \quad (13.1) \text{ với mọi } x; y \in \mathbb{R}$$

Cộng từng vế với vế của (3), ta thu được

$$|(g(x) - g(y))(x-y)| \leqslant 2M.|y-x|^{2+a}.$$

Suy ra

$$\left|\frac{g(x)-g(y)}{x-y}\right| \leqslant 2M.|x-y|^a,\ \forall x; y \in \mathbb{R},\ x \neq y.$$

Trong (4) ta cố định x, cho $y \to x$ ta được

$$g'(x) = 0,\ x \in \mathbb{R}, \text{nên } g(x) = c = \text{const},\ \forall x \in \mathbb{R}.$$

Mặt khác, thay $g(x) = c$ vào (1) và làm tương tự như trên, ta cũng nhận được

$$\left|\frac{f(x)-f(y)}{x-y} - c\right| \leqslant 2M.|x-y|^a,\ \forall x; y \in \mathbb{R},\ x \neq y.$$

Cố định x và cho $y \to x$ ta được

$$f'(x) = c,\ x \in \mathbb{R} \quad \text{nên } f(x) = cx + d,\ x \in \mathbb{R}\ (d := \text{const}).$$

Thử lại thấy hai hàm số $f(x) = cx + d\ ;\ g(x) = c$ thoả mãn yêu cầu bài ra. V hàm số cần tìm là

$$f(x) = cx + d\ ;\ g(x) = c \text{ với } c; d \text{ là các hằng số } \in \mathbb{R}.$$

Bài toán 6. Chứng minh rằng

$$|x| = \max_{|a| \leqslant 1}(ax).$$

Giải. Dễ dàng kiểm tra công thức

$$-|x| \geqslant ax \leqslant |x|,\ \forall a \in [-1, 1].$$

Từ đây ta có ngay đpcm.

2.3 Biểu diễn các đa thức dương trên một tập

Trong phần này ta xét một số biểu diễn của đa thức dương trên một tập dưới dạng tổng, hiệu, tích.... của các đa thức có dạng đặc biệt cho trước.

Bài toán 1. Cho đa thức $P(x) \in \mathbb{R}[x]$ và $P(x) \geqslant 0$ với mọi $x \in \mathbb{R}$. Chứng minh rằng đa thức $P(x)$ có thể biểu diễn được dưới dạng

$$P(x) = [A(x)]^2 + [B(x)]^2,$$

trong đó $A(x), B(x)$ cũng là các đa thức.

Giải. Do $P(x) \geqslant 0$ với mọi $x \in \mathbb{R}$ nên đa thức $P(x)$ có bậc bằng $2n$ và có thể phân tích được dưới dạng tích của các nhân tử bậc hai không âm, nghĩa là

$$P(x) = \prod_{j=1}^{n} [(a_j x + x_j)^2 + y_j^2],$$

trong đó $a_j, x_j, y_j \in \mathbb{R}$, $j = 1, 2, \ldots, n$.

Từ hằng đẳng thức

$$(p_1^2 + q_1^2)(p_2^2 + q_2^2) = (p_1 p_2 + q_1 q_2)^2 + (p_1 q_2 - p_2 q_1)^2,$$

ta có kết luận:

Tích của hai biểu thức dạng $[u(x)]^2 + [v(x)]^2$ cũng là một biểu thức có dạng đó.

Sau hữu hạn bước thực hiện quy trình đó ta thu được biểu thức dạng

$$P(x) = [A(x)]^2 + [B(x)]^2.$$

Bài toán 2. Cho $f(x) = ax^2 + bx + c \in \mathbb{R}[x]$ thỏa mãn điều kiện $f(x) \geqslant 0$ với mọi $x \geqslant 0$. Chứng minh rằng tồn tại đa thức $P(x)$ sao cho đa thức $Q(x) = f(x)P(x)$ có tất các hệ số đều không âm.

Giải.

Do $f(x) \geqslant 0$ với mọi $x \geqslant 0$ nên $a > 0$ và $c = f(0) \geqslant 0$.

Nếu $b \geqslant 0$ thì ta chọn $P(x) = 1$ và ta nhận được ngay điều phải chứng minh.

Nếu $b < 0$ thì $a > 0$. Ta tìm $P(x)$ dưới dạng $P(x) = (x+1)^n$ với $n \geqslant 2$.

Ta có

$$P(x) = (x+1)^n = \sum_{k=0}^{n} C_n^k x^k$$

nên

$$f(x)P(x) = (ax^2 + bx + c)(x+1)^n =$$

$$= ax^{n+2} + (b + na)x^{n+1} + \cdots + \sum_{k=0}^{n} (aC_n^{k-2} + bC_n^{k-1} + cC_n^k)x^k$$

$$+ \cdots + (b + nc)x + c.$$

Ta chọn n sao cho

$$\begin{cases} b + na \geqslant 0 & (1) \\ b + nc \geqslant 0 & (2) \\ aC_n^{k-2} + bC_n^{k-1} + cC_n^k \geqslant 0 \ \forall k \geqslant 2. & (3) \end{cases}$$

Nhận thấy ngay rằng với $n > \max\{-b/a, -b/c\}$ thì các điều kiện (1) và (2 thoả mãn (do $a > 0$).

Ta biến đổi vế trái của (3):

$$h(k) = (a - b + c)k^2 - [a - (n+2)b + (2n+3)c]k + c(n+1)(n+2) \geqslant$$

Do $b < 0$, $a \geqslant 0$, $c \geqslant 0$ nên $a - b + c > 0$.

Để (3) đúng với mọi k ta chọn n sao cho biệt thức của tam thức bậc h không dương ($\Delta_h \leqslant 0$). Biểu thức của Δ_h cũng là một tam thức bậc hai theo số của n^2 là

$$(b - 2c)^2 - 4c(a - b + c) = b^2 - 4ac \leqslant 0$$

(do $f(x) \geqslant 0 \ \forall x \geqslant 0$;$> 0, a > 0$.

Do vậy, ta có

$$\lim_{n\to\infty} \Delta_h = -\infty.$$

Do đó với n đủ lớn thì $\Delta_h \leqslant 0$.

Từ đó suy ra tồn tại n thỏa mãn đồng thời (1), (2) và (3).

Bài toán 3. Cho đa thức

$$g(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \ \ (n \geqslant 3)$$

thỏa mãn điều kiện $g(x) > 0$ với mọi $x > 0$. Chứng minh rằng khi đó tồn tại để đa thức $Q(x)$ dạng $Q(x) = g(x)(x+1)^s$ có các hệ số đều không âm.

Giải. Ta xét hai trường hợp $\deg g(x) = 2m$ và $\deg g(x) = 2m + 1$ với $m \in \mathbb{N}$

Khi $n = 2m$ thì ta có thể phân tích

$$g(x) = \prod_{k=1}^{m} (a_k x^2 + b_k x + c_k),$$

trong đó

$$a_k x^2 + b_k x + c_k > 0 \ \ \forall x > 0.$$

Theo Bài toán 2 với mỗi đa thức $a_k x^2 + b_k x + c_k$ đều tồn tại số tự nhiên m_k s đa thức

$$Q_k(x) = (a_k x^2 + b_k x + c_k)(x+1)^{m_k}$$

có các hệ số đều không âm.

Từ đó

$$\prod_{k=1}^{m} Q_k(x) = \prod_{k=1}^{m} g(x)(x+1)^{m_k} = g(x)(x+1)^{m_1 + \cdots + m_m}$$

là một đa thức cũng có các hệ số đều không âm.

Khi deg $g(x) = 2m+1$ thì $g(x)$ có ít nhất một nghiệm không dương là $-a$ ($a \geqslant 0$). Ta có

$$g(x) = (x+a)h(x) \quad \text{với } h(x) > 0 \text{ với mọi } x > 0 \text{ và deg } h(x) = 2m.$$

Do deg $h(x) = 2m$ nên theo trường hợp 1 tồn tại số nguyên dương s sao cho $h(x)(x+1)^s$ có các hệ số đều không âm và vì vậy đa thức $g(x)(x+1)^s$ cũng có các hệ số đều không âm.

Bài toán 4. Hỏi có tồn tại hay không tồn tại các đa thức $P(x), Q(x), T(x)$ với các hệ số nguyên dương và thoả mãn hệ thức

$$T(x) = (x^2 - 3x + 3)P(x), \;\; P(x) = \Big(\frac{x^2}{20} - \frac{x}{15} + \frac{1}{12}\Big)Q(x).$$

Giải. Viết lại các đẳng thức của đề bài dưới dạng

$$60T(x) = 60(x^2 - 3x + 3)P(x) = (3x^2 - 4x + 5)Q(x). \tag{4}$$

Các đa thức $(x^2 - 3x + 3)$ và $(3x^2 - 4x + 5)$ vô nghiệm và nguyên tố cùng nhau. Vì vậy từ (4) suy ra tồn tại các đa thức $P(x), Q(x), T(x)$ thoả mãn điều kiện đề bài khi và chỉ khi tồn tại đa thức $S(x)$ sao cho các đa thức

$$(3x^2 - 4x + 5)S(x), \;\; 60(x^2 - 3x + 3)S(x)$$

và

$$(3x^2 - 4x + 5)(x^2 - 3x + 3)S(x)$$

đều là những đa thức với hệ số nguyên dương.

Theo kết quả của Bài toán 3 thì tồn tại số nguyên dương k_1 đủ lớn sao cho

$$(3x^2 - 4x + 5)(x+1)^{k_1}$$

là một đa thức có các hệ số nguyên không âm và từ đó dễ dàng suy ra rằng không có hệ số nào của đa thức bằng 0 và tồn tại số nguyên dương k_2 đủ lớn để

$$(x^2 - 3x + 3)(x+1)^{k_2}$$

là đa thức có các hệ số đều nguyên dương. Từ đó suy ra

$$(3x^2 - 4x + 5)(x^2 - 3x + 3)(x+1)^{k_1+k_2}$$

cũng là một đa thức với hệ số nguyên dương. Như vậy câu trả lời của bài toán là khẳng định. Chẳng hạn ta có thể chọn

$$P(x) = (3x^2 - 4x + 5)(x+1)^{k_1+k_2},$$

$$Q(x) = 60(x^2 - 3x + 3)(x+1)^{k_1+k_2},$$

$$T(x) = (3x^2 - 4x + 5)(x^2 - 3x + 3)(x+1)^{k_1+k_2}.$$

(Bằng cách thử trực tiếp có thể thấy rằng $k_1 \geqslant 3$, $k_2 \geqslant 15$).

Bài toán 5. Chứng minh rằng nếu đa thức $P(x) \geqslant 0$ với mọi $x \geqslant 0$ thì tồi đa thức $A(x), B(x), C(x), D(x)$ để $P(x)$ biểu diễn được dưới dạng

$$P(x) = [A(x)]^2 + [B(x)]^2 + x\{[C(x)]^2 + [D(x)]^2\},$$

Giải.

1. Trường hợp deg $P(x) = 2m$.

Nếu $m = 0$ thì ta dễ dàng viết được biểu diễn (5).

Với $m \geqslant 1$, ta có thể phân tích đa thức $P(x)$ dưới dạng

$$P(x) = \prod_{k=1}^{m}(a_k x^2 + b_k x + c_k),$$

trong đó $a_k > 0$, $a_k x^2 + b_k x + c_k \geqslant 0\ \forall x \geqslant 0$.

Nhận xét rằng với mỗi đa thức

$$a_k x^2 + b_k x + c_k \geqslant 0\ \ \forall x \geqslant 0$$

ta đều có thể viết được

$$ax^2 + bx + c = (\alpha_k x^2 + \beta_k)^2 + x(\gamma_k^2 + \delta_k^2),$$

nên

$$P(x) = \prod_{k=1}^{m}\left[(\alpha_k x^2 + \beta_k)^2 + x(\gamma_k^2 + \delta_k^2)\right].$$

Mặt khác, ta cũng có tích của hai đa thức dạng $(p^2 + q^2) + x(r^2 + s^2)$ cũng là thức có dạng đó. Thật vậy, ta có

$$[(p_1^2 + q_1^2) + x(r_1^2 + s_1^2)][(p_2^2 + q_2^2) + x(r_2^2 + s_2^2)]$$

$$= [(p_1^2+q_1^2)(p_2^2+q_2^2)+x^2(r_1^2+s_1^2)(r_2^2+s_2^2)]+x[(p_1^2+q_1^2)(r_2^2+s_2^2)+(r_1^2+s_1^2)(p_2^2$$

Theo Bài toán 1 thì ta có biểu diễn

$$(p_1^2 + q_1^2)(p_2^2 + q_2^2) + x^2(r_1^2 + s_1^2)(r_2^2 + s_2^2) = [A(x)]^2 + [B(x)]^2,$$

$$(p_1^2 + q_1^2)(r_2^2 + s_2^2) + (r_1^2 + s_1^2)(p_2^2 + q_2^2) = [C(x)]^2 + [D(x)]^2.$$

Vậy nên

$$P(x) = [A(x)]^2 + [B(x)]^2 + x\{[C(x)]^2 + [D(x)]^2\}.$$

Trường hợp deg $P(x) = 2m + 1$.

Lập luận tương tự như đối với Bài toán 3 ta thu được

$$P(x) = \sum_{k=1}^{n}(x + d)(a_k x^2 + b_k x + c_k)$$

$$= [A(x)]^2 + [B(x)]^2 + x\{[B(x)]^2 + [C(x)]^2\} = [B(x)]^2 + [C(x)]^2.$$

(Do các biểu thức trong ngoặc nhọn là không âm với mọi x nên áp dụng được kết quả biểu diễn của Bài toán 1).

Bài toán 6. Cho đa thức $f(x) \in \mathbb{R}[x]$ thỏa mãn điều kiện

$$f(x) > 0 \ \forall x \in (-1;1).$$

Chứng minh rằng đa thức $f(x)$ có thể biểu diễn được dưới dạng

$$f(x) = \sum_{j=0}^{k} a_j (1+x)^{\alpha_j} (1-x)^{\beta_j}$$

với $a_j \geqslant 0, \ \alpha_j, \ \beta_j \in \mathbb{N}$.

Giải. Giả sử $\deg f(x) = m$. Đặt

$$\frac{1+x}{1-x} = t \ \Rightarrow \ x = \frac{t-1}{t+1}.$$

Do $x \in (-1;1)$ nên $t > 0$.

Vậy $f(x) = f\Big(\dfrac{t-1}{t+1}\Big) > 0 \ \forall t > 0$. Do đó đa thức $Q(t)$ với

$$Q(t) = (t+1)^m f\Big(\frac{t-1}{t+1}\Big)$$

là một đa thức thỏa mãn điều kiện $Q(t) > 0 \ \forall t > 0$.

Theo Bài toán 3 thì tồn tại $n \in \mathbb{N}$ sao cho

$$(t+1)^{m+n} Q(t) = (t+1)^{m+n} f(\frac{t-1}{t+1})$$

là một đa thức có các hệ số đều không âm. Suy ra

$$(t+1)^{m+n} f\Big(\frac{t-1}{t+1}\Big) = \sum_{j=0}^{k} b t^j,$$

với $b_j > 0, \ k \leqslant m+n$.

Mà

$$t+1 = \frac{1+x}{1-x} + 1 = \frac{2}{1-x}$$

nên ta thu được

$$\Big(\frac{2}{1-x}\Big)^{m+n} f(x) = \sum_{j=0}^{k} b_j \Big(\frac{1+x}{1-x}\Big)^j.$$

Suy ra

$$f(x) = \sum_{j=0}^{k} \frac{b_j}{2^{m+n}} (1+x)^j (1-x)^{m+n-j}$$

hay

$$f(x) = \sum_{j=0}^{k} a_j (1+x)^j (1-x)^{m+n-j},$$

với $a_j = \dfrac{b_j}{2^{m+n}} \geqslant 0$. Từ đó ta có điều phải chứng minh.

Bài toán 7. Chứng minh rằng tồn tại đa thức $P(x)$ bậc n và nhận giá trị trong khoảng $(-1;1)$ và nó không thể biểu diễn được dưới dạng

$$P(x) = \sum A_{\alpha\beta}(1-x)^{\alpha}(1+x)^{\beta},$$

trong đó $A_{\alpha\beta} \geqslant 0$, $\alpha + \beta \leqslant n$; α, β là các số nguyên không âm.

Giải. Xét đa thức $P(x) = x^2 + \varepsilon$, trong đó $\varepsilon > 0$. Giả sử có thể viết $P(x)$ dưới dạng

$$P(x) = x^2 + \varepsilon = \sum_{\alpha+\beta\leq 2} A_{\alpha\beta}(\varepsilon)(1-x)^{\alpha}(1+x)^{\beta},$$

trong đó $\varepsilon > 0$, $A(\varepsilon) \geqslant 0$, α và β chạy trên tất cả các số nguyên không $\alpha + \beta \leqslant 2$. Như vậy, với ε bất kỳ trong tổng này sẽ chứa vừa đúng sáu số hạng cách thế $x = 0$ vào (6) ta nhận được $A_{\alpha\beta}(\varepsilon)$ bị chặn với $0 < \varepsilon \leqslant 1$. Cho ε dần sao cho tồn tại $\lim\limits_{\varepsilon\to 0} A(\varepsilon) = A$ trong tất cả sáu số hạng, khi đó chuyển qua giới nhận được

$$x^2 = \sum_{\alpha+\beta\leqslant 2} A_{\alpha\beta}(1-x)^{\alpha}(1+x)^{\beta}.$$

Nhưng với $x = 0$ thì đồng nhất thức này không thoả mãn.

Vậy không phải đối với mọi đa thức $P(x)$ bậc n nhận giá trị dương trong $(-1;1)$ đều có thể biểu diễn được dưới dạng

$$P(x) = \sum_{\alpha+\beta\leqslant n} A_{\alpha\beta}(1-x)^{\alpha}(1+x)^{\beta}, \quad A_{\alpha\beta} \geqslant 0.$$

Bài tập

Bài 1. Xác định hàm số $f(x)$ đồng biến trong $[0, 2\pi]$ và thoả mãn điều kiện

$$f(x) \leqslant \sin x, \quad \forall x \in [0, 2\pi].$$

Bài 2. Xác định hàm số $f(x)$ đồng biến trong $[0, 2\pi]$ và thoả mãn điều kiện

$$f(x) \leqslant \cos x, \quad \forall x \in [0, 2\pi].$$

Bài 3. Xác định hàm số $f(x)$ đồng biến trong $[0, 4]$ và thoả mãn điều kiện

$$f(x) \leqslant x^3 - 3x, \quad \forall x \in [0, 4].$$

Bài 4. Xác định hàm số $f(x)$ nghịch biến trong $[0, 2\pi]$ và thoả mãn điều kiện

$$f(x) \geqslant \sin x, \ \ \forall x \in [0, 2\pi].$$

Bài 5. Xác định hàm số $f(x)$ nghịch biến trong $[0, 2\pi]$ và thoả mãn điều kiện

$$f(x) \geqslant \sin x, \ \ \forall x \in [0, 2\pi].$$

Bài 6. Xác định hàm số $f(x)$ nghịch biến trong $[0, 4]$ và thoả mãn điều kiện

$$f(x) \geqslant 4x^3 - 3x - 1, \ \ \forall x \in [0, 4].$$

PHƯƠNG TRÌNH HÀM LIÊN QUAN ĐẾN TAM GI

Nguyễn Văn Mậu

3.1. Hàm số chuyển đổi các tam giác

Ta nhắc lại (không chứng minh) một số hệ thức đặc trưng cho tam giác học sinh bậc THPT đều quen biết. Đây là những hệ thức đơn giản mô tả sự rà tự nhiên của các yếu tố cạnh và góc trong một tam giác.

Bài toán I. Điều kiện cần và đủ để 3 số dương A, B, C là độ đo các góc c tam giác ΔABC là

$$A + B + C = \pi.$$

Bài toán II. Điều kiện cần và đủ để 3 số dương a, b, c khi gắn với cùng một đo lường lập thành độ dài các cạnh của một tam giác ΔABC là

$$\begin{cases} a + b > c \\ b + c > a \\ c + a > b \end{cases}$$

Nói cách khác, ta có thể phát biểu ngắn gọn như sau.

Bài toán II'. Điều kiện cần và đủ để 3 số dương a, b, c là độ dài các cạnh c tam giác ΔABC là

$$|b - c| < a < b + c.$$

Trong phần này sẽ khảo sát các đặc trưng hàm cơ bản của một số hàm s bởi các phép biến hình sơ cấp dạng tịnh tiến, đồng dạng, phản xạ và nghịch đ đường thẳng thực.

Bài toán 1. Xác định α để hàm số $f(x) = x + \alpha$ có tính chất $f(a), f(b),$ độ dài các cạnh của một tam giác ứng với mọi ΔABC.

Bài giải

Để $f(a), f(b), f(c)$ là độ dài các cạnh của một tam giác, trước hết phải có

$$f(a) > 0,\ \ f(b) > 0,\ \ f(c) > 0.$$

Suy ra

$$a + \alpha > 0,\ \ b + \alpha > 0,\ \ c + \alpha > 0,\ \ \forall \Delta ABC$$

hay

$$\alpha > -a,\ \ \alpha > -b,\ \ \alpha > -c,\ \ \forall \Delta ABC.$$

Điều này tương đương với

$$\alpha > \max\{-a, -b, -c\},\ \ \forall \Delta ABC$$

hay $\alpha \geqslant 0$.

Ngược lại, với $\alpha \geqslant 0$ thì $f(a), f(b), f(c)$ là độ dài các cạnh của một tam giác do a, b, c là độ dài các cạnh của một tam giác. Vậy nên với $\alpha \geqslant 0$ thì hàm số $f(x) = x + \alpha$ có tính chất $f(a), f(b), f(c)$ là độ dài các cạnh của một tam giác ứng với mọi ΔABC.

Bài toán 2. Xác định α để hàm số $f(x) = \alpha x$ có tính chất $f(a), f(b), f(c)$ là độ dài các cạnh của một tam giác ứng với mọi ΔABC.

Bài giải

Để $f(a), f(b), f(c)$ là độ dài các cạnh của một tam giác, trước hết phải có

$$f(a) > 0,\ \ f(b) > 0,\ \ f(c) > 0,\ \ \forall \Delta ABC.$$

Suy ra

$$\alpha a > 0,\ \ \alpha b > 0,\ \ \alpha c > 0,\ \ \forall \Delta ABC. \tag{1}$$

Từ (1) ta thu được $\alpha > 0$. Thật vậy, nếu $\alpha \leqslant 0$ thì $f(a) \leqslant 0$.

Vậy với $\alpha > 0$ thì hàm số $f(x) = \alpha x$ có tính chất $f(a), f(b), f(c)$ là độ dài các cạnh của một tam giác ứng với mọi ΔABC.

Bài toán 3. Xác định α, β để hàm số $f(x) = \alpha x + \beta$ có tính chất $f(a), f(b), f(c)$ là độ dài các cạnh của một tam giác ứng với mọi ΔABC.

Bài giải

Để $f(a), f(b), f(c)$ là độ dài các cạnh của một tam giác, trước hết phải có

$$f(a) > 0,\ \ f(b) > 0,\ \ f(c) > 0,\ \ \forall \Delta ABC.$$

Suy ra

$$\alpha a + \beta > 0,\ \ \alpha b + \beta > 0,\ \ \alpha c + \beta > 0,\ \ \forall \Delta ABC. \tag{1}$$

Từ (1) ta thu được $\alpha \geqslant 0$. Thật vậy, nếu $\alpha < 0$, β tuỳ ý cho trước thì ta chọn ΔABC có a đủ lớn thì theo tính chất của nhị thức bậc nhất sẽ nhận được $\alpha a + \beta < 0$.

Tương tự, cũng từ (1) ta suy ra $\beta \geqslant 0$. Thật vậy, nếu $\beta < 0$, ta chọn ΔABC có a đủ nhỏ thì theo tính chất của nhị thức bậc nhất sẽ nhận được $\alpha a + \beta < 0$.

Trường hợp khi đồng thời xảy ra $\alpha = 0, \beta = 0$ thì $f(x) \equiv 0$ không thoả mãn bài toán.

Với $\alpha \geqslant 0,\ \beta \geqslant 0$ và $\alpha + \beta > 0$ thì ta thấy $f(a), f(b), f(c)$ là độ dài c
của một tam giác do a, b, c là độ dài các cạnh của một tam giác. Vậy nên:

Với $\alpha \geqslant 0,\ \beta \geqslant 0$ và $\alpha + \beta > 0$ thì hàm số $f(x) = \alpha x + \beta$ có t
$f(a), f(b), f(c)$ là độ dài các cạnh của một tam giác ứng với mọi ΔABC.

Bài toán 4. Xác định α, β để hàm số $f(x) = \dfrac{1}{\alpha x + \beta}$ có tính chất $f(a), f$
là độ dài các cạnh của một tam giác ứng với mọi ΔABC.

Bài giải Không mất tính tổng quát, ta luôn luôn giả thiết $a \geqslant b \geqslant c$.

Nhận xét rằng, phép nghịch đảo $g(x) = \dfrac{1}{x}$ không có tính chất: $g(a), g(b)$
độ dài các cạnh của một tam giác ứng với mọi ΔABC. Thật vậy, xét tam
với $a = b = 2, c = 1$ thì ta có

$$\frac{1}{a} + \frac{1}{b} = \frac{1}{c}.$$

Để $f(a), f(b), f(c)$ là độ dài các cạnh của một tam giác, trước hết phải c

$$f(a) > 0,\ \ f(b) > 0,\ \ f(c) > 0,\ \ \forall \Delta ABC.$$

Suy ra

$$\alpha a + \beta > 0,\ \ \alpha b + \beta > 0,\ \ \alpha c + \beta > 0,\ \ \forall \Delta ABC.$$

Từ (1) ta thu được $\alpha \geqslant 0$. Thật vậy, nếu $\alpha < 0$, β tuỳ ý cho trước thì ta chọn
có a đủ lớn thì theo tính chất của nhị thức bậc nhất sẽ nhận được $\alpha a + \beta <$

Tương tự, cũng từ (1) ta suy ra $\beta \geqslant 0$. Thật vậy, nếu $\beta < 0$, ta chọn ΔA
đủ nhỏ thì theo tính chất của nhị thức bậc nhất sẽ nhận được $\alpha a + \beta < 0$.

Trường hợp khi đồng thời xảy ra $\beta = 0$ thì $f(x) \equiv 0$ không thoả mãn
(theo nhận xét ở trên).

Với $\alpha = 0, \beta > 0$, ta thu được hàm hằng dương nên $f(a) = f(b) = f(c)$
$f(a), f(b), f(c)$ là độ dài các cạnh của một tam giác đều.

Xét trường hợp $\alpha > 0, \beta > 0$. Khi đó

$$f(a) \geqslant f(b) \geqslant f(c).$$

Vậy ta cần xác định các số dương α, β sao cho luôn có

$$f(a) + f(b) > f(c),\ \ \forall \Delta ABC,\ \ a \geqslant b \geqslant c$$

hay

$$\frac{1}{\alpha a + \beta} + \frac{1}{\alpha b + \beta} > \frac{1}{\alpha c + \beta},\ \ \forall \Delta ABC,\ \ a \geqslant b \geqslant c.$$

Xét các tam giác ABC cân đồng dạng với tam giác cạnh $3, 3, 1$, tức $a =$
$c = d$ với $d > 0$ tuỳ ý. Khi đó, (1) có dạng

$$\frac{1}{3d\alpha + \beta} + \frac{1}{3d\alpha + \beta} > \frac{1}{d\alpha + \beta},\ \ \forall d > 0$$

hay

$$\frac{2}{3d\alpha + \beta} > \frac{1}{d\alpha + \beta},\ \ \forall d > 0$$

$$\Leftrightarrow \frac{3d\alpha+\beta}{2} > \frac{d\alpha+\beta}{,} \quad \forall d>0$$

hay

$$\beta > 2d\alpha, \quad \forall d > 0.$$

Điều này không xảy ra khi d đủ lớn.

Vậy với $\alpha = 0, \ \beta > 0$ thì hàm số $f(x) = \dfrac{1}{\alpha x+\beta}$ có tính chất $f(a), f(b), f(c)$ là độ dài các cạnh của một tam giác ứng với mọi ΔABC.

Bài toán 5. Xác định các hàm số $f(x)$ liên tục trong $[0,\pi]$, $f(0) = 0$ và có đạo hàm trong $(0,\pi)$ sao cho $f(A), f(B), f(C)$ tạo thành độ đo các góc của một tam giác ứng với mọi ΔABC cho trước.

Bài giải

Ta cần xác định hàm khả vi $f(x)$ sao cho

$$\begin{cases} f(x) > 0, \ \forall x \in (0,\pi) \\ f(0) = 0 \\ f(A) + f(B) + f(C) = \pi. \end{cases}$$

Theo giả thiết thì $f(0) = 0$ nên $f(\pi) = \pi$ và $C = \pi - (A+B)$.

Suy ra

$$f(A) + f(B) + f(\pi - A - B) = \pi, \ \forall A, B, A+B \in [0,\pi]$$

hay

$$f(x) + f(y) + f(\pi - x - y) = \pi, \ \forall x, y, x+y \in [0,\pi]. \tag{1}$$

Lấy đạo hàm trong $(0,\pi)$ theo biến x, ta thu được

$$f'(x) - f'(\pi - x - y) = 0, \ \forall x, y, x+y \in [0,\pi]. \tag{2}$$

Từ (2) suy ra $f'(x)$ là hàm hằng trong $(0,\pi)$ và vì vậy $f(x) = px + q$. Do $f(0) = 0$ nên $q = 0$ và vì vậy $f(x) = px$. Do $f(\pi) = \pi$ nên $p = 1$ và ta thu được $f(x) = x$.

Vậy hàm số $f(x) = x$ là liên tục trong $[0,\pi]$, $f(0) = 0$ và có đạo hàm trong $(0,\pi)$ để $f(A), f(B), f(C)$ tạo thành độ đo các góc của một tam giác ứng với mọi ΔABC cho trước.

Bài toán 6. Xác định các hàm số $f(x)$ liên tục trong $[0,\pi]$ và

$$f(0) = 0, \ \ f(x) > 0 \ \ \forall x \in (0,\pi)$$

và $f(A), f(B), f(C)$ tạo thành độ đo các góc của một tam giác ứng với mọi ΔABC cho trước.

Bài giải

Ta phát biểu bài toán đã cho dưới dạng:

Xác định các hàm số $f(x)$ liên tục trong $[0,\pi]$ và

$$f(0)=0,\ \ f(x)>0,\ \ f(x)+f(y)+f(\pi-x-y)=\pi,\ \ \forall x,y\in(0,\pi), x+y<$$

Do $f(0)=0$ nên với $y=0$, ta thu được

$$f(x)+f(0)+f(\pi-x)=\pi,\ \ \forall x\in[0,\pi].$$

Đặt $f(x)=x+g(x)$ thì $g(0)=0$ và $g(x)$ là hàm liên tục trong $[0,\pi]$. Ta có

$$(1)\Leftrightarrow x+g(x)+(\pi-x)+g(\pi-x)=\pi$$

$$\Leftrightarrow g(x)+g(\pi-x)=0,\ \ \forall x\in[0,\pi]$$

hay

$$g(\pi-x)=-g(x),\ \ \forall x\in[0,\pi].$$

Thế $f(x)=x+g(x)$ vào (1) và sử dụng (2), ta thu được

$$x+g(x)+y+g(y)+\pi-(x+y)+g(\pi-(x+y))=\pi,\ \ \forall x,y\in[0,\pi], x+$$

hay

$$g(x)+g(y)-g(x+y)=0,\ \ \forall x,y\in[0,\pi], x+y\leqslant\pi$$

hay

$$g(x+y)=g(x)+g(y),\ \ \forall x,y\in[0,\pi], x+y\leqslant\pi.$$

Do $f(x)$ liên tục trong $[0,\pi]$ nên (3) là phương trình hàm Cauchy và $g(x)=$ $f(x)=(1+\alpha)x$. Để $f(x)>0$ với mọi $x\in(0,\pi)$, ta cần có $1+\alpha>0$ và để

$$f(A)+f(B)+f(C)=\pi$$

ta cần có $1+\alpha=1$. Suy ra $\alpha=0$ và $f(x)\equiv x$.

Bài toán 7. Xác định các hàm số $f(x)$ liên tục trong $[0,\pi]$ sao cho $f(A), f(B)$ tạo thành độ đo các góc của một tam giác ứng với mọi ΔABC cho trước.

Bài giải

Ta thấy có hai hàm số hiển nhiên thoả mãn bài toán, đó là $f(x)=x$ và $f(x)$

Ta phát biểu bài toán đã cho dưới dạng:

Xác định các hàm số $f(x)$ liên tục trong $[0,\pi]$ và

$$f(x)>0,\ \ f(x)+f(y)+f(\pi-x-y)=\pi,\ \ \forall x,y\in(0,\pi), x+y<\pi.$$

Cho $y\to 0$, ta thu được

$$f(x)+f(0)+f(\pi-x)=\pi,\ \ \forall x\in(0,\pi)$$

hay

$$f(\pi-x)=\pi-f(0)-f(x),\ \ \forall x\in[0,\pi].$$

Thế vào (1), ta thu được

$$x+g(x)+y+g(y)+\pi-(x+y)+g(\pi-(x+y))=\pi,\ \ \forall x,y\in[0,\pi], x+$$

hay

$$f(x)+f(y)+[\pi-f(0)-f(x+y)]=\pi,\ \ \forall x,y\in[0,\pi], x+y\leqslant\pi$$

hay

$$f(x+y)+f(0)=f(x)+f(y),\ \ \forall x,y\in[0,\pi], x+y\leqslant\pi. \tag{2}$$

Đặt $f(x)=f(0)+g(x)$. Khi đó $g(x)$ liên tục trong $[0,\pi]$ và (2) có dạng

$$g(x+y)=g(x)+g(y),\ \ \forall x,y\in[0,\pi], x+y\leqslant\pi. \tag{3}$$

Do $g(x)$ liên tục trong $[0,\pi]$ nên (3) là phương trình hàm Cauchy và $g(x)=\alpha x$ và $f(x)=\alpha x+\beta$. Ta cần xác định α,β để $f(x)>0$ với mọi $x\in(0,\pi)$ và để

$$f(A)+f(B)+f(C)=\pi$$

hay

$$\begin{cases}\alpha x+\beta & >0,\ \ \forall x\in(0,\pi)\\ \alpha(A+B+C)+3\beta=\pi.\end{cases}$$

hay

$$\begin{cases}\alpha x+\beta & >0,\ \ \forall x\in(0,\pi)\\ \alpha\pi+3\beta=\pi.\end{cases}$$

hay

$$f(x)=\alpha x+\frac{(1-\alpha)\pi}{3}>0,\ \ \forall x\in(0,\pi). \tag{4}$$

Cho $x\to 0$ và $x\to\pi$, từ (4) ta thu được

$$-\frac{1}{2}\leqslant\alpha\leqslant 1.$$

Với $-\frac{1}{2}<\alpha<1$ thì hiển nhiên (4) thoả mãn.

Xét $\alpha=-\frac{1}{2}$ thì $f(x)=-\frac{1}{2}x+\frac{\pi}{2}$ thoả mãn điều kiện bài ra.

Thậy vậy, với $0<x<\pi$ thì $f(x)>f(\pi)=0$.

Xét $\alpha==1$ thì $f(x)=x$ hiển nhiên thoả mãn điều kiện bài ra.

Vậy, các hàm cần tìm đều có dạng

$$f(x)=\alpha x+\frac{(1-\alpha)\pi}{3},\ \ -\frac{1}{2}\leqslant\alpha\leqslant 1.$$

Bài toán 8. Xác định các hàm số $f(x)$ liên tục trong $[0,1]$ sao cho $f(a),f(b),f(c)$ tạo thành độ đo các cạnh của một tam giác nội tiếp trong đường tròn đường kính 1 ứng với mọi ΔABC nội tiếp trong đường tròn đường kính 1 cho trước.

Bài giải

Ta có nhận xét sau:

Xét đường tròn O đường kính bằng 1. Ký hiệu $M(\Delta)$ là tập hợp tất cả giác nội tiếp trong đường tròn O đó. Khi đó điều kiện cần và đủ để ba s α, β, γ là ba góc của một tam giác thuộc $M(\Delta)$ là $\sin\alpha, \sin\beta, \sin\gamma$ tạo thàn các cạnh của một tam giác thuộc $M(\Delta)$.

Thật vậy, khi α, β, γ là ba góc của một tam giác thì $2R\sin\alpha, 2R\sin\beta,$ hay $\sin\alpha, \sin\beta, \sin\gamma$ là độ dài các cạnh tương ứng của tam giác nội tiếp đư đường tròn O đường kính bằng 1.

Ngược lại, khi $\sin\alpha, \sin\beta, \sin\gamma$ là độ dài các cạnh tương ứng của tam tiếp được trong đường tròn O đường kính bằng 1 thì do các góc α, β, γ đư α, β, γ là ba góc của một tam giác.

Vậy, theo kết quả bài toán 7 thì các hàm cần tìm có dạng

$$f(x) = \sin\left(\alpha x + \frac{(1-\alpha)\pi}{3}\right), \quad -\frac{1}{2} \leqslant \alpha \leqslant 1.$$

3.2. Phương trình hàm liên quan đến tam giác

Trong mục này, ta quan tâm đến bộ các hàm số (phương trình hàm đa ẩ lập nên một dãy các tam giác ứng với các giá trị tương ứng của đối số.

Trước hết, ta nhận xét rằng nghiệm của phương trình vô định $x^2 + y^2 = z$ tập các số thực dương có thể mô tả dưới dạng tham số

$$\begin{cases} x &= u\cos v, \\ y &= u\sin v, \\ z = & u, \ u \in \mathbb{R}^+, v \in \left(0, \frac{\pi}{2}\right) \end{cases}$$

Vậy ta có kết luận sau:

Bài toán 1.

Chứng minh rằng với mọi (u, v) với $u \in \mathbb{R}^+$, $v \in \left(0, \frac{\pi}{2}\right)$ đều tồn tại một t mà số đo các cạnh là những số

$$P_1(u,v) = u\cos v, \ \ P_2(u,v) = u\sin v, \ \ P_3(u,v) = u$$

và các tam giác đó ứng với mọi (u, v) với $u \in \mathbb{R}^+$, $v \in \left(0, \frac{\pi}{2}\right)$ cho trước đều giác vuông.

Giải.

Thật vậy, dễ thấy $P_1(u,v) > 0$, $P_2(u,v) > 0$, $P_3(u,v) > 0$ ứng với mọi $(u$ $u \in \mathbb{R}^+$, $v \in \left(0, \frac{\pi}{2}\right)$ và đẳng thức sau luôn luôn đúng

$$[P_1(u,v)]^2 + [P_2(u,v)]^2 = [P_3(u,v)]^2.$$

Từ đó suy ra $P_1(u,v)$, $P_2(u,v)$, $P_3(u,v)$ là độ dài các cạnh của một tam giác cạnh huyền $P_3(u,v)$.

Tiếp theo, ta xét các bộ hàm số một biến trong lớp các đa thức tạo thành các cạnh của một tam giác ứng với mọi đối số trong một miền cho trước.

Bài toán 2.

Chứng minh rằng với mọi $x > 1$ đều tồn tại một tam giác mà số đo các cạnh là những số

$$P_1(x) = x^4 + x^3 + 2x^2 + x + 1,$$
$$P_2(x) = 2x^3 + x^2 + 2x + 1,$$
$$P_3(x) = x^4 - 1$$

và các tam giác đó ứng với mọi $x > 1$ cho trước đều có góc lớn nhất như nhau.

Giải.

Đặt $x^2 + x + 1 = a > 0$, $2x + 1 = b > 0$ và $x^2 - 1 = c > 0$ thì

$$|b - c| = |x^2 - 2x| < a = x^2 + x + 1 < |b + c| = x^2 + 2x.$$

Vậy a, b, c là độ dài các cạnh của một tam giác. Do vậy

$$P_1(x) = a(x^2 + 1), \quad P_2(x) = b(x^2 + 1), \quad P_3(x) = c(x^2 + 1)$$

cũng là độ dài các cạnh của một tam giác. Cạnh có độ dài lớn nhất của tam giác ứng với $P_1(x)$ hay a. Gọi α là góc lớn nhất của tam giác. Khi đó thì

$$a^2 = b^2 + c^2 - 2bc\cos\alpha$$

hay

$$\cos\alpha = -\frac{1}{2}$$

hay

$$\alpha = \frac{2\pi}{3}.$$

Bài tập

Bài 1. Xác định các đa thức bậc nhất $T(x), U(x), V(x)$ sao cho $T(x)$, $U(x)$, $V(x)$ luôn luôn lập thành độ dài các cạnh của một tam giác thường ứng với mọi $x \geqslant 0$.

Bài 2. Xác định các đa thức $T(x), U(x), V(x)$ bậc không quá 2, sao cho $T(x)$, $U(x)$, $V(x)$ luôn luôn lập thành độ dài các cạnh của một tam giác thường ứng với mọi $x \geqslant 0$.

BẤT PHƯƠNG TRÌNH HÀM LIÊN QUAN ĐẾN TAM G

4.1. Bất phương trình hàm liên quan đến tam giác

4.2 Hàm số chuyển đổi thứ tự các yếu tố trong tam giác

4.1. Bất phương trình hàm liên quan đến tam giác

Trước hết, ta nhắc lại (không chứng minh) một số hệ thức đặc trưng cho t
mà mọi học sinh bậc THPT đều quen biết. Đây là những hệ thức đặc biệt qu
liên quan đến sự ràng buộc tự nhiên của các yếu tố cạnh và góc trong một ta

Bài toán I. Trong mọi ΔABC ta đều có: ứng với góc lớn hơn thì cạnh lớn

Nhận xét 1. Điều khẳng định trên cho ta một kết luận tương đương sau đâ

Trong ΔABC khi $A < B$ thì $\sin A < \sin B$.

Và như vậy, mặc dù hàm số $f(x) = \sin x$ không đồng biến trong $(0, \pi)$ t
hệ thức kiểu "đồng biến" cho cặp góc của một tam giác.

Bài toán II. Trong mọi ΔABC ta đều có:

$$\cos A + \cos B \leqslant 2 \cos \frac{A+B}{2}$$

Nhận xét 2. Như vậy, mặc dù hàm số $f(x) = \cos x$ không là hàm lõm (có
bậc hai luôn luôn âm) trong $(0, \pi)$ ta vẫn có hệ thức kiểu "hàm lõm" cho cặp
một tam giác.

Bài toán III. Trong mọi ΔABC ta đều có bất đẳng thức

$$\sin A + \sin B + \sin C \leqslant \frac{3\sqrt{3}}{2},$$

Bài toán IV. Trong mọi ΔABC ta đều có bất đẳng thức

$$\operatorname{tg} \frac{A}{2} + \operatorname{tg} \frac{B}{2} + \operatorname{tg} \frac{C}{2} \geqslant \sqrt{3},$$

Bài toán V. Trong mọi ΔABC ta đều có bất đẳng thức

$$\operatorname{cotg}\frac{A}{2}+\operatorname{cotg}\frac{B}{2}+\operatorname{cotg}\frac{C}{2}\geqslant 3\sqrt{3}.$$

Bài toán VI. Trong mọi ΔABC ta đều có bất đẳng thức

$$\cos A+\cos B+\cos C\leqslant\frac{3}{2},$$

Nhận xét 3. Điều khẳng định của các Bài toán III-V dễ dàng kiểm chứng được dựa trên bất đẳng thức Young W.H. quen biết đối với lớp hàm có đạo hàm không đổi dấu trong khoảng $(0,\pi)$.

Tuy nhiên, đối với khẳng định của Bài toán VI thì ta thấy ngay rằng tính chất của hàm lõm không còn được sử dụng như một công cụ cơ bản để kiểm chứng tính đúng đắn của bất đẳng thức. Vậy thì, một vấn đề xuất hiện tự nhiên là: Về tổng thể, ta có thể mô tả được hay không lớp các hàm tổng quát thoả mãn điều kiện

$$f(A)+f(B)+f(C)\leqslant 3f\Big(\frac{\pi}{3}\Big),$$

hoặc

$$f(A)+f(B)+f(C)\geqslant 3f\Big(\frac{\pi}{3}\Big).$$

với mọi ΔABC?

Sau đây ta xét một số minh hoạ thông qua cách xây dựng các phương trình hàm để mô tả những nhận xét đã nêu ở trên.

Bài toán 1. Cho hàm số $f(t)$ xác định trong khoảng $(0,\pi)$. Chứng minh rằng các điều kiện sau đây là tương đương:

$$f(x)+f(y)\leqslant 2f(\frac{x+y}{2})\ \ \forall x,y,x+y\in(0,\pi) \tag{1}$$

$$f(x)+f(y)+f(z)\leqslant 3f(\frac{x+y+z}{3})\ \ \forall x,y,z,x+y+z\in(0,\pi] \tag{2}$$

Giải. Thật vậy, từ (1) dễ dàng suy ra (2). Giả sử $x\geqslant y\geqslant z$ thì ta có

$$f(z)+f(\frac{x+y+z}{3})\leqslant 2f\Big(\frac{z+\frac{x+y+z}{3}}{2}\Big) \tag{3}$$

Từ (1) và (3) suy ra

$$f(x)+f(y)+f(z)+f(\frac{x+y+z}{3})\leqslant$$
$$2\Big[f(\frac{x+y}{2})+f\Big(\frac{z+\frac{x+y+z}{3}}{2}\Big)\Big]\leqslant 4f(\frac{x+y+z}{3})\ \ \forall x,y,z,x+y+z\in(0,\pi].$$

Ngược lại, từ (2) với giả thiết $x\leqslant z\leqslant y$, đặt $z=\frac{x+y}{2}$, ta thu được (1).

Bài toán 2. Xác định các hàm số $f(t)$ xác định trong khoảng $(0, \pi)$ và thỏ điều kiện:

Với mọi tam giác ABC thì $A < B$ khi và chỉ khi $f(A) < f(B)$.

Giải.

Trước hết, ta có nhận xét rằng điều kiện $A < B$ khi và chỉ khi $f(A) < f($ mọi cặp góc nhọn A, B tương đương với $f(t) = f_0(t)$ là một hàm đồng biến $(0, \frac{\pi}{2}]$.

Xét hàm số

$$g_0(t) = \begin{cases} f_0(t) & \text{khi} \quad 0 < t \leqslant \frac{\pi}{2} \\ f_0(\pi - t) & \text{khi} \quad \frac{\pi}{2} < t < \pi \end{cases}$$

Ta chứng minh rằng, khi đó $g_0(t)$ thỏa mãn điều kiện bài ra.

Thật vậy, ta có $g_0(A) < g_0(B)$ với mọi góc A, B nhọn và $A < B$. Xét trườ $0 < A < \frac{\pi}{2} < B < \pi$ với $A + B < \pi$.

Ta có $\pi - B > A$ và

$g_0(B) = f_0(\pi - B) > f_0(A) = g_0(A)$.

Tiếp theo, ta chứng minh rằng mọi hàm $f(t)$ thỏa mãn điều kiện bài toán dạng

$$f(t) = \begin{cases} g_0(t) & \text{khi} \quad 0 < t \leqslant \frac{\pi}{2} \\ \geqslant g_0(t) & \text{khi} \quad \frac{\pi}{2} < t < \pi \end{cases}$$

Thật vậy, với điều kiện $g_0(B) \leqslant f(B)$ với mọi góc B tù, ta có với $0 < A$ $B < \pi$ với $A + B < \pi$ thì $\pi - B > A$ và

$$f(B) \geqslant g_0(B) = f_0(\pi - B) > f_0(A) = g_0(A) = f(A).$$

Bài toán 3. Xét hàm số

$$f(t) = \begin{cases} \sin t & \text{khi} \quad 0 < t \leqslant \frac{\pi}{2} \\ 1 + \cos t & \text{khi} \quad \frac{\pi}{2} < t < \pi \end{cases}$$

Chứng minh rằng với mọi tam giác ABC ta đều có

$$f(A) + f(B) + f(C) \leqslant \frac{3\sqrt{3}}{2}.$$

Giải.

Khi ΔABC nhọn thì (4) có dạng quen biết

$$\sin A + \sin B + \sin C \leqslant \frac{3\sqrt{3}}{2}.$$

Xét trường hợp ΔABC tù với $C > \frac{\pi}{2}$ thì (4) có dạng

$$\sin A + \sin B + 1 + \cos C \leqslant \frac{3\sqrt{3}}{2}.$$

Để ý rằng với góc C tù thì

$$1 + \cos C \leqslant \sin C$$

nên ta có (5) là đúng.

4.2 Hàm số chuyển đổi thứ tự các yếu tố trong tam giác

Bài toán 1. Cho hàm số $f(x)$ xác định dương và hàm số $g(x) = xf(x)$ và đồng biến trong $(0, \infty)$. Chứng minh rằng hàm số $g(x)$ là hàm số bảo toàn hệ thức giữa r và R trong tam giác.

Nói cách khác, nếu r, R lần lượt là bán kính đường tròn nội tiếp và ngoại tiếp của tam giác ABC nào đó thì $g(r)$, $g(R)$ lần lượt sẽ là bán kính nội tiếp và ngoại tiếp của một tam giác nào đó.

Giải. Thật vậy, theo giả thiết thì $R \geqslant 2r$ (dấu đẳng thức xảy ra khi tam giác đều). Ta chứng minh $g(R) \geqslant 2g(r)$. Ta có $f(x) > 0$ và $f(2x) > f(x)$ với mọi $x > 0$ (do $f(x)$ đồng biến) suy ra $\dfrac{g(2x)}{2x} > \dfrac{g(x)}{x}$ hay $g(2x) > 2g(x)$. Từ đây suy ra $g(2r) > 2g(r)$. Mặt khác, $g(R) \geqslant g(2r)$ do $R \geqslant 2r$ và $g(x)$ đồng biến. Suy ra $g(R) \geqslant 2g(r)$.

Bài tập

Bài tập 1. Xét hàm số

$$f(t) = \begin{cases} \cos t & \text{khi} \quad 0 < t \leqslant \frac{\pi}{2} \\ g(t) & \text{khi} \quad \frac{\pi}{2} < t < \pi \end{cases}$$

Xác định các hàm số $g(t)$ xác định trong khoảng $(\frac{\pi}{2}, \pi)$ và thỏa mãn điều kiện:

Với mọi tam giác ABC ta đều có

$$f(A) + f(B) + f(C) \leqslant 3f(\frac{\pi}{3}).$$

Bài tập 2. Xét hàm số

$$f(t) = \begin{cases} \sin t & \text{khi} \quad 0 < t \leqslant \frac{\pi}{2} \\ g(t) & \text{khi} \quad \frac{\pi}{2} < t < \pi \end{cases}$$

Xác định các hàm số $g(t)$ xác định trong khoảng $(\frac{\pi}{2}, \pi)$ và thỏa mãn điều kiện:

Với mọi tam giác ABC ta đều có

$$f(A) + f(B) + f(C) \leqslant 3f(\frac{\pi}{3}).$$

Bài tập 3. Xét hàm số

$$f(t) = \begin{cases} g(t) & \text{khi} \quad 0 < t \leqslant \frac{\pi}{2} \\ \sin t & \text{khi} \quad \frac{\pi}{2} < t < \pi \end{cases}$$

Xác định các hàm số $g(t)$ xác định trong khoảng $(0, \frac{\pi}{2}]$ và thỏa mãn điều kiện:

Với mọi tam giác ABC ta đều có

$$f(A) + f(B) + f(C) \leqslant 3f(\frac{\pi}{3}).$$

Bài tập 4. Xét hàm số

$$f(t) = \begin{cases} g(t) & \text{khi} \quad 0 < t \leqslant \frac{\pi}{2} \\ \cos t & \text{khi} \quad \frac{\pi}{2} < t < \pi \end{cases}$$

Xác định các hàm số $g(t)$ xác định trong $(0, \frac{\pi}{2}]$ và thỏa mãn điều kiện:

Với mọi tam giác ABC ta đều có

$$f(A) + f(B) + f(C) \leqslant 3f(\frac{\pi}{3}).$$

Bài tập 5. Cho hàm số $p(t)$ xác định và lõm (có đạo hàm bậc hai âm) trong ((
Xét hàm số

$$f(t) = \begin{cases} q(t) & \text{khi} \quad 0 < t \leqslant \frac{\pi}{2} \\ g(t) & \text{khi} \quad \frac{\pi}{2} < t < \pi \end{cases}$$

Xác định các hàm số $g(t)$ xác định trong khoảng $(\frac{\pi}{2}, \pi)$ và thỏa mãn điều kiện:

Với mọi tam giác ABC ta đều có

$$f(A) + f(B) + f(C) \leqslant 3f(\frac{\pi}{3}).$$

Bài tập 6. Cho hàm số $p(t)$ xác định trong $(\frac{\pi}{2}, \pi)$. Xét hàm số

$$f(t) = \begin{cases} g(t) & \text{khi} \quad 0 < t \leqslant \frac{\pi}{2} \\ q(t) & \text{khi} \quad \frac{\pi}{2} < t < \pi \end{cases}$$

Xác định các hàm số $g(t)$ xác định trong khoảng $(0, \frac{\pi}{2}]$ và thỏa mãn điều kiện:

Với mọi tam giác ABC ta đều có

$$f(A) + f(B) + f(C) \leqslant 3f(\frac{\pi}{3}).$$

Bài tập 7. Xác định các hàm số $f(t)$ xác định trong khoảng $(0, \pi)$ và thỏa mãi
kiện:

Với mọi tam giác ABC ta đều có

$$f(A) + \cos B + \cos C \leqslant \frac{3}{2}.$$

Bài tập 8. Xác định các hàm số $f(t)$ xác định trong khoảng $(0, \pi)$ và thỏa mãi
kiện:

Với mọi tam giác ABC ta đều có

$$f(A) + \sin B + \sin C \leqslant \frac{3\sqrt{3}}{2}.$$

Bài tập 9. Xác định các hàm số $f(t)$ xác định trong khoảng $(0, \pi)$ và thỏa mãn điều kiện:

Với mọi tam giác ABC ta đều có

$$f(A) + \operatorname{tg}\frac{B}{2} + \operatorname{tg}^2\frac{C}{2} \geqslant 1.$$

Bài tập 10. Xác định các hàm số $f(t)$ xác định trong khoảng $(0, \pi)$ và thỏa mãn điều kiện:

Với mọi tam giác ABC ta đều có

$$f(A) + \operatorname{tg}\frac{B}{2} + \operatorname{tg}\frac{C}{2} \leqslant \sqrt{3}.$$

Bài tập 11. Xác định các hàm số $f(t)$ xác định trong khoảng $(0, \pi)$ và thỏa mãn điều kiện:

Với mọi tam giác ABC ta đều có

$$f(A) + \operatorname{cotg}^2\frac{B}{2} + \operatorname{cotg}^2\frac{C}{2} \geqslant 9.$$

Bài tập 12. Xác định các hàm số $f(t)$ xác định trong khoảng $(0, \pi)$ và thỏa mãn điều kiện:

Với mọi tam giác ABC ta đều có

$$f(A) + \operatorname{cotg}\frac{B}{2} + \operatorname{cotg}\frac{C}{2} \leqslant 3\sqrt{3}.$$

Bài tập 13. Xác định các hàm số $f(t)$ xác định trong khoảng $(0, \pi)$ và thỏa mãn điều kiện:

Với mọi tam giác ABC ta đều có

$$f(A) + f(B) \leqslant 2f(\frac{A+B}{2}).$$

Bài tập 14. Xác định các hàm số $f(t)$ xác định trong khoảng $(0, \pi)$ và thỏa mãn điều kiện:

Với mọi tam giác ABC ta đều có

$$f(A) + f(B) + \cos C \leqslant \frac{3}{2}.$$

Bài tập 15. Xác định các hàm số $f(t)$ xác định trong khoảng $(0, \pi)$ và thỏa mãn điều kiện:

Với mọi tam giác ABC ta đều có

$$f(A) + f(B) + \sin C \leqslant \frac{3\sqrt{3}}{2}.$$

BẤT PHƯƠNG TRÌNH HÀM TRONG TAM GIÁ ĐỐI VỚI BIẾN p, R, r

Bùi Công Huấn

0.1 Đặt vấn đề

Ta ký hiệu (R, r, p) tương ứng là bán kính đường tròn ngoại tiếp, đường tròn và nửa chu vi của tam giác có ba cạnh là a, b, c.

Gọi $f(R,r)$, $\mathcal{F}(R,r)$ là các hàm thuần nhất bậc hai của R, r. Gọi $q($ $\mathcal{Q}(R,r)$ là các dạng toàn phương bậc hai của R, r. Xét phương trình hàm

$$q(R,r) \leq f(R,r) \leq p^2 \leq \mathcal{F}(R,r) \leq \mathcal{Q}(R,r)$$

với mọi tam giác ABC sao cho dấu đẳng thức xảy ra khi tam giác đều hoặc c là bài toán hay. Sau đây chúng tôi giải quyết bất phương trình hàm (1) cho hàm cụ thể.

0.2 Lớp hàm thuần nhất bậc hai và biểu diễn đồ thị

Định lý 1. Cho $f(R,r)$ và $\mathcal{F}(R,r)$ là hai hàm thuần nhất bậc hai $f(R,r) \leq p^2 \leq \mathcal{F}(R,r)$ với mọi cặp tam giác (p,R,r) mà dấu đẳng thức xả tam giác đều. Vậy đúng với

$$f(R,r) = 2R^2 + 10Rr - r^2 + 2(R-2r)\sqrt{R^2-2Rr}$$
$$\mathcal{F}(R,r) = 2R^2 + 10Rr - r^2 - 2(R-2r)\sqrt{R^2-2Rr}$$

Chứng minh. Với a, b, c là ba cạnh của một tam giác, xét đa thức

$$\varphi(x) = (x-a)(x-b)(x-c)$$

Từ đó bằng cách khai triển đa thức ta suy ra rằng

$$\varphi(x) = x^3 - 2px^2 + (p^2 + 4Rr + r^2)x - 4pRr$$

Đa thức bậc ba này có ba nghiệm a, b, c, và có biệt thức

$$D = (a-b)^2(b-c)^2(c-a)^2$$

Rõ ràng $D \geq 0$ và dấu đẳng thứ xảy ra khi và chỉ khi tam giác cân. Mặt khá dàng tính được

$$D = 4r^2\{4Rr(R-2r)^2 - (p^2 + r - 10Rr - 2R^2)^2\} \geq 0$$

Vậy nên

$$(p^2 + r^2 - 10Rr - 2R^2)^2 \leq 4R(R - 2r)^3 \tag{5}$$

Dấu đẳng thức xảy ra khi tam giác cân. Từ (5) ta có

$$p^2 \geq 2R^2 + 10Rr - r^2 - 2(R - 2r)\sqrt{R^2 - 2Rr} \tag{6}$$

$$p^2 \leq 2R^2 + 10Rr - r^2 + 2(R - 2r)\sqrt{R^2 - 2Rr} \tag{7}$$

Biểu diễn đồ thị.

Tam giác (R, p, r) đồng dạng với tam giác $\left(\frac{R}{r}, \frac{p}{r}, 1\right)$. Gọi $x = R/r$ và $y = p/r$. Theo bất đẳng thức quan hệ giữa R và r của Euler thì $x \geq 2$. Từ bất đẳng thức (5), chia hai vế cho r^2 ta có bất đẳng thức tương đương dưới biến mới x, y

$$(y^2 + 1 - 10x - 2x^2)^2 \leq 4x(x - 2)^3 \tag{8}$$

Bất đẳng thức này lại tương đương với hai bất đẳng thức

$$y^2 \geq 2x^2 + 10x - 1 - 2(2 - x)\sqrt{x^2 - 2x} \tag{9}$$

$$y^2 \leq 2x^2 + 10x - 1 + 2(2 - x)\sqrt{x^2 - 2x} \tag{10}$$

Dấu đẳng thức xảy ra ở (9) và (10) khi và chỉ khi tam giác cân.

Trong mặt phẳng xOy trực chuẩn (8) là bất phương trình mô tả cho ta một miền S bao gồm các cặp điểm $x, y)$ thoả (8).

Bổ đề 1. Phép tương ứng $(R, p, r) \mapsto \left(\frac{R}{r}, \frac{p}{r}, 1\right)$ là một song ánh từ lớp tam giác đồng dạng sang miền S ở (8).
(Bạn đọc tự chứng minh).

Như vậy thay vì nghiên cứu tam giác tương ứng với bộ ba (R, p, r) ta nghiên cứu đồ thị của S ở (8).

Do miền S là miền cong có bờ liên tục nên cho ta khẳng định chặt của hàm $f(R, r)$ và $\mathcal{F}(R, r)$ như (2) và (3) của Định lý 1. Hay nói khác đi $f(R, r)$ và $\mathcal{F}(R, r)$ là nghiệm thuần nhất bậc hai của bất phương trình hàm

$$f(R, r) \leq p^2 \leq \mathcal{F}(R, r)$$

với dấu đẳng thức xảy ra cho tam giác cân.

0.3 Lớp các dạng toàn phương bậc hai

Định lý 2. Nếu $q(r, r)$ và $\mathcal{Q}(R, r)$ là hai dạng toàn phương bậc hai có hệ số thực thoả mãn bất phương trình hàm

$$q(R, r) \leq f(R, r) \leq p^2 \leq \mathcal{F}(R, r) \leq \mathcal{Q}(R, r)$$

Với mọi tam giác (R, p, r) mà dấu đẳng thức chỉ xảy ra cho tam giác đều thì
có

$$q(R,r) = 16Rr - 5r^2$$
$$\mathcal{Q}(R,r) = 4R^2 + 4Rr + 3r^2$$

Chứng minh. Ta có

$$\begin{aligned} 4R(R-2r^2) &= 4(R-2r^2)^2(R-r)^2 - 4r^2(R-2r^2) \\ &\leq 4(R-2r)^2(R-r)^2 \end{aligned}$$

Dấu đẳng thức xảy ra khi và chỉ khi $R = 2r$, tức là tam giác đều. Theo (5) ta

$$(p^2 + r^2 - 10Rr - 2R^2)^2 \leq 4(R-2r)^2(R-r)^2$$

hay là

$$16Rr - 5r^2 \leq p^2 \leq 4R^2 + 4Rr + 3r^2$$

Vậy ý thứ nhất của Định lý 2 đã được chứng minh.

Bây giờ ta chứng minh bất đẳng thức (13) không thể làm tốt hơn bằng c
dụng đồ thị S. Ta giả sử

$$\begin{aligned} 2x^2 + 10x - 1 + 2(x-2)\sqrt{x^2-2x} &\leq (4x^2+4x+3) - (\alpha x^2 + \beta x + \gamma \\ &\leq 4x^2 + 4x + 3, \ \forall x \geq 2 \end{aligned}$$

Thay $x = 2$ suy ra $4\alpha + 2\beta + \gamma = 0$. Ta phải có $\alpha x^2 + \beta x + \gamma \geq 0, \ \forall x >$
là

$$\alpha x^2 + \beta x - 4\alpha - 2\beta \geq 0, \ \forall x > 2$$

Giản ước cho $x - 2 > 0$ ta có

$$\alpha x + 2\alpha + \beta \geq 0, \ \forall x > 2$$

Lại có

$$2(x-2)\sqrt{x^2-2x} \leq (2-x)x^2 - (6+\beta)x + (4\alpha + 2\beta + 4), \ \forall x > 2$$

Giản ước cho $x - 2 > 0$ ta có

$$2\sqrt{x^2-2x} \leq (2-\alpha)x - (2\alpha + \beta + 2), \ \forall x > 2$$

Suy ra

$$\alpha(\alpha-4)x^2 + (4\alpha^2 + 2\alpha\beta - 4\alpha - 4\beta)x - (2\alpha + \beta + 2)^2 \geq 0 \forall x > 2$$

Từ (14) cho $x \to +\infty$ ta có $\alpha \geq 0$, cho $\alpha \to 2$ ta có $4\alpha + \beta \geq 0$.

Từ (15) cho $x \to \infty$ ta có $2 - \alpha \geq 0$, từ (16) cho $x \to +\infty$ ta có $\alpha(\alpha -$
suy ra $\alpha = 0, \beta = 0, \gamma = 0$. Đánh giá tương tự cho vế trái (13).

Vậy $q(R,r) = 16Rr - 5r^2$ và $\mathcal{Q}(R,r) = 4R^2 + 4Rr + 3r^2$ là nghiệm tốt nh
bất phương trình

$$q(R,r) \leq p^2 \leq \mathcal{Q}(R,r), \ \forall (R,p,r)$$

và dấu đẳng thức xảy ra khi tam giác đều.

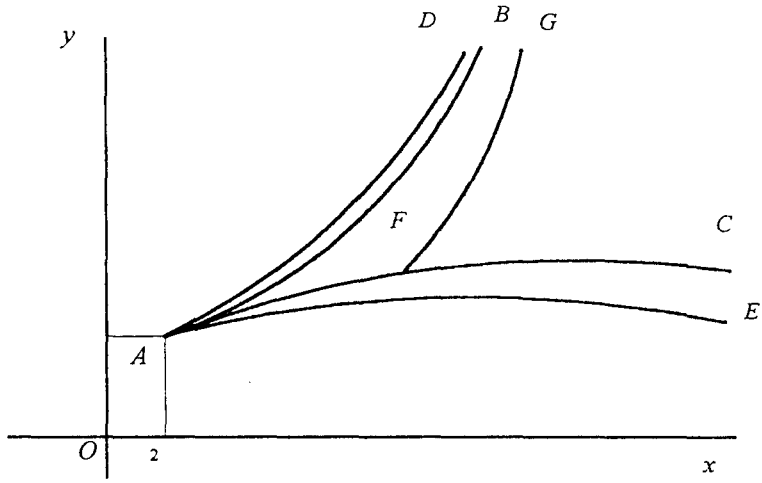
0.4 Một số vấn đề đồ thị

Gọi S là đồ thị của

$$(y^2 + 1 - 10x - 2x^2)^2 \leq 4x(x-2)^2$$

Theo bổ đề, ta có một phép song ánh từ tập gồm lớp các tam giác đồng dạng và đồ thị S. Ta nghiên cứu đồ thị S.

Xét đường cong



$$AB : y^2 = 2x^2 + 10x - 1 + 2(x-2)\sqrt{x^2 - 2x}$$
$$AC : y^2 = 2x^2 + 10x - 1 - 2(x-2)\sqrt{x^2 - 2x}$$
$$AD : y^2 = 4x^2 + 4x + 3$$
$$AE : y^2 = 16x - 5$$

Tất cả các đường cong này chung nhau tại điểm $A(2, 3, \sqrt{3})$. Từ các bất phương trình hàm ở trên ta có đường thẳng AD cao nhất và đường AE thấp nhất.

Đường cong AB và AC có độ nghiêng A đều là $\sqrt{3}$. Tam giác đều ứng với duy nhất điểm A. Độ nghiêng của AD tại A là $10\sqrt{3}/9$, độ nghiêng của AE tại A là $8\sqrt{3}/9$. Đường thẳng $y = 2x + 1$, $x \geq 2$ là tiệm cận của AB và AD. Vậy thì các điểm AB và AC chính là lớp tương đương của các tam giác cân.

áp dụng cho dạng bậc hai thay cho S là tập S' bị kẹp bởi hai biên AD và AE. Ta lại biết dấu của $p - 2R - r$ (là 0, là dương, là âm) cho ta phân loại (tam giác vuông, nhọn, hay tù)

Như vậy tam giác vuông là các điểm trên đường $y = 2x + 1$ của tập S nó là đường FG. Trong hình vẽ dưới đây ký hiệu $u = 2x + 3\sqrt{3} - 4$ và $t = s = 3\sqrt{3}$

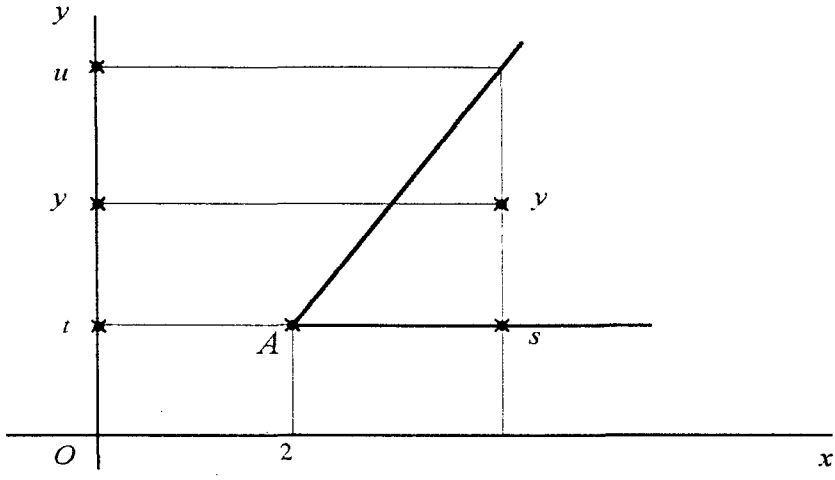
Điểm $F(1 + \sqrt{2}, 3 + 2\sqrt{2})$ đặc trưng cho lớp tam giác vuông. Miền tạo bởi BA, AF, FG tương ứng cho tam giác nhọn. Miền giữa FG và FC là miền tam giác

tù.

ứng dụng. Qua A kẻ đường thẳng song song với Ox và FG, khi đó miền k
hai đường này thoả mãn $3\sqrt{3} \le y \le 2x + (3\sqrt{3} - 4)$. Thay $x = R/r$ và $y = p$
có ngay bất đẳt thức tuyến tính

$$3\sqrt{3}r \le p \le 2R + (3\sqrt{3} - 4)r$$

Dấu đẳng thức xảy ra khi khi tam giác đều.



Gọi S là diện tích ta giác, ta đã biết $4S \le 3\sqrt{3}R^2$ suy ra $\sqrt{3}S \le 4Rr +$
(17) ta có bất phương trình hàm

$$S \le \varphi(R, r)$$

Cho nghiệm $\varphi(R, r) = 2Rr + (3\sqrt{3} - 4)r^2$.

Do $\sqrt{3abc} \le 2(R + r)$ suy ra

$$abc = 4pRr \le 8R^2r + (123\sqrt{3} - 16)Rr^2$$

Mà $\sin A + \sin B + \sin C = p/R \le \frac{3\sqrt{3}}{2}$. Vậy từ (17) ta có nghiệm của bất p
trình hàm

$$\sin A + \sin B + \sin C = p/R \le \varphi(R, r)$$

là $\varphi = 2 + (2\sqrt{3} - 4)r/R$.

Lại có $18Rr \le ab + bc + ca \le 9R^2$, áp dụng (13) ta có bất phương trình h

$$\varphi_1(Rr) = 20Rr - 4r^2 \le ab + bc + ca \le 4R^2 + 8Rr + 4r^2 = \varphi_2(R, r)$$

Từ định lý 1 ta có lời giải của bất phương trình hàm

$$2R^2 + 14Rr - 2(R - 2r)\sqrt{R^2 - 2Rr} \le ab + ca + bc$$
$$\le 2R^2 + 14Rr + 2(R - 2r)\sqrt{R^2 - 2Rr}$$
$$4R^2 + 16Rr - 3r^2 - 4(R - 2r)\sqrt{R^2 - 2Rr} \le a^2 + b^2 + c^2$$
$$\le 4R^2 + 16Rr - 3r^2 + 4(R - 2r)\sqrt{R^2 - 2Rr}$$

0.5 Tham số hoá

Đặt $\frac{R}{r} = 1 + \frac{1}{2}\left(t + \frac{1}{t}\right)$ với $t \leq 1$ thế thì $\frac{R}{r} = \frac{(t+1)^2}{2t}$, do tính đồng dạng của tam giác ta coi $r = 2t$ suy ra $R = (t+1)^2$ dẫn tới $R - 2r = (t-1)^2$ và $\sqrt{R^2 - 2Rr} = t^2 - 1$. Vậy (6) và (7) có dạng

$$4(2t+3) \leq p^2 \leq 4t(t+2)^3 \tag{20}$$

Trong (18) và (19) ta có

$$4(t+1)(2t+1)(5t+1) \leq ab + bc + ca \leq 4t(t+1)(2t+1)(5t+1)$$

và

$$8(2t+1)(3t^2+6t+1) \leq a^2 + b^2 + c^2 \leq 8t(t+2)(t^2+2t+3)$$

Chú ý. Với $t = 1$ là tam giác đều, $t \in (1, 1+\sqrt{2})$ là tam giác nhọn hoặc cân .

Định lý 3.

Với mọi $m \in [-1, 1]$ và mọi tam giác có bộ ba (R, r, p) thì

$$mp^2 \leq (m+1)^2R^2 - 2(m^2 - 5m + 2)Rr + (4-m)r^2 \tag{21}$$

Dấu đẳng thức xảy ra khi và chỉ khi tam giác đều hoặc cân có tỷ số độ dài cạnh đáy và cạnh bên là $1 - m$

Chứng minh.

Khi $m \in (0, 1)$ thì bất đẳng thức (21) tương đương với

$$p^2 \leq 4R^2 + 10Rr - r^2 + mR(R-2r) + \frac{1}{m}(R-2r)^2$$

hay là

$$p^2 + 2(R-2r)\sqrt{R(R-2r)} \leq F(R,r) + mR(R-2r) + \frac{1}{m}(R-2r)^2$$

mà $p^2 \leq \mathcal{F}(R, r)$ nên

$$2(R-2r)\sqrt{R^2 - 2Rr} \leq m(R^2 - 2Rr) + \frac{1}{m}(R-2r)^2$$

ta được điều phải chứng minh.

Khi $m \in (-1, 0)$ ta chứng minh tương tự. Khi $m = 0$ thì (21) cũng đúng
Sử dụng bổ đề ta có điều phải chứng minh.

Khi $m = 0$ thì Định lý 1. luôn đúng.

Ghi chú

a) Cho $m = -1$ ta có $p^2 \geq q(R,r) = 16Rr - 5r^2$

b) Cho $m = 1$ ta có $p^2 \leq \mathcal{Q}(R,r) = 4R^2 + 4Rr + 3r^2$

Định lý 4. Với mọi $m \in [-1,1)$, $u \geq 0$, $v > 0$ và mọi tam giác có (R,r,p) thì

$$mp^2 \leq (m+1)^2R^2 - 2(m^2-5m+2)Rr + (4-m)r^2 + ur(R-2r) + v(R-$$

Dấu đẳng thức xảy ra khi và chỉ khi tam giác đều.

Ghi chú.
Cho $m = \frac{1}{2}, u = 0, v = \frac{1}{4}$ ta có $p^2 \leq 5R^2 - Rr + 9r^2 = \varphi_1(R,r)$

Định lý 5. Cho $m \in (-1,0), m \in (0,1), u > 0$ và mọi (R,r,p) chứn rằng

$$mp^2 \leq (m+1)^2R^2 - 2(m^2-5m+2)Rr + (4-m)r^2 + u\left(R - \frac{2r}{1-m}\right.$$

Chứng minh. Như Định lý 3.

Ghi chú.
Cho $m = \frac{1}{2}, u = \frac{9}{4}$ ta có $p^2 \leq 9R^2 - 23Rr + 39r^2 = \varphi_2(R,r)$ với mọi $(R,r,$

Định lý 6. Nếu $f : (0, \frac{1}{2}) \to (0,\infty)$ là một hàm số sao cho $p \geq Rf$ mọi bộ ba (R,r,p). Khi đó dấu đẳng thức xảy ra khi tam giác đều hoặc tam g có đúng một góc lớn hơn $\pi/3$

Chứng minh. Giả sử tồn tại $\triangle ABC$ sao cho $A < \pi/3 < B \leq$ $p = Rf(\frac{r}{R})$.

Xét tam giác $A'B'C'$ mà

$$\begin{cases} \cos\frac{C'+B'}{2} = \cos\frac{C-B}{2} - \cos\frac{C+B}{2} \\ \cos\frac{C+B}{2} = \cos\frac{C'-B'}{2} - \cos\frac{C'+B'}{2} \end{cases}$$

Khi đó

$$\begin{aligned} \frac{r'}{R'} &= 4\sin\frac{A'}{2}\sin\frac{B'}{2}\sin\frac{C'}{2} \\ &= 2\cos\frac{C'+B'}{2}\left(\cos\frac{C'-B'}{2} - \cos\frac{C'+B'}{2}\right) \\ &= 2\left(\cos\frac{C-B}{2} - \cos\frac{C+B}{2}\right)\cos\frac{C+B}{2} = \frac{r}{R} \end{aligned}$$

Gọi $\cos\frac{C-B}{2} = x, \cos\frac{C+B}{2} = y$ với $x > y > 0$. Ta có

$$\begin{aligned}\frac{p}{R} &= \sin A + \sin B + \sin C \\ &= 2\sin\frac{C+B}{2}\left(\cos\frac{C+B}{2} + \cos\frac{C-B}{2}\right) \\ &= 2(x+y)\sqrt{1-y^2}\end{aligned}$$

$$\frac{p'}{R} = 2\sin\frac{C'+B'}{2}\left(\cos\frac{C'+B'}{2} + \cos\frac{C'-B'}{2}\right) = 2(2x-y)\sqrt{1-(x-y)^2}$$

Do đó ta có

$$\frac{p}{R} > \frac{p'}{R'}$$

Suy ra

$$p' \le p.\frac{R'}{R} = \frac{R'}{R}.R.f(\frac{r}{R}) = R'f'(\frac{r'}{R'})$$

Dẫn tới mâu thuẫn.

Định lý 7. Nếu $g : (0, \frac{1}{2} \to (0, \infty)$ là một hàm số sao cho $p \ge Rg(\frac{r}{R})$ đúng với mọi (R, r, p) của tam giác. Dấu đẳng thức xảy ra khi và chỉ khi tam giác đều hoặc có đúng một góc lớn hơn $\pi/3$.

Chứng minh. Như Định lý 6.

0.6 Phương trình hàm dạng $f(A+B, B) = f(A, A+B)$

Ký hiệu $\mathbb{R}[x, y]$ là vành các đa thức hai biến hệ số thực và $\mathbb{R}(x, y)$ là trường các phân thức hai biến hệ số thức. Coi $f \in \mathbb{R}(x, y)$ và xét phương trình hàm

$$f(a+b, b) = f(a, a+b) \tag{22}$$

hay là

$$f(x, y) = f(x-y, x) \tag{23}$$

Ta xác định tự đẳng cấu

$$T : F_{(x,y)} \to F_{(x,y)}$$

bởi $T(x) = x - y$ và $T(y) = x$. Gọi G là tập bất biến của T, ta có

$$\begin{aligned}T(x) &= x - y \\ T^2(x) &= -y \\ T^3(x) &= -x \\ T^4(x) &= -x + y \\ T^5(x) &= y \\ T^6(x) &= x\end{aligned}$$

Như vậy $T^6(y) = y$ và $T^6 = I$ (đồng nhất). Ta có $[\mathbb{R}(x,y) : G] = 6$. H
$T(x), T^2(x), T^3(x), ..., T^6(x) \in G$. Và

$$\prod_{i=1}^{6}[ww - T^i(x)] = (w^2 - x^2)(w^2 - y^2)(w^2 - (y-x)^2)$$

Gọi S_j $(j = \overline{1,6})$ là cac đa thức Viét của $T^i(x)$ $(i = \overline{1,6})$. Ta có

$$\begin{aligned}
S_1 &= 0\\
S_3 &= 0\\
S_5 &= 0\\
S_2 &= 2x^2 - x - y + 2y^2\\
S_4 &= x^2y^2 + x^2(x-y)^2 + y^2(x-y)^2\\
S_6 &= x^2y^2(x-y)^2\\
S_4 &= \frac{1}{4}(S_2)^2
\end{aligned}$$

Vậy $\mathbb{R}(S_1, S_2, S_3, S_4, S_5, S_6) = F(S_2, S_6) \supseteq G$. Và $G \subset \mathbb{R}(x,y)$ suy ra F
G. Với x là nghiệm của (24) là phương trình bậc sau có hệ số trùng $\mathbb{R}(S_2, S$
là nghiệm của phương trình bậc hai có hai hệ số trong $\mathbb{R}(S_2, S_6, x)$ do $2x^2 -$
$2y^2 - S_2 = 0$. Ta có $[\mathbb{R}(x,y) : \mathbb{R}(S_2, S_6)] \leq 12$. Vậy $[\mathbb{R}(x,y) : \mathbb{R}(S_2, S_2) =$
$[G : \mathbb{R}(S_2, S_6)] = 2$ suy ra

$$P = xy(x-y)(x^3 - x^2y - 2xy^2 + y^3)$$

và có $G = \mathbb{R}(S_2, S_6, P)$

Nhận xét.

1. Các kết quả Định lý 8 và 9 cho ta dấu hiệu kiểm nghiệm tính nghiêm n
bất phương trình hàm kiểu (1).
2. Tự nhiên phát triển của bài toán cho dạng bậc cao là vấn vấn đề cần ngh
tiếp
3. Xét bất phương trình hàm cho đa giác, cho tứ diện tương tự hay không'
4. Việc đưa sự nghiên cứu bất phương trình hàm về nghiên cứu S và S'
bài này là một hướng mở ra hay.

Mong rằng sẽ có điều kiện để chúng tôi trao đổi thêm về vấn đề này.

TÀI LIỆU THAM KHẢO

[1] **I. Bludon,** Canad. Math. Bull. (8) 1995, 615–626

[2] **Al. Lupas,** "On Some geometric. Inequality". R.M.T. 1/1984.

[3] **L. Nicolescu,** "Inequalities in R, r" Bulutin. Math Romanial 1987

ĐỒNG DƯ VÀ PHƯƠNG TRÌNH ĐỒNG DƯ

Đặng Hùng Thắng

I. Đồng dư Đồng dư là một khái niệm cực kỳ cơ bản và đầy sức mạnh trong lý thuyết số. Khái niệm này do nhà toán học Đức Gauss,(1777-1855) ông vua toán học, một trong những nhà toán học lỗi lạc nhất của nhân loại đưa ra .Nó được trình bày trong tác phẩm "Disquistiones Arthmeticcae"của ông xuất bản năm 1801khi ông mới 24 tuổi.

1.1 Định nghĩa Cho số nguyên dương n. Hai số nguyên $a, b \in \mathbb{Z}$ được gọi là đồng dư theo modun n và ta viết $a \equiv b \pmod{n}$ nếu khi chia cho n chúng cho cùng một số dư. Dễ thấy ba khẳng định sau là tương đương

1. $a \equiv b \pmod{n}$
2. $a - b$ chia hết cho n
3. $a = b + kn$ với $k \in \mathbb{Z}$

Ký hiệu đồng dư $\equiv$ nhằm nhấn mạnh sự kiện rằng đồng dư có rất nhiều tính chất giống với đẳng thức.

1.2 Tính chất

1. Nếu $a \equiv b \pmod{n}, c \equiv d \pmod{n}$ thì $a \pm c \equiv b \pm d \pmod{n}, ac \equiv bd \pmod{n}$
2. Với mọi $k \in \mathbb{N}^*$ $a \equiv b \pmod{n} \rightarrow a^k \equiv b^k \pmod{n}$
3. (Luật giản ước) Nếu $ac \equiv bc \pmod{n}, (c, n) = 1$ thì $a \equiv b \pmod{n}$.

   Nói riêng nếu n là số nguyên tố $ac \equiv bc \pmod{n}, c \not\equiv 0 \pmod{n} \rightarrow a \equiv b \pmod{n}$

II. Hệ thặng dư

2.1 Hệ thặng dư đầy đủ Cho tập $A = \{a_1, a_2, ..., a_n\}$. Giả sử $r_i, 0 \leqslant r_i \leqslant n - 1$ là số dư khi chia a_i cho r_i. Nếu tập các số dư $\{r_1, r_2, ..., r_n\}$ trùng với tập $\{0, 1, .., n - 1\}$ thì ta nói A là một hệ thặng dư đầy đủ (gọi tắt là HĐĐ)(modun n). Dễ thấy: Tập A lập thành một HĐĐ(modun n) nếu và chỉ nếu $i \neq j \rightarrow a_i \neq a_j \pmod{n}$

Nếu $A = \{a_1, a_2, ..., a_n\}$ là HĐĐ mod n thì từ định nghĩa dễ suy ra

- Với mọi $m \in \mathbb{Z}$ tồn tại và duy nhất $a_i \in A$ sao cho $a_i \equiv m \pmod{n}$
- Với mọi $a \in \mathbb{Z}$ tập $A + a = a_1 + a, a_2 + a, ..., a_n + a$ cũng lập thành HĐĐ modn

- Nếu $c \in \mathbb{Z}, (c,n) = 1$ thì tập $cA = ca_1, ca_2, ..., ca_n$ cũng lập thành HĐĐ

Ví dụ 1 Cho hai HĐĐ mod n $A = \{a_1, ..., a_n\}$ và $B = \{b_1, .., b_n\}$. Chứng m
nếu n là số chẵn thì tập $A + B = \{a_1 + b_1, ..., a_n + b_n\}$ không lập thành m
mod n. Có thể nói gì nếu n là số lẻ?

Giải Ta nhận xét rằng nếu $C = \{c_1, ..., c_n\}$ là HĐĐ mod n thì ta có $\sum$
$\sum_{i=1}^{n} i = n(n+1)/2 \not\equiv 0$(do n chẵn). Ta có$\sum_{i=1}^{n}(a_i + b_i) \equiv \sum_{i=1}^{n} ia_i + \sum$
$n(n+1)/2 + n(n+1)/2 = n(n+1) \equiv 0$. Vậy$A + B = \{a_1 + b_1, ..., a_n + b_n$
lập thành một HĐĐ.

Nếu n lẻ thì chưa kết luận được. Nghĩa là $A + B$ có thể là HĐĐ, có thể
HĐĐ. Chẳng hạn xét $n = 3$ Nếu $A = \{1, 2, 3\}, B = \{4, 5, 6\}$ thì $A + B = \{5$
HĐĐ mod 3. Tuy nhiên với $B' = \{5, 4, 6\}$ thì $A + B' = \{6, 6, 9\}$ lại không
mod 3.

Ví dụ 2 Cho hai số nguyên dương m, n và hai tập $A = \{a_1, ..., a_n\}$
$\{b_1, .., b_m\}$ trong đó A là HĐĐ mod n ,B là HĐĐ mod m. Chứng minh
$(m,n) > 1$ thì tập $AB = \{a_i b_j\} i = 1, 2, .., nj = 1, 2, ..., m$ không lập th
HĐĐ mod mn. Có thể nói gì nếu $(m,n) = 1$.

Giải Ta có nhận xét sau: Nếu $A = \{a_1, ..., a_n\}$ là HĐĐ mod n và p là ướ
tố của n thì trong A có đúng $n - n/p$ số không chia hết cho p. Thật vậ
$a_i = q_i n + r_i, 1 \leqslant r_i \leqslant n$. Do A là HĐĐ nên các r_i phân biệt. Ta có a_i chia
p khi và chỉ khi r_i chia hết cho p. Số phần tử của A chia hết cho p bằng s
nguyên dương $k, k \leqslant n$ là bội của n, Dễ thấy số đó là n/p. Do đó số các
chia hết cho p trong A là $n - n/p$

Một phần tử $a_i b_j \in AB$ không chia hết cho p khi và chỉ khi cả a_i và b_j đ
chia hết cho p. Nếu AB là một HĐĐ mod mn thì từ nhận xét trên ta suy ra

$$mn - \frac{mn}{p} = (n - \frac{n}{p})(m - \frac{m}{p}) \Leftrightarrow \frac{mn}{p} = \frac{mn}{p^2}$$

Đây là điều vô lý vì $p > 1$.

Nếu$(m,n) = 1$ thì chưa kết luận được.Nghĩa là $A + B$ có thể là
thể không là HĐĐ. Ví dụ $n = 2, m = 3$ Nếu $A = \{1, 2\}, B = \{5,$
$AB = \{5, 7, 9, 10, 14, 18\}$ là HĐĐ mod 6. Nếu $A = \{1, 2\}, B = \{5$
$AB = \{5, 6, 7, 10, 12, 14\}$ không là HĐĐ mod 6.

Ví dụ 3 Một số nguyên dương T gọi là số tam giác nếu nó có dạng $T = k$
. Tìm tất cả các số nguyên dương n có tính chất: Tồn tại một HĐĐ mod n
tam giác.

Giải Ta chứng minh số n có dạng $n = 2^s$.

i) Nếu $n = 2^s$. Ta xét tập $A = \{T_{2i-1}\}_{i=1}^{n}$ ở đó $T_k = k(k+1)/2$. T
HĐĐ mod n vì nếu$T_{2i-1} \equiv T_{2j-1} \to (i-j)(2i+2j-1)$ chia hết cho n. V
có ước lẻ nên $i - j$ chia hết cho n. Mâu thuẫn.

Đảo lại giả sử tồn tại một HĐĐ A mod n gồm n số tam giác với $n =$
$m > 1$ là số lẻ. Xét tập $B = \{T_i\}_{i=1}^{m}$. Ta chứng minh B là HĐĐ mod m.
lấy $x \in \{1, 2, ..., m\}$. Vì A là HĐĐ mod n nên tồn tại số tam giác $T_k \in$
$T_k \equiv x \pmod{n} \to T_k \equiv x \pmod{m}$. Giả sử $k \equiv i \pmod{m}, i \in \{1, 2, ..$
đó $k(k+1) \equiv i(i+1) \pmod{m}$. Vì m lẻ nên từ đó suy ra $T_i \equiv T_k \equiv x$
Vậy B là HĐĐ mod m. Nhưng điều này là mâu thuẫn vì $T_m = m(m +$
$\pmod{m}, T_{m-1} = m(m-1)/2 \equiv 0 \pmod{m}$

Chú thích Ví dụ 3 có thể phát biểu dưới dạng một bài toán vui như sau: Một lớp gồm n học sinh đứng thành vòng tròn để chuyền bóng ngược chiều kim đồng hồ theo quy tắc sau: Lớp trưởng (coi là học sinh mang số một) bỏ qua học sinh bên cạnh(học sinh mang số hai) chuyền bóng cho học sinh mang số ba. Học sinh mang số ba có bóng, bỏ qua hai học sinh kế tiếp (mang số bốnư và số năm) chuyền bóng cho học sinh mang số sáu. Học sinh mang số sáu có bóng , bỏ qua ba học sinh kế tiếp (mang số 7,8,9) chuyền bóng cho học sinh mang số 10 và cứ tiếp tục như thế. Chứng minh rằng nếu n không có ước lẻ thì luôn tồn tại ít nhất một học sinh không bao giờ nhận được bóng.

Thật vậy bằng quy nạp dễ dàng chứng minh được em thứ mang số i nhận được bóng khi và chỉ khi tồn tại $k \in \mathbb{N}^*$ để $T_k \equiv i \pmod n$. Như vậy tất cả mọi học sinh đều có bóng khi và chỉ khi tồn tại một HĐĐ mod n gồm các số tam giác.

2.1 Hệ thặng dư thu gọn

Cho $B = \{b_1, ..., b_k\}$ là một tập gồm k số nguyên và $(b_i, n) = 1$ với mọi $i = 1, 2, ..., k$. Giả sử $b_i = q_i n + r_i, 1 \leqslant r_i < n$. Khi đó dễ thấy $(r_i, n) = 1$. Nếu tập $\{r_1, r_2, ..., r_k\}$ bằng tập K gồm tất cả các số nguyên dương bé hơn n và nguyên tố với n thì B được gọi là hệ thặng dư thu gọn mod n. gọi tắt là hệ thu gọn mod n.

Dễ thấy một tập $B = \{b_1, ..., b_k\}$ gồm m số nguyên lập thành một hệ thu gọn khi và chỉ khi

1. $(b_i, n) = 1$
2. $b_i \equiv b_j \pmod n$
3. Số phần tử của B là $\phi(n)$ ở đó $\phi(n)$ là hàm Ole

Điều kiện 3) tương đương với

3'. Với mọi số $x \in \mathbb{Z}, (x, n) =$ tồn tại duy nhất $b_i \in B$ sao cho $x \equiv b_i \pmod n$

Từ định nghĩa ta suy ra nếu $B = \{b_1, ..., b_k\}$ là một hệ thu gọn mod n , c là số nguyên với $(c, n) = 1$ thì tập $cB = \{cb_1, ..., cb_k\}$ cũng là hệ thu gọn mod n

Ví dụ 1 Cho hai số nguyên dương m, n với $(m, n) = 1$. Giả sử $A = \{a_1, .., a_h\}$ và $B = \{b_1, ..., b_k\}$ tương ứng là các hệ thu gọn mod m và mod n. Xét tập $C = \{a_i n + b_j m\}, 1 \leqslant i \leqslant h, 1 \leqslant j \leqslant k$

a) Chứng minh rằng C là hệ thu gọn mod mn

b)Suy ra công thức tính hàm O le $\Phi(n)$

Giải a) Đầu tiên ta chứng minh $(a_i n + b_j m, mn) = 1$. Giả sử trái lại p là ước nguyên tố chung của $a_i n + b_j m$ và mn. Do $(m, n) = 1$ nên chẳng hạn $p|n$ và p không là ước của m. Suy ra $p|b_j m \rightarrow p|b_j$ Vậy p là ước chung của n và b_j. Mâu thuẫn.

Ta chứng minh 2). Giả sử có $a, a' \in A, b, b' \in B$ sao cho $an + bm \equiv a'n + b'm \pmod m n \rightarrow an \equiv a'n \pmod m \rightarrow a \equiv a' \pmod n$ (do $(m, n) = 1$). Điều này mâu thuẫn.

Ta chứng minh 3') Giả sử $(x, mn) = 1$. Suy ra $(x, m) = 1, (x, n) = 1$. Vì $(m, n) = 1$ nên tập $\{B = \{mb_1, ..., mb_k\}$ là hệ thu gọn mod n. Vậy tồn tại $b \in B$ để $x \equiv mb \pmod n$. Tương tự tồn tại $a \in A$ để $x \equiv na \pmod m$. Từ đó suy ra $x \equiv na + mb \pmod n, x \equiv na + mb \pmod m$. Từ đó do $(m, n) = 1$ ta rút ra $x \equiv na + mb \pmod{mn}$.

b) Theo định nghĩa hàm Ole ta có $h = \phi(m).k = \phi(n)$ và $|C| = \phi(mn)$. từ a) suy ra $|C| = hk \Leftrightarrow \phi(mn) = \phi(m)\phi(n)$. Như vậy $\phi(n)$ là một hàm nhân tính.

Nếu p là một số nguyên tố thì số i là nguyên tố với p^s khi và chỉ khi i chia hết cho p. Số các số chia hết cho p và không vượt quá p^s là p^{s-1}.Thì $\phi(p^s) = p^s - p^{s-1} = p^{s-1}(p-1) = p^s(1-1/p)$. Nếu n có phân tích ngư $n = p_1^{s_1}...p_k^{s_k}$ thì do $\phi(n)$ là hàm nhân tính nên

$$\begin{aligned}\phi(n) &= \phi\left(p_1^{s_1}\right)...\left(p_k^{s_k}\right)\\ &= p_1^{s_1}(1-1/p_1)...(p_k^{s_k}(1-1/p_k)\\ &= n(1-\frac{1}{p_1})....(1-\frac{1}{p_k})\end{aligned}$$

Ví dụ 2 Cho $p > 3$ là số nguyên tố có dạng $p = 3k+2$.

a) Chứng minh rằng tập $A = \{2^3-1, 3^3-1, ..., p^3-1\}$ là hệ thu gọn mo

b) Chứng minh rằng $\Pi_{i=1}^{p}(i^2+i+1) \equiv 3 \pmod p$

Giải Hiển nhiên mỗi phần tử của A đều không chia hết cho p. Giả sử $i^3-1 \equiv$ $\pmod p \rightarrow i^3 \equiv j^3 \pmod p \rightarrow i^{3k} \equiv j^{3k} \pmod p \rightarrow$. Theo định lý $i^{3k+1} \equiv j^{3k+1} \equiv 1 \pmod p$. Từ đó suy ra $i \equiv j \pmod p \rightarrow i = j$.

Vì $\phi(p) = p-1 = |A|$ nên A là hệ thu gọn mod p.

b)Vì $B = \{1, 2, ..., p-1\}$ là hệ thu gọn mod p nên ta có $\Pi_{i=2}^{p}(i^3-1) \equiv (p-$ $\Pi_{i=2}^{p}(i-1)\Pi_{i=2}^{p}(i^2+i+1) \equiv (p-1)! \pmod p \Leftrightarrow (p-1)!\Pi_{i=2}^{p}(i^2+i+1) \equiv$ $\pmod p \Leftrightarrow \Pi_{i=2}^{p}(i^2+i+1) \equiv 1 \pmod p$. Suy ra $\Pi_{i=1}^{p}(i^2+i+1) \equiv 3$ (mo

Định lý Euler Cho n là số nguyên dương và $a \in \mathbb{Z}$ sao cho $(a,n) = 1$.

$$a^{\phi(n)} \equiv 1 \pmod n$$

Một cách tổng quát với mọi số nguyên $a \in \mathbb{Z}$ ta có

$$a^n \equiv a^{n-\phi(n)} \pmod n$$

Chứng minh Lấy một hệ thu gọn B (mod n). Giả sử $B = \{b_1, b_2, ..., b_m$ $m = \phi(n)$. Vì $(a,n) = 1$ nên tập $aB = \{ab_1, ab_2, ..., ab_m\}$ cũng là hệ thu gọ n). Thành thử

$$(ab_1)(ab_2)...(ab_m) \equiv b_1.b_2....b_m \pmod n$$

Suy ra

$$a^m b_1.b_2....b_m \equiv b_1.b_2....b_m \pmod n \Leftrightarrow a^{\phi(n)} \equiv 1 \pmod n$$

b) Ta phải chứng minh

$$T = a^n - a^{n-\phi(n)} = a^{n-\phi(n)}(a^{\phi(n)}-1) \equiv 0 \pmod n$$

Giả sử n có phân tích tiêu chuẩn $n = p_1^{t_1}...p_k^{t_k}$. Với mỗi i cố định ta chứng chia hết cho $p_i^{t_i}$.Để cho gọn ta đặt $p = p_i, t = t_i$.

Nếu $(a,p) = 1$ theo phần a) ta có $a^{\phi(p^t)} - 1$ chia hết cho p^t. Vì hàm nhân tính nên $\phi(n)$ chia hết cho $\phi(p^t)$. Suy ra $a^{\phi(n)} - 1$ chia hết cho $a^{\phi(p^t)} -$ $a^{\phi(n)} - 1$ chia hết cho p^t. Vậy T chia hết cho p^t.

Nếu $p|a$. Khi đó $a^{n-\phi(n)}$ chia hết cho $p^{n-\phi(n)}$. Mặt khác $n-\phi(n) \geq t$ bởi nhất t số không nguyên tố với p là $p^1, p^2, ..., p^t$, Suy ra $a^{n-\phi(n)}$ chia hết cho chia hết cho p^t.

Tóm lại với mọi $i = 1, 2, ..., k$ ta đều có $A \equiv 0 \pmod{p_i^{t_i}}$. Suy ra A chia hết cho n.

Hệ quả (định lý Ferma) Nếu p là một số nguyên tố và $a \in \mathbb{Z}$ sao cho $(a, p) = 1$. Khi đó

$$a^{p-1} \equiv 1 \pmod{p}$$

Với số nguyên a bất kỳ thì $a^p \equiv a \pmod{p}$

Thật vậy nếu p là số nguyên tố thì $\phi(p) = p - 1$.

Định lý Wilson Cho $n > 1$ là số nguyên dương. Khi đó n là số nguyên tố khi và chỉ khi

$$(n-1)! \equiv -1 \pmod{n}$$

Chứng minh Giả sử p là số nguyên tố. Nếu $p = 2, 3$ thì kết luận đúng. Xét $p > 3$. Xét tập $A = \{2, 3, ..., p-2\}$. Với mỗi $k \in A$ tồn tại duy nhất $k', 1 \leqslant k' \leqslant p-1$ sao cho $kk' \equiv 1 \pmod{p}$. Ta có $k' \in A$ Thật vậy nếu $k' = 1 \rightarrow k = 1$ Mâu thuẫn. Nếu $k' = p-1 \rightarrow k = p-1$ Mâu thuẫn. Mặt khác ta lại có $k \neq k'$. Thật vậy nếu $k = k' \rightarrow k^2 \equiv 1 \pmod{p} \rightarrow (k-1)(k+1) \equiv 0 \pmod{p}$. Suy ra $k = 1$ hoặc $k = p-1$ Mâu thuẫn. Dễ thấy $(k')' = k$. Vậy các phần tử của A được ghép thành $(p-3)/2$ cặp (k, k') vưới $kk' \equiv 1 \pmod{p}$. Thành thử $\Pi_{k=2}^{p-2} k \equiv 1 \pmod{p}$. Do đó $(p-1)! \equiv 1(p-1) \equiv -1 \pmod{p}$.

Đảo lại giả sử $(n-1)! \equiv -1 \pmod{n}$ và $n = ab$ với $1 < a < b < n$. Khi đó $1 < a < (n-1)$ Như vậy $(n-1)!$ chia hết cho a . Vì $(n-1)! + 1$ cũng chia hết cho a nên suy ra 1 chia hết cho a.Mâu thuẫn.

Ví dụ Chứng minh rằng $61! \equiv 63! \equiv -1 \pmod{71}$.

Giải Với $k < p$ là một số nguyên dương ta có $-1 \equiv (p-1)! = (p-k-1)!(p-k)(p-k+1)...(p-1) \equiv (p-k-1)!(-1)^k k! \pmod{p}$ Do đó nếu $(-1)^k k! \equiv 1 \pmod{p}$ thì $(p-k-1)! \equiv -1 \pmod{p}$ Với p=71 ta có $k = 7$ và $k = 9$ thỏa mãn điều kiện $(-1)^k k! \equiv 1 \pmod{71}$. Vậy ta có điều cần chứng minh.

Định lý thặng dưTrung hoa Cho k số nguyên dương $n_1, n_2, ..., n_k$ đôi một nguyên tố cùng nhau và k số nguyên bất kỳ $a_1, a_2, ..., a_k$. Khi đó tồn tại số nguyên a thỏa mãn

$$a \equiv a_i \pmod{n_i} \quad \forall i = 1, 2, ..., k \tag{1}$$

Số nguyên b thỏa mãn (1) khi và chỉ khi $b \equiv a \pmod{n}$ ở đó $n = n_1...n_k$

Chứng minh Ký hiệu $N_i = n/n_i = \Pi_{j \neq i} n_j$. Khi đó $(N_i, n_i) = 1, N_j \equiv 0 \pmod{n_i}$ nếu $j \neq i$. Thành thử với mỗi i tồn tại b_i sao cho $N_i b_i \equiv 1 \pmod{n_i}$. Nếu $j \neq i$ thì hiển nhiên $N_j b_j \equiv 0 \pmod{n_i}$. Xét số

$$a = \sum_{j=1}^{k} N_j b_j a_j$$

Ta có với mỗi i do $N_i b_i \equiv 1 \pmod{n_i}, N_j b_j \equiv 0 \pmod{n_i}$nếu$i \neq j$. Vậy $a \equiv a_i \pmod{n_i}$.

Nếu $b \equiv a \pmod{n}$ thì $b \equiv a \equiv a_i \pmod{n_i}$. Ngược lại nếu b thỏa mãn (1) thì $b - a$ chia hết cho n_i với mọi i . Vì $n_1, n_2, ..., n_k$ đôi một nguyên tố cùng nhau nên suy ra $b - a$ chia hết cho n hay $b \equiv a \pmod{n}$.

Ví dụ 1 Tìm số nguyên dương nhỏ nhất có tính chất: Chia 7 dư 5, chia 11 dư 7 và chia 13 dư 3.

Giải Ta có $n_1 = 7, N_1 = 11.13 = 143; n_2 = 11, N_2 = 7.13 = 91; n_3 = 13$ $7.11 = 77$. Ta có $N_1 b_1 \equiv 3b_1 \equiv 1 \pmod 7 \rightarrow b_1 = -2$. Tương tự $b_2 = 4, b_3$ Vậy

$$a = (143)(-2)(5) + (91)(4)(7) + (77)(3)(-1) = -1430 + 2548 - 231 =$$

Tất cả các số thỏa mãn có dạng $b = 887 + 1001k$. Vậy 887 là số cần tìm.

Ví dụ 2 Chứng minh rằng tồn tại số nguyên dương k sao cho $u_n = 2^n k$ hợp số với mọi n.

Giải Xét các số Fecma $F_n = 2^{2^n} + 1$. Ta nhận thấy các số F_n đôi một ng cùng nhau. Thật vậy giả sử $m > n$ và $p|F_n, p|F_m$. Ta có

$$2^{2^m} = (2^{2^n})^{2^{m-n}} \equiv (-1)^{2^{m-n}} \equiv 1 \pmod p$$

Mà $2^{2^m} \equiv -1 \pmod p$. Suy ra $1 \equiv -1 \pmod p$. Vô lý vì p lẻ.

Ta đã biết F_5 có phân tích nguyên tố là $F_5 = (641)(6700417)$. Đặt $p = 6$ 6700417 .Theo định lý thặng dư Trung hoa tồn tại số nguyên dương k v $max(F_1, F_2, F_3, F_4, p, q)$ sao cho

$$\begin{cases} k \equiv 1 \pmod{F_m}, m = 1, 2, 3, 4 \\ k \equiv 1 \pmod p \\ k \equiv -1 \pmod q \end{cases}$$

Ta chứng minh k là số cần tìm. Thật vậy giả sử $n = 2^m b$ với b là số lẻ. Nếu thì $u_n = 2^n k + 1 \equiv 2^n + 1 = (2^{2^m})^b + 1 \equiv 0 \pmod{F_m}$ và $u_n > k > F_m$. D là hợp số. Nếu $m = 5$ ta có $u_n = 2^n k + 1 \equiv 2^n + 1 = (2^{2^5})^b + 1 \equiv 0$ (mc $u_n > k > p$ do đó u_n là hợp số. Nếu $m > 5$ ta có $n = 2^5 c$ với c là số chẵn.

$$2^n = (2^{2^5})^c = (F_5 - 1)^c \equiv (-1)^c \equiv 1 \pmod q$$

do đó

$$u_n = 2^n k + 1 \equiv -2^n + 1 \equiv -1 + 1 = 0 \pmod q$$

Vì $u_n > k > q$ nên u_n là hợp số.

Số chính phương(mod n)

Định nghĩa Cho số nguyên dương n. Số nguyên a được gọi là số chính (mod n) nếu tồn tại $x \in \mathbb{N}$ sao cho

$$x^2 \equiv a \pmod n$$

Rõ ràng một số chính phương sẽ là số chính phương (mod n) với mọi n. Tr một số không chính phương có thể là số chính phương theo một mod n nào đó hạn 2 là số chính phương (mod 7) vì $3^2 \equiv 2 \pmod 7$.

Bài toán: Có tồn tại chăng số không chính phương a nhưng là số chính (mod n) với mọi n?

Với mỗi số nguyên dương n cho trước ta muốn tìm một tiêu chuẩn để r một số a khi nào là số chính phương (mod n).

I. Trường hợp $n = p$ là số nguyên tố.

Hiển nhiên nếu $p|a \Leftrightarrow a \equiv 0 \pmod p$ thì a là số chính phương (mod p) ta chỉ xét $(a, p) = 1$

Định lý Cho p là số nguyên tố

i) Nếu $p = 2$ thì mọi số a lẻ đều là số chính phương (mod 2).

ii) Nếu $p > 2$. Khi đó

a là số chính phương (mod p) khi và chỉ khi

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

a là số không chính phương (mod p) khi và chỉ khi

$$a^{(p-1)/2} \equiv -1 \pmod{p} \tag{3}$$

Chứng minh Giả sử a là số chính phương (mod p). Vậy tồn tại tồn tại $x \in \mathbb{N}$ sao cho

$$x^2 \equiv a \pmod{n}$$

Do $(a,p) = 1$ nên $(x,p) = 1$. Từ đó $a^{(p-1)/2} \equiv x^{p-1} \equiv 1 \pmod{p}$ theo định lý Ferma.

Đảo lại giả sử có (2). Với mỗi $k \in \{1,2,..,p-1\}$ tồn tại duy nhất $k' \in \{1,2,..,p-1\}$ sao cho $kk' \equiv a \pmod{p}$. Nếu tồn tại $k = k'$ thì ta có $kk' = k^2 \equiv a \pmod{p}$ suy ra a là số chính phương (mod p). Nếu trái lại thì tập $\{1,2,...,p-1\}$ được chia thành (p-1)/2 tập con hai phần tử $\{k,k'\}$ mà tích của chúng đồng dư với a(mod p). Suy ra $(p-1)! \equiv a^{(p-1)/2} \equiv 1 \pmod{p}$. Nhưng theo định lý Wilson $(p-1)! \equiv -1 \pmod{p}$ .Vậy $1 \equiv -1 \pmod{p}$ Mâu thuẫn do p lẻ. Do định lý Ferma với mỗi số nguyên a không chia hết cho p hoặc $a^{(p-1)/2} \equiv 1 \pmod{p}$ hoặc $a^{(p-1)/2} \equiv$-1 $\pmod{p}$. Từ đó suy ra (3).

Hệ quả Cho p là số nguyên tố lẻ. Khi đó

- Tích của hai số chính phương (mod p) là số chính phương(mod p)
- Tích của hai số không chính phương (mod p) là số chính phương(mod p)
- Tích của một số không chính phương (mod p) với một số chính phương(mod p) là số không chính phương (mod p)
- (-1) là số chính phương (mod p) khi và chỉ khi $p = 4k + 1$

Chứng minh suy ra trực tiếp từ tiêu chuẩn trên.

Định lý Nếu p là số nguyên tố lẻ thì trong tập $S = \{1,2,...,p-1\}$ có $(p-1)/2$ số chính phương (modp) và $(p-1)/2$ số không chính phương (modp)

Chứng minh Với mỗi $i \in S_1 = \{1,2,...,(p-1)/2\}$ gọi $r_i \in S$ là số (duy nhất) mà $i^2 \equiv r_i \pmod{p}$. Ta thấy rằng $r_i \neq r_j$ nếu $i \neq j$. Thật vậy nếu $r_i = r_j \rightarrow i^2 - j^2 \equiv 0 \pmod{p} \rightarrow (i-j)(i+j) \equiv 0 \pmod{p}$. Nhưng điều này không xảy ra vì $i-j, i+j$ đều không chia hết cho p do $1 \leqslant |i-j| < i+j < p$. Vậy $|A| = (p-1)/2$.Ta chứng minh rằng A là tập tất cả các số chính phương (mod p) trong S. Thật vậy rõ ràng mỗi số thuộc A đều là số chính phương (mod p). Ngược lại giả sử $a \in S$ sao cho $a \equiv k^2 \pmod{p}$ với $k \in S$ .Nếu $k \in S_1$ thì $a = r_k \in A$.Nếu $k \notin S_1$ thì $h = p - k \in S_1$ và ta có $a \equiv h^2$ do đó $a = r_h \in A$.

Ta xét bài toán sau đây: Tìm tất cả các số nguyên tố p lẻ sao cho 2 là số chính phương(mod p).ư

Định lý Cho p là số nguyên tố lẻ. Gọi n là số các số chẵn nằm trong k
$(p/2;p)$. Khi đó

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

Chứng minh Giả sử $r_1, r_2, ..., r_n$ là tập tất cả các số chẵn trong khoảng $(p/2;p$
đó $p-r_1, p-r_2, ..., p-r_n$ là các số lẻ trong $(p/2;p)$. Giả sử $s_1, s_2, ..., r_m$ là tập
các số chẵn trong khoảng $(0;p/2)$. Ta có $m+n=(p-1)/2$ do có cả thảy $(p$
số chẵn trong khoảng $(0;p)$. Vì tập $A=\{s_1,...,s_m,p-r_1,...,p-r_n\} \subset (0$
$(p-1)/2$ số nên $A=\{1,2,...,(p-1)/2\}$.Vậy

$$s_1....s_m(p-r_1)...(p-r_n)=\left(\frac{p-1}{2}\right)! \Leftrightarrow s_1...s_m r_1...r_n \equiv (-1)^n \left(\frac{p-1}{2}\right)! \quad ($$

Nhưng

$$s_1...s_m r_1...r_n = 2^{(p-1)/2}\left(\frac{p-1}{2}\right)!.$$

Vậy suy ra

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

Hệ quả Cho $p=4k\pm 1$ là số nguyên tố lẻ. Khi đó

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

Từ đó suy ra 2 là số chính phương (mod p) khi và chỉ khi $p=8t\pm 1$

Chứng minh Giả sử $p=4k+1$. Tập tất cả các số chẵn trong khoảng (
$\{2i\}, i=1,...,2k$.Ta có $2i>p/2 \Leftrightarrow i>k+1/4 \Leftrightarrow i \geq k+1$. Vậy $n=k$. T
nếu $p=4k-1$ thì tập tất cả các số chẵn trong khoảng $(0,p)$ là $\{2i\}, i=1,...,2$
có $2i>p/2 \Leftrightarrow i>k-1/4 \Leftrightarrow i \geq k$. Vậy $n=k$. Từ đó suy ra $2^{(p-1)/2} \equiv 1$ (
khi và chỉ khi $k=2t \Leftrightarrow p=8t\pm 1$.

Sau đây là một áp dụng hay.

Ví dụ (Thi HSGQG 2004 bảng A) Ký hiệu $S(n)$ là tổng các chữ số của
giá trị nhỏ nhất của $S(n)$ khi n chạy trên các bội của 2003.

Giải Đặt $p=2003$. p là số nguyên tố. Rõ ràng $S(n)>1$ vì 10^k không
cho p . Giả sử tồn tại n là bội của p và $S(n)=2$. Suy ra tồn tại k để $10^$
(mod p). Chú ý rằng $2^{10}=1024 \equiv 10^7 \pmod{p}$ nên

$$(2^{5k})^2 = 2^{10k} \equiv 10^{7k} \equiv (10^k)^7 \equiv -1 \pmod{p}$$

Vậy -1 là số chính phương (mod p). Mâu thuẫn vì p không có dạng 4k+1.

Tiếp theo ta chứng minh tồn tại n là bội của 3 mà S(n)=3. Ta có

$$10^7 \equiv 2^{10} \rightarrow 2.10^{700} \equiv 2^{1001} = 2^{(p-1)/2} \equiv -1 \pmod{p}$$

vì $p \neq 8t\pm 1$. Vậy $n=2.10^{700}+1$ là bội của p và $S(n)=3$. Thành thử gi
nhất của $S(n)$ khi n chạy trên các bội của 2003 là 3.

Ta xét bài toán tiếp theo sau đây: Tìm tất cả các số nguyên tố p lẻ $(p,3)$
cho 3 là số chính phương(mod p)

Định lý Cho p là số nguyên tố lẻ $(p,3)=1$. Gọi n là số các số là bội củ
trong khoảng $(p/2;p)$. Khi đó

$$3^{(p-1)/2} \equiv (-1)^n \pmod{p}$$

Chứng minh Giả sử $r_1, r_2, ..., r_n$ là tập tất cả các số bội của 3 nằm trong khoảng $(p/2; p)$,$s_1, s_2, ..., s_m$ là tập tất cả các số bội của 3 nằm trong khoảng $(0; p/2)$ và$t_1, t_2, ..., t_h$ là tập tất cả các số bội của 3 nằm trong khoảng $(p; 3p/2)$. Ta có $m+n+h = (p-1)/2$. Thật vậy $m + n + h$ là số các bội của 3 nằm trong khoảng $(0; 3p/2)$ tức là số các số i với $3i < 3p/2 \Leftrightarrow 1 \leqslant i \leqslant (p-1)/2$. Xét tập $A = \{s_1, ..., s_m, p - r_1, ..., p - r_n, t_1 - p, ..., t_h - p\} \subset (0; p/2)$. Các số này phân biệt(vì nếu $s = p - r \to 3|r + s = p, s = t - p \to 3|t - s = p, p - r = t - p \to 3|t + r = 2p$ đều dẫn đến $3|p$). Vì $|A| = (p-1)/2$ nên $A = \{1, 2, ..., (p-1)/2\}$.Vậy

$$s_1....s_m(p - r_1)...(p - r_n)(t_1 - p)...(t_h - p) = \left(\frac{p-1}{2}\right)!$$

$$\Leftrightarrow s_1...s_m r_1...r_n t_1....t_h \equiv (-1)^n \left(\frac{p-1}{2}\right)! \pmod{p}$$

Nhưng

$$s_1...s_m r_1...r_n t_1...t_h = 3^{(p-1)/2} \left(\frac{p-1}{2}\right)!.$$

Vậy suy ra

$$3^{(p-1)/2} \equiv (-1)^n \pmod{p}$$

Hệ quả Cho $p = 6k \pm 1$ là số nguyên tố . Khi đó

$$3^{(p-1)/2} \equiv (-1)^k \pmod{p}$$

Từ đó suy ra 3 là số chính phương (mod p) khi và chỉ khi $p = 12t \pm 1$

Chứng minh Giả sử $p = 6k + 1$. Tập tất cả các số chia hết cho 3 trong khoảng $(0, p)$ là $\{3i\}, i = 1, ..., 2k$.Ta có $3i > p/2 \Leftrightarrow i > k + 1/6 \Leftrightarrow i \geq k + 1$. Vậy $n = k$. Tương tự nếu $pk - 1$ thì tập tất cả các số chia hết cho 3 trong khoảng $(0, p)$ là $\{3i\}, i = 1, ..., 2k - 1$.Ta có $3i > p/2 \Leftrightarrow i > k - 1/6 \Leftrightarrow i \geq k$. Vậy $n = k$. Từ đó suy ra $3^{(p-1)/2} \equiv 1 \pmod{p}$ khi và chỉ khi $k = 2t \Leftrightarrow p = 12t \pm 1$.

Ví dụ Tìm tất cả các số nguyên dương n sao cho $3^n - 1$ chia hết cho $2^n - 1$.

Giải Rõ ràng $n = 1$ thỏa mãn. Xét $n > 1$ và giả sử $3^n - 1$ chia hết cho $2^n - 1$. Nếu n chẵn thì $2^n - 1$ chia hết cho 3 nên $3^n - 1$ chia hết cho 3. Vô lý. Vậy n lẻ. Nếu p là một ước nguyên tố bất kỳ của $2^n - 1$ thì suy ra $3^n \equiv 1 \pmod{p} \to 3^{n+1} \equiv 3 \pmod{p}$. Vì $n + 1$ chẵn nên 3 là số chính phương (mod p).Theo định lý trên p có dạng $12t \pm 1$. Do mọi ước nguyên tố của $2^n - 1$ có dạng $12t \pm 1$ nên $2^n - 1$ có dạng đó. Nếu $2^n - 1 = 12t - 1 \to 2^n = 12t \to 2^n \equiv 0 \pmod{3}$. Mâu thuẫn. Nếu $2^n - 1 = 12t + 1 \to 2^n = 12t + 2 \to 2^{n-1} = 6t + 1$. Mâu thuẫn vì $6t + 1$ là số lẻ. Vậy $n = 1$ là số duy nhất thỏa mãn đề bài.

Ví dụ 1 Cho $p > 3$ là số nguyên tố có dạng $p = 3k + 1$. Chứng minh rằng $\Pi_{i=1}^{p}(i^2 + i + 1) \equiv 0 \pmod{p}$

Giải Đầu tiên ta chứng minh rằng nếu $p = 3k + 1$ thì -3 là số chính phương (mod p). Thật vậy k phải chẵn $k = 2l$ suy ra $p = 6l + 1$. Nếu $l = 2t \to p = 12t + 1 \to (p - 1)/2 = 6t$ là số chẵn nên (-1) là số chính phương (mod p) và 3 là số chính phương (mod p). Thành thử (-3)=(-1)3 là số chính phương (mod p). Nếu $l = 2t + 1 \to p = 12t + 7 \to (p - 1)/2 = 6t + 3$ là số lẻ nên (-1) là số không chính phương (mod p) và 3 cũng là số chính phương (mod p). Thành thử (-3)=(-1)3 là số chính phương (mod p). Do đó tồn tại $x \in \mathbb{N}$, x lẻ để $x^2 \equiv -3 \pmod{p}$. (Ta có thể giả sử x là số lẻ vì nếu x chẵn ta thay x bởi $x + p$). Giả sử

$x = 2k+1 \to (2k+1)^2+3 = 4(k^2+k+1) \equiv 0 \pmod p \to k^2+k+1$ $(\mathrm{mod}\ p)$. Giả sử $k \equiv i \pmod p$ với $1 \leqslant i \leqslant p$ ta có $i^2+i+1 \equiv 0 \pmod p$ $\Pi_{i=1}^{p}(i^2+i+1) \equiv 0 \pmod p$.

Chú ý: Kết hợp với kết quả ở ví dụ 2 trước đó ta thu được

$$\Pi_{i=1}^{p}(i^2+i+1) \equiv \begin{cases} 0 \pmod p & \text{nếu } p = 3k+1 \\ 3 \pmod p & \text{nếu } p = 3k+2 \\ 0 \pmod p & \text{nếu } p = 3 \end{cases}$$

Bây giờ ta xét bài toán tổng quát:

Cho q là một số nguyên tố. Tìm tất cả các số nguyên tố $p \neq q$ sao cho c chính phương (mod p). (Ta đã xét trường hợp $q = 2, 3$ ở trên.)

Để giải bài toán này ta cần các bổ đề sau

Bổ đề 1 Cho p là số nguyên tố lẻ, $a \in \mathbb{Z}$ sao cho $(a,p) = 1$.Xét dãy $(ka$ $1, 2, ..., (p-1)/2$. Giả sử

$$ka \equiv r_k \pmod p, 1 \leqslant r_k < p$$

Gọi n là số các r_k nằm trong $(p/2; p)$.Khi đó

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

Chứng minh Từ (4) nhân vế với vế ta được

$$\left(\frac{p-1}{2}\right)! a^{(p-1)/2} \equiv \Pi_{k=1}^{(p-1)/2} r_k \pmod p$$

Ký hiệu $A = \{r_k | r_k > p/2\}, B = \{r_k | r_k < p/2\}$. Ta có

$$\begin{aligned} \Pi_{k=1}^{(p-1)/2} r_k &= \Pi_{\{r_k \in A\}} r_k \Pi_{\{r_k \in B\}} r_k \\ &\equiv (-1)^n \Pi_{\{r_k \in A\}} (p - r_k) \Pi_{\{r_k \in B\}} r_k \pmod p \end{aligned}$$

Ta có với $r_k \in A$ thì $(p - r_k) \in (0; p/2)$. Thêm vào đó với $r_i \in A, r_j \in$ $(p - r_i) \neq r_j$. Thật vậy nếu $(p - r_i) = r_j \to r_i + r_j = p \to a(i +$ $(\mathrm{mod}\ p) \to i + j \equiv 0 \pmod p$. Điều này không thể vì $i + j < p$. N $\{(p - r_k) | r_k \in A\} \cup B = \{1, 2, ..., (p-1)/2\}$. Thành thử, từ (5) và (6) suy r

$$\left(\frac{p-1}{2}\right)! a^{(p-1)/2} \equiv (-1)^n \left(\frac{p-1}{2}\right)! \pmod p$$

suy ra

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

Bổ đề 2 Ký hiệu

$$S = \sum_{k=1}^{(p-1)/2} [\frac{ka}{p}]$$

Khi đó

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

Chứng minh Ta cần chứng minh $S - n$ là số chẵn. Ta có $ka = q_k p + r_k$. Suy ra $q_k = [\frac{ka}{p}]$. Vậy

$$\sum_{k=1}^{(p-1)/2} ka = pS + \sum_{k=1}^{(p-1)/2} r_k \tag{7}$$

Từ chứng minh bổ đề 1 ta có

$$\begin{aligned} L = \sum_{k=1}^{(p-1)/2} k &= \sum_{\{r_k \in B\}} r_k + \sum_{\{r_k \in A\}} (p - r_k) \\ &= \sum_{k=1}^{(p-1)/2} r_k + np - 2 \sum_{\{r_k \in A\}} r_k \end{aligned} \tag{8}$$

Từ (7) và (8) suy ra

$$La = pS + L - np + 2 \sum_{\{r_k \in A\}} r_k \to p(S - n) = L(a - 1) + 2 \sum_{\{r_k \in A\}} r_k$$

Vì $a - 1$ là số chẵn p lẻ nên suy ra $S - n$ chẵn.

Bổ đề 8 Cho p, q là hai số lẻ nguyên tố cùng nhau. Khi đó

$$\sum_{i=1}^{(p-1)/2} [\frac{iq}{p}] + \sum_{j=1}^{(q-1)/2} [\frac{jp}{q}] = (\frac{p-1}{2})(\frac{q-1}{2})$$

Chứng minh Gỉa sử $A = \{(i,j) | 1 \leqslant i \leqslant (p-1)/2; 1 \leqslant j \leqslant (q-1)/2\}$. Ta có

$$|A| = (\frac{p-1}{2})(\frac{q-1}{2})$$

Ta phân hoạch A thành các tập con

$$\begin{aligned} A_1 &= \{(i,j) | qi > pj\} \\ A_2 &= \{(i,j) | qi < pj\} \\ A_3 &= \{(i,j) | qi = pj\} \end{aligned}$$

Ta có $A_3 =$. Thật vậy $qi = pj \to p | i \to p \leqslant i$ không xảy ra. Ta có $A_1 = \bigcup_{i=1}^{(p-1)/2} A_{1i}$ ở đó $A_{1i} = \{(i,j) | j < qi/p\}$. Ta có $|A_{1i} = [\frac{iq}{p}]$ do đó

$$|A_1| = \sum_{i=1}^{(p-1)/2} [\frac{iq}{p}]$$

Tương tự

$$|A_2| = \sum_{j=1}^{(q-1)/2} [\frac{ip}{q}]$$

Vì $|A| = |A_1| + |A_2|$ nên bổ đề được chứng minh. Từ các bổ đề trên ta đi đến định lý sau đây được gọi là luật tương hỗ Gauss, một trong những thành tựu đẹp đẽ nhất của lý thuyết số.

Định lý (Luật tương hỗ Gauss).

Cho p, q là hai số nguyên tố lẻ phân biệt. Khi đó

1. Nếu có ít nhất một trong hai số có dạng 4k+1 thì p là số chính phương khi và chỉ khi q là số chính phương (mod p).

2. Nếu cả hai số có dạng 4k+3 thì p là số chính phương (mod q) khi và c là số không chính phương (mod p).

Chứng minh Giả sử có ít nhất một trong hai số có dạng 4k+1. Khi đó theo ta có

$$S_1 + S_2 = \sum_{i=1}^{(p-1)/2} [\frac{iq}{p}] + \sum_{j=1}^{(q-1)/2} [\frac{jp}{q}]$$

là một số chẵn do đó S_1, S_2 có cùng tính chẵn lẻ. Theo bổ đề 2 thì p là s phương(mod q) khi và chỉ khi S_2là số chẵn và q là số chính phương(mod p chỉ khi S_1là số chẵn . Vậy p là số chính phương (mod q) khi và chỉ khi q là phương (mod p).

Nếu cả hai số có dạng 4k+3 thì $S_1 + S_2$ lẻ do đó S_1 khác tính chẵn lẻ. có p là số chính phương (mod q) khi và chỉ khi q là số không chính phương

Ví dụ Tìm tất cả các số nguyên tố lẻ $p \neq 5$ sao cho 5 là số chính phương

Giải Vì 5 là số nguyên tố dạng 4k+1 nên theo luật tương hỗ 5 là số chính (mod p) khi và chỉ khi p là số chính phương (mod 5) tức là khi $p^{(5-1)/2} =$ (mod 5) $\Leftrightarrow p = 5t \pm 1$.

Ví dụ Tìm tất cả các số nguyên tố lẻ $p \neq 7$ sao cho 7 là số chính phương

Giải a)Nếu $p \equiv 1 \pmod 4$: Theo luật tương hỗ 7 là số chính phương khi và chỉ khi p là số chính phương (mod 7) tức là khi $p^{(7-1)/2} = p^3 \equiv 1$ (mo $p \equiv 1, 2, 4 \pmod 7$. Ta có

$$\begin{aligned} p &\equiv 1 \pmod 4, p \equiv 1 \pmod 7 \Leftrightarrow p \equiv 1 \pmod{28} \\ p &\equiv 1 \pmod 4, p \equiv 2 \pmod 7 \Leftrightarrow p \equiv 9 \pmod{28} \\ p &\equiv 1 \pmod 4, p \equiv 4 \pmod 7 \Leftrightarrow p \equiv 25 = -3 \pmod{28} \end{aligned}$$

b) Nếu $p \equiv -1 \pmod 4$: Theo luật tương hỗ 7 là số chính phương (mo và chỉ khi p là số không chính phương (mod 7) tức là khi $p^{(7-1)/2} = p^3$ (mod 7) $\Leftrightarrow p \equiv 3, 5, 6 \pmod 7$. Ta có

$$\begin{aligned} p &\equiv -1 \pmod 4, p \equiv -1 \pmod 7 \Leftrightarrow p \equiv -1 \pmod{28} \\ p &\equiv -1 \pmod 4, p \equiv 5 \pmod 7 \Leftrightarrow p \equiv 19 = -9 \pmod{28} \\ p &\equiv -1 \pmod 4, p \equiv 3 \pmod 7 \Leftrightarrow p \equiv 3 \pmod{28} \end{aligned}$$

Tóm lại 7 là số chính phương(mod p) khi và chỉ khi $p \equiv \pm 1, \pm 3, \pm 9 \pmod 2$

Ký hiệu Legendre Giả sử p là số nguyên tố lẻ, a là số nguyên không cho p. Ký hiệu Legendre $\left(\frac{a}{p}\right)$ được định nghĩa như sau

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{nếu } a \text{ là chính phương mod p} \\ -1 & \text{nếu } a \text{ là không chính phương mod p} \end{cases}$$

Với ký hiệu này ta có thể phát biểu các định lý trước một cách ngắn gọn nh

Định lý Giả sử p là số nguyên tố lẻ, a là số nguyên không chia hết cho

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

2. Nếu $a \equiv b \pmod{p}$ thì $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

3. $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$

4. $\left(\frac{a^2}{p}\right) = 1$

5. $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$

6. $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$

7. (Luật tương hỗ) Nếu $a = q$ là số nguyên tố lẻ thì
$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4}$$

Ví dụ Cho biết 1009 là số nguyên tố. Hỏi 713 có phải là số chính phương mod 1009 hay không?

Ta có 713=23.31. Do đó $\left(\frac{713}{1009}\right) = \left(\frac{23}{1009}\right)\left(\frac{31}{1009}\right)$ Vì $1009 = 4k+1$ nên $\left(\frac{23}{1009}\right) = \left(\frac{1009}{23}\right)$ Ta có $1009 \equiv 20 \pmod{2}3$ nên $\left(\frac{1009}{23}\right) = \left(\frac{20}{23}\right) =$.Vì $20 = 2^2.5$ nên ta có $\left(\frac{20}{23}\right) = \left(\frac{5}{23}\right) =$. Do 23 có dạng 5t+3 nên $\left(\frac{5}{23}\right) = -1 \Leftrightarrow \left(\frac{23}{1009}\right) = -1$.

Lại có $\left(\frac{31}{1009}\right) = \left(\frac{1009}{31}\right) = \left(\frac{17}{31}\right) = \left(\frac{31}{17}\right)\left(\frac{14}{17}\right) = \left(\frac{2}{17}\right)\left(\frac{7}{17}\right) = \left(\frac{17}{7}\right) = \left(\frac{3}{7}\right) = -1$.(Ta áp dụng các tiêu chuẩn để 2 và 3 là số chính phương p(mod p) do 17=8k+1 và $7 \neq 12k \pm 1$). Tóm lại $\left(\frac{713}{1009}\right) = 1$ do đó 713 là số chính phương mod 1009.

Bây giờ ta đề cập tới trường hợp số chính phương n với n là hợp số.

Trường hợp n là hợp số Giả sử n có phân tích tiêu chuẩn
$$n = \Pi_{i=1}^{k} p_i^{s_i}$$

Bổ đề Số nguyên a với $(a, n) = 1$ là số chính phương (mod p) khi và chỉ khi với mỗi p_i a là số chính phương (mod $p_i^{s_i}$).

Chứng minh Giả sử a là số chính phương(mod n). Khi đó tồn tại $x \in \mathbb{N}$ sao cho $x^2 \equiv a \pmod{n} \rightarrow x^2 \equiv a \pmod{p_i^{s_i}}$. Vậy a là số chính phương (mod $p_i^{s_i}$). Đảo lại giả sử với mỗi $i = 1, 2, ..., k$ a là số chính phương (mod $p_i^{s_i}$). Khi đó tồn tại $x \in \mathbb{N}$ sao cho $x_i^2 \equiv a \pmod{p_i^{s_i}}$. Theo định lý thặng dư Trung hoa tồn tại $x \in \mathbb{N}$ sao cho $x \equiv x_i \pmod{p_i^{s_i}}$ với mỗi $i = 1, 2, ..., k$. Thành thử $x^2 \equiv x_i^2 \equiv a \pmod{p_i^{s_i}}$. Suy ra $x^2 \equiv a \pmod{n}$. Vậy a là số chính phương mod n.

Vậy bài toán quy về xét các hợp số n có dạng lũy thừa của một số nguyên tố.

Định lý Giả sử $n = 2^s, s > 1$. và a là số lẻ. Khi đó a là số chính phương (mod n) khi và chỉ khi: i) $a \equiv 1 \pmod{4}$ nếu s=2.

ii) $a \equiv 1 \pmod{8}$ nếu $s \geq 3$.

Chứng minh i)Với s=2 tức là n=4. Nếu tồn tại $x \in \mathbb{N}$ sao cho $x^2 \equiv a \pmod{4} \rightarrow a \equiv 1 \pmod{4}$ vì với mọi số lẻ x $x^2 \equiv 1 \pmod{4}$. Đảo lại nếu $a \equiv 1 \pmod{4} \Leftrightarrow a \equiv 1^2 \pmod{n}$. Vậy a là số chính phương mod n.

ii) Với $s \geq 3$.Nếu tồn tại $x \in \mathbb{N}$ sao cho $a \equiv x^2 \pmod{n} \rightarrow a \equiv$ (mod 8) .Vì với mọi số lẻ x $x^2 \equiv 1 \pmod 8$ nên $a \equiv 1 \pmod 8$. Đảo $a \equiv 1 \pmod 8$ tức là $a = 8t + 1$. Với $s = 3 \Leftrightarrow n = 8$ thì hiển nhiên a là phương (mod 8). Xét $s > 3$.Như ví dụ 1 đã chỉ ra tồn tại hệ đầy đủ (mod 2^{s-3} số tam giác tức là tồn tại $k \in \mathbb{N}$ sao cho $k(k+1)/2 \equiv t \pmod{2^{s-3}} \rightarrow 4k(k$ $(\text{mod } n) \rightarrow (2k+1)^2 \equiv 8t + 1 = a \pmod n$.Vậy a là số chính phương m

Định lý Giả sử $n = p^s$ với p là số nguyên tố lẻ. Khi đó a là số chín mod n khi và chỉ khi a là số chính phương mod p.

Chứng minh Hiển nhiên nếu a là số chính phương mod n thì a là phương mod p. Giả sử a là số chính phương mod p. Ta chứng minh bằng khẳng định sau: Với mỗi k tồn tại $x_k \in \mathbb{N}$ sao cho $x_k^2 \equiv a \pmod{p^k}$. Với k định đúng vì a là số chính phương mod p. Giả sử đúng với k tức là tồn tại x $x_k^2 = a + tp^k$ với $t \in \mathbb{Z}$. Đặt $x_{k+1} = x_k + hp^k$ với h là số nguyên dương $2hx_k \equiv -t \pmod p$. Số h này tồn tại vì $(p, 2x_k) = 1$. Vậy

$$\begin{aligned} x_{k+1}^2 &= x_k^2 + 2hx_kp^k + p^{2k} \\ &= a + (2hx_k + t)p^k + p^{2k} \\ &\equiv a \pmod{p^{k+1}} \end{aligned}$$

bởi vì $2hx_k + t$ chia hết cho p và $2k \geq k+1$. Nói riêng tồn tại x_s để $x_s^2 \equiv a$ hay a là số chính phương(mod n).

Ký hiệu Jacobi Ký hiệu Jacobi là sự mở rộng của ký hiệu Lagendre là một số nguyên dương lẻ với phân tích tiêu chuẩn $n = \Pi_{i=1}^k p_i$. (Các p_i có nhau). Với $(a, n) = 1$ ta định nghĩa ký hiệu Jacobi như sau

$$\left(\frac{a}{n}\right) = \Pi_{i=1}^k \left(\frac{a}{p_i}\right)$$

Dễ thấy rằng nếu a là số chính phương mod n thì $\left(\frac{a}{p_i}\right) = 1 \quad \forall i \rightarrow \left(\frac{a}{n}\right) =$ ngược lại không đúng. Chẳng hạn $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1$ nhưng là số chính phương mod 15 vì 2 là không là chính phương mod 3. Tuy nhiê Jacobi cũng có đầy đủ các tính chất như ký hiệu Lagendre. Cụ thể

Định lý Giả sử n là số nguyên lẻ, a là số nguyên với $(a, n) = 1$.

1. Nếu $a \equiv b \pmod n$ thì $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$
2. $\left(\frac{a}{n}\right)\left(\frac{b}{n}\right) = \left(\frac{ab}{n}\right)$
3. $\left(\frac{a^2}{n}\right) = 1$
4. $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$
5. $\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$
6. (Luật tương hỗ) Nếu n, m là các số nguyên lẻ nguyên tố cùng nhau

$$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = (-1)^{(n-1)(m-1)/4}$$

Ví dụ Cho m, n là các số nguyên dương sao cho $n+1$ chia hết cho $4m$. Chứng minh rằng $-m$ là số không chính phương (mod n).

Giải Giả sử $-m$ là số chính phương mod n. Suy ra $\left(\frac{-m}{n}\right) = 1 \rightarrow \left(\frac{m}{n}\right)\left(\frac{-1}{n}\right) = 1 \rightarrow \left(\frac{m}{n}\right) = -1$ vì theo giả thiết $n = 4km - 1$ nên $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2} = -1$. Giả sử $m = 2^s b$ với b lẻ. Ta có

$$-1 = \left(\frac{m}{n}\right) = \left(\frac{2^s}{n}\right)\left(\frac{b}{n}\right) \tag{9}$$

a) Ta chứng minh $\left(\frac{2^s}{n}\right) = 1$. Nếu s chẵn thì hiển nhiên. Nếu s lẻ suy ra $m = 2l \rightarrow n = 4km - 1 = 8l - 1 \rightarrow \left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8} = 1 \rightarrow \left(\frac{2^s}{n}\right) = 1$. b)Ta chứng minh $\left(\frac{b}{n}\right) = 1$. Ta có theo luật tương hỗ

$$\left(\frac{b}{n}\right) = (-1)^{\left(\frac{n-1}{2}\right)\left(\frac{n-1}{2}\right)}\left(\frac{n}{b}\right) = (-1)^{(b-1)/2}\left(\frac{n}{b}\right)$$

do $(n-1)/2$ lẻ. Lại có do $n \equiv -1 \pmod{b} \rightarrow \left(\frac{n}{b}\right) = \left(\frac{-1}{b}\right) = (-1)^{(b-1)/2}$ .Vậy

$$\left(\frac{b}{n}\right) = (-1)^{b-1} = 1$$

do $b-1$ chẵn.

Từ a) và b) ta có $\left(\frac{m}{n}\right) = 1$ mâu thuẫn vớiư (6).

Ví dụ Chứng minh rằng phương trình $4xyz = x+y+t^2$ không có nghiệm nguyên dương.

Giải

$$4xyz = x + y + t^2 \rightarrow 16xyz = 4x + 4y + 4t^2$$
$$16xyz^2 = 4xz + 4yz + 4zt^2 \Leftrightarrow$$
$$4zt^2 + 1 = (4xz - 1)(4yz - 1) \Leftrightarrow (2zt)^2 \equiv -z \pmod{n}$$

ở đó $n = 4yz - 1$. Ta có $n+1$ chia hết cho $4z$ và $-z$ là số chính phương mod n. Trái với ví dụ 2.

Cấp của một số Cho số nguyên dương n. Nếu a là một số nguyên với $(a, n) = 1$ thì luôn tồn tại số nguyên dương k để $a^k \equiv 1 \pmod{n}$ (chẳng hạn $k = \phi n$).

Số nguyên dương k bé nhất thỏa mãn $a^k \equiv 1 \pmod{n}$ được gọi là cấp của a(mod n).

Định lý i) Giả sử cấp của a mod n là h. Khi đó $a^k \equiv 1 \pmod{n}$ khi và chỉ khi k chia hết cho h.

ii) Nếu a có cấp h (mod n), b có cấp l (mod n) và $(h, l) = 1$ thì ab có cấp hl (mod n).

iii) Cho các số $n_1, n_2, ..., n_k$ đôi một nguyên tố cùng nhau và $n = n_1...n_k$ Giả sử với mỗi i , h_i là cấp của a (mod p_i). Khi đó cấp của a (mod n) là h=BCNN $[h_1, h_2, .., h_k]$.

Chứng minh i) Giả sử $a^k \equiv 1 \pmod{n}$. Nếu $k = qh + r, 1 \leqslant r < h$ thì $a^k = a^r(a^h)^q \equiv a^r \pmod{n}$ do đó $a^r \equiv 1 \pmod{n}$. Điều này trái với cách chọn h. Vậy $r = 0$ hay k chia hết cho h. Điều ngược lại là hiển nhiên.

ii) Giả sử t là cấp của ab mod n. Ta có $(ab)^{hl} = a^{hl}b^{hl} \equiv 1 \pmod{n}$ nên
hết cho t. Ta có $1 \equiv (ab)^{th} = a^{th}b^{th} \equiv b^{th} \pmod{n}$. Suy ra th chia hết ch
$(h,l) = 1$ nên t chia hết cho h. Tương tự t chia hết cho l. Vì $(h,l) = 1$ nê
hết cho hl. Vậy $t = hl$.

iii) Gọi h là cấp của a (mod n) . Ta có $a^h \equiv 1 \pmod{n_i} \rightarrow h_i|h$ Vậy h
chung của $h_1, ..., h_n$. Nếu l là một bội chung bất kỳ của của $h_1, ..., h_n$ thì
$\pmod{n_i} \rightarrow a^l \equiv 1 \pmod{n} \rightarrow h|l$. Vậy h =BCNN $[h_1, h_2, .., h_k]$.

Từ iii) của định lý trên ta thấy rằng bài toán tìm cấp của a (mod n) quy
toán tìm cấp của a (mod p^s) với p là số nguyên tố.

Định lý Cho a là số lẻ và $n = 2^s$. Giả sử $a - 1 = 2^u b$ và $a^2 - 1 = 2^v c$ t
$1 \leqslant u < v, b, c$ là số lẻ. Gọi h là cấp của a (mod n). Khi đó

$$h = \begin{cases} 1 & \text{nếu } u \geq s \\ 2 & \text{nếu } u < s \leqslant v \\ 2^{s+1-v} & \text{nếu } s > v \end{cases}$$

Chứng minh Ta có $h|\phi(2^s) \rightarrow h = 2^t, t \leqslant s - 1$. Rõ ràng nếu $u \geq s$ thì $a -$
hết cho n do đó $h = 1$. Nếu $s > u$ thì $h \geq 2 \rightarrow t \geq 1$ Ta có

$$a^h - 1 = (a^2 - 1)(a^4 + 1)...(a^{2^{t-1}} + 1)$$

Nếu $u < s \leq v$ thì $n|a^2 - 1 \rightarrow h = 2$. Nếu $s > v$ thì từ đẳng thức ( ) suy ra

$$a^h - 1 = 2^{v+t-1}$$

Nó chia hết cho 2^s khi và chỉ khi $v + t - 1 \geq s \rightarrow t \geq s + 1 - v \geq 2$. Vậy t
là $t = s + 1 - v$.

Định lý Cho p là số nguyên tố lẻ $(a,p) = 1$ và $n = p^s$. Giả sử r là
a(mod p) và $a^r - 1 = p^u q, (q,p) = 1$. Gọi h là cấp của a (mod n). Khi đó

$$h = \begin{cases} r & \text{nếu } u \geq s \\ rp^{s-u} & \text{nếu } u < s \end{cases}$$

Chứng minh Đầu tiên xét trường hợp $r = 1$. Rõ ràng nếu $u \geq s$ thì $h = 1$. Xé
. Giả sử $h = p^t q, (q,p) = 1$. Nếu $q > 1$ thì do $a \equiv 1 \pmod{p}$ nên $a^h - 1 = (a$
với $(b,p) = 1$. Vậy $a^{p^t} - 1 \equiv 1 \pmod{n}$ trái giả thiết h là bé nhất. Vậy $h = p$
. Ta có bổ đề

Bổ đề Với mọi $n \in \mathbb{N}$

$$a^{p^n} - 1 = p^{n+u}A, (A,p) = 1$$

Chứng minh quy nạp theo n. Với $n = 0$ đúng. Giả sử đúng với n. Đặt $b = a^p$

$$a^{p^{n+1}} - 1 = b^p - 1 = (b-1)(b^{p-1} + \cdots + 1) = (a^{p^n} - 1)B$$

Vì $a \equiv 1 \pmod{p}$ và p lẻ nên dễ thấy B chỉ chia hết cho p mà không chia
p^2. Do đó $a^{p^{n+1}} - 1 = p^{n+u+1}A, (A,p) = 1$.Bổ đề được chứng minh.

Theo bổ đề ta có $a^h - 1 = p^{t+u}A, (A,p) = 1$.Vậy $t + u \geq s \rightarrow t \geq s -$
Vậy t bé nhất là $t = s - u \Leftrightarrow h = p^{s-u}$.

Trở lại trường hợp r bất kỳ. Khi đó $a^h \equiv 1 \pmod{n} \to a^h \equiv 1 \pmod{p} \to h = lr$. Đặt $b = a^r$. Vì $a^h = b^l$ dễ thấy cấp của b(mod p) là 1 và l là cấp của b (mod n). Vậy theo trường hợp đặc biệt $r = 1$ áp dụng đối với b ta có

$$l = \begin{cases} 1 & \text{nếu } u \geq s \\ p^{s-u} & \text{nếu } u < s \end{cases}$$

Vậy $h = rl$. Định lý được chứng minh.

Tóm lại việc tìm cấp của một số theo mod n được quy hoàn toàn về tìm cấp theo modun nguyên tố.

Ví dụ Xét số Fecma $F = F_n = 2^{2^n} + 1, n \geq 1$. Chứng minh rằng F là số nguyên tố khi và chỉ khi

$$3^{(F-1)/2} + 1$$

chia hết cho F.

Giải Dễ thấy F không có dạng $12k \pm 1$. Do dó nếu F là số nguyên tố thì 3 là số không chính phương (mod F). Vậy $3^{(F-1)/2} \equiv -1 \pmod{F}$ tức là $3^{(F-1)/2} + 1$ chia hết cho F.

Đảo lại giả sử

$$3^{(F-1)/2} \equiv -1 \pmod{F}. \tag{11}$$

Từ (11) suy ra $3^{F-1} \equiv 1 \pmod{F}$. Gọi h là cấp của 3 (mod F). Khi đó $h|F-1 = 2^{2^n}$. Vậy $h = 2^t, t \leqslant 2^n$. Nếu $t \leqslant 2^n - 1$ thì $h|(F-1)/2$ do đó $3^{(F-1)/2} \equiv 1 \pmod{F}$ mâu thuẫn với (11). Vậy $t = 2^n \Leftrightarrow h = F - 1$. Vì $h|\phi(F)$ nên $F - 1|\phi(F) \to F - 1 = \phi(F)$. Vậy F là số nguyên tố.

Phương trình đồng dư Cho $f(x)$ là một đa thức hệ số nguyên và m là một số nguyên dương. Số nguyên a được gọi là nghiệm của phương trình đồng dư

$$f(x) \equiv 0 \pmod{m} \tag{12}$$

nếu $f(a) \equiv 0 \pmod{m}$.

. Rõ ràng nếu a là nghiệm của (12) thì với mọi $b \equiv a \pmod{m}$ b cũng là nghiệm của (12). Do đó hai nghiệm đồng dư (mod m) được đồng nhất với nhau. Nói cách khác ta chỉ xét các nghiệm phân biệt (mod m).

Giống như với phương trình đại số ta quan tâm đến số nghiệm của một phương trình đồng dư.

Định lý Cho đa thức $f(x) = a_n x^n + \cdots + a_1 x + a_0$ hệ số nguyên . Xét phương trình đồng dư

$$f(x) \equiv 0 \pmod{p} \tag{13}$$

trong đó $m = p$ là một số nguyên tố. Nếu phương trình (13) có $n + 1$ nghiệm phân biệt (mod p) thì mọi hệ số $a_i (i = 0, 1, 2, ..., n)$ đều chia hết cho p. Nói riêng khi đó $f(a) \equiv 0 \pmod{p} \forall a \in \mathbb{Z}$

Chứng minh Chứng minh quy nạp theo n. Với $n = 1$ khẳng định đúng. Thật vậy giả sử $a_1 x_1 + a_0 \equiv 0 \pmod{p}, a_1 x_2 + a_0 \equiv 0 \pmod{p}$ và $x_1 \equiv x_2 \pmod{p}$. Trừ hai vế suy ra $a_1(x_1 - x_2) \equiv 0 \pmod{p} \to a_1 \equiv 0 \pmod{p} \to a_0 \equiv 0 \pmod{p}$.

Giả sử khẳng định đúng với mọi đa thức bậc $k < n$.Giả sử phương trình (13) có $n + 1$ nghiệm phân biệt $x_1, ..., x_{n+1}$ (mod p). Xét đa thức $g(x) = f(x) - a_n(x -$

$x_1)...(x-x_n)$. Ta có $\deg(g) < n$ và $g(x)$ có n nghiệm phân biệt $x_1,..,x$ giả thiết quy nạp suy ra $f(a) \equiv 0 \pmod p \forall a \in \mathbb{Z} \to f(x_{n+1}) \equiv 0$ (mc $a_n(x_{n+1}-x_1)...(x_{n+1}-x_n) \equiv 0 \pmod p \to a_n \equiv 0 \pmod p$. Xét đa thức $f(x) - a_n x^n = a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. Ta có $\deg(h) < n$ và $h(x)$ có n phân biệt $x_1,..,x_n$ Theo giả thiết quy nạp suy ra tất cả các hệ số $a_{n-1},...,a_0$ hết cho p. Định lý được chứng minh.

Phương trình (13) được gọi là có bậc n (mod p) nếu hệ số cao nhất a_n kh hết cho p. Từ định lý trên ta suy ra phương trình đồng dư bậc n (mod p) nhất n nghiệm phân biệt (mod p).

Chú ý Định lý trên không dúng nếu m là hợp số. Thí dụ xét phươ $x^2 - 1 \equiv 0 \pmod 8$ ta có 4 số $1,3,5,7$ đều là nghiệm phân biệt (mod 8).

Ví dụ Cho p là số nguyên tố lẻ và $k|p-1$. Khi đó phương trình $x^k \pmod p$ có đúng k nghiệm phân biệt.

Giải Vì $k|p-1$ nên dễ thấy $x^{p-1}-1 = (x^k-1)G(x)$ ở đó $G(x)$ là đa tl nguyên với h=deq Q = p-1-k .Gọi $A \subset S = \{1,2,...,p-1\}, B \subset S = \{1,2,$ tương ứng là nghiệm của $x^{p-1}-1 \equiv 0 \pmod p, Q(x) \equiv 0 \pmod p$ thì ta có $S \to |A| + |B| \geq p-1$ mà $|A| \leqslant k, |B| \leqslant p-1-k$ nên dấu bằng xảy ra.

Ví dụ Cho p là số nguyên tố lẻ. Với mỗi k nguyên dương,ký hiệu $S(k) =$ Tìm tất cả các k để S_k chia hết cho p.

Giải Nếu k chia hết cho $p-1$ thì $i^k \equiv 1 \pmod p \to S_k \equiv p-1$ (mc k không chia hết cho p giả sử $k = (p-1)l + h, 1 \leqslant h < p-1$. Khi đ $\pmod p \to S(k) \equiv S(h) \pmod p$.Xét phương trình $x^h - 1 \equiv 0$ (mo $h < p-1$ nên theo định lý trên tồn tại $a \in \{1,2,...,p-1\}$ sao cho $a^h \pmod p$. Tập $\{ai\}, i = 1,2,...,p-1$ là hệ thặng dư thu gọn (mod p) nên

$$S(h) \equiv \sum_{i=1}^{p-1}(ai)^h = a^h S(h) \pmod p \to S(h)(a^h-1) \equiv 0 \pmod$$

Vì $a^h - 1 \equiv 0 \pmod p$ nên $S(h) \equiv 0 \pmod p \to S(k) \equiv 0 \pmod p$

Tóm lại S_k chia hết cho p khi và chỉ khi k không chia hết cho $p-1$.

Định lý Giả sử $m = m_1...m_k$ và các số (m_i) đôi một nguyên tố cùng đó:

i) a là nghiệm của (13) khi và chỉ khi với mọi $i = 1,2,...,k$, a là n phương trình

$$f(x) \equiv 0 \pmod{m_i}$$

ii) Ký hiệu $N(m), N(m_i)$ tương ứng là số nghiệm phân biệt (mod m) của nghiệm phân biệt (mod m_i) của (14) thì ta có

$$N(m) = N(m_1)...N(m_k)$$

Chứng minh i) Khẳng định là hiển nhiên do giả thiết các số (m_i) đôi n tố cùng nhau.

ii)Ký hiệu A, C_i tương ứng là tập hợp các số nguyên dương trong đoạ nghiệm của phương trình (13) và tập hợp các số nguyên dương trong đoạ nghiệm của phương trình (14) và $C = C_1 \times C_2.. \times C_k$. Ta có $|C| = |C$ $N(m_1)...N(m_k)$. Ta sẽ chứng minh $|C| = |A|$. Nếu $a \in A$ là nghiệm của

mỗi i a là nghiệm của (14). Vậy có duy nhất $a_i \in [1; m_i]$ để $a \equiv a_i \pmod{m_i}$. Ta có một ánh xạ $T : A \to C$ xác định bởi $a \mapsto (a_1, .., a_k)$ trong đó $a \equiv a_i \pmod{m_i}$. Ta có T là đơn ánh. Thật vậy nếu $T(a) = T(b) \to a \equiv b \pmod{m_i} \forall i \to a \equiv b \pmod{m} \to a = b$. Ta chứng minh T là song ánh. Giả sử $(a_1, .., a_k) \in C$. Theo định lý Trung hoa tồn tại $a \in A$ sao cho $a \equiv a_i \pmod{m_i}, \forall i \to f(a) \equiv 0 \pmod{m_i}$.Theo phần i) ta có $a \in A$. Hiển nhiên $T(a) = (a_1, .., a_k)$

Chứng minh định lý trên cũng cho ta phương pháp tìm tập nghiệm của phương trình (13) dựa trên các tập nghiệm C_i của phương trình (14) .

Ví dụ Giải phương trình $f(x) = x^4 + 2x^3 + 8x + 9 \equiv 0 \pmod{35}$

Giải Phương trình $f(x) \equiv 0 \pmod{5}$ có tập nghiệm là $C_1 = \{1; 4\}$. Phương trình $f(x) \equiv 0 \pmod{7}$ có tập nghiệm là $C_2 = \{3; 5; 6\}$.

Ta phải giải hệ

$$\begin{cases} a & \equiv a_1 \pmod{5} \\ a & \equiv a_2 \pmod{7} \end{cases}$$

ở đó $a_1 \in C_1, a_2 \in C_2$.

Từ định lý thặng dư Trung hoa ta tìm được $a \equiv 21a_1 + 15a_2 \pmod{35}$. Từ đó lần lượt cho $a_1 \in C_1, a_2 \in C_2$ ta tìm được

$$A = \{6; 19; 24; 26; 31; 34\}$$

Nhận xét Định lý trên cho ta thấy việc nghiên cứu phương trình đồng dư với modun bất kỳ được quy về việc nghiên cứu phương trình đồng dư với modun là lũy thừa của số nguyên tố.

Ví dụ Cho phương trình

$$ax - b \equiv 0 \pmod{m} \tag{15}$$

i)Phương trình (15) có nghiệm khi và chỉ khi $d|b$ ở đó $d = (a, m)$.

ii)Nếu $d|b$ thì phương trình (15) có d nghiệm phân biệt.

Giải Giả sử (15) có nghiệm. Khi đó tồn tại $x, y \in \mathbb{Z}$ sao cho $ax - b = my \to d|b$. Ngược lại giả sử $d|b$. Ta có $a = da_1, m = dm_1, b = db_1$ và $(a_1, m_1) = 1$. Khi đó vì $(a_1, m_1) = 1$ nên tồn tại x để $a_1 x \equiv b_1 \pmod{m_1} \to da_1 x \equiv db_1 \pmod{dm_1} \to ax - b \equiv 0 \pmod{m}$.

ii) Giả sử x_0 là một nghiệm của (15). Khi đó $a_1 x_0 \equiv b_1 \pmod{m_1}$. Đặt $x_k = x_0 + km_1 (k = 0, 1, ..., d-1)$. Khi đó $a_1 x_k = a_1 x_0 + ka_1 m_1 \equiv a_1 x_0 \equiv b_1 \pmod{m_1}$. Vậy x_k là nghiệm của (15). Các nghiệm này phân biệt (mod m). Thật vậy $x_i \equiv x_j \pmod{m} \Leftrightarrow im_1 \equiv jm_1 \pmod{m} \Leftrightarrow i \equiv j \pmod{d} \to i = j$. Nếu x là một nghiệm bất kỳ thì $a_1 x \equiv b_1 \pmod{m_1} \to a_1(x - x_0) \equiv 0 \pmod{m_1} \to x = x_0 + lm_1 = x_0 + (k + td)m_1 = x_k + tm \to x \equiv x_k \pmod{m}$ **Ví dụ** Chứng minh rằng với mọi $n \geq 5$, phương trình

$$P(x) = x^3 + 153x^2 - 111x + 38 \equiv 0 \pmod{3^n}. \tag{16}$$

phương trình có đúng 9 nghiệm phân biệt .

Giải Trước hết ta chứng minh nhận xét 1: Nếu $a \equiv 1 \pmod{9}, a' = a + 3^{n-2}b$ thì

$$P(a') \equiv P(a) + 3^n bh \pmod{3^{n+1}}$$

với $(h, 3) = 1$.

Thật vậy dễ thấy do $3n-6, 2n-3, 2n-4 \geq n+1$ nên

$$P(a') \equiv P(a) + 3^{n-1}(a^2 + 102a - 37)$$

Vì $a^2 + 102a - 37 \equiv 66 \equiv 3 \pmod 9$ suy ra $a^2 + 102a - 37 = 3h$ với (h
Thay vào ta có điều phải chứng minh.

Bước 1:Phương trình (16) có ít nhất một nghiệm a và $a \equiv 1 \pmod 9$
minh bằng quy nạp. Với $n = 5$ có nghiệm $a = 19$. Giả sử khẳng định đúng
là tồn tại a_n với $P(a_n) \equiv 0 \pmod{3^n}$. Đặt $P(a_n) = 3^n v$. Đặt $a_{n+1} = a_n$
Ta sẽ tìm b để $P(a_{n+1}) \equiv 0 \pmod{3^{n+1}}$. Theo nhận xét 1

$$\begin{aligned} P(a_{n+1}) &\equiv P(a) + 3^n bh \pmod{3^{n+1}} \\ &\equiv 3^n(v + bh) \pmod{3^{n+1}} \end{aligned}$$

Vì $(b, h) = 1$ nên chọn được b để $v + bh$ chia hết cho 3 do đó $P(a_n$
$\pmod{3^{n+1}}$. Thêm vào đó $a_{n+1} \equiv a_n \equiv 1 \pmod 9$.

Bước 2: Phương trình (16) có ít nhất 9 nghiệm phân biệt. Theo bước
trình (16) có ít nhất một nghiệm a và $a \equiv 1 \pmod 9$. Đặt

$$a_k = a + 3^{n-2}k (k = 0, 1, 2, ..., 8)$$

Từ nhận xét 1 ta có $P(a_k) \equiv P(a) + 3^n bh \pmod{3^{n+1}} \rightarrow P(a_k) \equiv$
$\pmod{3^n}$ Ta có nếu $a_i \equiv a_j \pmod{3^n} \rightarrow i \equiv j \pmod 9 \rightarrow i = j$. Vậy
này phân biệt.

Bước 4: Trước hết bằng quy nạp ta chứng minh nếu nhận xét 2: Nếu $P(a$
$\pmod{3^n}$ thì $a \equiv a' \pmod{3^{n-2}}$. Với n=5 ta kiểm tra được nhận xét
sử đúng với n. Nếu $P(a) \equiv P(a') \pmod{3^{n+1}} \rightarrow P(a) \equiv P(a')$ (m
$a' = a + 3^{n-2}b$ theo giả thiết quy nạp. Theo nhận xét 1 $P(a') \equiv P($
$\pmod{3^{n+1}} \rightarrow 3|bh \rightarrow 3|b \rightarrow a' \equiv a \pmod{3^{n-1}}$. Nhận xét 2 được chứng

Giả sử a' là một nghiệm bất kỳ của (16). Theo nhận xét 2 $a' = a + 3^{n-}$
Giả sử $h = 9l + k (k = 0, 1, ..., 8)$ Suy ra $a' \equiv a + 3^{n-2}k = a_k \pmod{3^n}$. V
trình (16) có đúng 9 nghiệm phân biệt.

Ví dụ Cho p là số nguyên tố lẻ. Chứng minh rằng với mọi $n \geq 1$ phư

$$x^{p-1} - 1 \equiv 0 \pmod{p^n}$$

có đúng $p - 1$ nghiệm phân biệt.

Giải Chứng minh bằng quy nạp theo n. Với $n = 1$ khẳng định đúr
khẳng định đúng với n.Xét phương trình

$$x^{p-1} - 1 \equiv 0 \pmod{p^{n+1}}$$

Giả sử $\{a_1, ..., a_{p-1}\}$ là $p-1$ nghiệm của (17). Ta có $a_i^{p-1} - 1 = p^n h_i$.Với n
duy nhất $t_i \in \{1, 2, .., p\}$ thỏa mãn $(p-1)a_i t + h_i \equiv 0 \pmod p$ vì $(p-1)a_i$
hết cho p. Đặt $b_i = a_i + t_i p^n$. Ta có $b_i^{p-1} - 1 = (a_i + t_i p^n)^{p-1} \equiv a_i^{p-1} - 1 + ($
$\pmod{p^{n+1}}$ Ta có $a_i^{p-1} - 1 + (p-1)a_i t_i p^n = p^n(h + (p-1)a_i t_i) \equiv 0$ (
Do vậy b_i là nghiệm của (18). Đảo lại nếu $b_i \equiv b_j \pmod{p^{n+1}}$ –
$\pmod{p^n} \rightarrow i = j$. Vậy phương trình có ít nhất 9 nghiệm. Bây giờ giả sử

bất kỳ của (18). Khi đó b cũng là nghiệm của (17). Vậy tồn tại a_i, t để $b = a_i + tp^n$. Ta có $b^{p-1} - 1 = (a_i + tp^n)^{p-1} \equiv a_i^{p-1} - 1 + (p-1)a_i tp^n \equiv 0 \pmod{p^{n+1}}$. Suy ra $(p-1)a_i tp^n + h_i$ chia hết cho p. Vậy $t \equiv t_i \pmod p \rightarrow t = t_i + pl \rightarrow b = a_i + t_i p^n + lp^{n+1} \rightarrow b \equiv a_i \pmod{p^{n+1}}$.

Vậy phương trình (18) có đúng p-1 nghiệm là $b_1, ..., b_{p-1}$

Sau đây là một vài ứng dụng của phương trình đồng dư.

Định lý Cho p là một số nguyên tố lẻ. Số nguyên dương h là cấp của một số a (mod p) khi và chỉ khi h là ước của $p-1$.

Chứng minh Ta chỉ cần chứng minh : nếu $h|p-1$ thì h là cấp của một số a (mod p). Trước hết xét trường hợp $h = q^s$ với q là số nguyên tố. Gọi $A \subset \{1, 2, ..., p-1\}$ là tập các nghiệm của phương trình $x^h - 1 \equiv 0 \pmod p$ và $B \subset \{1, 2, ..., p-1\}$ là tập các nghiệm của phương trình $x^{p^{s-1}} - 1 \equiv 0 \pmod p$. Ta có $B \subset A$ và $B \neq A$ (do $|A| = h = p^s, |B| = p^{s-1}$). Lấy $a \in A, a \notin B$. Ta khẳng định rằng cấp của a(mod p) là h. Thật vậy giả sử l là cấp của a(mod p). Vì $a^h \equiv 1 \pmod p$ nên $l|h = p^s \rightarrow l = p^t, t \leqslant s$. Nếu $t < s$ thì $l = p^t | p^{s-1} \rightarrow a^{p^{s-1}} \equiv 1 \pmod p \rightarrow a \in B$. Điều này trái với cách chọn $a \notin B$. Vậy $t = s \Leftrightarrow l = h$.

Trong trường hợp tổng quát với $h|p-1$ bất kỳ giả sử $h = \Pi_{i=1}^k q^{s_i}$. Theo điều vừa chứng minh thì tồn tại a_i có cấp là q^{s_i}. Do định lý ta suy ra số $a = \Pi_{i=1}^k a_i$ có cấp là $h = \Pi_{i=1}^k q^{s_i}$.

Hệ quả Tồn tại số nguyên dương g có cấp là $p-1$. Số g được gọi là căn nguyên thủy (mod p).

Khi đó, tập $\{g, g^2, ..., g^{p-1}\}$ là một hệ thặng dư thu gọn (mod p).

Chứng minh Thật vậy giả sử tồn tại $i > j$ sao cho $g^i \equiv g^j \pmod p, \rightarrow g^{i-j} \equiv 1 \pmod p \rightarrow p-1|i-j$ Mâu thuẫn.

Định lý sau đây mở rộng ví dụ cho k bất kỳ (không nhất thiết là ước của $p-1$)

Định lý Cho k là số nguyên dương và $a \in \mathbb{Z}, (a, p) = 1$. Giả sử $d = (k, p-1)$. Khi đó phương trình

$$x^k \equiv a \pmod p \tag{19}$$

có nghiệm khi và chỉ khi

$$a^{(p-1)/d} \equiv 1 \pmod p \tag{20}$$

Nếu có nghiệm nó sẽ có đúng d nghiệm.

Chứng minh Điều kiện cần: Giả sử (19) có nghiệm x_0. Khi đó

$$a^{(p-1)/d} \equiv x_0^{k(p-1)/d} = (x_0^{p-1})^{k/d} \equiv 1 \pmod p$$

do định lý Fecma.

Điều kiện đủ: Gọi g là căn nguyên thủy (mod p). Tồn tại $b \in S = \{1, 2, ..., p-1\}$ sao cho $a \equiv g^b$.

Bước 1: Ta khẳng định $d|b$. Thật vậy

$$a^{(p-1)/d} \equiv g^{b(p-1)/d} \equiv 1 \pmod p.$$

Vì d là căn nguyên thủy nên suy ra $b(p-1)/d$ chia hết cho p tức là $d|b$.

Bước 2: Theo ví dụ thì phương trình $ku \equiv b \pmod{p-1}$ có d nghiệm ph
mod $(p-1)$. Nói cách khác gọi $U \subset S$ sao cho $ku \equiv b \pmod{p-1}$ thì $|U|$

Bước 3: Tập $\{x = g^u, u \in U\}$ là d nghiệm phân biệt (mod p) của phươn
đang xét. Thật vậy ta có

$$u \in U \to ku \equiv b \pmod{p-1} \to g^{ku} \equiv g^b \pmod{p} \to x^k \equiv a \pmod{}$$

Tiếp theo ta chứng minh chúng phân biệt. Giả sử $u, u' \in U$ sao cho $g^u \equiv g^{u'}$ (
thì $u \equiv u' \pmod{p-1}$ (do g là căn nguyên thủy). Vậy $u = u'$.

Bước 4: Nếu x là nghiệm của (1) thì $x \equiv g^u \pmod{p}$ trong đó $u \in U$.

Thật vậy tồn tại $u \in S$ sao cho $x \equiv g^u \pmod{p}$. Ta có

$$x^k \equiv a \pmod{p} \Leftrightarrow g^{ku} \equiv g^b \pmod{p} \Leftrightarrow ku \equiv b \pmod{p-1} \Leftrightarrow u \in$$

Định lý được chứng minh xong.

Ta có thể mở rộng khái niệm số chính phương (mod p) như sau: Cho $k \geq$
nguyên dương và số nguyên tố lẻ p. Số nguyên a gọi là số k-phương (mod p)
tại $x \in \mathbb{N}$ sao cho

$$x^k \equiv a \pmod{p}.$$

Từ định lý trên ta suy ra

Định lý a là số k-phương (mod p) khi và chỉ khi

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

tức là a là nghiệm của phương trình đồng dư

$$x^{(p-1)/d} \equiv 1 \pmod{p}$$

ở đó $d = (k, p-1)$.

Theo ví dụ phương trình (21) có đúng $\frac{p-1}{d}$ nghiệm phân biệt. Vậy

Định lý Có đúng $\frac{p-1}{d}$ số k-phương ở đó $d = (k, p-1)$.

Ví dụ Xét $k = 3, p > 3$. Nếu $p = 3s + 1$ thì $d = (3, 3s) = 3$. Do đó
phương (mod p) nếu và chỉ nếu $a^s \equiv 1 \pmod{p}$ và có đúng s số lập phương
Nếu $p = 3s + 2$ thì $d = (3, 3s + 1) = 1$. Vì $a^{p-1} \equiv 1 \pmod{p}$ nên mọi số
lập phương (mod p).

PHƯƠNG TRÌNH PELL

Đặng Hùng Thắng

I. Phương trình Pell

Phương trình Pell là phương trình có dạng

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

Đây là một phương trình rất nổi tiếng có nhiều ứng dụng trong việc giải nhiều bài toán số học hay và khó. Trong chương này khi nói đến nghiệm ta luôn hiểu đó là nghiệm nguyên dương.

I. Định lý 1 (về sự tồn tại nghiệm)

Phương trình (I) có nghiệm nguyên dương khi và chỉ khi d là số không chính phương.

Chứng minh Nếu $d = m^2$ thì (1) trở thành

$$x^2 - m^2y^2 = 1 \to (x - my)(x + my) = 1 \to x - my = x + my = 1 \to x = 1, y = 0$$

Đảo lại giả sử d là số không chính phương.Ta cần có các bổ đề sau

Bổ đề 1 Cho α là một số vô tỷ. Khi đó có tồn tại vô số cặp số nguyên dương (h, k) với $k > 0$ thỏa mãn

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

Chứng minh Trước hết ta chứng minh nhận xét: Với mọi số nguyên dương q tồn tại (h, k) nguyên dương với $1 \leqslant k \leqslant q$ sao cho

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

Ta chia đoạn [0;1] thành q đoạn bằng nhau $B_1, B_2, ..., B_q$ với $B_i = \{x \in [0;1] : \frac{i-1}{q} \leqslant x < \frac{i}{q}\}$. Xét dãy $\{t\alpha\}, (t = 0, 1, ..., q)$. Tồn tại tập B_i chứa hai số của dãy trên, chẳng hạn $\{t_1\alpha\}, \{t_2\alpha\}, t_2 < t_1$. Suy ra

$$|\{t_1\alpha\} - \{t_2\alpha\}| \leqslant \frac{1}{q} \qquad (22)$$

Giả sử $t_1\alpha = m_1 + \{t_1\alpha\}, t_2\alpha = m_2 + \{t_2\alpha\}$ .Từ (2) suy ra

$$|(m_1 - m_2) - \alpha(t_1 - t_2)| \leqslant \frac{1}{q}$$

Đặt $h = m_1 - m_2, k = t_1 - t_2$ ta có $1 \leqslant k \leqslant q$ và $|\alpha k - h| \leqslant \frac{1}{q}$. Điều này tương đương với nhận xét . Ký hiệu

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

Nếu A hữu hạn thì tồn tại ϵ sao cho $|\alpha - \frac{h}{k}| > \epsilon$ với mọi $(h,k) \in A$. Bây giờ $q \in \mathbb{N}$ sao cho

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

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

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

Từ (4) ta có $(h_0, k_0) \in A$. Vậy $\left|\alpha - \frac{h_0}{k_0}\right| > \epsilon$. Nhưng $\frac{1}{q} \geqslant \frac{1}{k_0 q} > \left|\alpha - \frac{h_0}{k_0}\right| >$ thuẫn với (3).Bổ đề được chứng minh.

Bổ đề 2 Tồn tại vô số cặp số nguyên dương (x,y) thỏa mãn

$$|x^2 - dy^2| < 1 + 2\sqrt{d}$$

Chứng minh Theo bổ đề 1 tồn tại vô số cặp số nguyên dương (x,y) thỏa

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

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

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

Ta bước vào chứng minh định lý. Theo bổ đề 2 tồn tại vô số cặp số nguy (x,y) thỏa mãn

$$|x^2 - dy^2| < 1 + 2\sqrt{d}$$

tức là trong đoạn $I = [-1 - 2\sqrt{d}; 1 + 2\sqrt{d}]$ có vô số cặp số nguyên dương (tồn tại $k \in I$ để với vô số cặp số (x,y) ta có

$$x^2 - dy^2 = k$$

Gọi $H = \{(x,y)|x^2 - dy^2 = k\}$ và với $1 \leqslant i,j \leqslant |k|$ ký hiệu $H_{ij} = \{(x,y)$ $(\mathrm{mod}\ |k|), y \equiv j\ (\mathrm{mod}\ |k|)\}$. Vì $|H| = \infty$ nên tồn tại (i,j) để $|H_{ij}| = \infty$. tồn tại hai cặp số nguyên dương $(x_1, y_1) \neq (x_1, y_1) \in H_{ij}$ thỏa mãn

$$\begin{gathered} x_1 \equiv x_2 \pmod{|k|}, \quad y_1 \equiv y_2 \pmod{|k|} \\ x_1^2 - dy_1^2 = x_2^2 - dy_2^2 = k \end{gathered}$$

Xét tích

$$(x_1 - y_1\sqrt{d})(x_2 + y_2\sqrt{d}) = x_1x_2 - dy_1y_2 + \sqrt{d}(x_1y_2 - x_2y_1)$$

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 các số nguyên u,v sao cho

$$x_1x_2 - dy_1y_2 = ku \tag{27}$$
$$x_1y_2 - x_2y_1 = kv \tag{28}$$

Vậy từ (6) (7) (8) 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 chú ý rằng $x_1^2 - dy_1^2 = x_2^2 - dy_2^2 = k$ ta được

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

Rõ ràng $u > 0$ Nếu $v = 0$ thì $u = \pm 1$ Suy ra $(x_1 - y_1\sqrt{d})(x_2 + y_2\sqrt{d}) = \pm k = \pm(x_1 - y_1\sqrt{d})(x_1 + y_1\sqrt{d})$, Vậy $x_2 + y_2\sqrt{d} = x_1 + y_1\sqrt{d} \longrightarrow x_1 = x_2, y_1 = y_2$ Ta có mâu thuẫn. Định lý 1 được chứng minh .

Chú ý: Nghiệm bé nhất của phương trình Pell có thể rất lớn. Thí dụ phương trình $x^2 - 61y^2 = 1$ có nghiệm nhỏ nhất là $a = 1766319049, b = 226153980$, phương trình $x^2 - 109y^2 = 1$ có nghiệm nhỏ nhất là $a = 158070671986249, b = 15140424455100$

Bây giờ chúng ta sẽ tìm công thức mô tả tất cả các nghiệm của (1).

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

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

nghĩa là b là số nguyên dương bé nhất để $1 + db^2$ là số chính phương (theo định lý 1 thì luôn tồn tại) Xét dãy (x_n) và (y_n) cho bởi hệ thức truy hồi sau

$$x_0 = 1, x_1 = a, x_{n+2} = 2ax_{n+1} - x_n \tag{29}$$
$$y_0 = 0, y_1 = b, y_{n+2} = 2ay_{n+1} - y_n \tag{30}$$

Khi đó (x_n, y_n) là tất cả các nghiệm của phương trình Pell (1).

Chứng minh Phương trình đặc trưng của dãy (9) là $x^2 - 2ax + 1 = 0$ có $\Delta' = a^2 - 1 = db^2$ do đó có hai nghiệm là $\lambda_1 = a + b\sqrt{d}, \lambda_2 = a - b\sqrt{d}$ Từ điều kiện ban đầu dễ tìm được

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

Từ đó

$$x_n + y_n\sqrt{d} = (a + b\sqrt{d})^n, x_n - y_n\sqrt{d} = (a - b\sqrt{d})^n. \tag{31}$$

Suy ra $(x_n^2 - dy_n^2) = (a^2 - db^2)^n = 1$. Dễ chứng minh quy nạp rằng (x_n) và (dãy tăng các số nguyên dương.

Đảo lại giả sử (x, y) là một nghiệm bất kỳ của (1). Ta sẽ chứng minh khẳng Tồn tại n để

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

Phản chứng: Giả sử trái lại với mọi n ta có $x + y\sqrt{d} \neq (a + b\sqrt{d})^n$. Khi đó tồn nguyên dương sao cho

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

Nhân hai vế của bất đẳng thức trên với $(a - b\sqrt{d})^m$ ta được

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

Do (11) ta có

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

với $u = xx_m - dyy_m, v = x_m y - y_m x$. Vậy

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

Ta có

$$u^2 - dv^2 = (x^2 - dy^2)(x_m^2 - dy_m^2) = 1$$

Lại có $x > y\sqrt{d}, x_m > y_m\sqrt{d}$ nên $u > 0$. Lại có $(u - v\sqrt{d})(u + v\sqrt{d})$ $1 < u + v\sqrt{d}$ nên $0 < u - v\sqrt{d} < 1 < 1 < u + v\sqrt{d} \to v > 0$. Vậy (u, v) là của (1) do đó $a \leqslant u, b \leqslant v \to a + b\sqrt{d} \leqslant u + v\sqrt{d}$. Điều này trái với (12).V giả sử của ta sai. Vậy điều khẳng định được chứng minh. Do d là số khôn phương ta suy ra $(x, y) = (x_n, y_n)$ Định lý được chứng minh.

Ví dụ 1 Tìm tất cả các số nguyên dương $x > 2$ sao cho tam giác có d cạnh là $x - 1, x, x + 1$ có diện tích là một số nguyên.

Giải Gọi S là diện tích tam giác. Theo công thức Hê rông ta tìm được

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

Ta có nếu $S \in \mathbb{Z}$ thì x chẵn . Đặt $x = 2y$ suy ra $S^2 = 3y^2(y^2 - 1)$ - $y\sqrt{3(y^2 - 1)} \longrightarrow 3(y^2 - 1) = h^2 \longrightarrow h = 3z \longrightarrow 3(y^2 - 1) = 9z^2 \longrightarrow y^2 -$

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

$$y^2 - 3z^2 = 1$$

thì dễ thấy $x = 2y, y > 1$ thỏa mãn điều kiện đầu bài. Nghiệm nhỏ nhất cí (2,1). Vậy tất cả các nghiệm của (13) là dãy(y_n) cho bởi

$$y_0 = 1, y_1 = 2, y_{n+2} = 4y_{n+1} - y_n$$

Suy ra nghiệm của bài toán là dãy (x_n) với $n \geq 1$ cho bởi

$$x_0 = 2, x_1 = 4, x_{n+2} = 4x_{n+1} - x_n$$

Đó là các số $4, 14, 52, ...$

Ví dụ 2 Tìm tất cả các nguyên dương T sao cho số tam giác $\frac{T(T+1)}{2}$ là một số chính phương.

Giải $T(T+1) = 2y^2 \longrightarrow 4T^2 + 4T + 1 = 8y^2 + 1 \longrightarrow (2T+1)^2 - 8y^2 = 1$ Đặt $x = 2T + 1$.Suy ra (x, y) là nghiệm của phương trình

$$x^2 - 8y^2 = 1. \tag{34}$$

Đảo lại nếu (x, y) là nghiệm của (14) thì x lẻ do đó $T = \frac{x-1}{2}$ thỏa mãn đầu bài.

Nghiệm nhỏ nhất của (14) là (3;1).Theo định lý trên phương trình (14) có nghiệm là dãy (x_n) xác định bởi

$$x_0 = 1, x_1 = 3, x_{n+2} = 6x_{n+1} - x_n$$

Khi đó với $x_n = 2T_n + 1$ ta có $2T_{n+2} + 1 = 6(2T_{n+1} + 1) - (2T_n + 1)$. Từ đó dãy (T_n) xác định bởi

$$T_0 = 0, T_1 = 1, T_{n+2} = 6T_{n+1} - T_n + 2$$

là dãy cần tìm. Đó là các số 1,8, 49,288,...

Ví dụ 3 Tìm tất cả các số nguyên dương n sao cho trung bình cộng của n số chính phương đầu tiên lại là một số chính phương.

Giải Ta có

$$\frac{1^2 + 2^2 + 3^2 + \cdots + n^2}{n} = \frac{(n+1)(2n+1)}{6}.$$

Vậy ta có phương trình $(n + 1)(2n + 1) = 6y^2 \longrightarrow (4n + 3)^2 - 48y^2 = 1$. Đặt $x = 4n + 3$ ta có phương trình $x^2 - 48y^2 = 1$.Nghiệm nhỏ nhất là (7,1). Dãy x_n tuân theo quy luật

$$x_0 = 1, x_1 = 7, x_{n+2} = 14x_{n+1} - x_n.$$

Bằng quy nạp dễ thấy Với n chẵn thì $x_k \equiv 1 \pmod 4$, Với n lẻ thì $x_k \equiv 3 \pmod 4$. Vậy $n_k = \frac{x_{2k+1}-3}{4}$ là dãy cần tìm.Sau đây ta thiết lập tường minh công thức truy hồi của n_k. Đặt $u_k = x_{2k+1}$. Ta có $x_{2k+3} = 14x_{2k+2} - x_{2k+1} = 14(14x_{2k+1} - x_{2k}) - x_{2k+1} = 196x_{2k+1} - 14x_{2k} - x_{2k+1} = 195x_{2k+1} - x_{2k+1} - x_{2k-1} = 194x_{2k+1} - x_{2k-1}$. Vậy $u_{k+2} = 194u_{k+1} - u_k$Vậy $4n_{k+2} + 3 = 194(4n_{k+1} + 3) - 4n_k - 3$ Từ đó

$$n_{k+2} = 194n_{k+1} - n_k + 144$$

với $n_0 = 1, n_1 = 337, n_2 = 65521$.....

Ví dụ 4 Tìm tất cả các số nguyên dương n sao cho cả $2n + 1$ và $3n + 1$ đều là số chính phương.

Giải Vì $(2n+1, 3n+1) = 1$ nên cả $2n+1$ và $3n+1$ đều là số chính phương khi và chỉ khi $(2n+1)(3n+1) = y^2$ Suy ra $(12n+5)^2 - 24y^2 = 1$ Đặt $x = 12n+5$ ta dẫn tới phương trình Pell $x^2 - 24y^2 = 1$ Nghiệm nhỏ nhất là$(5, 1)$, Vậy $x_{k+2} = 10x_{k+1} - x_k$. Để chứng minh $x_k \equiv 5 \pmod{12}$ khi và chỉ khi k lẻ.Đặt $u_k = x_{2k+1}$

Ta có $x_{2k+3} = 10x_{2k+2} - x_{2k+1} = 10(10x_{2k+1} - x_{2k}) - x_{2k+1} = 100x_{2k+1} - 10x_{2k} - x_{2k+1} = 99x_{2k+1} - x_{2k+1} - x_{2k-1} = 98x_{2k+1} - x_{2k-1}$. Vậy $u_{k+2} = 98u_{k+1} - u_k$ Vậy $u_{k+2} = 98u_{k+1} - u_k$Vậy $12n_{k+2} + 5 = 98(12n_{k+1} + 5) - 12n_k - 5$ Từ đó

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

với $n_0 = 0, n_1 = 40, n_2 = 3960, ..$

Từ đó suy ra một bài toán hay sau đây:

Chứng minh rằng nếu n là một số nguyên dương sao cho cả $2n+1$ và $3n$ là số chính phương thì n phải chia hết cho 40.

II.Phương trình Pell loại 2

Phương trình Pell loại 2 là phương trình

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

a) Nếu d là số chính phương $d = m^2$ thì phương trình (II) trở thành $(my-x$ $x) = 1 \to my - x = my + x = 1 \to x = 0$ Vậy phương trình không có nghiệ

b) Nếu d có ước nguyên tố $p = 4k+3$ thì phương trình cũng vô nghiệm. T giả sử (x, y) là nghiệm. Khi đó $x^2 + 1 = dy^2 \to p|x^2 + 1$. Vì p có dạng 4k theo một kết quả quen thuộc 1 chia hết cho p. Ta có mâu thuẫn.

Điều ngươc lại không đúng. Nếu d không có ước nguyên tố dạng 4k+3 thì trình có thể vẫn vô nghiệm .(Xem ví dụ 5) Tuy nhiên, nếu d là một số nguyê điều ngược lại cũng đúng. Cụ thể ta có

Định lý 3 Phương trình Pell loại 2 có nghiệm khi và chỉ khi $d \neq 4k+3$

Chứng minh Giả sử phương trình có nghiệm. Theo b) $d \neq 4k+3$. Ngu giả sử $d \neq 4k+3$. Nếu $p = 2$ phương trình $x^2 - 2y^2 = -1$ có nghiệm $(x, y) =$ Nếu $d \equiv 1 \pmod 4$. Xét phương trình Pell

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

Ta gọi đó là phương trình Pell lên kết với (II). Gọi (a, b) là nghiệm nhỏ nhất c Ta có $a^2 - 1 = db^2$. Nếu a chẵn thì b lẻ do đó $b^2 \equiv 1 \pmod 4 \to a^2 \equiv 1 +$ (mod 4). Điều này không xảy ra. Vậy a lẻ và b chẵn. Giả sử $a = 2a_1 + 1, b =$ có $(a-1)(a+1) = db^2 \Leftrightarrow a_1(a_1+1) = db_1^2$. Do d là số nguyên tố và $(a_1, a_1 +$ nên ta có $a_1 = u^2, a_1 + 1 = dv^2$ hoặc $a_1 = du^2, a_1 + 1 = v^2$.

Nếu $a_1 = u^2, a_1 + 1 = dv^2 \to u^2 - dv^2 = -1$. Vậy (II) có nghiệm nguyên (u, v).

Nếu $a_1 = du^2, a_1 + 1 = v^2 \to v^2 - du^2 = 1$. Vậy (v, u) là nghiệm của (6 ra $v \geq a \to a_1 + 1 = v^2 \geq v \geq a = 2a_1 + 1$. Mâu thuẫn. Vậy khả năng này xảy ra.

Định lý sau đây cho ta một điều kiện cần và đủ để (II) có nghiệm,

Định lý 4. Gọi (a, b) là nghiệm nhỏ nhất của phương trình Pell lên kết Khi đó (II) có nghiệm khi và chỉ khi hệ

$$\begin{cases} a = x^2 + dy^2 \\ b = 2xy \end{cases}$$

có nghiệm.

Chứng minh. Giả sử (x_0, y_0) là nghiệm của (16). Ta có $a^2 - db^2 =$ $(x_0^2 - dy_0^2)^2 = 1$. Vậy ta có $x_0^2 - dy_0^2 = 1$ hoặc $x_0^2 - dy_0^2 = -1$. Nếu trường h xảy ra thì (x_0, y_0) là nghiệm của (I) do đó $x_0 \geq a = x_0^2 + dy_0^2 > x_0$. Mâu thuẫ phải có $x_0^2 - dy_0^2 = -1$ tức là (x_0, y_0) là nghiệm của (II).

Đảo lại giả sử (II) có nghiệm. Gọi (x_0, y_0) là nghiệm nhỏ nhất của (II). Ta sẽ chứng minh rằng (x_0, y_0) chính là nghiệm của (16). Thật vậy đặt $u = x_0^2 + dy_0^2, v = 2x_0, y_0$. Ta có $u^2 - dv^2 = (x_0^2 - dy_0^2)^2 = 1$. Vậy (u, v) là nghiệm của (16). Suy ra $u \geq a, v \geq b$. Ta chứng minh $u = a, v = b$. Giả sử trái lại tức là $u > a, v > b$. Ta có $(a - b\sqrt{d}) < (a - b\sqrt{d})(a + b\sqrt{d}) = 1$ do đó

$$(a - b\sqrt{d})(x_0 + y_0\sqrt{d}) < x_0 + y_0\sqrt{d} \Leftrightarrow \tag{37}$$

$$(ax_0 - dby_0) + (ay_0 - bx_0)\sqrt{d} < x_0 + y_0\sqrt{d} \tag{38}$$

Chú ý rằng $a + b\sqrt{d} < u + v\sqrt{d} = (x_0 + y_0\sqrt{d})^2$ nên

$$\begin{aligned} -(ax_0 - dby_0) + (ay_0 - bx_0) &= (a + b\sqrt{d})(-x_0 + y_0\sqrt{d}) \\ &< (x_0 + y_0\sqrt{d})^2(-x_0 + y_0\sqrt{d}) = \\ &(dy_0^2 - x_0^2)(x_0 + y_0\sqrt{d}) = x_0 + y_0\sqrt{d} \end{aligned} \tag{39}$$

Đặt $s = (ax_0 - dby_0), t = (ay_0 - bx_0)$. Dễ kiểm tra được $s^2 - dt^2 = -1$ và $s \neq 0$. Ta có $t > 0$. Thật vậy $t > 0 \Leftrightarrow a^2y_0^2 > b^2x_0^2 \Leftrightarrow (db^2 + 1)y_0^2 > (dy_0^2 - 1)b^2 \Leftrightarrow y_0^2 > -b^2$. Điều này đúng. Nếu $s > 0$ thì (s, v) là nghiệm của (II) do đó $s + t\sqrt{d} \geqslant x_0 + y_0\sqrt{d}$. Mâu thuẫn với (18). Nếu $s < 0$ thì $(-s, t)$ là nghiệm của (II) nên suy ra $-s + t\sqrt{d} \geqslant x_0 + y_0\sqrt{d}$. Mâu thuẫn với (19). Định lý được chứng minh.

Ví dụ 5 Chứng minh rằng phương trình $x^2 - 34y^2$ vô nghiệm . (Chú ý rằng 34=2.17 không có ước nguyên tố dạng 4k+3)

Thật vậy 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 phương trình thứ 2, Vậy phương trình $x^2 - 34y^2 = -1$ vô nghiệm.

Nhận xét. Hệ (16) nếu có nghiệm thì có duy nhất nghiệm . Do đó theo chứng minh trên nghiệm duy nhất đó chính là nghiệm nhỏ nhất của (II).

Thật vậy giả sử $(x_0, y_0), (x_1, y_1)$ là hai nghiệm của (16). Khi đó ta có $x_0^2 + dy_0^2 + 2x_0y_0\sqrt{d} = x_1^2 + dy_1^2 + 2x_1y_1\sqrt{d} = a + b\sqrt{d}$. Suy ra $(x_0 + y_0\sqrt{d})^2 = (x_1 + y_1\sqrt{d})^2 \rightarrow x_0 + y_0\sqrt{d} = x_1 + y_1\sqrt{d}$. Do d là số không chính phương nên ta rút ra $x_0 = x_1, y_0 = y_1$.

Từ đó suy ra nghiệm nhỏ nhất của (II) luôn bé hơn nghiệm nhỏ nhất của (I).Nhận xét này giúp ta tìm nghiệm nhỏ nhất của phương trình Pell (I) nhanh chóng khi mà nghiệm mà nghiệm nhỏ nhất ấy lại rất lớn.

Ví dụ 6 Tìm nghiệm nhỏ nhất của $x^2 - 29y^2 = 1$

Phương trình $x^2 - 29y^2 = -1$ có nghiệm nhỏ nhất là (70;13). Vậy nghiệm nhỏ nhất của phương trình Pell đang xét là $a = 70^2 + 29(13)^2 = 9801, b = 2(70)(13) = 1820$.

Định lý sau cho ta công thức nghiệm.

Định lý 5. Giả sử hệ phương trình (16) có nghiệm và (u, v) là nghiệm duy nhất của nó.

Xét dãy số nguyên dương $(x_n), (y_n)$ xác định bởi

$$x_0 = u, x_1 = u^3 + 3duv^2, x_{n+2} = 2ax_{n+1} - x_n \tag{40}$$

$$y_0 = v, y_1 = dv^3 + 3u^2v, y_{n+2} = 2ay_{n+1} - y_n \tag{41}$$

Khi đó (x_n, y_n) là tất cả các nghiệm của của (II).

Chứng minh Đầu tiên ta chứng minh rằng

$$x_n + y_n\sqrt{d} = (u + v\sqrt{d})^{2n+1}$$
$$x_n - y_n\sqrt{d} = (u - v\sqrt{d})^{2n+1}$$

Phương trình đặc trưng của dãy (8) là $x^2 - 2ax + 1 = 0$ có $\Delta' = a^2 - 1 =$ dó có hai nghiệm là $\lambda_1 = a + b\sqrt{d}, \lambda_2 = a - b\sqrt{d}$. Do đó $x_n = C_1(a + b$ $C_2(a - b\sqrt{d})^n = C_1(u + \sqrt{d}v)^{2n} + C_2(u - \sqrt{d}v)^{2n}$. Từ điều kiện ban đầu được $C_1 = \frac{u+v\sqrt{d}}{2}, C_2 = \frac{u-v\sqrt{d}}{2}$ Do vậy

$$x_n = \frac{(u + v\sqrt{d})^{2n+1} + (u - v\sqrt{d})^{2n+1}}{2}$$

Tương tự

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

Suy ra (22) và (23). Nhân (22) với (23) vế với vế ta được $x_n^2 - y_n^2\sqrt{d} =$ $v^2\sqrt{d})^{2n+1} = 1$.

Đảo lại giả sử (x, y) là nghiệm của (II). Xét số $(x + y\sqrt{d})(u + v\sqrt{d}) =$ $dyv) + (yu + xv)\sqrt{d} = s + t\sqrt{d}$ với $s = xu + dyv, t = yu + xv$. Ta có $s^2 -$ $(x^2 - dy^2)(u^2 - dv^2) = (-1)(-1) = 1$ Vậy (s, t) là nghiệm của phương trì (I). Do đó tồn tại $n \in \mathbb{N}$ sao cho

$$s + t\sqrt{d} = (a + b\sqrt{d})^{n+1} \Leftrightarrow$$
$$(x + y\sqrt{d})(u + v\sqrt{d}) = (u + v\sqrt{d})^{2n+2} \Leftrightarrow$$
$$x + y\sqrt{d} = (u + v\sqrt{d})^{2n+1} = x_n + y_n\sqrt{d} \rightarrow$$
$$(x, y) = (x_n, y_n)$$

Ví dụ 7 Tìm tất cả các số nguyên dương n có tính chất $n^2 + (n + 1)^2$ là s phương.

Giải $n^2 + (n + 1)^2 = y^2 \Leftrightarrow (2n + 1)^2 + 1 = 2y^2 \Leftrightarrow (2n + 1)^2 - 2y^2 = -$ $x = 2n + 1$ ta có phương trình $x^2 - 2y^2 = -1$. Theo định lý trên nghiệm là $x_0 = 1, x_1 = 7, x_{k+2} = 6x_{k+1} - x_k$. Từ đó $2n_{k+2} + 1 = 6(2n_{k+1} + 1) - 2$ Các số cần tìm được cho bởi dãy (n_k) sau đây

$$n_0 = 0, n_1 = 3, n_{k+2} = 6n_{k+1} - n_k + 2$$

Đó là các số 3; 20; 119; ...

III.Phương trình Pell chứa tham số n

Phương trình Pell chứa tham số n là phương trình

$$x^2 - dy^2 = n \qquad \text{(III)}$$

trong đó d là số nguyên dương không chính phương còn n là số nguyên.

Định lý 6. Phương trình (III) hoặc vô nghiệm hoặc có vô số nghiệm.

Chứng minh. Giả sử (III) có nghiệm (x_n, y_n) tức là

$$x_n^2 - dy_n^2 = n$$

Gọi (a, b) là nghiệm của phương trình Pell (I). Khi đó t

$$a^2 - db^2 = n \tag{45}$$

Nhân (24) với (25) ta được

$$(x_n^2 - dy_n^2)(a^2 - db^2) = n \Leftrightarrow (x_n a + dy_n b)^2 - d(x_n b + y_n a)^2 = n$$

Đặt

$$x_{n+1} = x_n a + dy_n b \tag{46}$$
$$y_{n+1} = x_n b + y_n a \tag{47}$$

Ta thấy (x_{n+1}, y_{n+1}) là nghiệm và $x_n < x_{n+1}, y_n < y_{n+1}$. Vậy công thức () cho ta vô số nghiệm của (III) nếu (III) có một nghiệm khởi đầu (x_1, y_1).

Chú ý. Nếu ta chọn nghiệm khởi đầu là nghiệm bé nhất thì trong trường hợp $n = \pm 1$ công thức (26) và (27) cho ta *tất cả* các nghiệm.

Thật vậy : Với $n = 1$ theo công thức (11) $(a + b\sqrt{d})^n = x_n + y_n\sqrt{d}$. Suy ra

$$x_{n+1} + y_{n+1}\sqrt{d} = (a + b\sqrt{d})^{n+1} =$$
$$(a + b\sqrt{d})^n(a + b\sqrt{d}) = (x_n + y_n\sqrt{d})(a + b\sqrt{d})$$
$$= (x_n a + dy_n b) + (x_n b + y_n a)\sqrt{d}$$

Vậy

$$x_{n+1} = x_n a + dy_n b, \quad y_{n+1} = x_n b + y_n a.$$

Với $n = -1$ theo công thức (22) ta có $(x_0 + y_0\sqrt{d})^{2n+1} = x_n + y_n\sqrt{d}$. Suy ra

$$x_{n+1} + y_{n+1}\sqrt{d} = (x_0 + y_0\sqrt{d})^{2n+3} =$$
$$(x_0 + y_0\sqrt{d})^{2n+1}(x_0 + y_0\sqrt{d})^2 = (x_n + y_n\sqrt{d})(a + b\sqrt{d})$$
$$= (x_n a + dy_n b) + (x_n b + y_n a)\sqrt{d} \rightarrow$$

(vì $a = x_0^2 + dy_0^2, b = 2x_0 y_0$.) Vậy

$$x_{n+1} = x_n a + dy_n b, \quad y_{n+1} = x_n b + y_n a.$$

Tuy nhiên với $n \neq \pm 1$ điều này không đúng. Dãy (26) và (27) không nhất thiết vét cạn tất cả các nghiệm của phương trình (III). Thí dụ sau đây minh họa cho điều đó.

Ví dụ 7. Giải phương trình

$$x^2 - 5y^2 = -4. \tag{48}$$

Xét phương trình Pell tương ứng $x^2 - 5y^2 = 1$. Dễ thấy nghiệm nhỏ nhất của phương trình Pell là $(a, b) = (9, 4)$ và nghiệm nhỏ nhất của phương trình (48) là $(x_1, y_1) = (1; 1)$. Do vậy công thức (26) và (27) cho ta dãy nghiệm (x_n, y_n) sau đây

$$x_{n+1} = 9x_n + 20y_n, \quad y_{n+1} = 4x_n + 9y_n.$$

Cụ thể đó là các nghiệm sau $(1; 1), (29; 13), (521, 233), (9349, 4181), \ldots$

Tuy nhiên nó chưa vét hết nghiệm, Chẳng hạn rõ ràng $(4;2)$ là nghiệm của
trình nhưng không có mặt trong dãy trên. Bây giờ ta chứng minh tất cả các
(x_n, y_n) của phương trình (48) được xác định bởi quy luật sau

$$x_1 = 1, x_2 = 4, x_{n+2} = 3x_{n+1} - x_n$$
$$y_1 = 1, y_2 = 2, y_{n+2} = 3y_{n+1} - y_n$$

1) Trước hết ta chứng minh (x_n, y_n) là nghiệm.

Cách 1 Ta có

$$x_{n+1}^2 - 3x_{n+1}x_n + x_n^2 = x_{n+1}(x_{n+1} - 3x_n) + x_n^2 =$$
$$-x_{n+1}x_{n-1} + x_n^2 = x_n^2 - x_{n-1}(3x_n - x_{n-1} =$$
$$x_n^2 - 3x_n x_{n-1} + x_{n-1}^2$$

Vậy $x_{n+1}^2 - 3x_{n+1}x_n + x_n^2 = x_2^2 - 3x_1x_2 + x_1^2 = 5$

Tương tự $y_{n+1}^2 - 3y_{n+1}y_n + y_n^2 = y_2^2 - 3y_1y_2 + y_1^2 = -1$ Từ đó

$$x_{n+1}^2 = 3x_{n+1}x_n - x_n^2 + 5 =$$
$$3x_n(3x_n - x_{n-1}) - x_n^2 + 5 = 8x_n^2 + 5 - 3x_n x_{n-1} =$$
$$8x_n^2 + 5 + 5 - x_n^2 - x_{n-1}^2 = 7x_n^2 - x_{n-1}^2 + 10$$

Tương tự

$$y_{n+1}^2 = 7y_n^2 - y_{n-1}^2 - 2$$

Từ (49) và (50) ta suy ra

$$x_{n+1}^2 - 5y_{n+1}^2 + 4 = 7(x_n^2 - 5y_n^2 + 4) - (x_{n-1}^2 - 5y_{n-1}^2 + 4)$$

Bằng phương pháp quy nạp suy ra với mọi n=1,2,...

$$x_n^2 - 5y_n^2 + 4 = 0$$

Cách 2 Ta chứng minh bằng quy nạp rằng

$$x_{n+1} = \frac{3x_n + 5y_n}{2}$$
$$y_{n+1} = \frac{x_n + 3y_n}{2}$$

Thật vậy, với $n = 1, 2$ công thức (51) đúng. Giả sử (51) đúng cho $n = k, n =$
có $x_{k+3} = 3x_{k+2} - x_{k+1}$. Thay biểu diễn x_{k+2}, x_{k+1} theo (51) vào ta thu đ

$$x_{k+3} = \frac{3}{2}(3x_{k+1} - x_k) + \frac{5}{2}(3y_{k+1} - y_k) = \frac{3x_{k+2} + 5y_{k+2}}{2}$$

Chứng minh tương tự

$$y_{k+3} = \frac{x_{k+2} + 3y_{k+2}}{2}$$

Từ đó

$$x_{n+1}^2 - 5y_{n+1}^2 = \left(\frac{3x_n + 5y_n}{2}\right)^2 - 5\left(\frac{x_n + 3y_n}{2}\right)^2$$
$$= \frac{4x_n^2 - 20y_n^2}{4} = x_n^2 - 6y_n^2 = \cdots = x_1^2 - 5y_1^2 = 2$$

2) Ngược lại giả sử (u_0, v_0) là một nghiệm bất kỳ của (48). Ta phải chứng minh rằng tồn tại k sao cho $(u_0, v_0) = (x_k, y_k)$

Nếu $u_0 = 1 \to v_0 = 1$. Vậy $(u_0, v_0) = (x_1, y_1)$. Giả sử $u_0 > 1 \to v_0 > 1$.Xét

$$u_1 = \frac{3u_0 - 5v_0}{2}, v_1 = \frac{3v_0 - u_0}{2}$$

Vì $u_0^2 - 5v_0^2 = -4$ nên u_0, v_0 cùng tính chẵn lẻ, Vậy u_1, v_1 nguyên. Hơn nữa$u_1 > 0, v_1 > 0$. Thật vậy $u_1 > 0 \Leftrightarrow 3u_0 > 5v_0 \Leftrightarrow 9u_0^2 > 25v_0^2 \Leftrightarrow 9(5v_0^2 - 4) > 25v_0^2 \Leftrightarrow 20v_0^2 > 36$. Đúng vì $v_0 > 1$. Ta có $v_1 > 0 \Leftrightarrow 3v_0 > u_0 \Leftrightarrow 9v_0^2 > u_0^2 \Leftrightarrow 9v_0^2 > 5v_0^2 - 4$ Đúng. Ta cũng kiểm tra dễ dàng rằng $u_1^2 - 5v_1^2 = -4$ và $u_1 < u_0$ và

$$u_0 = \frac{3u_1 + 5v_1}{2} \tag{53}$$

$$v_0 = \frac{u_1 + 3v_1}{2} \tag{54}$$

Nếu $u_1 > 1 \to v_1 > 1$ thì ta lại xây dưựng được dãy (u_2, v_2) là nghiệm của phương trình(48) với $u_2 < u_1$. Quá trình này phải kết thúc ở bước thứ k và ta có $(u_k, v_k) = (1, 1) = (x_0, y_0)$ Vì

$$u_{n-1} = \frac{3u_n + 5v_n}{2}$$

$$v_{n-1} = \frac{u_n + 3v_n}{2}$$

nên $(u_{k-1}, v_{k-1}) = (x_1, y_1) \to (u_{k-2}, v_{k-2}) = (x_2, y_2 \to ... \to (u_0, v_0) = (x_k.v_k)$

Tóm lại tất cả các nghiệm của (48) là $(1; 1)(4; 2)(11; 5)(29; 13)(76; 34)$....

Định lý 7. Giả sử phương trình (III) có nghiệm. Nếu (x_0, y_0) là nghiệm nhỏ nhất của nó thì

$$y_0^2 \leqslant \max\left\{nb^2; \frac{-na^2}{d}\right\} \tag{55}$$

Chứng minh Xét số $u = ax_0 - dby_0, v = ay_0 - bx_0$. Dễ kiểm tra $u^2 - dv^2 = n$. Giả sử trái lại $y_0 > nb^2, y_0 > \frac{-na^2}{d}$. Khi đó $u > 0, v > 0$ Thật vậy $v > 0 \Leftrightarrow ay_0 > bx_0 \Leftrightarrow a^2y_0^2 > b^2x_0^2 \Leftrightarrow (1 + db^2)y_0 > b^2x_0 \Leftrightarrow y_0^2 > b^2(x_0^2 - dy_0) = nb^2$. Bất đẳng thức đúng.$u > 0 \Leftrightarrow a^2x_0^2 > d^2b^2y_0^2 \Leftrightarrow x_0^2(1 + db^2) > d^2b^2y_0^2 \Leftrightarrow x_0^2 > -db^2(x_0^2 - dy_0^2) = -ndb^2 \Leftrightarrow dy_0^2 > -n(db^2 + 1) \Leftrightarrow dy_0^2 > -na^2$ Bất đẳng thức đúng. Vậy (u, v) là nghiệm của (III). Mặt khác từ hệ phương trình bậc nhất $ax_0 - dby_0 = u; -bx_0 + ay_0 = v$(ẩn là x_0, y_0) giải ra ta được $x_0 = au + dbv, y_0 = bu + av \to x_0 > u, y_0 > v$. Điều này mâu thuẫn với việc chọn (x_0, y_0) là nghiệm nhỏ nhất.

Định lý 8 Giả sử phương trình (III) có nghiệm. Giả sử $(\alpha_1, \beta_1), ..., (\alpha_m, \beta_m)$ là tất cả các nghiệm của (III) thỏa mãn bất đẳng thức

$$v_i^2 \leqslant \max\left\{nb^2; \frac{-na^2}{d}\right\} \quad i = 1, 2, ..., m \tag{56}$$

Xét m dãy sau đây: dãy thứ i (i=1,2,...m) $(x_{n,i}, y_{n,i})$ xác định bởi

$$x_{0,i} = \alpha_i, y_{0,i} = \beta_i$$

$$x_{n+1,i} = x_{n,i}a + dy_{n,i}b$$

$$y_{n+1,i} = x_{n,i}b + y_{n,i}a$$

Khi đó các dãy $(x_{n,i}, y_{n,i})$ sẽ vét hết nghiệm của (III).

Chứng minh Ta đã chứng minh các số hạng của dãy trên là nghiệm của
Ngược lại giả sử. Ngược lại giả sử (u_0, v_0) là một nghiệm bất kỳ của (48). Ta
chứng minh rằng tồn tại k, i sao cho $(u_0, v_0) = (x_{k,i}, y_{k,i})$

Nếu $v_0 \leqslant \max\left\{nb^2; \frac{-na^2}{d}\right\}$ thì tồn tại i để $(u_0, v_0) = (\alpha_i, \beta_i) = (x_{0,i}, y_{0,i})$
ta có $k = 0$. Giả sử trái lại . Xét số $u_1 = au_0 - dbv_0, v_1 = av_0 - bu_0$. Dễ kiể
$u_1^2 - dv_1^2 = n$. Ngoài ra vì $v_0 > nb^2, v_0 > \frac{-na^2}{d}$ nên lý luận như trong chứng
định lý 7 ta có $u_1 > 0, v_1 > 0$ do đó (u_1, v_1) là nghiệm của (III) và

$$u_0 = u_1 a + dv_1 b$$
$$v_0 = u_1 b + v_1 a$$

Từ đó $v_1 < v_0$. Nếu $v_1 > nb^2, v_1 > \frac{-na^2}{d}$ thì ta lại xây dưựng được dãy $(u_2,$
nghiệm của phương trình(48) với $v_2 < v_1$. Quá trình này phải kết thúc ở bước
với $v_k \leqslant \max\left\{nb^2; \frac{-na^2}{d}\right\}$. Khi đó tồn tại i để $(u_k, v_k) = (\alpha_i, \beta_i) = (x_{0,i}, y_{0,i})$

$$u_{n-1} = au_n + dv_n b$$
$$v_{n-1} = u_n b + v_n a$$

$(u_{k-1}, v_{k-1}) = (x_{1,i}, y_{1.i}) \to (u_{k-2}, v_{k-2}) = (x_{2,i}, y_{2,i} \to \ldots \to (u_0, v_0) = (x_{k,i}$
Định lý được chứng minh

Ví dụ Chứng minh rằng phương trình $x^2 - 34y^2 = -1$ không có nghiệm.

Giải Phương trình $x^2 - 34y^2 = 1$ có nghiệm $(a, b) = (35; 6)$. Nếu phương
có nghiệm thì nghiệm nhỏ nhất (x_0, y_0) thỏa mãn $y_0^2 \leqslant \frac{(35)^2}{34} = 36,029 \to y_0$
Thử các số 1,2,3,4,5,6 ta đều không tìm được nghiệm.

Ví dụ 8. Trở lại phương trình $x^2 - 5y^2 = -4$. Phương trình $x^2 - 5y^2 =$
nghiệm $(a, b) = (9; 4)$Các nghiệm $(\alpha; \beta)$ thỏa mãn $\beta^2 \leqslant \frac{4.81}{5} = 64,8 \to \beta \leqslant$
$(1, 1)(4; 2)(11, 5)$. Vậy ta có ba dãy sau

$$x_{0,1} = 1, y_{0,1} = 1, x_{n+1,1} = 9x_{n,1} + 20y_{n,1}, \quad y_{n+1,1} = 4x_{n,1} + 9y_{n,1}$$
$$x_{0,2} = 4, y_{0,2} = 2, x_{n+1,2} = 9x_{n,2} + 20y_{n,2}, \quad y_{n+1,2} = 4x_{n,2} + 9y_{n,2}$$
$$x_{0,3} = 11, y_{0,3} = 5, x_{n+1,3} = 9x_{n,3} + 20y_{n,3}, \quad y_{n+1,3} = 4x_{n,3} + 9y_{n,3}$$

Ba dãy này vét hết nghiệm của phương trình đã cho .

Sau đây ta sẽ biện luận sự có nghiệm của một số phương trình Pell có tham

I. Biện luận phương trình

$$x^2 - 2y^2 = n$$

Bài toán đặt ra là : Tìm điều kiện cần và đủ mà n phải thỏa mãn để phương trình
có nghiệm nguyên dương. Ký hiệu $\mathcal{D}$ là tập hợp các số n như vậy.

Định lý 9 Giả sử $n = p$ là số nguyên tố. Khi đó $p \in \mathcal{D}$ khi và chỉ khi p
hoặc $p \equiv \pm 1 \pmod 8$

Chứng minh Giả sử phương trình có nghiệm (x, y) và $p \equiv \pm 3 \pmod 8$. I
chia hết cho p thì y chia hết cho p. Vế trái chia hết cho p^2 . Vô lý. Vậy $x^2 \equiv$
$\pmod p \to x^{p-1} \equiv 2^{(p-1)/2} y^{p-1} \to 2^{(p-1)/2} \equiv 1 \pmod p$ Mâu thuẫn với kết q
biết.

Đảo lại: Nếu p=2 thì (57) có nghiệm (2; 1).Xét $p \equiv \pm 1 \pmod 8$. Khi đó tồn tại $a \in \mathbb{N}$ thỏa mãn $a^2 \equiv 2 \pmod p$. Xét tập $\{x + ay\}$ trong đó $x = 0, 1, 2, ..., m; y = 0, 1, 2, ..., m$ với $m = [\sqrt{p}]$. Tập này có $(m+1)^2$ số và vì $p < (m+1)^2$ nên tồn tại $(x_1, y_1) \neq (x_2, y_2)$ để $x_1 + ay_1 \equiv x_2 + ay_2 \pmod p \to (x_1 - x_2) \equiv a(y_2 - y_1) \pmod p \to (x_1 - x_2)^2 \equiv a^2(y_2 - y_1)^2 \pmod p$. Đặt $x = |x_1 - x_2|, y = |y_1 - y_2|$. Ta có $x^2 \leqslant m^2 < p, y^2 \leqslant m^2 < p$. Ta có $x^2 \equiv a^2 y^2 \to x^2 \equiv 2y^2 \pmod p$. Vậy $x^2 - 2y^2$ chia hết cho p. Dễ thấy $x^2 - 2y^2 \neq 0, p > x^2 \geq x^2 - 2y^2 \geq -2y^2 > -2p$, do đó $x^2 - 2y^2 = -p \to (x + 2y)^2 - 2(x + y)^2 = p$. Đặt $a = x + 2y, b = x + y$ ta có (a, b) là nghiệm của (57).

Bổ đề 1 Nếu $n \in \mathcal{D}, m \in \mathcal{D}$ thì $nm \in \mathcal{D}$.

Chứng minh Giả sử $(a^2 - 2b^2) = n, (c^2 - 2d^2) = m$. Khi đó

$$nm = (a^2 - 2b^2)(c^2 - 2d^2) = (ac + 2bd)^2 - 2(bc + ad)^2$$

Điều này chứng minh $nm \in \mathcal{D}$.

Bổ đề 2 Giả sử q là số nguyên tố $q \equiv \pm 3 \pmod 8$. Nếu $x^2 - 2y^2$ chia hết cho q thì x, y đều phải chia hết cho q và do đó $x^2 - 2y^2$ chia hết cho q^2

Chứng minh Phản chứng. Giả sử trái lại. Khi đó x, y đều không chia hết cho p. Ta có

$$x^2 \equiv 2y^2 \pmod p \to x^{p-1} \equiv 2^{(p-1)/2} y^{p-1} \to 2^{(p-1)/2} \equiv 1 \pmod p.$$

Mâu thuẫn với kết quả đã biết : Nếu $p \equiv \pm 3 \pmod 8$ thì $2^{(p-1)/2} \equiv -1 \pmod p$.

Định lý 10. Giả sử n có phân tích tiêu chuẩn

$$n = \epsilon 2^r \Pi p_i^{s_i} \Pi q_i^{t_i}$$

ở đó $\epsilon = \pm 1$, p_i là các số nguyên tố dạng $8k \pm 1$, q_i là các số nguyên tố dạng $8k \pm 3$ Khi đó $n \in \mathcal{D}$ nếu và chỉ nếu t_i là số chẵn với mọi i.

Chứng minh Giả sử t_i là số chẵn với mọi i. Đặt $m = \epsilon 2^r \Pi p_i^{s_i}$. Ta có $\epsilon \in \mathcal{D}, 2 \in \mathcal{D}, p_i \in \mathcal{D}$ do đó theo bổ đề 1 $m \in \mathcal{D}$. Vậy tồn tại x, y nguyên dương sao cho $x^2 - 2y^2 = m$.Vì t_i là số chẵn với mọi t_i nên $\Pi q_i^{t_i} = h^2$. Thành thử $n = mh^2 = (xh)^2 - 2(yh)^2$. Chứng tỏ $n \in \mathcal{D}$.

Đảo lại giả sử $n \in \mathcal{D}$ tức là tồn tại x, y sao cho $x^2 - 2y^2 = n$. Giả sử q là ước nguyên tố của n , $q = 8k \pm 3$ và q có số mũ s là số lẻ. Kki đó $x^2 - 2y^2 = q^s b$ với $(b, q) = 1$. Theo bổ đề 2 $x = qx_1, y = qy_1 \to x_1^2 - 2y_1^2 = q^{s-2} b$ nếus ≥ 2. Sau một số hữu hạn bước ta dẫn đến $x_k^2 - 2y_k^2 = qb$, Theo bổ đề 2, ta có mâu thuẫn.

II. **Biện luận phương trình**

$$x^2 - 3y^2 = n \tag{58}$$

Bài toán đặt ra là : Tìm điều kiện cần và đủ mà $n \in \mathbb{Z}$ phải thỏa mãn để phương trình (58) có nghiệm nguyên dương. Ký hiệu C là tập hợp các số n như vậy.

Định lý 11. Giả sử n không chia hết cho 3. Khi đó $n \in C$ nếu và chỉ nếu a) $n \equiv 1 \pmod 3$

b) Trong phân tích tiêu chuẩn của $|n| = \Pi p_i^{s_i} \Pi q_i^{t_i}$ với $p_i \equiv \pm 1 \pmod{12}, q_i \equiv \pm 5 \pmod{12}$ thì t_i là số chẵn với mọi i.

Chứng minh Điều kiện cần: a)Giả sử $n \in C$. Tồn tại x, y nguyên dương sao cho $x^2 - 3y^2 = n \to x^2 \equiv n \pmod 3$. Vậy $n \equiv 1 \pmod 3$.

b)Ta có bổ đề sau

Bổ đề 3: Nếu q là số nguyên tố , $q_i \equiv \pm 5 \pmod{12}$ và $x^2 - 3y^2 \equiv 0$ (r thì x, y dều chia hết cho q và do đó $x^2 - 3y^2$ chia hết cho q^2

Thật vậy Giả sử trái lại. Khi đó x, y đều không chia hết cho p. Ta có

$$x^2 \equiv 3y^2 \pmod{p} \to x^{p-1} \equiv 3^{(p-1)/2} y^{p-1} \to 2^{(p-1)/2} \equiv 1 \pmod{p}$$

.Mâu thuẫn với kết quả đã biết : Nếu $p \equiv \pm 5 \pmod 8$ thì $3^{(p-1)/2} \equiv -1$ (r Bổ đề 3 được chứng minh.

Giả sử $q = q_i$ là ước nguyên tố của n , $q = 12k \pm 5$ và $q = q_i$ có số mũ là số lẻ. Kki đó $x^2 - 3y^2 = q^s b$ với $(b, q) = 1$. Theo bổ đề 3 $x = qx_1, y =$ $x_1^2 - 3y_1^2 = q^{s-2} b$ nếus ≥ 2. Sau một số hữu hạn bước ta dẫn đến $x_k^2 - 3y_k^2$ Theo bổ đề 3, ta có mâu thuẫn.

Điều kiện đủ: Giả sử các điều kiện a) và b) được thực hiện. Theo b) $n =$ trong đó hoặc $|h| = 1$ hoặc$|h| = \Pi p_i$ ở đó $p_i \equiv \pm 1 \pmod{12}$.

Nếu $|h| = 1$: Vì $n \equiv 1 \pmod 3 \to h = 1 \Leftrightarrow n = m^2$ phương trình có n $(2m, m)$. Xét $h \neq \pm 1$. Vì $n \equiv 1 \pmod 3 \to h \equiv 1 \pmod 3$ (do m^2 $\pmod 3$). Với mỗi p_i tồn tại a_i sao cho $a_i^2 \equiv 3 \pmod{p_i} \equiv \pm 1 \pmod{12}$ t a_i sao cho $a_i^2 \equiv 3 \pmod{p_i}$. Theo định lý Trung hoa tồn tại a sao cho a $\pmod{p_i}$ với mọi i. Từ đó $a^2 \equiv 3 \pmod{p_i} \quad \forall i \Leftrightarrow a^2 \equiv 3 \pmod h$. X $\{x + ay\}$ trong đó $x = 1, 2, ..., u; y = 1, 2, ..., u$ với $u = \lfloor \sqrt{h} \rfloor$. Tập này có $(u$ số và vì $h < (u+1)^2$ nên tồn tại $(x_1, y_1) \neq (x_2, y_2)$ để $x_1 + ay_1 \equiv x_2$ $\pmod h \to (x_1 - x_2) \equiv a(y_2 - y_1) \pmod h \to (x_1 - x_2)^2 \equiv a^2 (y_2 - y_1)^2$ (mc Đặt $x = |x_1 - x_2|, y = |y_1 - y_2|$. Ta có $x^2 \leqslant u^2 < h, y^2 \leqslant u^2 < h$. $x^2 \equiv a^2 y^2 \to x^2 \equiv 3y^2 \pmod h$. Vậy $x^2 - 3y^2$ chia hết cho h.

Ta có $-3h < x^2 - 3y^2 \leqslant x^2 < h$. Mà $x^2 - 3y^2 \neq 0$ nên $x^2 - 3y^2 =$ hoặc $x^2 - 3y^2 = -2h$. Nếu $x^2 - 3y^2 = -h \to h \equiv -1 \pmod 3$. Mâu t Vậy$x^2 - 3y^2 = -2h$. Khi đó x, y có cùng tính chẵn lẻ. Đặt

$$a = \frac{x + 3y}{2} . b = \frac{x + y}{2}$$

Ta có do x, y không đồng thời bằng 0 nên a, b là số nguyên dương và

$$a^2 - 3b^2 = \frac{x^2 + 6xy + 9y^2 - 3x^2 - 6xy - 3y^2}{4}$$
$$= \frac{3y^2 - x^2}{2} = \frac{2h}{h} = h$$

Vậy $(ma)^2 - 3(mb)^2 = m^2 h = n$. Nói cách khác $n \in C$. Định lý được chứng r

Bây giờ ta đi đến định lý tổng quát xét cho n bất kỳ.

Định lý 12. Giả sử $n = 3^k m$ với $(m, 3) = 1$. Khi đó $n \in C$ khi và chỉ khi

a) $m \equiv (-1)^k \pmod 3$

b) Trong phân tích tiêu chuẩn của $|m| = \Pi p_i^{s_i} \Pi q_i^{t_i}$ với $p_i \equiv \pm 1 \pmod{12}, q_i \equiv$ $\pmod{12}$ thì t_i là số chẵn.

Chứng minh Điều kiện cần: Giả sử k chẵn và tồn tại x, y sao cho $x^2 - 3$ $n = 3^k m$. Nếu $k = 0$ thì định lý 12 suy từ định lý 11. Nếu $k \geq 2$ ta có $x = 3x$ $3x_1^2 - y^2 = 3^{k-1} m \to x_1^2 - 3y_1^2 = 3^{k-2} m$. Sau một số hữu hạn bước ta đi đến

$$x_r^2 - 3y_r^2 = m$$

Theo định lý 11 ta có m thỏa mãn điều kiện a) và b)

Giả sử k lẻ. Tương tự như trên ta có $x = 3x_1 \to 3x_1^2 - y^2 = 3^{k-1}m \to x_1^2 - 3y_1^2 = 3^{k-2}m$. Sau một số hữu hạn bước ta đi đến

$$x_r^2 - 3y_r^2 = 3m \to x_r = 3u \to 3u^2 - y_r^2 = m \to y_r^2 - 3x_r^2 = -m$$

Ta có $-m$ phải thỏa mãn điều kiện a) và b) của định lý 11 tức là m thỏa mãn điều kiện a) và b) của định lý 12

Điều kiện đủ:Giả sử n thỏa mãn các điều kiện a) b)

+ Nếu k chẵn, $k = 2t$. Theo định lý 11 tồn tại x, y sao chp $x^2 - 3y^2 = m \to (3^t x)^2 - 3(3^t y)^2 = 3^{2t}m = n$. Vậy $n \in C$.

Nếu k lẻ $k = 2t + 1$. Theo định lý 11 tồn tại x, y sao cho $x^2 - 3y^2 = -m \Leftrightarrow 3y^2 - x^2 = m \to (3^{t+1}y)^2 - 3(3^t x)^2 = 3^{2t+1}m = n$. Vậy $n \in C$. Định lý 12 được chứng minh.

Bài toán tổng quát: Giải và biện luận phương trình

$$x^2 - py^2 = n$$

với p là số nguyên tố

Ta đã biện luận sựu có nghiệm của phương trình trên với $p = 2$ và $p = 3$. Trường hợp p là số nguyên tố bất kỳ theo chỗ chúng tôi biết còn đang bỏ ngỏ.

IV. Phương trình Pell tổng quát

Phương trình Pell tổng quát là phương trình

$$Ax^2 - By^2 = n \qquad \text{(IV)}$$

Trong trường hợp $n = 1$ ta có kết quả sau đây

Định lý 13. Cho phương trình

$$Ax^2 - By^2 = 1 \tag{59}$$

với AB không chính phương và $A > 1$ Gọi (a, b) là nghiệm nhỏ nhất của phương trình Pell kết hợp $x^2 - ABy^2 = 1$. Xét hệ

$$\begin{cases} a &= Ax^2 + By^2 \\ b &= 2xy \end{cases}$$

a) Nếu hệ trên có nghiệm thì nó có nghiệm duy nhất. Gọi (x_0, y_0) là nghiệm duy nhất đó. Nếu $Ax_0^2 - By_0^2 \neq -1$ thì phương trình (59) có nghiệm và (x_0, y_0) chính là nghiệm nhỏ nhất của nó.

b) Đảo lại nếu phương trình (59) có nghiệm và (x_0, y_0) là nghiệm nhỏ nhất của nó thì (x_0, y_0) là nghiệm duy nhất của hệ trên.

c) Giả sử phương trình (59) có nghiệm và (x_0, y_0) là nghiệm nhỏ nhất của nó. Với mọi số tự nhiên n tồn tại duy nhất (x_n, y_n) thỏa

$$(x_0\sqrt{A} + y_0\sqrt{B})^{2n+1} = x_n\sqrt{A} + y_n\sqrt{B}$$

Hơn nữa dãy (x_n, y_n) vét hết nghiệm của (59) .

Độc giả tự chứng minh, bằng phương pháp tương tự như chứng minh định l

Chú ý: Ta có thể mô tả nghiệm dưới dạng dãy truy hồi như sau

Ta có

$$(x_0\sqrt{A} - y_0\sqrt{B})^{2n+1} = x_n\sqrt{A} - y_n\sqrt{B}$$

Suy ra

$$x_n = \frac{(x_0\sqrt{A} + y_0\sqrt{B})^{2n+1} + (x_0\sqrt{A} - y_0\sqrt{B})^{2n+1}}{2\sqrt{A}} \to$$

$$\begin{aligned} x_n &= C_1(Ax_0^2 + By_0^2 + 2x_0y_0\sqrt{AB})^n + C_2(Ax_0^2 + By_0^2 - 2x_0y_0\sqrt{AB})^n \\ &= C_1(a + b\sqrt{AB})^n + C_2(a - b\sqrt{AB})^n \end{aligned}$$

Từ đó (x_n) là dãy truy hồi cấp 2

$$x_{n+2} = 2ax_{n+1} - x_n$$

với các giá trị ban đầu $x_0, x_1 = Ax_0^3 + 3Bx_0y_0^2$.

Tương tự (y_n) là dãy truy hồi cấp 2

$$y_{n+2} = 2ay_{n+1} - y_n$$

với các giá trị ban đầu $y_0, y_1 = By_0^3 + 3Ay_0x_0^2$.

Ví dụ Giải phương trình $3x^2 - 2y^2 = 1$

Phương trình Pell kết hợp $x^2 - 6y^2 = 1$ có nghiệm nhỏ nhất $(a, b) = (5, 2)$ Ph trình đang xét có nghiệm nhỏ nhất $(x_0, y_0) = (1, 1)$ Vậy tập nghiệm $(x_n, y_n$ phương trình được cho bởi công thức

$$x_{n+2} = 10x_{n+1} - x_n$$

với các giá trị ban đầu $x_0 = 1, x_1 = Ax_0^3 + 3Bx_0y_0^2 = 3 + 6 = 9$ và

$$y_{n+2} = 10y_{n+1} - y_n$$

với các giá trị ban đầu $y_0 = 1, y_1 = By_0^3 + 3Ay_0x_0^2 = 2 + 9 = 11$.

Định lý 14. Phương trình (IV) hoặc vô nghiệm hoặc có vô số nghiệm.

Chứng minh. Giả sử (IV) có nghiệm (x_n, y_n) tức là

$$Ax_n^2 - By_n^2 = n$$

Gọi (a, b) là nghiệm của phương trình Pell kết hợp $x^2 - ABy^2 = 1$. Khi đó ta c

$$a^2 - ABb^2 = 1$$

Nhân (40) với (41) ta được

$$\begin{aligned} &(Ax_n^2 - By_n^2)(a^2 - ABb^2) = n \\ \Leftrightarrow\ &A(x_na + By_nb)^2 - B(Ax_nb + y_na)^2 = n \end{aligned}$$

Đặt

$$\begin{aligned} x_{n+1} &= x_na + By_nb \\ y_{n+1} &= Ax_nb + y_na \end{aligned}$$

Ta thấy (x_{n+1}, y_{n+1}) là nghiệm và $x_n < x_{n+1}, y_n < y_{n+1}$. Vậy công thức (42) và (43) cho ta vô số nghiệm của (IV) nếu (IV) có một nghiệm khởi đầu (x_1, y_1).

Bằng phương pháp tương tự như định lý 7 ta có định lý sau

Định lý 15. Giả sử phương trình (IV) có nghiệm. Giả sử $(\alpha_1, \beta_1), ..., (\alpha_m, \beta_m)$ là tất cả các nghiệm của (IV) thỏa mãn bất đẳng thức

$$\beta_i^2 \leqslant \max\left\{Anb^2; \frac{-na^2}{B}\right\} \quad i = 1, 2, ..., m \tag{64}$$

Xét m dãy sau đây: dãy thứ i (i=1,2,...m) $(x_{n,i}, y_{n,i})$ xác định bởi

$$\begin{aligned} x_{0,i} &= \alpha_i, y_{0,i} = \beta_i \\ x_{n+1,i} &= x_{n,i}a + By_{n,i}b \\ y_{n+1,i} &= Ax_{n,i}b + y_{n,i}a \end{aligned}$$

Khi đó các số hạng (x_n, y_n) của tất cả các dãy trên sẽ vét hết nghiệm của (IV).

Chú ý. Có thể mô tả dưới dạng dãy truy hồi cấp 2 như sau: Để cho gọn, cố định i đặt $x_n = x_{n,i}, y_n = y_{n,i}$. ta có $x_0 = \alpha_i, x_1 = a\alpha_i + Bb\beta_i, y_0 = \beta_i, y_1 = a\beta_i + Ab\alpha_i$ và

$$\begin{aligned} x_{n+2} &= x_{n+1}a + By_{n+1}b \\ By_{n+1}b &= ABb^2x_n + Bbay_n \rightarrow \\ x_{n+2} &= x_{n+1}a + ABb^2x_n + a(x_{n+1} - x_na) = \\ &= 2ax_{n+1} - (a^2 - ABb^2)x_n = 2ax_{n+1} - x_n \end{aligned}$$

Ví dụ Giải phương trình $x^2 - 2y^2 = 7$.

Phương trình $x^2 - 2y^2 = 1$ có nghiệm nhỏ nhất $(a, b) = (3, 2)$.Ta có $\beta_i^2 \leqslant 7.2^2 = 28$. Vậy $\beta_i \in \{1, 2, 3, 4, 5\}$, Ta thấy có hai nghiệm thỏa mãn đó là $(3; 1); (5; 3)$. Vậy tất cả các nghiệm của phương trình được mô tả bởi hai dãy $(x_{n,1}, y_{n,1})$ và $(x_{n,2}, y_{n,2})$ xác định bởi công thức sau

$$x_{0,1} = 3, y_{0,1} = 1$$

$$\begin{cases} x_{n+1,1} &= 3x_{n,1} + 4y_{n,1} \\ y_{n+1,1} &= 2x_{n,1} + 3y_{n,1} \end{cases}$$

và

$$x_{0,2} = 5, y_{0,2} = 3$$

$$\begin{cases} x_{n+1,2} &= 3x_{n,2} + 4y_{n,2} \\ y_{n+1,2} &= 2x_{n,2} + 3y_{n,2} \end{cases}$$

Dãy đầu cho các nghiệm $(3; 1)(13; 9)(75, 53), ...$ .Dãy thứ hai cho các nghiệm $(5, 3)$ $(27, 19)$ $(157, 111), ...$ Cũng có thể mô tả hai dãy trên bằng dãy truy hồi cấp 2 như sau

$$\begin{cases} x_0 = 3, x_1 = 13 & x_{n+2} = 6x_{n+1} - x_n \\ y_0 = 1, y_1 = 9 & y_{n+2} = 6y_{n+1} - y_n \end{cases}$$

$$\begin{cases} x_0 = 5, x_1 = 27 & x_{n+2} = 6x_{n+1} - x_n \\ y_0 = 3, y_1 = 19 & y_{n+2} = 6y_{n+1} - y_n \end{cases}$$

LIÊN PHÂN SỐ VÀ ỨNG DỤNG

Đặng Hùng Thắng

I. Liên phân số hữu hạn

Biểu thức có dạng

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

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

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

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

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

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

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

Từ đó dễ thấy

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

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

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

Do vậy

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

Chú ý: Biểu diễn không duy nhất. Chẳng hạn

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

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

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

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

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

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

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

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

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

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

Với $k = 1$ ta có

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

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

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

Vậy

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

Định lý được chứng minh.

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

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

Định lý 1.3

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

Từ đó suy ra $(p_k, q_k) = 1$

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

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

Chứng minh Với đẳng thức thứ nhất ta có

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

Với đẳng thức thứ hai ta có

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

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

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

Định lý 1.5 Ta có

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

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

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

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

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

II. Liên phân số vô hạn

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

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

Khi đó tồn tại giới hạn

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

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

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

Chứng minh Theo định lý trên ta có

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

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

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

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

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

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

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

Định lý được chứng minh.

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

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

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

Cho $k \to \infty$ ta có mâu thuẫn.

Ngược lại ta có

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

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

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

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

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

Từ đó

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

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

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

Vậy $\alpha = [a_0; a_1, a_2, ...]$.

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

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

Chú ý rằng

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

III. Liên phân số vô hạn tuần hoàn

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

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

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

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

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

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

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

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

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

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

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

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

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

Chứng minh Giả sử

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

Tính toán cho ta

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

Định nghĩa Số vô tỷ

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

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

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

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

Bằng phép tính ta dễ thấy

Bổ đề 3.4 Ta có các hệ thức sau

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

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

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

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

Giả sử

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

Đặt

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Để chứng minh phần ngược lại ta cần bổ đề sau

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

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

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

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

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

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

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

Ta sẽ đặt

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

Khi đó tính toán cho thấy

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

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

Có thể chứng minh được rằng

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Suy ra

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

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

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

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

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

ở đó $a = [\sqrt{d}]$

Ví dụ 3.3

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

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

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

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

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

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

IV. Ap dụng vào vấn đề tính gần đúng.

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

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

thì $s \geq q_{k+1}$.

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

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

Suy ra

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

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

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

Tương tự ta có

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

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

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

Mâu thuẫn.

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

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

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

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

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

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

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

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

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

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

Trái với bổ đề.

Ví dụ 4.1 Ta có biểu diễn của π là

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

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

V. Ap dụng vào phương trình Diophant

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

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

$$ax + by = c$$

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

Xét phương trình

$$ax + by = 1$$

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

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

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

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

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

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

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

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

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

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

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

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

Ta có

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

Do vậy

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

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

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

với $t \in \mathbb{Z}$.

b) Phương trình $x^2 - dy^2 = \pm 1$

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

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

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

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

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

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

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

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

Do đó

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

Từ đó suy ra (do$\sqrt{d} \notin Q$)

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

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

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

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

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

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

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

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

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

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

Mâu thuẫn.

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

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

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

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

. Ta có

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

Vậy k phải là bội của chu kỳ r.

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

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

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

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

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

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

. Theo bổ đề 1 ta có

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

Suy ra

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

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

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

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

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

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

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

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

Giả sử $n < 0$. Khi đó

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

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

Định lý 5.2 Cho phương trình Pell

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

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

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

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

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

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

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

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

Xét phương trình

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

Ta có kết quả sau.

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

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

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

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

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

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

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

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

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

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

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

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

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

Ví dụ 6.1 Phân tích 1047 ra thừa số . Ta có $Q_1 = 13, Q_2 = 49 =$ có $p_1 \equiv (-1)^2 Q_2 \pmod{n}$, $p_1 = 129$ Vậy $(129 - 7, 1037) = (122, 103$ $61, (129 + 7, 1037) = (136, 1037) = 17$Ta có 61.17=1037.

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

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

MỘT SỐ PHƯƠNG TRÌNH ĐIOPHANT PHI TUYẾN

Đặng Hùng Thắng

I. Phương trình Pitago Phương trình Pitago là phương trình sau

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

Bộ ba số nguyên dương (x, y, z) thỏa mãn (1) được gọi là một bộ ba Pitago.

Rõ ràng nếu (x, y, z) là một bộ ba Pitago thì với mọi $d \in \mathbb{N}^*$, (dx, dy, dz) là một bộ ba Pitago. Vì thế chúng ta chỉ cần tìm các bộ ba Pitago (x, y, z) $(x, y, z) = 1$. Một bộ ba Pitago như vậy gọi là một bộ ba Pitago nguyên thủy.

Bổ đề 1 Nếu (x, y, z) là một bộ ba Pitago nguyên thủy thì x, y, z đôi một ng tố cùng nhau. Hơn nữa, x, y không cùng tính chẵn lẻ và z lẻ.

Chứng minh Giả sử $(x, y) > 1$. Nếu p là số nguyên tố với $p|x, p|y$ thì $p^2|x^2+$ $z^2 \to p|z$. Điều đó trái với giả thiết. Vậy $(x, y) = 1$. Tương tự $(x, z) = 1, (y, z)$

Vì $(x, y) = 1$ nên x, y không thể cùng chẵn. Giả sử chúng cùng lẻ. Kh $x^2 \equiv y^2 \equiv 1 \pmod 4 \to z^2 \equiv 2 \pmod 4$. Điều này không xảy ra. Vậy x, y kl cùng tính chẵn lẻ. Do đó z lẻ.

Vì vai trò của (x, y) bình đẳng nên không giảm tổng quát ta giả thiết y chẵn.

Định lý 1 Bộ ba (x, y, z) là một bộ ba Pitago nguyên thủy (với y chẵn) nế chỉ nếu nó có dạng

$$\begin{aligned} x &= m^2 - n^2 \\ y &= 2mn \\ z &= m^2 + n^2 \end{aligned}$$

trong đó m, n là các số nguyên dương $m > n, (m, n) = 1$ và m, n khác tính chẵ

Chứng minh Giả sử (x, y, z) là bộ ba Pitago nguyên thủy. Ta có $y^2 = z^2 - x$ $(z + x)(z - x)$. Vì x, z lẻ và y chẵn nên $z + x = 2l, z - x = 2t, y = 2h$. Thay ta được $h^2 = lt$.Ta có $z = l + t, x = l - t$. Theo bổ đề $(x, z) = 1 \to (l, t) = 1$. tồn tại m, n sao cho $l = m^2, t = n^2 \to h = mn$. Vậy x, y, z có biểu diễn đã Hơn nữa vì z lẻ nên m, n khác tính chẵn lẻ. Nếu có số nguyên tố p với $p|m, p|$ $p^2|m^2, p^2|n^2 \to p|x, p|z$ Mâu thuẫn. Vậy $(m, n) = 1$.

Đảo lại nếu (x, y, z) có dạng trên thì dễ kiểm tra chúng là một bộ ba Pitago chứng minh nó là một bộ ba Pitago nguyên thủy ta chỉ cần chứng minh (x, z) Thật vậy giả sử có số nguyên tố p với $p|x, p|z$. Suy ra $p|x + z = 2m^2, p|z - x =$ Vì z lẻ nên p lẻ. Vậy $p|m^2, p|n^2 \to p|m, p|n \to (m, n) > 1$. Mâu thuẫn .

Ví dụ Lấy $m = 2, n = 1$ ta được bộ ba Pitago nguyên thủy nhỏ nhất (3, Lấy $m = 5, n = 2$ Khi đó theo công thức trên ta thu được bộ ba Pitago nguyên $(21, 20, 29)$

II. Phương trình Fecma . Bên lề của một cuốn sách số học của Diophant xuất bản vào năm 1637, người ta đã tìm thấy Fecma đã viết như sau :" Phương trình $x^n + y^n = z^n$ không có nghiệm nguyên dương với $n \geq 3$. Tôi đã tìm được một cách chứng minh tuyệt diệu điều khẳng định này nhưng vì lề sách quá nhỏ nên không thể trình bày được". Phương trình $x^n + y^n = z^n$ được gọi là phương trình Fecma. Khẳng định:" Phương trình $x^n + y^n = z^n$ không có nghiệm nguyên dương với $n \geq 3$" được gọi là định lý lớn Fecma. Định lý này sau mới được chứng minh đầy đủ năm 1995 bởi Wiles. Người ta không tin Fecma đã chứng minh được định lý này một cách chính xác.

Định lý 2 Phương trình

$$x^4 + y^4 = z^2 \tag{71}$$

không có nghiệm nguyên dương. Từ đó suy ra định lý lớn Fecma đúng với $n = 4$.

Chứng minh Giả sử phương trình (2) có nghiệm. Gọi (x_0, y_0, z_0) là nghiệm sao cho z_0 là nhỏ nhất. Ta có:

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

ii) Vậy (x_0^2, y_0^2, z_0) là một bộ ba Pitago nguyên thủy. Giả sử y_0 chẵn, x_0 lẻ. Khi đó theo định lý 1 ta có

$$\begin{aligned} x_0^2 &= m^2 - n^2 \\ y_0^2 &= 2mn \\ z_0 &= m^2 + n^2 \end{aligned} \tag{72}$$

trong đó m, n là các số nguyên dương $m > n, (m, n) = 1$ và m, n khác tính chẵn lẻ.

Từ (3) suy ra (x_0, n, m) lập thành bộ ba Pitago nguyên thủy. Lại theo định lý 1

$$\begin{aligned} x_0 &= a^2 - b^2 \\ n &= 2ab \\ m &= a^2 + b^2 \end{aligned} \tag{73}$$

trong đó a, b là các số nguyên dương $a > b, (a, b) = 1$ và a, b khác tính chẵn lẻ.

Giả sử $y_0 = 2y_1$. Ta có từ (3) $y_0^2 = 4y_1^2 = 2mn = 4ab(a^2 + b^2) \to y_1^2 = ab(a^2 + b^2) = abm$. Lại có $(a, b) = 1 \to (a, m) = (b, m) = 1 \to a = a_1^2, b = b_1^2, m = m_1^2$. Thay vào (4) ta được $m_1^2 = a_1^4 + b_1^4$. Vậy (a_1, b_1, m_1) là nghiệm của (2) với $m_1 \leqslant m_1^2 = m < m^2 + n^2 = z_0$. Mâu thuẫn.

Hệ quả Định lý lớn Fecma đúng với $n = 2^s, s \geq 2$.

Thật vậy suy từ $x^{2^s} + y^{2^s} = z^{2^s} \to (x^{2^{s-2}})^4 + (y^{2^{s-2}})^4 = (z^{2^{s-2}})^4$.

Mệnh đề Nếu định lý Fecma lớn đúng cho mọi số nguyên tố lẻ p thì nó đúng với mọi $n \geq 3$.

Chứng minh Theo định lý trên ta chỉ cần chứng minh với trường hợp n có ước nguyên tố lẻ p. Giả sử $n = mp$. Khi đó $x^n + y^n = z^n \to (x^m)^p + (y^m)^p = (z^m)^p$. Mâu thuẫn vì định lý Fecma lớn đúng cho mọi số nguyên tố lẻ p.

Ole đã chứng minh định lý Fecma lớn với $n = 3$, Diricle với $n = 5$ năm 182 và Lame với $n = 7$ năm 1825. Năm 1993 đã chứng minh định lý Fecma với mọi s nguyên tố $p < 4.10^6$.

Định lý 3 Phương trình

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

không có nghiệm nguyên dương.

Chứng minh Giả sử phương trình (5) có nghiệm. Gọi (x_0, y_0, z_0) là nghiệm cho x_0 là nhỏ nhất. Ta có:

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

ii) Ta có $(x_0^2)^2 = (y_0^2)^2 + z_0^2$. Do đó (y_0^2, z_0, x_0^2) là bộ ba Pitago nguyên thủy

a) Nếu y_0 lẻ. Theo định lý 1 tồn tại m, n là các số nguyên dương $m > n, (m, n)$ và m, n khác tính chẵn lẻ sao cho $y_0^2 = m^2 - n^2, x_0^2 = m^2 + n^2$. Suy ra $m^4 - $ $(x_0 y_0)^2$. Vậy $(m, n, x_0 y_0)$ là một nghiệm của (5). Nhưng $m^2 < m^2 + n^2 = x$ $m < x_0$ Mâu thuẫn.

b) Nếu $y_0 = 2y_1$ chẵn.Theo định lý 1 tồn tại m, n là các số nguyên d $m > n, (m, n) = 1$ và m, n khác tính chẵn lẻ sao cho $y_0^2 = 2mn, x_0^2 = m^2 +$ Vậy (m, n, x_0) là một bộ ba Pitago nguyên thủy.Theo định lý 1 tồn tại các số ng dương $a > b, (a, b) = 1$ và a, b khác tính chẵn lẻ sao cho $x_0 = a^2 + b^2$ còn $a^2 - b^2, n = 2ab$ hoặc $m = 2ab, n = a^2 - b^2$. Trong mọi trường hợp ta luô $mn = 2ab(a^2 - b^2) \to y_0^2 = 2mn = 4ab(a^2 - b^2) \to y_1^2 = ab(a^2 - b^2)$. Vì (a, b) nên $(a, a^2 - b^2) = 1; (b, a^2 - b^2) = 1$. Vậy $a = a_1^2, b = b_1^2, a^2 - b^2 = r^2 \to a_1^4 - b_1^4 =$ Vậy (a_1, b_1, r) là nghiệm của (5). Nhưng $a_1 < a_1^2 + b_1^2 = a + b \leqslant a^2 + b^2 =$ Mâu thuẫn với cách chọn x_0 là nhỏ nhất.

Ví dụ 1 Chứng minh rằng phương trình $x^4 - 4y^4 = z^2$ không có nghiệm ng dương.

Giải Giả sử phương trình có nghiệm. Gọi (x_0, y_0, z_0) là nghiệm với z_0 bé Tương tự như trên ta có $(x_0, y_0) = 1$. Giả sử x_0 chẵn $x_0 = 2k$. Thay vào 16 $4y_0^4 = z_0^2 \to z_0 = 2h, 4k^4 - y_0^4 = h^2$. Vì $(x_0, y_0) = 1$ nên y_0 lẻ. Vậy y_0^4 $(\text{mod } 4) \to h^2 \equiv -1 \ (\text{mod } 4)$ không xảy ra. Vậy x_0 lẻ. Ta có $(x_0^2)^2 = z_0^2 + (2$ Do x_0 lẻ và $(x_0, y_0) = 1$ nên $(x_0^2, 2y_0^2) = 1$. Suy ra $(z^2, 2y_0^2, x_0^2)$ là bộ ba P nguyên thủy. Do đó tồn tại các số nguyên dương $a > b, (a, b) = 1$ và a, b khác chẵn lẻ sao cho $2y_0^2 = 2ab, x_0^2 = a^2 + b^2 \to a = r^2, b = s^2 \to x_0^2 = r^4 + s^4$ trá định lý 2.

Ví dụ 2 Chứng minh rằng phương trình $x^4 + 4y^4 = z^2$ không có nghiệm ng dương.

Giải Giả sử phương trình có nghiệm. Gọi (x_0, y_0, z_0) là nghiệm với z nhất.Tương tự như trên ta có $(x_0, y_0) = 1$.Giả sử x_0 chẵn $x_0 = 2k$. Thay $16k^4 + 4y_0^4 = z_0^2 \to z_0 = 2h, 4k^4 + y_0^4 = h^2$. Vậy (y_0, k, h) là nghiệm $h < 2h = z_0$. Mâu thuẫn.Vậy x_0 lẻ. Ta có $(x_0^2)^2 + (2y_0^2)^2 = z_0^2$. Do x_0 l $(x_0, y_0) = 1$ nên $(x_0^2, 2y_0^2) = 1$. Suy ra $(x_0^2, 2y_0^2, z_0)$ là bộ ba Pitago nguyên thủy đó tồn tại các số nguyên dương $a > b, (a, b) = 1$ và a, b khác tính chẵn lẻ sao $2y_0^2 = 2ab, x_0^2 = a^2 - b^2 \to a = r^2, b = s^2 \to x_0^2 = r^4 - s^4$ trái với định lý 3.

Ví dụ 3 Giải các phương trình:

1. $x^4 - 2y^4 = 1$
2. $x^4 - 2y^4 = -1$

Giải

1. $x^4 - 2y^4 = 1 \Leftrightarrow x^4 + (y^2)^4 = (y^4+1)^2$. Từ định lý 2 suy ra phương trình vô nghiệm.

2. $x^4 - 2y^4 = -1 \Leftrightarrow (y^2)^4 - x^4 = (y^4-1)^2$. Từ định lý 3 suy ra ta phải có $(y^4-1) = 0 \rightarrow y = 1 \rightarrow x = 1$. Vậy phương trình có nghiệm duy nhất $x = y = 1$.

III. Phương trình kiểu Fecma

Xét bài toán sau: Cho số nguyên dương $n \geq 2$. Tìm tất cả các số nguyên dương (a, b, c) phân biệt sao cho a^n, b^n, c^n là một cấp số cộng.

Bài toán này tương đương với tìm nghiệm nguyên dương $x \neq y$ của phương trình

$$x^n + y^n = 2z^n. \tag{75}$$

Phương trình (6) gọi là phương trình kiểu Fecma(Fermat-like equations).

1. Xét trường hợp $n = 2$. Phương trình (6) trở thành $x^2 + y^2 = 2z^2$. Ta chỉ cần xét bộ nghiệm (x, y, z) nguyên thủy tức là $(x, y, z) = 1$. Ta có x, y không cùng chẵn.Giả sử x lẻ. Suy ra y lẻ. Vậy vế trái đồng dư 2 mod 4 vậy z lẻ. Nếu $p|x, p|y \rightarrow p|z \rightarrow p = 1$. Vậy $(x, y) = 1$. Giả sử $x > y$.Đặt $u = (x+y)/2, v = (x-y)/2 \rightarrow u^2 + v^2 = z^2$. Từ $(x, y) = 1, x = u + v, y = u - v \rightarrow (u, v) = 1$. Vậy (u, v, z) là bộ ba Pitago nguyên thủy. Vậy

$$\begin{aligned} u &= m^2 - n^2 (= 2mn) \\ v &= 2mn (= m^2 - n^2) \\ z &= m^2 + n^2 \end{aligned}$$

trong đó m, n là các số nguyên dương $m > n, (m, n) = 1$ và m, n khác tính chẵn lẻ hay

$$\begin{aligned} x &= m^2 - n^2 + 2mn = (m+n)^2 - 2n^2 \\ z &= m^2 + n^2 \end{aligned}$$

Vì vai trò x, y bình đẳng nên ta kết luận nghiệm là

$$\begin{aligned} x &= (m+n)^2 - 2n^2 \\ y &= (m+n)^2 - 2m^2 \\ z &= m^2 + n^2 \end{aligned}$$

ở đó m, n là các số nguyên dương nguyên tố cùng nhau và m, n khác tính chẵn lẻ .

Với $m = 2, n = 1$ ta được bộ ba số chính phương $(1, 25, 49)$ lập thành một cấp số cộng.

2. Xét trường hợp $n > 2$. Fecma đã chứng minh rằng ba số dạng a^4, b^4, c^4 không thể lập thnhf cấp số cộng. Euler chứng minh rằng 3 số dạng a^3, b^3, c^3 không thể lập thành cấp số cộng. Mới đây (1997) Merel và Darmon đã chứng minh

với mọi $n > 2$ không tồn tại ba số nguyên dương (a, b, c) phân biệt sao a^n, b^n, c^n là một cấp số cộng.

Chú thích Nhà toán học Euler đã phỏng đoán rằng phương trình Fecma c biến

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

cũng không có nghiệm. Tuy nhiên năm 1988 nhà toán học Elkies đã chỉ ra phỏng đoán trên là sai bằng cách chỉ ra một nghiệm sau đây

$$2682440^4 + 15365639^4 + 18796760^4 = 20615673^4.$$

IV. Biểu diễn số nguyên dương thành tổng các bình phương

Các nhà toán học của nhiều thời đại đã quan tâm tới bài toán biểu diễn số nguyên dương thàng tổng các bình phương (tổng các số chính phương). phant,Ferma,Euler, Gauss và Lagrange là những nhà toán học đã có đóng góp lớ bài toán này.

1. Biểu diễn số nguyên dương thành tổng của hai bình phươ

Ta xét bài toán: Số nguyên dương nào biểu diễn được thành tổng của hai phương tức là

Với n nào thì phương trình $x^2 + y^2 = n$ có nghiệm $x, y \in \mathbb{N}$.

Định lý 4 Cho p là số nguyên tố. Khi đó phương trình $x^2 + y^2 = p$ có ng tự nhiên khi và chỉ khi p không có dạng $4k + 3$.

Chứng minh Giả sử phương trình có nghiệm (x, y). Nếu $p = 4k+3 \to p|x, p$ $p^2|p$. Mâu thuẫn. Ngược lại giả sử p không có dạng $4k + 3$. Nếu $p = 2$ thì (là nghiệm. Xét $p = 4k + 1$.Vì -1 là số chính phương(mod p) nên tồn tại $a \in$ $a^2 \equiv -1 \pmod{p}$. Đặt $q = [\sqrt{p}]$. Xét $(q+1)^2$ số sau $\{x + ay\}, x = 0, 1, ..., q$ $0, 1, ..., q$. Vì $(q+1)^2 > p$ nên tồn tại $(x_1, y_1) \neq (x_2, y_2)$ sao cho $x_1 + ay_1 \equiv x_2 -$ $\pmod{p} \to (x_1 - x_2) \equiv a(y_2 - y_1) \pmod{p} \to u^2 \equiv a^2v^2 \equiv -v^2 \pmod{p}$ $u^2 + v^2 \equiv 0 \pmod{p}$ ở đó $u = |x_1 - x_2| \leqslant q < \sqrt{p}$; $v = |y_1 - y_2| \leqslant q < \sqrt{p}$. $u^2 + v^2$ chia hết cho p . Vì $0 < u^2 + v^2 < p + p = 2p$ nên suy ra $u^2 + v^2 = p$.

Bổ đề 2 Nếu $p \equiv 3 \pmod{4}, p|x^2 + y^2$ thì $p|x \quad p|y$.

Thật vậy nếu trái lại thì $(x, p) = (y, p) = 1 \to x^2 \equiv -y^2 \pmod{} \to x^{p-}$ $(-1)^{(p-1)/2}x^{p-1} \to (-1)^{(p-1)/2} \equiv 1 \pmod{p} \to -1 \equiv 1 \pmod{p}$. Mâu thuẫn.

Bổ đề 3 Nếu n, m biểu diễn được thành tổng của hai bình phương thì mn biểu diễn được thành tổng của hai bình phương .

Thật vậy nếu $m = a^2 + b^2, n = c^2 + d^2$ thì $mn = (a^2 + b^2)(c^2 + d^2) = ($ $bd)^2 + (ad - bc)^2$

Định lý 5 Cho $n > 1$ là số nguyên dương với phân tích tiêu chuẩn

$$n = 2^r \Pi p_i^{s_i} \Pi q_i^{t_i}$$

trong đó $p_i \equiv 1 \pmod{4}, q_i \equiv 3 \pmod{4}$.

Khi đó n biểu diễn được thành tổng của hai bình phương khi và chỉ khi t_i chẵn với mọi i.

Chứng minh Điều kiện cần: Giả sử n biểu diễn được thành tổng của hai phương và giả sử q là ước nguyên tố của n , $q = 4k+3$ và q có số mũ t là số lẻ. K $n = x^2 + y^2 = q^t b$ với $(b, q) = 1$. Theo bổ đề 2 $x = qx_1, y = qy_1 \to x_1^2 + y_1^2 =$

nếu$t \geq 2$. Sau một số hữu hạn bước ta dẫn đến $x_k^2 + y_k^2 = qb$, Theo bổ đề 1, ta có mâu thuẫn.

Điều kiện đủ:Gọi $\mathcal{D}$ là tập các số n biểu diễn được thành tổng của hai bình phương . Giả sử t_i là số chẵn với mọi i. Đặt $m = 2^r \Pi p_i^{s_i}$. Ta có $2 \in \mathcal{D}, p_i \in \mathcal{D}$ do đó theo bổ đề 2 $m \in \mathcal{D}$. Vậy tồn tại x, y nguyên dương sao cho $x^2 + y^2 = m$.Vì t_i là số chẵn với mọi t_i nên $\Pi q_i^{t_i} = h^2$. Thành thử $n = mh^2 = (xh)^2 + (yh)^2$. Chứng tỏ $n \in \mathcal{D}$.

2. Biểu diễn số nguyên dương thành tổng của ba bình phương

Ta xét bài toán: Số nguyên dương nào biểu diễn được thành tổng của ba bình phương tức là

Với n nào thì phương trình $x^2 + y^2 + z^2 = n$ có nghiệm $x, y, z \in \mathbb{N}$.

Định lý 6 Nếu n có dạng $n = 4^m(8k+7), m, k \in \mathbb{N}$ thì n không biểu diễn được thành tổng của ba bình phương.

Chứng minh Giả sử trái lại $n = 4^m(8k+7) = x^2 + y^2 + z^2$. Ta thấy $x^2 \equiv a \in \{0;1;4\} \pmod 8$ do đó $n = x^2 + y^2 + z^2 \equiv a \in \{0,1,2,3,4,5,6\} \pmod 8$. Nếu $m > 0$ thì $n \equiv 0 \pmod 4$ do đó $x^2 + y^2 + z^2 \equiv a \in \{0,4\} \pmod 8 \rightarrow x^2 + y^2 + z^2 \equiv 0 \pmod 4$. Vì $x^2 \equiv a \in \{0;1;\} \pmod 4$ suy ra $x^2 \equiv y^2 \equiv z^2 \equiv 0 \pmod 4 \rightarrow x = 2x_1, y = 2y_1, z = 2z_1 \rightarrow x_1^2 + y_1^2 + z_1^2 = 4^{m-1}(8k+7)$. Tiếp tục như thế ta dẫn đến $x_m^2 + y_m^2 + z_m^2 = 8k + 7 \equiv 7 \pmod 8$. Mâu thuẫn.

Điều ngược lại cũng đúng tức là nếu n không có dạng $n = 4^m(8k+7), m, k \in \mathbb{N}$ thì n biểu diễn được thành tổng của ba bình phương. Chứng minh khó nên ta công nhận. Như vậy ta có định lý sau

Định lý 7 Số nguyên dương n biểu diễn được thành tổng của ba bình phương khi và chỉ khi $n \neq 4^m(8k+7)$ với $k, m \in \mathbb{N}$

Tiếp theo ta xét bài toán :Biểu diễn được thành tổng của ba bình phương, trong đó có hai bình phương trùng nhau tức là tìm n để phương trình $n = x^2 + 2y^2$ có nghiệm tự nhiên.

Bổ đề 4 Nếu $p|x^2 + 2y^2$ và p là số nguyên tố $p \equiv a \in \{5,7\} \pmod 8$ thì $p|x \quad p|y$ Thật vậy nếu trái lại thì $(x,p) = (y,p) = 1 \rightarrow x^2 \equiv -2y^2 \pmod \rightarrow x^{p-1} \equiv (-2)^{(p-1)/2} y^{p-1} \rightarrow (-1)^{(p-1)/2} 2^{p-1/2} \equiv 1 \pmod p$. Nếu $p = 8k+5$ thì 2 là số không chính phương (mod p) còn $p - 1/2 = 4k+2$ chẵn do đó $(-1)^{(p-1)/2} 2^{p-1/2} \equiv -1 \pmod p$. Mâu thuẫn. Nếu $p = 8k+7$ thì 2 là số chính phương(mod p) còn $(p-1)/2 = 4k+3$ lẻ do đó $(-1)^{(p-1)/2} 2^{p-1/2} \equiv -1 \pmod p$. Mâu thuẫn.

Ký hiệu $\mathcal{D}$ là tập hợp các số n để phương trình $n = x^2 + 2y^2$ có nghiệm tự nhiên

Định lý 8 Giả sử $n = p$ là số nguyên tố. Khi đó $p \in \mathcal{D}$ khi và chỉ khi $p = 2$ hoặc $p \equiv 1, 3 \pmod 8$

Chứng minh Giả sử phương trình có nghiệm (x,y) và $p \equiv \pm 5, 7 \pmod 8$. Theo bổ đề 1 x chia hết cho p , y chia hết cho p. Vế trái chia hết cho p^2 . Vô lý Đảo lại: Nếu $p = 2$ thì $2 = 0^2 + 2.1^2$.Xét $p \equiv 1, 3 \pmod 8$. Khi đó -2 là số chính phương (mod p) (Suy từ 2 là chính phương (mod p) khi và chỉ khi $p \equiv \pm 1 \pmod 8$). Vậy tồn tại $a \in \mathbb{N}$ thỏa mãn $a^2 \equiv -2 \pmod p$. Xét tập $\{x + ay\}$ trong đó $x = 1, 2, ..., m; y = 1, 2, ..., m$ với $m = \lfloor \sqrt{p} \rfloor$. Tập này có $(m+1)^2$ số và vì $p < (m+1)^2$ nên tồn tại $(x_1, y_1) \neq (x_2, y_2)$ để $x_1 + ay_1 \equiv x_2 + ay_2 \pmod p \rightarrow (x_1 - x_2) \equiv a(y_2 - y_1) \pmod p \rightarrow (x_1 - x_2)^2 \equiv a^2(y_2 - y_1)^2 \pmod p$ Đặt $x = |x_1 - x_2|, y = |y_1 - y_2|$. Ta có $x^2 \leqslant m^2 < q, y^2 \leqslant m^2 < q$. Ta có $x^2 \equiv a^2 y^2 \rightarrow x^2 \equiv -2y^2 \pmod p$. Vậy $x^2 + 2y^2$ chia hết cho p. Dễ thấy $0 < x^2 + 2y^2 < p + 2p = 3p$ do đó $x^2 + 2y^2 = p$(dpcm) hoặc $x^2 + 2y^2 = 2p$. Nếu

trường hợp này xảy ra thì $x = 2z \to 4z^2 + 2y^2 = 2p \to y^2 + 2z^2 = p$. ta có p diễn dược.

Bổ đề 5 Nếu $n \in \mathcal{D}, m \in \mathcal{D}$ thì $nm \in \mathcal{D}$.

Chứng minh Giả sử $n = a^2 + 2b^2, m = c^2 + 2d^2$. Khi đó

$$nm = (a^2 + 2b^2)(c^2 + 2d^2) = (ac - 2bd)^2 + 2(bc + ad)^2$$

Điều này chứng minh $nm \in \mathcal{D}$.

Định lý 9. Giả sử n có phân tích tiêu chuẩn

$$n = 2^r \Pi p_i^{s_i} \Pi q_i^{t_i}$$

ở đó p_i là các số nguyên tố dạng $8k+1, 8k+3$, q_i là các số nguyên tố dạng $8k+5, 8$ Khi đó $n \in \mathcal{D}$ nếu và chỉ nếu t_i là số chẵn với mọi i.

Chứng minh Giả sử t_i là số chẵn với mọi i. Đặt $m = 2^r \Pi p_i^{s_i}$. Ta có $2 \in \mathcal{D}$ $\mathcal{D}$ do đó theo bổ đề 1 $m \in \mathcal{D}$. Vậy tồn tại x, y nguyên dương sao cho $x^2 + 2y^2 =$ t_i là số chẵn với mọi t_i nên $\Pi q_i^{t_i} = h^2$. Thành thử $n = mh^2 = (xh)^2 + 2(yh)^2$. C tỏ $n \in \mathcal{D}$.

Đảo lại giả sử $n \in \mathcal{D}$ tức là tồn tại x, y sao cho $x^2 + 2y^2 = n$. Giả sử q l nguyên tố của n , $q = 8k + 3, 8k + 7$ và q có số mũ t là số lẻ. Kki đó $x^2 + 2y^2$ với $(b, q) = 1$. Theo bổ đề 2 $x = qx_1, y = qy_1 \to x_1^2 + 2y_1^2 = q^{s-2}b$ nếu $s \geq 2$ một số hữu hạn bước ta dẫn đến $x_k^2 + 2y_k^2 = qb$, Theo bổ đề 2, ta có mâu thuẫn

Ví dụ $14 = 1^2 + 2^2 + 3^2$ là tổng của 3 bình phương nhưng $14 = 2.7$ và $7 = 8$ có số mũ lẻ nên phương trình $14 = x^2 + 2y^2$ vô nghiệm.

3. Biểu diễn số nguyên dương thành tổng của bốn bình phư

Nếu một số không biểu diễn thành tổng của hai hay ba bình phương thì li có thể thành tổng của bốn bình phương hay không? Câu trả lời là:□*Mọi số ng dương đều biểu diễn được thành tổng của bốn bình phương*□. Đó là đị nổi tiếng của Lagrange. Sau đây ta sẽ chứng minh định lý này.

Ký hiệu $\mathcal{D}$ là tập hợp các số n sao cho n biểu diễn được thành tổng của bốn phương tức là để phương trình $n = x^2 + y^2 + z^2 + t^2$ có nghiệm tự nhiên.

Bổ đề 1. Nếu $m \in \mathcal{D}, n \in \mathcal{D}$ thì $mn \in \mathcal{D}$.

Chứng minh Giả sử $m = a^2 + b^2 + c^2 + d^2, n = e^2 + f^2 + g^2 + h^2$. Khi đó hằng đẳng thức sau

$$mn = (ae + bf + cg + dh)^2 + (af - be + ch - dg)^2$$
$$+(ag - bh - ce + df)^2 + (ah + bg - cf - de)^2$$

Vậy $mn \in \mathcal{D}$.

Chẳng hạn $7 = 2^1 + 1^1 + 1^1 + 1^1, 10 = 3^1 + 1^1 + 0^0 + 0^0$ thì áp dụng công trên cho ta $70 = 7^2 + 1^2 + 2^2 + 4^2$.

Sau đây ta sẽ chứng minh với mọi số nguyên tố p ta có $p \in \mathcal{D}$. Vì $2 = 1^1 +$ $0^0 + 0^0 \in \mathcal{D}$ nên ta chỉ cần xét $p \geq 3$.

Bổ đề 2 Cho p là số nguyên tố lẻ. Khi đó tồn tại $1 \leqslant k < p$ để $kp \in \mathcal{D}$.

Chứng minh Xét tập $A = \{x^2\}, x = 0, 1, 2, ..., (p-1)/2 \quad B = \{-y^2 - 1$ $0, 1, 2, ..., (p-1)/2$. Các số của A phân biệt (mod p), các số của B phân biệt (n và $|A| + |B| = p + 1$ nên tập $A \cup B$ không thể gồm $p+1$ số phân biệt mod p. V

tại $x, y \in \{0, 1, 2, ..., (p-1)/2\}$ sao cho $x^2 \equiv -y^2 - 1 \pmod{p} \to x^2 + y_1^2 = kp \to kp = x^2 + y^2 + 1^2 + 0^2$. Vậy $kp \in \mathcal{D}$. Lại có $kp = x^2 + y_1^2 < p^2/2 + p^2/2 + 1 = p^2/2 + 1 < p^2 \to k < p$.

Ký hiệu $M = \{1 \leqslant k < p | kp \in \mathcal{D}\}$. Theo bổ đề 2 M khác rỗng. Giả sử m là số nhỏ nhất của m.

Định lý 10 $m = 1$. Suy ra với mọi số nguyên tố p ta có $p \in \mathcal{D}$.

Chứng minh Giả sử trái lại $1 < m < p$. Vì $mp \in \mathcal{D}$ nên $mp = x^2 + y^2 + z^2 + t^2$.

i) Nếu m chẵn: Khi đó $mp = x^2 + y^2 + z^2 + t^2 \equiv a \in \{0, 2\} \pmod{4}$. Vì $x^2 \equiv 0 \pmod{4}$ nếu x chẵn và $x^2 \equiv 1 \pmod{4}$ nếu x lẻ nên số các số lẻ trong 4 số (x, y, z, t) là 0,2 hoặc 4, tức là hoặc tất cả chẵn, hoặc tất cả lẻ, hoặc hai chẵn,hai lẻ. Nếu tất cả chẵn, hoặc tất cả lẻ thì 4 số $(x+y)/2, (x-y)/2, (z+t)/2, (z-t)/2 \in \mathbb{Z}$ và

$$(x+y)^2/4 + (x-y)^2/4, (z+t)^2/4, (z-t)^2/4 = \frac{x^2+y^2+z^2+t^2}{2} = \frac{m}{2}p$$

Vậy $(m/2)p \in \mathcal{D} \Leftrightarrow m/2 \in M$. Mâu thuẫn với việc m là số nhỏ nhất của M.

Nếu có hai số chẵn,hai số lẻ chẳng hạn x, y chẵn và z, t lẻ thì ta cũng có 4 số $(x+y)/2, (x-y)/2, (z+t)/2, (z-t)/2 \in \mathbb{Z}$ và lập luận như trên cũng dẫn tới mâu thuẫn.

i) Nếu m lẻ: Xét tập $S = \{0, \pm 1, \pm 2, ..., \pm(m-1)/2\}$. S là một hệ đầy đủ (mod m). Vậy tồn tại các số $a, b, c, d \in S$ sao cho $x \equiv a \pmod{m}; y \equiv b \pmod{m}, z \equiv c \pmod{m}, t \equiv d \pmod{m}$. Suy ra $a^2 + b^2 + c^2 + d^2 \equiv x^2 + y^2 + z^2 + t^2 = mp \equiv 0 \pmod{m}$. Vậy tồn tai $k \in \mathbb{N}$ sao cho

$$a^2 + b^2 + c^2 + d^2 = km$$

Vì $a^2 + b^2 + c^2 + d^2 < m^2/4 + m^2/4 + m^2/4 + m^2/4 = m^2 \to 0 \leqslant k < m$.

+Nếu $k = 0 \to a = b = c = 0 \to x \equiv y \equiv z \equiv t \equiv 0 \pmod{m}$. Vậy $m^2 | x^2 + y^2 + z^2 + t^2 = mp \to m | p \to m = p \to m \geq p$ (do $m > 1$ và p nguyên tố). Mâu thuẫn .

+ Vậy $1 \leqslant k < m$. Ta có

$$\begin{aligned}(mp)(km) &= (x^2 + y^2 + z^2 + t^2)(a^2 + b^2 + c^2 + d^2) \\ &= (ax + by + cz + dt)^2 + (bx - ay + dz - ct)^2 \\ &= (cx - dy - az + bt)^2 + (dx + cy - bz - at)^2\end{aligned}$$

Ta có

$$\begin{aligned}X &= ax + by + cz + dt \equiv a^2 + b^2 + c^2 + d^2 \equiv 0 \pmod{m} \\ Y &= bx - ay + dz - ct \equiv ab - ab + dc - cd = 0 \pmod{m} \\ Z &= cx - dy - az + bt \equiv ca - db - ac + bd = 0 \pmod{m} \\ T &= dx + cy - bz - at \equiv da + cb - bc - ad = 0 \pmod{m}\end{aligned}$$

Suy ra

$$\begin{aligned}&X^2 + Y^2 + Z^2 + T^2 = m^2(X_1^2 + Y_1^2 + Z_1^2 + T_1^2) = m^2 kp \\ &\to X_1^2 + Y_1^2 + Z_1^2 + T_1^2 = kp\end{aligned}$$

Vậy $kp \in \mathcal{D} \Leftrightarrow k \in M$. Mâu thuẫn với việc m là số nhỏ nhất của M.

Từ định lý 2 và bổ đề 1 ta rút ra

Định lý 11(Lagrande) Mọi số nguyên dương đều biểu diễn được thành tổn bốn bình phương.

Tiếp theo ta xét bài toán : Số nguyên dương nào biểu diễn được thành tổn bốn bình phương, trong đó có ba bình phương trùng nhau tức là tìm n để phương $n = x^2 + 3y^2$ có nghiệm tự nhiên.

Bổ đề 1 Nếu $p|x^2 + 3y^2$ và p là số nguyên tố $p \equiv 2 \pmod 3$ thì $p|x$ Thật vậy nếu trái lại thì $(x, p) = (y, p) = 1 \to x^2 \equiv -3y^2 \pmod{} \to)x^p$ $(-3)^{(p-1)/2}y^{p-1} \to (-1)^{(p-1)/2}3^{p-1/2} \equiv 1 \pmod p$. Vì $p = 3k+2$ nên $p = 12$ hoặc $p = 12k + 11$. Nếu $p = 12h + 5$ thì 3 là số không chính phương (mod p $p - 1/2 = 6k + 4$ chẵn do đó $(-1)^{(p-1)/2}3^{p-1/2} \equiv -1 \pmod p$. Mâu thuẫn. $p = 12k + 11$ thì 3 là số chính phương(mod p) còn $(p - 1)/2 = 6k + 5$ lẻ $(-1)^{(p-1)/2}3^{p-1/2} \equiv -1 \pmod p$. Mâu thuẫn.

Ký hiệu $\mathcal{D}$ là tập hợp các số n để phương trình $n = x^2 + 3y^2$ có nghiệm tự r

Định lý 12 Giả sử $n = p$ là số nguyên tố. Khi đó $p \in \mathcal{D}$ khi và chỉ khi p hoặc $p \equiv 1 \pmod 3$

Chứng minh Giả sử phương trình có nghiệm (x, y) và $p \equiv 2 \pmod 3$. Th đề 1 x chia hết cho p , y chia hết cho p. Vế trái chia hết cho p^2 . Vô lý. Đảo lại $p = 3$ thì $3 = 0^2 + 3.1^2$.Xét $p \equiv 1 \pmod 3$. Khi đó -3 là số chính phương (m (Suy từ 3 là chính phương (mod p) khi và chỉ khi $p \equiv \pm 1 \pmod 1)2)$. Vậy t $a \in \mathbb{N}$ thỏa mãn $a^2 \equiv -3 \pmod p$. Xét tập $\{x + ay\}$ trong đó $x = 1, 2, ..., m$ $1, 2, ..., m$ với $m = \lfloor \sqrt{p} \rfloor$. Tập này có $(m + 1)^2$ số và vì $p < (m + 1)^2$ nên t $(x_1, y_1) \neq (x_2, y_2)$ để $x_1 + ay_1 \equiv x_2 + ay_2 \pmod p \to (x_1 - x_2) \equiv a(y_2$ $\pmod p \to (x_1 - x_2)^2 \equiv a^2(y_2 - y_1)^2 \pmod p$. Đặt $x = |x_1 - x_2|, y = |y_1$. Ta có $x^2 \leqslant m^2 < q, y^2 \leqslant m^2 < q$. Ta có $x^2 \equiv a^2y^2 \to x^2 \equiv -3y^2 \pmod p$ x^2+3y^2 chia hết cho p. Dễ thấy $0 < x^2+2y^2 < p+3p = 4p$ do đó $x^2+3y^2 = p($ hoặc $x^2 + 3y^2 = 2p$ hoặc$x^2 + 3y^2 = 3p$. Nếu $x^2 + 2y^2 = 2p$ xảy ra thì x, y tính chẵn lẻ. Suy ra $x^2 + 3y^2 \equiv 0 \pmod 4 \to 2|p$. Mâu thuẫn. Nếu $x^2 + 3y^2$ thì $x = 3z \to 9z^2 + 3y^2 = 3p \to y^2 + 3z^2 = p \to p \in \mathcal{D}$.

Bổ đề 2 Nếu $n \in \mathcal{D}, m \in \mathcal{D}$ thì $nm \in \mathcal{D}$.

Chứng minh Giả sử $n = a^2 + 3b^2, m = c^2 + 3d^2$. Khi đó

$$nm = (a^2 + 3b^2)(c^2 + 3d^2) = (ac - 3bd)^2 + 3(bc + ad)^2$$

Điều này chứng minh $nm \in \mathcal{D}$.

Định lý 13. Giả sử n có phân tích tiêu chuẩn

$$n = 3^r \Pi p_i^{s_i} \Pi q_i^{t_i}$$

ở đó p_i là các số nguyên tố dạng $3k + 1$, q_i là các số nguyên tố dạng $3k + 2$ K $n \in \mathcal{D}$ nếu và chỉ nếu t_i là số chẵn với mọi i.

Chứng minh Giả sử t_i là số chẵn với mọi i. Đặt $m = 3^r \Pi p_i^{s_i}$. Ta có $3 \in \mathcal{D}$ $\mathcal{D}$ do đó theo bổ đề 1 $m \in \mathcal{D}$. Vậy tồn tại x, y nguyên dương sao cho $x^2+3y^2 =$ t_i là số chẵn với mọi t_i nên $\Pi q_i^{t_i} = h^2$. Thành thử $n = mh^2 = (xh)^2+3(yh)^2$. (tỏ $n \in \mathcal{D}$.

Đảo lại giả sử $n \in \mathcal{D}$ tức là tồn tại x, y sao cho $x^2 + 3y^2 = n$. Giả sử q l nguyên tố của n , $q = 3k + 2$ và q có số mũ t là số lẻ. Kki đó $x^2 + 3y^2 = q$

$(b,q)=1$. Theo bổ đề 2 $x=qx_1, y=qy_1 \to x_1^2+3y_1^2=q^{s-2}b$ nếu $s\geq 2$. Sau một số hữu hạn bước ta dẫn đến $x_k^2+3y_k^2=qb$, Theo bổ đề 2 suy ra vế trái chia hết cho q^2. Ta có mâu thuẫn.

4. Bài toán Waring: Biểu diễn một số thành tổng các lũy thừa k.

Vào thế kỷ 18 nhà toán học Anh Waring đã phỏng đoán rằng, mọi số nguyên dương đều biểu diễn được thành tổng của 9 lập phương các số tự nhiên và đều biểu diễn được thành tổng của 19 lũy thừa 4 các số tự nhiên, tức là với mọi $n\in\mathbb{N}^*$ các phương trình

$$x_1^3+x_2^3+\cdots+x_9^3=n$$

$$x_1^4+x_2^3+\cdots+x_{19}^4=n$$

luôn có nghiệm tự nhiên. Ông đã nêu giả thiết sau

Cho số nguyên dương k. Khi đó có tồn tại số nguyên dương m (phụ thuộc vào k) sao cho mọi số nguyên dương n đều biểu diễn được thành tổng của m số , mỗi số có dạng $x^k, x\in\mathbb{N}$ tức là:

Tồn tại số nguyên dương m sao cho với mọi số nguyên dương n phương trình

$$\sum_{i=1}^{m} x_i^k=n$$

có nghiệm tự nhiên.

Năm 1906 nhà toán học lỗi lạc Davit Hilbert đã chứng minh được phỏng đoán trên. Chứng minh của ông cực kỳ phức tạp.

Gọi $g(k)$ là số m nhỏ nhất có tính chất trên tức là mọi số nguyên dương n đều biểu diễn được thành tổng của $g(k)$ số, mỗi số có dạng $x^k, x\in\mathbb{N}$ và tồn tại số n không biểu diễn được thành tổng của $m-1$ số , mỗi số có dạng $x^k, x\in\mathbb{N}$. Ta có $g(2)=4$ (vì số 7 không biểu diễn được thành tổng của 3 bình phương và mọi số nguyên dương n đều biểu diễn được thành tổng của bốn bình phương).Đến nay người ta đã chứng minh được $g(3)=9, g(4)\geqslant 19, g(5)=37$ và với $6\leqslant 471600000$ thì

$$g(k)=[(3/2)^k]+2^k-2.$$

Vẫn còn nhiều câu hỏi mở xung quanh hàm $g(k)$.

V. Biểu diễn một số thành tổng các bình phương nguyên dương

1. Tổng của hai bình phương nguyên dương

Một số có thể là tổng của hai bình phương song có thể một số bằng 0 (chẳng hạn $9=3^2, 16=4^2$ nhưng không thể có $9=a^2+b^2, 16=c^2+d^2$ với a,b nguyên dương.Định lý 1 có thể phát biểu cách khác là: Để một số ngưuyên dương$n$ biểu diễn được thành tổng của không quá hai bình phương nguyên dương điều kiện cần và đủ là trong phân tích tiêu chuẩn của n các ước nguyên tố dạng $4k+3$ phải có số mũ chẵn.

Bây giờ ta đi tìm điều kiện của n để nó biểu diễn được thành tổng của đúng hai bình phương nguyên dương.

Định lý 14 Để n để nó biểu diễn được thành tổng của đúng hai bình phương nguyên dương (tức là để phương trình $n=x^2+y^2$ có nghiệm ngưuyên dương điều kiện cần và đủ là

- Nếu n là số chính phương thì n phải có ít nhất một ước nguyên tố dạng 4k+1

- Nếu n là số không chính phương thì trong phân tích tiêu chuẩn của n c nguyên tố dạng $4k+3$ phải có số mũ chẵn.

Chứng minh 1. Giả sử $n = m^2 = a^2 + b^2, a, b \in \mathbb{N}^*$ và

$$n = 2^{2r}\Pi q_i^{2t_i-2}$$

với q_i dạng $4k+3$. Xét $q = q_i \to a = qa_1, b = qb_1 \to a_1^2 + b_1^2 = 2^{2r}\Pi q_i^{2t_i-2}$. S số hữu hạn bước ta đi đến $c^2+d^2 = 2^{2r} = 4^r \to$
$2d_1 \to c_1^2 + d_1^2 = 4^{r-1}$. Sau một số hữu hạn bước ta đi đến $u^2 + v^2 = 1$ với u, v Mâu thuẫn.

Đảo lại giả sửu $p|n, p = 4k+1 \to p|m \to m = pk \to n = p^2k^2$. $p = a^2 + b^2, a > b \to p^2 = (a^2+b^2)^2 = (a^2-b^2)^2 + (2ab)^2 = A^2 + B^2,$ $\mathbb{N}^* \to n = (kA)^2 + (kB)^2$

2. Điều kiện cần hiển nhiên do định lý 1. Ngược lại , do n là số không phương và trong phân tích tiêu chuẩn của n các ước nguyên tố dạng $4k+3$ p số mũ chẵn nên $n = m^2h$ với $h = p_1p_2...p_k$, p_i là các số nguyên tố phân biệt có dạng $4k+3$. Theo định lý 1 $h = a^2 + b^2$. Do h là tích các số nguyên tố phâ nên $a, b \neq 0$. Vậy $n = (ma)^2 + (mb)^2$.

2. Tổng của ba bình phương nguyên dương

Định lý 15 Để phương trình $n = x^2 + 2y^2$ có nghiệm nguyên dương điề cần và đủ là

- Nếu n là số chính phương thì n phải có ít nhất một ước nguyên tố dạng 8 hay $8k+3$
- Nếu n là số không chính phương thì trong phân tích tiêu chuẩn của n c nguyên tố $p = 2 \vee p = 8k+5 \vee p = 8k+7$ phải có số mũ chẵn.

Chứng minh 1. Giả sử trái lại $n = m^2 = a^2 + 2b^2, a, b \in \mathbb{N}^*$ và

$$n = 2^{2r}\Pi q_i^{2t_i}$$

với $q_i = 8k+5 \vee 8k+7$. Xét $q = q_i$. Theo bổ đề 1 $a = qa_1, b = qb_1 \to a_1^2 -$ $2^{2r}\Pi q_i^{2t_i-2}$. Sau một số hữu hạn bước ta đi đến $c^2 + 2d^2 = 2^{2r} = 4^r \to c = 2c$ $2d_1 \to c_1^2 + 2d_1^2 = 4^{r-1}$. Sau một số hữu hạn bước ta đi đến $u^2 + 2v^2 =$ $u, v \in \mathbb{N}^*$. Mâu thuẫn.

Đảo lại giả sử $p|n, p = 8k+1 \vee 8k+3 \to p|m \to m = pk \to n = p^2$ có $p = a^2 + 2b^2, \to p^2 = (a^2+2b^2)^2 = (a^2-2b^2)^2 + 2(2ab)^2 = A^2 + 2B^2,$ $\mathbb{N}^* \to n = (kA)^2 + 2(kB)^2$

2. Điều kiện cần : Do định lý 1 thì trong phân tích tiêu chuẩn của n c nguyên tố, $p = 8k+5 \vee 8k+7$ phải có số mũ chẵn. Giả sử số mũ của 2 là s.Tương tự như trên sau một số hữu hạn bước ta đi đến $c^2 + 2d^2 = 2^s$. Với s suy ra c chẵn do đó d chẵn. Vậy $c = 2c_1, d = 2d_1 \to c_1^2 + 2d_1^2 = 2^{s-2}$. Sau hữu hạn bước ta đi đến $u^2 + 2v^2 = 2$ với $u, v \in \mathbb{N}^*$. Mâu thuẫn.

Ngược lại , do n là số không chính phương và trong phân tích tiêu chuẩn các ước nguyên tố q dạng $q = 8k+5, q = 8k+7$ và $q = 2$ phải có số mũ ch $n = m^2h$ với $h = p_1p_2...p_k$, p_i là các số nguyên tố phân biệt $p_i = 8k+1 \vee 8$ Theo định lý 1 $h = a^2 + 2b^2$. Nếu $b = 0$ thì $h = a^2$ vô lý do h là tích

nguyên tố phân biệt . Nếu $a = 0 \to h = 2b^2$ vô lý do h lẻ. Vậy $a, b \in \mathbb{N}^*$ và $n = (ma)^2 + 2(mb)^2$.

Định lý 16 Để phương trình $n^2 = x^2 + y^2 + z^2$ có nghiệm nguyên dương điều kiện cần và đủ là $n \neq 2^s$ và $n \neq 5.2^s$

Chứng minh Điều kiện cần : Nếu $n = 2^s \to 4^s = x^2 + y^2 + z^2 \to x = 2x_1, y = 2y_1, z = 2z_1 \to 4^{s-1} = x_1^2 + y_1^2 + z_1^2$. Sau một số hữu hạn bước ta đi đến $1 = x_s^2 + y_s^2 + z_s^2$. Mâu thuẫn.

Nếu $n = 5.2^s \to 25.4^s = x^2+y^2+z^2 \to x = 2x_1, y = 2y_1, z = 2z_1 \to 25.4^{s-1} = x_1^2 + y_1^2 + z_1^2$.Sau một số hữu hạn bước ta đi đến $25 = x_s^2 + y_s^2 + z_s^2$. Phương trình này không có nghiệm nguyên dương.

Điều kiện đủ: Vì $n \neq 2^s$ nên n có ước nguyên tố lẻ .

- n có một ước nguyên tố lẻ $p \neq 5$. Vậy $n = ph \to n^2 = p^2h^2$. Ta chỉ cần chứng minh

$$p^2 = X^2 + Y^2 + Z^2 \quad \text{với} \quad X, Y, Z \in \mathbb{N}^*$$

+Nếu $p \equiv 3 \pmod 4$ thì $p = 8k + 3 \vee p = 8k + 7$. Nếu $p = 8k + 3$ thì theo định lý 2

$$p = u^2 + v^2 + t^2, \quad \text{với} \quad u, v, t \in \mathbb{N}$$

Nếu có một số chẳng hạn $t = 0$ thì $p = u^2 + v^2$ vô lý vì $p \equiv 3 \pmod 4$. Vậy $u, v, t \in \mathbb{N}^*$. Do vậy

$$p^2 = (u^2 + v^2 - t^2)^2 + (2ut)^2 + (2vt)^2 = X^2 + Y^2 + Z^2$$

Vì p lẻ nên $u^2 + v^2 \neq t^2 \to X, Y, Z \neq 0$.

Nếu $p = 8k + 7$ thì $2p \neq 4^s(8l + 7)$ do đó

$$2p = u^2 + v^2 + t^2 \to 4p^2 = (u^2 + v^2 - t^2)^2 + (2ut)^2 + (2vt)^2$$

$$\to p^2 = \left(\frac{u^2 + v^2 - t^2}{2}\right)^2 + (uv)^2 + (vt)^2$$

$$= (p - t^2)^2 + (uv)^2 + (vt)^2 = X^2 + Y^2 + Z^2, \quad \text{với} \quad X, Y, Z \in \mathbb{N}^*$$

+ Nếu $p \equiv 1 \pmod 4$. Theo định lý $p^2 = a^2 + b^2, a, b \in \mathbb{N}^*$. Nếu cả hai số a, b đều không chia hết cho 5 thì $p^2 = a^2 + b^2 \equiv 0, \pm 2 \pmod 5$. Mâu thuẫn. Vậy phải có một số chia hết cho 5 chẳng hạn $a = 5m$. Khi đó

$$p^2 = 25m^2 + b^2 = (3m)^2 + (4m)^2 + b^2 = X^2 + Y^2 + Z^2$$

- n chỉ có ước nguyên tố lẻ $p = 5$. Vậy

$$n = 5^t 2^s.$$

Ta có $n \neq 5.2^s \to t \geq 2 \to n = 25m \to n^2 = 625m^2 = (20m)^2 + (12m)^2 + (9m)^2$

3. Tổng của bốn bình phương nguyên dương

Ta biết rằng với mọi số nguyên dương n thì n biểu diễn được thành tổng của bốn bình phương. Tuy nhiên không nhất thiết n biểu diễn được thành tổng của bốn bình phương dương.

Ví dụ Chứng minh rằng $n = 2^s$ với s lẻ không biểu diễn được thành tổn bốn bình phương dương.

Thật vậy nếu $2^s = x^2 + y^2 + z^2 + t^2$ thì x, y, z, t chẵn. Đặt $x = 2x_1$ $2y_1, z = 2z_1, t = 2t_1 \to 2^{s-2} = x_1^2 + y_1^2 + z_1^2 + t_1^2$. Sau một số hữu hạn bước $2 = a^2 + b^2 + c^2 + d^2 \geq 4$. Mâu thuẫn.

Định lý 17 Phương trình $n^2 = x^2 + y^2 + z^2 + t^2$ có nghiệm nguyên dươn và chỉ khi $n \neq 1, 3$.

Chứng minh Dễ chứng minh 1 và 9 không biểu diễn được thành tổng củ bình phương dương. Bây giờ ta chứng minh Với mọi số nguyên dương $n \neq 1$ phương trình $n^2 = x^2 + y^2 + z^2 + t^2$.

Nếu $n = 2k \to n^2 = 4k^2 = k^2 + k^2 + k^2 + k^2$.

Giả sử $n > 1$ lẻ. Dễ thấy chỉ cần chỉ ra n có một ước nguyên tố p biểu diễn thành tổng của bốn bình phương dương.

- n có một ước nguyên tố $p > 26 \to p^2 - 676 \in \mathbb{N}^*$. Ta có $p^2 - 676 \equiv 1 -$ (mod 8). Do đó $p^2 - 676 = a^2 + b^2 + c^2$. Nếu $a, b, c > 0 \to p^2 = 2$ $a^2 + b^2 + c^2$. Nếu $a, b > 0, c = 0 \to p^2 = 10^2 + 24^2 + a^2 + b^2$. $a > 0, b = c = 0 \to p^2 = 6^2 + 8^2 + 24^2 + a^2$.

- Mọi ước nguyên tố của n nhỏ hơn 26 : Khi đó hoặc

  + n có ước nguyên tố p thuộc tập $S = \{5, 7, 13, 17, 11, 19, 23\}$. Khi đ $p \in \{5, 13, 17, 11, 19\} \to p \neq 8k + 7$ do đó $p = a^2 + b^2 + c^2$. Nếu a $0, c = 0 \to p^2 = (a^2 + b^2)^2 = (a^2)^2 + (b^2)^2 + (ab)^2 + (ab)^2$. Nếu $a, b,$ thì không thể 3 số bằng nhau chẳng hạn $a \neq b$. Khi đó $p^2 = (a^2 + b^2 + c$ $(2ab + c^2)^2 + (a^2 - b^2)^2 + (ca - cb)^2 + (ca - cb)^2$.

  Còn nếu $p \in \{7; 23\}$ thì ta có $7^2 = 1^2 + 4^2 + 4^2 + 4^2, 23^2 = 1^2 + 4^2 + 16^2$

  + n chỉ có ước nguyên tố $p = 3$. Khi đó $n = 3^s, s \geq 2 \to n = 9m \to$ $81m^2 = (2m)^2 + (2m)^2 + (3m)^2 + (8m)^2$

Định lý 18 Để phương trình $n = x^2 + 3y^2$ có nghiệm nguyên dương điều kiệ và đủ là

- Nếu n là số chính phương thì n phải có ít nhất một ước nguyên tố dạng $3k$

- Nếu n là số không chính phương thì trong phân tích tiêu chuẩn của n ước n tố $p = 3, p = 3k + 2$ phải có số mũ chẵn.

Chứng minh 1. Giả sử trái lại $n = m^2 = a^2 + 3b^2, a, b \in \mathbb{N}^*$ và

$$n = 3^{2r} \Pi q_i^{2t_i}$$

với $q_i = 3k+2$. Xét $q = q_i$. Theo bổ đề 1 $a = qa_1, b = qb_1 \to a_1^2 + 3b_1^2 = 3^{2r} \Pi q$ Sau một số hữu hạn bước ta đi đến $c^2 + 3d^2 = 3^{2r} = 9^r \to c = 3c_1, d = 3$ $c_1^2 + 3d_1^2 = 9^{r-1}$. Sau một số hữu hạn bước ta đi đến $u^2 + 3v^2 = 1$ với u, v Mâu thuẫn.

Đảo lại giả sử $p|n, p = 3k + 1 \to p|m \to m = pk \to n = p^2k^2$. $p = a^2 + 3b^2, \to p^2 = (a^2 + 3b^2)^2 = (a^2 - 3b^2)^2 + 3(2ab)^2 = A^2 + 3B^2, A$ $\mathbb{N}^* \to n = (kA)^2 + 3(kB)^2$

2. Điều kiện cần : Do định lý 1 thì trong phân tích tiêu chuẩn của n các ước nguyên tố, $p = 3k + 2$ phải có số mũ chẵn. Giả sử số mũ của 3 là số lẻ s.Tương tự như trên sau một số hữu hạn bước ta đi đến $c^2 + 3d^2 = 3^s$. Với $s \geq 3$ ta suy ra $3|c$ do đó $3|d$ chẵn. Vậy $c = 3c_1, d = 3d_1 \rightarrow c_1^2 + 3d_1^2 = 3^{s-2}$. Sau một số hữu hạn bước ta đi đến $u^2 + 3v^2 = 3$ với $u, v \in \mathbb{N}^*$. Mâu thuẫn.

Ngược lại , do n là số không chính phương và trong phân tích tiêu chuẩn của n các ước nguyên tố q dạng $q = 3k + 1$ và $p = 3$ phải có số mũ chẵn nên $n = m^2h$ với $h = p_1p_2...p_k$, p_i là các số nguyên tố phân biệt $p_i = 3k + 1$. Theo định lý 1 $h = a^2 + 3b^2$. Nếu $b = 0$ thì $h = a^2$ vô lý do h là tích các số nguyên tố phân biệt . Nếu $a = 0 \rightarrow h = 3b^2$ vô lý do h không chia hết cho 3. Vậy $a, b \in \mathbb{N}^*$ và $n = (ma)^2 + 3(mb)^2$.

Cuối cùng ta có

Định lý 19 Mọi số nguyên dương $n \geq 169$ đều biểu diễn tổng của năm bình phương dương.

Chứng minh Ta có $n - 169 = a^2 + b^2 + c^2 + d^2$.

- Nếu $a, b, c, d > 0$ thì $n = 13^2 + a^2 + b^2 + c^2 + d^2$
- $a, b, c > 0, d = 0$ thì $n = 12^2 + 5^2 + a^2 + b^2 + c^2$
- Nếu $a, b > 0, c = d = 0$ thì $n = 12^2 + 4^2 + 3^2 + a^2 + b^2$
- Nếu $a > 0, b = c = d = 0$ thì $n = 10^2 + 8^2 + 2^2 + 1^2 + a^2$
- Nếu $a = b = c = d = 0$ thì $n = 169 = 2^2 + 2^2 + 5^2 + 6^2 + 10^2$

Bằng cách thử trực tiếp với các số $n < 169$ ta thấy tất cả chỉ trừ ra các số: $1, 2, 3, 4, 6, 7, 9, 10, 12, 15, 18, 33$ là biểu diễn tổng của năm bình phương dương. Vậy

Định lý 20 Mọi số nguyên dương $n \notin \{1, 2, 3, 4, 6, 7, 9, 10, 12, 15, 18, 33\}$ đều biểu diễn tổng của năm bình phương dương.

Sau đây chúng ta sẽ áp dụng các kết quả trên để khảo sát một hàm số học được định nghĩa như sau:

Với mỗi số nguyên dương $n \geq 5$ gọi $S(n)$ là số nguyên dương k lớn nhất có tính chất: Với mọi $1 \leqslant k \leqslant S(n)$ thì n^2 biểu diễn tổng của k bình phương dương. Ta có định lý sau

Định lý 21

$$S(n) = \begin{cases} 1 & \text{nếu } n \text{ không có ước nguyên tố } p = 4k + 1 \\ 2 & \text{nếu } n = 5.2^s \\ n^2 - 14 & \text{nếu trái lại} \end{cases}$$

Chứng minh Trước hết nhận xét rằng n^2 luôn biểu diễn tổng của 1 bình phương dương. Vậy $S(n) \geqslant 1$Giả sử n không có ước nguyên tố $p = 4k + 1$. Theo định lý thì n^2 không biểu diễn tổng của 2 bình phương dương. Vậy $S(n) < 2 \rightarrow S(n) = 1$.

Giả sử $n = 5.2^s$. Theo định lý 1 (vì 5 là ước nguyên tố dạng $4k + 1$) nên n^2 biểu diễn tổng của 2 bình phương dương. Theo định lý 2 n^2 không biểu diễn tổng của 3 bình phương dương. Vậy $S(n) < 3 \rightarrow S(n) = 2$.

Bây giờ xét các n còn lại tức là $n \neq 5.2^s$ và n có ước nguyên tố $p = 4k + 1$. Vì n có ước nguyên tố $p = 4k + 1$ nên n^2 biểu diễn tổng của 2 bình phương dương. Vì

n có ước nguyên tố $p = 4k + 1$ suy ra $n \neq 2^s$. Vì $n \neq 5.2^s, n \neq 2^s$ nên theo lý 2 n^2 biểu diễn tổng của 3 bình phương dương. Ta có tồn tại $a, b \in \mathbb{N}^*$ sao $n^2 = a^2 + b^2$. Theo định lý Pitago n có dạng

$$\begin{aligned} n = d(m^2 + n^2) \to n^2 &= d^2(m^4 + n^4 + (mn)^2 + (mn)^2) \\ &= (dm^2)^2 + (dn^2)^2 + (dmn)^2 + (dmn)^2 \end{aligned}$$

Vậy n^2 biểu diễn tổng của 4 bình phương dương.

Tiếp theo ta chứng minh với mọi $5 \leqslant k \leqslant n^2 - 14$ thì n^2 biểu diễn tổng k bình phương dương, nhưng không biểu diễn được thành tổng của $n^2 - 13$ phương dương. Thật vậy vì $k \leqslant n^2 - 14 \to n^2 - k + 5 \geq 19$. Đầu tiê $k \neq n^2 - 28 \to n^2 - k + 5 \neq 33$. Theo định lý phương trình $n^2 - k + 5 = \sum_i^5$ có nghiệm nguyên dương x_i. Vậy

$$n^2 = \sum_{i=1}^{5} x_i^2 + \underbrace{1 + 1 \cdots + 1}_{k-5}$$

hay n^2 biểu diễn tổng của k bình phương dương. Nếu $k = n^2 - 28 \to k \geq 6$. V

$$n^2 = k - 6 + 34 = \underbrace{1 + 1 \cdots + 1}_{k-6} + 3^2 + 3^2 + 2^2 + 2^2 + 2^2 + 2^2$$

hay n^2 biểu diễn tổng của k bình phương dương.

Giả sử trái lại n^2 biểu diễn tổng của k bình phương dương với $k = n^2 - 13$ tồn tại k số nguyên dương $x_1, ..., x_k$ sao cho

$$\begin{aligned} n^2 &= \sum_{i=1}^{k} x_i^2 \\ n^2 - k &= \sum_{i=1}^{k} (x_i^2 - 1) \\ 13 &= \sum_{i=1}^{k} (x_i^2 - 1) \\ &= \sum_{i=1}^{k} b_i \end{aligned}$$

Vì $0 \leqslant b_i \leqslant 13$ và $b_i + 1$ là số chính phương nên $b_i \in \{3; 8\}$ Vậy (7) tương đươn phương trình

$$13 = 3x + 8y$$

có nghiệm tự nhiên. Nhưng điều này không xảy ra (Vì $y < 2$ và thử với $y =$ không thỏa). Định lý được chứng minh xong.

5. Tổng bình phương của n số nguyên dương liên tiếp Gọi $\mathcal{K}$ các số nguyên dương n có tính chất: Tồn tại n số chính phương liên tiếp mà tổ là số chính phương. Nói cách khác $n \in \mathcal{K}$ nếu và chỉ nếu phương trình

$$\sum_{i=1}^{n} (x + i)^2 = y^2$$

có nghiệm tự nhiên.

Thí dụ $2, 11, 23, 24 \in \mathcal{K}$ vì

$$\begin{aligned} 3^2 + 4^2 &= 5^2 \\ 18^2 + 19^2 + \cdots + 27^2 + 28^2 &= 77^2 \\ 7^2 + 8^2 + \cdots + 28^2 + 29^2 &= 92^2 \\ 1^2 + 2^2 + \cdots + 24^2 &= 70^2 \end{aligned}$$

Định lý 22 Giả sử n có dạng $n = p^s q - 1$ ở đó s lẻ, $p > 3$ là số nguyên tố dạng $4k + 3$,$(q; p) = 1$ Khi đó $n \notin \mathcal{K}$. Nói riêng, có vô số số nguyên dương chẵn và vô số số nguyên dương lẻ $n \notin \mathcal{K}$

Chứng minh Giả sử trái lại $n \in \mathcal{K}$

$$\begin{aligned} y^2 &= \sum_{i=1}^{n} (x+i)^2 \to \\ y^2 &= nx^2 + n(n+1)x + \frac{n(n+1)(2n+1)}{6} \to \\ x^2 + y^2 &= (n+1)\left(x^2 + nx + \frac{n(2n+1)}{6}\right) \to \\ (6x)^2 + (6y)^2 &= 6(n+1)\left(6x^2 + 6nx + n(2n+1)\right) \to \\ &= 6p^s qA \to \\ u^2 + v^2 &= p^s M \quad \text{với } u = 6x, v = 6y, M = 6qA \end{aligned}$$

Ta có $p|u^2+v^2 \to p|u = 6x$ (do $p = 4k+3$). Lại có $2n+1 = 2p^s q-1$ không chia hết cho p do đó $n(2n+1)$ không chia hết cho p, Vậy $A = 6x^2 + 6nx + n(2n+1)$ không chia hết cho p. Vì $p > 3$ nên $(M, p) = 1$. Lại có $u^2 + v^2 = p^s M \to u = pu_1, v = pv_1 \to u_1^2 + v_1^2 = p^{s-2}M$. Sau một số hữu hạn bước dẫn đến $p(a^2 + b^2) = M$. Mâu thuẫn.

Định lý 23 Có vô số số nguyên dương lẻ $n \in \mathcal{K}$.

Chứng minh Ta xét tổng

$$P = \sum_{i=1}^{k} (x-j)^2 + x^2 + \sum_{i=1}^{k} (x+j)^2 \quad \text{với } x > k$$

Ta có p là tổng của $n = 2k + 1$ bình phương liên tiếp bắt đầu từ số $(x-k)^2$. Đẳng thức trên tương đương với

$$P = (2k+1)\left(x^2 + \frac{k(k+1)}{3}\right) \tag{77}$$

Đặt $k = 6a^2 - 1 \Leftrightarrow n = 12a^2 - 1, x = 2a(12a^2 - 1) + a$ vào (8) ta được

$$\begin{aligned} P &= (12a^2-1)\left(4(12a^2-1)^2a^2 + 4a^2(12a^2-1) + a^2(12a^2-1)\right) \\ &= a^2(12a^2-1)^2(48a^2+1) \end{aligned}$$

Nếu (b, a) là nghiệm nguyên dương của phương trình Pell

$$b^2 - 48a^2 = 1$$

ta suy ra

$$P = a^2(12a^2 - 1)^2b^2$$

và rõ ràng $x = 2a(12a^2 - 1) + a = a(24a^2 - 1) \geqslant 24a^2 - 1 > 6a^2 - 1 = k$ Vậ
là số chính phương tức là $n = 12a^2 - 1 \in \mathcal{K}$ nếu chọn (b, a) là nghiệm nguyên dư
của phương trình Pell $b^2 - 48a^2 = 1$. Vì phương trình Pell $b^2 - 48a^2 = 1$ có v
nghiệm và $n = 12a^2 - 1$ là số lẻ nên định lý được chứng minh.

Bài toán mở Hỏi có hữu hạn hay vô hạn số chẵn thuộc $\mathcal{K}$.

Ta thấy 2 là số chẵn bé nhất (và cũng là số bé nhất) trong $\mathcal{K}$. Ta hãy tìm số
nhất.

Định lý 24 Số lẻ n bé nhất trong $\mathcal{K}$ là $n = 11$.

Chứng minh Vì $(7; 1)$ là nghiệm phương trình Pell $b^2 - 48a^2 = 1$ nên theo
lý trên $n = 12 - 1 = 11 \in \mathcal{K}$. Giả sử tồn tại $n = 2k + 1 < 11 \in \mathcal{K} \Leftrightarrow k < 5$. T
từ (8)

$$y^2 = (2k + 1)x^2 + \frac{k(k + 1)(2k + 1)}{3}$$

- Nếu y lẻ. Ta có $\frac{k(k+1)(2k+1)}{3} = 2(1^2 + \cdots + k^2)$ chẵn nên x lẻ. Suy ra $8|y^2 - x$
  $8|2k + \frac{k(k+1)(2k+1)}{3} \to 4|k + \frac{k(k+1)(2k+1)}{6} \to 8|k(2k^2 + 3k + 7)$.

  + Nếu k chẵn suy ra $k|8 \to k \geq 8$. Mâu thuẫn.

  + Nếu k lẻ suy ra $8|2k^2+3k+7 \to 2k^2+3k+1 \equiv 3k+1 \equiv 0 \pmod 8 \to k$
  $\pmod 8 \to k \geq 5$. Mâu thuẫn.

- Nếu y chẵn. Từ (8) suy ra x chẵn do đó $4|k(k + 1)(2k + 1)$.

  + Nếu k lẻ suy ra $4|k + 1 \to k = 3$. Thay vào (8) ta được $y^2 = 7(x^2 +$
  $x^2 + 4 \equiv 0 \pmod 7 \to x^2 \equiv 3 \pmod 7$. Mâu thuẫn.

  + Nếu k chẵn: $4|k(k + 1)(2k + 1) \to 4|k \to k = 4$. Thay vào (8) ta
  $y^2 = 3(3x^2 + 20) \to 3|3x^2 + 20$ .Mâu thuẫn.

Định lý đươợc chứng minh.

PHƯƠNG TRÌNH DIOPHANT

Trần Nam Dũng

0.1 Mở đầu

Phương trình nghiệm nguyên hay còn được gọi là phương trình Diophant là một trong những dạng toán lâu đời nhất của toán học. Từ Euclid, Diophantus, qua Fibonacci, rồi đến Fermat, Euler, Lebesgue ... và thời hiện đại là Gelfold, Matiasevic, Shenzel, Serpinsky ... phương trình Diophant đã trải qua một lịch sử phát triển lâu dài.

Thông qua việc giải các phương trình Diophant, các nhà toán học đã tìm ra được những tính chất sâu sắc của số nguyên, số hữu tỷ, số đại số. Giải phương trình Diophant đã đưa đến sù ra đêi của Liên phân số, Lý thuyết đường cong elliptic, Lý thuyết xấp xỉ Diophant, Thặng dư bình phương, Sè học modular ...

Trong các kỳ thi học sinh giỏi quốc gia và quốc tế, phương trình Diophant vẫn thường xuyên xuất hiện dưới các hình thức khác nhau và luôn được đánh giá là khó do tính không mẫu mực của nó.

Bài giảng này có mục đích đưa ra một số phương pháp cơ bản để tấn công các bài toán về phương trình Diophant. Tuy nhiên, với khả năng còn hạn hẹp của mình, chúng tôi hòan tòan không có tham vọng bao quát hết các vấn đề về phương trình Diophant. Chúng tôi chủ yếu chỉ giới hạn trong các phương trình đa thức, bỏ qua các phương trình Diophant bậc nhất và không đề cập đến các phương trình có chứa hàm mũ. Đây là một tập tài liệu mở, một số chứng minh được bỏ qua, một số lời giải chỉ trình bày sơ lược hoặc bỏ qua. Chúng tôi rất mong nhận được ý kiến đóng góp của quý thầy cô, quý anh chị và bạn bè đồng nghiệp, cũng như của các em sinh viên, học sinh để tập tài liệu được hoàn thiện hơn.

Chúng tôi xin chân thành cảm ơn GS Nguyễn Văn Mậu và Trường Đại học Khoa học Tự nhiên ĐHQG HN đã tổ chức khoá bồi dưỡng này và cho phép chúng tôi được báo cáo trước các anh chị và các bạn.

0.2 Phương pháp chọn mô-đun

Một số chính phương không thể tận cùng bằng $2, 3, 7, 8$. Một số chính phương chia 3 dư 0 hoặc 1. Một số chính phương chia 8 dư $0, 1$ hoặc 4. Những tính chất đơn giản đó nhiều khi lại là chìa khoá để giải nhiều phương trình Diophant. Và đó chính là ý

tưởng chính của phương pháp chọn mô-đun.

Ví dụ 2.1. (Việt Nam 2003, Bảng B) Hỏi có tồn tại hay không các số ng
x, y, u, v, t thoả mãn điều kiện sau

$$x^2 + y^2 = (x+1)^2 + u^2 = (x+2)^2 + v^2 = (x+3)^2 + t^2$$

Lời giải:

Cách 1. Thật vậy, giả sử hệ trên tồn tại nghiệm. Đặt N là giá trị chung c
bốn biểu thức. Ta có $x^2 \mod 8 \in \{0,1,4\}$, suy ra $x^2 + y^2 \in \{0,1,2,4,5\}$. N
ra, nếu x chạy qua một hệ thặng dư đầy đủ $\mod 4$ thì $x^2 \mod 8$ sẽ là $(0,1$
hay một hoán vị vòng quanh của bộ trên. Như thế $N \mod 8 \in \{0,1,4\} \cap \{1,2,$
$\{0,1,4\} \cap \{0,4,5\} = \emptyset$. Mâu thuẫn. Vậy không tồn tại các số nguyên $x, y,$
thoả mãn điều kiện đầu bài.

Cách 2. Từ hai phương trình đầu ta suy ra $y^2 + v^2 - 2u^2 = 2(x+1)^2 - x^2 -$
$2)^2 = -2$. Như thế, $y^2 + v^2 = 2(u^2 - 1)$, suy ra y, v cùng tính chẵn lẻ. Nếu y, v
lẻ thì về trái chia 8 dư 2, suy ra u chẵn, nhưng khi đó, vế trái chia 8 dư -2, mâu t

Ví dụ 2. Chứng minh rằng phương trình $x^2 - 3y^2 = -1$ không có nghiệm ng
dương.

Lời giải: $x^2 + 1$ không thể chia hết cho 3!

Ví dụ 3. (Đề đề nghị IMO 1981) Cho phương trình nghiệm nguyên $z^2 = ($
$1)(y^2 - 1) + n$. Hỏi phương trình có nghiệm không nếu

(a) $n = 1981$ (b) $n = 1985$ (c) $n = 1984$?

Lời giải. a) Ta có $z^2 \equiv (x^2-1)(y^2-1)+5 \mod 8$. Vì $z^2 \equiv 0,1,4 \mod 8,$
$1 \equiv 0,3,7 \mod 8$, $(x^2-1)(y^2-1) \equiv 0,1,5 \mod 8$ và $(x^2-1)(y^2-1)+5 \equiv$
$\mod 8$ nên ta có $z^2 \neq (x^2-1)(y^2-1)+5 \mod 8$. Mâu thuẫn.

(b) Tương tự, xét $\mod 9$.

(c) $n = 1984$. Rút gọn phương trình, ta được $x^2 + y^2 + z^2 - x^2y^2 = 198$
ý tưởng của ta là đi tìm biểu diễn $x^2 + y^2 = 1985$. Khi đó $z = xy$ cho ta ng
Bằng cách xét chữ số cuối cùng, ta nhanh chóng đi đến nghiệm $7^2 + 44^2$ và 31^2
bằng phương pháp thử và sai. Từ đó được các nghiệm $(x, y, z) = (7, 44, 7.4$
$(31, 32, 31.32)$.

Ghi chú: Phương trình (1) có vô số nghiệm nguyên dương, hãy thử chứng

BÀI TẬP

2.1 (Thuỵ Điển 2003) Tìm tất cả các cặp số nguyên dương x, y sao cho

$$x^2 - 3xy = 2002$$

2.2 Tìm nghiệm nguyên của các phương trình

a) $x^2 - 2y^2 = 3$ b) $2x^2 - 5y^2 = 7$ c) $5x^2 + 6x + 11 = y^2 + 4y$

2.3 Tìm nghiệm nguyên của phương trình $x^{10} + y^{10} - z^{10} = 1999$.

2.4 Chứng minh rằng phương trình $x^2 - 2y^2 + 8z = 3$ không có nghiệm nguyên x, y, z

2.5 Tìm tất cả các giá trị nguyên dương $1 < k < 10$ sao cho hệ phương trình $x^2 + ky^2 = z^2$, $kx^2 + y^2 = t^2$ có nghiệm nguyên dương.

2.6 Chứng minh rằng phương trình $x^2 + y^2 + z^2 + x + y + z = 1$ không có nghiệm hữu tỷ.

0.3 Giới hạn miền nghiệm. Thử và sai

Cho x là số nguyên. Nếu $|x| \leqslant N$ với số nguyên dương N cho trước thì x chỉ có thể nhận hữu hạn giá trị. Cụ thể $x \in \{-N, -N+1, ..., 0, 1, ..., N\}$. Điều đơn giản này là chìa khoá để giải nhiều phương trình Diophante, sau đó dùng phép thử.

Ví dụ 3.1. (Bài toán Arnold) Tìm tất cả các bộ ba số nguyên dương sao cho tích của hai số bất kỳ cộng 1 chia hết cho số còn lại.

Ví dụ 3.2. (Olympic 30/4 năm 1999) Trong mặt phẳng tọa độ Oxy cho ba đường thẳng có hệ số góc lần lượt là $1/m, 1/n, 1/p$ với m, n, p là các số nguyên dương. Tìm m, n, p sao cho ba đường thẳng đó tạo với trục hoành ba góc có tổng số đo là 45°.

BÀI TẬP

3.1 Tìm tất cả các nghiệm nguyên dương của phương trình

$$\frac{1}{x^2} + \frac{1}{y^2} + \frac{1}{z^2} + \frac{1}{t^2} = 4$$

3.2 Giải phương trình trong tập hợp các số nguyên dương

$$\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = 1$$

3.3 Tìm tất cả các bộ số nguyên dương (x, y) sao cho $x^2 + 1$ chia hết cho y, $y^3 + 1$ chia hết cho x^2.

3.4 (Bulgaria 2001) Tìm tất cả các bộ số nguyên dương (a, b, c) sao cho $a^3 + b^3 + c^3$ chia hết cho a^2b, b^2c, c^2a.

3.5 (Ailen 2003) Tìm tất cả các nghiệm nguyên của phương trình $(m^2+n)(n^2+m) = (m+n)^3$.

3.6 (Moldova 2003) Chứng minh rằng phương trình $1/a + 1/b + 1/c + 1/abc = 12/(a+b+c)$ có vô số nghiệm nguyên dương.

3.7 (Rio Plate 2002) Tìm tất cả các cặp số nguyên dương (a, b) sao cho

$$\frac{a^b + b}{ab^2 + 9}$$

là một số nguyên.

3.8 (Litva 2003) Tìm tất cả nghiệm nguyên của phương trình $3xy - x - 2y =$

3.9 (IMO 2003) Tìm tất cả các cặp số nguyên dương (a, b) sao cho số

$$\frac{a^2}{2ab^2 - b^3 + 1}$$

là số nguyên.

3.10 (Na Uy 2003) Tìm tất cả các bộ số nguyên (x, y, z) sao cho $x^3+y^3+z^3-3x$
2003.

3.11 (THTT 3/209) Tìm tất cả nghiệm nguyên (x, y) của phương trình

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

0.4 Phương pháp xuống thang

Fermat đã dùng phương pháp này để chứng minh phương trình $x^4 + y^4 = z^4$ k
có nghiệm nguyên dương. Và cũng từ đây, bằng vài dòng ngắn ngủi trên lề cuốn
Diophantus, ông đã làm đau đầu các nhà toán học suốt 300 năm qua bằng định l
nổi tiếng mang tên ông.

Cơ sở của phương pháp xuống thang là tính sắp thứ tự tốt của N (và N^k, tíc
các của k phiên bản N): Một tập con khác rỗng bất kỳ của N đều có phần tử nhỏ

Để chứng minh một phương trình là vô nghiệm, ta giả sử ngược lại rằng t
các nghiệm nguyên (tự nhiên, nguyên dương) của phương trình khác rỗng. Ta đ
một thứ tự tốt trên R và giả sử α_0 là nghiệm nhỏ nhất (theo thứ tự nêu trên).
bằng cách nào đó ta xây dựng được nghiệm a_1 nhỏ hơn α_0 thì chúng ta sẽ đi đến
thuẫn. Mâu thuẫn này chứng tỏ điều giả sử là sai và như vậy phương trình đó c
nghiệm.

Ví dụ 1. Chứng minh rằng nghiệm nguyên duy nhất của phương trình $x^3 - 3$
$9z^3 = 0$ là $(0, 0, 0)$.

Ví dụ 2. Chứng minh rằng phương trình $x^4 + y^4 = z^2$ không có nghiệm ng
dương.

Lời giải. Giả sử rằng phương trình đó cho có nghiệm nguyên dương. G
$(x, y) = d$, tức là $x = da, y = db$, trong đó $(a, b) = 1$. Khi đó $a^4 + b^4 = (z/d^2)^2$
sử $z = d^2c$, trong đó $c \in Q$, khi đó

$$a^4 + b^4 = c^2$$

Vì $c \in Q, c^2 \in N$ nên theo Định lý 6.1, $c \in N^+$. Trong tất cả các nghiệm của phương trình (1), chọn nghiệm có c nhỏ nhất. Ta có $(a^2)^2 + (b^2)^2 = c^2$ trong đó $(a, b) = 1$, suy ra $(a^2, b^2) = 1$, tức là (a^2, b^2, c) là bộ ba Pythagore nguyên thủy. Theo định lý 6.5, tồn tại các số nguyên dương m, n sao cho $a^2 = m^2 - n^2, b^2 = 2mn, c = m^2 + n^2$ trong đó m, n khác tính chẵn lẻ, $m > n$ và $(m, n) = 1$, nghĩa là $a^2 = m^2 - n^2$ lẻ. Giả sử m chẵn, n lẻ. Khi đó n^2, a^2 chia 4 dư 1, nghĩa là $m^2 = n^2 + a^2$ chia 4 dư 2 mâu thuẫn. Vậy m lẻ, n chẵn, ngòai ra (a, n, m) lập thành bộ Pythagore nguyên thủy, do đó tồn tại $p, q \in \mathbb{N}^+$ sao cho $a = p^2 - q^2, n = 2pq, m = p^2 + q^2$, trong đó p, q khác tính chẵn lẻ, $p > q$ và $(p, q) = 1$, ngòai ra $b^2 = 2mn$, nghĩa là $b^2 = 4pq(p^2 + q^2)$, suy ra $b = 2h$, $h \in N^+$, khi đó

$$h^2 = pq(p^2 + q^2) \tag{2}$$

Giả sử rằng tồn tại số nguyên tố r chia hết $pq, p^2 + q^2$. Vì r chia hết pq nên không mất tổng quát, có thể giả sử r chia hết p, khi đó r chia hết $(p^2 + q^2) - p^2 = q^2$, suy ra r chia hết q, mâu thuẫn vì $(p, q) = 1$. Vậy $(pq, p^2 + q^2) = 1$, như thế, từ (2), theo định lý 6.1, ta có $pq = s^2, p^2 + q^2 = t^2$ với $s, t \in \mathbb{N}^+$. Vì $pq = s^2, (p, q) = 1$ nên $p = u^2, q = v^2$ với $u, v \in N^+$, nghĩa là $(u^2)^2 + (v^2)^2 = t^2$ hay $u^4 + v^4 = t^2$, trong đó $c = m^2 + n^2 > m = p^2 + q^2 = t^2 > t$, mâu thuẫn với cách chọn c. Như vậy điều giả sử ban đầu là sai và ta có điều phải chứng minh.

BÀI TẬP

4.1 Chứng minh rằng phương trình $x^2 + y^2 + z^2 = 2xyz$ không có nghiệm nguyên khác $(0, 0, 0)$

4.2 Chứng minh rằng hệ phương trình

$$\begin{cases} x^2 + y^2 =^2 -t^2 \\ xy = zt \end{cases}$$

không có nghiệm nguyên dương.

4.3 (Hungary 2001) Tìm tất cả các số nguyên x, y, z sao cho $5x^2 - 14y^2 = 11z^2$.

4.4 Chứng minh rằng hệ phương trình $x^2 + 2y^2 = z^2$, $2x^2 + y^2 = t^2$ không có nghiệm nguyên dương.

4.5 Chứng minh rằng phương trình $x^4 - y^4 = z^2$ không có nghiệm nguyên dương.

4.6

0.5 Xây dựng nghiệm

Có nhiều bài toán không yêu cầu tìm tất cả các nghiệm của phương trình, mà chỉ yêu cầu chứng minh phương trình có vô số nghiệm. Trong trường hợp như thế, ta chỉ cần xây dựng một họ nghiệm chứa tham số là đủ. Việc xây dựng như thế có thể được thực hiện bằng các giả định, giới hạn miền nghiệm. Các siêu phẳng là những miền giới hạn thông dụng.

Ví dụ 5.1. (Italy 1996) Chứng minh rằng phương trình $a^2+b^2=c^2+3$ có nghiệm nguyên (a,b,c).

Lời giải. Chọn $c=b+1$ thì ta được phương trình $a^2=2b+4$ (*). Bây gi cần chọn $a=2k, b=2(k^2-1)$ là ta được nghiệm của (*) và như vậy phương ban đầu có họ nghiệm $a=2k, b=2(k^2-1), c=2k^2-1$.

Ví dụ 5.2 (Canada 1991) Chứng minh rằng phương trình $x^2+y^3=z^5$ có nghiệm nguyên dương.

Lời giải. Chú ý rằng $2^m+2^m=2^{m+1}$. Đặt $x=2^{m/2}, y=2^{m/3}, z=2^{(m}$ khi đó $x^2+y^3=z^5$. Ta chỉ cần tìm m sao cho $m/2, m/3$ và $(m+1)/5$ nguy xong. Đây là một bài toán bậc nhất đơn giản và ta có thể tìm được $m=6(5k+$

Ví dụ 5.3 Chứng minh rằng với mọi $n\geqslant 2$, phương trình $x^2+y^2=z^n$ luôn có vô số nghiệm nguyên dương.

Lời giải. Xét số phức $\alpha=a+bi$. Giả sử $\alpha^n=x+yi$ thì ta có

$$\sqrt{x^2+y^2}=|\alpha^n|=|\alpha|^n=(\sqrt{a^2+b^2})^n$$

Từ đó $x^2+y^2=(a^2+b^2)^n$.

BÀI TẬP

5.1 Dựa vào hằng đẳng thức $\{2(3x+2y+1)+\}^2-2(4x+3y+2)^2=(2x+1)^2$ chứng minh rằng phương trình $x^2+(x+1)^2=y^2$ có vô số nghiệm n dương.

5.2 Dựa vào hằng đẳng thức $\{2(7y+12x+6)\}^2-3\{2(4y+7x+3)+$ $(2y)^2-3(2x+1)^2$ chứng minh rằng phương trình $(x+1)^3-x^3=y^2$ có nghiệm nguyên dương.

5.3 Chứng minh rằng tồn tại vô số các cặp số hữu tỷ dương (x,y) sao cho x^3+y

5.4 (Bulgaria 1999) Chứng minh rằng phương trình $x^3+y^3+z^3+t^3=1999$ số nghiệm nguyên.

5.5 Chứng minh rằng với mọi $n\geqslant 2$, luôn tồn tại n số nguyên dương có tổn tích.

5.6 (IMO 82) Chứng minh rằng nếu n là số nguyên dương sao cho phươn $x^3-3xy^2+y^3=n$ có nghiệm nguyên (x,y), thì phương trình này có ba nghiệm như vậy. Chứng minh rằng phương trình đó cho không có n khi $n=2891$.

5.7 Chứng minh rằng phương trình $(x^2+x+1)(y^2+y+1)=z^2+z+1$ c nghiệm nguyên.

5.8 (THTT 4/187, dự tuyển IMO 92) Chứng minh rằng, với số nguyên dương m bất kỳ sẽ tồn tại vố số các cặp số nguyên (x, y) sao cho

1) x và y nguyên tố cùng nhau
2) y chia hết $x^2 + m$;
3) x chia hết $y^2 + m$.

5.9 (Saint Peterburg 2003) Chứng rằng tồn tại các số nguyên dương $a > 1, b > 1, c > 1$ sao cho $a^2 - 1$ chia hết cho $b, b^2 - 1$ chia hết cho c và $c^2 - 1$ chia hết cho a và $a + b + c > 2003$.

5.10 Chứng minh rằng phương trình $x^2 + y^2 + z^2 = xyz$ có vô số nghiệm nguyên dương.

0.6 Phương pháp số học

Các tính chất của số nguyên liên quan đến số nguyên tố, ước số chung, bội số chung như Định lý cơ bản của số học, các định lý Fermat, Euler, Wilson ... đóng một vai trò quan trọng trong việc tìm kiếm lời giải của phương trình Diophant. Chúng tôi nhắc lại một số định lý (không chứng minh) và đưa ra một số ví dụ áp dụng.

Định lý 6.1 (Bổ đề)

1) Cho $n > 1$ là một số nguyên dương. Nếu a, b, c là các số nguyên thỏa mãn điều kiện $a.b = c^n$ và $(a, b) = 1$ thì $a = (a')^n, b = (b')^n$ với các số nguyên a', b' nào đó.

2) Nếu a hữu tỷ, a^n nguyên với n nguyên dương nào đó thì a nguyên.

3) Nếu a nguyên $\sqrt[n]{a}$ hữu tỷ thì $\sqrt[n]{a}$ nguyên.

Định lý 6.2. (Định lý nhỏ Fermat) Nếu p là số nguyên tố và a là một số nguyên tùy ý thì $a^p - a$ chia hết cho p. Nếu $(a, p) = 1$ thì $a^{p-1} \equiv 1 \pmod{p}$.

Định lý 6.3. (Định lý Euler). Nếu m là số nguyên dương, $(a, m) = 1$ thì $a^{\phi(m)} \equiv 1 \pmod{m}$, trong đó ϕ là Phi-hàm Euler - số các số nguyên dương nhỏ hơn m nguyên tố cùng nhau với m.

Định lý 6.4. (Định lý Wilson). p là số nguyên tố khi và chỉ khi $(p-1)! + 1$ chia hết cho p.

Định lý 6.5. (Định lý Fermat-Euler) Nếu $p = 4k + 1$ thì tồn tại các số nguyên dương a, b sao cho $p = a^2 + b^2$.

Định lý 6.6. (Một tính chất quan trọng) Cho p là số nguyên tố dạng $4k + 3$ và $(a, b) = 1$. Khi đó $a^2 + b^2$ không chia hết cho p.

Ví dụ 6.1. (Phương trình Pythagore) Tìm nghiệm tổng quát của phương $x^2 + y^2 = z^2$ trong tập hợp các số nguyên dương.

Giải bài toán này ta có kết quả sau mà ta phát biểu như một định lý:

Định lý 6.7 Mọi nghiệm nguyên dương của phương trình $x^2 + y^2 = z^2$ đ thể viết dưới dạng $x = (m^2 - n^2)k, y = 2mnk, z = (m^2 + n^2)k$ hoặc $x = 2mnk$ $(m^2-n^2)k, z = (m^2+n^2)k$, trong đó các số nguyên m, n, k thỏa mãn các điều kiệ

1) $(m, n) = 1, (x, y) = k$
2) các số m, n khác tính chẵn lẻ
3) $m > n > 0, k > 0$.

Chứng minh. Giả sử $(x, y) = k$, khi đó $x = ka, y = kb$ trong đó $(a, b) =$ có $(ka)^2 + (kb)^2 = z^2$ tương đương với $a^2 + b^2 = (z/k)^2$. Đặt $z = kc, c \in \mathbb{Q}$, k $a^2 + b^2 = c^2$. Do $c \in \mathbb{Q}, c^2 \in \mathbb{N}$ nên theo định lý 6.1, $c \in \mathbb{N}$. Vì $(a, b) = 1$ nhất một trong hai số a, b phải lẻ. Giả sử rằng b lẻ, khi đó a^2, b^2 khi chia 4 dư 1 thế c^2 chia 4 dư 2, điều này không thể vì c^2 chia hết cho 2 mà không chia hết c Vậy b chẵn và như thế $c^2 = a^2 + b^2$ lẻ. Ta có

$$b^2 = (c - a)(c + a) \quad \text{hay là} \quad \left(\frac{b}{2}\right)^2 = \frac{c-a}{2} \cdot \frac{c+1}{2}$$

Dễ dàng kiểm tra rằng $(c-a)/2, (c+a)/2$ là các số nguyên nguyên tố cùng Như thế, theo định lý 6.1, tồn tại các số nguyên dương m, n sao cho $(c - a)$ $n^2, (c+a)/2 = m^2$, từ đó $c = m^2+n^2, a = m^2-n^2$ và $b = 2mn$, trong đó (m, n)

Ví dụ 6.2. (Lebesgue) Giải phương trình $x^2-y^3 = 7$ trong tập hợp các số tự n

Lời giải. Nếu y là số chẵn, tức là $y = 2k$ thì $x = 8k^3 + 7$ chia 8 dư 7 là không thể. Vậy y lẻ. Ta có

$$x^2 + 1 = y^3 + 8 \quad \text{hay là} \quad x^2 + 1 = (y + 2)(y^2 - 2y + 4)$$

Nếu y chia 4 dư 1 thì $y + 2$ có dạng $4k + 3$. Nếu y chia 4 dư 3 thì $y^2 - 2$ có dạng $4k + 3$. Vì vậy, trong mọi trường hợp, vế trái đều có ước dạng $4k + 3$ đó có ước nguyên tố dạng $4k + 3$, điều này mâu thuẫn với định lý 6.6.

Ví dụ 6.3. (Euler) Chứng minh rằng phương trình $4xy - x - y = z^2$ khô nghiệm nguyên dương.

Hướng dẫn. Viết phương trình dưới dạng $(4x - 1)(4y - 1) = 4z^2 + 1$ và sử định lý 6.6.

Ví dụ 6.4. a) Cho x, y, z là các số nguyên thỏa mãn điều kiện $x/y + y/z +$ nguyên. Chứng minh rằng xyz là lập phương của một số nguyên.
b) Tìm nghiệm nguyên của phương trình $x/y + y/z + z/x = 3$.

Hướng dẫn. Viết phương trình dưới dạng $x^2z + y^2x + z^2y = kxyz$. Gọi p là ước nguyên tố của (x, y). Hãy chứng minh rằng xyz chia hết cho p^3.

BÀI TẬP

6.1 Giải phương trình trong tập hợp các số nguyên dương

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{2003}$$

6.2 Tìm nghiệm nguyên của phương trình $x^3 - 5y^2 = 13$.

6.3 Chứng minh rằng phương trình $x^3 + 3 = 4y(y + 1)$ không có nghiệm nguyên.

6.4 Chứng minh rằng phương trình $x^7 + y^7 = 1998^z$ không có nghiệm nguyên dương.

6.5 Chứng minh rằng nếu p là số nguyên tố, n là số nguyên dương thì phương trình

$$x(x + 1) = p^{2n}y(y + 1)$$

không có nghiệm nguyên dương.

6.6 Tìm tất cả nghiệm của phương trình

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

trong tập hợp các số nguyên.

6.7 Chứng minh rằng nếu c là số nguyên dương lẻ thì phương trình

$$x^2 - y^3 = (2c)^3 - 1$$

không có nghiệm nguyên dương.

6.8 (Euler) Chứng minh rằng phương trình

$$4xyz - x - y - t^2 = 0$$

không có nghiệm nguyên dương.

6.9 (Nga 1997) Tìm tất cả các cặp số nguyên tố sao cho $p^3 - q^5 = (p + q)^2$.

6.10 (Legendre) Chứng minh rằng phương trình $ax^2 + by^2 = cz^2$, trong đó a, b, c là các tham số không có ước chính phương, đôi một nguyên tố cùng nhau có nghiệm nguyên dương khi và chỉ khi hệ phương trình đồng dư sau có nghiệm (α, β, γ):

$$bc \equiv \alpha^2 \pmod{a}, \quad ca \equiv \beta^2 \pmod{b} \quad ab \equiv -\gamma^2 \pmod{c}$$

0.7 Phương pháp hình học

Hình học có những ứng dụng rất bất ngờ trong việc giải các bài toán số học. C
ta chắc chắn còn nhớ bài toán của IMO 42 "Cho các số nguyên dương $a, b, c,$
$a > b > c > d > 0$. Giả sử $ac + bd = (b + d + a - c)(b + d - a + c)$. Chứng
rằng $ab + cd$ không phải là số nguyên tố" đó được giải hết sức ấn tượng bằng ...
lý hàm số cos và định lý Ptolémé. Dưới đây, ta sẽ xét hai ví dụ ứng dụng của hìn
trong số học với hai phương pháp tiếp cận khác nhau.

Phương pháp thứ nhất được gọi là phương pháp cát tuyến, sử dụng ý tưởn
hình học giải tích vào việc nghiên cứu các điểm nguyên và điểm hữu tỷ trên c
cong. Chính hướng đi này đó dẫn đến khái niệm đường cong elliptic, một trong r
viên gạch cơ bản đặt nền móng cho việc chứng minh định lý lớn Fermat. ở đây, c
ta chỉ giới hạn ở một ví dụ nhỏ.

Ví dụ 1. Tìm tất cả các nghiệm nguyên khác $(0, 0, 0)$ của phương trình

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

Lời giải. Chia hay vế của phương trình cho z^2, ta được phương trình

$$(\frac{x}{z})^2 + 2(\frac{y}{z})^2 = 3$$

Đặt $u = x/z, v = y/z$, ta được phương trình

$$u^2 + 2v^2 = 3$$

trong đó u, v hữu tỷ. Bài toán quy về việc tìm tất cả các nghiệm hữu tỷ của (2). T
tìm tất cả các điểm hữu tỷ nằm trên đường cong $(E) : u^2 + 2v^2 = 3$. Chú ý rằ
1) là một điểm hữu tỷ của (E). Nếu (u_0, v_0) là một điểm hữu tỷ khác $(1, 1)$ thì
thẳng qua $(1, 1)$ và (u_0, v_0) sẽ có hệ số góc hữu tỷ. Mặt khác, nếu $y = k(x -$
là đường thẳng qua $(1, 1)$ với hệ số góc k hữu tỷ thì, áp dụng định lý Viét cho p
trình hoành độ giao điểm, giao điểm thứ hai của đường thẳng trên với (C) cũng
độ hữu tỷ. Tính toán trực tiếp ta có tọa độ của điểm này là

$$u = \frac{2k^2 - 4k - 1}{2k^2 + 1}, \quad v = \frac{-2k^2 - 2k + 1}{2k^2 + 1}$$

Từ đây ta cũng tìm được nghiệm tổng quát của (1). Ví dụ với $k = -1$ ta
$u = 5/3, v = 1/3$ và ta có nghiệm $(5, 1, 3)$ của (1).

Phương pháp thứ hai là phương pháp điểm nguyên, lưới nguyên. Rất nhiều c
sâu sắc của số học được chứng minh bằng cách tính số điểm nguyên trong một
Chẳng hạn Luật thuận nghịch bình phương cho ký hiệu Legendre đó được chứng
như vậy. Dưới đây, chúng ta xét một ứng dụng khác của phương pháp lưới ngu

Ví dụ 2. Bổ đề Minkowsky và định lý Minkowsky

Định lý Minkowsky là một ví dụ rất thú vị về ứng dụng của hình học tr
thuyết số. Chúng ta bắt đầu từ một kết qu rất đơn giản nhưng hữu ích.

Bổ đề 7.1 Trên mặt phẳng cho hình F có diện tích lớn hơn 1. Khi đó tồn tại hai điểm A, B thuộc F, sao cho véctơ $\overrightarrow{AB}$ có tọa độ nguyên.

Chứng minh. Lưới nguyên cắt hình G thành các mẩu nhỏ. Chồng các mẩu này lên nhau, do tổng diện tích của các mẩu lớn hơn 1, nên có ít nhất hai mẩu có điểm chung. Gọi A, B là hai điểm nguyên thuỷ ứng với điểm chung này thì A, B là hai điểm cần tìm.

Bổ đề 7.2 (Bổ đề Minkowsky) Trên mặt phẳng cho hình lồi F nhận gốc tọa độ làm tâm đối xứng và có diện tích lớn hơn 4. Khi đó nó chứa một điểm nguyên khác gốc tọa độ.

Chứng minh. Xét phép vị tự tâm O, tỷ số $1/2$, biến F thành G. Do G có diện tích lớn hơn 1 nên theo bổ đề 1, tồn tại hai điểm A, B thuộc G sao cho véctơ $\overrightarrow{AB}$ có toạ độ nguyên. Gọi A' là điểm đối xứng với A qua O. Do hình G đối xứng qua gốc toạ độ nên A' thuộc G. Do G lồi nên trung điểm M của $A'B$ thuộc G. Gọi N là điểm đối xứng của O qua M thì N thuộc F và $ON = AB$, suy ra N là điểm nguyên khác O (đpcm).

Định lý 7.3 (Định lý Minkowsky) Cho a, b, c là các số nguyên, trong đó $a > 0$ và $ac - b^2 = 1$. Khi đó phương trình $ax^2 + 2bxy + cy^2 = 1$ có nghiệm nguyên.

BÀI TẬP

7.1 Tìm tất cả các cặp (x, y) các số hữu tỷ dương sao cho $x^2 + 3y^2 = 1$.

7.2 Chứng minh rằng một đường cong bậc hai bất kỳ hoặc không chứa điểm hữu tỷ nào, hoặc chứa vô số điểm hữu tỷ.

7.3 Hãy tìm ví dụ một đường cong bậc hai không chứa điểm hữu tỷ nào.

7.4 Chứng minh rằng nếu D là số nguyên không chính phương thì phương trình $x^2 - Dy^2 = 1$ luôn có nghiệm nguyên dương.

7.5 Cho p, q là các số nguyên dương nguyên tố cùng nhau. Bằng cách đếm các điểm nguyên, hãy chứng minh công thức

$$\left[\frac{p}{q}\right] + \left[\frac{2q}{p}\right] + \cdots + \left[\frac{(p-1)q}{p}\right] = \frac{(p-1)(q-1)}{2}$$

0.8 Phương pháp đại số (phương pháp gien)

Nếu từ một nghiệm của phương trình đó cho ta có quy tắc để xây dựng ra một nghiệm mới thì quy tắc đó chính là gien. phương pháp gien là phương pháp dựa vào gien để tìm tất cả các nghiệm của phương trình đó cho từ các nghiệm cơ sở. Để tìm các nghiệm cơ sở, ta áp dụng bước lùi, tức là quy tắc ngược của quy tắc tiến nói trên. Minh họa tốt nhất cho ý tưởng này là phương trình Pell và phương trình Markov. Ta bắt đầu bằng phương trình Pell.

Phương trình Pell cổ điển là phương trình dạng, $x^2 - Dy^2 = 1$ trong đó D nguyên dương không chính phương. Nếu $D = k^2$ thì từ phân tích $(x-ky)(x+k$ ta suy ra phương trình đó cho có các nghiệm nguyên duy nhất là $(1,0)$. Trong hợp D bất kỳ thì $(1,0)$ cũng là nghiệm của phương trình Pell. Ta gọi nghiệm nghiệm tầm thường.

Với số nguyên dương D không chính phương cho trước, đặt $S = \{(x$ $(N^+)^2 | x^2 - Dy^2 = 1\}$ là tập hợp tất cả các nghiệm nguyên dương của p trình Pell

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

Ta có định lý quan trọng sau

Định lý 8.1 Nếu D là số nguyên dương không chính phương thì $S \neq \emptyset$, phương trình (1) có nghiệm không tầm thường.

Chứng minh định lý này khá phức tạp, dựa vào lý thuyết liên phân số hoặc p pháp hình học. Tuy nhiên, về mặt ứng dụng (trong các bài toán phổ thông), đ này là không thực sự cần thiết vì với D cho trước, ta có thể tìm ra một nghiệm n dương của (1) bằng phương pháp thử vẫ sai. Ta bỏ qua định lý này và chuyển định lý mô tả tất cả các nghiệm của (1) khi biết nghiệm cơ sở.

Với $(x,y),(x',y') \in S$ ta có nếu $x > x'$ thì $y > y'$. Do đó có thể định $(x,y) > (x'y')$ hay là $x > x'$. Với thứ tự này, S là một tập sắp thứ tự tốt. Gọi là phần tử nhỏ nhất của S theo thứ tự trên. Ta gọi (a,b) là nghiệm cơ sở của (

Định lý 8.2 Nếu (a,b) là nghiệm cơ sở của (1) và (x,y) là một nghiệm n dương tùy ý của (1) thì tồn tại số nguyên dương n sao cho $x + y\sqrt{D} = (a + b$ và từ đó mọi nghiệm của (1) đều có thể tìm được bởi công thức

$$x = \frac{(a+b\sqrt{D})^n + (a-b\sqrt{D})^n}{2}, \quad y = \frac{(a+b\sqrt{D})^n - (a-b\sqrt{D})^n}{2\sqrt{D}}$$

Chứng minh. Nhận xét rằng nếu (x,y) là nghiệm của (1) thì $x' = ax - D$ $y' = ay - bx$ cũng là nghiệm của (1) (có thể không nguyên dương)

Trước hết, do $\sqrt{D}$ vô tỷ nên nếu $x + y\sqrt{D} = (a + b\sqrt{D})^n$ thì $x - y\sqrt{}$ $(a - b\sqrt{D})^n$ và từ đó $x^2 - Dy^2 = (a + b\sqrt{D})^n(a - b\sqrt{D})^n = (a^2 - Db^2)^n =$ ra (x,y) là nghiệm của (1) và ta có công thức như trên.

Tiếp theo, giả sử không phải nghiệm nào của (1) cũng có dạng (2). Gọi $(x$ là nghiệm nhỏ nhất không có dạng (2) thì rõ ràng $x* > a, y* > b$. Theo nhận

$$x' = ax^* - Dby* \quad y' = ay* - bx*$$

là nghiệm của (1).

Dễ dàng kiểm tra được rằng 1) $x* > x' > 0$ và 2) $y* > y' > 0$. Từ đó, do tính nhỏ nhất của $(x*, y*)$, tồn tại n nguyên dương sao cho $x' + y'\sqrt{D} = (a + b\sqrt{D})^n$. Giải hệ (3) với ẩn là $(x*, y*)$, ta được (chú ý $a^2 - Db^2 = 1$) $x* = ax' + Dby', y* = ay' + bx'$. Từ đó

$$x* + y*\sqrt{D} = ax' + Dby' + (ay' + bx')\sqrt{D} = (a + b\sqrt{D})(x' + y'\sqrt{D}) = (a + b\sqrt{D})$$

mâu thuẫn!

Vậy điều giả sử là sai và (2) là tất cả các nghiệm của (1).

Tiếp theo, ta xét phương trình dạng Pell, tức là phương trình dạng

$$x^2 - Dy^2 = k \tag{4}$$

trong đó D không chính phương và $k \notin \{0, 1\}$.

Ta có một số nhận xét sau

(i) Không phải với cặp D, k nào phương trình (4) cũng có nghiệm. Chẳng hạn, phương trình $x^2 - 3y^2 = -1$.

(ii) Nếu phương trình (4) có nghiệm nguyên dương thì nó có vô số nghiệm nguyên dương. Lý do: nếu (x, y) là nghiệm của (4) thì

$$x' = ax + Dby \quad y' = ay + bx$$

cũng là nghiệm của (4), trong đó (a, b) là nghiệm cơ sở của phương trình.

Như thường lệ, ta đặt $S = \{(x, y) \in (N^+)^2 | x^2 - Dy^2 = k\}$ và gọi (a, b) là nghiệm cơ sở của phương trình Pell tương ứng $x^2 - Dy^2 = 1$. Nghiệm (x_0, y_0) thuộc S được gọi là nghiệm cơ sở của (4) nếu không tồn tại $(x', y') \in S$ sao cho

$$x = ax' + Dby' \quad y = ay' + bx'$$

Gọi S_0 là tập hợp tất cả các nghiệm cơ sở. Ta có định lý quan trọng sau:

Định lý 8.3 Với mọi D, k ta có $|S0| < \infty$.

Chứng minh. Nếu $S_0 = \emptyset$ thì $|S_0| = 0 < \infty$. Tiếp theo giả sử $S_0 \neq \emptyset$. Gọi (x, y) là một nghiệm cơ sở nào đó của (4). Xét hệ

$$ax' + Dby' = x \quad ay' + bx' = y$$

có nghiệm $x' = ax - Dby, y' = ay - bx$. Dễ dàng chứng minh được $(x')^2 - D(y')^2 = 1$. Vì $(x, y) \in S_0$ nên theo định nghĩa $(x', y') \notin S$. Điều này xảy ra khi và chỉ khi $x' \leqslant 0$ hoặc $y' \leqslant 0$ nghĩa là $ax \leqslant Dby$ hoặc $ay \leqslant bx$, tương đương với $x^2 \leqslant -kDb^2$ (5) hoặc $y^2 \leqslant kb^2$ (6).

Nếu (5) xảy ra thì ta có đánh giá $y^2 = (x^2 - k)/D \leqslant -k(Db^2 + 1)/D$. Nếu (6) xảy ra thì ta có $x^2 = Dy^2 + k \leqslant Dkb^2 + D$. Trong cả hai trường hợp, ta có $|S_0| < \infty$.

Cuối cùng, chú ý rằng từ một nghiệm (x, y) bất kỳ của (4) không thuộc S_0 cách đi ngược xuống bằng công thức $x' = ax - Dby, y' = ay - bx$ ta luôn có đến một nghiệm cơ sở của (4). Như vậy, với định lý trên, phương trình dạng P được giải quyết hòan toàn. Dưới đây chúng ta xem xét một ví dụ:

Ví dụ 8.1 Tìm tất cả các nghiệm nguyên dương của phương trình $x^2 - 5y^2$ (1).

Lời giải. Bằng phép thử tuần tự, ta tìm được nghiệm cơ sở của phương $x^2 - 5y^2 = 1$ là $(9, 4)$. Theo phép chứng minh định lý 8.3, nghiệm cơ sở của (1 mãn

$$x^2 \leqslant 4.5.4^2, \quad y^2 \leqslant (4.5.42 + 4)/5$$

Từ đây suy ra $x < 17$, $y < 9$. Dùng phép thử tuần tự, ta tìm được hai nghiệm là $(1, 1)$ và $(11, 5)$. Từ hai nghiệm này, bằng công thức

$$x' = 9x + 20y, \quad y' = 4x + 9y$$

ta tìm được tất cả các nghiệm của (1).

Với phép giải phương trình dạng Pell, trên thực tế ta đó có thể giải tất cả phương trình Diophant bậc hai, tức là phương trình dạng

$$ax^2 + bxy + cy^2 + dx + ey + f = 0$$

Dựa vào lý thuyết đường cong bậc hai, ta có thể đưa phương trình trên v trong các dạng chính sau

(i) Dạng ellip: $ax^2 + by^2 = c$ $(a, b, c > 0)$, có hữu hạn nghiệm, giải bằng p pháp thử và sai

(ii) Dạng parabol: $ax^2 + by + c$, giải bằng đồng dư bậc hai

(iii) Dạng hypebol: $ax^2 - by^2 = c$, phương trình dạng Pell

Ngoài ra còn có các dạng suy biết như hai đường thẳng cắt nhau, hai đường song song, ellip o ... Dưới đây, ta xét một ví dụ áp dụng:

Ví dụ 8.2. Tìm tất cả các cặp số nguyên dương (m, n) thỏa mãn phương tr

$$m(m + 1) + n(n + 1) = 3mn$$

Lời giải. Xét phương trình đó cho như phương trình bậc hai theo m

$$m^2 - (3n - 1)m + n(n + 1) = 0$$

Phương trình này có nghiệm nguyên dương khi và chỉ khi Δ là số chính phươ là

$$(3n - 1)^2 - 4n(n + 1) = y^2 \text{ hay là } y^2 - 5(n - 1)^2 = -4$$

ta thu được phương trình dạng Pell mà ta đó biết cách giải.

Phương trình Markov cổ điển là phương trình dạng

$$x_1^2 + x_2^2 + \cdots + x_n^2 = kx_1x_2x_n \tag{1}$$

ở đây n và k là các tham số nguyên dương. Trường hợp riêng khi $n = k = 3$ thì phương trình

$$x^2 + y^2 + z^2 = 3xyz \tag{2}$$

được nghiên cứu chi tiết trong bài báo của A.Amarkov về dạng toàn phương đăng ở Báo cáo VHL KH Liên Xô năm 1951; "Dạng Markov", liên quan chặt chẽ đến phương trình dạng (2) được sử dụng trong lý thuyết xấp xỉ các số vô tỷ bằng các số hữu tỷ.

Đầu tiên, ta chú ý đến một tính chất thú vị của phương trình Markov. Nếu phương trình (1) có một nghiệm thì nó sẽ có rất nhiều nghiệm và có thể tạo ra các nghiệm đó bằng cách sau đây. Ta sẽ coi một biến, chẳng hạn xn, là "ẩn số", còn tất cả các biến khác như các tham số. Khi đó, vì phương trình

$$x^2 - kx_1x_{n-1}x + x_1^2 + \cdots + x_{n-1}^2 = 0$$

là phương trình bậc hai theo x và có nghiệm $x = xn$, nên nó có nghiệm nguyên thứ hai $x'_n = u$; theo định lý Viet ta có

$$u = kx_1x_{n-1} - x_n = (x_1^2 + \cdots + x_{n-1}^2)/x_n \tag{3}$$

Chú ý rằng $u < x_n$ khi và chỉ khi

$$x_1 + \cdots + x_{n-1}^2 < x_1^2 \text{ hay là } 2x_n > kx_1..x_{n-1} \tag{4}$$

Quá trình này có thể thực hiện với mọi biến số x_j trong vai trò của x_n. Nhưng chỉ đối với một biến - biến lớn nhất là có thể xảy ra (4) và ta thu được nghiệm mới $(x_1, x_2, , x'_n)$ "nhỏ hơn" nghiệm cũ (thứ tự theo tổng các biến); như vậy, theo đa số là các nghiệm tăng lên và ta có cây nghiệm.

Tiếp theo, trừ những trường hợp đặc biệt, ta sẽ giả sử rằng $x_1 \leqslant x_2 \leqslant \cdots \leqslant x_n$. Ta sẽ nói nghiệm $(x_1, x_2, , x_n)$ là nghiệm gốc (nghiệm cơ sở), nếu

$$x_1^2 + \cdots + x_{n-1}^2 \geqslant x - n^2 \quad \text{hay là} \quad 2x_n \leqslant kx_1...x_{n-1} \tag{5}$$

(từ nghiệm này, tất cả các nhánh cây đi đến các nghiệm bên cạnh, đều tăng)

Bổ đề 8.4 Nếu phương trình (1) có nghiệm nguyên dương thì nó có nghiệm gốc.

Bổ đề 8.5 Nếu $n > 2$, $(x_1, x_2, , x_n)$ là nghiệm gốc, ngoài ra, $x_1 \leqslant x_2 \leqslant \cdots \leqslant x_n$. Khi đó

$$x_1x_{n-2} \leqslant \frac{2(n-1)}{k}$$

Chứng minh.

$$\begin{aligned} kx_1x_{n-2}x_{n-1}^2 = & \\ & kx_1x_{n-2}x_{n-1}x_n \\ & = x_1^2 + \cdots + x_{n-1}^2 + x_n^2 \\ & = 2(x_1^2 + \cdots + x_{n-1}^2) \\ & = 2(n-1)x_{n-1}^2 \end{aligned}$$

Bổ đề 8.6 Nếu $x_1 \leqslant x_2 \leqslant \cdots \leqslant x_n$ là các số nguyên dương bất kỳ tho mãn kiện $1 < x_n^2 \leqslant x_1^2 + \cdots + x_{n-1}^2$, thì tỷ số $R = (x_1^2 + \cdots + x_n^2)/x_1x_2...x_n$ không quá $(n+3)/2$.

Định lý 8.7 Nếu phương trình (1) có nghiệm và $n \neq k$, thì $n \geqslant 2k-3$ khi và $n > 4k-6$ khi $n = 3, n = 4$.

Từ các định lý và bổ đề trên, với n cho trước, việc tìm tất cả các giá trị k sao cho có nghiệm thực hiện được dễ dàng. Hơn nữa, phương pháp gien được sử dụng ở trên thể áp dụng cho các phương trình dạng tương tự, ví dụ phương trình $(x+y+z)^2 =$

Cuối cùng là một ví dụ khác về ứng dụng của gien

Ví dụ 8.3 (Iran 2001) Giả sử x, y, z là các số nguyên dương thỏa mãn điều $xy = z^2 + 1$. Chứng minh rằng tồn tại các số a, b, c và d sao cho $x = a^2 + b^2$ $c^2 + d^2$ và $z = ac + bd$.

BÀI TẬP

8.1 (Ailen 1995) Tìm tất cả các số nguyên a sao cho phương trình $x^2 + axy + y$ có vô số nghiệm nguyên phân biệt x, y.

8.2 (Đài Loan 1998) Tồn tại hay không nghiệm của phương trình

$$x^2 + y^2 + z^2 + u^2 + v^2 = xyzuv - 65$$

trong tập hợp các số nguyên lớn hơn 1998?

8.3 (Việt Nam 2002) Tìm tất cả các số nguyên dương n sao cho phương $x + y + z + t = n\sqrt{xyzt}$ có nghiệm nguyên dương.

8.4 (Ba Lan 2002) Tìm tất cả các cặp số nguyên dương x, y thỏa mãn phương $(x+y)^2 - 2(xy)^2 = 1$.

8.5 (Mỹ 2002) Tìm tất cả các cặp sắp thứ tự các số nguyên dương (m, n) sa $mn - 1$ chia hết $m^2 + n^2$.

8.6 (Việt Nam 2002, vòng 2) Chứng minh rằng tồn tại số nguyên $m \geqslant 2002$ số nguyên dương phân biệt $a_1, a_2, ..., a_m$ sao cho

$$\prod_{i=1}^{m} a_i^2 - 4\sum_{i=1}^{m} a_i^2$$

là số chính phương.

8.7 (Việt Nam 2002, vòng 2) Tìm tất cả các đa thức $p(x)$ với hệ số nguyên sao cho đa thức

$$q(x) = (x^2 + 6x + 10)(p(x))^2 - 1$$

là bình phương của một đa thức với hệ số nguyên.

8.8 (THTT 6/181) Với giá trị nguyên dương nào của p thì phương trình $x^2+y^2+1 = pxy$ có nghiệm nguyên dương?

8.9 (THTT 4/202) Cho ba số nguyên $a, b, c; a > 0, ac - b^2 = p_1p_2p_m$ trong đó $p_1, p_2, , p_m$ là các số nguyên tố khác nhau. Gọi $M(n)$ là số các cặp số nguyên (x, y) thỏa mãn

$$ax^2 + 2bxy + cy^2 = n$$

8.10 (Đề đề nghị IMO 95) Tìm số nguyên dương n nhỏ nhất sao cho $19n + 1$ và $95n + 1$ đều là các số chính phương.

8.11 Tam giác với cạnh $3, 4, 5$ và tam giác với cạnh $13, 14, 15$ có các cạnh là các số nguyên liên tiếp và có diện tích nguyên. Hãy tìm tất cả các tam giác có tính chất như vậy.

8.12 Chứng minh rằng nếu cả $3n + 1$ và $4n + 1$ đều là các số chính phương thì n chia hết cho 56.

8.13 Trong các hàng của tam giác Pascal, hãy tìm hàng có chứa ba số hạng liên tiếp lập thành một cấp số cộng.

8.14 (Mỹ 1986) Tìm số nguyên dương $n > 1$ nhỏ nhất sao cho trung bình bình phương của n số nguyên dương đầu tiên là một số nguyên.

8.15 Nếu $a, b, q = (a^2+b^2)/(ab+1)$ là các số nguyên dương thì q là số chính phương.

8.16 (MOCP 03) Tìm tất cả giá trị n sao cho phương trình $(x + y + z)^2 = nxyz$ có nghiệm nguyên dương.

8.17 (PTNK 03). Tìm tất cả các số nguyên dương k sao cho phương trình $x^2 - (k^2 - 4)y^2 = -24$.

8.18 Chứng minh rằng phương trình $(k^2 - 4)x^2 - y^2 = 1$ không có nghiệm nguyên với mọi $k > 3$.

8.19 (Mathlinks) Cho $\mathcal{A}$ là tập hợp hữu hạn các số nguyên dương. Chứng minh rằng tồn tại tập hợp hữu hạn các số nguyên dương $\mathcal{B}$ sao cho $\mathcal{A} \subset \mathcal{B}$ và $\prod_{x\in\mathcal{B}} x = \sum_{x\in\mathcal{B}} x^2$.

TÀI LIỆU THAM KHẢO

1. Jean-Marie Monier. *Đại số 1 - Giáo trình toán tập 5*, NXBGD-Dunod 1999.

2. Hà Huy Khoái - Phạm Huy Điển. *Số học thuật toán*, NXB ĐHQG HN 2

3. Lê Hải Châu. *Các bài thi học sinh giỏi Tóan PTTH tòan quốc*, NX 1994.

4. Nguyễn Sinh Nguyên, Nguyễn Văn Nho, Lê Hoành Phò. *Tuyển tập các dự tuyển Olympic Tóan học Quốc tế 1991-2001*, NXBGD 2003.

5. Nguyễn Văn Nho. *Olympic Toán học châu á - Thái Bình Dương 1 2002*, NXBGD 2003.

6. Tập thể tácgiả. *Tuyển tập 5 năm Tạp chí Toán học và Tuổi trẻ*, NX 2003.

7. Arthur Engel. *Problem Solving Strategies*, Springer 1998

8. Goeoge Polya. Gabor Szego, *Problems and Theorems in Analysi* Springer 1976

9. Harvey Cohn. *Advanced Number Theory*, Dover Publications 1980

10. Titu Andreescu, Juming Feng. *Mathematical Olympiads 1999-2000: O Problems from Around the World*, MMA 2000.

11. Titu Andreescu, Juming Feng, Hojoo Lee. *Mathematical Olympiads 2 2002: Olympiads Problems from Around the World*, MMA 2002.

12. Titu Andreescu Razvan Gelca. *Mathematical Olympiads Challenge*. Bi 2000.

13. Walter Mientka others. *Mathematical Olympiads 1996-1997: Olymp Problems from Around the World*, MMA 1997.

14. Walter Mientka others. *Mathematical Olympiads 1997-1998: Olymp Problems from Around the World*, MMA 1998.

15. Bugaenko B.O. *Phương trình Pell* (tiếng Nga), Matxcơva 2001.

16. Badzylev D.F. *Phương trình Diophăng* (tiếng Nga), Minxk 1999.

17. Gelphond A.O. *Giải phương trình nghiệm nguyên* (tiếng Nga), Nauka

18. Serpinski B. *Về giải phương trình nghiệm nguyên* (tiếng Nga), FML

19. Serpinski B. *250 bài toán sơ cấp về lý thuyết số* (tiếng Nga), FML 19

20. Các tạp chí Kvant, AMM, Toán Học Tuổi trẻ, Toán học trong nhà trường

21. Tài liệu trên Internet, đặc biệt là website *www.mccme.ru* và *www.mathli*

PHƯƠNG PHÁP GIẢI BÀI TOÁN CHIA HẾT

Đặng Huy Ruận

Khi có số nguyên a và số tự nhiên b một trong những câu hỏi hiển nhiên được đặt ra là: Liệu a có chia hết cho b không? Có nhiều phương pháp giải bài toán chia hết. Song việc vận dụng phương pháp lại phải phụ thuộc vào dạng bài toán. Dưới đây xin trình bầy một trong các phương pháp đó: phương pháp dùng phép chia có dư, phương pháp đồng dư, phương pháp dùng tính tuần hoàn khi nâng lên lũy thừa, phương pháp quy nạp và sử dụng tiêu chuẩn chia hết.

0.1 Các số nguyên và các phép tính số nguyên

Tập hợp các số nguyên gồm các số tự nhiên $1, 2, 3$, số không 0 và các số nguyên âm $-1, -2, -3$ Trong tập hợp đó luôn luôn thực hiện được phép cộng và phép trừ. Nói cách khác, nếu m và n là các số nguyên, thì tổng $m+n$ của chúng cũng là số nguyên. Hơn nữa, với hai số nguyên m, n tuỳ ý tồn tại duy nhất một số x thoả mãn phương trình

$$n + x = m$$

Số đó được gọi là hiệu của các số m và n đồng thời ký hiệu bằng $m - n$. Hiệu hai số nguyên bất kỳ cũng là số nguyên.

Trong tập hợp các số nguyên cũng luôn luôn thực hiện được phép nhân, nghĩa là, nếu m và n là các số nguyên, thì tích $m.n$ của chúng cũng là số nguyên. Tuy vậy, phép chia (là phép tính ngược của phép nhân) không phải khi nào cũng thực hiện được trong tập hợp các số nguyên. Kết quả của phép chia số a cho số $b \neq 0$ là số x được ký hiệu bằng $a : b$ hoặc $\frac{a}{b}$ thoả mãn phương trình

$$bx = a$$

Số x đó tồn tại và duy nhất. Song kết quả của phép chia một số nguyên cho một số nguyên khác không phải khi nào cũng là một số nguyên. Thí dụ, các thương $3 : 2, 6 : 5, (-50) : 7, (-60) : (-21)$ không phải là các số nguyên. Điều đó có nghĩa là phép chia không phải luôn luôn thực hiện được trong tập hợp các số nguyên. Thương của phép chia số nguyên a cho số nguyên $b \neq 0$ có thể không thuộc tập hợp các số nguyên; còn chính trong tập hợp các số nguyên không tìm được một số nào để ta có thể gọi là thương của phép chia a cho b.

Tất nhiên, ta cũng gặp các trường hợp: Thương của phép chia một số nguyên cho số nguyên khác cũng lại là một số nguyên, chẳng hạn

$$8 : (-2) = -4, 48 : 12 = 4, (-6) : 6 = -1$$

Định nghĩa. Nếu a và b $(b \neq 0)$ là các số nguyên, mà thương $a : b$ cũng nguyên, thì ta nói rằng số a chia hết cho số b và viết $a : b$.

Cũng có thể nói cách khác: Số nguyên a chia hết cho số nguyên $b \neq 0$, nế tại một số nguyên k, sao cho $a = kb$. Định nghĩa về chia hết trên đây sẽ thường sau này.

Vì chỉ nói đến các số nguyên, nên để ngắn gọn ta sẽ viết "số", nhưng luôn hiểu là số nguyên. Xin nhấn mạnh rằng, chỉ có thể nói về thương $a : b$ khi b Trường hợp $b = 0$ thương $a : b$ không xác định, nghĩa là biểu thức $a : 0$ hay $\frac{a}{0}$ k có nghĩa. Tóm lại không thể chia cho số không.

Ngược lại, khi $a = 0$ (và với mọi $b \neq 0$) thương $a : b$ xác định (và bằng khô

$$\frac{0}{b} = 0 \text{ khi } b \neq 0$$

Vì trong trường hợp này số không là số nguyên, nên nó chia hết cho mọi số n khác không (ngoài ra thương bằng không).

0.2 Các định lý về chia hết

Định lý 1. Nếu các số $a_1, a_2, ..., a_n$ chia hết cho m, thì tổng $a_1 + a_2 + \cdots + a$ hết cho m.

Thật vậy, vì $a_i (1 \leqslant i \leqslant n)$ chia hết cho m, nên tồn tại số nguyên k_i , để $a_i =$ Bởi vậy

$$\begin{aligned} a_1 + a_2 + \cdots + a_i + \cdots + a_n &= k_1 m + k_2 m + \cdots + k_i m + \cdots + k_n m \\ &= (\sum_{i=1}^{n} k_i) m. \end{aligned}$$

Vì tổng các số nguyên là số nguyên, nên tổng $a_1 + a_2 + \cdots + a_i + \cdots + a$ hết cho m.

Định lý 2. Nếu c hai số a và b đều chia hết cho m, thì hiệu $a - b$ và $b -$ chia hết cho m.

Thật vậy, vì a, b đều chia hết cho m, nên tồn tại các số nguyên t, s để $a = b = s.m$. Do đó,

$$\begin{aligned} a - b &= tm - sm = (t - s)m \\ b - a &= sm - tm = (s - t)m \end{aligned}$$

Vì hiệu hai số nguyên là một số nguyên nên $(a - b) \vdots m$ và $(b - a) \vdots m$.

Hệ quả 1. Nếu tổng một số số hạng chia hết cho m và trừ một số hạng, còn tất cả các số khác đều chia hết cho m, thì số hạng này cũng chia hết cho m.

Thật vậy, giả sử tổng $S = a_1 + a_2 + \cdots + a_{i-1} + a_i + a_{i+1} + \cdots + a_n$ chia hết cho m và chỉ có a_i, còn $a_1, a_2, ..., a_{i-1}, a_{i+1}, ..., a_n$ đều chia hết cho m. Khi đó tồn tại các số nguyên $s, t_j (1 \leqslant j \leqslant n,\ j \neq i)$ để $S = sm, a_j = t_j m$. Và

$$a_i = S - a_1 - a_s - \cdots - a_{i-1} - a_{i+1} - \cdots - a_n$$
$$a_i = sm - t_1 m - t_2 m - \cdots - t_{i-1} m - t_i m - t_{i+1} m - \cdots - t_n m$$
$$a_i = (s - t_1 - t_2 - \cdots - t_{i-1} - t_i - t_{i+1} - \cdots - t_n) m$$

nêna_i chia hết cho m.

Định lý 3. Nếu mỗi số a_i chia hết cho $m_i (1 \leqslant i \leqslant n)$ thì tích $a_1 a_2 ... a_i a_{i+1} ... a_n$ chia hết cho tích $m_1 m_2 ... m_i m_{i+1} ... m_n$.

Thật vậy, vì a_i chia hết cho $m_i (1 \leqslant i \leqslant n)$, nên tồn tại số nguyên $k_i (1 \leqslant i \leqslant n)$ để $a_i = k_i m_i$. Khi đó

$$a_1.a_2 a_i.a_{i+1} ... a_{n-1} a_n = k_1 m_1.k_2 m_2 ... k_i m_i k_{i+1} m_{i+1} ... k_{n-1} m_{n-1} k_n m_n$$
$$= (k_1 k_2 k_i k_{i+1} ... k_{n-1} k_n)(m_1.m_2 ... m_i.m_{i+1} ... m_{n-1} m_n)$$

Nên tích $a_1.a_2 a_n$ chia hết cho tích $m_1 m_2 ... m_n$.

Hệ quả 2. Nếu a chia hết cho m, thì với số tự nhiên n tuỳ ý a^n chia hết cho m^n.

Hệ quả 3. Nếu chỉ một thừa số chia hết cho m, thì tích cũng chia hết cho m.

Thật vậy, giả sử số a_i chia hết cho m, còn $a_1, a_2, , a_{i-1}, a_{i+1}, ..., a_n$ là các số tuỳ ý. Do a_i chia hết cho m nên tồn tại số nguyên t, để $a_i = t_m$. Khi đó

$$a_1.a_2 a_{i-1}.a_i.a_{i+1} ... a_n = a_1.a_2 ... a_{i-1} t.m a_{i+1} ... a_n = (a_1.a_2 ... a_{i-1} t.a_{i+1} ... a_n) m,$$

nên $a_1.a_2 ... a_{i-1}.a_i.a_{i+1} ... a_n$ chia hết cho m.

0.3 Phép chia có dư

Nếu số a chia cho b có thương là q và số dư là r, thì có thể viết

$$a = bq + r$$

Tuy vậy, không phải mọi cách viết $a = bq + r$ đều được xem là cách viết phép chia có dư. Chẳng hạn, đẳng thức $30 = 4.5 + 10$ đúng, nhưng không thể nói rằng 30 chia cho 5 còn dư 10, vì số dư phải bé hơn số chia. Tương tự như vậy, cách viết $30 = 4.8 + (-2)$ cũng không có nghĩa là 30 chia cho 4 còn dư -2,vì số dư không thể âm. Từ những điều phân tích ở trên nhận thấy rằng, để cách viết

$$a = bq + r$$

Biểu thị phép chia a cho b với số dư r, cần đặt điều kiện cho r không âm hơn b, nghĩa là $0 \leqslant r < b$. Bởi vậy có định nghĩa

0.3.1 Định nghĩa

Giả sử a, b là hai số nguyên và $b > 0$. Ta nói rằng số a chia cho số b có thươn và số dư là r, nếu a có thể biểu diễn bằng đẳng thức $a = bq + r$, trong đó $0 \leqslant$

0.3.2 Sự tồn tại và duy nhất của phép chia có dư

Có hai vấn đề được đặt ra đối với định ngnĩa phép chia có dư là

1. Liệu có thể luôn luôn thực hiện được phép chia có dư hay không? Nói khác, nếu cho số nguyên a và số tự nhiên b, thì luôn luôn có thể chọn đượ số nguyên q và r, để $0 \leqslant r < b$ và $a = bq + r$ hay không?

2. Phép chia có dư có duy nhất hay không? Nói cách khác, nếu số a được diễn bằng hai cách khác nhau dưới dạng

$$a = bq_1 + r_1,\ 0 \leqslant r_1 < b$$
$$a = bq_2 + r_2,\ 0 \leqslant r_2 < b$$

thì hai cách này có nhất thiết phải trùng nhau hay không, nghĩa là, phải có $q_1 = r_1 = r_2$?

Định lý sau sẽ giải đáp cả hai câu hỏi trên và khẳng định phép chia có dư luôn tồn tại và duy nhất.

Định lý 4. Giả sử a là số nguyên và b là số tự nhiên. Khi đó có thể chọn các số nguyên q và r, sao cho $0 \leqslant r < b$ và $a = bq + r$. Các số q, và r xác định các điều kiện trên là duy nhất.

Chọn số tự nhiên c, sao cho $|a| < c$ và xét dãy số

$$-cb,\ (-c+1)b,\ (-c+2)b,\ ...,\ -2b,\ -b,\ 0b,\ 2b,\ ...,\ (c-1)b,\ cb$$

Trong đó kể từ số thứ hai đều lớn hơn số ngay trước nó b đơn vị. Nên đây l dãy tăng và có số đầu $-cb < a$, số cuối $cb > a$ (do $|a| \leqslant c \leqslant cb$ vì $b \geqslant 1$). Điề chứng tỏ rằng trong dãy (1) có một số bé hơn hay bằng a, còn số tiếp theo lớn h Ký hiệu số này là qb. Khi đó số tiếp theo là $(q+1)b$ đã lớn hơn a.

$$qb \leqslant a < (q+1)b$$

Như vậy là thương q đã chọn được. Ký hiệu r là số $a - qb$, nên

$$a = qb + r$$

Khi đó bất đẳng thức (2) có dạng

$$q_b \leqslant qb + r < (q+1)b$$

Bớt cả hai vế của bất đẳng thức trên đi qb đơn vị ta có

$$0 \leqslant r < b$$

Vậy thương q và số dư r đã tìm được.

Ta chứng minh tính duy nhất của dạng biểu diễn phép chia có dư. Giả sử số a có thể biểu diễn bằng ít nhất hai cách khác nhau và hai trong các cách biểu diễn đó là

$$a = bq_1 + r_1, \text{ với } 0 \leqslant r_1 < b$$
$$a = bq_2 + r_2, \text{ với } 0 \leqslant r_2 < b$$

Trừ vế với vế hai đẳng thức trên có

$$(q_1 - q_2)b + (r_1 - r_2) = 0, \tag{3}$$

nghĩa là $r_1 - r_2 = -(q_1 - q_2)b$. Do đó $r_1 - r_2$ chia hết cho b.

Giả sử $r_1 \neq r_2$ và để xác định, ta giả sử $r_1 > r_2$. Khi đó $r_1 - r_2 > 0$. Mặt khác $r_1 - r_2 \leqslant r_1 < b$. Khi đó $r_1 - r_2$ là số tự nhiên bé hơn b, nên nó không thể chia hết cho b. Ta đã đi tới mâu thuẫn, nên $r_1 = r_2$. Bởi vậy đẳng thức (3) có dạng

$$(q_1 - q_2)b = 0$$

Vì $b \neq 0$ (b là số tự nhiên), nên suy ra $q_1 - q_2 = 0$. Nghĩa là $q_1 = q_2$ và dạng biểu diễn phép chia có dư là duy nhất.

Từ định lý trên suy ra rằng, mỗi số nguyên a có thể biểu diễn bằng một trong các dạng sau

$$a = b.q$$
$$a = b.q + 1,$$
$$a = b.q + 2,$$
$$\cdots\cdots\cdots\cdots$$
$$a = b.q + (b-1).$$

0.4 Phương pháp dùng phép chia có dư

Căn cứ vào số chia b, mà xét mọi khả năng phân tích $a = b.q + k$ với $k \in \{1, 2, ..., q-1\}$. Sau đó, với mỗi khả năng phân tích này lý luận để suy ra đáp án của bài toán. Chẳng hạn với $q = 3$ mỗi số nguyên a có thể phân tích thành một trong ba dạng là $3q, 3q+1, 3q+2$. Sau đó thế mỗi dạng biểu diễn vào các vị trí của a rồi lý luận để suy ra đáp số.

Ví dụ 1. Chứng minh rằng với mọi số nguyên a, số $a^3 - a$ chia hết cho 6

Giải. Phân tích biểu thức $a^3 - a$ thành tích của ba thừa số

$$a^3 - a = a(a-1)(a+1)$$

Số a có thể biểu diễn bằng một trong các dạng sau

$$6q,\ 6q+1,\ 6q+2,\ 6q+3,\ 6q+4,\ 6q+5$$

Ta xét từng khả năng phân tích số a

Với $a = 6q$ số $a^3 - a = 6q(6q-1)(6q+1)$ chia hết cho 6;

Với $a = 6q+1$ số $a^3 - a = (6q+1)6q(6q+2)$ chia hết cho 6

Với $a = 6q+2$ số

$$\begin{aligned} a^3 - a &= (6q+2)(6q+1)(6q+3) \\ &= 2(3q+1)(6q+1)3(2q+1) \\ &= 6(3q+1)(6q+1)(2q+1) \end{aligned}$$

chia hết cho 6

Với $a = 6q+3$ số

$$\begin{aligned} a^3 - a &= (6q+3)(6q+2)(6q+4) \\ &= 3(2q+1)2(3q+1)2(3q+2) \\ &= 12(2q+1)(3q+1)(3q+2) \end{aligned}$$

chia hết cho 6.

Với $a = 6q+4$ số

$$\begin{aligned} a^3 - a &= (6q+4)(6q+3)(6q+5) \\ &= 2(3q+2)3(2q+1)(6q+5) \\ &= 6(3q+2)(2q+1)(6q+5) \end{aligned}$$

chia hết cho 6.

Với $a = 6q+5$ số

$$\begin{aligned} a^3 - a &= (6q+5)(6q+4)(6q+6) \\ &= (6q+5)2(3q+2)6(q+1) \\ &= 12(6q+5)(3q+2)(q+1) \end{aligned}$$

chia hết cho 6.

Vậy với mọi số nguyên a số $a^3 - a$ chia hết cho 6.

Nhận xét.

Ngoài cách giải trên có thể lý luận ngắn gọn như sau.

Số

$$a^3 - a = (a-1)a(a+1)$$

chứa hai số nguyên liên tiếp, nên nó chia hết cho 2. Ngoài ra, số này còn chứa ba số nguyên liên tiếp, nên nó chia hết cho 3. Bởi vậy số $a^3 - a$ chia hết cho 6.

Ví dụ 2. Chứng minh rằng với mọi số nguyên a, số $a(a^6 - 1)$ chia hết cho 7 ?

Giải.

Phân tích biểu thức $a(a^6 - 1)$ thành tích ta được

$$a(a^6 - 1) = a(a^3 - 1)(a^3 + 1) = a(a-1)(a+1)(a^2 - a + 1)(a^2 + a + 1)$$

Số a có thể biểu diễn bằng một trong các dạng sau

$$a = 7q,\ a = 7q+1,\ a = 7q+2,\ a = 7q+3,\ a = 7q+4,\ a = 7q+5,\ a = 7q+6$$

Ta xét từng khả năng phân tích số a

Với$a = 7q$ số

$$a(a^6 - 1) = 7q(7q-1)(7q+1)\{(7q)^2 - 7q + 1)\}\{(7q)^2 + 7q + 1)\}$$

chia hết cho 7.

Với $a = 7q+1$ số

$$a(a^6 - 1) = (7q+1)7q(7q+2)\{(7q+1)^2 - 7q\}\{(7q+1)^2 + 7q + 2\}$$

chia hết cho 7.

Với $a = 7q+2$ số

$$\begin{aligned} a(a^6 - 1) &= (7q+2)(7q+1)(7q+3)\{(7q+2)^2 - 7q - 1\}\{(7q+2)^2 + 7q + 3)\} \\ &= (7q+2)(7q+1)(7q+3)\{49q^2 + 28q + 4 - 7q - 1\}\{49q^2 + 28q + 4 + 7q + 3)\} \\ &= (7q+2)(7q+1)(7q+3)\{49q2 + 21q + 3\}7\{7q^2 + 5q + 1\} \end{aligned}$$

chia hết cho 7;

Với $a = 7q+3$ số

$$\begin{aligned} a(a^6 - 1) &= (7q+3)(7q+2)(7q+4)\{(7q+3)^2 - 7q - 2\}\{(7q+3)^2 + 7q + 4)\} \\ &= (7q+3)(7q+2)(7q+4)\{(49q^2 + 42q + 9 - 7q - 2\}\{49q^2 + 42q + 9 + 7q + 4)\} \\ &= (7q+3)(7q+2)(7q+4)7\{7q^2 + 5q + 1\}\{49q^2 + 7q + 13\} \end{aligned}$$

chia hết cho 7.

Với $a = 7q + 4$ số

$$a(a^6 - 1) = (7q + 4)(7q + 3)(7q + 5)\{(7q + 4)^2 - 7q - 3\}\{(7q + 4)^2 + 7q -$$
$$= (7q + 4)(7q + 3)(7q + 5)\{49q^2 + 56q + 16 - 7q - 3\}\{49q^2 + 56q + 16 + 7($$
$$= (7q + 4)(7q + 3)(7q + 5)\{49q^2 + 49q + 13\}7\{7q^2 + 9q +$$

chia hết cho 7.

Với $a = 7q + 5$ số

$$a(a^6 - 1) = (7q + 5)(7q + 4)(7q + 6)\{(7q + 5)^2 - 7q - 4\}\{(7q + 5)^2 + 7q -$$
$$= (7q + 5)(7q + 4)(7q + 6)\{49q^2 + 70q + 25 - 7q - 4\}\{49q^2 + 70q + 25 + 7($$
$$= (7q + 5)(7q + 4)(7q + 6).7.\{7q^2 + 9q + 3\}\{49q^2 + 77q +$$

chia hết cho 7.

Với $a = 7q + 6$ số

$$a(a^6 - 1) = (7q + 6)(7q + 5)(7q + 7)\{(7q + 6)^2 - 7q - 5\}\{(7q + 6)^2 + 7q -$$
$$= (7q + 6)(7q + 5).7.(q + 1)\{49q^2 + 84q + 36 - 7q - 5\}\{49q^2 + 84q + 36 + 7($$
$$= (7q + 6)(7q + 5).7.(q + 1)\{49q^2 + 77q + 31\}\{49q^2 + 91q +$$

chia hết cho 7.

Vậy số $a(a^6 - 1)$ chia hết cho 7.

Ví dụ 3. Chứng minh rằng không có giá trị nào của a, để số a^2+1 chia hết

Giải. Số a có thể biểu diễn bằng một trong ba cách sau

$$a = 3q,\ a = 3q + 1,\ a = 3q + 2$$

Xét mọi khả năng phân tích số a

Với $a = 3q$ số$a^2+1 = 9q^2+1$ chia cho 3 còn dư 1, nên a^2+1 không chia hết

Với $a = 3q + 1$ số

$$a^2 + 1 = (3q + 1)2 + 1$$
$$= 9q^2 + 6q + 2$$
$$= 3(3q^2 + 2q) + 2$$

chia cho 3 còn dư 2, nên $a^2 + 1$ không chia hết cho 3.

Với $a = 3q+2$ số

$$\begin{aligned} a^2 + 1 &= (3q+2)^2 + 1 \\ &= 9q^2 + 12q + 4 + 1 \\ &= 3(3q^2 + 4q + 1) + 2 \end{aligned}$$

chia cho 3 còn dư 2, nên $a^2 + 1$ không chia hết cho 3.

Vậy $a^2 + 1$ không chia hết cho 3.

BÀI TẬP

1. Chứng minh rằng nếu các số a và b không chia hết cho 3. Nhưng có cùng số dư khi chia cho 3, thì số $ab - 1$ chia hết cho 3. Ngược lại nếu $ab - 1$ chia hết cho 3 thì các số a và b không chia hết cho 3 và có cùng dư số khi chia cho 3.
2. Chứng minh rằng nếu các số a và b không chia hết cho 3 và có số dư khác nhau khi chia cho 3, thì số $ab + 1$ chia hết cho 3. Ngược lại, nếu $ab + 1$ chia hết cho 3, thì các số a và b không chia hết cho 3 và có số dư khác nhau khi chia cho 3.
3. Chứng minh rằng với các số a và b bất kỳ số $ab(a^2 - b^2)(4a^2 - b^2)$ luôn luôn chia hết cho 5.
4. Chứng minh rằng nếu dù chỉ một số a hay b không chia hết cho 7 thì $a^2 + b^2$ cũng không chia hết cho 7.
5. Chứng minh rằng với các số nguyên a, b, c bất kỳ, số $a^2 + b^2 + c^2 + 1$ không chia hết cho 8.
6. Chứng minh rằng nếu tổng của ba số nguyên chia hết cho 6, thì tổng lập phương của chúng cũng chia hết cho 6.
7. Cho hai số gồm ba chữ số, không có số nào chia hết cho 37, còn tổng của chúng chia hết cho 37. Viết số này kề với số kia, ta nhận được một số gồm sáu chữ số. Chứng minh rằng số này chia hết cho 37.
8. Cho hai số gồm ba chữ số có cùng số dư khi chia cho 7. Viết số này kề số kia ta nhận được một số gồm sáu chữ số. Chứng minh rằng số đó chia hết cho 7.
9. Cho x, y là các số nguyên. Chứng minh rằng $x^2 + y^2$ chia hết cho 3 khi và chỉ khi cả hai số x, y đồng thời chia hết cho 3.
10. Với a là số nguyên. Chứng minh rằng $a^5 - a$ chia hết cho 3.

0.5 Phương pháp đồng dư

0.5.1 Phép đồng dư

Định nghĩa. Nếu hai số a và b có cùng số dư khi chia cho m, thì ta nói rằng a và b đồng dư theo modun m và viết

$$a \equiv b \pmod{m}$$

Và đọc là a đồng dư với b theo modun m. Sử dụng cách viết trên đây thuận tiệ
việc phát biểu và tính toán. Sau đây sẽ trình bày một số định lý đơn giản về đồi

Định lý 5. Phép đồng dư $a \equiv b \pmod{m}$ có nghĩa khi và chỉ khi hiệu
chia hết cho m. Nói cách khác, các số a và b có cùng số dư khi chia cho m, n
chỉ nếu hiệu $a - b$ chia hết cho m.

Chứng minh. Giả sử $a \equiv b \pmod{m}$. Khi đó các số a và b có cùng số c
khi chia cho m. Bởi vậy

$$a = mq + r,\ b = mq' + r,$$

trong đó q, q' là các số nguyên nào đó. Trừ vế với vế hai đẳng thức trên ta được

$$a - b = mq - mq' = m(q - q')$$

Do đó hiệu $a - b$ chia hết cho m.
Ngược lại, giả sử hiệu $a - b$ chia hết cho m. Khi đó tồn tại số nguyên k, để

$$a - b = k.m$$

Chia (có dư) số b cho m:

$$b = q.m + r, \quad \text{trong đó } 0 \leqslant r < m$$

Cộng vế với vế đẳng thức (1) và (2) ta được

$$a = k.m + q.m + r = (k + q).m + r$$

đồng thời r vẫn thoả mãn bất đẳng thức kép $0 \leqslant r < m$, nghĩa là a có cùng số c
b khi chia cho m, tức $a \equiv b \pmod{m}$.

Định lý 6. Các phép đồng dư có thể cộng vế với vế, nghĩa là, nếu a_i
$\pmod{m}$ $(0 \leqslant i \leqslant n)$, thì

$$a_1 + a_2 + \cdots + a_i + \cdots . + a_n \equiv b_1 + b_2 + \cdots + b_i + \cdots . + b_n \pmod{m}$$

Nói cách khác, nếu a_i và $b_i (0 \leqslant i \leqslant n)$ có cùng số dư khi chia cho m, thì các t

$$a_1 + a_2 + \cdots + a_n \quad \text{và} \quad b_1 + b_2 + \cdots + b_n$$

cũng có cùng số dư khi chia cho m.

Chứng minh. Vì $a_i \equiv b_i$ $(0 \leqslant i \leqslant n)$, nên theo Định lý 5, các số $a_i - b_i$
$i \leqslant n)$ chia hết cho m. Bởi vậy tồn tại các số nguyên k_i để $a_i - b_i = k_i m$. Khi

$$\begin{aligned}(a_1 + a_2 + \cdots + a_n) - (b_1 + b_2 + \cdots + b_n) &= (a_1 - b_1) + (a_2 - b_2) + \cdots + (a \\ &= k_1 m + k_2 m + \cdots + k_n m \\ &= (k_1 + k_2 + \cdots + k_n)m\end{aligned}$$

Vậy hiệu $(a_1 + a_2 + \cdots + a_n) - (b_1 + b_2 + \cdots + b_n)$ chia hết cho m, nên, theo
lý 5,

$$a_1 + a_2 + \cdots + a_i + \cdots + a_n \equiv b_1 + b_2 + \cdots + b_i + \cdots + b_n \pmod{m}$$

Định lý 7. Các phép đồng dư có thể trừ vế với vế, nghĩa là từ $a \equiv b \pmod m$, $c \equiv d \pmod m$ suy ra $a - c \equiv b - d \pmod m$.

Chứng minh. Vì $a \equiv b \pmod m$ và $c \equiv d \pmod m$, nên theo định lý 5, các số $a - b$ và $c - d$ chia hết cho m. Do đó tồn tại các số nguyên k, l, để $a - b = k.m$, $c - d = l.m$. Trừ vế với vế hai đẳng thức trên ta được

$$(a - c) - (b - d) = (a - b) - (c - d) = km - lm = (k - l)m$$

Bởi vậy $(a - c) - (b - d)$ chia hết cho m. Do đó, theo định lý 5, $(a - c) \equiv (b - d) \pmod m$.

Định lý 8. Các phép đồng dư có thể nhân vế với vế, nghĩa là, nếu $a_1 \equiv b_1 \pmod m$, $a_2 \equiv b_2 \pmod m$, ..., $a_i \equiv b_i \pmod m$, ..., $a_n \equiv b_n \pmod m$, thì

$$a_1 a_2 ... a_i .... a_n \equiv b_1 b_2 ... b_i ... b_n \pmod m$$

Chứng minh. Định lý được chứng minh bằng quy nạp theo n.

Cơ sở quy nạp: Với $n = 2$ ta có $a_1 \equiv b_1 \pmod m$, $a_2 \equiv b_2 \pmod m$ nên theo định lý 5, các hiệu $a_1 - b_1$, $a_2 - b_2$ chia hết cho m. Khi đó tồn tại các số nguyên k_1, k_2 để

$$a_1 - b_1 = k_1 m, \quad a_2 - b_2 = k_2 m$$

Do đó

$$\begin{aligned} a_1 a_2 - b_1 b_2 &= a_1 a_2 - a_1 b_2 + a_1 b_2 - b_1 b_2 \\ &= (a_1 a_2 - a_1 b_2) + (a_1 b_2 - b_1 b_2) \\ &= a_1 (a_2 - b_2) + b_2 (a_1 - b_1) \\ &= a_1 k_2 m + b_2 k_1 m \\ &= (a_1 k_2 + b_2 k_1) m \end{aligned}$$

Bởi vậy $a_1 a_2 - b_1 b_2$ chia hết cho m nên, theo định lý 4, $a_1 a_2 \equiv b_1 b_2 \pmod m$.

Quy nạp, giả sử khẳng định đã đúng với $n = t$, $t \geqslant 2$, nghĩa là từ t phép đồng dư tùy ý

$a_1 \equiv b_1 \pmod m$, $a_2 \equiv b_2 \pmod m$, ..., $a_i \equiv b_i \pmod m$, ..., $a_t \equiv b_t \pmod m$

đã suy ra được

$$a_1 a_2 ... a_i ... a_t \equiv b_1 b_2 ... b_i ... b_t \pmod m \tag{1}$$

Xét $t + 1$ phép đồng dư bất kỳ, $a_1 \equiv b_1 \pmod m$, $a_2 \equiv b_2 \pmod m$, ..., $a_t \equiv b_t \pmod m$, ..., $a_{t+1} \equiv b_{t+1} \pmod m$.
Khi đó, theo giả thiết quy nạp từ t phép đồng dư đầu đã có

$$a_1 a_2 ... a_t \equiv b_1 b_2 ... b_t \pmod m$$

Ký hiệu, $a_1a_2...a_t$ bằng A_t, còn $b_1b_2...b_t$ bằng B_t. Khi đó, theo định lý 5, hiệu A chia hết cho m, nên tồn tại số nguyên l, để $A_t - B_t = l.m$.

Do $a_{t+1} \equiv b_{t+1} \pmod{m}$, nên, theo định lý 5, $a_{t+1} - b_{t+1}$ chia hết cho m vậy tồn tại số nguyên k, để $a_{t+1} - b_{t+1} = k.m$.
Xét hiệu

$$\begin{aligned} A_t a_{t+1} - B_t.b_{t+1} &= A_t a_{t+1} - A_t b_{t+1} + A_t b_{t+1} - B_t b_{t+1} \\ &= A_t(a_{t+1} - b_{t+1}) + b_{t+1}(A_t - B_t) \\ &= A_t.k.m + b_{t+1}.l.m \\ &= (A_t.k + b_{t+1}.l)m \end{aligned}$$

nên $a_1a_2....a_ta_{t+1} - b_1b_2...b_tb_{t+1} = A_ta_{t+1} - B_tb_{t+1}$ chia hết cho m. Do đó, định lý 5, thì

$$a_1a_2...a_n \equiv b_1b_2...b_n \pmod{m}$$

Từ định lý 7 suy ra các hệ quả sau:

Hệ quả 2. Các phép đồng dư có thể nâng lên lũy thừa, nghĩa là, nếu a (mod m) thì với mọi số nguyên không âm n đều có $a^n \equiv b^n \pmod{m}$.

Hệ quả 3. Giả sử $P(x)$ là đa thức tùy ý với hệ số nguyên

$$P(x) = t_o + t_1x + t_2x^2 + \cdots . + t_nx^n$$

Khi đó nếu $a \equiv b \pmod{m}$, thì

$$P(a) = t_0 + t_1a + t_2a^2 + \cdots + t_na^n \equiv t_o + t_1b + t_2b^2 + \cdots + t_nb^n = P(b) \quad (:$$

0.5.2 Phương pháp đồng dư

Ta sẽ vận dụng các tính chất của phép đồng dư để giải bài toán chia hết.

Ví dụ 4. Chứng minh rằng số $5^{8^{2004}} + 23$ chia hết cho 24.

Giải. Ta sẽ chứng minh khẳng định tổng quáát rằng với mọi số tự nhiên $5^{8^n} + 23$ chia hết cho 24. Thật vậy, do $5^{8^n} = 5^{8.8^{n-1}} = 25^{4.8^{n-1}}$ và $25 \equiv 1 \pmod{}$ nên $25^{4.8^{n-1}} \equiv 1 \pmod{24}$. Bởi vậy, $5^{8^n} \equiv 1 \pmod{24}$. Do đó

$$5^{8^n} + 23 \equiv 24 \equiv 0 \pmod{24}$$

Nên $5^{8^n} + 23$ chia hết cho 24.

Ví dụ 5. Chứng minh rằng với mọi số tự nhiên n, số $12^{2n+1} + 11^{n+2}$ chi cho 133.

Giải. Ta có $12^{2n+1} = 12.12^{2n} = 12\{(12)^2\}^n = 12.144^n$. Vì $144 \equiv 11 \pmod{133}$, nên $144^n \equiv 11^n \pmod{133}$. Nhân cả hai vế với 12 ta có

$$12.144^n = 12.11^n$$

Bởi vậy

$$12^{2n+1} \equiv 12.11^n \pmod{133} \tag{1}$$

Mặt khác,

$$1^{n+2} = (11^2)^n = 121^n$$

Do

$$121 \equiv -12 \pmod{133}$$

Nên

$$121.11^n \equiv -12.11^n \pmod{1)33}$$

Bởi vậy

$$11^{n+2} \equiv -12.11^n \pmod{133} \tag{2}$$

Cộng vế với vế các phép đồng dư (1) và (2) được

$$12^{2n+1} + 11^{n+2} \equiv 0 \pmod{133}$$

Do đó $12^{2n+1} + 11^{n+2}$ chia hết cho 133.

Ví dụ 6. Chứng minh rằng, nếu $a^2 + b^2 + c^2$ chia hết cho 9, thì ít nhất một trong các hiệu $a^2 - b^2$, $a^2 - c^2$, $b^2 - c^2$ chia hết cho 9.

*Giải.*Khi chia số nguyên tuỳ ý n cho 9 nhận được một trong các số dư $0, 1, 2, 3, 4, 5, 6$ Bởi vậy,

Nếu $n \equiv 0 \pmod{9}$, thì $n^2 \equiv 0 \pmod{9}$

Nếu $n \equiv 1 \pmod{9}$, thì $n^2 \equiv 1 \pmod{9}$

Nếu $n \equiv 2 \pmod{9}$, thì $n^2 \equiv 4 \pmod{9}$

Nếu $n \equiv 3 \pmod{9}$, thì $n^2 \equiv 9 \equiv 0 \pmod{9}$

Nếu $n \equiv 4 \pmod{9}$, thì $n^2 \equiv 16 \equiv 7 \pmod{9}$

Nếu $n \equiv 5 \pmod{9}$, thì $n^2 \equiv 25 \equiv 7 \pmod{9}$

Nếu $n \equiv 6 \pmod{9}$, thì $n^2 \equiv 36 \equiv 0 \pmod{9}$

Nếu $n \equiv 7 \pmod{9}$, thì $n^2 \equiv 49 \equiv 4 \pmod{9}$

Nếu $n \equiv 8 \pmod{9}$, thì $n^2 \equiv 64 \equiv 1 \pmod{9}$

Vậy dù với số nguyên n nào đi chăng nữa, số n^2 cũng chỉ có thể có một các số dư $0, 1, 4, 7$ khi chia cho 9. Dùng r_1, r_2, r_3 để ký hiệu các số dư tương ứ a_2, b_2, c_2 khi chia cho 9.
Khi đó

$$a_2 \equiv r_1 \pmod 9,\ b_2 \equiv r_2 \pmod 9,\ c_2 \equiv r_3 \pmod 9$$

Cộng vế với vế các phép đồng dư trên ta được

$$a^2 + b^2 + c^2 \equiv r_1 + r_2 + r_3 \pmod 9$$

Vì $a^2 + b^2 + c^2$ chia hết cho 9, nên

$$a^2 + b^2 + c^2 \equiv 0 \pmod 9$$

Do đó

$$r_1 + r_2 + r_3 \equiv 0 \pmod 9$$

Vì mỗi số r_1, r_2, r_3 chỉ có thể nhận các giá trị $0, 1, 4, 7$, nên $r_1 + r_2 + r_3$ chỉ chia hết cho 9 trong các trường hợp sau

1) $r_1 = r_2 = r_3 = 0$,

2) Một trong các số r_1, r_2, r_3 bằng 1 và hai số còn lại bằng 4,

3) Một trong các số r_1, r_2, r_3 bằng 7, hai số còn lại bằng 1,

4) Một trong các số r_1, r_2, r_3 bằng 4, hai số còn lại bằng 7,

Trong mọi trường hợp đều có ít nhất hai trong các số r_1, r_2, r_3 bằng nhau. Điề có nghĩa là ít nhất hai trong các số a_2, b_2, c_2 có cùng số dư khi chia cho 9, nên nhất một trong các hiệu $a^2 - b^2$, $a^2 - c^2$, $b^2 - c^2$ chia hết cho 9.

BÀI TẬP

11. Với mọi số nguyên không âm n hãy chứng minh rằng
    a) $6^{2n} + 3^{n+2} + 3^n$ chia hết cho 11.
    b) $6.2^{5n+3} + 5^n.3^{n+1}$ chia hết cho 17
    c) $5^{2n+1}.2^{n+2} + 3^{n+2}.2^{2n+1}$ chia hết cho 19.

12 Chứng minh rằng không tồn tại một số n nào để các số $3n - 1$, $5n + 2$, 2, $7n + 3$, $7n - 2$ là các số chính phương.

13 Chứng minh rằng, với các số tự nhiên k, n tuỳ ý số $1^{2k-1} + 2^{2k-1} + \cdots + (2n$ chia hết cho $2n + 1$.

14 Chứng minh rằng số 100...001 (với số số 0 chẵn) chia hết cho 11.

0.6 Phương pháp sử dụng tính tuần hoàn khi nâng lên lũy thừa

0.6.1 Sự tuần hoàn của các số dư khi nâng lên lũy thừa

Xét các lũy thừa liên tiếp của số 2;

$$2^1, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9, ...$$

và tìm xem khi chia các luỹ thừa này cho 5 nhận được các loại số dư nào? Nếu tìm trực tiếp thì khá phức tạp và lũy thừa càng lớn, thì càng khó khăn. Song, nhờ việc nâng lên lũy thừa hai vế của phép đồng dư có thể tìm các số dư của lũy thừa một cách dễ dàng.

Thật vậy, ta có

$$2^1 = 2,\ 2^2 = 4,\ 2^3 = 8 \equiv 3 \pmod 5,\ 2^4 = 16 \equiv 1 \pmod 5 \qquad (1)$$

Để tìm số dư khi chia 25 cho 5 ta nhân cả hai vế phép đồng dư (1) với 2 sẽ được

$$2^5 \equiv 2 \pmod 5$$
$$2^6 \equiv 4 \pmod 5$$
$$2^7 \equiv 4.2 \equiv 8 \equiv 3 \pmod 5$$

Tiếp theo

$$2^8 \equiv 3.2 \equiv 6 \equiv 1 \pmod 5$$
$$\cdots\cdots\cdots\cdots$$

Viết các kết quả vào hai hàng. Hàng trên ghi các luỹ thừa, hàng dưới ghi số dư tương ứng khi chia các lũy thừa này cho 5.

2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}	2^{11}	...
2	4	3	1	2	4	3	1	2	4	3	...

Hàng thứ hai cho ta thấy rằng các số dư lập lại một cách tuần hoàn: sau 4 số dư $2, 4, 3, 1$ lại lặp lại theo đúng thứ tự trên và cứ tiếp tục lặp lại theo thứ tự trên v.v

Xét các số dư của phép chia lũy thừa của 3 cho 7

Ta có

$$3^1 = 3$$
$$3^2 = 9 \equiv 2 \pmod 7$$

Nhân phép đồng dư trên với 3, sau lại nhân phép đồng dư nhận được với 3, ta được

$$3^3 \equiv 6 \pmod 7$$
$$3^4 \equiv 6 \times 3 \equiv 4 \pmod 7$$
$$3^5 \equiv 4 \times 3 \equiv 5 \pmod 7$$
$$3^6 \equiv 5 \times 3 \equiv 1 \pmod 7$$

Tiếp tục tính toán như trên sẽ được hai hàng sau

3	3^2	3^3	3^4	3^5	3^6	3^7	3^8	3^9	3^{10}	3^{11}	3^{12}	...
3	2	6	4	5	1	3	2	6	4	5	1	...

(dưới mỗi lũy thừa là số dư của nó khi chia cho 7)

Xét các số dư khi chia luỹ thừa của 5 cho 16 ta được hai hàng tương ứng:

5	5^2	5^3	5^4	5^5	5^6	5^7	5^8	5^9	5^{10}	5^{11}	...
5	9	13	1	5	9	13	1	5	13	1	...

(dưới mỗi lũy thừa là số dư của nó khi chia cho 16)

Nhìn vào hàng hai ta dễ dàng nhận thấy các số dư lặp lại sau 4 số dư $5, 9,$ rồi lại lặp lại đúng thứ tự như trên.vv...

quảan sát sự tuần hoàn của các số dư khi nâng lên lũy thừa trong các ví dụ một câu hỏi tự nhiên đặt ra là: Phải chăng với các số tự nhiên bất kỳ a và m c dư của phép chia các lũy thừa của a cho m lặp lại một các tuần hoàn? Thật vậ giải đáp câu hỏi trên ta chứng minh khẳng định sau

Định lý 9. Đối với các số tự nhiên a và m tùy ý các số dư của phép $a, a^2, a^3, a^4, a^5, a^6 \cdots$ cho m lặp lại một cách tuần hoàn (có thể không bắt đ đầu).

Chứng minh. Ta lấy $m+1$ lũy thừa đầu tiên

$$a,\ a^2,\ a^3, ..., a^m, a^{m+1}$$

và xét các số dư của chúng khi chia cho m. Vì khi chia cho m chỉ có thể c số dư $\{0, 1, 2, ..., m-2, m-1\}$, mà lại có $m+1$ số, nên trong các số trên ph hai số có cùng số dư khi chia cho m. Chẳng hạn, hai số đó là a^k và a^{k+l}, trong đó l

Khi đó

$$a^k \equiv a^{k+l} \pmod{m}$$

Với mọi $n \geqslant k$ nhân cả hai vế của phép đồng dư (1) với a^{n-k} sẽ được

$$a^n \equiv a^{n+l} \pmod{m}$$

Điều này chứng tỏ rằng bắt đầu từ vị trí tương ứng với a^k các số dư lặp lại hoàn, tức bắt đầu từ số tương ứng với a^k có một số dư lặp lại và lặp lại v.v...

Số l được gọi là chu kỳ tuần hoàn của các số dư khi chia lũy thừa của a cho

Nhận xét.

Từ chứng minh trên nhận thấy rằng sự tuần hoàn của các số dư bắt đầu từ c phát hiện ra hai số dư trùng nhau. Mặt khác để phát hiện ra hai số dư giống nha

chia cho m ta không phi quảảan tâm đến cả số a mà chỉ cần lấy $m+1$ lũy thừa đầu tiên là đủ.

Nếu tồn tại số l, để $a^l \equiv l \pmod m$, thì với mọi số tự nhiên n $a^{n+l} \equiv a^n \pmod m$, nên l chẳng những là chu kỳ tuần hoàn của các số dư, mà còn có thể xem là chỉ số bắt đầu sự tuần hoàn của các số dư.

0.6.2 Thuật toán

Để giải bài toán chia hết, cần xác định số dư của lũy thừa a^n chia cho m, ta cần tìm các số tự nhiên k, l nhỏ nhất, để

$$a^k \equiv a^{k+l} \pmod m$$

Sau đó căn cứ vào số dư r của n chia cho l, mà xác định số dư tương ứng với a^{k+r}.

Chú ý.

1) Trong trường hợp tồn tại số tự nhiên s, để

$$a^s \equiv 1 \pmod m$$

ta chỉ việc tìm các số tự nhiên nhỏ nhất k, l sao cho

$$a^k \equiv a^{k+l} \equiv 1 \pmod m$$

sau đó tìm số dư r của n chia cho l và xác định số dư của a^r khi chia cho m. Đây chính là số dư của a^n chia cho m.

2) Khi lũy thừa có số mũ không phải là hàm tuyến tính của n, chẳng hạn, $a^{p(n)}$ với $p(n)$ là một hàm mũ, mà ta có thể thay đổi cơ số từ a sang b, để có

$$a^{p(n)} = b^{q(n)} \quad \text{và} \quad b \equiv 1 \pmod m$$

thì

$$a^{p(n)} \equiv 1^{q(n)} \equiv 1 \pmod m$$

Trường hợp không biến đổi được cơ số như trên cần tìm cách thay đổi cơ số, để lũy thừa có số mũ là một số tự nhiên rồi tìm số dư như thuật toán đã nêu.

Ví dụ 7. Chứng minh rằng số $5^{8^{2004}} + 5$ chia hết cho 6.

Giải. Ta sẽ chứng minh trường hợp tổng quảát: Với mọi số tự nhiên n số $5^{8^n} + 5$ chia hết cho 6. Do

$$5^{8^n} = 5^{8 \times 8^{n-1}} = 5^{2 \times 4 \times 8^{n-1}} = (25)^{4 \times 8^{n-1}}$$

Vì $25 \equiv 1 \pmod 6$, nên

$$5^{8^n} = (25)^{4 \times 8^{n-1}} \equiv 1 \pmod 6$$

Mặt khác $5 \equiv 5 \pmod 6$.
Vậy $5^{8^n} + 5 \equiv 6 \equiv 0 \pmod{}$. Do đó $5^{8^n} + 5$ chia hết cho 6. Thay $n = 2004$ ta $5^{8^{2004}} + 5$ chia hết cho 6.

Ví dụ 8. Chứng minh rằng $14^{8^{2004}} + 10$ chia hết cho 11.

Giải. Tìm số dư của $14^{8^{2004}} + 8$ chia cho 11. Do $14 \equiv 3 \pmod{11}$, nên $1 \pmod{11}$.

Do $3^8 = 6561 \equiv 5 \pmod{11}$, nên $3^{8^{2004}} = 6561^{2004} \equiv 5^{2004} \pmod{11}$.

Xét các số dư thuộc lũy thừa của 5 khi chia cho 11

5	5^2	5^3	5^4	5^5	5^6	5^7	5^8
5	4	9	1	5	4	9	1

nên

$$5^{4\times 501} = (5^4)^{501} \equiv 1^{501} \equiv 1 \pmod{11}$$

Mặt khác,

$$10 \equiv 10 \pmod{11}$$

Cộng vế với vế phép đồng dư (1) và (2) có

$$14^{8^{2004}} + 10 \equiv 11 \equiv 0 \pmod{11}$$

Nên $14^{8^{2004}} + 10$ chia hết cho 11.

Ví dụ 9. Chứng minh rằng số $222^{555} + 555^{222}$ chia hết cho 7.

Giải.
1) Do $222 = 7 \times 31 + 5$, nên $222 \equiv 5 \pmod 7$. Bởi vậy,

$$222^{555} \equiv 5^{555} \pmod 7$$

Xét sự tuần hoàn của các số dư khi chia lũy thừa của 5 cho 7 ta được

5	5^2	5^3	5^4	5^5	5^6	5^7	5^8	$\cdots$
5	4	6	2	3	1	5	4	$\cdots$

Như vậy

$$5^6 \equiv 1 \pmod 7$$

Với mọi số tự nhiên t, nâng cả hai vế của phép đồng dư (1) lên lũy thừa t ta

$$5^{6t} \equiv 1 \pmod 7$$

Mặt khác $555 = 6.92 + 3$, nên $5^{555} = 5^{6.92+3} = 5^{6.92}.5^3 \equiv 6 \pmod 7$. Do đó

$$222^{555} \equiv 6 \pmod 7 \tag{2}$$

2) Do $555 = 7.79 + 2$, nên $555 \equiv 2 \pmod 7$. Bởi vậy, $555^{222} \equiv 2^{222} \pmod 7$.

Xét sự tuần hoàn của các số dư khi chia lũy thừa của 2 cho 7 ta được

2	2^2	2^3	2^4	2^5	2^6	2^7	2^8	...
2	4	1	2	4	2	4	1	...

Như vậy

$$2^3 \equiv 1 \pmod 7 \tag{3}$$

Với mọi số tự nhiên s nâng cả hai vế của phép đồng dư (3) lên lũy s ta có

$$2^{3s} \equiv 1 \pmod 7$$

Mặt khác, $222 = 3.74$, nên

$$555^{222} \equiv 2^{3\times 74} \equiv 1 \pmod 7 \tag{4}$$

Cộng vế với vế các phép đồng dư (2) và (4) có

$$222^{555} + 555^{222} \equiv 6 + 1 \equiv 0 \pmod 7$$

Vậy số $222^{555} + 555^{222}$ chia hết cho 7.

BÀI TẬP

15 Chứng minh rằng số $7^{100} + 11^{100}$ chia hết cho 13.

16 Chứng minh rằng số $6^{592} + 8$ chia hết cho 11.

17 Chứng minh rằng số $11^{10} - 1$ chia hết cho 100.

18 Chứng minh rằng $777^{777} - 7$ chia hết cho 10.

19 Hãy tìm chữ số tận cùng của số

$$7^{7^7} - 7^{7^7}$$

20 Chứng minh rằng số $14^{14^{14}} - 6$ chia hết cho 10.

21 Chứng minh rằng số $11^{10^{1967}} - 1$ chia hết cho 10^{1968}.

22 Chứng minh rằng số $222^{333} + 333^{222}$ chia hết cho 13.

23 Với mọi số nguyên không âm chứng minh rằng số

$$2^{5n+3} + 5^n.3^{n+1}$$

chia hết cho 17.

0.7 Phương pháp quy nạp

Phương pháp quy nạp có vai trò vô cùng quảan trọng trong toán học, khoa học và sống. Đối với nhiều bài toán chia hết, phương pháp quy nạp cũng cho ta cách giả hiệu.

Suy diễn là quảá trình từ "tính chất" của tập thể suy ra "tính chất" của cá thể luôn luôn đúng, còn quảá trình ngược lại, tức quảá trình quy nạp: đi từ "tính chất của một số cá thể suy ra "tính chất" của tập thể, thì không phi lúc nào cũng đúng quảá trình này chỉ dùng khi nó tho mãn một số điều kiện nào đó, tức tho mãn nguyên lý quy nạp.

0.7.1 Nguyên lý quy nạp

Nếu khẳng định $S(n)$ thoả mãn hai điều kiện sau

a) Đúng với $n = k_o$ (số tự nhiên nhỏ nhất mà $S(n)$ xác định).

b) Từ tính đúng đắn của $S(n)$ đối với $n = t$ (hoặc đối với mọi giá trị c $k_0 \leqslant n \leqslant t$) suy ra tính đúng đắn của $S(n)$ đối với $n = t + 1$, thì $S(n)$ với mọi $n \geqslant k_0$.

0.7.2 Phương pháp chứng minh bằng quy nạp

Giả sử khẳng định $T(n)$ xác định với mọi $n \geqslant t_0$. Để chứng minh $T(n)$ đúng vớ $n\,(n \geqslant t_0)$ bằng quy nạp, ta cần thực hiện hai bước.

a. Cơ sở quy nạp.

Thực hiện bước này tức là ta thử xem sự đúng đắn của $T(n)$ với $n = t_0$, ng xét $T(t_0)$ có đúng hay không?

b. Quy nạp.

Giả sử khẳng định $T(n)$ đã đúng đối với $n = t$ (hoặc đối với mọi n $(t_0 \leqslant n$ $(t \geqslant t_0)$. Trên cơ sở giả thiết này mà suy ra tính đúng đắn của $T(n)$ đối với $n =$ tức $T(t + 1)$ đúng. Nếu cả hai bước trên đều thoả mãn, thì theo nguyên lý quy $T(n)$ đúng với mọi $n \geqslant t_0$.

Chú ý. Trong quảá trình quy nạp nếu không thực hiện đầy đủ cả hai bước quy nạp và quy nạp, thì có thể dẫn đến kết luận sai lầm, chẳng hạn:

- Do bỏ bước cơ sở quy nạp, ta đưa ra kết luận không đúng: Mọi số tự nhiê bằng nhau! Bằng cách quy nạp như sau: giả sử các số tự nhiên không vượt quảá đã bằng nhau. Khi đó ta có $k = k + 1$.

Thêm vào mỗi vế của đẳng thức trên một đơn vị sẽ có

$$k + 1 = k + 1 + 1 = k + 2$$

Cứ như vậy suy ra mọi số tự nhiên không nhỏ hơn k đều bằng nhau. Kết hợp với giả thiết quy nạp: mọi số tự nhiên không vượt quáá k đều bằng nhau, đi đến kết luận sai lầm: Tất cả các số tự nhiên đều bằng nhau!

- Do bỏ qua khâu quy nạp, nên nhà Toán học Pháp P. Fermat (1601 - 1665) đã cho rằng các số dạng $2^{2^n}+1$ đều là số nguyên tố. P. Fermat xét 5 số đầu tiên

Với $n=0$ cho $2^{2^n}+1=2^1+1=3$ là số nguyên tố.

Với $n=1$ cho $2^{2^1}+1=2^2+1=5$ là số nguyên tố.

Với $n=2$ cho $2^{2^2}+1=2^4+1=17$ là số nguyên tố.

Với $n=3$ cho $2^{2^3}+1=2^8+1=257$ là số nguyên tố.

Với $n=4$ cho $2^{2^4}+1=2^{16}+1=65537$ là số nguyên tố.

Nhưng vào thế kỷ 18 Euler đã phát hiện với $n=5$ khẳng định trên không đúng bởi vì

$$2^{2^5}+1=4294967297=641\times 6700417$$

là hợp số.

0.7.3 Vận dụng phương pháp quy nạp để giải các bài toán chia hết

Phương pháp quy nạp được sử dụng trong tính toán, trong chứng minh và suy luận dưới nhiều dạng khác nhau, nhưng trong phần này chỉ trình bày việc vận dụng phương pháp quy nạp để giải các bài toán chia hết.

Ví dụ 11. Với n là số tự nhiên, đặt

$$A_n=7^{7^{\cdot^{\cdot^{7}}}}\Big\}n \text{ lần}$$

Chứng minh rằng với mọi số tự nhiên $n\geqslant 2$ số A_n+17 chia hết cho 20?

Giải.

Để có khẳng định phát biểu trong bài toán trước hết ta chứng minh: Với mọi số tự nhiên $n\geqslant 2$ đều có

$$A_n=20t_n+3 \tag{1}$$

Khẳng định (1) được chứng minh bằng quy nạp theo n.

1. Cơ sở quy nạp.

Với $n=2$ có $A_2=7^7=7^4.7^3$, mà

$$7^3=343=20.17+3=20.p+3 \tag{2}$$

$$7^4=2401=20.120+1=20.q+1, \tag{3}$$

Nên

$$\begin{aligned} A_2 &= (20.17+3)(20.120+1) \\ &= 20.20.17.120 + 20.17 + 20.120.3 + 3 \\ &= 20.41177 + 3 \end{aligned}$$

2. Quy nạp

Giả sử đẳng thức (1) đã đúng với $n = k \geqslant 2$, tức đã có

$$A_k = 20t_k + 3$$

Cần chứng minh đẳng thức (1) đúng với $n = k+1$.

Thật vậy, theo định nghĩa, và (2), (3), (4) có

$$\begin{aligned} A_{k+1} 7^{A_k} &= 7^{20t_k+3} = 7^{4.5t_k+3} = (7^4)^{5t_k}.7^3 = (20q+1)^{5t_k}(20p+3) \\ &= \{(20q)^{5t_k} + C^1_{5t_k}(20q)^{5t_k-1} + \cdots + C^{5t_k-1}_{5t_k}.20q + 1\}(20p+3) \\ &= 20p\{(20)^{5t_k} + C^1_{5t_k}(20q)^{5t_k-1} + \cdots + C^{5t_k-1}_{5t_k}.20q + 1\} + \\ &20q\{(20q)^{5t_k-1} + C^1_{5t_k}(20q)^{5t_k-2} + \cdots + C^{5t_k-1}_{5t_k}\}3 + 3 = 20t_{k+1} + 3 \end{aligned}$$

Từ (1) có:

$$A_n + 17 = 20t_n + 3 + 17 = 20t_n + 20 = 20(t_n + 1)$$

nên $A_n + 17$ chia hết cho 20.

Ví dụ 12. Chứng minh rằng với mọi số tự nhiên $n \geqslant 2$ số

$$2^{2^n} + 4$$

chia hết cho 10 (hay tận cùng bằng số 0)?

Giải. Chứng minh bằng quy nạp theo n.

1. Cơ sở quy nạp.

Với $n = 2$ có $2^{2^2} = 2^4 + 4 = 16 + 4 = 20$ chia hết cho 10.

2. Quy nạp.

Giả sử khẳng định đã đúng với $n = k \geqslant 2$, nghĩa là

$$2^{2^k} + 4 = 10t_k$$

Cần chứng minh khẳng định đúng với $n = k+1$.

Thật vậy, từ (1) có

$$\begin{aligned} 2^{2^{k+1}} + 4 &= (3^{2^k})^2 + 4 \\ &= (10t_k - 4)^2 + 4 \\ &= (10t_k)^2 - 8.10t_k + 16 + 4 \\ &= 10(10t_k^2 - 8t_k + 2) \end{aligned}$$

nên số $2^{2^{k+1}} + 4$ chia hết cho 10.

Ví dụ 12. Chứng minh rằng với mọi số tự nhiên n

$$A(n) = 4^n + 15n - 1$$

chia hết cho 9.

Giải. Chứng minh bằng quy nạp theo n.

1. Cơ sở quy nạp.

Với $n = 1$, $A(1) = 4^1 + 15.1 - 1 = 18$ chia hết cho 9.

2. Quy nạp.

Giả sử khẳng định đã đúng với số tự nhiên $n = k \geqslant 1$, nghĩa là,

$$A(k) = 4^k + 15k - 1$$

đã chia hết cho 9.

Cần chứng minh khẳng định cũng đúng với $n = k + 1$.

Thật vậy,

$$\begin{aligned} A(k+1) &= 4^{k+1} + 15(k+1) - 1 \\ &= 4.4^k + 15k + 14 \\ &4.4^k + 4.15k + 14 + 3.15k - 4 + 4 - 3.15k \\ &= 4.4^k + 4.15k - 4 + 3.15k + 18 \\ &= 4(4^k + 15k - 1) + 9(5k + 2) \end{aligned}$$

Theo giả thiết quy nạp $4^k + 15k - 1$ chia hết cho 9, nên $4(4^k + 15k - 1)$ chia hết cho 9 và $9(5k + 2)$ chia hết cho 9. Bởi vậy $A(k + 1)$ chia hết cho 9.

Ví dụ 13. Chứng minh rằng tổng lập phương của ba số tự nhiên liên tiếp bao giờ cũng chia hết cho 9.

Giải. Chứng minh bằng quy nạp theo thứ tự số tự nhiên.

1. Cơ sở quy nạp.

Với ba số tự nhiên đầu tiên $1, 2, 3$ ta có

$$1^3 + 2^3 + 3^3 = 1 + 8 + 27 = 36$$

chia hết cho 9.

2. Quy nạp.

Giả sử khẳng định đã đúng với ba số tự nhiên liên tiếp tùy ý nào đó k
1), $k+1$, $k+2$, nghĩa là số

$$A(k) = k^3 + (k+1)^3 + (k+2)^3$$

đã chia hết cho 9. Khi đó

$$(k+1)^3 + (k+2)^3 + (k+3)^3 = k^3 + (k+1)^3 + (k+2)^3 + (k+3)^3 - k$$

Do

$$\begin{aligned}(k+3)^3 - k^3 &= (k+3-k)\{(k+3)^2 + k(k+3) + k^2\} \\ &= 3\{k^2 + 6k + 9 + k^2 + 3k + k^2\} \\ &= 3\{3k^2 + 9k + 9\} \\ &= 9(k^2 + 3k + 3)\end{aligned}$$

chia hết cho 9, và theo giả thiết quy nạp $A(k) \vdots 9$, nên $(k+1)^3 + (k+2)^3 + (k$
chia hết cho 9. Khẳng định được chứng minh.

Ví dụ 14. Chứng minh rằng với mọi số nguyên $n \geqslant 0$ số $2^{3^n} + 1$ chia hế
3^{n+1} và không chia hết cho 3^{n+2}.

Giải. Khẳng định được chứng minh bằng quy nạp theo n.

1. Cơ sở quy nạp

Với $n = 0$ số $2^{3^0} + 1 = 2^1 + 1 = 2 + 1 = 3$ chia hết cho 3 $(3 = 3^{0+1})$ và k
chia hết cho 9 $(9 = 3^2 = 3^{0+2})$.

Với $n = 1$ số $2^{3^1} + 1 = 2^3 + 1 = 8 + 1 = 9$ chia hết cho 9.

2. Quy nạp

Giả sử khẳng định đã đúng với $n = k \geqslant 2$, nghĩa là

$$A_k = 2^{3^k} + 1$$

đã chia hết cho 3^{k+1} và không chia hết cho 3^{k+2}. Khi đó tồn tại số nguyên M, để

$$A_k = M.3^{k+1}$$

và do A_k không chia hết cho 3^{k+2}, nên M không chia hết cho 3.

Cần chứng minh $A_{k+1} = 2^{3^{k+1}} + 1$ chia hết cho 3^{k+2} và không chia hết cho 3^{k+3}.

Thật vậy, do

$$\begin{aligned} A_{k+1} &= 2^{3^{k+1}} + 1 = 2^{3^{k}.2} + 1 = (2^{3^k})^2 + 1 \\ &= (2^{3^k} + 1)\{(2^{3^k})^2 - 2^{3^k} + 1\} \\ &= 3^{k+1}.M\{(2^{3^k})^2 + 2.2^{3^k} + 1 - 3.2^{3^k}\} \\ &= 3^{k+1}.M.\{(2^{3^k} + 1)^2 - 3.2^{3^k}\} \\ &= 3^{k+1}.M.\{(2^{3^k}.M)^2 - 3.2^{3^k}\} \\ &= 3^{k+1}M\{3^{2k+2}M^2 - 3.2^{3^k}\} \\ &= 3^{k+2}.M.\{3^{2k+1}.M^2 - 2^{3^k}\} \end{aligned}$$

nên A_{k+1} chia hết cho 3^{k+2}.

Vì M không chia hết cho 3, nên $3^{k+2}.M$ không chia hết cho 3^{k+3}.

Do $k \geqslant 2$, nên $k - 2 \geqslant 0$, và có

$$3^{2k+1}.M = 3^{k+3+k-2}.M = 3^{k+3}.3^{k-2}.M$$

chia hết cho 3^{k+3}.

Mặt khác $2^{3^k} = (2^3)^k = 8^k \equiv \pm 1 \pmod 9$ và $3^{k+3} = 9.3^{k+1}$, nên 2^{3^k} không chia hết cho 3^{k+3}.

Do $3^{2k+1}.M^2 - 2^{3^k}$ không chia hết cho 3^{k+3}. Bởi vậy A_{k+1} không chia hết cho 3^{k+2}. Khẳng định được chứng minh.

BÀI TẬP

23 Chứng minh rằng với mọi số nguyên $n \geqslant 0$
   a) $(2^{5n+3} + 5^n.3^{n+2})$ chia hết cho 17
   b) $(2^{n+5}.3^{4n} + 5^{3n+1})$ chia hết cho 37
   c) $(5^{2n+1} + 2^{n+4} + 2^{n+1})$ chia hết cho 23
   d) $(7^{n+2} + 8^{2n+1})$ chia hết cho 57

24 Chứng minh rằng với mọi số tự nhiên n tổng

$$2^0 + 2^1 + 2^2 + \cdots + 2^{5n-3} + 2^{5n-2} + 2^{5n-1}$$

chia hết cho 31?

25 Giả sử a là số tự nhiên nào đó, mà $2^a - 2$ chia hết cho a, chẳng hạn $a = 2^3 - 2 = 8 - 2 = 6$ chia hết cho 3. Xác định dãy số (x_n) nhờ các điều kiệ

$$x_1 = a, \quad x_{k+1} = 2^{x_k} - 1$$

Chứng minh rằng với mọi só tự nhiên k số $2^{x_k} - 2$ chia hết cho x_k?

0.8 Tiêu chuẩn chia hết

Đối với số nguyên tuỳ ý a và số tự nhiên bất kỳ m để trả lời câu hỏi: a có ch cho m không? Trong rất nhiều trường hợp có thể dựa vào tiêu chuẩn chia hết. Bở việc tìm ra các tiêu chuẩn chia hết dễ vận dụng là hết sức cần thiết. Căn cứ vào chất của dãy số dư nhận được khi chia lũy thừa cơ số 10 cho m, mà có thế xác các tiêu chuẩn chia hết tiện ích khác nhau. Trong phần này trình bày một số các định tiêu chuẩn chia hết, như

Phương pháp sử dụng tính đồng dư với 1 của lũy thừa cơ số 10, mà gọi "phương pháp đồng dư với 1".

Phương pháp dựa vào dãy số dư của lũy thừa cơ số 10, mà gọi tắt là "ph pháp dãy số dư".

Phương pháp chia các chữ số thành các nhóm, mà gọi tắt là "phương pháp chữ số".

0.8.1 Phương pháp đồng dư với 1

Với số tự nhiên tuỳ ý $m \geqslant 2$ cần tìm tiêu chuẩn, để số nguyên bất kỳ

$$\begin{aligned} a &= \overline{a_n a_{n-1} \ldots a_i a_{i-1} \ldots a_1 a_0} \\ &= a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_i 10^i + a_{i-1} 10^{i-1} + \cdots + a_i 10 + a_0 \end{aligned}$$

chia hết cho m.

Nếu tồn tại số tự nhiên k, để $10^k \equiv 1 \pmod{m}$ thì với mọi số tự nhiên t đ $10^{kt} \equiv 1 \pmod{m}$. Ta thực hiện thuật toán sau

Thuật toán.

1. Tìm số tự nhiên l nhỏ nhất, để $10^l \equiv 1 \pmod{m}$.

2. Chia dãy chữ số của a từ phi sang trái theo các nhóm liên tiếp độ dài l. K với số tự nhiên s, mà $sl < n \leqslant (s+1)l$ có

$$\begin{aligned} a &= \overline{a_n a_{sl+1} a_{sl}} 10^{sl} + \cdots + \overline{a_{2l-1} \ldots a_{l+1} a_l} 10^l + \overline{a_{l-1} \ldots a_1 a_0} \\ &\equiv \overline{a_n a_{sl+1} a_{sl}} + \cdots + \overline{a_{2l-1} \ldots a_{l+1} a_l} + \overline{a_{l-1} \ldots a_1 a_0} \pmod{m} \end{aligned}$$

Bởi vậy ta có tiêu chuẩn chia hết sau đây.

Tiêu chuẩn chia hết 1

Nếu l là số tự nhiên nhỏ nhất để $a^l \equiv 1 \pmod{m}$ và s là số tự nhiên để $sl < n \leqslant (s+1)l$, thì a chia hết cho m khi và chỉ khi tổng

$$\overline{a_n a_{sl+1} a_{sl}} + \cdots + \overline{a_{2l-1} \ldots a_{l+1} a_l} + \overline{a_{l-1} \ldots a_1 a_0}$$

chia hết cho m.

Vận dụng tiêu chuẩn chia hết 1 cho các trường hợp $m = 3, 9, 11, 111$ ta được các tiêu chuẩn chia hết tương ứng sau đây.

1. Với $m = 3$, ta có $10 \equiv 1 \pmod{3}$, nên $l = 1$ và dãy chữ số a được chia thành các nhóm gồm một chữ số và ta có tiêu chuẩn chia hết cho 3 như sau

Số nguyên $a = \overline{a_n a_{n-1} a_1 a_0}$ chia hết cho 3 khi và chỉ khi tổng các chữ số $a_n + a_{n-1} + \cdots + a_1 + a_0$ chia hết cho 3.

Tương tự ta cũng có tiêu chuẩn chia hết cho 9 như sau:

Số nguyên $a = \overline{a_n a_{n-1} \ldots a_1 a_0}$ chia hết cho 9 khi và chỉ khi tổng

$$a_n + a_{n-1} + \cdots +_a 1 + a_0$$

chia hết cho 9.

Ví dụ.

$23456781 \equiv 2+3+4+5+6+7+8+1 \equiv 0 \pmod{3}$ nên $23456781 \vdots 3$.

$54326781 \equiv 5+4+3+2+6+7+8+1 \equiv 0 \pmod{9}$, nên $54326781 \vdots 9$

$4354063 = 4+3+5+4+0+6+3 = 25 \equiv 1 \pmod{3}$

nên 4354063 không chia hết cho 3.

$1997199819991 = 1+9+9+7+1+9+9+8+1+9+9+9+1 = 82 \equiv 1 \pmod{m}$

nên 1997199819991 không chia hết cho 9.

2. Với $m = 11$ ta có $10^2 \equiv 1 \pmod{1}1$, nên $l = 2$ và dãy chữ số của a được phân thành các nhóm độ dài 2 từ phải sang trái và ta có tiêu chuẩn chia hết cho 11 như sau

Với n lẻ số nguyên $a = \overline{a_n a_{n-1} \ldots a_1 a_0}$ chia hết cho 11 khi và chỉ khi tổng

$$\overline{a_n a_{n-1}} + \overline{a_{n-2} a_{n-3}} + \cdots + \overline{a_1 a_0}$$

chia hết cho 11.

Với n chẵn số nguyên $a = \overline{a_n a_{n-1} ... a_1 a_0}$ chia hết cho 11 khi và chỉ khi tổn

$$a_n + \overline{a_{n-1} a_{n-2}} + \cdots + \overline{a_1 a_0}$$

chia hết cho 11.

Ví dụ.

$$719981999 \equiv 7 + 19 + 98 + 19 + 99 = 242 \equiv 0 \pmod{1)1}$$

nên 719981999 chia hết cho 11.

$$53467874 \equiv 53 + 46 + 78 + 74 = 251 \equiv 8 \pmod{1)1}$$

nên 53467874 không chia hết cho 11.

3. Với $m = 111$ ta có $10^3 \equiv 1 \pmod{1)11}$, nên $l = 3$ và dãy chữ số của a phân thành các nhóm độ dài 3 từ phi sang trái và ta có tiêu chuẩn chia hết cho 11 nh

- Với $n = 3t$ (t là số tự nhiên) số nguyên $a = \overline{a_n a_{n-1} ... a_1 a_0}$ chia hết cho 1 và chỉ khi tổng

$$\overline{a_n a_{n-1} a_{n-2}} + \overline{a_{n-3} a_{n-4} a_{n-5}} + \cdots + \overline{a_2 a_1 a_0}$$

chia hết cho 111.

- Với $n = 3t + 1$ số nguyên $a = \overline{a_n a_{n-1} ... a_1 a_0}$ chia hết cho 111 khi và ch tổng

$$a_n + \overline{a_{n-1} a_{n-2} a_{n-3}} + \cdots + \overline{a_2 a_1 a_0}$$

chia hết cho 111.

- Với $n = 3t + 2$ số nguyên $a = \overline{a_n a_{n-1} ... a_1 a_0}$ chia hết cho 111 khi và ch tổng

$$\overline{a_n a_{n-1}} + \overline{a_{n-2} a_{n-3} a_{n-4}} + \cdots + \overline{a_2 a_1 a_0}$$

chia hết cho 111.

Ví dụ.

$$582004080 = 582 + 004 + 080 = 582 + 4 + 80 = 666 \equiv 0 \pmod{111}$$

nên 582004080 chia hết cho 111.

$$6573864 = 6 + 573 + 864 = 1443 \equiv 0 \pmod{111}$$

nên 6573864 chia hết cho 111.

$$13661325 \equiv 13 + 661 + 325 = 999 \equiv 0 \pmod{111}$$

nên 13661325 chia hết cho 111.

$$154635811 \equiv 154 + 63 = 1600 \equiv 35 \pmod{111}$$

nên 15463811 chia hết cho 111.

0.8.2 Phương pháp dãy số dư

Giả sử

$$a = \overline{a_n a_{n-1}...a_i.a_1 a_0} = a_n 10^n + a_{n-1}10^{n-1} + \cdots + a_i 10_i + \cdots a_1 10 + a_0$$

là số nguyên tùy ý và m là số tự nhiên bất kỳ không nhỏ hơn 2. Khi đó, theo các tính chất của phép đồng dư, ta có hệ quả: Nếu $d_i\ (i = 0, 1, 2)$ là số nguyên tùy ý đồng dư với 10^i theo modun m, thì

$$a \equiv a_n d_n + a_{n-1}d_{n-1} + \cdots + a_i d_i + \cdots + a_1 d_1 + a_0 \pmod{m}$$

Từ hệ quả trên suy ra thuật toán xây dựng tiêu chuẩn chia hết cho m.

Thuật toán.

Để có một tiêu chuẩn chia hết cho m ta thực hiện các bước sau

1. Đối với mỗi $i = 1, 2$ chọn số nguyên d_i đồng dư với 10^i theo modun m và có trị tuyệt đối ($|d_i|$) nhỏ nhất;
2. Viết dãy số đồng dư $d_i\ (i = 1, 2.)$ một cách tương ứng dưới dãy chữ số của a;

$$\begin{array}{cccccccc} a_n & a_{n-1} & ...a_{i+1} & a_i & ... & a_1 & a_0 \\ d_n & d_{n-1} & ... & d_{i+1} & d_i & ... & d_i 1 \end{array}$$

3. Tìm tổng

$$d = a_n d_n + a_{n-1}d_{n-1} + a_{i+1}d_{i+1} + a_i d_i + \cdots + a_1 d_1 + a_0$$

4. Xét tổng d

   - Nếu $d \equiv 0 \pmod{m}$, thì a chia hết cho m

   - Nếu $d \equiv 0 \pmod{m}$, thì a không chia hết cho m.

   Khi đó tiêu chuẩn chia hết cho m được phát biểu như sau: Số a chia hết m khi và chỉ khi d chia hết cho m.

Dựa vào thuật toán trên ta có thể xây dựng tiêu chuẩn chia hết cho bất kỳ số tự nhiên $m \geqslant 2$, chẳng hạn, $m = 4, 7, 11, 13$.

1. Tiêu chuẩn chia hết cho 4

Xét tính đồng dư của lũy thừa cơ số 10 theo modun 4 ta có

$10 \equiv 2 \pmod{4}$, $10^2 \equiv 20 \equiv 0 \pmod{4}$, $10^i \equiv 0 \pmod{4}$ $(i = 3, 4...)$

Tổng d tưng ứng với số $a = \overline{a_n a_{n-1}...a_{i+1}a_i...a_2 a_1 a_0}$ có dạng

$$d = a_n 0 + a_{n-1}0 + \cdots + a_{i+1}0 + a_i 0 + \cdots + a_2 0 + a_1 2 + a_0 = 2a_1 + a_0$$

Vậy tiêu chuẩn chia hết cho 4 là: Số a chia hết cho 4 khi và chỉ khi $d = 2a_1 + a_0$ chia hết cho 4.

Ví dụ.

453452 có $d = 2 \times 5 + 2 = 12$ chia hết cho 4, nên $453452 \vdots 4$,

582422 có $d = 2 \times 2 + 2 = 6$ không chia hết cho 4, nên 582422 không chia hết

2. Tiêu chuẩn chia hết cho 7

Xét tính đồng dư của lũy thừa cơ số 10 theo modun 7 ta có

$10 \equiv 3 \pmod 7$, $10^2 \equiv 30 \equiv 2 \pmod 7$, $10^3 \equiv 20 \equiv -1 \pmod 7$

$10^4 \equiv -10 \equiv -3 \pmod 7$, $10^5 \equiv -30 \equiv -2 \pmod 7$, $10^6 \equiv -20 \equiv 1$ (

Giả sử $n = 6t + 1$ với $t \geqslant 2$. Khi đó dãy số đồng dư tương ứng với dãy c của a sẽ là

$$\begin{array}{l} a_n\ a_{n-1}\ a_{n-2}\ a_{n-3} \ldots a_6\ a_5\ a_4\ a_3\ a_2\ a_1\ a_0 \\ 1\ -2\ -3\ -1 \ldots 1\ -2\ -3\ -1\ 2\ 3\ 1 \end{array}$$

Và tổng d tương ứng với a có dạng

$$d = a_n - 2a_{n-1} - 3a_{n-2} - a_{n-3} + \cdots + a_6 - 2a_5 - 3a_4 - a_3 + 2a_2 + 3a_1 +$$

Vậy tiêu chuẩn chia hết cho 7 là: Số $a \vdots 7$ khi và chỉ khi tổng

$$d = a_n - 2a_{n-1} - 3a_{n-2} - a_{n-3} + \cdots + a_6 - 2a_5 - 3a_4 - a_3 + 2a_2 + 3a_1 +$$

chia hết cho 7,

7546357 có $d = 7 - 2 \times 5 - 3 \times 4 - 6 + 2 \times 3 + 3 \times 5 + 7 = 7$ chia hết c nên $7546357 \vdots 7$.

863425 có

$$d = -2 \times 8 - 3 \times 6 - 3 + 2 \times 4 + 2 \times 3 + 5 = -16 - 18 - 3 + 8 + 6 + 5 =$$

không chia hết cho 7, nên 863425 không chia hết cho 7.

3. Tiêu chuẩn chia hết cho 11

Xét tính đồng dư của lũy thừa cơ số 10 theo mod 11, ta có

$10 \equiv -1 \pmod{11}$, $10^2 \equiv -10 \equiv 1 \pmod{11}$,

$10^{2k+1} \equiv -1 \pmod{11}$, $10^{2k} \equiv 1$ (mod

Với $k = 0, 1, 2, ...$ khi đó dãy đồng dư tương ứng với dãy chữ số của a sẽ là

$$\begin{array}{l} a_n,\ a_{n-1},\ a_{n-2},\ \ a_2\ a_1\ a_0 \\ (-1)^n(-1)^{n-1}(-1)^{n-2}...1\ -1\ 1 \end{array}$$

Và tổng d tương ứng với a có dạng

$$d(-1)^n a_n + (-1)^{n-1}a_{n-1} + (-1)^{n-2}a_{n-2} + \cdots + a_2 - a_1 + a_0$$

Vậy tiêu chuẩn chia hết cho 11 là: Số $a \vdots 11$ khi và chỉ khi

$$d = (-1)^n a_n + (-1)^{n-1}a_{n-1} + (-1)^{n-2}a_{n-2} + \cdots + a_2 - a_1 + a_0$$

chia hết cho 11.

Ví dụ.
3811581939 có $d = -3 + 8 - 1 - 5 + 8 - 1 + 9 - 3 + 9 = 22$ chia hết cho 11, nên $3811581939 \vdots 11$

256743258 có $d = 2 - 5 + 6 - 7 + 4 - 3 + 2 - 5 + 8 = 2$ không chia hết cho 11, nên 256743258 không chia hết cho 11.

4. Tiêu chuẩn chia hết cho 13

Xét tính đồng dư của lũy thừa cơ số 10 theo modun 13 ta có
$10 \equiv -3 \pmod{13}$, $10^2 \equiv -4 \pmod{13}$, $10^3 \equiv -40 \equiv -1 \pmod{13}$, $10^4 \equiv -10 \equiv 3 \pmod{13}$, $10^5 \equiv 30 \equiv 4 \pmod{13}$, $10^6 \equiv 40 \equiv 1 \pmod{13}$, $10^7 \equiv 10 \equiv -3 \pmod{13}$

Giả sử $n = 6t$ với $t \geqslant 2$. Khi đó dãy số đồng dư tương ứng với dãy chữ số của a là

a_n	a_{n-1}	a_{n-2}	a_{n-3}	a_{n-4}	a_{n-5}	...	a_6	a_5	a_4	a_3	a_2	a_1	a_0
1	4	3	-1	-4	-3	1	4	3	-1	-4	-3	1	

và tổng d tương ứng với a có dạng

$$d = a_n + 4a_{n-1} + 3a_{n-2} - a_{n-3} - 4a_{n-4} - 3a_{n-5} + \cdots + a_6 + 4a_5 + 3a_4 - a_3 - 4a_2 - 3a_1 + a_0$$

Vậy tiêu chuẩn chia hết cho 13 là: Số a chia hết cho 13 khi và chỉ khi tổng

$$d = a_n + 4a_{n-1} + 3a_{n-2} - a_{n-3} - 4a_{n-4} - 3a_{n-5} + \cdots + a_6 + 4a_5 + 3a_4 - a_3 - 4a_2 - 3a_1 + a_0$$

chia hết cho 13.

Ví dụ.

8588112 có $d = 8 + 20 + 24 - 8 - 4 - 3 + 2 = 39$ chia hết cho 13, nên 85 chia hết cho 13.

1111111 có $d = 1 + 4 + 3 - 1 - 4 - 3 + 1 = 1$ không chia hết cho 13, nên 11 không chia hết cho 13.

0.8.3 Phương pháp nhóm chữ số

Giả sử $a = \overline{a_n a_{n-1} ... a_i ... a_1 a_0}$ là số nguyên tùy ý, còn m là số tự nhiên bất kỳ nhỏ hơn 2. Với số tự nhiên l tuỳ ý không nhỏ hơn 2. Giả sử d_i là số nguyên đồ với 10^{il} $(i = 0, 1, 2,)$ theo modun m và có trị tuyệt đối nhỏ nhất. Khi đó nhờ cá chất của phép đồng dư ta có hệ quả sau:
Số

$$\begin{aligned} a &= \overline{a_n a_{n-1} ... a_{tl} a_{tl-1} a_{tl-2} ... a_{(t-1)l} ... a_l a_{l-1} ... a_1 a_0} \\ &= \overline{a_n a_{n-1} ... a_{tl} d_t}.10^{tl} + \overline{a_{tl-1} a_{tl-2} ... a_{(t-1)l}} 10^{(t-1)l} + \\ &\quad \cdots + \overline{a_{2l-1} a_{2l-2} ... a_l} 10^l + \overline{a_{l-1} a_{l-2} ... a_1 a_0} \\ &\equiv \overline{a_n a_{n-1} ... a_{tl}} d_t + \overline{a_{tl-1} a_{tl-2} ... a_{(t-1)l}} d_{t-l} + \cdots \\ &\quad + \overline{a_{2l-1} a_{2l-2} ... a_l} d_1 + \overline{a_{l-1} a_{l-2} ... a_l a_0} \pmod m \end{aligned}$$

Dựa vào hệ quả trên có thuật toán xây dựng tiêu chuẩn chia hết cho m như sau

Thuật toán.

1. Chọn số tự nhiên bé nhất có thể $l \geqslant 2$ thích hợp với m theo nghĩa: Số d_i dư với 10^{il} theo modun m có trị tuyệt đối bé nhất.

2. Liệt kê dãy các số đồng dư tương ứng với dãy 10^{il} $(i = 1, 2,)$

10^{tl}	$10^{(t-1)l}$	...	10^{il}	...	10^{2l}	10^l	10^0
d_0	d_{t-1}	...	d_i	...	d_2	d_1	1

3. Lập tổng

$$\begin{aligned} d = \overline{a_n a_{n-1} ... a_{tl}} d_t + \overline{a_{tl-1} a_{tl-2} ... a_{(t-1)l}} d_{t-1} + \cdots \\ + \overline{a_{2l-1} a_{2l-2} ... a_{l+1} a_1} d_1 + \overline{a_{l-1} a_{l-2} ... a_1} \end{aligned}$$

4. Nếu d chia hết cho m, thì a chia hết cho m. Nếu d không chia hết cho r a không chia hết cho m. Bằng thuật toán trên ta có tiêu chuẩn chia hết c bằng phương pháp nhóm chữ số như sau: Số a chia hết cho m khi và ch tổng

$$\begin{aligned} d = \overline{a_n a_{n-1} ... a_{tl}} d_t + \overline{a_{tl-1} a_{tl-2} ... a_{(t-1)l}} d_{t-1} + \cdots \\ + \overline{a_{2l-1} a_{2l-2} ... a_{l+1} a_1} d_1 + \overline{a_{l-1} a_{l-2} ... a_1} \end{aligned}$$

chia hết cho m.

Dựa vào thuật toán trên ta có thể xây dựng tiêu chuẩn chia hết cho bất kỳ số tự nhiên m nào không nhỏ hơn 2, chẳng hạn $m = 7, 33$.

Tiêu chuẩn chia hết cho 7

Để có tiêu chuẩn chia hết cho 7 ta thực hiện các bước của thuật toán trên như sau

1. Do $1000 \equiv -1 \pmod 7$, $1000^2 \equiv 1 \pmod 7$, $1000^{2i} \equiv 1 \pmod 7$, $1000^{2i+l} \equiv -1 \pmod 7$ $i = 0, 1, 2$, nên chọn $l = 3$.

2. Dãy số đồng dư tưng ứng với 1000^k, $k = 0, 1, 2$,

$$\begin{array}{cccccc} 1000^t & 1000^{t-1} & ... & 1000^2 & 1000 & 1 \\ (-1)^t & (-1)^{t-1} & ... & 1 & -1 & 1 \end{array}$$

3. Tổng d tương ứng với số a có dạng

$$d = (-1)^t\overline{a_n a_{n-1} a_{3t}} + (-1)^{t-1}\overline{a_{3t-1} a_{3t-2} a_{3(t-1)}} + \cdots - \overline{a_5 a_4 a_3} + \overline{a_2 a_1 a_0}$$

Khi đó tiêu chuẩn chia hết cho 7 được phát biểu như sau: Số a chia hết cho 7 khi và chỉ khi tổng d chia hết cho 7.

Ví dụ.

5781139 có $d = 5 - 781 + 139 = 637$ chia hết cho 7, nên 5781139 chia hết cho 7
811582 có $d = -811 + 582 = 229$ không chia hết cho 7, nên 811582 không chia hết cho 7.

Tiêu chuẩn chia hết cho 33

Để có tiêu chuẩn chia hết cho 33 ta thực hiện các bước của thuật toán trên như sau

1. Do $100 \equiv 1 \pmod{33}$, nên với mọi $s = 0, 1, 2...$ đều có $100^s \equiv 1 \pmod{33}$ nên chọn $l = 2$.

2. Dãy số đồng dư tương ứng với 100^k, $k = 0, 1, 2$

$$\begin{array}{cccccc} 100^t & 100^{t-1} & ... & 100^2 & 100 & 1 \\ 1 & 1 & ... & 1 & 1 & 1 \end{array}$$

3. Tổng d tương ứng với số a có dạng

$$d = \overline{a_n a_{n-1}} + \overline{a_{n-2} a_{n-3}} + \cdots + \overline{a_3 a_2} + \overline{a_1 a_0}, \text{ nếu } n \text{ lẻ}$$
$$d = a_n + \overline{a_{n-1} a_{n-2}} + \cdots + \overline{a_3 a_2} + \overline{a_1 a_0}, \text{ nếu } n \text{ chẵn.}$$

Khi đó tiêu chuẩn chia hết cho 33 được phát biểu như sau: Số a chia hết cho 3
và chỉ khi d chia hết cho 33.

Ví dụ.

6021939 có $d = 6 + 02 + 19 + 39 = 66$ chia hết cho 33, nên 6021939 ch
cho 33.
524631 có $d = 52 + 46 + 31 = 129$ không chia hết cho 33, nên 524531 khôn
hết cho 33.