Nơi huyền thoại lưu danh

Lê Quốc Dũng

2023

Đường đi ngàn dặm, bắt đầu bằng một bước chân.

Lão Tử

Mục lục

Bảng các ký hiệu dùng trong sách

$\#S$ số lượng phần tử của tập hợp S (lực lượng của S)

1 Đại số tuyến tính

1.1 Nhắc lại các khái niệm cơ bản

Hạng của ma trận

Cho ma trận $\mathbf{M}_{m\times n}$ có m hàng và n cột. **Hạng** của ma trận $\mathbf{M}$ là cấp của ma trận vuông con lớn nhất của $\mathbf{M}$ có định thức khác 0.
Ký hiệu. Hạng (hay rank) của ma trận $\mathbf{M}$ ký hiệu là $r = \text{rank}(\mathbf{M})$
Nhận xét. Nếu r là hạng của ma trận $\mathbf{M}_{m\times n}$ thì $r \leq \min(m, n)$

2 Số học

2.1 Hàm Euler

ϕ hàm Euler

Cho số nguyên dương n. Số lượng các số dương nhỏ hơn n và nguyên tố cùng nhau với n được ký hiệu bởi $\phi(n)$ và gọi là ϕ hàm Euler.
Nghĩa là, $\phi(n) = \#\{a|(a,n) = 1\}$

Hàm Euler có ý nghĩa quan trọng trong lý thuyết số, công cụ giúp chúng ta giải các vấn đề về số mũ trong modulo.

Sau đây chúng ta xem xét hệ thặng dư đầy đủ và hệ thặng dư thu gọn.

Với số nguyên dương n, ta định nghĩa:

Hệ thặng dư đầy đủ

Định nghĩa 2.1. Hệ thặng dư đầy đủ của n là tập $\{0, 1, \ldots, n-1\}$.

Nói cách khác, hệ thặng dư đầy đủ của n là các số dư có thể có khi chia một số bất kì cho n.

Hệ thặng dư thu gọn

Định nghĩa 2.2. Hệ thặng dư thu gọn của n là tập các số a mà $1 \leq a < n$ và $(a, n) = 1$. Số lượng các số a như vậy là $\phi(n)$.

Nhận xét. Hệ thặng dư thu gọn của n gồm $\phi(n)$ phần tử là

$$\{a_1, a_2, \ldots, a_{\phi(n)}\}$$

Nhận xét. Nếu n là số nguyên tố thì $\phi(n) = p - 1$

2.2 Định lý Euler

Định lý Euler

Cho số nguyên dương n. Với mọi số nguyên a mà $(a, n) = 1$ thì

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

Chứng minh. Giả sử $S = \{a_1, a_2, \ldots, a_{\phi(n)}\}$ là hệ thặng dư thu gọn của n. Ta sẽ chứng minh rằng nếu a là số sao cho $(a, n) = 1$ thì tập hợp

$$\{aa_1, aa_2, \ldots, aa_{\phi(n)}\}$$

là hoán vị của tập S.

Thật vậy, giả sử $aa_i \equiv aa_j \pmod{n}$ với $1 \leq i, j \leq \phi(n)$ và $i \neq j$.

Do $(a, n) = 1$ nên tồn tại nghịch đảo $a' \pmod{n}$, nhân a' cho 2 vế ta còn $a_i \equiv a_j \pmod{n}$.

Nói cách khác, nếu $a_i \not\equiv a_j \pmod{n}$ thì $aa_i \not\equiv aa_j \pmod{n}$. Suy ra tập

$$\{aa_1, aa_2, \ldots, aa_{\phi(n)}\}$$

là hoán vị của S.

Ta nhân tất cả phần tử của S thì sẽ bằng tích phần tử của tập trên

$$aa_1 \cdot aa_2 \ldots aa_{\phi(n)} \equiv a_1 \cdot a_2 \ldots a_{\phi(n)} \pmod{n}$$

Đặt $I = a_1 \cdot a_2 \ldots a_{\phi(n)}$ thì phương trình trên tương đương với

$$a^{\phi(n)} I \equiv I \pmod{n}$$

Mà $(I, n) = 1$ do là tích các số nguyên tố cùng nhau với n nên rút gọn 2 vế ta được

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

Ta có điều phải chứng minh. □

2.3 Định lý Fermat nhỏ

Định lý Fermat nhỏ

Cho số nguyên tố p. Với mọi số nguyên a thì

$$a^p \equiv a \pmod{p}$$

Khi $(a, p) = 1$ thì

$$a^{p-1} \equiv 1 \pmod{p}$$

Nhận xét. Khi $(a, p) = 1$ thì định lý Fermat là hệ quả trực tiếp từ định lý Euler.

2.4 Tính chất hàm Euler

Nhận xét. Với $(m, n) = 1$ thì

$$\phi(mn) = \phi(m)\phi(n)$$

Chứng minh. Ta viết các số từ 1 tới mn thành bảng như sau

$$\begin{array}{cccc} 1 & m+1 & \cdots & (n-1)m+1 \\ 2 & m+2 & \cdots & (n-1)m+2 \\ \cdots & \cdots & \cdots & \cdots \\ m & m+m & \cdots & (n-1)m+m \end{array}$$

Hàng r gồm các phần tử dạng $rm + k$ với $0 \leq r \leq n-1$ và $1 \leq k \leq m$. Ta thấy rằng nếu $(rm + k, m) = 1$ thì $(k, m) = 1$.

Do đó trên mỗi hàng có $\phi(m)$ phần tử nguyên tố cùng nhau với m.

Tiếp theo, trên các hàng vừa tìm được, do $(m, n) = 1$ nên để $(rm + k, n) = 1$ thì $(r, n) = 1$. Nghĩa là có $\phi(n)$ hàng như vậy.

Tổng kết lại, ta có $\phi(m)\phi(n)$ phần tử trong bảng nguyên tố cùng nhau với mn. Do đó có điều phải chứng minh. □

3 Lý thuyết nhóm

Câu chuyện bắt đầu vào một ngày khi mình vẫn còn sống ngày tháng tươi đẹp.

Cho tới khi học **lý thuyết nhóm** thì đời bớt đẹp hơn tí.

Để bắt đầu mình cần hiểu nhóm là gì.

Nhóm (Group)

Một tập hợp G và toán tử 2 ngôi $\star$ trên G tạo thành một nhóm nếu:

1. Tồn tại phần tử $e \in G$ sao cho với mọi $g \in G$ thì $g \star e = e \star g = g$. Khi đó e được gọi là **phần tử đơn vị** của G.
2. Với mọi $g \in G$, tồn tại $g' \in G$ sao cho $g \star g' = g' \star g = e$. Khi đó g' được gọi là **phần tử nghịch đảo** của g.
3. Tính kết hợp: với mọi $a, b, c \in G$ thì $a \star (b \star c) = (a \star b) \star c$.

Nhóm Abel

Nếu nhóm G có thêm tính giao hoán, tức là với mọi $a, b \in G$ thì $a \star b = b \star a$ thì G gọi là nhóm giao hoán hay nhóm Abel

Lý thuyết nhóm thuộc toán trừu tượng, và nó trừu tượng thật. Tuy nhiên khi học về nó mình dần hiểu hơn về cách toán học vận hành và phát triển.

4 Ba đường Conic

Ba đường Conic bao gồm ellipse, hyperbol và parabol.

4.1 Ellipse

Ellipse

Đường ellipse là tập hợp các điểm sao cho tổng khoảng cách từ nó tới 2 điểm cố định là 1 hằng số.

Nghĩa là, với 2 điểm cố định F_1, F_2, tập hợp các điểm M sao cho $MF_1 + MF_2 = 2a$ với a là hằng số tạo thành đường ellipse.

Ở trên hệ tọa độ, nếu ta chọn F_1 và F_2 nằm trên Ox và đối xứng qua Oy, tức là $F_1 = (-c, 0)$ và $F_2 = (c, 0)$, thì các điểm $M = (x, y)$ nằm trên ellipse thỏa

$$MF_1 + MF_2 = \sqrt{(x+c)^2 + y^2} + \sqrt{(x-c)^2 + y^2} = 2a$$

Tương ứng với biển đổi thành phương trình

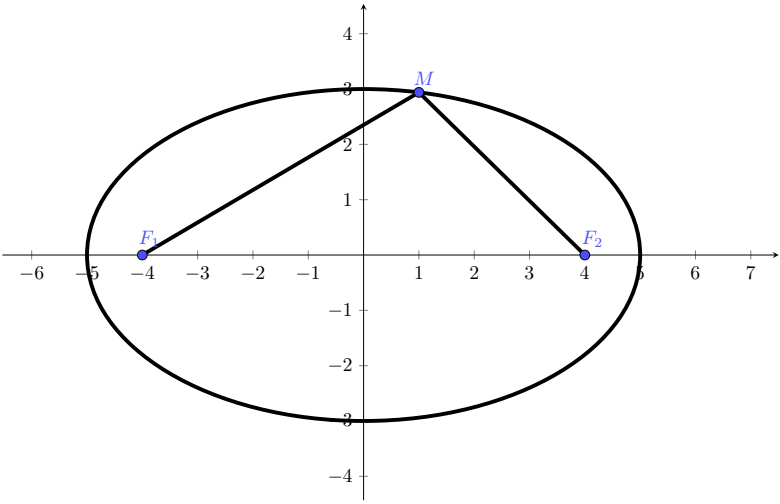
$$\frac{x^2}{a^2} + \frac{y^2}{a^2 - c^2} = 1$$

Đặt $b^2 = a^2 - c^2$ thì phương trình của ellipse trở thành

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$$

Phương trình này gọi là **phương trình chính tắc**.
Trong phương trình

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$$



Hình 1: Ellipse với phương trình $\frac{x^2}{25} + \frac{y^2}{9} = 1$

thì a là khoảng cách từ tâm tới 2 biên trái hoặc phải, nên a là **độ dài bán trục lớn**.

Tương tự, b là **độ dài bán trục nhỏ** (khoảng cách từ tâm tới 2 biên trên dưới).

Từ cách đặt $b^2 = a^2 - c^2$ tương đương $c^2 = a^2 - b^2$ thì c gọi là **tiêu cự** của ellipse.

Các điểm F_1, F_2 gọi là **tiêu điểm** của ellipse.

Với ví dụ trên $\frac{x^2}{25} + \frac{y^2}{9} = 1$ thì $a = 5, b = 3$. Suy ra $c = 4$ (lưu ý là $a, b > 0$ và $c \geq 0$).

Các đỉnh nằm ở các tọa độ $(-a, 0), (a, 0), (0, b), (0, -b)$. Các tiêu điểm nằm ở $(-c, 0), (c, 0)$.

Nhận xét. Khi $c = 0$, tức là 2 tiêu điểm trùng nhau, ta có đường tròn.

Tâm sai của ellipse là $e = \frac{c}{a} < 1$

4.2 Hyperbol

Hyperbol

Đường hyperbol là tập hợp các điểm sao cho giá trị tuyết đối hiệu số khoảng cách từ nó tới 2 điểm cố định là 1 hằng số.

Nghĩa là, với 2 điểm cố định F_1, F_2, tập hợp các điểm M sao cho $|MF_1 - MF_2| = 2a$ với a là hằng số tạo thành đường hyperbol.

Ở trên hệ tọa độ, nếu ta chọn F_1 và F_2 nằm trên Ox và đối xứng qua Oy, tức là $F_1 = (-c, 0)$ và $F_2 = (c, 0)$, thì các điểm $M = (x, y)$ nằm trên hyperbol thỏa

$$|MF_1 - MF_2| = |\sqrt{(x+c)^2 + y^2} - \sqrt{(x-c)^2 + y^2}| = 2a$$

Tương ứng với biển đổi thành phương trình

$$\frac{x^2}{a^2} - \frac{y^2}{a^2 - c^2} = 1$$

Đặt $b^2 = a^2 - c^2$ thì phương trình của hyperbol trở thành

$$\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1$$

Đường hyperbol cắt trục Ox tại 2 điểm $A_1 = (-a, 0)$ và $A_2 = (a, 0)$.

Tiêu điểm của hyperbol ở $F_1 = (-c, 0)$ và $F_2 = (c, 0)$.

Đường hyperbol có 2 tiệm cận là đường thẳng $y = \frac{b}{a}x$ và $y = -\frac{b}{a}x$.

Tâm sai của hyperbol là $e = \frac{c}{a} > 1$.

4.3 Parabol

Parabol

Đường parabol là tập hợp các điểm cách đều một điểm cố định và một đường thẳng cố định.

Nghĩa là, với 1 điểm cố định F và đường thẳng cố định (d), parabol là tập hợp các điểm M sao cho $MF = d(M, d)$ với $d(M, d)$ là khoảng cách từ M tới đường thẳng (d).

Phép dời tọa độ cho phép ta dời một hình parabol có đỉnh ở bất kì điểm nào về gốc tọa độ.

Tức là, không mất tính tổng quát, ta chỉ cần xét các parabol dạng $y = ax^2$ là đủ.

Điểm cố định ở trên được gọi là **tiêu điểm**. Đường thẳng cố định ở trên gọi là **đường chuẩn**.

Parabol có tính đối xứng nên tiêu điểm nằm trên Oy. Đặt tọa độ của nó là $F = (0, f)$.

Đường chuẩn nằm ngang nên ta có parabol là các điểm $M = (x, y)$ sao cho

$MF = \sqrt{x^2 + (y - f)^2}$ và $d(M, d) = y + f$ (trường hợp M trùng với đỉnh nên điều kiện của parabol xảy ra tương đương với M cách đều tiêu điểm và đường chuẩn, nghĩa là đường chuẩn có dạng $y = -f$).

Do đó $\sqrt{x^2 + (y - f)^2} = y + f$. Bình phương và biến đổi ta thu gọn được

$$f = \frac{1}{4a}$$

Thường thì ta đặt $p = f$, khi đó phương trình parabol trở thành

$$x^2 = 4py$$

Đây là dạng chính tắc của parabol với trục đối xứng dọc.

Tâm sai của hyperbol là $e = \frac{c}{a} = 1$.