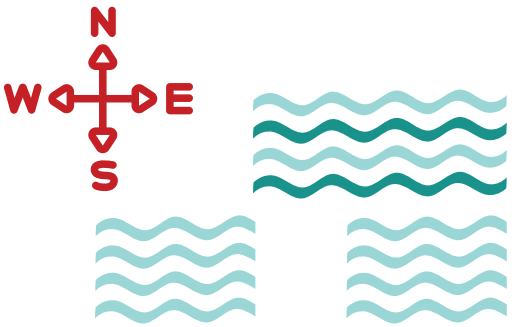
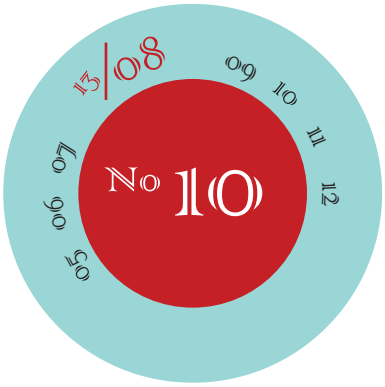


Kĩ năng tự học là kĩ năng quan trọng nhất mà một người có thể sở hữu."

TONY BUZAN

"Logic là cơ sở của hầu như toàn bộ kiến thức mà chúng ta thu nhận được.

LEONARD EULER

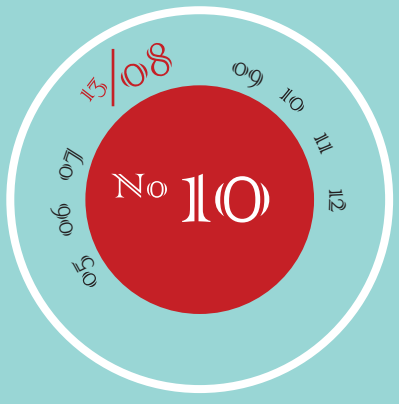


Epsilon

Tạp chí online của cộng đồng những người yêu toán

Epsilon

Tạp chí online của cộng đồng
những người yêu toán



LỜI NGỎ

Nắng tháng 8 vàng rực trên những con đường, mùa hè đã đến độ chín mùi. Những cuộc vui, những chuyến đi xa đang đúng dịp tưng bừng nhất. Nhưng đâu đó, vào độ tháng tám lưng chừng, vài cơn mưa chợt đi chợt đến, vài ngọn gió sớm mát lành đưa đến mùi vị một mùa thu tựu trường chẳng còn bao xa.

Tạp chí Epsilon, ra mắt vào những tuần lễ cuối cùng của mùa hạ, cũng là số ra mắt lần thứ 10, một con số đẹp và trọn vẹn để mọi người cùng nhìn lại một chặng đường đã đi qua. Đối với những người trong ban biên tập, số 10, coi như đã tròm trèm một chu kỳ, và bắt đầu một chặng đường mới để phấn đấu.

Chúng tôi cũng hy vọng rằng với bạn đọc, đặc biệt với những người gắn bó với bảng đen bục giảng, ít nhiều số 10 này cũng sẽ có ý nghĩa vào thời khắc giao mùa. Để khi tháng tám trôi qua, tháng 9 gõ cửa, chúng ta lại cùng bắt đầu một chặng mới trên con đường truy tầm tri thức mênh mông.

Đi nhiều người, bạn sẽ đi rất xa ...

Mục lục

BẤT ĐẲNG THỨC KHÔNG-SHANNON

Ngô Quang Hưng
LogicBlox

TÓM TẮT

Tiếp theo bài giới thiệu về entropy, các bất đẳng thức Shannon và vài ứng dụng trong Epsilon số 7, bài này giới thiệu một bất đẳng thức không-Shannon cùng với một số tính chất mà các bất đẳng thức mà hàm entropy phải thoả mãn. Trong hành trình nho nhỏ này, ta sẽ tình cờ gặp một mối quan hệ giữa lý thuyết số và lý thuyết thông tin, và giữa bất đẳng thức thông tin và quy hoạch tuyến tính.

Trước hết, xin tóm tắt lại một số ký hiệu đã được giới thiệu và dùng trong bài trước [5]. Ta chỉ xét các phân bố xác suất trên n biến rời rạc $X_0, \ldots, X_n$, trên các miền $\chi_1, \ldots, \chi_n$ tương ứng. Ta dùng $\mathbf{X}_S = (X_i)_{i\in S}$ để ký hiệu một bộ biến ngẫu nhiên có chỉ số trong tập $S \subseteq [n]$, và $\mathbf{x}_S = (x_i)_{i\in S} \in \prod_{i\in S} \chi_i$ để ký hiệu một bộ giá trị cụ thể của các biến này. Entropy của một phân bố cho ta một con số $H[\mathbf{X}_S]$ với mỗi tập con $\emptyset \neq S \subseteq [n]$. Do đó, ta viết $H(S)$ thay vì $H[\mathbf{X}_S]$. Entropy của một phân bố cho trước là một hàm tập hợp $H : 2^{[n]} - \{\emptyset\} \to \mathbb{R}_+$. Hàm entropy H cũng là một vector trên không gian $\mathbb{R}_+^{2^n-1}$, tại vì có tất cả $2^n - 1$ tập con khác rỗng của $[n]$, và mỗi tập con là một toạ độ. Với một phân bố khác thì ta lại có entropy khác, nghĩa là một hàm tập hợp khác và một vector khác trong không gian $\mathbb{R}_+^{2^n-1}$. Bài trước đã chứng minh định lý sau đây:

Định lý 0.1. *Xét một phân bố xác suất liên kết của n biến tuỳ hỉ. Entropy H của phân bố này thoả ba tính chất sau đây:*

- Tính không âm*:* $H(S) \geq 0, \forall S \subseteq [n]$, $S \neq \emptyset$.
- Tính đơn điệu*:* $H(S) \leq H(T), \forall S \subseteq T \subseteq [n]$.
- Tính sub-modular*:* $H(S \cup T) + H(S \cap T) \leq H(S) + H(T), \forall S, T \subseteq [n]$.

Nói cách khác, entropy H là một polymatroid.

Tất cả các bất đẳng thức được thoả mãn bởi mọi polymatroid thì tất nhiên cũng được thoả mãn bởi mọi hàm entropy. Ta gọi chúng là các *bất đẳng thức kiểu-Shannon*.

1. Bất đẳng thức Zhang-Yeung

Trong hơn nửa thế kỷ, tất cả các bất đẳng thức entropy mà chúng ta biết thì đều là bất đẳng thức kiểu Shannon. Năm 1998, Zhang và Yeung [7] khám phá ra một bất đẳng thức không chứng minh được bằng các tính chất của polymatroid:

$$2I(C;D) \leq I(A;B) + I(A;C,D) + 3I(C;D|A) + I(C;D|B). \tag{1}$$

Nhớ rằng thông tin tương hỗ là một hàm tuyến tính của entropy:

$$\begin{aligned} I(X;Y) &= H(X) + H(Y) - H(XY), \\ I(X;Y|Z) &= H(XZ) + H(YZ) - H(XYZ) - H(Z), \end{aligned}$$

cho nên bất đẳng thức (1) là một bất đẳng thức entropy. Bất đẳng thức này cho thấy sự tồn tại của một bất đẳng thức đúng với mọi entropy nhưng không đúng với mọi polymatroids. Làm thế nào mà Zhang-Yeung tìm ra và chứng minh được rằng

1. Bất đẳng thức (1) *không* suy ra được từ các tính chất của polymatroid?
2. Tất cả các hàm entropy đều phải thoả bất đẳng thức (1)?

1.1. Quy hoạch tuyến tính

Ta đi đường vòng để trả lời câu hỏi đầu tiên. Nếu đi đường thẳng thì chỉ cần chỉ ra một polymatroid không thoả mãn bất đẳng thức (1) là xong. Một bất đẳng thức suy ra được từ các tính chất của polymatroids nếu và chỉ nếu nó được thoả mãn bởi tất cả các polymatroids. Nhưng nói vậy thì quá mù mờ, ta cần một phương pháp có hệ thống nào để kiểm tra xem một bất đẳng thức kiểu như $H(AB) + H(AC) + H(BC) \geq 2H(ABC)$ có được thoả mãn bởi tất cả các polymatroids (trên 3 biến) hay không.

Nhớ rằng, như đã viết ở trên, một hàm tập hợp $h : 2^{[n]} \to \mathbb{R}_+$ cũng được xem như một vector $\mathbf{h} \in \mathbb{R}_+^{2^n-1}$ (vì $h(\emptyset) = 0$ trong ngữ cảnh của ta). Ta dùng các tập con không rỗng của $[n]$ để đánh chỉ số các toạ độ của vector $\mathbf{h}$. Một hàm tập hợp là một polymatroid nếu và chỉ nếu nó nằm trong đa diện $P = \{\mathbf{Mh} \geq \mathbf{0}, \mathbf{h} \geq \mathbf{0}\}$, trong đó $\mathbf{M}$ là ma trận của các tính chất đơn điệu và sub-modular ở trên. Ví dụ, với tính chất sub-modular trên tập S, T thì sẽ có một hàng của ma trận $\mathbf{M}$ tương ứng với bất đẳng thức

$$h(S) + h(T) - h(S \cup T) - h(S \cap T) \geq 0.$$

Hàng này của ma trận $\mathbf{M}$ có hai số 1 ở các toạ độ S, T, và hai số -1 ở các toạ độ $S \cup T$ và $S \cap T$.

Một bất đẳng thức tuyến tính sẽ có dạng $\mathbf{c}^T\mathbf{h} \geq 0$, trong đó $\mathbf{c} \in \mathbb{R}^{2^n-1}$ là một vector hệ số. Ví dụ, trong bất đẳng thức

$$h(AB) + h(AC) + h(BC) - 2h(ABC) \geq 0$$

thì vector $\mathbf{c}$ có ba số 1 ở các toạ độ AB, AC, BC, và một số -2 ở toạ độ ABC. Câu hỏi thứ nhất ở trên tương đương với câu hỏi: "làm thế nào để biết là $\mathbf{c}^T\mathbf{h} \geq 0$ đúng với mọi $\mathbf{h} \in P$?" Lưu ý rằng vector $\mathbf{0} \in P$, ta có

$$\mathbf{c}^T\mathbf{h} \geq \mathbf{0}, \forall \mathbf{h} \in P \text{ nếu và chỉ nếu } \min\{\mathbf{c}^T\mathbf{h} \mid \mathbf{M}\mathbf{h} \geq \mathbf{0}, \mathbf{h} \geq \mathbf{0}\} = 0.$$

Bài toán $\min\{\mathbf{c}^T\mathbf{h} \mid \mathbf{M}\mathbf{h} \geq \mathbf{0}, \mathbf{h} \geq \mathbf{0}\}$ là một bài toán quy hoạch tuyến tính cơ bản. Và ta có thể giải nó (bằng máy tính) để kiểm tra xem bất đẳng thức $\mathbf{c}^T\mathbf{h} \geq 0$ có đúng với mọi polymatroids hay không. Một cách khác là ta dùng tính chất đối ngẫu của quy hoạch tuyến tính; tính chất này nói rằng

$$\min\{\mathbf{c}^T\mathbf{x} \mid \mathbf{A}\mathbf{x} \geq \mathbf{b}, \mathbf{x} \geq \mathbf{0}\} = \max\{\mathbf{b}^T\mathbf{y} \mid \mathbf{A}^T\mathbf{y} \leq \mathbf{c}, \mathbf{y} \geq \mathbf{0}\},$$

nếu như một trong hai bài toán có hàm mục tiêu hữu hạn. Bài toán $\min\{\mathbf{c}^T\mathbf{h} \mid \mathbf{M}\mathbf{h} \geq \mathbf{0}, \mathbf{h} \geq \mathbf{0}\}$ có quy hoạch đối ngẫu của nó viết là

$$\min\{\mathbf{c}^T\mathbf{h} \mid \mathbf{M}\mathbf{h} \geq \mathbf{0}, \mathbf{h} \geq \mathbf{0}\} = \max\{\mathbf{0}^T\mathbf{y} \mid \mathbf{M}^T\mathbf{y} \leq \mathbf{c}, \mathbf{y} \geq \mathbf{0}\}.$$

Bài toán đối ngẫu có hàm mục tiêu hữu hạn (bằng 0) nếu và chỉ nếu nó có nghiệm! Như vậy, ta vừa chứng minh được bổ đề sau[1]:

Bổ đề 1.1. *Bất đẳng thức $\mathbf{c}^T\mathbf{h} \geq 0$ đúng với mọi polymatroid $\mathbf{h}$ nếu và chỉ nếu hệ bất phương trình sau đây có nghiệm:*

$$\mathbf{M}^T\mathbf{y} \leq \mathbf{c},\ \mathbf{y} \geq \mathbf{0}.$$

Trong đó, $\mathbf{M}$ là ma trận của các bất đẳng thức sub-modularity và đơn điệu.

Nói cách khác, bất đẳng thức $\mathbf{c}^T\mathbf{h} \geq 0$ đúng nếu mà chỉ nếu ta tìm được các hệ số $\mathbf{y}$ không âm và tổ hợp tuyến tính dùng các hệ số $\mathbf{y}$ của các bất đẳng thức sub-modularity và đơn điệu "suy ra" $\mathbf{c}^T\mathbf{h} \geq 0$ được. "Đối ngẫu trong quy hoạch tuyến tính" nghe có vẻ hơi vang vang, nhưng nó là một tính chất đơn giản; nếu hệ bất phương trình có nghiệm thì ta suy ra được rằng

$$\mathbf{c}^T\mathbf{h} \geq (\mathbf{M}^T\mathbf{y})^T\mathbf{h} = \mathbf{y}^T\mathbf{M}\mathbf{h} \geq \mathbf{y}^T\mathbf{0} = 0.$$

Tất nhiên, chứng minh trực tiếp chiều ngược lại của bổ đề trên mà không dùng quy hoạch tuyến tính thì khó hơn một chút; và làm việc này không cần thiết lắm trong ngữ cảnh của bài viết. Tóm lại, Bổ Đề 1.1 cho chúng ta một thuật toán để kiểm tra xem một bất đẳng thức kiểu (1) có phải là bất đẳng thức Shannon hay không? Ta chỉ cần kiểm tra xem hệ bất phương trình tuyến tính tương ứng có nghiệm hay không; bất kỳ một LP-solver nào (như cplex, Gurobi) đều làm được điều này dễ dàng.

1.2. Lên không gian nhiều chiều hơn

Bây giờ ta quay lại câu hỏi thứ hai: làm thế nào để chứng minh rằng (1) là một bất đẳng thức mà tất cả các hàm entropy trên 4 biến đều phải thoả? Đây thật sự là câu hỏi mấu chốt cần một phát kiến tuyệt vời của Zhang và Yeung. Đại khái, họ xây dựng một biến ngẫu nhiên thứ 5, gọi là R, và dùng một bất đẳng thức kiểu Shannon cho phân bố (A, B, C, D, R). Biến R có một tính chất

[1] Đây chẳng qua là một dạng của bổ đề Farkas

đặc biệt, mà nhờ đó khi ta "chiếu" bất đẳng thức kiểu Shannon từ không gian (A, B, C, D, R) xuống không gian (A, B, C, D) thì ta có bất đẳng thức (1).

Một cách nôm na hơn, gọi Γ_n^* là tập tất cả các hàm entropies H của n biến, và Γ_n là tập tất cả các hàm polymatroids của n biến. Định lý 0.1 cho ta biết $\Gamma_n^* \subseteq \Gamma_n$. Ngoài ra, Γ_n là một tập lồi, và Γ_n^* không phải là tập đóng, nhưng bao đóng của nó cũng là một tập lồi. Một bất đẳng thức như $\mathbf{c}^T\mathbf{h} \geq 0$, nếu đúng với mọi polymatroid, thì chẳng qua là vì $\mathbf{c}^T\mathbf{h}$ là một siêu phẳng nằm ngoài Γ_n; vector $\mathbf{c}$ là một pháp tuyến của siêu phẳng này. Một bất đẳng thức như (1) đúng với Γ_n^* nhưng không đúng với Γ_n thì phải là một siêu phẳng nằm ngoài tập Γ_n^* và cắt vào trong Γ_n. Ở trên ta đã chứng minh rằng cái siêu phẳng tương ứng với (1) cắt Γ_4. Để chứng minh rằng nó nằm ngoài Γ_4^*, ta tìm một siêu phẳng nằm ngoài Γ_5 sao cho "hình chiếu" của nó xuống không gian (A, B, C, D) chính là siêu phẳng tương ứng với (1).

Cụ thể hơn, ta ghị lại toàn bộ phương pháp của Zhang-Yeung dùng một chứng minh mới hơn [2].

Bổ đề 1.2. *Gọi A, B, C, D là bốn biến từ một phân bố liên kết nào đó. Thì, tồn tại một biến ngẫu nhiên R phân bố liên kết với A, B, C, D, với các tính chất như sau:*

(i) Phân bố ngoại vi của (A, B, C) và (A, B, R) giống hệt nhau (với C thay bằng R)

(ii) $I(CD; R|AB) = 0$.

Tóm tắt. Gọi $p(a, b, c, d)$ là hàm cân nặng xác suất của phân bố liên kết của (A, B, C, D). Gọi R là một biến ngẫu nhiên mới có cùng miền với C, và định nghĩa hàm cân nặng xác suất

$$p'(a, b, c, d, r) = \frac{p(a, b, c, d) \sum_d p(a, b, r, d)}{\sum_{c,d} p(a, b, c, d)}.$$

Dễ thấy rằng $\sum_r p'(a, b, c, d, r) = p(a, b, c, d)$: nghĩa là phân bố ngoại vi trên (A, B, C, D) của p' chính là phân bố cũ của (A, B, C, D). Và từ đó ta cũng có p' là một hàm cân nặng xác suất (tổng bằng 1). Từ đây, kết thúc chứng minh bổ đề chỉ còn là cơ bắp. □

Ta viết lại bất đẳng thức (1) một chút. Trước hết, chuyển $I(C; D)$ sang vế phải và sắp xếp lại, dễ thấy bất đẳng thức (1) tương đương với bất đẳng thức sau đây:

$$\begin{aligned}
& I(C; D) \\
\leq\ & I(A; B) + 2I(C; D|A) + I(C; D|B) + I(A; C, D) + I(C; D|A) - I(C; D) \\
=\ & I(A; B) + 2I(C; D|A) + I(C; D|B) + H(A) + H(CD) - H(ACD) \\
& + H(AC) + H(AD) - H(ACD) - H(A) - H(C) - H(D) + H(CD) \\
=\ & I(A; B) + 2I(C; D|A) + I(C; D|B) \\
& + H(CD) + H(AC) - H(ACD) - H(D) + H(AD) + H(CD) - H(ACD) - H(C) \\
=\ & I(A; B) + 2I(C; D|A) + I(C; D|B) + I(A; D|C) + I(A; C|D).
\end{aligned}$$

Sau đó, đổi biến $A \leftrightarrow C$ và $B \leftrightarrow D$ thì ta có (1) tương đương với (2) dưới đây.

Định lý 1.3 (Zhang-Yeung)**.** *Gọi A, B, C, D là các biến ngẫu nhiên từ một phân bố liên kết bất kỳ, thì*

$$I(A;B) \leq 2I(A;B|C) + I(A;C|B) + I(B;C|A) + I(A;B|D) + I(C;D). \tag{2}$$

Chứng minh. Gọi R là biến ngẫu nhiên từ Bổ Đề 1.2. Lưu ý rằng thông tin tương hỗ (giữa hai biến) và thông tin tương hỗ có điều kiện là các đại lượng không âm. Ta có

$$\begin{aligned}
& I(A;B) \\
\leq\ & I(A;B) \\
& +I(C;R|A) + I(C;D|R) + I(AB;R|CD) + I(D;R|B) \\
& +I(A;B|RD) + I(D;R|A) + I(R;C|B) + I(A;B|CR) + I(C;R|ABD) \\
=\ & 2I(A;B|C) + I(A;C|B) + I(B;C|A) + I(A;B|D) + I(C;D) \\
(=0)\quad & +2I(CD;R|AB) \\
(=0)\quad & +I(A;B|R) - I(A;B|C) \\
(=0)\quad & +I(A;R|B) - I(A;C|B) \\
(=0)\quad & +I(B;R|A) - I(B;C|A).
\end{aligned}$$

□

2. Bất đẳng thức thông tin và bất đẳng thức nhóm

Định nghĩa 2.1 (Bất đẳng thức thông tin)**.** Nếu bất đẳng thức

$$\mathbf{c}^T\mathbf{h} \geq 0,$$

đúng với mọi $\mathbf{h} \in \Gamma_n^*$ thì nó gọi là một *bất đẳng thức thông tin*.

Do tất cả các hàm entropy đều là polymatroid, tất cả các bất đẳng thức Shannon đều là các bất đẳng thức thông tin. Ngược lại, có một số vô hạn [4] các bất đẳng thức thông tin không phải là bất đẳng thức Shannon. Ví dụ cụ thể là bất đẳng thức (1). Bổ Đề 1.1 đã cho ta biết cách (bằng một thuật toán) kiểm tra xem một bất đẳng thức có phải là bất đẳng thức Shannon hay không. Từ đó nảy ra câu hỏi rất tự nhiên là: có kết quả nào cho chúng ta một thuật toán xác minh một bất đẳng thức thông tin không? Tiếc rằng cho đến nay chưa có kết quả nào như vậy. Tuy nhiên, có một kết quả thú vị của Chan và Yeung [1] liên kết bất đẳng thức thông tin và cái gọi là "bất đẳng thức nhóm".

Định nghĩa 2.2 (Hàm đặc tính nhóm)**.** Gọi $\mathbf{h} : 2^{[n]} - \{\emptyset\} \to \mathbb{R}_+$ là một hàm tập hợp. Hàm này được gọi là *hàm đặc tính nhóm*[2] nếu tồn tại một nhóm hữu hạn G, và n nhóm con $G_1, \ldots, G_n$, sao cho

$$h(S) = \log_2 \frac{|G|}{|G_S|},\ \forall S \subseteq [n], S \neq \emptyset.$$

Trong đó, $G_S = \bigcap_{i\in S} G_i$ là một nhóm con của G. Gọi Υ_n là tập tất cả các hàm đặc tính nhóm vừa định nghĩa.

[2]Group-characterizable function

Định nghĩa 2.3 (Bất đẳng thức nhóm)**.** Nếu bất đẳng thức $\mathbf{c}^T\mathbf{h} \geq 0$ đúng với mọi $\mathbf{h} \in \Upsilon_n$, thì nó được gọi là một *bất đẳng thức nhóm*. Cụ thể hơn, một bất đẳng thức nhóm là bất đẳng thức có dạng

$$\sum_{\emptyset \neq S \subseteq [n]} c(S) \cdot \log_2 \frac{|G|}{|G_S|} \geq 0, \tag{3}$$

sao cho nó đúng *với mọi* nhóm hữu hạn G và n nhóm con $G_1, \ldots, G_n$. (Nhớ rằng $G_S = \bigcap_{i \in S} G_i$.)

Ta đã gặp nhiều bất đẳng thức thông tin [5], nhưng chưa gặp bất đẳng thức nhóm nào. Đòi hỏi (3) đúng với mọi nhóm hữu hạn và n nhóm con có vẻ rất mạnh. Có tồn tại bất đẳng thức nhóm nào hay không? Trước hết ta xét một ví dụ đơn giản:

Ví dụ 2.4. Gọi G là một nhóm hữu hạn bất kỳ, và G_1, G_2 là hai nhóm con. Ta có

$$\log_2 \frac{|G|}{|G_1|} + \log_2 \frac{|G|}{|G_2|} - \log_2 \frac{|G|}{|G_1 \cap G_2|} \geq 0.$$

Để chứng minh bất đẳng thức này, ta viết nó ở dạng khác: $|G| \cdot |G_1 \cap G_2| \geq |G_1| \cdot |G_2|$. Định nghĩa $G_1 \circ G_2 = \{a \circ b \mid a \in G_1, b \in G_2\}$[3], thì ta có thể chứng minh

$$|G_1| \cdot |G_2| = |G_1 \times G_2| = |G_1 \circ G_2| \cdot |G_1 \cap G_2| \leq |G| \cdot |G_1 \cap G_2|.$$

Bài tập 2.5. Chứng minh rằng $|G_1 \times G_2| = |G_1 \circ G_2| \cdot |G_1 \cap G_2|$, với mọi nhóm con G_1, G_2 của một nhóm G hữu hạn.

Kết quả rất đẹp của Chan và Yeung [1] là định lý sau đây:

Định lý 2.6. *Bất đẳng thức $\mathbf{c}^T\mathbf{h} \geq 0$ là bất đẳng thức thông tin nếu và chỉ nếu nó là bất đẳng thức nhóm.*

Chứng minh. Trước khi chứng minh, ta thảo luận một chút về kết quả này. Thoạt nhìn, nó hơi có vẻ lừa đảo vì nó chỉ chuyển từ một câu hỏi khó về lý thuyết thông tin sang một câu hỏi khó trong lý thuyết nhóm. Nó không cho chúng ta thông tin gì về phương pháp để xác minh xem một bất đẳng thức có phải là bất đẳng thức thông tin hay bất đẳng thức nhóm hay không. Mặt khác, liên hệ này lại rất thú vị. Để chứng minh một bất đẳng thức nhóm mới, ta chỉ cần chứng minh bất đẳng thức thông tin mới mà không cần biết gì về lý thuyết nhóm. Quyển sách của Yeung [6] có một vài ví dụ bất đẳng thức nhóm mới chứng minh được bằng lý thuyết thông tin mà trước đó các nhà đại số chưa biết. Ngược lại, nhờ định lý này mà các nhà lý thuyết thông tin có thể "cầu cứu" các nhà đại số, nhờ họ chứng minh hộ bất đẳng thức cho mình.

Bây giờ ta chứng minh định lý. Gọi $\bar{\Gamma}_n^*$ là bao đóng của tập Γ_n^*, và $\overline{\mathsf{conv}}(\Upsilon_n)$ là bao đóng lồi của tập Υ_n. Ta quan sát rằng

- Bất đẳng thức $\mathbf{c}^T\mathbf{h} \geq 0$ là bất đẳng thức thông tin nếu và chỉ nếu $\Gamma_n^* \subseteq \left\{\mathbf{h} \in \mathbb{R}^{2^n-1} \mid \mathbf{c}^T\mathbf{h} \geq 0\right\}$. Do tập $\{\mathbf{h} \in \mathbb{R}^{2^n-1} \mid \mathbf{c}^T\mathbf{h} \geq 0\}$ là tập đóng và lồi, điều này tương đương với

$$\bar{\Gamma}_n^* \subseteq \left\{\mathbf{h} \in \mathbb{R}^{2^n-1} \mid \mathbf{c}^T\mathbf{h} \geq 0\right\}. \tag{4}$$

[3] $G_1 \circ G_2$ không nhất thiết là nhóm con của G.

- Tương tự như vậy, bất đẳng thức $\mathbf{c}^T\mathbf{h} \geq 0$ là bất đẳng thức nhóm nếu và chỉ nếu

$$\overline{\mathsf{conv}}(\Upsilon_n) \subseteq \left\{\mathbf{h} \in \mathbb{R}^{2^n-1} \mid \mathbf{c}^T\mathbf{h} \geq 0\right\}. \tag{5}$$

Để chứng minh rằng (4) tương đương với (5), ta chứng minh $\bar{\Gamma}_n^* = \overline{\mathsf{conv}}(\Upsilon_n)$ bằng hai bước. Bổ đề 2.7 chứng minh rằng $\Upsilon_n \subseteq \Gamma_n^*$; do đó $\overline{\mathsf{conv}}(\Upsilon_n) \subseteq \bar{\Gamma}_n^*$ vì $\bar{\Gamma}_n^*$ là một hình nón lồi [6]. Bổ đề 2.8 chứng minh chiều ngược lại $\bar{\Gamma}_n^* \subseteq \overline{\mathsf{conv}}(\Upsilon_n)$. □

Bổ đề 2.7. *Ta có $\Upsilon_n \subseteq \Gamma_n^*$, nghĩa là mọi hàm đặc tính nhóm đều là hàm entropy*

Chứng minh. Gọi $\mathbf{h} \in \Upsilon_n$ là một hàm đặc tính nhóm, và G là một nhóm hữu hạn với các nhóm con $G_1, \ldots, G_n$ sao cho $h(S) = \log_2 \frac{|G|}{G_S}$ với mọi $\emptyset \neq S \subseteq [n]$. Xét không gian xác suất $\Omega = G$ với phân bố đều $p(g) = \frac{1}{|G|}$ với mọi $g \in G$. Với mọi $i \in [n]$, định nghĩa biến ngẫu nhiên $X_i : \Omega \to 2^G$ như sau $X_i(g) = gG_i$ – là lớp trái[4] của nhóm G_i. Với một tập $S \subseteq [n]$ và bộ $(g_i)_{i\in S}$ bất kỳ, dễ thấy

$$\begin{aligned}
\mathop{\mathsf{Prob}}_{g\in\Omega}\left[X_i = g_iG_i, \forall i \in S\right] &= \mathop{\mathsf{Prob}}_{g\in\Omega}\left[gG_i = g_iG_i, \forall i \in S\right] \\
&= \mathop{\mathsf{Prob}}_{g\in\Omega}\left[g \in g_iG_i, \forall i \in S\right] \\
&= \frac{|\bigcap_{i\in S} g_iG_i|}{|G|}.
\end{aligned}$$

Nếu $\bigcap_{i\in S} g_iG_i \neq \emptyset$, lấy một phần tử $a \in \bigcap_{i\in S} g_iG_i$ tuỳ ý, thì ta có

$$\bigcap_{i\in S} g_iG_i = \bigcap_{i\in S} aG_i = a\bigcap_{i\in S} G_i = aG_S.$$

Vậy thì $\bigcap_{i\in S} g_iG_i$ hoặc là tập rỗng hoặc có kích thước bằng đúng $|G_S|$. Hơn nữa, có tổng cộng $|G|/|G_S|$ tập không rỗng như thế. Do đó,

$$\frac{|\bigcap_{i\in S} g_iG_i|}{|G|} = \begin{cases} \frac{|G_S|}{|G|} & \text{nếu } \bigcap_{i\in S} g_iG_i \neq \emptyset \\ 0 & \text{nếu } \bigcap_{i\in S} g_iG_i = \emptyset. \end{cases}$$

Từ đó, dễ thấy $H[\mathbf{X}_S] = \log_2(|G|/|G_S|)$ và $\mathbf{h} \in \Gamma_n^*$. □

Bổ đề 2.8. *Ta có $\bar{\Gamma}_n^* \subseteq \overline{\mathsf{conv}}(\Upsilon_n)$, với mọi $n \geq 1$.*

Chứng minh. Ta theo trình bày của Lun [3]. Gọi $\mathbf{h} \in \Gamma_n^*$ là một hàm entropy tuỳ ý, nghĩa là có n biến ngẫu nhiên $X_1, \ldots, X_n$ sao cho $H(S) = h(S)$. Để đơn giản, ta giả sử là miền χ_i của biến X_i là miền hữu hạn, và cụ thể hơn là các xác suất đều là số hữu tỉ. (Trong trường hợp tổng quát, ta dùng một chuỗi số hữu tỉ tiến đến số vô tỉ.) Ta chứng minh rằng tồn tại một chuỗi $\mathbf{f}^{(r)} \in \Upsilon_n$ sao cho $\lim_{r\to\infty} \mathbf{f}^{(r)}/r = \mathbf{h}$.

Gọi q là mẫu số chung của các xác suất $\mathsf{Prob}\left[\mathbf{X}_{[n]} = \mathbf{x}_{[n]}\right]$. Chọn $r = q, 2q, 3q, \ldots$ là một bội số của q, và $\mathbf{A}$ là một ma trận $n \times r$ sao cho mỗi cột $\mathbf{x}_{[n]}$ của $\mathbf{A}$ xuất hiện đúng $r \cdot \mathsf{Prob}\left[\mathbf{X}_{[n]} = \mathbf{x}_{[n]}\right]$ lần.

[4] Left coset

Với $\emptyset \neq S \subseteq [n]$, gọi $\mathbf{A}_S$ là ma trận con của $\mathbf{A}$ xây dựng bằng cách lấy các hàng số i của $\mathbf{A}$ với $i \in S$. Dễ thấy rằng, một cột $\mathbf{x}_S$ xuất hiện trong $\mathbf{A}_S$ đúng $r \cdot \mathsf{Prob}\big[\mathbf{X}_S = \mathbf{x}_S\big]$ lần.

Gọi $G = S_r$ là nhóm hoán vị của các cột của $\mathbf{A}$. Gọi G_i là nhóm các hoán vị các cột của $\mathbf{A}$ sao cho hàng thứ i của $\mathbf{A}$ không thay đổi. Vậy thì G_S là nhóm các hoán vị làm cho ma trận $\mathbf{A}_S$ không đổi. Dễ thấy rằng

$$|G_S| = \prod_{\mathbf{x}_S \in \prod_{i\in S} \chi_i} (r \cdot \mathsf{Prob}\big[\mathbf{X}_S = \mathbf{x}_S\big])!$$

Dùng xấp xỉ Stirling, ta có

$$\begin{aligned}
& \lim_{r\to\infty} \frac{1}{r} \log_2 \frac{|G|}{|G_S|} \\
= \; & \lim_{r\to\infty} \frac{1}{r} \log_2 \frac{r!}{\prod_{\mathbf{x}_S} (r \cdot \mathsf{Prob}\big[\mathbf{X}_S = \mathbf{x}_S\big])!} \\
= \; & \lim_{r\to\infty} \frac{1}{r} \left(r \log_2 r - \sum_{\mathbf{x}_S} r \cdot \mathsf{Prob}\big[\mathbf{X}_S = \mathbf{x}_S\big] \log_2 \left(r \cdot \mathsf{Prob}\big[\mathbf{X}_S = \mathbf{x}_S\big] \right) + O(\log_2 r) \right) \\
= \; & \lim_{r\to\infty} \left(\log_2 r - \sum_{\mathbf{x}_S} \mathsf{Prob}\big[\mathbf{X}_S = \mathbf{x}_S\big] \log_2 \left(r \cdot \mathsf{Prob}\big[\mathbf{X}_S = \mathbf{x}_S\big] \right) \right) \\
= \; & \lim_{r\to\infty} \left(- \sum_{\mathbf{x}_S} \mathsf{Prob}\big[\mathbf{X}_S = \mathbf{x}_S\big] \log_2 \mathsf{Prob}\big[\mathbf{X}_S = \mathbf{x}_S\big] \right) \\
= \; & - \sum_{\mathbf{x}_S} \mathsf{Prob}\big[\mathbf{X}_S = \mathbf{x}_S\big] \log_2 \mathsf{Prob}\big[\mathbf{X}_S = \mathbf{x}_S\big] \\
= \; & H[\mathbf{X}_S] \\
= \; & h(S).
\end{aligned}$$

Định nghĩa $\mathbf{f}^{(r)} = \log_2 \frac{|G|}{|G_S|}$ thì ta có $\lim_{r\to\infty} \mathbf{f}^{(r)}/r = \mathbf{h}$.

□

Tài liệu

[1] Chan, T. H., and Yeung, R. W. On a relation between information inequalities and group theory. *IEEE Trans. Information Theory 48*, 7 (2002), 1992–1995.

[2] Dougherty, R., Freiling, C. F., and Zeger, K. Non-shannon information inequalities in four random variables. *CoRR abs/1104.3602* (2011).

[3] Lun, D. S. A relationship between information inequalities and group theory, 2002.

[4] Matus, F. Infinitely many information inequalities. In *2007 IEEE International Symposium on Information Theory* (June 2007), pp. 41–44.

[5] NGÔ QUANG HƯNG. Bất đẳng thức kiểu Shannon và vài ứng dụng. *Epsilon*, 7 (Feb 2016).

[6] YEUNG, R. W. *A first course in information theory*. Information Technology: Transmission, Processing and Storage. Kluwer Academic/Plenum Publishers, New York, 2002. With a foreword by Toby Berger, With 1 CD-ROM.

[7] ZHANG, Z., AND YEUNG, R. W. On characterization of entropy function via information inequalities. *IEEE Trans. Inform. Theory 44*, 4 (1998), 1440–1452.

BẤT ĐẲNG THỨC TAM GIÁC, ĐA GIÁC VÀ ĐA DIỆN

Lê Tự Quốc Thắng
(School of Mathematics, Georgia Institute of Technology, Atlanta)

1. Bất đẳng thức tam giác, đa giác, và đa diện

1.1. Không gian chuẩn d chiều

Ký hiệu $\mathbb{R}$ là tập hợp số thực, và $\mathbb{R}_+$ là tập hợp các số thực dương. Xét không gian chuẩn d chiều $\mathbb{R}^d$ với tích vô hướng

$$\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^{d} x_i y_i, \quad \text{cho } \mathbf{x} = (x_1, \ldots, x_d), \mathbf{y} = (y_1, \ldots, y_d).$$

Khi $d = 2$ đây là mặt phẳng, và $d = 3$ là không gian 3 chiều. Một điểm $\mathbf{x} \in \mathbb{R}^d$ đôi khi được gọi là một vector.

Định nghĩa *chuẩn* của một vector

$$\|\mathbf{x}\| = \sqrt{\langle \mathbf{x}, \mathbf{x} \rangle},$$

và khoảng cách giữa 2 vector $\mathbf{x}, \mathbf{y}$, hoặc còn gọi là chiều dài đoạn $[\mathbf{x}, \mathbf{y}]$, là $\|\mathbf{x} - \mathbf{y}\|$. Một vector được gọi là vector đơn vị nếu nó có chuẩn bằng 1.

Với khái niệm độ dài này, ta có thể định nghĩa diện tích của một đa giác trong $\mathbb{R}^3$ cũng như thể tích của một đa diện trong $\mathbb{R}^3$.

Hai vector $\mathbf{x}, \mathbf{y}$ là *song song* nếu tồn tại một số thực k sao cho $\mathbf{x} = k\mathbf{y}$ hoặc $\mathbf{y} = k\mathbf{x}$.

Nếu $U \subset \mathbb{R}^d, \mathbf{a} \in \mathbb{R}^d$, và $k \in \mathbb{R}$, ta định nghĩa

$$\mathbf{a} + U = \{\mathbf{a} + \mathbf{x} \mid \mathbf{x} \in U\}$$
$$kU = \{k\mathbf{x} \mid \mathbf{x} \in U\}.$$

1.2. Bất đẳng thức tam giác

Như thông thường, ta đồng nhất chiều dài một cạnh của đa giác với chính cạnh ấy.

Mệnh đề 1.1. *Trong một tam giác, mỗi cạnh nhỏ hơn tổng của hai cạnh còn lại.*

Dùng ký hiệu vector, bất đẳng thức tam giác thường được phát biểu dưới dạng: Nếu $\mathbf{x}, \mathbf{y} \in \mathbb{R}^d$ không song song với nhau, ta có

$$\|\mathbf{x} + \mathbf{y}\| < |\mathbf{x}\| + \mathbf{y}\|.$$

Bất đẳng thức tam giác có thể chứng minh khá dễ dàng, trực tiếp từ định nghĩa khoảng cách, bằng cách sử dụng bất đẳng thức Cauchy về giá trị trung bình. Bất đẳng thức tam giác là một bất đẳng thức rất căn bản trong toán học. Nó là nền tảng của nhiều ngành toán học. Nó thể hiện nguyên lý đường thẳng là đường cực tiểu.

Ta cũng có phần đảo của mệnh đề về bất đẳng thức tam giác như sau, mà các học sinh cấp 2 đều biết qua phương pháp dựng hình.

Mệnh đề 1.2. *Nếu 3 số dương thỏa mãn tính chất mỗi số nhỏ hơn tổng của 2 số còn lại thì chúng là cạnh của một tam giác duy nhất, tùy theo các đẳng cự (isometry) của không gian.*

1.3. Bất đẳng thức đa giác

Bất đẳng thức tam giác có thể dễ dàng tổng quát hoá cho đa giác.

Mệnh đề 1.3. *(a) Trong một đa giác, mỗi cạnh nhỏ hơn tổng của các cạnh còn lại.*

(b) Ngược lại, nếu $n \geq 3$ số dương thoả mãn điều kiện mỗi số nhỏ hơn tổng các số còn lại thì chúng là cạnh của một đa giác lồi nào đó.

Bài tập 1.1. (a) Chứng minh mệnh đề trên.

(b) Chứng minh rằng nếu $n > 3$ thì ta không có tính duy nhất trong phần (b) của mệnh đề trên.

1.4. Bất đẳng thức đa diện

Thay vì xét tam giác, đa giác là các vật thể 2 chiều, ta hãy xét đa diện là các vật thể 3 chiều.

Định lý 1.4 (Bất đẳng thức đa diện)**.** *(a) Trong một đa diện, diện tích của một mặt nhỏ hơn tổng diện tích các mặt còn lại.*

(b) Ngược lại, nếu $n \geq 4$ số dương thoả mãn điều kiện mỗi số nhỏ hơn tổng các số còn lại thì chúng là diện tích của các mặt của một đa diện lồi nào đó.

Bài tập 1.2. Chứng minh phần (a) của định lý trên. (Gợi ý: Giả sử F là một mặt của đa giác. Hay chiếu trực giao các mặt khác xuống mặt phẳng chứa F.)

Phần (b) của định lý trên khó hơn phần (a) nhiều. Ở mục sau chúng ta sẽ đưa ra một chứng minh đơn giản dựa vào định lý Minkowski về đa diện, một định lý rất hay trong hình học không gian nhưng ít được biết đến.

Đến đây độc giả có thể đoán rằng định lý trên có thể tổng quát hoá cho không gian nhiều chiều.

2. Định lý Minkowksi

2.1. Trường hợp 2 chiều

Giả sử P là một đa giác. Nếu F là một cạnh của P, ký hiệu $A(F)$ là độ dài của F, và định nghĩa *vector pháp tuyến* của F, ký hiệu $\mathbf{u}(F)$, là vector đơn vị vuông góc với F va hướng ra ngoài đa giác P.

Định lý 2.1 (Định lý Minkowski 2 chiều)**.** *(a) Giả sử P là một đa giác lồi với các cạnh $F_1, \ldots, F_n$. Khi đó các vector $\mathbf{u}(F_1), \ldots, \mathbf{u}(F_n)$ không cùng nằm trên môt đường thẳng, và*

$$\sum_{i=1}^{n} A(F_i)\mathbf{u}(F_i) = \overrightarrow{0}.$$

(b) Ngược lại: Giả sử các vector đơn vị khác nhau $\mathbf{u}_1, \ldots, \mathbf{u}_n$ trong $\mathbb{R}^2$ và các số dương $a_1, \ldots a_n$ thỏa mãn điều kiện

- *$\mathbf{u}_1, \ldots, \mathbf{u}_n$ không cùng nằm trên một đường thẳng,*
- *$\sum_{i=1}^{n} a_i\mathbf{u}_i = \overrightarrow{0}$.*

Khi đó tồn tại duy nhất một đa giác lồi P với các cạnh $F_1, \ldots, F_n$ sao cho $a_i = A(F_i), \mathbf{u}_i = \mathbf{u}(F_i)$ với mọi $i = 1, \ldots, n$.

Định lý này không khó chứng minh lắm, và ta sẽ chứng minh nó trong mục 3.

2.2. Trường hợp 3 chiều

Định ly Minkowski trong trường hợp nhiều chiều hoàn toàn tương tự. Giả sử P là một đa diện lồi. Nếu F là một mặt của P, ký hiệu $A(F)$ là diện tích của mặt F, và định nghĩa *vector pháp tuyến* của F, ký hiệu $\mathbf{u}(F)$, là vector đơn vị vuông góc với F và hướng ra ngoài.

Định lý 2.2 (Định lý Minkowski 3 chiều)**.** *(a) Giả sử P là một đa diện lồi với các mặt $F_1, \ldots, F_n$. Khi đó các vector $\mathbf{u}(F_1), \ldots, \mathbf{u}(F_n)$ không cùng nằm trên một mặt phẳng, và*

$$\sum_{i=1}^{n} A(F_i)\mathbf{u}(F_i) = \overrightarrow{0}. \tag{1}$$

(b) Ngược lại: Giả sử các vector đơn vị khác nhau $\mathbf{u}_1, \ldots, \mathbf{u}_n$ trong $\mathbb{R}^3$ và các số dương $a_1, \ldots a_n$ thoả mãn điều kiện

- *các vector $\mathbf{u}_1, \ldots, \mathbf{u}_n$ không cùng nằm trên một mặt phẳng, và*

- $\sum_{i=1}^{n} a_i \mathbf{u}_i = \overrightarrow{0}$.

Khi đó tồn tại duy nhất một đa diện lồi P với các mặt $F_1, \ldots, F_n$ sao cho $a_i = A(F_i), \mathbf{u}_i = \mathbf{u}(F_i)$ với mọi $i = 1, \ldots, n$.

Chú ý 2.3. Định lý Minkowksi đúng trong không gian nhiều chiều.

Phần (a) của định lý trên không khó lắm, và sẽ được chứng minh trong mục 3. Phần (b) khó hơn nhiều và là phần thú vị nhất của định lý. Tính duy nhất của phần (b) làm định lý là một kết quả rất hay. Nếu các vector $\mathbf{u}_1, \ldots, \mathbf{u}_n$ và các số dương $a_1, \ldots a_n$ thoả mãn điều kiện của phần (b) trong định lý, ta không dễ xác định số cạnh của các mặt của đa giác P! Định lý Minkowksi có nhiều ưng dụng trong toán hiện đại.

Chúng ta sẽ thảo luận các chứng minh của định lý Minkowski trong các mục sau. Trước hết chúng ta sẽ chứng minh phần (b) của Định Lý 1.4 (định ly bất đẳng thức đa diện) bằng cách sử dụng định lý Minkowski.

2.3. Chứng minh định lý 1.4 (bất đẳng thức đa diện)

Chứng minh. (a) Chứng minh phần (a) được đưa ra trong bài tập 1.2. Phần (a) cũng dễ dàng suy ra từ định lý Minkowski như sau. Từ (1), ta có

$$A(F_1)\mathbf{u}(F_1) = -\left(\sum_{i=2}^{n} A(F_i)\mathbf{u}(F_i)\right).$$

Các vector $\mathbf{u}(F_2), \ldots, \mathbf{u}(F_n)$ không cùng nằm trên một đường thẳng (vì nếu không thì tất cả $\mathbf{u}(F_1), \ldots, \mathbf{u}(F_n)$ sẽ nằm trên một mặt phẳng). Tư bất đẳng thức tam giác ta có

$$A(F_1) < \sum_{i=2}^{n} A(F_i).$$

Lý luận tương tự, ta thấy mỗi một $A(F_i)$ nhỏ hơn tổng của các số còn lại.

(b) Giả sử $a_1, \ldots, a_n$ là các số dương sao cho mỗi số nhỏ hơn tổng các số còn lại. Theo định lý 1.3, tồn tại một đa giác lồi Q với các cạnh có độ dài $a_1, \ldots, a_n$. Giả sử các đỉnh của Q là $q_1, \ldots, q_n$ theo chiều kim đồng hồ. Đặt $\mathbf{x}_i = \overrightarrow{q_i q_{i+1}}$ (với $n+1 = 1$). Giả sử $\tau : \mathbb{R}^3 \to \mathbb{R}^3$ là phép quay quanh đường thẳng đi qua $q_1 q_3$ với góc quay 90^o. Đặt $\mathbf{x}_1 = \tau(\mathbf{x}_1)$ và $\mathbf{x}'_2 = \tau(\mathbf{x}_1)$. Ta có $\mathbf{x}'_1 + \mathbf{x}'_2 = \mathbf{x}_1 + \mathbf{x}_2$, vì vậy nếu đặt $\mathbf{x}'_i = \mathbf{x}_i$ voi $i > 2$, ta có

$$\sum_{i=1}^{n} \mathbf{x}'_i = \overrightarrow{0}.$$

Các vector $\mathbf{x}'_1, \ldots, \mathbf{x}'_n$ không cùng nằm trên một mặt phẳng. Theo định lý Minkowski, tồn tại một đa diện lồi P sao cho $|\mathbf{x}'_i| = a_i$ là diện tích của các mặt của đa diện lồi này.

□

Bài tập 2.1. (a) Hãy tìm hiểu điều kiện $n \geq 4$ được sử dụng như thế nào trong chứng minh trên.

(b) Hãy chứng minh rằng nếu $n \geq 4$ số thực dương thoả mãn mỗi một số nhỏ hơn tổng các số còn lại thì tồn tại vô hạn đa giác lồi mà diện tích các mặt là các số đã cho.

3. Chứng minh định lý Minkowski, phần I

Mặc dù là một định lý với phát biểu sơ cấp, các chứng minh được biết đến của phần (b) định lý Minkowski 3 chiều đều dùng đến công cụ toán cao cấp. Định lý Minkowski 2 chiều và phần (a) của định lý Minkowski 3 chiều có thể dễ dàng chứng minh bằng phương sơ cấp, và chúng ta sẽ thảo luận các chứng minh trong mục này.

3.1. Định lý Minkowski 2 chiều, phần (a)

Chứng minh 1. Giả sử các đỉnh của P theo chiều kim đồng hồ là $p_1, \ldots, p_n$. Ta có thể giả sử F_i là cạnh $p_i p_{i+1}$. Đặt $\mathbf{v}_i = \overrightarrow{p_i p_{i+1}}$. Ta có

$$\sum_{i=1}^{n} \mathbf{v}_i = \overrightarrow{0}.$$

Đặt τ là phép quay 90^o ngược chiều kim đồng hồ. Ta có $\tau(\mathbf{v}_i) = A(F_i)\mathbf{u}_i$. Vì vậy nếu các vector $\mathbf{u}(F_i)$ nằm trên một đường thẳng thì đa giác P sẽ nằm trên một đường thẳng là điều không thể xảy ra. Ta có

$$\sum_{i=1}^{n} A(F_i)\mathbf{u}_i = \tau\left(\sum_{i=1}^{n} \mathbf{v}_i\right) = \overrightarrow{0}.$$

□

Chứng minh 2. Mặc dù chứng minh này dài hơn, nhưng nó sẽ dễ dàng tổng quát hoá cho trường hợp nhiều chiều. Ý tưởng chính là nếu chiếu P lên một đường thẳng, thì ảnh của nó được phủ 2 lần bởi các điểm trên chu vi của P, một lần từ hướng trên xuống và một lần từ hướng dưới lên.

Giả sử $\mathbf{v}$ là một vector đơn vị bất kỳ. Ký hiệu $\mathbf{v}^\perp$ đường thẳng vuông góc với $\mathbf{v}$ đi qua góc toạ độ, và $\mathrm{pr}_\mathbf{v}$ là phép chiếu trực giao lên $\mathbf{v}^\perp$. Khi đó $X = \mathrm{pr}_\mathbf{v}(P)$ là một đoạn thẳng. Đặt $\mathring{X} = X \setminus \mathrm{pr}(V)$, với V là tập hợp các đỉnh của P. Dễ dàng thấy chiều dài của $\mathrm{pr}_\mathbf{v}(F_i)$ được tính bởi

$$\|\mathrm{pr}_\mathbf{v}(F_i)\| = A(F_i)\,|\langle \mathbf{u}(F), \mathbf{u}\rangle|. \tag{2}$$

Đặt

$$\mathcal{F}_+ = \bigcup_{\langle \mathbf{u}(F_i), \mathbf{v}\rangle > 0} F_i, \quad \mathcal{F}_- = \bigcup_{\langle \mathbf{u}(F_i), \mathbf{v}\rangle < 0} F_i.$$

Mệnh đề. Với mỗi $x \in \mathring{X}$, tồn tại duy nhất $x_+ \in \mathcal{F}_+$ và duy nhất $x_- \in \mathcal{F}_-$ sao cho $\mathrm{pr}_\mathbf{v}(x_+) = x = \mathrm{pr}_\mathbf{v}(x_-)$.

Theo mệnh đề trên, ta có

$$\sum_{\langle \mathbf{u}(F_i),\mathbf{v}\rangle>0} \|\mathrm{pr}_{\mathbf{v}}(F_i)\| = \|\mathrm{pr}_{\mathbf{v}}(P)\| = \sum_{\langle \mathbf{u}(F_i),\mathbf{v}\rangle<0} \|\mathrm{pr}_{\mathbf{v}}(F_i)\|. \tag{3}$$

Từ (2) và (3), ta có

$$\begin{aligned}\langle \sum_i A(F_i)\mathbf{u}(F_i), \mathbf{v}\rangle &= \sum_{\langle \mathbf{u}(F_i),\mathbf{v}\rangle>0} A(F_i)\langle \mathbf{u}(F_i),\mathbf{v}\rangle + \sum_{\langle \mathbf{u}(F_i),\mathbf{v}\rangle<0} A(F_i)\langle \mathbf{u}(F_i),\mathbf{v}\rangle \\ &= \|\mathrm{pr}_{\mathbf{v}}(P)\| - \|\mathrm{pr}_{\mathbf{v}}(P)\| = 0.\end{aligned}$$

Vì $\mathbf{v}$ là vector đơn vị bất kỳ, ta có thể kết luận $\sum_i A(F_i)\mathbf{u}(F_i) = \overrightarrow{0}$. □

Bài tập 3.1. Chứng minh mệnh đề được sử dụng trong chứng minh trên. (Gợi ý: Giả sử đường thẳng $(\mathrm{pr}_{\mathbf{v}})^{-1}(x)$ cắt P theo đoạn thẳng x_-x_+, với vector $\overrightarrow{x_-x_+}$ cùng phương với $\mathbf{v}$. Giả sử $x_- \in F_i$. Vector từ x_- hướng đến x_+ là môt vector hướng vào trong đa giác P. Vì vậy $\langle \overrightarrow{x_-x_+}, \mathbf{u}_i\rangle < 0$.)

Bài tập 3.2. Giả sử P la đa giác lồi, với các đỉnh $p_1, \ldots, v_n$ theo chiều kim đồng hồ và cạnh $F_i = p_ip_{i+1}$. Chứng minh rằng trên đường tròn đơn vị, theo chiều kim đồng hồ bắt đầu từ $\mathbf{u}_1$, ta sẽ lần lượt gặp $\mathbf{u}_2 \ldots, \mathbf{u}_n$.

3.2. Định lý Minkowski 2 chiều phần (b)

Chứng minh. Đánh số lại các vector $\mathbf{u}_1, \ldots, \mathbf{u}_n$ sao cho nếu đi trên đường trơn đơn vị theo chiều kim đồng hồ bắt đầu từ $\mathbf{u}_1$, ta sẽ lần lượt gặp $\mathbf{u}_2 \ldots, \mathbf{u}_n$. Giả sử $\mathbf{v}_i$ là ảnh của $\mathbf{u}_i$ dưới phép quay 90^o cùng chiều kim đồng hồ.

Chọn điểm p_1 bất kỳ. Lần lượt dựng các điểm $p_2, p_3, \ldots, p_n$ sao cho $\overrightarrow{p_ip_{i+1}} = a_i\mathbf{v}_i$ voi $i = 1, \ldots, n-1$. Vì $\sum_{i=1}^n a_i\mathbf{v}_i = \overrightarrow{0}$, ta cũng có $a_n\mathbf{v}_n = \overrightarrow{p_np_1}$. Đa giác P với các đỉnh $p_1, \ldots, p_n$ là đã giác thoả mãn các điệu kết luận của phần (b).

Bài tập 3.3. Chứng minh tính duy nhất của phần (b) định lý Minkowski 2 chiều.

□

Chú ý 3.1. Ta có thể thấy là chứng minh này không thể mở rộng lên cho trường hợp 3 chiều. Khác với trường hợp 2 chiều, trong trường hợp 3 chiều, bản chất của một mặt và bản chất của vector pháp tuyến của nó hoàn toàn khác nhau.

3.3. Định lý Minkowski 3 chiều, phần (a)

Phần (a) khá đơn giản.

Chứng minh. Giả sử $\mathbf{v}$ là một vector đơn vị bất kỳ. Ký hiệu $\mathbf{v}^\perp$ mặt phẳng vuông góc với $\mathbf{v}$ đi qua gốc toạ độ, và $\mathrm{pr}_\mathbf{v}$ là phép chiếu trực giao lên $\mathbf{v}^\perp$. Khi đó $X = \mathrm{pr}_\mathbf{v}(P)$ là một đa giác lồi. Đặt $\mathring{X} = X \setminus \mathrm{pr}(E)$, với E là hợp của các cạnh của P. Dễ dàng thấy rằng diện tích của $\mathrm{pr}_\mathbf{v}(F_i)$ được tính bởi

$$A(\mathrm{pr}_\mathbf{v}(F_i)) = A(F_i)\,|\langle \mathbf{u}(F), \mathbf{u}\rangle|.$$

Lý luận tương tự như trường hợp 2 chiều, ta có

$$\sum_{\langle \mathbf{u}(F_i),\mathbf{v}\rangle>0} A(\mathrm{pr}_\mathbf{v}(F_i)) = A(\mathrm{pr}_\mathbf{v}(P)) = \sum_{\langle \mathbf{u}(F_i),\mathbf{v}\rangle<0} A(\mathrm{pr}_\mathbf{v}(F_i)).$$

Và từ đó,

$$\begin{aligned}\langle \sum_i A(F_i)\mathbf{u}(F_i), \mathbf{v}\rangle &= \sum_{\langle \mathbf{u}(F_i),\mathbf{v}\rangle>0} A(F_i)\langle \mathbf{u}(F_i), \mathbf{v}\rangle + \sum_{\langle \mathbf{u}(F_i),\mathbf{v}\rangle<0} A(F_i)\langle \mathbf{u}(F_i), \mathbf{v}\rangle \\ &= A(\mathrm{pr}_\mathbf{v}(P)) - A(\mathrm{pr}_\mathbf{v}(P)) = 0.\end{aligned}$$

Vì $\mathbf{v}$ là vector đơn vị bất kỳ, ta có thể kết luận $\sum_i A(F_i)\mathbf{u}(F_i) = \overrightarrow{0}$. □

Phần (a) cũng có một chứng minh "vật lý" như sau (từ blog của Đàm Thanh Sơn). Mặc dù không được chặt chẽ về mặt toán học, nhưng chứng minh này cũng chỉ ra một số ý tưởng thú vị. Ta hãy nhúng đa diện P vào một chất lỏng đồng nhất. Áp lực của chất lỏng lên mỗi mặt F_i bằng $kA(F_i)\mathbf{u}(F_i)$, với k là một hằng số khác 0 không phụ thuộc i. Vì P sẽ đứng bất động trong chất lỏng (điều này không giải thích toán học được), tổng tất các lực áp lên nó phải bằng $\vec{0}$. Vì vậy $\sum_i A(F_i)\mathbf{u}(F_i) = \overrightarrow{0}$.

4. Chứng minh định lý Minkowski, phần II

Phần (b) là phần hay nhất trong định lý Minkowski. Các chứng minh phần (b) của định lý Minkowski với số chiều ≥ 3 đều sử dụng toán cao cấp. Có lẽ chính vì vậy mà mặc dù được phát biểu dưới dạng sơ cấp, định lý Minkowski ít được biết đến trong toán sơ cấp. Ở đây ta chỉ chứng minh định lý Minkowski cho trường hợp $n = 4$, trường hợp này chỉ cần sử dụng kiến thức của toán phổ thông. Với một ít kiến thức về giải tích nhiều biến, bạn có thể hiểu được chứng minh định lý Minskowski tổng quát, xem mục 4.4.

4.1. Tập hợp các đa giác có vector pháp tuyến cho trước

Giả sử $\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3, \mathbf{u}_4 \in \mathbb{R}^3$ và các số dương a_1, a_2, a_3, a_4 thoả mãn các điều kiện của phần (b) định lý Minkowski 3 chiều. Từ giả thiết, ta có thể thấy rằng

$$\mathbf{u}_2, \mathbf{u}_3, \mathbf{u}_4 \text{ không cùng trên một mặt phẳng.} \tag{4}$$

Bài tập 4.1. Hãy chứng minh rằng $\mathbf{u}_2, \mathbf{u}_3, \mathbf{u}_4$ là độc lập tuyến tính, tức là nếu các số thực k_2, k_3, k_4 thỏa $k_2\mathbf{u}_2 + k_3\mathbf{u}_3 + k_3\mathbf{u}_4 = \vec{0}$ thì $k_1 = k_2 = k_3 = 0$.

Giả sử P là một đã diễn thoa điều kiện

$$\text{các vector pháp tuyến mặt của } P \text{ là } \mathbf{u}_1, \ldots, \mathbf{u}_4. \tag{5}$$

Khi đó tồn tại các số thực z_1, z_2, z_3, z_4 sao cho

$$P = \{\mathbf{x} \in \mathbb{R}^3 \mid \langle \mathbf{x}, \mathbf{u}_i \rangle \leq z_i \; \forall i = 1, 2, 3, 4\}. \tag{6}$$

Các số $z_1, \ldots, z_4$ xác định hoàn toàn đa diện P. Tuy nhiên không phải bất cứ 4 số thực $z_1, \ldots, z_4$ cũng xác định một đa diện theo (6), vì tập hợp định nghĩa bởi vế phải của (6) có thể không phải là đa diện, thậm chí có thể rỗng.

Bài tập 4.2. (a)Giả sử P được xác định bởi $(z_1, \ldots, z_4)$ theo (6), và $\mathbf{v} \in \mathbb{R}^3$. Chứng minh rằng $\mathbf{v} + P$ được xác định bởi $z_1', \ldots, z_4'$, định nghĩa bởi $z_i' = z_i + \langle \mathbf{v}, \mathbf{u}_i \rangle$.

(b) Chứng minh rằng $(z_1, \ldots, z_4)$ xác định một đa giác P nếu và chỉ nếu tồn tại $\mathbf{x} \in \mathbb{R}^3$ sao cho

$$\langle \mathbf{x}, \mathbf{u}_i \rangle < z_i \quad \forall i = 1, 2, 3, 4.$$

(c) Chứng minh rằng $z_1 = z_2 = z_3 = z_4 = 1$ xác định một đa diện nào đó thoả mãn (5).

Vì ta sẽ đồng nhất P với $P + \mathbf{v}$, ta sẽ chọn $\mathbf{v}$ sao cho $(z_1, \ldots, z_4)$ là đơn giản, như sau. Từ tính chất (4) dễ dàng suy ra rằng các mặt phẳng qua F_2, F_3, F_4 cắt nhau tại một điểm duy nhất. Ở đây F_i là mặt của P có vector pháp tuyến $\mathbf{u}_i$. Sau một phép tịnh tiến, ta có thể giả sử

$$\text{các mặt phẳng qua } F_2, F_3, F_4 \text{ cắt nhau tại gốc tọa độ } \vec{0}. \tag{7}$$

Giả sử $\mathcal{P}'$ là tập hợp tất cả các đa giác thoả mãn (5) và (7). Với $P \in \mathcal{P}'$, và các số z_1, z_2, z_3, z_4 của (6), ta có $z_2 = z_3 = z_4 = 0$. Vì vậy P được xác định duy nhất bởi $z_1 = z_1(P)$. Ta có ánh xạ $z_1 : \mathcal{P}' \to \mathbb{R}$. Gọi $\mathcal{P} = z_1(\mathcal{P}')$ là ảnh của $\mathcal{P}$.

Bài tập 4.3. Chứng minh $\mathcal{P} = \mathbb{R}_+ = \{x \in \mathbb{R} \mid x > 0\}$, và $z_1 : \mathcal{P}' \to \mathcal{P}$ là song ánh.

Như vậy tập hợp tất cả các đa giác thoả mãn (5) và (7) có thể đồng nhất với tập hợp $\mathcal{P} = \mathbb{R}_+$. Vói $z \in \mathcal{P} = \mathbb{R}_+$, ta ký hiệu $P(z) \in \mathcal{P}'$ là đa giác thoả mãn $z_1 = z, z_2 = z_3 = z_4 = 0$. Khi đó $P : \mathcal{P} \to \mathcal{P}'$ là song ánh.

4.2. Tập hợp các diện tích có thể có

Giả sử $\mathcal{Q}'$ là tập hợp tất cả $(y_1, y_2, y_3, y_4) \in (\mathbb{R}_+)^4$ sao cho

$$y_1\mathbf{u}_1 + y_2\mathbf{u}_2 + y_3\mathbf{u}_3 + y_4\mathbf{u}_4 = \vec{0}.$$

Một vector trong $\mathbb{R}^3$ có 3 thành phần, vì vậy đẳng thức trên cho ra 3 phương trinh tuyến tính với 4 ẩn số y_1, y_2, y_3, y_4. Nói chung tập hợp lời giải sẽ là không gian 1 chiều. Ngoài ra ta còn phải giới hạn $y_i > 0$.

Đặt $\pi : \mathbb{R}^4 \to \mathbb{R}$ là phép chiếu lên toạ độ thứ nhất, tức là

$$\pi(y_1, \ldots, y_4) = y_1.$$

Đặt $\mathcal{Q} = \pi(\mathcal{Q}')$, và ký hiệu $\alpha : \mathcal{Q}' \to \mathcal{Q}$ là giới hạn của π trên tập $\mathcal{Q}'$.

Bài tập 4.4. (a) Chứng minh rằng $\mathcal{Q}'$ thoả mãn: nếu $\mathbf{x}, \mathbf{y} \in \mathcal{Q}'$ và $k \in \mathbb{R}_+$ thì $\mathbf{x} + \mathbf{y} \in \mathcal{Q}'$ va $k\mathbf{x} \in \mathcal{Q}'$.

(b) Sử dụng điều kiện (4), chứng minh rằng α là song ánh.

(b) Chứng minh rằng $\mathcal{Q} = \mathbb{R}_+$.

4.3. Ánh xạ diện tích mặt

Giả sử $\mathbf{z} \in \mathcal{P}$. Đặt $A_i(\mathbf{z})$ là diện tích mặt F_i của đa giác $P(\mathbf{z})$, và $\mathbf{A} : \mathcal{Q} \to \mathbb{R}^4$ là ánh xạ

$$A(\mathbf{z}) = (A_1(\mathbf{z}), \ldots, A_4(\mathbf{z})).$$

Phần (a) của định lý Minkowski chứng minh rằng $\mathbf{A}(\mathcal{P}) \subset \mathcal{Q}'$. Phần (b) của định lý Minkowski 3 chiều tương đương với mệnh đề sau đây mà ta sẽ chứng minh.

Lemma 4.1. *Ánh xạ $\mathbf{A} : \mathcal{P} \to \mathcal{Q}'$ là song ánh.*

Chứng minh. Dễ dàng thấy rằng $P(kz) = kP(z)$ voi moi $k \in \mathbb{R}_+$. Từ đó suy ra rằng

$$\mathbf{A}(kz) = k^2\mathbf{A}(z). \tag{8}$$

Đặt $\mathbf{B} : \mathcal{P} \to \mathcal{Q}$ là composition $\mathbb{R}_+ = \mathcal{P} \xrightarrow{\mathbf{A}} \mathcal{Q}' \xrightarrow{\alpha} \mathcal{Q} = \mathbb{R}_+$. Đẳng thức (8) chứng tỏ rằng

$$\mathbf{B}(kz) = k^2\mathbf{B}(z) \quad \forall z \in \mathbb{R}_+ \ \& \ \forall k \in \mathbb{R}_+.$$

Dễ dàng thấy rằng bất kỳ ánh xạ $\mathbf{B} : \mathbb{R}_+ \to \mathbb{R}_+$ nào thoả mãn điều kiện trên là một song ánh. Vì α là song ánh, ta suy ra $\mathbf{A}$ cũng là song ánh. □

Ta đã kết thúc chứng minh định lý Minkowski 3 chiều cho trường hợp $n = 4$. Trường hợp $n > 4$ được chứng minh tương tự, mặc dù phức tạp hơn, và sử dụng bất đẳng thức Brunn-Minkowski. Độc giả có thể tham khảo [1, 2].

4.4. Sơ lược về trường hợp $n > 4$

Bằng cách đánh số lại, ta có thể giả sử

$$\mathbf{u}_{n-2}, \mathbf{u}_{n-1}, \mathbf{u}_n \text{ không cùng trên một mặt phẳng.} \tag{9}$$

Một đa giác P thỏa điều kiện

$$\text{các vector pháp tuyến mặt của } P \text{ là } \mathbf{u}_1, \ldots, \mathbf{u}_n \tag{10}$$

sẽ được hoàn toàn xác định bởi các số thực $z_1, \ldots, z_n$ sao cho

$$P = \{\mathbf{x} \in \mathbb{R}^3 \mid \langle \mathbf{x}, \mathbf{u}_i \rangle \leq z_i \ \forall i = 1, \ldots, n\}. \tag{11}$$

Tuy nhiên không phải bất cứ n số thực $z_1, \ldots, z_n$ cũng xác định một đa diện theo (11).

Bài tập 4.5. (b) Chứng minh rằng $(z_1, \ldots, z_n)$ xác định một đa giác P nếu và chỉ nếu tồn tại $\mathbf{x} \in \mathbb{R}^3$ sao cho

$$\langle \mathbf{x}, \mathbf{u}_i \rangle < z_i \quad \forall i = 1, \ldots, n.$$

(c) Chứng minh rằng $z_1 = \cdots = z_n = 1$ xác định một đa diện nào đó thỏa mãn (10).

Tính chất (9) suy ra rằng các mặt phẳng qua F_{n-2}, F_{n-1}, F_n cắt tại một điểm duy nhất. Sau một phép tịnh tiến, ta có thể giả sử

$$\text{các mặt phẳng qua } F_{n-2}, F_{n-1}, F_n \text{ cắt nhau tại gốc tọa độ } \vec{0}. \tag{12}$$

Giả sử $\mathcal{P}'$ là tập hợp tất cả các đa giác thỏa mãn (10) và (12). Voi $P \in \mathcal{P}'$, ta có $z_{n-2} = z_{n-1} = z_n = 0$, vì vậy P được xác định duy nhất bởi $z_1, \ldots, z_m$. O day $m = n - 3$. Đặt $\mathcal{P} \subset \mathbb{R}^m$ là tập hợp tất cả $\mathbf{z} = (z_1, \ldots, z_m)$ sao cho $(\mathbf{z}, 0, 0, 0)$ xác sinh một đa giác $P \in \mathcal{P}'$. Ánh xạ $\mathcal{P} \to \mathcal{P}'$, $\mathbf{z} \to P(\mathbf{z})$ là song ánh.

Bài tập 4.6. (a) Chứng minh $\mathcal{P}$ là một cone lồi, tức là nếu $\mathbf{z}, \mathbf{z}' \in \mathcal{P}$ và $k \in \mathbb{R}_+$ thì $k\mathbf{z} \in \mathcal{P}$ và $\mathbf{z} + \mathbf{z}' \in \mathcal{P}$.

(b) Chứng minh $\mathcal{P}$ là một tập hợp mở, tức là nếu $\mathbf{z} \in \mathcal{P}$ thì tồn tại $\varepsilon > 0$ sao cho nếu $\|\mathbf{z}' - \mathbf{z}\| < \varepsilon$ thì $\mathbf{z}' \in \mathcal{P}$.

Giả sử $\mathcal{Q}'$ là tập hợp tất cả $(y_1, \ldots, y_n) \in (\mathbb{R}_+)^n$ sao cho $\sum_{i=1}^n y_i \mathbf{u}_i = \vec{0}$. Đặt $\pi : \mathbb{R}^n \to \mathbb{R}^m$ là phép chiếu lên m tọa độ đầu tiên. Đặt $\mathcal{Q} = \pi(\mathcal{Q}')$, và ký hiệu $\alpha : \mathcal{Q}' \to \mathcal{Q}$ là giới hạn của π trên tập $\mathcal{Q}'$.

Bài tập 4.7. (a) Chứng minh rằng $\mathcal{Q}'$ là mot cone loi.

(b) Sử dụng điều kiện (4), chứng minh rằng α la song ánh.

(b) Chứng minh rang $\mathcal{Q}$ là một cone lồi mở trong $\mathbb{R}^m$.

Với $\mathbf{z} \in \mathcal{P}$ dat $A_i(\mathbf{z})$ la diện tích mặt F_i của đa giác $P(\mathbf{z})$, và $\mathbf{A} : \mathcal{Q} \to \mathbb{R}^n$ là ánh xạ

$$A(\mathbf{z}) = (A_1(\mathbf{z}), \ldots, A_n(\mathbf{z})).$$

Đăt $\mathbf{B} = \alpha \circ \mathbf{A}$. Phần (a) của định lý Minkowski chứng minh rằng $\mathbf{A}(\mathcal{P}) \subset \mathcal{Q}$. Phần (b) của định lý Minkowski 3 chiều tương đương với mệnh đề sau

Lemma 4.2. *Ánh xạ $\mathbf{B} : \mathcal{P} \to \mathcal{Q}$ là song ánh.*

Như vậy ta phải chứng minh với mọi $\mathbf{a} \in \mathcal{Q}$ tồn tại duy nhất $\mathbf{z} \in \mathcal{P}$ sao cho $\mathbf{B}(\mathbf{z}) = \mathbf{a}$. Bài toán tìm $\mathbf{z}$ sẽ đuược đưa về bài toán tìm cực trị của một hàm số lồi và trơn, và lời giải duy nhất của nó được khẳng định bởi đính lồi và trơn của hàm số. em chi tiết tại [2]. Alexandrov có một chứng minh thú vị khác, bằng cách trước hết chứng minh tính duy nhát, rồi dùng tính chât tôpô của miền xác định và miền giá trị của $\mathbf{B}$ để chứng minh tính tồn tại. Xem chi tiết tại [1].

Tài liệu

[1] A. D. Alexandrov, *Convex polyhedra* (translation of the 1950 Russian original), Springer, Berlin, 2005.

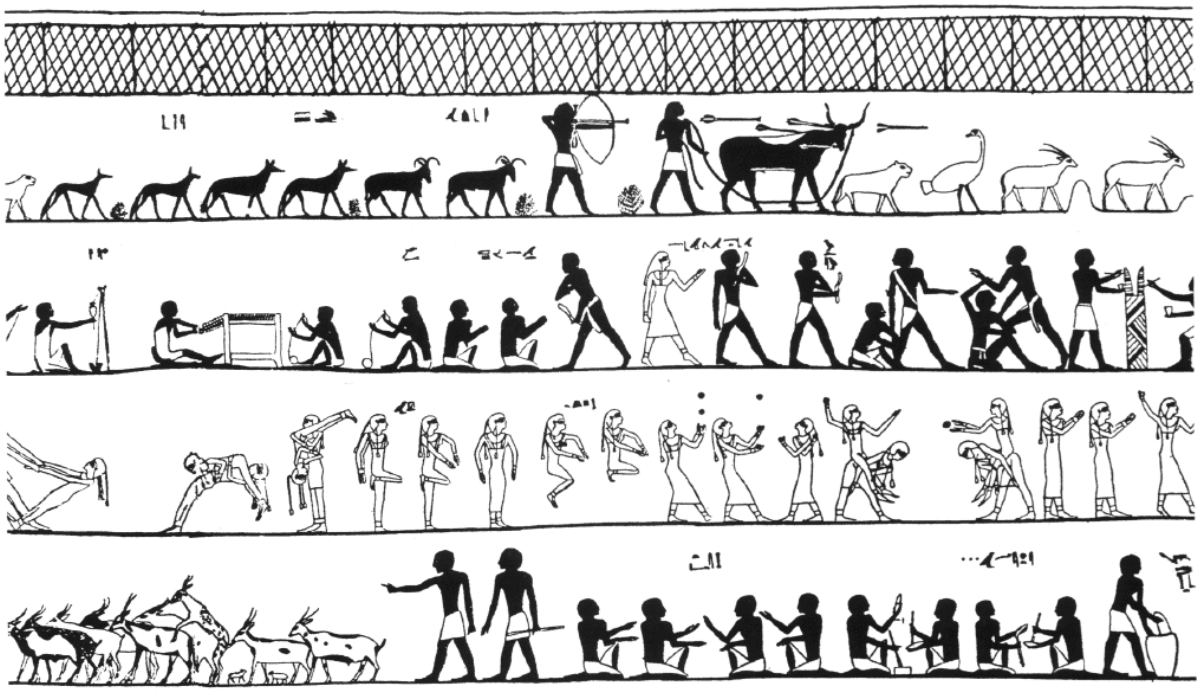
[2] I. Pak, *Lectures on Discrete and Polyhedral Geometry*, online at http://www.math.ucla.edu/~pak/geompol8.pdf

TOÁN HỌC VÀ NGHỆ THUẬT TUNG HỨNG

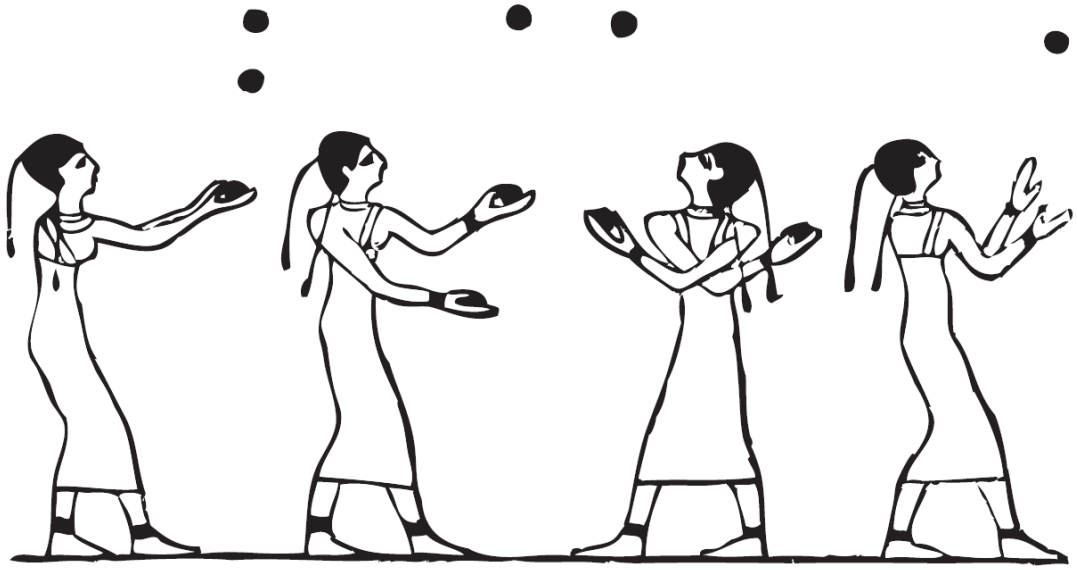
Nguyễn Hùng Sơn

GIỚI THIỆU

Tung hứng là một bộ môn nghệ thuật cổ xưa, dường như luôn đồng hành với lịch sử của nhân loại. Nhiều bản vẽ mô tả những người phụ nữ đang tung hứng được tìm thấy trong một ngôi mộ của Ai Cập có niên đại vào khoảng thế kỷ thứ hai mươi trước công nguyên. Chỉ cần một vài viên đá và một chút luyện tập là bạn đã có thể tung hứng. Vì vậy không có gì đáng ngạc nhiên khi loài người quan tâm đến môn nghệ thuật này từ rất lâu rồi.



Tuy nhiên, chỉ mới gần đây khía cạnh toán học của tung hứng mới bắt đầu được quan tâm một cách nghiêm túc. Các nghiên cứu toán học về các mô hình tung hứng được tiến hành lần đầu tiên cùng một lúc vào những năm 80 của thế kỷ XX tại vài trường đại học, trong đó có Đại học California tại Santa Cruz, Caltech và Đại học Cambridge. Trong bài báo nhỏ này chúng ta sẽ liệt kê một cách ngắn gọn về các kết quả mà các nhà toán học có thể giúp các nghệ sĩ xiếc trong việc tạo ra các mô hình tung hứng và các lợi ích do sự hợp tác liên ngành này có thể đem lại cho các nhà toán học.



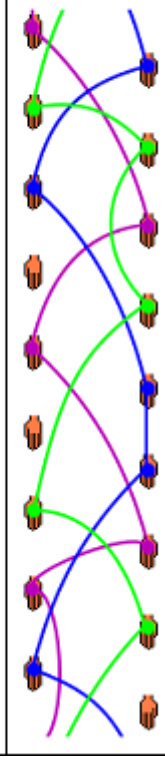
Hình 1: Những hình ảnh cổ nhất về tung hứng cách đây khoảng 4000 năm.

Bước đầu tiên là tạo ra các mô hình toán học cho các kỹ thuật tung hứng để có thể nói về chúng một cách chính xác. Trong các mô hình đơn giản nhất, ta giả sử thời gian là rời rạc (chính xác hơn, thời gian là một chuỗi các thời điểm $1, 2, 3, \ldots$), và rằng nghệ sĩ tung hứng có hai tay, mỗi tay chỉ có thể giữ được nhiều nhất một vật trong mỗi thời điểm. Không mất tính tổng quát ta giả sử các vật dùng để tung hứng là các quả bóng. Các tay thay đổi nhau liên tục, có nghĩa là một tay sẽ luôn bắt (hứng) và tung bóng ở các thời điểm lẻ: $1, 3, 5, ...$ (ta gọi đó là tay lẻ), còn tay thứ hai (tay chẵn) thì luôn tung và hứng ở các thời điểm chẵn: $2, 4, 6, ...$

Và bây giờ sẽ là vấn đề thú vị hơn: làm thế nào để mô hình hóa các cách tung bóng khác nhau và đồng thời cho nhiều quả bóng khác nhau? Phương pháp thường dùng nhất là phân loại các cách tung bóng theo thời gian (số khoảnh khắc) mà quả bóng bay trên không. Điều đó có nghĩa rằng nếu tại thời điểm i ta tung bóng theo kiểu t (với t là một số tự nhiên nào đó) thì bóng sẽ rơi (vào một trong hai tay) vào thời điểm $i + t$. Lưu ý rằng với cách ký hiệu này, nếu bóng được tung theo kiểu chẵn bằng một trong hai tay thì nó sẽ rơi vào đúng tay đó, còn theo kiểu lẻ thì bóng sẽ rơi vào tay thứ hai. Ta cũng ký hiệu kiểu 0 cho trường hợp không tung bóng, tức là một trong hai tay được gọi là tung bóng theo kiểu 0 tại thời điểm i nếu tay đó không có bóng tại thời điểm này.

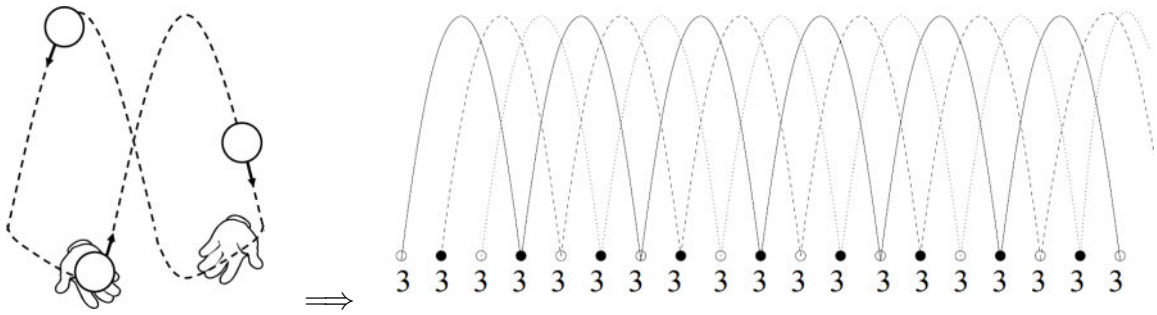
Hình 2 là ví dụ của một dãy các cách tung hứng bóng theo trình tự thời gian. Trong ví dụ này người nghệ sĩ tung hứng dùng ba quả bóng được đánh dấu bằng ba mầu. Ngoài ra trên hình vẽ còn có một số thông tin bổ sung (về cấu hình) và sẽ được giải thích sau.

Hoạt động của người nghệ sĩ tung hứng trong ví dụ này có thể được mô tả ở dạng một dãy các cách tung bóng trong từng thời điểm, đó là $\langle 5, 3, 1, 4, 5, 3, 0, 5, 5, 2, 0, 5, 3, 1, 4, 5, 3, 0\rangle$. Cách ký hiệu này được gọi là phương pháp dãy hoán đổi (tiếng Anh là *siteswap model*). Tuy nhiên, trong thực tế các nghệ sĩ tung hứng thường quan tâm đến các *mô hình tung hứng* (tiếng Anh gọi là juggling pattern) hơn là cái dãy dài dằng dặc như ở trên. Tốt nhất là nếu ta tìm được các dãy tuần hoàn để một dãy con hữu hạn có thể lặp đi lặp lại nhiều lần cho đến vô cùng. Ví dụ: một trong

Thời điểm		Kiểu tung	Cấu hình
1		5	xx--x
2		3	x-xx-
3		1	xxx--
4		4	xx-x-
5		5	x-x-x
6		3	-xxx-
7		0	xxx--
8		5	xx--x
9		5	x--xx
10		2	-xxx-
11		0	xxx--
12		5	xx--x
13		3	x-xx-
14		1	xxx--
15		4	xx-x-
16		5	x-x-x
17		3	-xxx-
18		0	xxx--

Hình 2: Ví dụ một dãy các cách tung hứng bằng hai tay

các mô hình phổ biến nhất mà mọi người thường bắt đầu học là tung hứng 3 quả bóng theo kiểu *thác nước*. Kiểu tung hứng này tương đương với dãy $\langle 3, 3, 3, 3, 3, 3, 3 \ldots \rangle$.



Để tránh trùng lặp các thông tin vô ích, ta thường ký hiệu các dãy tuần hoàn bằng các thông tin trong một chu kỳ của nó. Như vậy mô hình tung hứng kiểu thác nước là dãy tuần hoàn (3).

Tới đây ta có thể thấy hàng loạt các vấn đề toán học được đặt ra. Phải chăng tất cả các dãy hoán đổi đều khả thi (hợp thức)? Số quả bóng ảnh hưởng như thế nào đến mô hình? Tồn tại bao nhiêu mô hình tung hứng nếu ta cố định một số yếu tố như số lượng quả bóng hoặc số lần tung bóng?

Trước khi tìm hiểu các câu hỏi trên ta hãy làm quen với một số tính chất của mô hình tung hứng ở dạng dãy hoán đổi (siteswap patterns):

Định nghĩa 1 *Gọi* $\mathbf{P} = \langle t_0 \cdots t_{k-1} \rangle$ *là dãy hoán đổi với độ dài* k*. Dãy* $\mathbf{P}$ *được gọi là* **dãy tung hứng** *khi và chỉ khi hàm số*

$$\sigma : \{0, \ldots, k-1\} \to \{0, \ldots, k-1\} \text{ xác định bởi } \sigma(i) = i + t_i \mod k$$

là một hoán vị của tập $\{0, \ldots, k-1\}$.

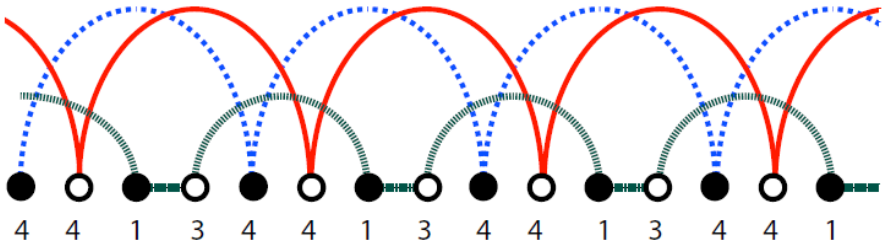
Định nghĩa trên chỉ muốn nói rằng trong dãy tung hứng là dãy hoán đổi của quá trình tung hứng thực sự. Khi tung hứng, không tay nào được bắt hai quả bóng cùng một lúc, điều đó co nghĩa rằng các quả bóng đều phải rơi vào một trong hai tay ở các thời điểm khác nhau. Dễ thấy mọi dãy có độ dài $k = 1$ đều là dãy tung hứng và mọi dãy tuần hoàn dạng (n) cũng là dãy tung hứng tương ứng với tung hứng kiểu thác nước dùng n quả bóng.

Bổ đề 1 (về giá trị trung bình) *Trong mọi dãy hoán đổi tung hứng tuần hoàn* $\mathbf{a} = (a_0, a_1, ..., a_{d-1})$ *có độ dài* d*, giá trị trung bình của dãy* $\overline{\mathbf{a}} = \frac{a_0 + a_1 + \ldots + a_{d-1}}{d}$ *là một số tự nhiên và bằng đúng số quả bóng được dùng để tung hứng.*

Xin bỏ qua phần chứng minh bổ đề 1 và mong bạn đọc yêu thích toán học coi đây là một bài tập thú vị.

Bổ đề trên đây có thể coi như là điều kiện cần để kiểm tra dãy hoán đổi có phải là dãy tung hứng khay không: nếu giá trị trung bình của dãy không phải là số nguyên thì đó không phải là dãy tung hứng. Ví dụ:

- Dãy $(5, 2, 1)$ có giá trị trung bình bằng $\frac{8}{3}$, vì vậy đây không phải là dãy tung hứng.
- Dãy $(3, 2, 1)$ có giá trị trung bình bằng 2 nên có thể là dãy tung hứng cho 2 quả bóng. Tuy nhiên $\sigma(1) = \sigma(2) = \sigma(3) = 0$, vì vậy theo định nghĩa đây không phải là dãy tung hứng.
- Các dãy $(4, 4, 1)$, $(5, 3, 1)$, $(4, 4, 1, 3)$ $(5, 5, 5, 0, 0)$ là các dãy tung hứng cho 3 quả bóng; còn $(6, 4, 5, 1)$, $(7, 3, 3, 3)$, $(7, 1)$ là các dãy tung hứng cho 4 quả bóng. Hy vọng sau khi đọc xong bài viết này, bạn đọc có thể dễ dàng kiểm tra các thông tin trên.



Hình 3: Ví dụ của dãy tung hứng tuần hoàn $(4, 4, 1, 3)$.

Benoît Guerville đã phát hiện và chứng minh kết quả tuyệt vời liên quan đến điều kiện đủ xác định dãy tung hứng như sau:

Định lý 2 (về tái cơ cấu) *Nếu dãy số tự nhiên có giá trị trung bình cũng là số nguyên thì ta có thể hoán vị dãy đó thành một dãy tung hứng.*

Quay lại ví dụ trên Hình 2. Tại mỗi thời điểm ta hãy quan sát "vị trí" của quả bóng, tức là thời gian từ thời điểm đó cho đến khi quả bóng rơi vào một trong hai tay. Vì không tay nào được bắt hai quả bóng cùng một lúc nên tại một thời điểm tất cả các quả bóng phải ở các vị trí khác nhau. Ta có thể nói rằng bóng được tung lên vị trí k thay vì nói rằng bóng được tung theo kiểu k.

Cấu hình tại một thời điểm bất kỳ là một dãy $s_0 s_1 s_2 \dots$ gồm các ký hiệu $\times$ và $-$. Ký hiệu $s_k = \times$ nếu vị trí của một trong các quả bóng bằng k, còn $s_k = -$ khi không quả bóng nào ở vị trí này. Chiều dài của cấu hình thường là số tự nhiên hữu hạn tương ứng với vị trí cao nhất của các quả bóng. Trong ví dụ ở Hình 2 cấu hình tại mọi thời điểm đều có chiều dài bằng 5 (cột cuối cùng).

Vị trí đầu tiên (ký hiệu s_0) của cấu hình mô tả tình trạng của bàn tay chủ động, tức là tay lẻ ở thời điểm lẻ hoặc tay chẵn ở thời điểm chẵn. Điều đó có nghĩa là nếu ký hiệu đầu tiên của cấu hình là $-$ thì bàn tay tương ứng không có bóng và tiếp theo tay đó sẽ tung bóng theo kiểu 0. Còn nếu ký hiệu đầu tiên là $\times$ thì quả bóng trong tay sẽ phải được tung lên một trong các vị trí có ký hiệu $\times$ (vị trí còn trống). Lưu ý: ta luôn có thể tung bóng lên vị trí cao nhất (tại sao?).

Nếu cấu hình tại thời điểm i là $\mathcal{C}_i = s_0 s_1 s_2 \dots s_{d-1}$ và $s_0 = -$ thì cấu hình tiếp theo sẽ là $\mathcal{C}_{i+1} = s_1 s_2 \dots s_{d-1} -$. Hai cấu hình được nối với nhau bằng mũi tên có trọng số bằng 0:

$$\mathcal{C}_i = -s_1 s_2 \dots s_{d-1} \xrightarrow{0} \mathcal{C}_{i+1} = s_1 s_2 \dots s_{d-1} -$$

Còn nếu $s_0 = \times$ thì các cấu hình tại thời điểm tiếp theo sẽ được hình thành như sau:

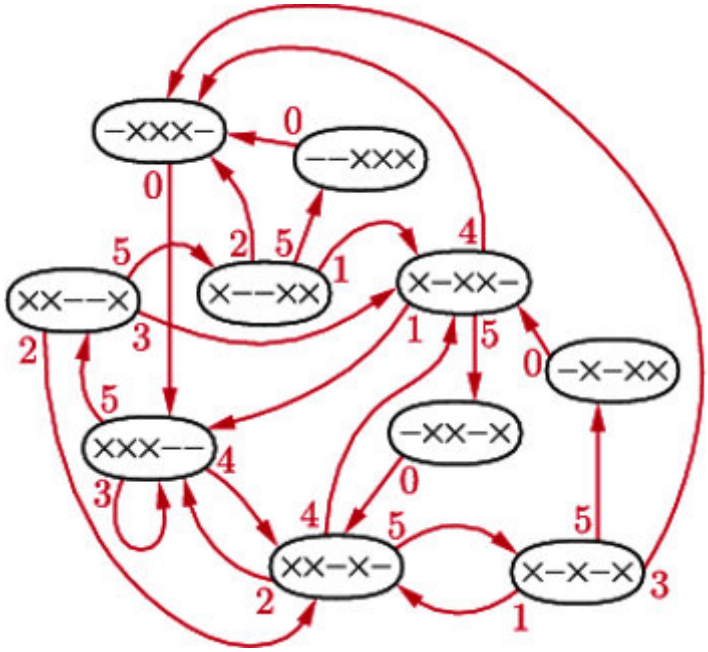
1. Kéo dài cấu hình $\mathcal{C}_i$ thành $\mathcal{C}'_i = s_0 s_1 s_2 \dots s_{d-1} s_d$ với $s_d = -$;
2. Nếu $s_h = -$ và quả bóng được tung lên vị trí h thì ta sẽ đổi $s_h = \times$;
3. Xóa s_0 từ $\mathcal{C}'_i$. Cấu hình tại thời điểm $i+1$ sẽ là $\mathcal{C}_{i+1} = s_1 s_2 \dots s_{d-1} s_d$
4. Ta nối hai cấu hình bằng mũi tên có trọng số bằng h:

$$\mathcal{C}_i \xrightarrow{h} \mathcal{C}_{i+1}$$

Bằng cách này ta có thể thiết lập biểu đồ chuyển dịch giữa các cấu hình. Hình 4 là ví dụ minh họa của biểu đồ hoán chuyển giữa các cấu hình khi tung hứng 3 quả bóng và vị trí cao nhất là 5. Biểu đồ này, thực chất là *đồ thị có hướng và có trọng số*.

Sử dụng các cấu hình ta có thể dễ dàng kiểm tra xem một dãy hoán đổi có là dãy tung hứng hay không. Dễ dàng nhận thấy rằng mỗi một dãy tung hứng tương ứng với một *dây chuyền* trong biểu đổ. Hơn nữa dãy tung hứng tuần hoàn tương ứng với một *chu trình* trong biểu đồ. Cũng có thể sử dụng biểu đồ này để tạo ra các bài biểu diễn tung hứng mới và kỳ lạ. Nhiều nghệ sĩ (ví dụ ở công ty Gandini Juggling) đã sử dụng mô hình này để thiết kế các chương trình biểu diễn của mình.

Bổ đề 1 có thể tổng quát hóa như sau:



Hình 4: Biểu đồ dịch chuyển giữa các cấu hình.

Định lý 3 (tổng quát về giá trị trung bình) *Nếu* $\mathbf{a} = \langle a_0, a_1, a_2, \ldots \rangle$ *là một dãy tung hứng có độ cao hữu hạn thì giới hạn*

$$\lim_{|I|\to\infty} \frac{\sum\limits_{i\in I} a_i}{|I|}$$

hội tụ và bằng số quả bóng, ở đây giới hạn được xác định cho tập hợp tất cả các khoảng $I = \{b, b+1, \ldots, c\} \subset \mathbb{Z}$ *và* $|I| = c - b + 1$ *là số số tự nhiên trong khoảng* I*.*

Để ý rằng các kết quả toán học trong bài báo này không sử dụng đến giả thiết về hai bàn tay. Các kết quả trên đây vẫn đúng cho trường hợp tung hứng dùng nhiều *"chi"* hơn, ví dụ: 2 chân, 2 tay, đầu, nhiều người. Nghiên cứu về các dãy hoán chuyển vẫn là vấn đề thời sự và được tổng quát hóa cho nhiều trường hợp như:

- Thời gian đồng bộ: nhiều chi cùng bắt bóng và tung bóng trong cùng một thời điểm;
- Multiplexes: một tay có thể tung nhiều quả bóng trong cùng một thời điểm.

Các nghiên cứu cơ bản về đề tài này cũng được tiến hành và khá nhiều bài báo đã được đăng, chủ yếu là về các vấn đề tổ hợp liên quan đến mô hình tung hứng. Một điều thú vị là một số kết quả liên quan đến tung hứng lại có thể sử dụng trong các ngành khác trong toán học. Một số nghiên cứu, kể cả một số luận án tiến sĩ (ví dụ như "Combinatorial aspects of juggling" của Anthony Mays) đã phát hiên rất nhiều sự liên hệ giữa các dãy hoán đổi (siteswap) với một số lý thuyết tiên tiến nhất trong toán học như tính toán chuỗi Poincare cho nhóm affine của Weyl A_{d-1} hoặc để chứng minh định lý liên quan đến số q-Stirling. Trước đó, nhiều người cho rằng các lý thuyết này là các mô hình toán học tưởng tượng, không thực dụng.

Không có lý thuyết vô dụng trong toán học: sự liên kết giữa các kết quả toán học và cuộc sống thường xuất hiện một cách tình cờ trong các lĩnh vực mà bản thân các nhà toán học cũng không ngờ tới.

Tài liệu

[1] Tạp chí 'Delta' của Ba lan. Số 9. 2014

[2] Beek, Peter J. & Arthur Lewbel (1995), 'The Science of Juggling', Scientific American, Vol. 273, No 5, November 1995, p92–97.

[3] Beever, Ben (2002), 'Siteswap Ben's guide to juggling patterns', available at: www.jugglingdb.com/compendium/geek/notation/siteswap/bensguide.html.

[4] Buhler, Joe, David Eisenbud, Ron Graham & Colin Wright (1994), 'Juggling drops and descents', The American Mathematical Monthly, Vol. 101, No. 6, June–July 1994, p507–519.

[5] Cardinal, Jean, Steve Kremer & Stefan Langerman (2006), 'Juggling with pattern matching', Theory of Computing Systems, 39(3), June 2006, p425– 437.

[6] Carstens, Ed (1992), 'The mathematics of juggling', online publication, available at: www.juggling.org/papers/carstens/.

[7] Polster, Burkard (2003), 'The mathematical of juggling'. Springer-Verlag, New York.

[8] Shannon Claude E. (1980), 'Scientific Aspects of Juggling'. In N.J.A. Sloane and A. D. Wyner (eds) (1993) Claude Elwood Shannon: Collected Papers. IEEE Press.

[9] Anthony Mays (2006), 'Combinatorial aspects of juggling'. Ph.D Thesis at University of Melbourne.

HỆ MẬT MÃ KHÓA CÔNG KHAI DỰA TRÊN ĐƯỜNG CONG ELLIPTIC - MỘT SỐ ỨNG DỤNG

Đặng Minh Tuấn (Vietkey)

TÓM TẮT

Ở Epsilon số 9, chúng tôi đã giới thiệu tổng quan về hệ mật mã khóa công khai dựa trên đường cong Elliptic qua phần đầu của chuyên đề có cùng tên gọi của tác giả Đặng Minh Tuấn. Trong số này, Epsilon trân trọng giới thiệu phần tiếp theo (và cũng là phần kết) của loạt chuyên đề thông qua các ứng dụng của hệ mật mã khóa công khai dựa trên đường cong Elliptic.

1. Bài toán Logarithm rời rạc

Định nghĩa 1.1. Bài toán Logarithm rời rạc trên đường cong Elliptic (ECDLP): *Cho đường cong E trên trường hữu hạn $\mathbb{F}_q$, điểm $P \in E(\mathbb{F}_q)$ với bậc n ($nP = \mathcal{O} = \infty$) và điểm $Q \in E(\mathbb{F}_q)$, tìm số nguyên $k \in [0, n-1]$ sao cho $Q = kP$. Số nguyên k được gọi là Logarithm rời rạc của Q với cơ sở P, và thường được viết là $k = \log_P Q$.*

Bất kỳ một hệ mật khóa công khai nào cũng phải sử dụng một bài toán khó để xây dựng hàm một chiều. Ý nghĩa một chiều ở đây có nghĩa là tính thuận thì dễ (thuật toán giải trong thời gian đa thức) và tính ngược thì khó (thuật toán giải với thời gian không phải là đa thức - thường là hàm mũ hoặc nửa mũ). Các tham số của Hệ mật dựa trên đường cong Elliptic (ECC) cần phải được lựa chọn cẩn thận để tránh được các tấn công đối với bài toán ECDLP. Thuật toán vét cạn để giải bài toán ECDLP là lần lượt tính thử các điểm $P, 2P, 3P, ...$ cho đến khi điểm mới tính được đúng bằng điểm Q. Trong trường hợp xấu nhất sẽ phải cần đến n bước thử, trung bình thường là $n/2$ là đạt được điểm Q, do đó cần phải chọn n đủ lớn để bài toán vét cạn là không khả thi ($n \geq 2^{160}$).

Thuật toán tốt nhất hiện nay để tấn công bài toán ECDLP là sự kết hợp của thuật toán Pohlih-Hellman và Pollard's rho, thuật toán này có thời gian tính là $O(\sqrt{p})$, với p là ước số nguyên tố lớn nhất của n do đó phải chọn số n sao cho nó chia hết số nguyên tố p lớn nhất có $\sqrt{p}$ đủ lớn để giải bài toán này là không khả thi.

Trong phần tiếp theo, một số phương pháp tấn công bài toán Logarithm rời rạc sẽ được trình bày, đa số các phương pháp này có thể áp dụng được cho một nhóm bất kỳ. Chi tiết có thể tham khảo trong [3, 8, 21].

Cho G là nhóm các điểm trên đường cong E. $P, Q \in G$ là các điểm trên đường cong E, chúng ta cần giải bài toán $kP = Q$, N là bậc của G.

1.1. Phương pháp bước nhỏ, bước lớn

Phương pháp này do Shanks đề xuất và được H. Cohen mô tả trong [22].

Thuật toán 1 Phương pháp bước nhỏ, bước lớn

1: Chọn $m \geq \sqrt{N}$ và tính mP.
2: Tính và lưu trữ danh sách iP với $0 \leq i < m$
3: Tính $Q - jmP$ với $j = 0, 1, \ldots, m-1$
4: **if** $iP = Q - jmP$ **then**
5: $\quad k = i + jm(\mod N)$
6: **end if**
7: Quay về bước 3

Dễ dàng nhận thấy $Q = iP + jmP$ hay $Q = (i + jm)P$ từ đó $k = i + jm$. Điểm iP được tính bằng cách cộng thêm P vào $(i-1)P$ và giá trị này được gọi là bước nhỏ. $Q - jmP$ được tính bằng cách cộng thêm mP vào $Q - (j-1)mP$ và giá trị này được gọi là bước lớn.

1.2. Phương pháp Pollard's ρ và λ

Phương pháp này do Pollard đề xuất trong [23].

Định nghĩa hàm $f : G \to G$ một cách ngẫu nhiên $P_{i+1} = f(P_i)$ với P_0 cũng được chọn một cách ngẫu nhiên. Bởi vì G là tập hữu hạn do đó sẽ có các chỉ số $i_0 < j_0$ mà $P_{i_0} = P_{j_0}$, từ đó ta có:

$$P_{i_0+1} = f(P_{i_0}) = f(P_{j_0}) = P_{j_0+1}$$

Tương tự sẽ có $P_{i_0+l} = P_{j_0+l}$ với $l \geq 0$, từ đó chuỗi P_i là chuỗi tuần hoàn với chu kỳ là $j_0 - i_0$. Hàm biểu diễn chuỗi P_i thường giống chữ cái Hi Lạp ρ và đó là lý do tại sao phương pháp này có tên là phương pháp ρ.

Hàm f được chọn như sau: Chia tập G thành s tập con không trùng nhau $S_1, S_2, \ldots, S_s$ có kích thước tương đương nhau, s thường được chọn là 20, chọn $2s$ số ngẫu nhiên $a_i, b_i \mod N$. Đặt:

$$M_i = a_i P + b_i Q$$

Và định nghĩa:

$$f(g) = g + M_i, \quad g \in S_i$$

Biểu diễn P_j dưới dạng $P_j = u_j P + v_j Q$, khi $P_{i_0} = P_{j_0}$ ta có:

$$\begin{aligned} u_{j_0} P + v_{j_0} Q &= u_{i_0} P + v_{i_0} Q \\ (u_{i_0} - u_{j_0}) P &= (v_{j_0} - vx`_{j_0}) Q \\ k &= (v_{j_0} - vx`_{j_0})_1 (u_{i_0} - u_{j_0}) \pmod N \end{aligned}$$

Phương pháp này cũng tương tự như phương pháp trên cần $\sqrt{N}$ bước, tuy nhiên không gian lưu trữ sẽ nhỏ hơn.

1.3. Phương pháp Pohlig-Hellman

Pohlig và Hellman đề xuất phương pháp này trong [24].

Nếu có thể phân tích bậc N của G thành các thừa số nguyên tố thì có thể viết:

$$N = \prod_i q_i^{e_i}$$

Ý tưởng của phương pháp này là tìm $k \pmod{q_i^{e_i}}$ với mỗi i, sau đó áp dụng định lý đồng dư Trung Hoa để tính $k \pmod N$. Coi q là số nguyên tố và q^e là lũy thừa e của q được chia hết bởi N, viết k dưới dạng sau:

$$k = k_0 + k_1 q + k_2 q^2 + \cdots, \quad 0 \le k_i < q$$

Lý giải thuật toán 2 như sau:

$$\begin{aligned} \frac{N}{q} Q &= \frac{N}{q} \left(k_0 + k_1 q + \cdots\right) P \\ &= k_0 \frac{N}{q} P + \left(k_1 + k_2 q + \cdots\right) NP = k_0 \frac{N}{q} P \end{aligned}$$

Bởi vì $NP = \infty$ và từ đây có thể tìm được k_0. Tiếp theo:

$$\begin{aligned} Q_1 = Q - k_0 P &= \left(k_1 q + k_2 q^2 + \cdots\right) P \\ \frac{N}{q^2} Q_1 &= \frac{N}{q} \left(k_1 + k_2 q + \cdots\right) P \\ &= k_1 \frac{N}{q} P + \left(k_2 + k_3 q + \cdots\right) NP = k_1 \frac{N}{q} P \end{aligned}$$

Từ đó tìm được k_1, tương tự như vậy chúng ta sẽ tìm được $k_2, k_3 \ldots$ Thuật toán sẽ dừng khi $e = r + 1$, khi đó N/q^{e+1} không còn là số nguyên nữa và chúng ta không thể nhân Q_e với một số hữu tỷ.

Thuật toán 2 Phương pháp Pohlig-Hellman

1: Tính $T = \left\{ j \left(\frac{N}{q} P \right) \right\} \mid \quad 0 \leq j \leq q-1$.
2: Tính $\frac{N}{q} Q$. Đó là phần tử $k_0 \left(\frac{N}{q} P \right)$ của T.
3: **if** $e = 1$ **then**
4: Nhảy đến bước 15.
5: **end if**
6: $Q_1 \leftarrow Q - k_0 P$
7: Tính $\frac{N}{q^2} Q_1$. Đó là phần tử $k_1 \left(\frac{N}{q} P \right)$ của T.
8: **if** $e = 2$ **then**
9: Nhảy đến bước 15.
10: **end if**
11: Lần lượt tính được các giá trị $k_0, k_1, \ldots, k_{r-1}$ và $Q_0, Q_1, \ldots, Q_{r-1}$
12: $Q_r \leftarrow Q_{r-1} - k_{r-1} q^{r-1} P$
13: Xác định k_r sao cho $\frac{N}{q^{r+1}} Q_r = k_r \left(\frac{N}{q} P \right)$
14: **if** $e = r + 1$ **then**
15: $k = k_0 + k_1 q + k_2 q^2 + \cdots + k_{e-1} q^{e-1} (\mod q^e)$
16: Stop.
17: **end if**
18: Quay về bước 11.

1.4. Phương pháp tấn công MOV

Tấn công MOV là tên viết tắt của các tác giả Menezes, Okamoto, và Vanstone [25], sử dụng cặp Weil để chuyển đổi bài toán Logarithm rời rạc trong $E(\mathbb{F}_q)$ thành bài toán Logarithm rời rạc trong $\mathbb{F}_{q^m}^{\times}$. Bởi vì giải bài toán Logarithm rời rạc trong trường hữu hạn sẽ dễ dàng và nhanh hơn giải Logarithm rời rạc trong nhóm các điểm trên đường cong Elliptic. Chọn m sao cho:

$$E[N] \subseteq \mathbb{F}_{q^m}^{\times}$$

Bởi vì tất cả các điểm trong $E[N]$ đều có tọa độ trong $\overline{\mathbb{F}}q = \cup_{j \geq 1} \mathbb{F}q^j$, nên m tồn tại. Theo định nghĩa về cặp Weil và các thuộc tính của cặp song tuyến tính:

$$\zeta_2 = e_N(Q, T_1) = e_N(kP, T_1) = e_N(P, T_1)^k = \zeta_1^k$$

Thuật toán 3 Tấn công MOV

1: Chọn điểm ngẫu nhiên $T \in E(\mathbb{F}_{q^m})$.
2: Tính bậc M của T.
3: Cho $d = \gcd(M, N)$ và cho $T_1 = (M/d)T$ có nghĩa là T_1 có bậc là d, chia hết bởi N, do đó $T_1 \in E[N]$.
4: Tính các cặp Weil $\zeta_1 = e_N(P, T_1)$ và $\zeta_2 = e_N(Q, T_1)$. Cả hai $\zeta_1, \zeta_2 \in \mu_d \subseteq \mathbb{F}_{q^m}^{\times}$.
5: Giải bài toán Logarithm rời rạc $\zeta_2 = \zeta_1^k$ trong $\mathbb{F}_{q^m}^{\times}$, sẽ tính được $k \pmod N$.
6: Lặp lại với điểm ngẫu nhiên T cho đến khi bội số chung nhỏ nhất của các số d là N, từ đó xác định được $k \pmod N$.

2. Tham số của hệ mật ECC

Các tham số của hệ mật ECC cần được lựa chọn kỹ càng để tránh các tấn công như MOV, trong quá trình lựa chọn hệ ECC cần phải đạt được một số tiêu chí được mô tả trong chuẩn [26].

Định nghĩa 2.1. *Tham số hệ mật* $D = (q, FR, S, a, b, P, n, h)$ *là một tập hợp gồm:*

1. *Bậc của trường* $\mathbb{F}_q$ *là* q.
2. *Phương pháp biểu diễn trường FR (field representation) được sử dụng cho các phần tử của* $\mathbb{F}_q$.
3. S *là mầm được sử dụng trong trường đường cong Elliptic được tạo ra một cách ngẫu nhiên.*
4. *Hai hệ số* $a, b \in \mathbb{F}_q$ *được dùng để định nghĩa đường cong E trên* $\mathbb{F}_q$ *(nghĩa là* $y^2 = x^3 + ax + b$*).*
5. P *là một điểm có bậc nguyên tố* n *và gọi là điểm cơ sở* $P = (x_P, y_P) \in E(\mathbb{F}_q)$.
6. *Đồng hệ số* $h = \#E(\mathbb{F}_q)/n$.

3. Trao đổi khóa

Trong các mục còn lại, chuyên đề sẽ đề cập đến một số thuật toán ứng dụng trong trao đổi khóa, mã hóa và ký số cơ bản. Chuẩn do công ty Certicom xây dựng [26] mô tả chi tiết việc triển khai ứng dụng ECC. Tác giả D. Hankerson [18] phân tích việc triển khai ECC bằng phần mềm, trong khi đó tác giả L. Cao [27] phân tích thực hiện các giao thức cơ bản của ECC bằng phần cứng.

3.1. Trao đổi khóa Diffie–Hellman ECDH

Năm 1998, Laurie và cộng sự đề xuất giao thức trao đổi khóa dựa trên ECC [28]. Sau đó giao thức này đã được đưa vào các tiêu chuẩn ANSI X9.42, ANSI X9.63 và IEEE P1363.

Hai bên A và B cần tạo khóa phiên bí mật trao đổi trong một kênh truyền công khai, hai bên cùng thỏa thuận điểm cơ sở P trên E. Bên A tạo khóa bí mật d_A và gửi giá trị d_AP cho bên B, ngược lại bên B tạo khóa bí mật d_B nhân với P sau đó gửi lại cho A. Khi đó khóa phiên của bên A sẽ là $K_A = d_Ad_BP$, và của bên B sẽ là $K_B = d_Bd_AP$. Dễ dàng nhận thấy $K_A = K_B$, khóa này chỉ riêng hai bên A và B có thể tính được. Xem sơ đồ dưới đây:

Bên A		Bên B
d_A	$\xrightarrow{d_AP}$	d_AP
d_BP	$\xleftarrow{d_BP}$	d_B
$K_A = d_Ad_BP$		$K_B = d_Bd_AP$

Đánh giá bảo mật: Để tìm được khóa chia sẻ K_A hoặc K_B, Hacker buộc phải tìm được cả 2 khóa bí mật d_A, d_B, trong khi chỉ có thể bắt được thông tin trên đường truyền là d_AP và d_BP, khi biết P, Hacker buộc phải giải bài toán Logarithm rời rạc $d_A = \log_P(d_AP)$ và $d_B = \log_P(d_BP)$ và đây là bài toán khó không giải được trong thời gian đa thức.

3.2. Tạo khóa bí mật chia sẻ ECMQV

Tên đầy đủ của giao thức là Elliptic Curve Menezes-Qu-Vanstone. Thuật toán đã được đưa vào trong các chuẩn ANSI X9.63, IEEE 1363-2000, và ISO/IEC 15946-3. Theo các tiêu chuẩn này điểm cơ sở được ký hiệu là G thay vì là P như thường gặp. Lược đồ này thường được sử dụng khi các bên A và B có cặp khóa công khai và bí mật cố định, tương ứng là (a, aG) và (c, cG).

Bên A sinh cặp số ngẫu nhiên (b, bG) và bên B tương ứng sinh cặp số ngẫu (d, dG), và trao đổi 2 cặp nay cho nhau giá trị bG và dG. Kí hiệu hàm $x : E \to \mathbb{N}$, lấy giá trị x của một điểm trên đường cong E.

Thuật toán 4 Tạo khóa bí mật chia sẻ ECMQV

INPUT: Các tham số của hệ mật (K, E, q, h, G), các số a, b, aG, bG, cG và dG.
OUTPUT: Khóa bí mật chia sẻ Q (chia sẻ với với đối tượng có khóa công khai cG).

1: $n \leftarrow \lceil log_2(\#k) \rceil / 2$.
2: $u \leftarrow (x(bG) (\text{mod } 2^n) + 2^n$.
3: $s \leftarrow b + ua((\text{mod } q)$.
4: $v \leftarrow (x(dG) (\text{mod } 2^n) + 2^n$.
5: $Q \leftarrow s(dG + v(cG))$.
6: **if** $Q = \infty$ **then**
7: Quay lại bước 1.
8: **end if**
9: Trả về khóa Q.

Bên B có thể tính ra cùng số Q bằng cách thay (a, b, c, d) trong thuật toán trên bằng (c, d, a, b). Bên A sẽ có các giá trị u_A, v_A, s_A và bên B sẽ có u_B, v_B, s_B. Dễ dàng nhận thấy [10]:

$$\begin{aligned}
u_A &= v_B \\
u_B &= v_A \\
Q_A &= s_A(dG + v_A(cG)) = s_A(d + v_Ac)G \\
&= s_A(d + u_Bc)G = s_As_BG \\
Q_B &= s_B(bG + v_B(aG)) = s_B(b + v_Ba)G \\
&= s_B(b + u_Aa)G = s_Bs_AG \\
Q_A &= Q_B = Q
\end{aligned}$$

Đánh giá bảo mật: Để hack được khóa chia sẻ, Hacker cần phải tính được các giá trị a, b, c, d, muốn vậy Hacker phải giải các bài toán Logarithm rời rạc $a = \log_G(aG)$, $b = \log_G(bG)$, $c = \log_G(cG)$, $d = \log_G(dG)$. Đây là các bài toán khó không thể giải được trong thời gian đa thức.

4. Xác thực - chữ ký số

4.1. ECDSA(The Elliptic Curve Digital Signature Algorithm)

Năm 1999, ECDSA (The Elliptic Curve Digital Signature Algorithm) đã được phê duyệt thành tiêu chuẩn của ANSI (ANSI X9.62-1998 ECDSA, phiên bản mới nhất là X9.62-2005), năm 2000 ECDSA cũng được IEEE và NIST phê duyệt thành tiêu chuẩn FIPS PUB 186-4 (DSS - Digital Signature Standard), phiên bản mới nhất ban hành 7-2013. ISO năm 2002 cũng ban hành tiêu chuẩn ISO/IEC 15946-2:2002 trong đó có phần dành riêng về ECDSA. Mô tả chi tiết về ECDSA có thể tìm thấy trong [29].

Người ký sẽ chọn số d làm khóa bí mật và tạo ra khóa công khai là $Q = dP$, sử dụng hàm băm H để tạo ra giá trị tóm lược văn bản e của văn bản m. Chữ ký số sẽ là cặp (r, s) được tính theo thuật toán 5.

Thuật toán 5 Sinh chữ ký số ECDSA

INPUT: Tham số D = (q, FR, S, a, b, P, n, h), khóa bí mật d, thông điệp m.
OUTPUT: Chữ ký số (r, s).

1: Chọn ngẫu nhiên $k \in [1, n-1]$,
2: $R \leftarrow kP = (x_1, y_1)$ và chuyển đổi $\bar{x_1} \leftarrow x_1$.
3: $r \leftarrow \bar{x_1} \pmod{n}$.
4: **if** $r = 0$ **then**
5: Nhảy đến bước 1:
6: **end if**
7: $e \leftarrow H(m)$.
8: $s \leftarrow k^{-1}(e + dr) \pmod{n}$.
9: **if** $s = 0$ **then**
10: Nhảy đến bước 1:
11: **end if**
12: Trả về (r, s)

Người xác thực chữ ký nhận được văn bản m' và chữ ký số (r, s) của người ký, sẽ tính giá trị tóm lược e' của văn bản nhận được là m' và áp dụng thuật toán 6 để xác định sự phù hợp của chữ ký số với văn bản nhận được, từ đó có thể khẳng định văn vản có do đúng người ký ký hay có sự giả mạo từ người khác hoặc văn bản có bị sửa đổi hay bị lỗi do đường truyền hay không.

Thuật toán 6 Xác thực chữ ký số ECDSA

INPUT: Tham số D = (q, FR, S, a, b, P, n, h), khóa công khai $Q = dP$, thông điệp nhận được m', chữ ký (r, s).
OUTPUT: Chữ ký hợp lệ hoặc không hợp lệ.

1: Kiểm tra r và s có phải là những số nguyên nằm trong khoảng $[1, n-1]$. Nếu không trả về return("Chữ ký không hợp lệ").
2: $e' \leftarrow H(m')$.
3: $w \leftarrow s^{-1} \pmod n$.
4: $u_1 \leftarrow e'w \pmod n$ và $u_2 \leftarrow rw \pmod n$.
5: $R' \leftarrow u_1 P + u_2 Q$.
6: **if** $R' = \infty$ **then**
7: return("Chữ ký không hợp lệ").
8: **end if**
9: Chuyển đổi x_1 của $R' \rightarrow$ số nguyên $\bar{x_1}$.
10: $r' \leftarrow \bar{x_1} \pmod n$.
11: **if** $r' = r$ **then**
12: return("Chữ ký hợp lệ").
13: **else**
14: return("Chữ ký không hợp lệ").
15: **end if**

Chứng minh tính đúng đắn của thuật toán: cần phải chứng minh rằng nếu $m' = m$ hay $e = e'$ thì $r' = r$. Thực vậy:

$$\begin{aligned} w = s^{-1} &= k(e + dr)^{-}1 \\ R' = u_1 P + u_2 Q &= (u_1 + u_2 d)P = (e' + rd)wP \\ &= (e' + rd)s^{-1}P = k(e' + rd)(e + rd)^{-1}P \end{aligned}$$

Nếu $e = e'$ ta sẽ có $R' = k(e + rd)(e + rd)^{-1}P = kP = R$ là điều cần phải chứng minh.

Đánh giá bảo mật: Để giả mạo được chữ ký, Hacker cần phải tìm được giá trị k và khóa bí mật d, để tìm được 2 giá trị này Hacker buộc phải giải 2 bài toán Logarithm rời rạc $k = \log_P R$ và $d = \log_P Q$ và đây đều là 2 bài toán khó, chưa giải được trong thời gian đa thức.

4.2. Chữ ký số ElGamal

Dựa trên lược đồ ký số do ElGamal đề xuất năm 1984 [30], phiên bản sửa đổi đã được đưa vào thành chuẩn về chữ ký số DSS (Digital Signature Standard) trong FIPS 186 [31].

Định nghĩa hàm f như sau:

$$f : E(\mathbb{F}_{\shortparallel}) \rightarrow \mathbb{Z}$$

Có thể chọn hàm $f(x, y) = x$, trong đó x là số nguyên $0 \leq x < q$. Cặp khóa bí mật và công khai của người ký là $(x, Y) \mid Y = xP$. N là bậc của điểm P thường là số nguyên tố lớn.

Thuật toán 7 Sinh chữ ký số Elgamal

INPUT: Khóa bí mật x, thông điệp m.
OUTPUT: Chữ ký số (R, s).

1: Chọn ngẫu nhiên $k \in [1, n-1]$,
2: $R \leftarrow kP$.
3: $s = k^{-1}(m - xf(R))$.
4: Trả về (R, s)

Thuật toán 8 Xác thực chữ ký số Elgamal

INPUT: Khóa công khai $Y = xP$, thông điệp nhận được m', chữ ký (R, s).
OUTPUT: Chữ ký hợp lệ hoặc không hợp lệ.

1: Tính $V_1 = f(R)Y + sR$.
2: Tính $V_2 = m'P$.
3: **if** $V_1 = V_2$ **then**
4: return("Chữ ký hợp lệ").
5: **else**
6: return("Chữ ký không hợp lệ").
7: **end if**

Chứng minh tính đúng đắn của thuật toán: khi $m' = m$:

$$V_1 = f(R)Y + sR = f(R)xP + k^{-1}(m - xf(R))R = mP = m'P = V_2$$

Đánh giá bảo mật: Muốn giả mạo chữ ký số, Hacker buộc phải tính được s, để tính được s buộc phải tính được k và khóa bí mật x, để tính được 2 giá trị này Hacker buộc phải giải bài toán Logarithm rời rạc $k = \log_P R$ và $x = \log_P Y$, là 2 bài toán không giải được trong thời gian đa thức.

5. Mã hóa - Giải mã

5.1. Mã hóa Massey-Omura

Massey-Omura là hai tác giả để xuất lược đồ mã hóa được mô tả trong Patent [32] vào năm 1986. Lược đồ mã hóa này ít được sử dụng trong thực tế nhưng nó có ý nghĩa về mặt lịch sử.

Bên A		Bên B
Biểu diễn thông điệp như $M \in E(\mathbb{F}_{\shortparallel})$		
Chọn $m_A \mid \gcd(m_A, N) = 1$	$\xrightarrow{M_1 = m_A M}$	M_1
M_2	$\xleftarrow{M_2 = m_B M_1}$	Chọn $m_B \mid \gcd(m_B, N) = 1$
Tính $m_A^{-1} \in \mathbb{Z}_{\mathbb{N}}$	$\xrightarrow{M_3 = m_A^{-1} M_2}$	M_3
		$M = m_B^{-1} M_3$

Dễ dàng nhận thấy:

$$m_B^{-1} m_A^{-1} m_B m_A M = M$$

Đánh giá bảo mật: Muốn phá khóa trong lược đồ này, Hacker phải tìm được giá trị m_A, m_B để tìm được các giá trị này Hacker phải lần lượt giải 2 bài toán Logarithm rời rạc $m_A = \log_M M_1$ và $m_B = \log_{M_1} M_2$, và đây là 2 bài toán chưa giải được trong thời gian đa thức.

5.2. Mã hóa ElGamal

Trên cơ sở hệ mật ElGamal [30], lược đồ mã hóa được phát biểu như sau:

Bên A		Bên B
Thông điệp $M \in E(\mathbb{F}_{\|})$		Chọn cặp khóa $(x_B, Y_B) \mid Y_B = x_B P$
Chọn k, tính $M_1 = kP$		
Tính $M_2 = M + kY_B$	$\xrightarrow{M_1, M_2}$	M_1, M_2
		$M = M_2 - x_B M_1$

Chứng minh tính đúng đắn của lược đồ mã hóa:

$$M = M_2 - x_B M_1 = M + kY_B - x_B M_1 = M + k(x_B P) - x_B(kP) = M$$

Đánh giá bảo mật: Để giải mã được văn bản M, Hacker buộc phải tìm được k và x_B, do đó Hacker cần phải giải 2 bài toán Logarithm rời rạc $k = \log_P M_1$ và $x_B = \log_P Y_B$, và đây là 2 bài toán khó.

5.3. Mã hóa ECIES (The Elliptic Curve Integrated Encryption System)

ECIES do Bellare và Rogaway đề xuất và là một biến thể của mã hóa dùng hệ mật ElGamal, sau đó thuật toán này đã được đưa vào các chuẩn ANSI X9.63 và ISO/IEC 15946-3, IEEE P1363a và [26].

Tham số D = (q, FR, S, a, b, P, n, h) được chọn tương tự như với ECDSA. Ở đây cần lựa chọn thêm các hàm mã hóa/giải mã đối xứng ký hiệu là $E_k(m)$ và $D_k(c)$. Trong đó m là bản rõ cần mã hóa, c là bản đã được mã. Thuật toán mã hóa đối xứng được chọn ở đây để phục vụ quá trình mã hóa/giải mã được dễ dàng hơn và nhanh hơn so với các thuật toán bất đối xứng. Ngoài ra thay vì sử dụng hàm băm đơn giản, ECIES sẽ sử dụng hai hàm băm sau:

- Message authentication code $MAC_k(c)$:

$$MAC : \{0,1\}^n \times \{0,1\}^* \longrightarrow \{0,1\}^n$$

- Key derivation function $KD(T, l)$:

$$KD : E \times \mathbb{N} \longrightarrow \{0,1\}^*$$

l là độ dài khóa $(k_1||k_2)$. $\{0,1\}$ là chuỗi bit có giá trị $0, 1$ có độ dài n hoặc không xác định (*).

Người nhận có cặp khóa công khai/bí mật là (Y, x) trong đó $Y = xP$.

Thuật toán 9 Mã hóa ECIES

INPUT: Văn bản cần mã hóa m, khóa công khai Y.
OUTPUT: Văn bản đã được mã hóa (U, c, r).

1: Chọn $k \in [1, q-1]$.
2: $U \leftarrow kP$.
3: $T \leftarrow kY$.
4: $(k_1 \| k_2) \leftarrow KD(T, l)$.
5: Mã hóa văn bản, $c \leftarrow E_{k_1}(m)$.
6: Tính giá trị MAC cho văn bản mã hóa $r = MAC_{k_2}(C)$
7: Trả về return(U, c, r).

Bên giải mã sẽ nhận được tập hợp (U, c, r) gồm các thành phần sau:

- U cần thiết để tính khóa phiên Diffie–Hellman T.
- c là bản đã được mã hóa.
- r được dùng để xác thực mã văn bản..

Thuật toán 10 Giải mã ECIES

INPUT: Văn bản mã hóa U, c, r, khóa bí mật x.
OUTPUT: Văn bản đã giải mã m hoặc thông báo "văn bản mã không hợp lệ".

1: $T \leftarrow xU$.
2: $(k_1 \| k_2) \leftarrow KD(T, l)$.
3: Giải mã văn bản, $m \leftarrow D_{k_1}(c)$.
4: **if** $r \neq MAC_{k_2}(C)$ **then**
5: xuất thông báo "văn bản mã không hợp lệ"
6: **end if**
7: Trả về văn bản đã được giải mã m.

Khóa phiên T sau khi được tính trong phần giải mã sẽ có giá trị giống như trong phần mã hóa. Thực vậy:

$$T_{Decryption} = xU = x(kP) = k(xP) = kY = T_{Encryption}$$

Đánh giá bảo mật: Để phá khóa được lược đồ này Hacker cần phải tìm được khóa bí mật x hoặc giá trị k bằng cách giải bài toán $x = \log_P Y$ hoặc $k = \log_P U$, và đây là 2 bài toán khó chưa giải được trong thời gian đa thức.

Một số thuật toán và giao thức khác sử dụng đường cong Elliptic ứng dụng trong mật mã có thể xem thêm trong [10, 21]. Tài liệu "*Guide to Elliptic Curve Cryptography*" [19] với rất nhiều thuật toán chi tiết có thể coi là cẩm nang để triển khai cho những bài toán ứng dụng cụ thể của ECC.

Tài liệu

[1] J. W. Bos, J. A. Halderman, N. Heninger, J. Moore, M. Naehrig, and E. Wustrow, "Elliptic Curve Cryptography in Practice," *Financial Cryptography and Data Security*, vol. 8437, pp. 157–175, 2014.

[2] J. H. Silverman and J. T. Tate, *Rational Points on Elliptic Curves - Second Edition*. Springer, 2015.

[3] L. C. Washington, *Elliptic Curves Number Theory and Cryptography, Second Edition*. CRC Press, 2008.

[4] J. W. S. Cassels, *Lectures on Elliptic Curves*. University of Cambridge, 1991.

[5] S. Lang, *Elliptic Curves Diophantine Analysis*. Springer, 1978.

[6] C. Kenig, A. Ranicki, and M. Rockner, *Elliptic Curves A Computational Approach*. Walter de Gruyter GmbH & Co., 2003.

[7] H. Cohen and G. Frey, *Handbook of Elliptic and Hyperelliptic Curve Cryptography*. Chapman Hall/CRC, 2006.

[8] J. H. Silverman, *The Arithmetic of Elliptic Curves*. Springer, 2009.

[9] L. Berger, G. Bockle, L. D. M. Dimitrov, T. Dokchitser, and J. Voight, *Elliptic curves, Hilbert modular forms and Galois deformations*. Birkhauser, 2013.

[10] I. F. Blake, G. Seroussi, and N. P. Smart, *Advances in Elliptic Curve Cryptography*. Cambridge University Press, 2005.

[11] I. Connell, *Elliptic Curve Handbook*. McGill University, 1999.

[12] T. H. Otway, *Elliptic Hyperbolic Partial Differential Equations*. Springer, 2015.

[13] Dang Minh Tuan, "Che tao thiet bi VPN IPSec bang phan cung dau tien o Vietnam," *Tap chi CNTT & TT*, no. 2, pp. 41–45, 2014.

[14] H. Lenstra., "Factoring Integers with Elliptic Curves," *The Annals of Matematics*, vol. 126, no. 3, pp. 649–673, 1987.

[15] V. S. Miller, "Use of elliptic curves in cryptography," *CRYPTO '85*, pp. 417–428, 1985.

[16] N. Koblitz, "Elliptic curve cryptosystem," *Math.Comp*, vol. 48, no. 16, pp. 203–209, 1987.

[17] A. Enge, *Elliptic Curves and Their Applications to Cryptography*. Kluwer Academic Publishers, 2001.

[18] D. Hankerson, J. L. Hernandez, and A. Menezes, "Software Implementation of Elliptic Curve Cryptography over Binary Fields," *CHES2000*, vol. 1965, pp. 243–267, 2000.

[19] D. Hankerson, A. Menezes, and S. Vanstone, *Guide to Elliptic Curve Cryptography*. Springer-Verlag, 2004.

[20] R. Schoof, "Elliptic Curves Over Finite Fields and the Computation of Square Roots," *Matematics of Computation*, pp. 483–495, 1985.

[21] I. Blake, G. Seroussi, and N. Smart, *Elliptic Curves in Cryptography*. Cambridge University Press, 1999.

[22] H. Cohen, *A Course in Computational Algebraic Number Theory*. Springer-Verlag, 1993.

[23] J. M. Pollard, "Monte Carlo Methods for Index Computations (mod p)," *Mathematics of Computation*, vol. 32, no. 143, pp. 918–924, 1978.

[24] S. C. Pohlig and M. E. Hellman, "An Improved Algorithm for Computing Logarithms over GF(p) and its Cryptographic Significance," *IEEE Transactions on Information Theory*, vol. 24, pp. 106–110, 1978.

[25] A. J. Menezes, T. Okamoto, and S. A. Vanstone, "Reducing elliptic curve logarithms to logarithms in a finite field," *IEEE Trans. Inform. Theory*, vol. 39, no. 5, pp. 1639–1646, 1993.

[26] C. Research, *Standards For Efficient Cryptography, SEC 1: Elliptic Curve Cryptography*. Certicom Corp, 2000.

[27] L. Gao, S. Shrivastava, and G. E. Sobelman, "Elliptic Curve Scalar Multiplier Design Using FPGAs," *CHES'99*, vol. 1717, pp. 257–268, 1999.

[28] L. Laurie, M. Alfred, Q. Minghua, S. Jerry, and V. Scott, "An Efficient Protocol for Authenticated Key Agreement," *Designs Codes and Cryptography*, vol. 28, no. 2, 1998.

[29] D. Johnson, A. Menezes, and S. Vanstone, "The Elliptic Curve Digital Signature Algorithm (ECDSA)," 2001.

[30] T. E. Gamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," *CRYPTO '84*, vol. 196, pp. 10–18, 1985.

[31] NIST, *Digital Signature Standard (DSS) FIPS 186-4*. National Institute of Standards and Technology, 2013.

[32] J. Massey and J. Omura, "Method and apparatus for maintaining the privacy of digital messages conveyed by public transmission," Jan. 28 1986, US Patent 4,567,600. [Online]. Available: https://www.google.com/patents/US4567600

VẬT LÝ, HÌNH HỌC VÀ TRÁI ĐẤT TRÒN

Nguyễn Ái Việt
(Viện Công nghệ Thông tin, Đại học Quốc gia Hà Nội)

GIỚI THIỆU

Nhắc tới chuyện Trái Đất tròn là người ta nghĩ tới các nhà vật lý N.Copernicus, G.Galilei, G.Bruno và thường nghĩ rằng đó là một vấn đề thuộc về vật lý. Thực ra đây là một vấn đề ứng dụng hình học được tìm ra trước đó gần 2000 năm bởi nhà bác học Hy Lạp Erasthonenes. Vì sao nhân loại lại bỏ quên một phát kiến vĩ đại như vậy? Vì sao các nhà bác học Trung Quốc, vẫn chưa bao giờ biết và nghĩ tới việc này cho đến khi bị văn minh phương Tây tràn vào và lấn át.

Hình học và Vật lý

Thời Hy Lạp cổ, khoa học không phân biệt, chuyên môn hóa như bây giờ. Một nhà bác học thường nghiên cứu các vấn đề Triết học, Toán học, Vật lý, Logic, Ngôn ngữ và các khoa học nhân văn. Các ngành khác nhau, như ta biết bây giờ, chỉ là các vấn đề mà họ quan tâm.

Trái với ngày nay, khi đó hình học gắn liền với ứng dụng thực tế thời Hy Lạp cổ là việc đo đất đai. Vật lý là khoa học siêu hình trừu tượng chỉ giành riêng cho các nhà hiền triết lớn nhất giải thích mọi hiện tượng xảy ra trong tự nhiên. Các vấn đề vật lý mà họ bàn luận hết sức xa thực tế như tại sao mũi tên không có người đẩy lại bay được. Khi đó, hình học và vật lý là hai vấn đề khoa học song sinh, cùng nghiên cứu tính chất và quan hệ của các vật thể trong không gian sống của con người.

Dần dần, hình học cố gắng thoát ra khỏi các nội dung ứng dụng cụ thể, ngày càng trừu tượng hơn. Điều đó tốt, giúp hình học bớt thiển cận có thể vươn tới những khái niệm hiện hữu nhưng ở bên ngoài suy diễn trực giác của con người. Như thế phạm vi ứng dụng của hình học ngày càng mở rộng.

Vật lý phát triển theo chiều ngược lại, cố gắng thoát khỏi tháp ngà siêu hình học, tìm đến với quan sát thực tiễn, để giải thích các hiện tượng tự nhiên có căn cứ hơn. Và cũng như thế, vật lý ngày càng giúp con người hiểu nhiều về bản chất của vũ trụ.

Tuy vậy, do việc chuyên môn hóa quá sâu, ngày nay người ta, kể cả các nhà khoa học có chuyên môn sâu, có nhiều ngộ nhận. Họ cho rằng, Hình học là khoa học về những hình thể không tồn tại, chẳng liên quan gì tới thực tiễn. Ngược lại, vật lý là phải gắn liền với số liệu của các quá trình cụ thể. Do đó, chính các nhà khoa học cũng tự băn khoăn, nghiên cứu các khoa học như hình học và vật lý lý thuyết sẽ đem lại điều gì.

Hình học ở Trung Hoa và Hy Lạp cổ

Người ta thường nói các nhà hiền triết Trung Quốc cũng đã tìm ra hình học riêng theo cách của họ. Có người còn gắn Kinh Dịch, tâm linh và các yếu tố siêu hình khác với các tỷ lệ Lỗ Ban quy định cho thợ mộc.

Sau hơn 2000 năm, mạc dù phát minh ra rất nhiều điều kinh ngạc, lập được những bản đồ thiên văn đầu tiên của nhân loại, kiến thức hình học của người Trung Quốc vẫn hết sức thô sơ, không tiến gì được thêm so với Lỗ Ban, ở thế kỷ 4 trước Công nguyên.

Nói một cách khác, hình học, nếu có ở Trung Quốc thời cổ, chỉ là một dạng tiền thân khoa học hết sức sơ đẳng. Khi đó việc thờ phụng cúng bái các tỷ lệ hình học của Lỗ Ban, cũng như việc các tín đồ của Pythagoras tin rằng nhờ Thượng đế họ mới phát mình được ra định lý về tam giác vuông và phải mổ tới 100 con bò để tạ ơn với hy vọng rằng Thượng đế sẽ cho họ có nhiều định lý khác đẹp đẽ hơn. Chính lòng tin mù quáng và hạn chế với các ứng dụng ngay trước mắt đã làm các hiểu biết về hình học ở Trung Quốc trở nên thiển cận và dẫm chân tại chỗ.

Mặc dù các tư duy sơ khai đều có thể chứa đựng rất nhiều minh triết, nhưng chúng vẫn chưa phải là khoa học. Cho đến khi văn minh phương Tây tràn vào, người Á Đông vẫn tin rằng Trái Đất hình vuông, bầu trời hình bán cầu chụp lên mặt đất như một cái lồng bàn, bốn phương có bốn cột chống trời đỡ toàn bộ cái lồng bàn.

Một chú bé lớp hai ngày nay cũng có thể đặt rất nhiều câu hỏi làm mô hình vũ trụ quan hình học này đổ sụp. Tôi tin rằng các nhà hiền triết Trung Hoa cũng đã từng đặt ra được các câu hỏi như thế. Nhưng điều gì khiến họ không dám trả lời để thay đổi vũ trụ quan đó? Chúng ta sẽ quay lại vấn đề này sau khi nhìn lại cách nghĩ của các nhà bác học Hy Lạp cổ.

Nhà bác học Hy Lạp Erasthostene sống vào thế kỷ 3 trước Công Nguyên, tức là sau Lỗ Ban hơn 200 năm. Ông chỉ dùng suy luận và dựa trên một số dữ liệu quan sát đã biết được Trái đất có hình cầu và tính được chu vi của hình cầu đó một cách chính xác. Đó mới chính là khoa học đích thực.

Ý tưởng của Erasthostene khá đơn giản so với hiểu biết của chúng ta ngày nay: Người Hy Lạp, người A rập cổ đã biết chế tạo ra các đồng hồ mặt trời tương đối chính xác dựa trên bóng của các đỉnh tháp khi có mặt trời. Vào thời điểm giữa trưa, bóng của các cọc đóng vuông góc trên mặt đất là ngắn nhất. Nếu giả thiết các tia sáng đến mặt đất đều song song và mặt đất là phẳng, các hình chiếu của các cọc cao như nhau phải giống hệt nhau. Tuy nhiên, Erasthostene nhận thấy hình chiếu của các cọc có cùng độ dài vào giữa trưa tại Syene và Alexandria không giống nhau. Điều đó có nghĩa là các cọc không song song và lập thành một góc nhất định với nhau xấp xỉ $\frac{2\pi}{50}$. Như vậy, Trái Đất phải là hình cầu có chu vi gấp 50 lần khoảng cách từ Syene đến Alexandria. Bài toán trên có thể giải trong trường hợp các tia sáng không song song và đều xuất phát từ một điểm là Mặt Trời. Tuy nhiên do khoảng cách giữa Mặt Trời vào Trái Đất là quá lớn so với các dữ liệu trong bài toàn, đóng góp của sự sai lệch này không đáng kể.

Điều quan trọng ở đây không phải là giải một bài toán mà ở phương pháp suy luận, sáng tạo, trí tưởng tượng và khả năng liên tưởng giữa các khái niệm trừu tượng và thực tế. Các nhà hiều triết Á Đông đi trước, có rất nhiều ưu thế, nhưng thiếu đi những thành phần quan trọng nhất để tạo ra sáng tạo khoa học có tầm cỡ thực sự. Nếu có ai đó vẽ sẵn cho họ các tia sáng, cọc, đường

dây cung giữa Syene và Alexandria và tâm Trái Đất, các học trò của họ cũng có thể tính toán dễ dàng chu vi của vòng tròn, cho dù họ chưa bao giờ biết đến số π.

Điểm quan trọng trong phát kiến vượt thời gian gần 2000 năm so với minh triết phương Đông của Erasthostene là óc tưởng tượng gắn liền với các dữ liệu có thể quan sát được. Dữ liệu quan sát được mới giúp chúng ta "nhìn" thấy những sự vật mà những người minh triết đến đâu cũng không nhìn thấy được. Các giáo điều, giả thiết, định kiến có sẵn sẽ bịt mắt làm các nhà khoa học mù lòa. Nói một cách khác, Erasthostene đã nhìn ra Trái Đất tròn từ các bóng nắng, điều mà các nhà hiền triết Á Đông không thể nào làm được do phương pháp nhận thức của mình.

Nghiên cứu hình học không chỉ bao gồm việc suy luận ra các tính chất của các vật thể dựa trên một số tiên đề có sẵn mà còn là việc nhìn thấy được sự hiện hữu của một hình học xác định qua các vật thể và hiện tượng có trong thực tế.

Hình học, vật lý và rào cản vô hình

Hình học, xây dựng trên những tiên đề cố định, và cố gắng tìm ra những tính chất bất biến với thời gian. Với toán học, một tam giác được giả thiết là được sinh ra cùng với vũ trụ và tồn tại mãi mãi như thế. Các câu hỏi, tại sao một vật lại có hình tam giác, hình thành như thế nào, trước đó là hình gì và trong tương lai sẽ là hình gì, đều được cho là không thuộc phạm vi nghiên cứu của hình học.

Hình học như một bức tranh tĩnh, một lát cắt đồng thời gian của các sự vật và đông cứng lại chúng lại để nghiên cứu. Vật lý, người anh em song sinh của hình học là khoa học của vận động, nhờ đến toán học để biết các thuộc tính của sự vật tại mỗi thời điểm, nhưng tìm các quy luật điều khiển vận động, thay đổi của sự vật.

Thực ra, hình học có sức mạnh hơn là một trật tự tĩnh. Chính cách nhìn nhận, của nhà khoa học, bị ảnh hưởng không ít bởi môi trường sống, công luận xung quanh, tự hạn chế mình giống như các hiền triết Á Đông thời cổ.

Không ít các nhà Toán học lớn như Leibnitz, Gauss, Poincaré, Hilbert, Cartan đã thoát được khỏi những tín điều đó. Leibnitz đã cùng với Newton phát hiện ra tính toán giải tích và xây dựng hệ thống vũ trụ cơ học của Newton. Gauss, Poincaré đã đặt nền tảng cho hệ thống vũ trụ với các hiện tượng điện từ của Maxwell. Hilbert, Cartan đã cùng Einstein xây dựng mô hình thế giới bằng các đa tạp Riemann cho các hiện tượng hấp dẫn.

Trong các mô hình vũ trụ quan như thế, hình học trở thành cuốn phim sinh động, mô tả những vụ nổ lớn, sóng lan truyền từ những khoảng cách không thời gian tới hàng tỷ năm ánh sáng. Không có hàng rào nào cản trở sự suy nghĩ, biết các khái niệm trừu tượng thành chuyện giành riêng của một số người, cũng không có hàng rào nào ngăn cách hình học và vật lý. Các tín điều đều là con người tưởng tượng ra để ngăn cấm chính mình.

Ý nghĩa thực tiễn của hình học và vật lý

Ngày nay, nhân loại đang đứng trước những phát kiến lớn lao với những quan sát mới về sóng hấp dẫn, vật chất tối, lực thứ năm hứa hẹn một cuộc cách mạng mới về khoa học công nghệ. Có những người và những dân tộc sẽ trở nên hùng cường, có những người và những dân tộc sẽ lỡ chuyến tàu lịch sử bởi không chịu từ bỏ thói quen suy nghĩ của chính mình.

Khoa học công nghệ không thể phát triển dựa trên một động lực ứng dụng thiển cận vào những khái niệm có sẵn và cố định xung quanh ta. Có lẽ động lực tìm đến các khái niệm mới quan trọng hơn chính bản thân nội dung các phát kiến khoa học.

Trong khi đó, như một tất yếu, mặc dù không phải là động lực ban đầu, khoa học luôn mang đến những công nghệ mới. Khi sóng điện từ được tìm ra từ lời giải của phương trình Maxwell, không ai nghĩ được có một ngày, sóng vô tuyến truyền hình, Internet, điện thoại di động lại tràn ngập không gian sống của chúng ta như ngày nay. Công thức năng lượng $E = mc^2$ của lý thuyết tương đối đem lại nguồn năng lượng khổng lồ cho nhân loại. Phương trình Schrödinger và các hệ thức giao hoán ma trận của Heisenberg mở đầu công nghệ vật liệu mới, bán dẫn và các linh kiện điện tử mở ra cuộc cách mạng về công nghệ thông tin.

Nói về thành tựu do khoa học đúnng nghĩa đem lại, chúng ta cũng không bao giờ quên những vật cản đường do chính chúng ta tạo ra là hệ quả của thói quen cổ hủ, định kiến sai lầm, thực dụng thiển cận. Chúng ta đã thấy bài học của khoa học thời cổ ở Á Đông. Để kết thúc tôi xin nhắc lại một câu chuyện để nói lên cách suy nghĩ thực dụng thiển cận có thể gây nên một sai lầm quyết định vận mệnh của cả một dân tộc như thế nào.

Trước chiến tranh thế giới lần thứ 2, nước Đức là trung tâm của khoa học thế giới, nơi phát minh ra Cơ học Lượng tử và Thuyết tương đối. Về mặt công nghệ, nước Đức đi đầu và hoàn toàn sẵn sàng chế tạo thành công bom nguyên tử. Do chính sách của Hitler, rất nhiều nhà khoa học giỏi đã rời khỏi Đức, do không muốn hợp tác với chính quyền phát xít. Với lực lượng còn lại, nước Đức vẫn đủ khả năng làm ra bom nguyên tử trước Mỹ và Liên Xô. Tuy nhiên, Hitler đã ban hành một chính sách là mọi nghiên cứu khoa học phải có kết quả thực tiễn trong vòng 6 tháng. Chính điều đó làm nước Đức không thể chế tạo bom nguyên tử vì không đủ các nghiên cứu cơ bản cần thiết.

Có thể đó là một may mắn cho nhân loại, nhưng không hề ngẫu nhiên. Một sự ngu dốt về chính sách cũng chỉ là hệ quả tất yếu của cách nghĩ phát xít mà thôi. Độc tài, phân biệt chủng tộc bao giờ cũng sẽ tự kìm hãm chính mình. Chính vì thế mà nhân loại còn tồn tại.

Bạn nghĩ sao nếu Lỗ Ban cũng tìm ra được Trái Đất hình cầu như Erasthostene, hình học Euclide được tìm ra và cách mạng cơ khí nổ ra tại Trung Quốc? Với cách nghĩ Á Đông, cho dù có những kiến thức khoa học vĩ đại nhất, liệu có phải là may mắn hơn cho nhân loại hay không?

SỐT MAYONNAISE VÀ BẦU CỬ TỔNG THỐNG MỸ

Nils Berglund (Đại học Orleans, Cộng hòa Pháp)
Người dịch: Dương Đức Lâm (Đại học Sussex, Vương quốc Anh)

LỜI NGƯỜI DỊCH

Nils Berglund là giáo sư toán học của Đại học Orléans, Pháp. Lĩnh vực nghiên cứu chính của ông là vật lý toán, lí thuyết hệ động lực và lí thuyết xác suất. Ngoài chuyên môn ông còn có sở thích trượt tuyết và nấu ăn. Ông cũng có khá nhiều bài viết phổ biến khoa học, một số đăng trên các tạp chí, website khoa học của Pháp, điển hình là *Images des Mathématiques*. Bài viết sau đây được dịch từ nguyên bản tiếng Pháp "Mayonnaise et élections américaines" đã đăng trên tạp chí *Dossier Pour La Science* số 91, tháng 4 - 6 năm 2016. Bản dịch đã được sự cho phép của tác giả. Một số thuật ngữ, do chưa được dịch ra tiếng Việt một cách thống nhất, hoặc để cho độc giả có thể tìm hiểu rõ hơn, chúng tôi chú thích thêm dưới dạng tiếng Anh. Tất cả các chú thích là của người dịch.

Chắc hẳn là bạn đã biết đến phương trình vi phân, nhưng liệu bạn có biết phương trình vi phân đạo hàm riêng ngẫu nhiên? Có nguồn gốc từ những vấn đề sống động quanh ta, chúng rất hữu ích cho việc nghiên cứu các hiện tượng khác nhau trong tự nhiên cũng như trong chính xã hội loài người. Nó là lĩnh vực nghiên cứu trung tâm dẫn đến giải thưởng Fields của một nhà toán học năm 2014.

Hãy bắt đầu với hai bài toán thực tế sau đây. Trộn lẫn một hỗn hợp dầu ăn với nước, quan sát (với các công cụ hỗ trợ tùy ý theo lựa chọn của bạn) sự lắng đọng của các phân tử trên bề mặt, và so sánh nó với trò chơi xếp hình Tetris[1]. Theo dõi sự thay đổi quan điểm chính trị của người Mỹ trong tiến trình của cuộc bầu cử tổng thống sẽ diễn ra vào tháng 11 năm nay. Thật ngạc nhiên là để hiểu được những hiện tượng khác nhau từ những nguồn gốc rất khác nhau như thế, chúng ta lại cần đến sự hỗ trợ của cùng một công cụ toán học. Đó là phương trình đạo hàm riêng ngẫu nhiên (được kí hiệu là SPDE[2]), một công cụ toán học mà đã trở nên hiệu quả hơn rất nhiều nhờ các nghiên cứu gần đây của Martin Hairer, Giáo sư Đại học Warwick, Vương quốc Anh. Với những đóng góp quan trọng đó, ông được trao tặng Huy chương Fields danh giá năm 2014. Vậy SPDE là gì?

Điểm khác nhau căn bản giữa SPDE với phương trình vi phân thường là ở chỗ, SPDE được áp dụng cho các hệ mô hình toán học có chiều vô hạn với một đại lượng được gọi là *tiếng ồn*[3] (hay các nhiễu loạn ngẫu nhiên). Nhờ đó chúng ta có thể nghiên cứu các tình huống phức tạp nơi có sự tương tác, giao thoa của rất nhiều yếu tố, như các bọt dầu, các phân tử vật chất hay những

[1] Một trò chơi điện tử rất phổ biến từ cuối những năm 90 của thế kỉ XX
[2] Stochastic Partial Differential Equations
[3] noise

Hình 1: *Sự phát triển quan điểm chính trị của người dân Mỹ có thể được mô tả bởi phương trình đạo hàm riêng ngẫu nhiên!*

người Mỹ! Chúng ta sẽ cùng vén bức màn bí mật về các phương trình này, cũng như không quên tìm hiểu những tiến bộ quan trọng nào trong các công trình của Martin Hairer đã đưa đến cho ông ấy một giải thưởng tương đương với giải Nobel. Nhưng trước khi bắt đầu, hãy cầm lấy ngọn đuốc của bạn!

Đốt nóng một thanh kim loại một cách không đồng đều, tức là chỉ đốt ở một số chỗ nhất định trên thanh. Làm thế nào để xác định được nhiệt độ ở một vị trí nào đó của thanh kim loại theo thời gian? Chúng ta có thể trả lời câu hỏi này nhờ lí thuyết phương trình truyền nhiệt (xem Phụ lục 1 ở cuối bài viết), được giới thiệu bởi Joseph Fourier vào năm 1811. Biến trong phương trình truyền nhiệt là hàm $T(x,t)$, mô tả nhiệt độ tại điểm x và ở thời gian t. Đây là một phương trình vi phân đạo hàm riêng, nó biểu thị sự phụ thuộc của các thông số về sự biến thiên theo không gian và theo thời gian của nhiệt độ. Người ta đã biết cách giải phương trình này, và do đó dự đoán, biết được sự phân bố nhiệt độ tại thời điểm ban đầu $T(x,0)$, nhiệt độ tại bất kì điểm nào cũng như tại bất kì thời gian nào sau đó.

Đốt nóng thanh kim loại

Phương trình truyền nhiệt có hai tính chất quan trọng. Tính chất thứ nhất, *nguyên lí chồng chất nghiệm*[4], nói rằng nếu ta biết được các nghiệm mô tả sự phân bố nhiệt độ của thanh kim loại cho bởi hai nguồn nhiệt khác nhau, chẳng hạn đốt nóng thanh tại điểm x hoặc ở điểm y, thì ta cũng biết được nghiệm mô tả sự phân bố nhiệt độ của nó khi đốt nóng thanh cùng lúc tại hai điểm x và y. Nghiệm này chỉ đơn giản là nhận được bằng cách cộng hai nghiệm trước đó với nhau.

Tính chất thứ hai nói rằng phương trình truyền nhiệt có tính *chính quy*[5]. Giả sử sự phân bố nhiệt độ ban đầu rất khác nhau, chẳng hạn, đặt nửa trái của thanh kim loại vào lò nung ở 1000 độ C (rồi bỏ ra), còn nửa phải ở nhiệt độ phòng. Thế thì gần như ngay lập tức, nhiệt độ ở nửa trái sẽ lan truyền một cách đều đặn và liên tục ra toàn bộ thanh cho đến khi toàn bộ thanh đạt được một nhiệt độ ổn định[6].

[4] superposition principle
[5] regularity, hay tính trơn
[6] nói cách khác, ngay sau khi bỏ thanh kim loại ra khỏi lò, đồ thị nhiệt độ trong thanh là một hàm liên tục

Chúng ta cũng mô tả được sự truyền nhiệt trong các đối tượng phức tạp hơn, khi thay thanh kim loại bởi một tấm kim loại hình chữ nhật, hình đĩa, hay một khối kim loại hình lập phương. Với những hình khối tổng quát hơn, mặc dù không phải lúc nào ta cũng tìm được nghiệm một cách chính xác, nhưng nguyên lí chồng chất nghiệm và tính chính quy thì vẫn luôn đúng cho mọi trường hợp.

Một sự tổng quát khả dĩ khác cho phương trình truyền nhiệt là khi thanh kim loại được tiếp tục cung cấp một nguồn nhiệt thay đổi theo thời gian, ta có phương trình truyền nhiệt *cưỡng bức*[7] (còn gọi là bài toán không thuần nhất). Lúc này nghiệm của bài toán nhận được nhờ áp dụng nguyên lí Duhamel, nói rằng nghiệm ở thời điểm t có thể viết như một sự chồng chất nghiệm của các thời điểm trước đó.

Món sốt mayonnaise thất bại và bề mặt lượn sóng của tấm tôn

Có nhiều phương trình đạo hàm riêng có dạng tương tự như phương trình truyền nhiệt, nhưng chứa thêm một số đại lượng khác làm cho việc nghiên cứu chúng trở nên khó khăn hơn rất nhiều. Một ví dụ điển hình là phương trình Allen - Cahn, mô phỏng hiện tượng *tách pha*[8]. Khi trộn một hỗn hợp nước với dầu ăn vào một cái bình thủy tinh và lắc mạnh, ta nhận được một thể nhũ: chúng không thể trộn lẫn hoàn toàn vào nhau, mà hình thành những giọt nhỏ li ti dầu và nước có thể quan sát thấy qua kính lúp.

Nguyên lí tương tự cũng xảy ra với nước sốt mayonnaise, một hỗn hợp nhũ tương của dầu ăn và dấm được kết dính với nhau bằng lòng đỏ trứng gà. Thiếu thành phần cuối cùng này (hoặc một thành phần có vai trò tương đương), thì dù bạn có cố gắng cách mấy, các giọt li ti dầu ăn và giấm cũng sẽ tụ họp dần dần thành hai lớp khác nhau! Đó là sự tách pha. Hiện tượng tương tự cũng được quan sát thấy trong một số loại hợp kim.

Để mô hình hóa hiện tượng này, hãy tưởng tượng có một chuỗi hạt cườm được nối với nhau bởi những chiếc lò xo. Đặt ngang chuỗi hạt lên trên một tấm tôn lượn sóng gồm hai rãnh song song cách nhau bởi phần chõm nhô lên cao ở giữa (xem Hình 2). Dưới tác dụng của trọng lực, mỗi hạt cườm đều có xu hướng lăn xuống đáy một trong hai rãnh. Tuy nhiên vì có sợi lò xo, các hạt lân cận hạt đó cũng có xu hướng bị kéo xuống rãnh theo. Các tương tác này là một sự mô phỏng tương tự cho hỗn hợp nhũ tương ở trên khi chúng tách thành hai phần dầu ăn và dấm, và xu hướng chuyển động của các phân tử của hai chất lỏng bao quanh các phân tử cùng loại[9].

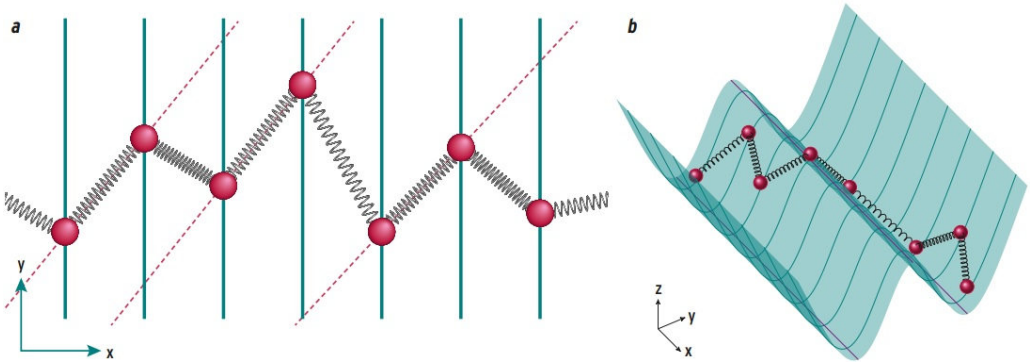
Bây giờ lấy các chuỗi với số hạt cườm tăng dần còn lò xo thì ngắn dần[10]. Tại điểm tới hạn, chuỗi hạt có thể được đặc trưng bởi một hàm $Y(x,t)$, cho biết sự chuyển dịch ngang của chuỗi tại điểm x và tại thời gian t. Giả sử hai rãnh tương ứng với $Y = 1$ và $Y = -1$, trong khi phần chõm là $Y = 0$. Người ta chứng minh được rằng sự chuyển dịch ngang này tuân theo một phương

[7] forced

[8] phase separation

[9] Bạn đọc có thể xem một minh họa thú vị cho hiện tượng này ở đây https://www.youtube.com/watch?v=NDQHepkSeS8

[10] đương nhiên kích thước hạt sẽ phải bé dần



Hình 2: *Chuỗi hạt cườm và mayonnaise. Các hạt gắn với nhau bởi lò xo có thể chuyển động tự do theo phương y nhưng bị cố định theo phương x với một khoảng cách đều nhau (a). Khi chiều dài lo xo ngắn lại, ngắn hơn khoảng cách nhỏ nhất giữa các hạt, chúng sẽ có xu hướng xếp thành hàng (đường nét đứt). Đặt chuỗi hạt này lên một tấm tôn (b). Mỗi hạt cườm sẽ bị thu hút bởi các hạt lân cận của nó và bởi rãnh tấm tôn. Khi số hạt tăng lên vô hạn, sự chuyển động của chuỗi hạt được mô tả bởi phương trình Allen - Cahn một chiều.*

trình đạo hàm riêng, nhận được bằng cách thêm vào phương trình truyền nhiệt một đại lượng $Y - Y^3$, biểu thị cho hiệu ứng đẩy các hạt về một trong hai rãnh. Phương trình này được đưa ra vào năm 1972 một cách độc lập bởi hai nhóm nghiên cứu, một nhóm gồm Nathaniel Chafee và Ettore Infante, nhóm kia là John Allen và Sam Cahn (xem Phụ lục 2).

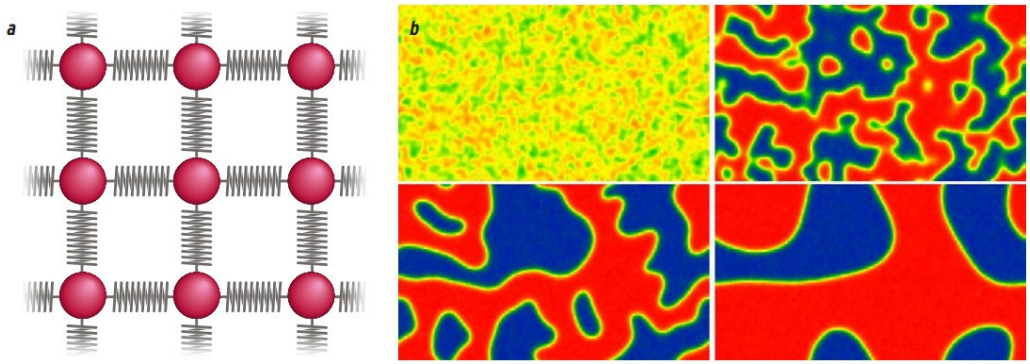
Khác với phương trình truyền nhiệt, phương trình Allen - Cahn không có nghiệm hiển, cũng không thỏa mãn nguyên lí chồng chất nghiệm. Nguyên nhân là bởi có sự xuất hiện của đại lượng phi tuyến Y^3. Tuy vậy, ta có thể xây dựng được một nghiệm của nó bằng phương pháp xấp xỉ liên tiếp. Trước hết, hãy tạm quên đi đại lượng $Y - Y^3$ để trở về với phương trình truyền nhiệt, và gọi nghiệm của nó là Y_0. Ý tưởng là sau đó thay thế đại lượng $Y - Y^3$ bởi $Y_0 - Y_0^3$ và nhận được một phương trình truyền nhiệt không thuần nhất mà ta đã biết cách giải. Gọi nghiệm của nó là Y_1, lại thay thế đại lượng trên bởi $Y_1 - Y_1^3$, và cứ tiếp tục như thế, với hi vọng rằng chúng ta sẽ tiến một cách từ từ đến nghiệm chính xác của phương trình. Và điều này thực tế là đúng, thật vậy, phương pháp này chẳng qua là một biến thể của *phép lặp Picard*, nó cung cấp một con đường để tìm nghiệm của phương trình Allen - Cahn và vẫn hoạt động rất tốt trong trường hợp số chiều tăng lên (xem Hình 3).

Nhắc lại rằng, phép lặp Picard là một phương pháp giải phương trình vi phân bằng các phép xấp xỉ liên tiếp, càng nhiều phép lặp càng chính xác. Thực tế quy trình này thường được sử dụng để chứng minh sự tồn tại nghiệm của một phương trình vi phân hay phương trình đạo hàm riêng cụ thể nào đó.

Trong mô hình tách pha, chúng ta cũng có thể quan tâm đến sự biến đổi của kích cỡ các nhóm phân tử cùng loại theo thời gian, và các *mặt phân cách*[11] giữa chúng (xem Hình 4).

Các hiện tượng tương tự như sự tách pha cũng được quan sát thấy trong các mô hình nam châm hay các mô hình về sinh thái (chẳng hạn mô tả sự hình thành các vết vằn hay lốm đốm trên lông động vật trong quá trình chúng lớn lên). Thêm một chút tưởng tượng, chúng ta thậm chí nhìn thấy điều tương tự trong một hệ mô tả sự phát triển của các quan điểm cá nhân. Xét một đất

[11] interface



Hình 3: *Sự tách pha. Chúng ta có thể mô phỏng hiện tượng này với một "thảm" hạt cườm được sắp xếp theo một mạng lưới ô vuông, liên kết với nhau bởi các lò xo (a). Chúng có thể chuyển động vuông góc với mặt phẳng. Sự tiến hóa của hệ này (b) được cho bởi nghiệm của phương trình Allen - Cahn ngẫu nhiên hai chiều, giải thích hiện tượng tách pha. Vùng màu đỏ và xam lam tương ứng với các pha nguyên chất (dầu ăn hoặc dấm), các vùng màu cam, vàng hoặc xanh lá cây là các vùng trộn lẫn với tỉ lệ khác nhau giữa hai pha. Bốn hình ảnh mô tả trạng thái của hệ sau 10, 50, 100 và 300 đơn vị thời gian.*

nước có hai đảng đối lập, ví dụ nước Mỹ. Những điểm xanh và những điểm đỏ tượng trưng cho một cách tương ứng những người tin vào Đảng Dân chủ và tin vào Đảng Cộng hòa, những điểm có màu trung gian tượng trưng cho những người chưa quyết định sẽ theo bên nào, với một thiên hướng mạnh hay yếu hướng đến một trong hai đảng. Chúng ta giả sử ở đây rằng mỗi người dân bị ảnh hưởng bởi những người hàng xóm của họ, và do đó hình thành những vùng mà trong đó mọi người cùng chia sẻ một quan điểm chính trị. Vậy phe nào sẽ chiến thắng trong cuộc bầu chọn tổng thống sắp tới? Câu trả lời sẽ có vào tháng 11 này[12]!

Tình huống trong hệ của chúng ta sẽ phức tạp hơn một chút khi thêm một đại lượng ngoại lực ngẫu nhiên (nhiễu loạn) vào phương trình. Đó là kết quả của chẳng hạn sự chuyển động nhiệt của các phân tử không khí bao quanh các hạt cườm trong chuỗi. Khi các phân tử khí tác động qua lại với nhau, ta có thể mô tả tương tác giữa chúng bằng một khái niệm gọi là *tiếng ồn trắng thời gian*[13], mà tác động của nó tới hệ tại những thời điểm khác nhau là độc lập với nhau.

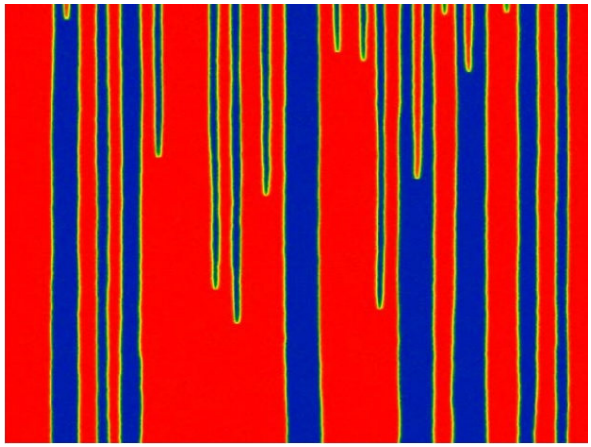
Khi ta đi đến một giá trị tới hạn mà số hạt trên chuỗi tiến ra vô cùng, tiếng ồn trắng khi đó trở thành *tiếng ồn trắng không-thời gian*[14]. Nó tác động một cách độc lập tại những thời điểm và vị trí khác nhau. Chúng ta vì vậy đang đối mặt một SPDE, vì đã thêm vào một đại lượng tương ứng với tiếng ồn để mô tả một hệ vô hạn: đó là phương trình Allen - Cahn ngẫu nhiên. Chúng ta sẽ thấy rằng tiếng ồn này, *hoàn toàn không chính quy*[15] trong các điều kiện của ta, đã cản trở việc tìm nghiệm của phương trình khi chiều lớn hơn hay bằng 2.

[12]Một ví dụ minh hoạ rõ nét khác và vẫn còn nóng hổi là cuộc trưng cầu dân ý về việc ở lại hay rời liên minh châu Âu của người Anh ngày 23 tháng 6 vừa rồi. Sau khi có kết quả kiểm phiếu với chiến thắng cho phe Brexit, rất nhiều người dân tỏ ra hối hận vì đã để lá phiếu của họ bị ảnh hưởng bởi những người xung quanh!

[13]temporal white noise

[14]spatiotemporal white noise

[15]highly irregular



Hình 4: *Bài toán sự tách pha từ mô hình các hạt cườm nảy sinh nhiều câu hỏi thú vị. Hình dạng, kích thước của các nhóm hạt cùng loại (tức các vùng cùng màu) thay đổi như thế nào theo thời gian? Liệu mặt phân cách giữa các nhóm cuối cùng có biến mất? Có thể mô tả được chuyển động của các bề mặt phân cách này theo thời gian? Lược đồ không-thời gian sẽ cho một câu trả lời. Không gian là bề ngang, thời gian là bề dọc từ cao xuống thấp. Các vị trí hạt cườm được đánh dấu bởi màu sắc như trên hình. Tại các điểm trên các phần "mõm" nhô ra sẽ xảy ra xung đột giữa các mặt phân cách, kéo theo sự biến mất dần của chúng.*

Tetris và mặt phân cách

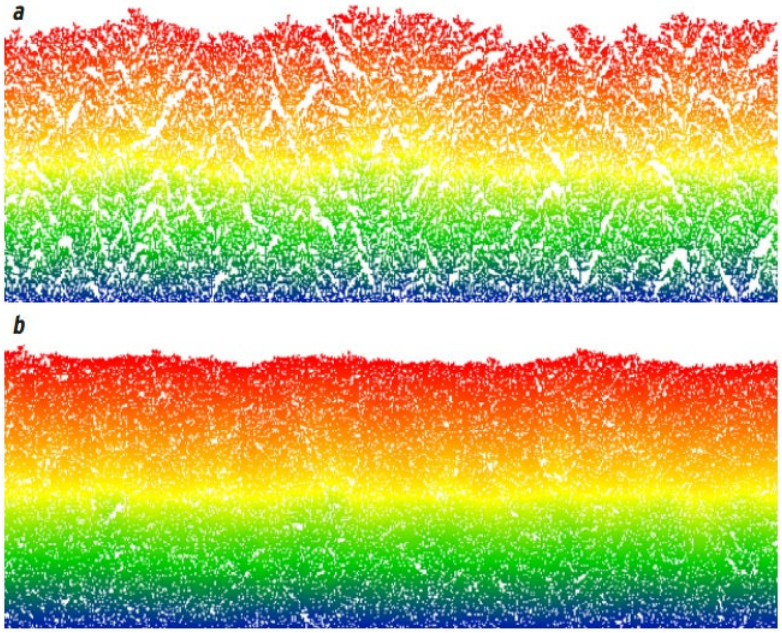
Một ví dụ khác về SPDE là khi ta phun các phân tử lên một vật chất nền, được sử dụng chẳng hạn trong công nghệ chế tạo vật liệu bằng kĩ thuật *epitaxy*[16] cho các thiết bị điện tử. Để mô hình hóa quá trình này, hãy bắt đầu nguồn cảm hứng từ một dạng biến thể của nó là trò chơi Tetris. Xét trong không gian một chiều với một vật thể làm nền đặt nằm ngang cho trước. Các phân tử tạm coi là những hình vuông nhỏ, rơi thẳng từ một vị trí ngẫu nhiên từ trên xuống. Quy luật là khi hình vuông chạm vào nền, hoặc chạm vào một hình vuông khác bên cạnh hay bên dưới nó, nó sẽ không di chuyển được nữa. Tuy nhiên, các hình vuông có thể, với một xác suất nhỏ, di chuyển sang hai bên một khi nó xuất hiện. Câu hỏi là, làm thế nào biết được mức độ gồ ghề trên bề mặt của các vật liệu được sản xuất như vậy? (Xem Hình 5).

Vào năm 1986, Mehran Kardar, Giorgio Parisi và Yi-Cheng Zhang đã thiết lập được một SPDE mô tả quá trình tới hạn nhận được khi kích cỡ hình vuông tiến dần về 0 (xem Phụ lục 2). Phương trình này, được kí hiệu là KPZ, từ chữ cái đầu của tên ba tác giả, chứa các đại lượng của phương trình truyền nhiệt, mô tả sự chuyển động của các phân tử phun vào, cũng như một tiếng ồn trắng không-thời gian và một đại lượng phi tuyến đặc trưng bởi hình dạng của bề mặt nền phân cách. Thật không may, phương trình này lại *không đặt chỉnh*[17] do tính không chính quy của đại lượng tiếng ồn, và cho đến gần đây chúng ta đã không thể đưa ra được một lời giải có ý nghĩa toán học nào cho nó.

Để hiểu được bài toán, chúng ta phải lượng hóa tính không chính quy của các đại lượng có trong phương trình. Chúng ta có thể liên kết mỗi hàm f với một số r mà càng lớn khi hàm càng trơn.

[16] tạm dịch là kĩ thuật *cấy ghép*, một kĩ thuật cho phép chế tạo màng mỏng đơn tinh thể có độ tinh khiết rất cao, thực hiện trong môi trường chân không siêu cao, được phát minh vào những năm 60 của thế kỉ XX

[17] ill-posed



Hình 5: *Một sự đơn giản hóa của trò chơi Tetris. Việc phun các phân tử lên bề mặt vật liệu nền có thể mô hình hóa bởi một quá trình tăng trưởng ngẫu nhiên. Ở đó các phân tử được biểu diễn bởi các hạt hình vuông rơi xuống một vị trí ngẫu nhiên trên mặt phẳng nằm ngang, tương tự trò chơi Tetris. Mỗi hạt sẽ dừng lại khi nó chạm vào hạt khác. Hơn nữa, các hạt ở trên cao có thể di chuyển sang hai bên với một xác suất nhỏ. Độ thô ráp của bề mặt tăng lên khi xác suất này giảm xuống: bề mặt ở hình (a) thô hơn hình (b).*

Nếu đồ thị của hàm số có tiếp tuyến tại mọi điểm thì r lớn hơn hoặc bằng 1. Hơn nữa nếu tại mọi điểm của f ta đều xác định được một độ cong, thì r ít nhất bằng 2. Nếu f chính quy bậc r, thì các đạo hàm riêng của f chính quy bậc $r-1$. Một cách ngược lại, nghiệm của phương trình truyền nhiệt cưỡng bức bởi f có bậc chính quy cao hơn r.

Phương trình không đặt chỉnh

Bậc chính quy r không nhất thiết phải là một số nguyên. Chẳng hạn chuyển động Brown, mô tả quỹ đạo hỗn loạn của một hạt phấn hoa giữa những hạt khác trong nước, có bậc chính quy nhỏ hơn $1/2$ một chút[18]. Các quỹ đạo của chuyển động Brown là không khả vi (chúng không có tiếp tuyến tại bất cứ điểm nào). Tuy nhiên, người ta có thể định nghĩa đạo hàm của chúng theo nghĩa phân phối.

Phân phối[19], một đối tượng tổng quát hơn hàm số, là một lí thuyết được phát triển vào nửa đầu thế kỉ XX bởi các nhà toán học Jacques Hadamard, Salomon Bocher, Sergei Sobolev và Laurent Schwartz. Thay vì xác định giá trị của phân phối tại một điểm cụ thể, ta xác định giá trị trung bình của nó trong một lân cận nhỏ xung quanh điểm nó. Một số toán tử đại số được định nghĩa

[18] thực tế thì có thể xem nó là một số tùy ý nhỏ hơn và gần bằng $1/2$

[19] distribution, còn gọi là hàm suy rộng

trên hàm phân phối: chúng ta có thể chẳng hạn thực hiện phép cộng và phép lấy đạo hàm chúng. Tuy nhiên, nhìn chung ta không thể thực hiện phép nhân hai phân phối.

Tiếng ồn trắng thời gian có thể xem như đạo hàm theo nghĩa phân phối của một quỹ đạo Brown, với bậc chính quy hơi bé hơn một chút so với $-1/2$ (chúng ta sẽ coi rằng giá trị này gần như bằng $-1/2$). Tiếng ồn trắng không-thời gian, trong khi đó, có bậc chính quy phụ thuộc vào chiều của không gian. Giá trị này xấp xỉ $-3/2$ trong không gian một chiều, xấp xỉ -2 trong không gian hai chiều, và xấp xỉ $-5/2$ trong không gian ba chiều. Đây là nơi chúng ta sẽ tìm ra lời giải của bài toán.

Thật vậy, chúng ta chứng minh được rằng nghiệm Y_0 của phương trình truyền nhiệt cưỡng bức bởi một tiếng ồn trắng có bậc chính quy lớn hơn 2 đơn vị, cụ thể là xấp xỉ $1/2$, xấp xỉ 0 hoặc xấp xỉ $-1/2$ tùy theo số chiều của không gian.

Quá trình lặp Picard áp dụng cho phương trình Allen - Cahn yêu cầu tính toán, ở bước thứ hai, đại lượng $Y_0 - Y_0^3$. Trong không gian chiều 1, Y_0 có bậc chính quy dương, vấn đề không đáng ngại. Với không gian chiều 2 hoặc 3, Y_0 lúc này là một phân phối từ việc nó có bậc chính quy âm. Như chúng ta đã biết, không thể thực hiện phép nhân các phân phối, đại lượng Y_0^3 trở nên vô định, và quá trình lặp do đó không thể thực hiện được. Phương trình KPZ, cũng vậy, chứa bình phương đạo hàm của Y_0. Đạo hàm này có bậc chính quy âm thậm chí với chiều không gian 1, phép lặp Picard không thể áp dụng cho phương trình KPZ.

Tái chuẩn hóa và lí thuyết cấu trúc chính quy

Đến lúc này, chúng ta có thể tự hỏi rằng liệu có thực sự nên đâm đầu vào các bài toán SPDE không đặt chỉnh như vậy? Thực tế, trong hai ví dụ mà ta đã thảo luận, chúng ta đã bắt đầu với một mô hình rời rạc với một số hữu hạn các đối tượng (các hạt cườm hay các hình vuông), chúng đương nhiên là hoàn toàn xác định. Vấn đề chỉ xuất hiện khi ta chuyển qua giới hạn khi cho kích thước của các đối tượng này tiến dần một cách liên tục về 0.

Tuy nhiên ta sẽ thấy rằng việc đâm đầu vào nó là không vô ích, và lí do cho những việc làm này của chúng ta đến từ khái niệm về tính phổ quát. Mô hình rời rạc của sự phát triển của bề mặt phân giới là một trường hợp đặc biệt giữa rất nhiều mô hình có thể có. Chúng ta tuy vậy biết rằng một lượng lớn các mô hình này bị điều chỉnh, trong diện rộng, bởi phương trình KPZ. Đây chính là một đặc tính phổ quát, và sự hiểu biết về nó sẽ làm sáng tỏ cùng một lúc toàn bộ các mô hình cùng loại.

Bài toán giới hạn liên tục đã và đang xuất hiện trong vật lý lượng tử, nơi nó được gọi là sự phân kì *tia tử ngoại*[20]. Thực tế, phương trình Allen - Cahn tương đương một cách hình thức với một mô hình của lí thuyết trường, gọi là mô hình Φ^4. Từ những năm 1930, các nhà vật lý đã đề xuất việc giải bài toán này bằng một phương pháp gọi là *tái chuẩn hóa*[21]. Ý tưởng là đưa vào các tham số của *lí thuyết tỉ lệ*[22] mà trên đó hệ có thể quan sát được.

[20] ultraviolet, còn gọi là tia cực tím, hay tia UV
[21] renormalization
[22] scaling theory

Trong trường hợp phương trình Allen - Cahn, phương pháp này là làm cho phần sườn giữa chõm và rãnh tấm tôn ngày càng dốc khi khoảng cách giữa các hạt cườm giảm dần (xem Hình 2). Với sự lựa chọn thích hợp độ cong của phần chõm, ta nhận được một phương trình *đặt chỉnh*[23] tại trường hợp tới hạn. Điều lấn cấn duy nhất còn lại của quy trình này là nó được thiết đặt hoàn toàn dựa trên các tính toán hình thức mà không có một lập luận toán học chính xác nào.

Tuy nhiên, vào năm 1997, Lorenzo Bertini và Giambattista Giacomin, bằng việc sử dụng phép đổi biến rất khéo léo, đã đạt được một kết quả chứng minh sự hội tụ của mô hình sự phát triển của bề mặt phân cách đến một dạng tái chuẩn hóa của phương trình KPZ. Sau đó, vào năm 2003, Giuseppe da Prato và Arnaud Debussche đã có thể chứng minh được sự tồn tại nghiệm cho phương trình Allen - Cahn tái chuẩn hóa hai chiều. Chỉ còn một khiếm khuyết duy nhất, các kĩ thuật này không sử dụng được nữa trong không gian chiều ba.

Đóng góp quan trọng của Martin Hairer là phát triển một lí thuyết cho phép xử lí một cách có hệ thống một lượng lớn SPDE cổ điển không đặt chỉnh. Nó không những cho phép tìm lại các kết quả đã biết cho phương trình KPZ và phương trình Allen - Cahn hai chiều, mà còn áp dụng được cho phương trình Allen - Cahn ba chiều và nhiều phương trình khác.

Khái niệm trung tâm của lý thuyết này là *cấu trúc chính quy*[24]. Cùng với phương pháp tái chuẩn hóa, nó cho phép xây dựng một không gian mà trong đó các phép lặp Picard vẫn hoạt động tốt. Nét đẹp cũng như sức mạnh của lí thuyết là nó cung cấp một lược đồ tổng quát, cho phép xử lí một cách có hệ thống các phương trình thay vì tìm kiếm từng lời giải riêng rẽ. Lí thuyết này là một trong những bước tiến quan trọng hướng tới việc chứng minh một số bài toán mở liên quan đến tính phổ quát, và chúng ta có thể hi vọng vào những tiến bộ mạnh mẽ hơn trong tương lai.

Phụ lục

1 Phương trình truyền nhiệt. Nhiệt độ $T(x,t)$ tại điểm x và thời gian t của thanh kim loại được xác định bởi phương trình $\partial T/\partial t = D\partial^2 T/\partial x^2$ ở đó D là hệ số dẫn nhiệt. Trong phương trình này, số hạng bên trái, đạo hàm riêng của hàm nhiệt độ T đối với biến thời gian t (khi xem x như hằng số), mô tả tốc độ biến đổi của nhiệt độ. Số hạng bên phải, đạo hàm riêng cấp hai của hàm nhiệt độ đối với biến không gian, đặc trưng cho tính không đồng nhất của vật liệu. Hàm $G(x,t) = e^{-x^2/4DT}/\sqrt{4\pi Dt}$ là một nghiệm riêng của phương trình, với việc lí tưởng hóa thanh kim loại dài vô hạn.

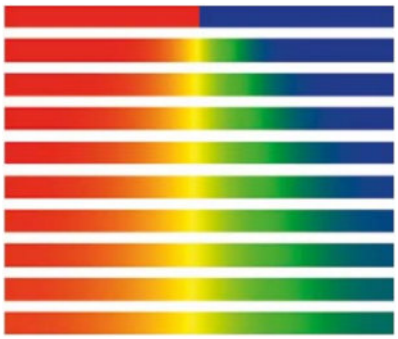
Khi cố định thời gian, G là một đường cong Gauss có dạng hình chuông, một đối tượng đóng một vai trò nền tảng trong lí thuyết xác suất. Bề rộng của chuông, tỉ lệ với $\sqrt{Dt}$, tăng lên theo thời gian, nhưng bằng 0 tại 0. Nghiệm này cho ta biết rằng, nhiệt độ ban đầu bằng 0 ở mọi nơi trừ điểm 0, điểm nguồn nơi mà thanh kim loại được tiếp xúc nguồn nhiệt. Nếu điểm nguồn là một điểm y nào đó, thì nghiệm sẽ được cho bởi $G(x-y,t)$.

Nguyên lí chồng chất nghiệm, một tính chất của phương trình truyền nhiệt, chỉ ra rằng nghiệm tổng quát của phương trình truyền nhiệt viết được dưới dạng $T(x,t) = \int G(x-y,t)T(y,0)dy$.

[23] well-posed
[24] regularity structure

Nếu thay thanh kim loại bởi một đĩa kim loại hai chiều, hàm nhiệt độ sẽ là $T(x, y, t)$ với hai biến tọa độ không gian x và y và biến thời gian t. Phương trình lúc này có dạng $\partial T/\partial t = D\Delta T$ với ΔT là tổng đạo hàm riêng cấp hai của T đối với x và y (toán tử Laplace). Phương trình nhiệt ba chiều có dạng tương tự, với ba tọa độ không gian.

Một tính chất khác của phương trình truyền nhiệt là tính chính quy (xem Hình 6).



Hình 6: *Sự lan truyền đều đặn của nhiệt độ. Ban đầu, nhiệt độ nửa trái thanh sắt đang ở mức cao (màu đỏ), trong khi nửa phải đang ở nhiệt độ phòng. Sai khác này mất dần khi nhiệt độ lan dần ra toàn thanh, và không có bước nhảy nhiệt độ trong thanh trừ thời điểm ban đầu.*

2 Phương trình Allen - Cahn và phương trình KPZ. Phương trình Allen - Cahn ngẫu nhiên mô tả sự tách pha có thể viết dưới dạng $\partial Y/\partial t = D\Delta Y + Y - Y^3 + \xi$. Ở đây ΔY biểu thị liên kết giữa mỗi hạt cườm với các hạt lân cận với nó thông qua lò xo. Đại lượng $Y - Y^3$ đặc trưng cho lực tổng hợp giữa trọng trường và phản lực của tấm tôn, là nguyên nhân làm cho hạt cườm có xu hướng chạy về các vị trí $Y = 1$ và $Y = -1$. Số hạng cuối cùng ξ mô tả tiếng ồn trắng không-thời gian, một ngoại lực ngẫu nhiên mà sự tác động của nó tại các thời điểm và vị trí khác nhau tới phương trình là độc lập với nhau.

Phương trình KPZ mô tả sự phát triển của một bề mặt phân cách, đặc trưng bởi hàm cao độ của nó $h(x, t)$ tại điểm x và thời gian t, có dạng $\partial h/\partial t = D\partial^2 h/\partial x^2 + (1/2)(\partial h/\partial x)^2 + \xi$. Số hạng đầu tiên bên tay phải xuất hiện do sự hoán đổi vị trí của các phân tử cạnh nhau. Tiếng ồn trắng không-thời gian ξ mô tả ngoại lực ngẫu nhiên tác động lên chúng. Hạng tử cuối cùng $(\partial h/\partial x)^2$ đến từ thực tế rằng mặt phân cách không nhất thiết phải phát triển theo phương thẳng đứng, mà còn theo phương vuông góc với chính nó. Giá trị này nhận được bằng cách chiếu tốc độ phát triển của bề mặt lên phương thẳng đứng, kết hợp với định lí Pythagoras và một số phép xấp xỉ những giá trị nhỏ.

3 Lí thuyết cấu trúc chính quy. Lí thuyết phát triển bởi Martin Hairer được lấy cảm hứng từ một khái niệm gọi là *đường thô*[25] do Terry Lyons đưa ra vào năm 1998 và mở rộng bởi Massimiliano Gubinelli. Nó có thể xem như một sự tổng quát hóa của chuỗi Taylor, cho phép xấp xỉ các hàm đủ trơn bởi các đa thức. Chẳng hạn, khai triển Taylor bậc hai của hàm f tại x được cho bởi $f(y) = f(x) + c_1(x)(y - x) + c_2(x)(y - x)^2 + r(x, y)$, ở đó phần dư $r(x, y)$ tiến đến 0 khi y tiến dần về x. Các hệ số $c_1(x), c_2(x)$ phụ thuộc vào f, chẳng hạn $c_1(x)$ là đạo hàm của f tại điểm x. Kiểu khai triển này thường được sử dụng để xác định nghiệm của một phương trình vi phân gần một điểm cụ thể cho trước.

Lí thuyết của Martin Hairer cho phép có nhiều đối tượng trừu tượng phức tạp hơn đa thức trong khai triển Taylor của nghiệm. Các đối tượng này bao gồm chẳng hạn nghiệm Y_0 của phương trình truyền nhiệt cưỡng bức bởi tiếng ồn trắng không-thời gian. Thay vì xem xét phương trình gốc, chúng ta nghiên cứu các phương trình thỏa mãn tất cả các hệ số trong khai triển Taylor.

[25] rough paths

Phương pháp xấp xỉ liên tiếp Picard cho phép chứng minh sự tồn tại nghiệm trong không gian của các hệ số này. Cuối cùng, một định lí xây dựng lại liên kết một phân phối với nghiệm này. Định lí này sử dụng lí thuyết sóng nhỏ *wavelet*, một lí thuyết cũng được áp dụng nhiều trong kĩ thuật rửa ảnh, bao gồm cả ảnh kĩ thuật số.

4 Một phiên bản trước của bài viết này tựa đề *Qu'est-ce qu'une Équation aux Dérivées Partielles Stochastique?*[26] (có một số điểm khác, đặc biệt có nhiều video minh họa), đã được đăng trên *Images des Mathématiques* (một tạp chí toán học online của Trung tâm Nghiên cứu Khoa học Quốc gia Pháp - CNRS, trình bày các nghiên cứu toán học ra đại chúng bằng từ ngữ và hình ảnh, với mục tiêu *tất cả bài viết được viết bởi các nhà toán học nhưng không có bài viết nào được viết dành cho các nhà toán học!*), có thể đọc online tại địa chỉ http://images.math.cnrs.fr.

Tài liệu

[1] M. Hairer, A theory of regularity structures, *Inventiones Mathematicae*, vol. 198, pp. 269-504, 2014.

[2] G. Da Prato and A. Debussche, Strong solution to the stochastic quantization equations, *Ann. Probab.*, vol. 31, pp. 1900-1916, 2003.

[3] L. Bertini and G. Giacomin, Stochastic Burgers and KPZ equations from particle systems, *Comm. Math. Phys.*, vol. 183, pp. 571-607, 1997.

[4] M. Kardar *et al.*, Dynamic scaling of growing interfaces, *Physical Review Letters*, vol. 56, pp. 889-892, 1986.

[26] do tác giả bài viết gửi cho người dịch

HỌC CÁCH HỌC: MỘT BÀI HỌC QUAN TRỌNG BẬC NHẤT ĐANG BỊ BỎ QUÊN

Dương Trọng Tấn

Hình 1: *Khi giải một bài toán, não sẽ tập trung với số ít các tế bào thần kinh.*

Nếu bạn gặp một bài toán khó, dù cố gắng nhiều mà giải mãi không xong, thì làm thế nào? Câu trả lời phổ biến nhất là cố gắng tìm ra chỗ sai trong lập luận rồi đi tiếp hoặc "*làm lại từ đầu*". Cả hai phương án theo kinh nghiệm này không phù hợp với những lời khuyên của các chuyên gia về não bộ.

Theo họ, não bộ của chúng ta hoạt động theo hai cơ chế khác nhau: tập trung (focused mode) và thư giãn (diffused mode). Khi ta tập trung cao độ vào giải quyết một bài toán, não sẽ vào cuộc sử dụng cơ chế tập trung với số ít các tế bào thần kinh tại một vùng tập trung của não bộ được huy động. Khi ta rơi vào thế bí như tình huống đã dẫn, thì dù có cố gắng đến mấy, cũng chỉ có vùng não tập trung được hoạt động. Có nghĩa là chúng ta có xu hướng lặp đi lặp lại các cách giải quyết vấn đề, và khó lòng thoát ra khỏi bế tắc. Khi đó hành động rà soát lại lời giải hay đi lại từng bước từ đầu không có ích gì mấy. Như thiên tài Albert Einstein từng nhận xét đại ý "*bạn không thể giải bài toán theo* 1000 *cách giống nhau rồi hy vọng có lời giải khác!*". Trong những lúc bí bách như thế này, cách tốt nhất là tạm rời xa bài toán đấy, đi chơi, thư giãn rồi hẵng quay lại với bài toán. Đây không phải là lời xúi bậy vô trách nhiệm. Việc bạn tạm rời bài toán đó để đi bộ, hóng gió, hoặc ngồi thiền ít phút sẽ giúp não bộ chuyển sang chế độ thư giãn, lúc này các vùng khác của não bộ được kích hoạt. Nếu quay trở lại giải toán, bạn sẽ có khả năng tìm ra một con đường khác, không bế tắc như lúc đầu.

Trên đây chỉ là một trong hàng tá ví dụ cho thấy những nghiên cứu về não bộ có thể giúp cải thiện đáng kể cách thức chúng ta học tập và làm việc. Tuy nhiên, bấy lâu nay chúng ta vẫn không mấy khi nghĩ về việc tìm hiểu các kiến thức loại này để cải thiện cách học tập, vì chúng ta thường phó mặc cho thói quen sai khiến trong các hoạt động của mình.

Có thể dẫn ra đây một thói quen tai hại khác vẫn chiếm chỗ trong trường học của chúng ta: Các bài giảng dài. Bạn có thể gặp ở bất kì trường học nào các tiết học kéo dài từ 45 phút tới vài tiếng. Bạn cũng dễ dàng bắt gặp cảnh tượng hàng tá học sinh lơ đãng, ngủ gật, hoặc ngồi làm việc riêng trong lớp vì không thể chú tâm vào bài giảng. Trong khi hầu hết các giáo viên đổ lỗi cho các cô cậu học trò, thì các chuyên gia não bộ có một lời giải thích đơn giản cho hiện tượng này:

Não chúng ta chỉ có khả năng chú tâm suy nghĩ trong một thời gian rất ngắn, chừng 10 phút[1], sau đó là sẽ đến giai đoạn mất tập trung. Đây là cơ chế phòng vệ hết sức tự nhiên của não người, vì vậy hãy phân chia các bài giảng thành từng phân đoạn ngắn hơn. Sau mỗi 10 phút tập trung, hãy thiết kế một hoạt động để thư giãn và chuyển đổi sang phân đoạn tiếp theo. Thực ra đã từ lâu người ta đã biết dùng kĩ thuật phân giờ Pomodoro với các quy tắc đơn giản kể trên để gia tăng đáng kể năng suất làm việc và học tập.

Một nghiên cứu đăng trên Psychological Science in the Public Interest năm 2013[2] cho thấy, những phương pháp học tập được sử dụng phổ biến trong nhà trường như "*tóm tắt nội dung bài giảng*", "*dùng bút đánh dấu đoạn văn bản quan trọng khi đọc sách*", "*đọc đi đọc lại một chương sách*" hoá ra lại là những cách không mang lại mấy hiệu quả về ghi nhớ. Có những cách khác hữu hiệu hơn nhiều để giúp gia tăng hiệu quả học tập như: tích cực làm các bài luyện tập, hay học tập các kiến thức theo hình thức luyện tập phân tán với các khối kiến thức được chia nhỏ và học tập qua thời gian đủ dài.

Nhìn từ những tình huống kể trên, trường học hiện nay có vẻ đang phí phạm rất nhiều thời gian của học trò chỉ vì ưa thích kinh nghiệm mà ít quan tâm tới việc tìm hiểu và vận dụng các kiến thức khoa học về việc con người học tập như thế nào để từ đó xây dựng các hoạt động giáo dục cho tối ưu.

Chúng ta có thể liên hệ việc học tập như câu chuyện cái cần câu và con cá. Cách dạy truyền thống phổ biến hiện nay là dạng cho đi con cá, trong khi nếu ta trang bị năng lực tự học cho học sinh thì tức là cho họ một cái cần câu để tự lập suốt đời.

Sự thiếu vắng những bài học liên quan đến việc rèn luyện kĩ năng học tập sẽ mang lại hậu quả mà chúng ta đã được chứng kiến là những thế hệ học trò thụ động chỉ biết trông chờ kiến thức và chân lý từ giáo viên và những người đi trước mà không để chủ động tự mình xây dựng tri thức cho mình. Điều này càng trở nên tai hại trong bối cảnh thời đại tri thức và số hóa hiện nay khi mà lượng thông tin mỗi năm tăng trưởng theo cấp số mũ. Kiến thức ngày hôm nay còn đúng, ngày mai có thể đã sai đi nhiều. Chỉ có cách làm chủ việc học như thế nào mới giúp học sinh đứng vững trong thế giới ngày nay. Thế cho nên, nhiều nhà giáo hiện nay đã thừa nhận rằng tiêu chuẩn xóa mù hiện nay không chỉ là biết đọc biết viết mà còn phải thạo cách tự học. Nhìn theo hướng này, chúng ta có thể dễ dàng đồng tình với nhận định của cha đẻ phương pháp Bản đồ Tư duy Tony Buzan: "*Kĩ năng tự học là kĩ năng quan trọng nhất mà một người có thể sở hữu*".

Thật may mắn là chúng ta có thể tìm thấy những sáng kiến mới trong một số chương trình giáo dục có để ý tới việc rèn luyện năng lực tự học trong chương trình giáo dục. Như sáng kiến Khung Kỹ năng thế kỷ XXI (p21.org) đã xếp kĩ năng học tập và sáng tạo thành một trong bốn hạng mục chính trong các năng lực cốt lõi mà học sinh thế kỉ XXI này phải thành thục.

Hay như nhóm Cánh Buồm chủ trương xây dựng chương trình giáo dục tiểu học hiện đại xoay quanh tư tưởng chủ đạo với một từ duy nhất: tự học. Theo đó học sinh được rèn luyện phương pháp học tập từ tiểu học. Kết thúc bậc tiểu học, trẻ em có được năng lực tự học vững vàng để sang bậc học cao hơn các em sẽ sử dụng năng lực ấy để tự mình đến với tri thức thay vì phụ

[1]Medina, J. (2011). Brain Rules: 12 Principles for Surviving and Thriving at Work, Home, and School (Large Print 16pt). `ReadHowYouWant.com`

[2]Dunlosky, J., Rawson, K. A., Marsh, E. J., Nathan, M. J., & Willingham, D. T. (2013). Improving students' learning with effective learning techniques promising directions from cognitive and educational psychology.Psychological Science in the Public Interest, 14(1), 4-58

thuộc vào sự truyền tải thông tin một chiều từ nhà trường. Nhóm Cánh Buồm xác quyết: "*Giáo dục tức là tự giáo dục, tự làm ra chính mình!*". Nhóm đã đi xa hơn việc tuyên ngôn vài bước với sự quy trình hóa kĩ thuật để trẻ em thực sự xây dựng được phương pháp học cho mình.

Người xưa có câu, phàm phải trong tình huống khó lường thì "*lấy bất biến ứng vạn biến*". Đối với việc học tập, cái bất biến là phương pháp tự học, cái vận động không ngừng là tri thức của thời đại. Không gì bằng trang bị cho được cái bất biến đó để người học của thế kỉ 21 có thể tự mình đi trên đôi chân tự do khám phá cánh đồng tri thức của nhân loại trong suốt cuộc đời. Thiếu kĩ năng thiết yếu này thì những khẩu hiệu rổn rảng về xã hội học tập, hay học tập suốt đời chỉ cùng lắm là những lời nói cho sang miệng. Bài học về cách học cần phải là bài học căn cơ nhất mà mỗi học sinh cần phải được luyện rèn.

LEONHARD EULER - NGƯỜI THẦY VĨ ĐẠI

Nguyễn Đức Hưng

GIỚI THIỆU

Euler là một nhà toán học, vật lý học, thiên văn học vĩ đại. Ông là người đã đặt nền móng cho không biết bao nhiêu lý thuyết sâu sắc giúp giải quyết cho rất rất nhiều các bài toán thực tế và quả thật ông là một người thầy vĩ đại của tất cả chúng ta. Bài viết này giới thiệu giản lược về cuộc sống của ông và tóm tắt các công trình của ông.

Kỳ 1 : Cuộc sống thăng trầm của Euler

Thời niên thiếu

Leonhard Euler sinh ngày 15/04/1707 và là con trai cả của Paulus Euler và Margaretha Brucker. Khi mới sinh Euler, cha của ông là Paulus khi ấy còn đang là một cha xứ tại nhà thờ thánh Jakob ngoại ô Basel. Mặc dù là một cha xứ nhưng ông lại rất yêu thích Toán học, vì vậy trong hai năm đầu đại học, ông đã đăng ký để được học các môn Toán với nhà Toán học nổi tiếng Jakov Bernuly. Sau đó, gia đình Euler chuyển tới Riehen, một vùng ngoại ô của thành phố Basel, tại đây cha của Euler đã trở thành mục sư Tin Lành của giáo xứ địa phương cho tới cuối đời.

Năm 8 tuổi Euler được gửi tới trường Latin để học tập, nhưng trước đó Euler đã được học Toán và các kiến thức khác từ cha của mình. Trong thời gian học ở trường Latin, Euler sống cùng với bà ngoại và học thêm với gia sư Johannes Burckhardt, một nhà Thần học trẻ tuổi và đặc biệt say mê Toán học. Tháng 10/1720, ở tuổi mười ba [1] Leonhard theo học tại Đại học Basel với chuyên ngành Triết học, đồng thời đăng ký học phần toán sơ cấp và được chính Johann Bernoulli [2] giảng dạy. Bằng sự đam mê và nhiệt huyết của mình trong việc học tập mà chàng trai trẻ Leonhard nhanh chóng được Bernoulli để ý và khuyến khích Leonhard học tập và nghiên cứu Toán học. Năm 1723, Euler tốt nghiệp thạc sĩ và có một bài giảng đại chúng [3] với chủ đề "*so sánh triết học Descart và triết học Newton*".

Năm 19 tuổi, Euler đã giành được một giải thưởng từ Viện Hàn lâm Khoa học Paris với lý thuyết về vị trí tối ưu của cánh buồm trên các con tàu. Điều đặc biệt là trong suốt quãng thời gian trước đó, Euler hầu như không thấy một con tàu nào. Một năm sau, khi chiếc ghế giáo sư vật lý tại Đại

[1] 13 tuổi Leonhard vào đại học không phải là điều bất thường vào thời điểm đó.

[2] Là một nhà Toán học nổi tiếng với khái niệm vô hạn. Ông cũng là em trai của Jakob Bernoulli thầy của cha Leonhard.

[3] Bài giảng bằng tiếng Latin.

Hình 1: Chân dung Euler, hiện được treo ở Bảo tàng Mỹ thuật Basel.

học Basel bị khuyết, Euler đã được Johann Bernoulli hỗ trợ rất nhiều để có thể ngồi vào vị trí này, nhưng thất bại, cũng dễ hiểu bởi khi đó Euler còn quá trẻ và thiếu các nghiên cứu được công bố rộng rãi. Sau thất bại này, Euler nhận lời mời từ Viện Hàn lâm Khoa học ở St.Petersburg, mới được thành lập vài năm trước đó bởi Nga Hoàng Peter I (căn nguyên của lời mời này xuất phát từ Johann Bernoulli và hai con trai của ông bởi tất cả đã từng làm việc tại đây).

Bước chuyển lớn

Đầu năm 1727, Euler chuyển tới St.Petersburg. Tại đây ngoài việc nghiên cứu Toán, Euler còn tham vấn cho Nga về các câu hỏi khoa học và công nghệ trong bài kiểm tra trong các kỳ thi dành cho thiếu sinh quân Nga.

Khác biệt với các nghiên cứu viên nước ngoài tại viện, Euler nhanh chóng thích nghi với điều kiện sống khắc nghiệt ở Bắc Âu và đồng thời Euler cũng nhanh chóng học và sử dụng thành thạo tiếng Nga để phục vụ cho đời sống và các nghiên cứu của mình. Trong thời gian này, Euler sống cùng với Daniel Bernoulli và trở thành bạn thân của Christian Goldbach [4], thư ký của Viện. Những trao đổi giữa Euler và Goldbach đã trở thành những cứ liệu quan trọng cho lịch sử khoa học thế kỷ XVIII.

Khoảng thời gian ở Viện là khoảng thời gian Euler làm việc hiệu quả và sáng tạo nhất, ông đã cho ra nhiều kết quả đặc biệt và chúng đã mang lại cho ông vị trí và sự nổi tiếng tại Viện và trên toàn thế giới sau này.

Tháng 1/1734, Euler kết hôn với Katharina Gsell, con gái của một họa sĩ Thụy Sĩ cũng đang giảng dạy trong Viện. Cuộc sống gia đình của Euler không hề suôn sẻ như công việc của ông tại Viện, họ có tới 13 người con nhưng chỉ có 5 trong số đó là phát triển khỏe mạnh, trong đó có

[4]Christian Goldbach nhà Toán học người Đức, ông nổi tiếng với giả thuyết Goldbach mà cho tới ngày nay vẫn còn đang là một bài toán chưa có lời đáp.

một người trở thành một nhà Toán học và là trợ lý của ông sau này. Năm 1735 ông bệnh nặng, và tưởng như không qua khỏi. Một phép màu đã giúp ông vượt qua nó, nhưng suốt ba năm sau đó bệnh tật tiếp tục hành hạ Euler và lần này nó khiến ông mất con mắt bên phải (có thể nhận thấy rất rõ điều này qua những bức chân dung của Euler từ khoảng thời gian này).

Cùng với thời điểm cuộc khủng hoảng chính trị ở Nga năm 1740, gây ra cái chết của nữ hoàng Nga Anna Ivanovna, Euler nhận được lời mời từ Quốc vương Phổ Frederick II đến Berlin để giúp thành lập Viện Hàn lâm Khoa học tại đây và ông đã quyết định rời St. Petersburg. Thêm nữa, ông cũng đã viết trong hồi ký của mình như sau: "... *năm* 1740, *khi Nhà vua Phổ bắt đầu lên nắm quyền hành, tôi nhận được một lời mời từ Berlin, và tôi nhận lời không chút ngần ngại, sau khi nữ hoàng Anne bị sát hại và kéo theo đó là sự trì trệ của vương triều* ..."

Tháng 6/1741, Euler cùng với vợ và hai người con của mình khi ấy là Johann Albrecht sáu tuổi và Karl mới một tuổi rời St. Petersburg để tới Berlin.

Thời ở Berlin 1741 - 1766

Một khởi đầu có vẻ không thuận lợi như Euler nghĩ, vì còn dang dở cuộc chiến ở Silesia, Frederick II chưa thể tập trung cho việc xây dựng viện, vì thế mãi tới tận 1746 viện mới chính thức ra đời. Viện trưởng là nhà toán học Pháp, còn Euler phụ trách ngành Toán. Trong suốt thời gian dài chờ đợi, Euler đã hoàn thành cuốn hồi ký viết tới 200 lá thư cùng năm bài luận lớn.

Tuy phải đảm trách rất nhiều công việc tại Viện từ quản lý đài thiên văn, vườn bách thảo, làm việc trực tiếp với nhân viên, nghiên cứu viên, thậm chí đảm trách cả việc bán những cuốn niên giám để đảm bảo nguồn thu cho Viện, nhưng không vì vậy mà năng suất làm Toán của Euler bị suy giảm.

Trong thời gian này Euler tham gia cuộc tranh luận về nguồn gốc của "*nguyên lý tác động tối thiểu (principle of least action)*" [5]. Năm 1740, nguyên lý này được phát biểu bởi Pierre - Louis Moreau de Maupertuis, nhưng Johann Samuel căn cứ vào bức thư của Leibniz gửi Jakob đã cho rằng người phát biểu nguyên lý này đầu tiên là Leibniz. Euler được lôi vào cuộc tranh luận nhằm làm sáng tỏ vấn đề, nhưng do không mấy đồng tình với triết học của Leibniz, Euler đã đứng về phía Maupertuis và cáo buộc Johann làm giả tài liệu. Cuộc tranh cãi này càng trở nên sôi nổi khi Voltaire tham gia cuộc tranh luận và ông đứng về phía Johann, Voltaire đã chỉ trích rất gay gắt cả Euler và Maupertuis. Trước áp lực dư luận Maupertuis đã rời khỏi Berlin và Euler chịu trách nhiệm mọi công việc ở Viện.

Quan hệ của Euler với Fredric II không được "*suôn sẻ*", do sự khác biệt rõ rệt về tính cách cũng như tư tưởng. Fredric tự tin, hài hước và quảng giao còn Euler khiêm tốn, sống kín đáo và là một tín đồ theo đạo Tin Lành. Mặt khác sau khi Maupertuis rời Berlin, Euler là người đã chèo chống con thuyền Viện Hàn lâm nhưng Ferderic khi đó đã phớt lờ mọi lời giới thiệu Euler vào vị trí viện trưởng và bỏ qua tất cả để rồi sau đó tuyên bố chính mình mới là Viện trưởng Viện Hàn lâm. Tất cả các điều trên cùng với việc không được sự ủng hộ của các quý tộc khác dẫn tới Euler chấp nhận một lời mời của nữ hoàng Catherine II để trở về St.Petersburg.

[5] Nguyên lý tác động tối thiểu là một nguyên lý biến phân được áp dụng rộng rãi trong vật lý. Áp dụng nguyên lý này có thể dễ dàng tìm ra được phương trình quỹ đạo của các chuyển động.

St.Petersburg 1766 – 1783

Thời kỳ này cuộc sống của Euler có nhiều trắc trở về mặt cá nhân, mắt phải của ông bị đục thủy tinh thể (mắt còn tốt) và làm giảm thị lực rất nhiều. Năm 1771, sau ca phẫu thuật, thị lực của mắt phải của ông suy giảm nhanh chóng, và gần như mù hẳn. Cũng trong năm này, nhà của Euler bị cháy trong trong vụ đại hoả hoạn ở St.Peterburg vào tháng năm thiêu rụi hơn 5000 ngôi nhà, Euler được cứu bởi người hầu của mình là Peter Grimm.

Hình 2: Euler được Peter cứu thoát từ ngôi nhà của mình trong trận đại hoả.

Bù đắp lại một phần khó khăn của Euler, nữ hoàng Catherine đã cho xây dựng lại một căn nhà khác cho Euler.

Thêm một nỗi đau năm 1773, vợ ông, Katharina Gsell chết. Euler tái hôn ba năm sau đó để không phải phụ thuộc vào con cái của mình.

Trong hoàn cảnh gặp nhiều khó khăn như vậy nhưng Euler không hề nản chí, ông vẫn làm việc và say sưa nghiên cứu với sự giúp đỡ từ những người khác, đầu tiên là từ nữ hoàng Catherine, sau đó là Niklaus Fuss, một người đồng hương tới từ Thuỵ Sỹ, cháu rể tương lai của Euler và người con trai của mình. Gần một nửa các công trình khoa học, các bài báo của Euler được viết trong quãng thời gian ở St.Petersburg lần thứ hai này.

Leonhard Euler chết vì đột quỵ ngày 18/9/1783 trong khi chơi với một trong những đứa cháu của mình. Cũng chính vào ngày này, trên hai phiến đá lớn, ông đã viết ra công thức diễn giải bản chất Toán học có liên quan tới việc chuyển động của khinh khí cầu mà chuyến bay đầu tiên do hai em nhà Montgolfier thực hiện vào ngày 5/6/1783. Đó là bài viết cuối cùng của ông, và chuẩn bị xuất bản bởi con trai của ông là Johann Albrecht. Nhưng việc xuất bản các công trình cũng như bài viết của Euler vẫn còn kéo dài suốt 50 năm kể từ sau ngày ông mất.

GIÁ TRỊ NÀO CHO $1+1+1+\cdots$? $+\infty$ HAY $-\frac{1}{2}$?

Lý Ngọc Tuệ
Mathworks, Inc.

LỜI GIỚI THIỆU CỦA BAN BIÊN TẬP

Tổng của dãy vô hạn $1+1+1+\cdots=\infty$ hay $-\frac{1}{2}$? Hẳn phần lớn bạn đọc sẽ nhanh chóng trả lời là ∞, nhưng liệu $-\frac{1}{2}$ cũng là một câu trả lời đúng? Xa hơn nữa, tổng vô hạn $1-1+1-1+\cdots$ là ∞, là 0 hay $-\frac{1}{12}$? Hẳn nhiều bạn đọc sẽ còn ngạc nhiên hơn nữa khi chúng tôi nói rằng con số $-\frac{1}{12}$ không chỉ không vô lý mà kết quả này lại liên quan đến lý thuyết dây trong Vật lý!

Để làm rõ vấn đề thú vị này, chuyên mục Toán học Giải trí trân trọng giới thiệu đến bạn đọc loạt bài viết về các chuỗi vô hạn từ tác giả Lý Ngọc Tuệ.

1. Giới thiệu

Sau khi biết được các tính chất của các phép tính cơ bản như: cộng, trừ, nhân, chia với 2 số thực và thứ tự thực hiện, chúng ta có thể mở rộng ra để tính được giá trị của một biểu thức bao gồm hữu hạn các phép toán trên. Bước phát triển tự nhiên tiếp theo sẽ là tìm cách gán giá trị cho một biểu thức với vô số (đếm được) các phép tính cơ bản, mà trong đấy, dạng biểu thức đơn giản nhất chỉ bao gồm phép cộng hoặc trừ, được gọi là *chuỗi*[1]:

$$a_0+a_1+a_2+\cdots=\sum_{n=0}^{\infty}a_n \tag{1.1}$$

với $a_0, a_1, a_2, \ldots \in \mathbb{R}$ là các số thực.

Việc gán giá trị cho những chuỗi số đã được thực hiện bởi các nhà khoa học từ cách đây hơn 2000 năm. Cách tính giá trị của những chuỗi cấp số nhân chẳng hạn như:

$$\sum_{n=0}^{\infty}\left(\frac{1}{2}\right)^n=1+\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\cdots=2$$

[1] series

đã được biết đến trong các ghi chép từ thời Hy Lạp cổ đại. Tuy nhiên, mãi đến tận thế kỷ 17 và 18 với sự ra đời của giải tích, đạo hàm và tích phân, việc tính toán với các chuỗi vô hạn mới trở nên phổ biến. Nhiều phương pháp biến đổi và gán giá trị cho chuỗi được đưa ra, tuy nhiên các kết quả đạt được lại thường không nhất quán. Mặc dù các nhà toán học lớn thời đấy như Newton, Leibnitz, hay Euler dường như biết được những chuỗi nào là an toàn trong tính toán, họ (đặc biệt là Euler) vẫn sử dụng các chuỗi 'không an toàn' để thu được nhiều kết quả quan trọng. Những kết quả này sau đấy đã được xác nhận lại bằng các phương pháp khác một cách độc lập.

Mãi đến tận thế kỷ 19, định nghĩa chính xác và tổng quát về chuỗi hội tụ mới được đưa ra bởi Cauchy [1]. Định nghĩa của Cauchy, cùng với mở rộng giải tích[2] cho đến hiện nay có thể nói là phương pháp chính thống được sử dụng rộng rãi nhất trong tính toán chuỗi và hàm số. Tuy nhiên không phải các chuỗi không hội tụ theo Cauchy (gọi là chuỗi phân kỳ) đều vô dụng. Có nhiều phương pháp tính toán có thể được áp dụng cho các chuỗi phân kỳ, gọi chung là các *phương pháp tính tổng*[3]. Lý thuyết tổng quát về các phương pháp tính tổng được xây dựng và hoàn thiện vào cuối thế kỷ 19, đầu thế kỷ 20, và hiện nay những phương pháp này được ứng dụng phổ biến trong lý thuyết số và vật lý.

Trong phần đầu của loạt bài về chuỗi vô hạn này, chúng ta sẽ giới thiệu về 2 phương pháp lấy tổng của Cauchy và Abel, và một số tính chất mong muốn cho phương pháp lấy tổng.

2. Chuỗi hình thức và Chuỗi lũy thừa hình thức

Với mỗi dãy số vô hạn $(a_0, a_1, a_2, ...)$, ngoài chuỗi (1.1), chúng ta còn quan tâm đến dạng *chuỗi lũy thừa với hệ số* $(a_0, a_1, a_2, ...)$ *với tâm ở* c như sau:

$$\sum_{n=0}^{\infty} a_n(x-c)^n = a_0 + a_1(x-c) + a_2(x-c)^2 + ... \tag{2.1}$$

Khi chưa được gán giá trị, các chuỗi $\sum_{n=0}^{\infty} a_n$ và $\sum_{n=0}^{\infty} a_n(x-c)^n$ được tạo bởi dãy $(a_0, a_1, ...)$ còn được gọi là các *chuỗi hình thức*[4] và *chuỗi lũy thừa hình thức*[5]. Thông qua phép gán các chuỗi / chuỗi lũy thừa với dãy các hệ số:

$$\sum_{n=0}^{\infty} a_n \longleftrightarrow (a_0, a_1, ...),$$

$$\sum_{n=0}^{\infty} a_n(x-c)^n \longleftrightarrow (a_0, a_1, ...),$$

[2] analytic continuation
[3] summation methods
[4] formal series
[5] formal power series

chúng ta có được mối tương quan 1-1 giữa không gian các chuỗi hình thức và không gian các dãy vô hạn đếm được[6]. Thông qua mối tương quan này, không gian các chuỗi hình thức / chuỗi lũy thừa hình thức có thể được thường hưởng cấu trúc của một không gian véc tơ với số chiều là vô hạn đếm được, mà trong đấy, các phép cộng và nhân với một số thực được thực hiên theo từng thành phần:

$$\sum_{n=0}^{\infty} a_n + \sum_{n=0}^{\infty} b_n = \sum_{n=0}^{\infty} (a_n + b_n),$$
$$c \sum_{n=0}^{\infty} a_n = \sum_{n=0}^{\infty} c a_n.$$

Ngoài cấu trúc không gian véc tơ ra, không gian các dãy còn có phép nhân từng phần tử:

$$(a_0, a_1, a_2, ...) \cdot (b_0, b_1, b_2, ...) = (a_0 b_0, a_1 b_1, a_2 b_2, ...),$$

tuy nhiên nếu chúng ta đưa phép nhân này sang không gian các chuỗi, kết quả thu được sẽ không giống như mở rộng của tích của 2 tổng hữu hạn.

Cách mở rộng tự nhiên của phép nhân với 2 tổng hữu hạn ra chuỗi vô hạn được định nghĩa như sau:

$$\left(\sum_{n=0}^{\infty} a_n \right) \cdot \left(\sum_{n=0}^{\infty} b_n \right) := \sum_{n=0}^{\infty} \left(\sum_{i=0}^{n} a_i b_{n-i} \right).$$

Tương tự như vậy, các chuỗi lũy thừa hình thức có một phép nhân tự nhiên được thường hưởng / mở rộng từ phép nhân đa thức:

$$\left(\sum_{n=0}^{\infty} a_n (x-c)^n \right) \cdot \left(\sum_{n=0}^{\infty} b_n (x-c)^n \right) = \sum_{n=0}^{\infty} \left(\sum_{i=0}^{n} a_i b_{n-i} \right) (x-c)^n.$$

Với phép nhân này, tập các chuỗi lũy thừa hình thức trở thành một vành giao hoán, thường được ký hiệu bởi $\mathbb{R}[[x-c]]$. Vành các chuỗi lũy thừa hình thức có thể được ký hiệu bởi $\mathbb{R}[[1]]$.

Bài tập 1. Tìm phần tử đơn vị $1_{\mathbb{R}[[x]]}$ sao cho với mọi $\sum_{n=0}^{\infty} a_n x^n$,

$$1_{\mathbb{R}[[x]]} \cdot \left(\sum_{n=0}^{\infty} a_n x^n \right) = \sum_{n=0}^{\infty} a_n x^n.$$

Nhắc lại phần tử a của một vành giao hoán R được gọi là *khả nghịch*[7] nếu như tồn tại $b \in R$ sao cho $a \cdot b = 1_R$.

Bài tập 2. Chứng minh rằng một chuỗi hình thức $\sum_{n=0}^{\infty} a_n$ là một phần tử khả nghịch khi và chỉ khi $a_n \neq 0$ với mọi $n \in \mathbb{N}$.

[6] có thể được xem như là không gian các hàm số $\mathbb{R}^{\mathbb{N}} := \{f : \mathbb{N} \to \mathbb{R}\}$

[7] invertible

Bài tập 3. Chứng minh rằng một chuỗi lũy thừa hình thức $\sum_{n=0}^{\infty} a_n(x-c)^n$ là một phần tử đơn vị (khả nghịch) khi và chỉ khi $a_0 \neq 0$.

Bài tập 4. Tìm dãy (a_n) sao cho:

$$\left(\sum_{n=0}^{\infty} x^n\right) \cdot \left(\sum_{n=0}^{\infty} a_n x^n\right) = 1_{R[[x]]}.$$

3. Chuỗi hội tụ theo Cauchy

Với mỗi chuỗi hình thức $\sum_{n=0}^{\infty} a_n$, chúng ta có thể xây dựng dãy các tổng từng phần (s_n) như sau:

$$\begin{aligned} s_0 &= a_0, \\ s_1 &= a_0 + a_1, \\ s_2 &= a_0 + a_1 + a_2, \\ &\vdots \\ s_n &= a_0 + a_1 + a_2 + \cdots + a_n \\ &\vdots \end{aligned}$$

Định nghĩa 5. Nếu như dãy s_n hội tụ về một số thực s, ký hiệu là $s_n \to s$ hoặc $\lim\limits_{n\to\infty} s_n = \lim\limits_{n} s_n = \lim s_n = s$, chúng ta sẽ gọi chuỗi $\sum_{n=0}^{\infty} a_n$ là một *chuỗi hội tụ*, và gán giá trị s cho chuỗi $\sum_{n=0}^{\infty} a_n$. Nếu $\sum_{n=0}^{\infty} a_n$ được gọi là một chuỗi *phân kỳ* nếu như nó không hội tụ.

Đây là cách gán giá trị cho chuỗi phổ biến nhất, thường được ký hiệu bởi $\sum_{n=0}^{\infty} a_n = s$. Tuy nhiên, trong loạt bài này, để tiện cho việc phân biệt giữa chuỗi hình thức và các cách tính tổng khác nhau, chúng ta sẽ ký hiệu cách gán giá trị cho chuỗi hình thức này là:

$$(\mathcal{C})\left(\sum_{n=0}^{\infty} a_n\right) = \lim_{n\to\infty} s_n = \lim_{n\to\infty} \sum_{i=0}^{n} a_i = s,$$

theo tên của Cauchy.

Bài tập 6. Chứng minh rằng nếu như $\sum_{n=0}^{\infty} a_n$ và $\sum_{n=0}^{\infty} b_n$ là 2 chuỗi hội tụ, c, d là 2 số thực bất kỳ, thì:

$$(\mathcal{C})\left(c\sum_{n=0}^{\infty} a_n + d\sum_{n=0}^{\infty} b_n\right) = c\cdot(\mathcal{C})\left(\sum_{n=0}^{\infty} a_n\right) + d\cdot(\mathcal{C})\left(\sum_{n=0}^{\infty} b_n\right).$$

Bài tập trên cho ta thấy:

1. Tập các chuỗi hội tụ là một không gian véc tơ con.
2. Cách gán giá trị $(\mathcal{C})$ là một hàm tuyến tính từ không gian các chuỗi hội tụ vào $\mathbb{R}$.

Bài tập 7. Tìm 2 chuỗi hội tụ $\sum_{n=0}^{\infty} a_n$ và $\sum_{n=0}^{\infty} b_n$ sao cho chuỗi $\left(\sum_{n=0}^{\infty} a_n\right) \cdot \left(\sum_{n=0}^{\infty} b_n\right)$ không hội tụ.

Như vậy tập các chuỗi hình thức hội tụ không phải là một tập đóng đối với phép nhân, hay nói một cách khác, cách gán giá trị $(\mathcal{C})$ không tương thích với phép nhân các chuỗi hình thức. Tuy vậy, nếu như a_n, b_n đều là các số không âm, và các chuỗi $\sum_{n=0}^{\infty} a_n$ và $\sum_{n=0}^{\infty} b_n$ hội tụ thì tích của chúng cũng là một chuỗi hội tụ. Tính chất được chứng minh bởi Cauchy với định nghĩa và kết quả sau:

Định nghĩa 8. Chuỗi $\sum_{n=0}^{\infty} a_n$ được gọi là *hội tụ tuyệt đối*[8] nếu như chuỗi $\sum_{n=0}^{\infty} |a_n|$ hội tụ.

Định lý 9. *(1)* $\sum_{n=0}^{\infty} a_n$ *hội tụ tuyệt đối* $\Longrightarrow \sum_{n=0}^{\infty} a_n$ *hội tụ.*

(2) $\sum_{n=0}^{\infty} a_n$ *và* $\sum_{n=0}^{\infty} b_n$ *hội tụ tuyệt đối* $\Longrightarrow \left(\sum_{n=0}^{\infty} a_n\right) \cdot \left(\sum_{n=0}^{\infty} b_n\right)$ *hội tụ tuyệt đối.*

Hay nói một cách khác, tập các chuỗi hội tụ tuyệt đối tạo thành một vành con đồng thời cũng là một không gian tuyến tính con (hay còn gọi là một $\mathbb{R}$-đại số con) của tập các chuỗi hình thức.

4. Chuỗi lũy thừa hội tụ và phương pháp của Abel

Định nghĩa 10. Một chuỗi lũy thừa hình thức $\sum_{n=0}^{\infty} a_n(x-c)^n$ được gọi là hội tụ tại $z \in \mathbb{R}$ nếu như chuỗi $\sum_{n=0}^{\infty} a_n(z-c)$ hội tụ.

Có thể dễ dàng thấy được rằng các chuỗi lũy thừa có tâm tại c đều hội tụ tại c. Hơn nữa, định lý sau chỉ ra rằng các chuỗi lũy thừa chỉ hội tụ trong một đoạn thẳng có tâm ở c (bán kính có thể là $+\infty$):

[8] absolutely convergent

Định lý 11. *Với mỗi chuỗi lũy thừa* $\sum_{n=0}^{n} a_n(x-c)^n$*, đặt (cho phép bằng* $+\infty$*):*

$$R = \frac{1}{\limsup|a_n|^{1/n}}.$$

(1) Với mọi $|z-a| < R$*, chuỗi lũy thừa* $\sum_{n=0}^{\infty} a_n(x-c)^n$ *hội tụ tuyệt đối tại* z*,*

(2) Với mọi $|z-a| < R$*, chuỗi lũy thừa* $\sum_{n=0}^{\infty} a_n(x-c)^n$ *phân kỳ tại* z*.*

Số R *được định nghĩa như trên được gọi là* bán kính hội tụ *của chuỗi* $\sum_{n=0}^{\infty} a_n(x-c)^n$*.*

Bài tập 12. Chứng minh rằng nếu dãy $\left(\left|\frac{a_0}{a_1}\right|, \left|\frac{a_1}{a_2}\right|, \left|\frac{a_2}{a_3}\right|, ...\right)$ hội tụ, thì

$$R = \lim_{n\to\infty}\left|\frac{a_n}{a_{n+1}}\right|.$$

Bài tập 13. Chứng minh rằng nếu như cả 2 chuỗi $\sum_{n=0}^{n} a_n(x-c)^n$ và $\sum_{n=0}^{n} b_n(x-c)^n$ đều có bán kính hội tụ $\geq r > 0$, thì cả 2 chuỗi lũy thừa: $\left(\sum_{n=0}^{n} a_n(x-c)^n\right) + \left(\sum_{n=0}^{n} a_n(x-c)^n\right)$ và $\left(\sum_{n=0}^{n} a_n(x-c)^n\right) \cdot \left(\sum_{n=0}^{n} a_n(x-c)^n\right)$ đều có bán kính hội tụ $\geq r$.

Quan sát kỹ một tí, chúng ta có thể thấy rằng khi $x - c = 1$, chuỗi lũy thừa $\sum_{n=0}^{\infty} a_n(x-c)^n$ sẽ trở thành chuỗi $\sum_{n=0}^{\infty} a_n$. Để cho đơn giản, chúng ta xét chuỗi lũy thừa có tâm ở 0 $\sum_{n=0}^{\infty} a_n x^n$. Nếu như chuỗi lũy thừa này có bán kính hội tụ $R \geq 1$, và tồn tại giới hạn:

$$\lim_{x\to 1^-} \sum_{n=0}^{\infty} a_n x^n,$$

thì chúng ta gọi chuỗi $\sum_{n=0}^{\infty} a_n$ là *Abel-khả tổng*[9] (hoặc $(\mathcal{A})$-khả tổng), và gán giá trị của giới hạn này cho chuỗi:

$$(\mathcal{A})\sum_{n=0}^{\infty} a_n := \lim_{x\to 1^-} \sum_{n=0}^{\infty} a_n x^n.$$

[9] Abel summable

Bài tập 14. Chứng minh rằng nếu như $\sum_{n=0}^{\infty} a_n$ và $\sum_{n=0}^{\infty} b_n$ là 2 chuỗi Abel-khả tổng, c, d là 2 số thực bất kỳ, thì:

$$(\mathcal{A})\left(c\sum_{n=0}^{\infty} a_n + d\sum_{n=0}^{\infty} b_n\right) = c\cdot(\mathcal{A})\left(\sum_{n=0}^{\infty} a_n\right) + d\cdot(\mathcal{A})\left(\sum_{n=0}^{\infty} b_n\right).$$

5. Chuỗi phân kỳ - Một số tính chất mong muốn

Trở lại với ví dụ ở đầu bài, xét chuỗi $\sum_{n=0}^{\infty} 1 = 1+1+1+...$, dãy các tổng từng phần có thể dễ dàng tính ra được:

$$(s_0, s_1, s_2, ..., s_n, ...) = (1, 2, 3, ..., (n+1), ...),$$

và như vậy chuỗi $1+1+1+...$ là phân kỳ theo cách gán giá trị của Cauchy:

$$\lim_{n\to\infty} s_n = \lim_{n\to\infty} (n+1) = \infty.$$

Bài tập 15. Chứng minh rằng chuỗi $1+1+1+...$ không phải là một chuỗi Abel khả tổng.

Vậy liệu có tồn tại mộ cách gán giá trị cho chuỗi $(\mathcal{T})$ nào đó sao cho $(\mathcal{T})(1+1+1+...)$ là hữu hạn? Điều này tùy thuộc vào việc chúng ta muốn $(\mathcal{T})$ sở hữu thêm những tính chất nào khác nữa.

Chúng ta tạm thời liệt kê một số tính chất mà $(\mathcal{T})$ nên có như sau:

(1) $\mathcal{T}$ là hàm tuyến tính.

(2) Nếu như chuỗi $\sum_{n=0} a_n$ hội tụ thì $\sum_{n=0} a_n$ $(\mathcal{T})$-khả tổng.

(2*) $(\mathcal{T})$ đồng ý với $(\mathcal{C})$: nếu như chuỗi $\sum_{n=0} a_n$ hội tụ thì

$$(\mathcal{T})\left(\sum_{n=0} a_n\right) = (\mathcal{C})\left(\sum_{n=0} a_n\right).$$

(3) Nếu như chuỗi $\sum_{n=0} a_n$ là $(\mathcal{T})$-khả tổng thì:

$$(\mathcal{T})\left(\sum_{n=0} a_n\right) = (\mathcal{T})(a_0 + a_1 + a_2 + ...) = a_0 + (\mathcal{T})(a_1 + a_2 + a_3 + ...).$$

Tính chất (3) tương đương với việc phương pháp tính tổng vô hạn $(\mathcal{T})$ không vụ thuộc vào một số hữu hạn các số hạng đầu tiên, có thể xem như là một mở rộng của phép cộng hữu hạn số hạng. Tính chất này tuy có vẻ hợp lý, nhưng lại có thể dẫn đến một số kết luận có vẻ vô lý như sau:

Nếu như $(\mathcal{T})$ gán một giá trị hữu hạn s cho tổng $1+1+1+...$, đồng thời thỏa mãn các tính chất (3), thì:

$$s = (\mathcal{T})(1+1+1+...) = 1 + (\mathcal{T})(1+1+1+...) = 1+s.$$

Từ đó ta suy ra:

$$(\mathcal{T})(1+1+1+...) = s = +\infty \quad (!!!).$$

Như vậy để gán được giá trị hữu hạn cho chuỗi $(1+1+1+...)$, chúng ta sẽ mất đi tính chất (3).

Một trong những phương pháp phổ biến để gán giá trị hữu hạn cho chuỗi $(1+1+1+...)$ là sử dụng *mở rộng giải tích*[10] của chuỗi:

$$\sum_{n=1}^{\infty} n^{-s} = 1^{-s} + 2^{-s} + 3^{-s} + ...$$

Về mặt hình thức,

$$\sum_{n=1}^{\infty} n^{-0} = 1^0 + 2^0 + 3^0 + ... = 1+1+1+...$$

Tuy nhiên, chuỗi $\sum_{n=1}^{\infty} n^{-s}$ chỉ hội tụ tuyệt đối khi $s > 1$ và phân kỳ khi $s = 1$. Khó khăn này được giải quyết bằng cách mở rộng ra không gian số phức $\mathbb{C}$ thay cho số thực. Khi đấy, chuỗi $\sum_{n=1}^{\infty} n^{-s}$ là đại diện của hàm giải tích $\zeta(s)$ trên tập $\{s \in \mathbb{C} : \Re(s) > 1\}$. Hàm này có một mở rộng giải tích duy nhất ra $\mathbb{C} \setminus \{1\}$, và chúng ta có thể gán giá trị của hàm này tại 0 này cho chuỗi $(1+1+1+...)$. Chúng ta sẽ ký hiệu phương pháp tính tổng này bởi $(\mathfrak{E})$:

$$(\mathfrak{E})(1+1+1+...) = \zeta(0) = -\frac{1}{2}.$$

Trong phần sau, chúng ta sẽ đi sâu hơn vào chi tiết của mở rộng giải tích, một trong những khái niệm và phương pháp rất quan trọng của toán học.

Tài liệu

[1] A. L. Cauchy, *Analyse algébrique*, Paris (1821).

[2] J. B. Conway, *Functions of One Complex Variable*, Graduate Texts of Mathematics **11**, Springer-Verlag (1973).

[3] G. H. Hardy, *Divergent series*, Oxford (1949).

[10] analytic continuation

TIẾP NỐI CÂU CHUYỆN VỀ MỘT TỔNG LŨY THỪA

Trịnh Đào Chiến
(Cao đẳng Sư phạm Gia Lai)

Giả sử n và k là các số nguyên dương. Trong [2], tác giả Trần Nam Dũng đã đề cập những điều thú vị về tổng

$$S_k(n) = \sum_{j=1}^{n} j^k = 1^k + 2^k + \cdots + n^k. \tag{1}$$

Trong [3], Nguyễn Mạnh Linh tiếp tục đề cập một số tính chất của tổng (1), bằng cách tiếp cận các đa thức $S_k(x)$ xác định bởi các hệ thức truy hồi.

Tiếp nối mạch suy nghĩ trên, bài viết này đề cập đến một số trường hợp đặc biệt của tổng

$$S_k(n) = \sum_{j=1}^{n} {x_j}^k = {x_1}^k + {x_2}^k + \cdots + {x_n}^k, \tag{2}$$

một dạng tổng quát hóa trực tiếp của tổng (1).

Trước hết, ta nhắc lại Đồng nhất thức Newton, một đồng nhất thức quan trọng, liên quan đến tổng (2).

1. Đồng nhất thức Newton

Đồng nhất thức Newton, lần đầu tiên được nhà toán học Newton thiết lập vào Thế kỷ 17. Từ đó đến nay, đã có nhiều cách chứng minh cho đồng nhất thức này.

Với $n = 3$, đồng nhất thức Newton được thiết lập như sau: Giả sử $x_1,\ x_2, x_3 \in \mathbb{R}$. Thế thì $x_1,\ x_2, x_3$ là nghiệm của phương trình

$$(x - x_1)(x - x_2)(x - x_3) = 0,$$

hay

$$x^3 - (x_1 + x_2 + x_3)x^2 + (x_1x_2 + x_2x_3 + x_3x_1)x - x_1x_2x_3 = 0.$$

Đặt

$$\begin{cases} c_1 = -(x_1 + x_2 + x_3) \\ c_2 = x_1x_2 + x_2x_3 + x_3x_1 \\ c_3 = -x_1x_2x_3 \end{cases}$$

Thế thì $x_1,\ x_2,\ x_3$ là nghiệm của phương trình $x^3 + c_1x^2 + c_2x + c_3 = 0$. Đặt $S_k = {x_1}^k + {x_2}^k + {x_3}^k$, $k = 1,\ 2,\ 3,\ 4,\ \ldots$ Thế thì ta có đồng nhất thức sau

$$\begin{cases} S_1 + c_1 = 0, \\ S_2 + S_1c_1 + 2c_2 = 0, \\ S_3 + S_2c_1 + S_1c_2 + 3c_3 = 0, \\ S_4 + S_3c_1 + S_2c_2 + S_1c_3 = 0, \\ S_5 + S_4c_1 + S_3c_2 + S_2c_3 = 0, \\ \ldots \\ S_k + S_{k-1}c_1 + S_{k-2}c_2 + S_{k-3}c_3 = 0,\ k \geqslant 4. \end{cases}$$

Đồng nhất thức trên được gọi là đồng nhất thức Newton, trong trường hợp $n = 3$.

Từ khi được thiết lập, đã có nhiều cách chứng minh cho đồng nhất thức Newton. Với những giá trị đầu tiên của số nguyên dương n, đồng nhất thức Newton có thể được kiểm tra một cách dễ dàng. Tuy nhiên, trong trường hợp n tổng quát, các cách chứng minh đều phải dùng đến việc khai triển chuỗi Taylor đối với một số hàm số quen thuộc, trong khi khái niệm chuỗi và việc khai triển này chưa có ở phổ thông.

Dưới đây là một trong những phương pháp thiết lập Đồng nhất thức Newton trong trường hợp $n = 3$ và trường hợp n bất kì.

1.1. Thiết lập đồng nhất thức Newton, trường hợp $n = 3$

Ta có

$$(x - x_1)(x - x_2)(x - x_3) = x^3 + c_1x^2 + c_2x + c_3. \tag{3}$$

Trong (3), thay x bởi $\dfrac{1}{x}$, ta có

$$\left(\frac{1}{x} - x_1\right)\left(\frac{1}{x} - x_2\right)\left(\frac{1}{x} - x_3\right) = \frac{1}{x^3} + \frac{c_1}{x^2} + \frac{c_2}{x} + c_3,$$

hay

$$\frac{(1 - x_1x)(1 - x_2x)(1 - x_3x)}{x^3} = \frac{1}{x^3} + \frac{c_1}{x^2} + \frac{c_2}{x} + c_3.$$

Một cách tương đương, ta có

$$(1 - x_1x)(1 - x_2x)(1 - x_3x) = 1 + c_1x + c_2x^2 + c_3x^3. \tag{4}$$

Bây giờ, xét chuỗi lũy thừa "hình thức"

$$\sum_{k=1}^{\infty} S_k x^k.$$

Lưu ý rằng, bởi khai triển Taylor, ta có

$$\sum_{k=0}^{\infty} x^k = \frac{1}{1-x}.$$

Suy ra rằng

$$1 + \sum_{k=1}^{\infty} x^k = \frac{1}{1-x}$$

hay

$$\sum_{k=1}^{\infty} x^k = \frac{x}{1-x}. \tag{5}$$

Do đó, bởi (4) và (5), ta có

$$\begin{aligned}
\sum_{k=1}^{\infty} S_k x^k &= \sum_{k=1}^{\infty} \left({x_1}^k + {x_2}^k + {x_3}^k\right) x^k = \sum_{k=1}^{\infty} \left((x_1 x)^k + (x_2 x)^k + (x_3 x)^k\right) \\
&= \sum_{k=1}^{\infty} (x_1 x)^k + \sum_{k=1}^{\infty} (x_2 x)^k + \sum_{k=1}^{\infty} (x_3 x)^k = \frac{x_1 x}{1-x_1 x} + \frac{x_2 x}{1-x_2 x} + \frac{x_3 x}{1-x_3 x} \\
&= -x \cdot \frac{\dfrac{d}{dx}\left(\left(1-x_1 x\right)\left(1-x_2 x\right)\left(1-x_3 x\right)\right)}{\left(1-x_1 x\right)\left(1-x_2 x\right)\left(1-x_3 x\right)} = -x \cdot \frac{c_1 + 2c_2 x + 3c_3 x^2}{1 + c_1 x + c_2 x^2 + c_3 x^3} \\
&= -\frac{c_1 x + 2c_2 x^2 + 3c_3 x^3}{1 + c_1 x + c_2 x^2 + c_3 x^3}.
\end{aligned}$$

Suy ra rằng

$$\left(\sum_{k=1}^{\infty} S_k x^k\right)\left(1 + c_1 x + c_2 x^2 + c_3 x^3\right) = -\left(c_1 x + 2c_2 x^2 + 3c_3 x^3\right),$$

hay

$$\sum_{k=1}^{\infty} S_k x^k + \left(\sum_{k=1}^{\infty} S_k x^k\right)\left(c_1 x + c_2 x^2 + c_3 x^3\right) = -\left(c_1 x + 2c_2 x^2 + 3c_3 x^3\right).$$

Nói cách khác, ta có

$$\sum_{k=1}^{\infty} S_k x^k = -\left(\sum_{k=1}^{\infty} S_k x^k\right)\left(c_1 x + c_2 x^2 + c_3 x^3\right) - \left(c_1 x + 2c_2 x^2 + 3c_3 x^3\right). \tag{6}$$

Vế trái của (6) được khai triển như sau

$$S_1x + S_2x^2 + S_3x^3 + S_4x^4 + S_5x^5 + \cdots \tag{7}$$

Vế phải của (6) được viết lại dưới dạng

$$\begin{aligned} &-c_1x - (S_1c_1 + 2c_2)\,x^2 - (S_2c_1 + S_1c_2 + 3c_3)\,x^3 \\ &\quad - (S_3c_1 + S_2c_2 + S_1c_3)\,x^4 - (S_4c_1 + S_3c_2 + S_2c_3)\,x^5 - \cdots \end{aligned} \tag{8}$$

So sánh các hệ số tương ứng của (7) và (8), ta thu được

$$\begin{cases} S_1 = -c_1, \\ S_2 = -S_1c_1 - 2c_2, \\ S_3 = -S_2c_1 - S_1c_2 - 3c_3, \\ S_4 = -S_3c_1 - S_2c_2 - S_1c_3, \\ S_5 = -S_4c_1 - S_3c_2 - S_2c_3, \\ \quad \cdots \\ S_k = -S_{k-1}c_1 - S_{k-2}c_2 - S_{k-3}c_3, \ k \geqslant 4. \end{cases}$$

hay

$$\begin{cases} S_1 + c_1 = 0, \\ S_2 + S_1c_1 + 2c_2 = 0, \\ S_3 + S_2c_1 + S_1c_2 + 3c_3 = 0, \\ S_4 + S_3c_1 + S_2c_2 + S_1c_3 = 0, \\ S_5 + S_4c_1 + S_3c_2 + S_2c_3 = 0, \\ \quad \cdots \\ S_k + S_{k-1}c_1 + S_{k-2}c_2 + S_{k-3}c_3 = 0, \ k \geqslant 4. \end{cases}$$

1.2. Đồng nhất thức Newton, trường hợp tổng quát

Giả sử $x_1,\ x_2,\ \ldots,\ x_n$ là n số thực xác định. Đặt

$$\begin{cases} c_1 = -\left(x_1 + x_2 + \cdots + x_n\right) \\ c_2 = x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n \\ c_3 = -\left(x_1x_2x_3 + x_1x_2x_4 + \cdots + x_{n-2}x_{n-1}x_n\right) \\ \cdots \\ c_n = (-1)^n x_1x_2x_3\cdots x_n \end{cases}$$

và

$$S_k = {x_1}^k + {x_2}^k + \cdots + {x_n}^k; \;\; k = 1,\, 2,\, 3,\, \ldots,\, n,\, n+1,\, n+2,\, \ldots$$

Ta có đồng nhất thức sau

$$\begin{cases} S_1 + c_1 = 0, \\ S_2 + S_1 c_1 + 2c_2 = 0, \\ \cdots \\ S_n + S_{n-1} c_1 + \cdots + S_1 c_{n-1} + n c_n = 0, \\ S_k + S_{k-1} c_1 + \cdots + S_1 c_{k-1} = 0, \; \forall k \geqslant n+1. \end{cases}$$

Đồng nhất thức trên được gọi là đồng nhất thức Newton.

Dựa vào cách thiết lập đồng nhất thức Newton trong trường hợp $n = 3$, ta có cách chứng minh sau đây cho đồng nhất thức Newton, trong trường hợp n bất kì.

Ta có

$$\prod_{i=1}^{n} (x - x_i) = x^n + \sum_{i=0}^{n-1} c_{n-i} x^i. \tag{9}$$

Trong (9), thay x bởi $\dfrac{1}{x}$, ta có

$$\prod_{i=1}^{n} \left(\frac{1}{x} - x_i \right) = \frac{1}{x^n} + \sum_{i=0}^{n-1} \frac{c_{n-i}}{x^i},$$

hay

$$\frac{\prod\limits_{i=1}^{n} (1 - x_i x)}{x^n} = \frac{1}{x^n} + \sum_{i=0}^{n-1} \frac{c_{n-i}}{x^i}.$$

Quy đồng và rút gọn, ta được

$$\prod_{i=1}^{n} (1 - x_i x) = 1 + \sum_{i=1}^{n} c_i x^i. \tag{10}$$

Bây giờ, xét chuỗi lũy thừa "hình thức"

$$\sum_{k=1}^{\infty} S_k x^k.$$

Bởi (10), ta có

$$\sum_{k=1}^{\infty} S_k x^k = \sum_{k=1}^{\infty} \left(\sum_{i=1}^{n} {x_i}^k \right) x^k = \sum_{k=1}^{\infty} \left(\sum_{i=1}^{n} (x_i x)^k \right) = \sum_{i=1}^{n} \left(\sum_{k=1}^{\infty} (x_i x)^k \right)$$
$$= \sum_{i=1}^{n} \frac{x_i x}{1 - x_i x} = -x \cdot \frac{\dfrac{d}{dx}\left(\prod\limits_{i=1}^{n} (1 - x_i x) \right)}{\prod\limits_{i=1}^{n} (1 - x_i x)} = -x \cdot \frac{\dfrac{d}{dx}\left(1 + \sum\limits_{i=1}^{n} c_i x^i \right)}{1 + \sum\limits_{i=1}^{n} c_i x^i}$$
$$= -\frac{x \sum\limits_{i=1}^{n} i c_i x^{i-1}}{1 + \sum\limits_{i=1}^{n} c_i x^i} = -\frac{\sum\limits_{i=1}^{n} i c_i x^i}{1 + \sum\limits_{i=1}^{n} c_i x^i}.$$

Tóm lại, ta có

$$\sum_{k=1}^{\infty} S_k x^k = -\frac{\sum\limits_{i=1}^{n} i c_i x^i}{1 + \sum\limits_{i=1}^{n} c_i x^i}.$$

Suy ra rằng

$$\sum_{k=1}^{\infty} S_k x^k \left(1 + \sum_{i=1}^{n} c_i x^i \right) = -\sum_{i=1}^{n} i c_i x^i$$

hay

$$\sum_{k=1}^{\infty} S_k x^k + \left(\sum_{k=1}^{\infty} S_k x^k \right) \left(\sum_{i=1}^{n} c_i x^i \right) = -\sum_{i=1}^{n} i c_i x^i.$$

Nói cách khác, ta có

$$\sum_{k=1}^{\infty} S_k x^k = -\left(\sum_{k=1}^{\infty} S_k x^k \right) \left(\sum_{i=1}^{n} c_i x^i \right) - \sum_{i=1}^{n} i c_i x^i. \tag{11}$$

Tương tự các bước như trong trường hợp $n = 3$, so sánh các hệ số tương ứng ở 2 vế của (11), ta thu được đồng nhất thức Newton.

2. Bài toán liên quan đến tổng $S_k\,(n)$

Những bài toán liên quan đến tổng (2) thường là những bài toán khó. Dưới đây là một trong nhiều bài toán minh họa cho nhận định này, mà giả thiết đã được "giảm nhẹ" đi rất nhiều.

Bài toán 1. *Giả sử $x_1,\ x_2,\ \ldots,\ x_n$ là n số nguyên dương tùy ý, xác định trước. Đặt*

$$S_k = {x_1}^k + {x_2}^k + \cdots + {x_n}^k, \quad k = 1,\ 2,\ 3,\ \ldots,\ n,\ n+1,\ n+2,\ \ldots$$

Biết rằng $S_k = k$, với $k = 1,\ 2,\ 3,\ \ldots,\ n$. Tính S_{n+1}.

Lời giải. Kí hiệu

$$\begin{cases} \sigma_1 = x_1 + x_2 + ... + x_n, \\ \sigma_2 = x_1x_2 + x_1x_3 + ... + x_{n-1}x_n, \\ \sigma_3 = x_1x_2x_3 + x_1x_2x_4 + ... + x_{n-2}x_{n-1}x_n, \\ ... \\ \sigma_n = x_1x_2x_3...x_n. \end{cases}$$

Xét đa thức

$$f(x) = \prod_{i=1}^{n} (x - x_i) = x^n + \sum_{j=1}^{n} c_j x^{n-j},$$

trong đó

$$c_j = (-1)^j \sigma_j,\ j = 1, 2, ..., n.$$

Theo Đồng nhất thức Newton, ta có

$$S_1 + c_1 = 0 \Leftrightarrow 1 - \sigma_1 = 0 \Leftrightarrow \sigma_1 = 1$$

và, với mọi $k = 2, 3, ..., n$

$$S_k + S_{k-1}c_1 + \ S_{k-2}c_2 + \ ... \ + \ S_2c_{k-2} + \ S_1c_{k-1} + kc_k = 0$$

$$\Leftrightarrow S_k + \sum_{j=1}^{k-1} S_{k-j}c_j + kc_k = 0 \Leftrightarrow k + \sum_{j=1}^{k-1} (k-j)\, c_j + kc_k = 0$$

$$\Leftrightarrow kc_k = -k - \sum_{j=1}^{k-1} (k-j)\, c_j \Leftrightarrow c_k = -1 - \frac{1}{k} \sum_{j=1}^{k-1} (k-j)\, c_j$$

$$\Leftrightarrow (-1)^k \sigma_k = -1 - \frac{1}{k} \sum_{j=1}^{k-1} (k-j)\, (-1)^j \sigma_j.$$

Vậy

$$\begin{cases} \sigma_1 = 1 \\ \sigma_k = (-1)^{k+1} + \dfrac{(-1)^k}{k} \displaystyle\sum_{j=1}^{k-1} (-1)^{j+1} (k-j)\, \sigma_j, k = 2, 3, ..., n \end{cases} \tag{12}$$

Cũng theo Đồng nhất thức Newton, ta có

$$S_{n+1} + S_nc_1 + \ S_{n-1}c_2 + \ ... + \ S_2c_{n-1} + \ S_1c_n = \ 0 \Leftrightarrow S_{n+1} + \sum_{j=1}^{n} S_{n\,-j\,+1}c_j = 0$$

$$\Leftrightarrow S_{n+1} + \sum_{j=1}^{n} (n-j+1)(-1)^j \sigma_j = 0 \Leftrightarrow S_{n+1} = -\sum_{j=1}^{n} (n-j+1)(-1)^j \sigma_j.$$

Suy ra

$$S_{n+1} = \sum_{j=1}^{n} (-1)^{j+1}(n-j+1)\sigma_j. \tag{13}$$

Lưu ý rằng, giá trị của các σ_k không phụ thuộc vào biến x. Do đó

$$\sigma_n = (-1)^{n+1} + \frac{(-1)^n}{n} \cdot S_n. \tag{14}$$

Bởi (13) và (14), ta có

$$\mathrm{S}_{n+1} = \sum_{j=1}^{n} (n-j+1) .(-1)^{j+1}. \left((-1)^{j+1} + \frac{(-1)^j}{j} \cdot S_j \right).$$

Suy ra

$$\mathrm{S}_{n+1} = \sum_{j=1}^{n} (n-j+1) . \left(1 - \frac{S_j}{j} \right), n \geqslant 1, \tag{15}$$

với $S_1 = 0$.

Ngoài ra, (15) còn được viết lại dưới dạng

$$\mathrm{S}_{n+1} = \sum_{j=1}^{n-1} (n-j+1) . \left(1 - \frac{S_j}{j} \right) + \left(1 - \frac{S_n}{n} \right), \ n \geqslant 2, \tag{16}$$

với $S_1 = 0, S_2 = 1$.

Với $n \geqslant 2$, từ (16) , lần lượt thay chỉ số $n+1$ bởi $n, n-1$, ta có

$$\mathrm{S}_n = \sum_{j=1}^{n-1} (n-j) . \left(1 - \frac{S_j}{j} \right), \tag{17}$$

$$\begin{aligned} \mathrm{S}_{n-1} &= \sum_{j=1}^{n-2} (n-j-1) . \left(1 - \frac{S_j}{j} \right) = \sum_{j=1}^{n-2} (n-j-1) . \left(1 - \frac{S_j}{j} \right) + 0 \\ &= \sum_{j=1}^{n-2} (n-j-1) . \left(1 - \frac{S_j}{j} \right) + (n-(n-1)-1) \left(1 - \frac{S_{n-1}}{n-1} \right). \end{aligned}$$

Suy ra

$$\mathrm{S}_{n-1} = \sum_{j=1}^{n-1} (n-j-1) . \left(1 - \frac{S_j}{j} \right). \tag{18}$$

Bởi (16), (17), (18), ta có

$$\begin{aligned} \mathrm{S}_{n+1} + \mathrm{S}_{n-1} &= \sum_{j=1}^{n-1} 2\,(n-j) . \left(1 - \frac{S_j}{j} \right) + \left(1 - \frac{S_n}{n} \right) \\ &= 2 \sum_{j=1}^{n-1} (n-j) . \left(1 - \frac{S_j}{j} \right) + \left(1 - \frac{S_n}{n} \right) = 2\mathrm{S}_n + \left(1 - \frac{S_n}{n} \right) = 1 + \frac{2n-1}{n} \cdot S_n. \end{aligned}$$

Do đó, ta thu được phương trình sai phân tuyến tính cấp hai, với hệ số biến thiên

$$\begin{cases} S_{n+1} - \dfrac{2n-1}{n} \cdot S_n + S_{n-1} = 1, \ n \geqslant 2 \\ S_1 = 0, S_2 = 1. \end{cases} \tag{19}$$

Để giải phương trình sai phân này, ta xét hàm sinh sau

$$\mathrm{g}\,(x) = \sum_{n=1}^{\infty} S_{n+1} x^n.$$

Khi đó, bởi (19), ta có

$$(1-x)^2 . g\,(x) = \frac{x}{1-x} - \int_0^x g\,(t) dt. \tag{20}$$

Lấy đạo hàm, theo từng vế của (20), ta có

$$-2\,(1-x)\,.g\,(x) + (1-x)^2 . g'\,(x) = \frac{1}{(1-x)^2} - (g\,(x) - g\,(0))\,, \tag{21}$$

với $g(0) = 0$.

Rút gọn (21), ta được phương trình vi phân tuyến tính cấp một

$$\begin{cases} (1-x)^2 . g'\,(x) + (2x-1)\,.g\,(x) = \dfrac{1}{(1-x)^2} \\ g\,(0) = 0. \end{cases} \tag{22}$$

Giải phương trình vi phân (22), ta được nghiệm

$$g\,(x) = \frac{1 - e^{-\dfrac{x}{x-1}}}{(1-x)^2}.$$

Khai triển hàm này theo Công thức Taylor đối với chuỗi lũy thừa, ta thu được

$$S_{n+1} = \sum_{k=1}^{n} \frac{(-1)^{k-1}}{k!} C_{n+1}^{k+1}.$$

Bài toán đã được giải quyết. □

3. Một số đồng nhất thức lượng giác liên quan đến tổng $S_k(n)$

Trong phần này, ta xét một trường hợp đặc biệt của tổng (2), với n là số nguyên dương tùy ý và x_j là hàm cosin theo biến j. Có thể tương tự đối với những hàm lượng giác khác. Những kết quả tìm được là những đồng nhất thức lượng giác thường gặp trong chương trình toán phổ thông.

Các kết quả dưới đây sẽ giúp ta tính được tổng hữu hạn của một số hàm cosin. Chẳng hạn, tổng sau đây

$$\sum_{j=1}^{\left\lfloor \frac{n-1}{2} \right\rfloor} \cos^k\left(\frac{j\pi}{n}\right), \tag{23}$$

trong đó $\lfloor x \rfloor$ là kí hiệu của số nguyên lớn nhất không vượt quá x.

Trước hết, cần lưu ý một kết quả quan trọng sau mà chứng minh nó có thể xem, chẳng hạn, trong [5].

Bổ đề 1. *Nếu $f(x) = a_0 + a_1x + +a_2x^2 + ... + a_nx^n + ...$ là hữu hạn hoặc chuỗi vô hạn hội tụ, thì với $0 \leqslant r < n$, tổng $a_rx^r + a_{r+n}x^{r+n} + a_{r+2n}x^{r+2n} + ...$ được xác định bởi công thức*

$$\sum_{j\geqslant 0} a_{r+jn}x^{r+jn} = \frac{1}{n}\sum_{j=0}^{n-1} z^{-jr} f\left(z^j x\right), \tag{24}$$

trong đó $z = e^{\frac{2\pi i}{n}}$ là nghiệm thứ n của 1.

Ta chứng minh các kết quả sau

Định lý 1. *Giả sử n và k là hai số nguyên dương. Thế thì*

$$\sum_{j=1}^{\left\lfloor \frac{n-1}{2} \right\rfloor} \cos^{2k}\left(\frac{j\pi}{n}\right) = -\frac{1}{2} + \frac{n}{2^{2k+1}} \sum_{j=-\left\lfloor \frac{k}{n} \right\rfloor}^{\left\lfloor \frac{k}{n} \right\rfloor} C_{2k}^{k+jn}.$$

Chứng minh. Áp dụng công thức (24), với $r = k - n\left\lfloor \frac{k}{n} \right\rfloor$ và $f(x) = (1+x)^{2k}$.

Khi đó, với $x = 1$, ta có

$$\sum_{j=-\left\lfloor \frac{k}{n} \right\rfloor}^{\left\lfloor \frac{k}{n} \right\rfloor} C_{2k}^{k+jn} = \frac{1}{n}\sum_{j=0}^{n-1} z^{-j\left(k-n\left\lfloor \frac{k}{n} \right\rfloor\right)} \left(1+z^j\right)^{2k}, \tag{25}$$

trong đó $z = e^{\frac{2\pi i}{n}}$.

Ta có

$$e^{-ir\varphi}\left(1+e^{i\varphi}\right)^k = e^{-ir\varphi}\left(e^{\frac{i\varphi}{2}-\frac{i\varphi}{2}} + e^{\frac{i\varphi}{2}+\frac{i\varphi}{2}}\right)^k$$

$$= e^{-ir\varphi}e^{\frac{ik\varphi}{2}}\left(e^{-\frac{i\varphi}{2}} + e^{\frac{i\varphi}{2}}\right)^k = 2^k\cos^k\frac{\varphi}{2}e^{i\left(\frac{k}{2}-r\right)\varphi} \tag{26}$$

Hơn nữa, ta có thể viết

$$z^{-j\left(k-n\left\lfloor\frac{k}{n}\right\rfloor\right)}\left(1+z^j\right)^{2k} = 2^{2k}\cos^{2k}\left(\frac{j\pi}{n}\right)e^{i.2.j.\left\lfloor\frac{k}{n}\right\rfloor.\pi}.$$

Khi đó, (25) trở thành

$$\sum_{j=-\left\lfloor\frac{k}{n}\right\rfloor}^{\left\lfloor\frac{k}{n}\right\rfloor} C_{2k}^{k+jn} = \frac{2^{2k}}{n}\sum_{j=0}^{n-1}\cos^{2k}\left(\frac{j\pi}{n}\right). \tag{27}$$

Bởi tính chất

$$\cos\left(\frac{(n-j)\,\pi}{n}\right) = -\cos\left(\frac{j\pi}{n}\right),\ J = 0,1,2,...,n,$$

nên định lí 1 được chứng minh. □

Định lý 2. *Giả sử n và k là hai số nguyên dương sao cho $n \equiv k\,(\mathrm{mod}2)$. Thế thì*

$$\sum_{j=1}^{\left\lfloor\frac{n-1}{2}\right\rfloor}(-1)^j\cos^k\left(\frac{j\pi}{n}\right) = -\frac{1}{2} + \frac{n}{2^{k+1}}\sum_{j=-\left\lfloor\frac{k}{2n}\right\rfloor}^{\left\lfloor\frac{k}{2n}\right\rfloor} C_k^{\frac{k+n}{2}+jn},$$

trong đó $[x]$ là kí hiệu của số nguyên gần nhất của x, nghĩa là $[x] = \left\lfloor x+\frac{1}{2}\right\rfloor$.

Chứng minh. Áp dụng công thức (24) với $r = \frac{k+n}{2} - n\left\lfloor\frac{k+n}{2n}\right\rfloor$ và $f(x) = (1+x)^k$.

Khi đó, với $x = 1$, ta có

$$\sum_{j=-\left\lfloor\frac{k+n}{2n}\right\rfloor}^{\left\lfloor\frac{k+n}{2n}\right\rfloor} C_k^{\frac{k+n}{2}+jn} = \frac{1}{n}\sum_{j=0}^{n-1} z^{-j\left(\frac{k+n}{2}-n\left\lfloor\frac{k+n}{2n}\right\rfloor\right)}\left(1+z^j\right)^k,$$

trong đó $z = e^{\frac{2\pi i}{n}}$.

Bởi (26), ta suy ra rằng

$$z^{-j\left(\frac{k+n}{2}-n\left\lfloor\frac{k+n}{2n}\right\rfloor\right)}\left(1+z^j\right)^k = 2^k\cos^k\left(\frac{j\pi}{n}\right)e^{i.j.\pi\left(2\left\lfloor\frac{k+n}{2n}\right\rfloor-1\right)}.$$

Khi đó, ta có

$$\sum_{j=-\left\lceil\frac{k+n}{2n}\right\rceil}^{\left\lceil\frac{k+n}{2n}\right\rceil} C_k^{\frac{k+n}{2}+jn} = \frac{2^k}{n}\sum_{j=0}^{n-1}(-1)^j\cos^k\left(\frac{j\pi}{n}\right). \tag{28}$$

Mặt khác, ta có

$$\sum_{j=0}^{n-1}(-1)^j\cos^k\left(\frac{j\pi}{n}\right) = 1+\sum_{j=1}^{\left\lfloor\frac{n-1}{2}\right\rfloor}(-1)^j\cos^k\left(\frac{j\pi}{n}\right)+\sum_{j=1}^{\left\lfloor\frac{n-1}{2}\right\rfloor}(-1)^{n-j}\cos^k\left(\frac{(n-j)\,\pi}{n}\right) =$$

$$1+\sum_{j=1}^{\left\lfloor\frac{n-1}{2}\right\rfloor}(-1)^j\cos^k\left(\frac{j\pi}{n}\right)+\sum_{j=1}^{\left\lfloor\frac{n-1}{2}\right\rfloor}(-1)^{n+k-j}\cos^k\left(\frac{j\pi}{n}\right) = 1+2\sum_{j=1}^{\left\lfloor\frac{n-1}{2}\right\rfloor}(-1)^j\cos^k\left(\frac{j\pi}{n}\right). \tag{29}$$

Bởi (25) và (29), định lí 2 được chứng minh. □

Định lý 3. *Giả sử n và k là hai số nguyên dương. Thế thì*

$$\sum_{j=1}^{\left\lfloor\frac{n}{2}\right\rfloor}\cos^{2k}\left(\frac{2j-1}{n}.\frac{\pi}{2}\right) = -\frac{1}{2}+\frac{n}{2^{2k+1}}\sum_{j=-\left\lfloor\frac{k}{n}\right\rfloor}^{\left\lfloor\frac{k}{n}\right\rfloor}(-1)^j C_{2k}^{k+jn}.$$

Chứng minh. Để chứng minh định lí, ta sử dụng công thức sau

$$\sum_{j=1}^{\left\lfloor\frac{n}{2}\right\rfloor} f\left(2j-1\right) = \frac{1}{2}\left(\sum_{j=1}^{n-1} f\left(k\right)-\sum_{j=1}^{n-1}(-1)^k f\left(k\right)\right), \tag{30}$$

với $f(k) = \cos^{2k}\left(\frac{j\pi}{2n}\right)$.

Bởi định lí 1 (nếu thay n bởi $2n$) và định lí 2 (nếu thay n và k bởi $2n$ và $2k$, theo thứ tự), ta có

$$\sum_{j=1}^{\left\lfloor\frac{n}{2}\right\rfloor} f(2j-1) = \frac{1}{2}\left(-\frac{1}{2} + \frac{2n}{2^{2k+1}} \sum_{j=-\left\lfloor\frac{k}{2n}\right\rfloor}^{\left\lfloor\frac{k}{2n}\right\rfloor} C_{2k}^{k+2jn}\right) + \frac{1}{2} - \frac{2n}{2^{2k+1}} \sum_{j=-\left\lfloor\frac{k}{2n}\right\rfloor}^{\left\lfloor\frac{k}{2n}\right\rfloor} C_{2k}^{k+(2j+1)n}$$

$$= \frac{n}{2^{2k+1}} \sum_{j=-\left\lfloor\frac{k}{2n}\right\rfloor}^{\left\lfloor\frac{k}{2n}\right\rfloor} \left(C_{2k}^{k+2jn} + C_{2k}^{k+(2j+1)n}\right) = \frac{n}{2^{2k+1}} \sum_{j=-\left\lfloor\frac{k}{n}\right\rfloor}^{\left\lfloor\frac{k}{n}\right\rfloor} (-1)^j C_{2k}^{k+jn}.$$

Định lí 3 được chứng minh. □

Hệ quả 4. *Giả sử n là số nguyên dương. Thế thì*

1. $\sum_{j=1}^{\left\lfloor\frac{n-1}{2}\right\rfloor} cos^{2n}\left(\frac{j\pi}{n}\right) = -\frac{1}{2} + \frac{n}{2^{2n}} + \frac{n}{2^{2n+1}} C_{2n}^{n}$;

2. $\sum_{j=1}^{\left\lfloor\frac{n-1}{2}\right\rfloor} (-1)^j cos^{n}\left(\frac{j\pi}{n}\right) = -\frac{1}{2} + \frac{n}{2^{n}}$;

3. $\sum_{j=1}^{\left\lfloor\frac{n}{2}\right\rfloor} cos^{2n}\left(\frac{2j-1}{n}.\frac{\pi}{2}\right) = -\frac{n}{2^{2n}} + \frac{n}{2^{2n+1}} C_{2n}^{n}$.

Hệ quả 5. *Giả sử n và k là hai số nguyên dương sao cho $k < n$. Thế thì*

1. $\sum_{j=1}^{\left\lfloor\frac{n-1}{2}\right\rfloor} cos^{2k}\left(\frac{j\pi}{n}\right) = -\frac{1}{2} + \frac{n}{2^{2k+1}} C_{2k}^{k}$;

2. $\sum_{j=1}^{\left\lfloor\frac{n-1}{2}\right\rfloor} (-1)^j cos^{k}\left(\frac{j\pi}{n}\right) = -\frac{1}{2}$, *với* $n \equiv k \pmod 2$;

3. $\sum_{j=1}^{\left\lfloor\frac{n}{2}\right\rfloor} cos^{2k}\left(\frac{2j-1}{n}.\frac{\pi}{2}\right) = \frac{n}{2^{2k+1}} C_{2k}^{k}$.

Bởi định lí 1, định lí 2, định lí 3, ta thu được một số đồng nhất thức tổ hợp sau

Hệ quả 6. *Giả sử k là số nguyên dương. Thế thì*

1. $\sum\limits_{j=0}^{k} C_{2k}^{k-j} = \frac{1}{2}C_{2k}^{k} + 2^{2k-1}$;

2. $\sum\limits_{j=0}^{\left\lfloor \frac{k}{2} \right\rfloor} C_{2k}^{k-2j} = \frac{1}{2}C_{2k}^{k} + 2^{2k-2}$;

3. $\sum\limits_{j=0}^{\left\lfloor \frac{k}{3} \right\rfloor} C_{2k}^{k-3j} = \dfrac{1}{2}C_{2k}^{k} + \dfrac{1+2^{2k-1}}{3}$;

4. $\sum\limits_{j=0}^{\left\lfloor \frac{k}{4} \right\rfloor} C_{2k}^{k-4j} = \dfrac{1}{2}C_{2k}^{k} + 2^{2k-3} + 2^{k-2}$;

5. $\sum\limits_{j=0}^{\left\lfloor \frac{k}{5} \right\rfloor} C_{2k}^{k-5j} = \dfrac{1}{2}C_{2k}^{k} + \dfrac{\left(3+\sqrt{5}\right)^{k} + \left(3-\sqrt{5}\right)^{k} + 2^{3k-1}}{5.2^{k}}$;

6. $\sum\limits_{j=0}^{\left\lfloor \frac{k}{6} \right\rfloor} C_{2k}^{k-6j} = \dfrac{1}{2}C_{2k}^{k} + \dfrac{3^{k} + 2^{2k-1} + 1}{6}$.

Hệ quả 7. *Giả sử k là số nguyên dương. Thế thì*

1. $\sum\limits_{j=1}^{k} C_{2k-1}^{k-j} = 4^{k-1}$;

2. $\sum\limits_{j=1}^{\left\lfloor \frac{k}{3} \right\rfloor} C_{2k-3}^{k-3j} = \dfrac{4^{k-2}-1}{3},\ k>1$;

3. $\sum\limits_{j=1}^{\left\lfloor \frac{k}{5} \right\rfloor} C_{2k-5}^{k-5j} = \dfrac{4^{k-3}}{5} - \dfrac{\left(\sqrt{5}+1\right)^{2k-5} - \left(\sqrt{5}-1\right)^{2k-5}}{5.2^{2k-5}},\ k>2.$

Hệ quả 8. *Giả sử k là số nguyên dương. Thế thì*

1. $\sum\limits_{j=0}^{k} (-1)^{j} C_{2k}^{k-j} = \frac{1}{2}C_{2k}^{k}$;

2. $\displaystyle\sum_{j=0}^{\left\lfloor \frac{k}{2} \right\rfloor} (-1)^j C_{2k}^{k-2j} = \frac{1}{2} C_{2k}^k + 2^{k-1};$

3. $\displaystyle\sum_{j=0}^{\left\lfloor \frac{k}{3} \right\rfloor} (-1)^j C_{2k}^{k-3j} = \frac{1}{2} C_{2k}^k + 3^{k-1};$

4. $\displaystyle\sum_{j=0}^{\left\lfloor \frac{k}{4} \right\rfloor} (-1)^j C_{2k}^{k-4j} = \frac{1}{2} C_{2k}^k + \frac{\left(2+\sqrt{2}\right)^k + \left(2-\sqrt{2}\right)^k}{4};$

5. $\displaystyle\sum_{j=0}^{\left\lfloor \frac{k}{5} \right\rfloor} (-1)^j C_{2k}^{k-5j} = \frac{1}{2} C_{2k}^k + \frac{\left(5+\sqrt{5}\right)^k + \left(5-\sqrt{5}\right)^k}{5.2^k}.$

Tài liệu

[1] Trịnh Đào Chiến, *Đa thức nội suy Lagrange và Đồng nhất thức Newton dưới góc nhìn của toán phổ thông*, Kỷ yếu hội thảo khoa học "Nghiên cứu và Giảng dạy Toán học phổ thông", Trường Đại học Khoa học Tự nhiên Thành phố Hồ Chí Minh, 8-9/8/2014.

[2] Trần Nam Dũng, *Những điều thú vị về tổng* $P_k(n) = \sum_{j=1}^{n} j^k = 1^k + 2^k + \cdots + n^k$, Các phương pháp giải toán qua các ký thi Olympic, Nhà xuất bản Đại học Quốc gia Thành phố Hồ Chí Minh, 2013.

[3] Nguyễn Mạnh Linh, *Một số vấn đề xung quanh tổng lũy thừa*, Kỷ yếu "Gặp gỡ toán học", Vũng Tàu, 7/2015.

[4] Mircea Merca, *A note on cosine power sums*, Article 12.5.3 Journal of Integer Sequences, Vol. 15 (2012).

[5] J. Riordan, *Combinatorial Identities*, John Wiley and Sons, 1968.

VỀ MỘT ĐỀ TOÁN HAY TRÊN TẠP CHÍ THTT

Trần Quang Hùng, THPT chuyên KHTN, Hà Nội
Nguyễn Đức Bảo, THPT chuyên Phan Bội Châu, Nghệ An

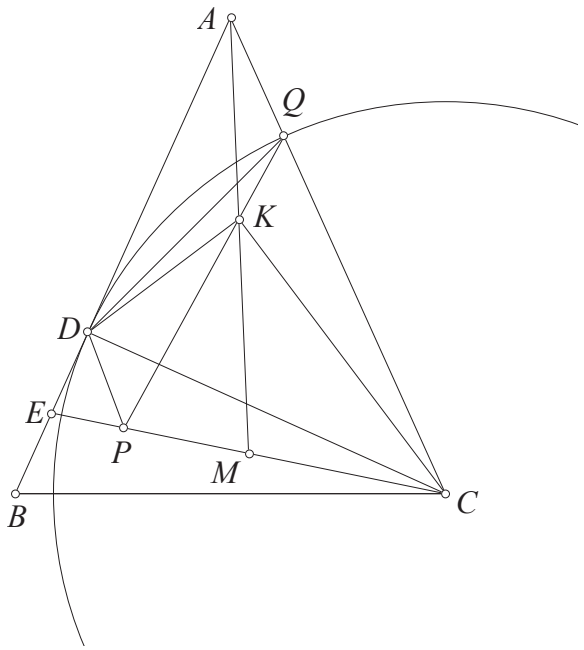
TÓM TẮT

Bài viết đưa ra cách chứng minh và các phát triển cho bài toán T12/465 của tạp chí Toán học và tuổi trẻ, đồng thời cũng ứng dụng các bài toán đó vào các bài toán khác nhau.

1. Một số bài toán mở đầu

Trên báo THTT số 465 [1] có bài toán T12 của thầy **Nguyễn Xuân Hùng** như sau

Bài toán 1. Cho tam giác ABC cân tại A có đường cao CD. Gọi E là trung điểm của BD, M là trung điểm CE, phân giác của $\angle BDC$ cắt CE tại P. Đường tròn tâm C bán kính CD cắt AC tại Q. Gọi K là giao điểm của PQ và AM. Chứng minh rằng tam giác CKD vuông.



Hình 1.

Biên tập: Ngô Quang Dương

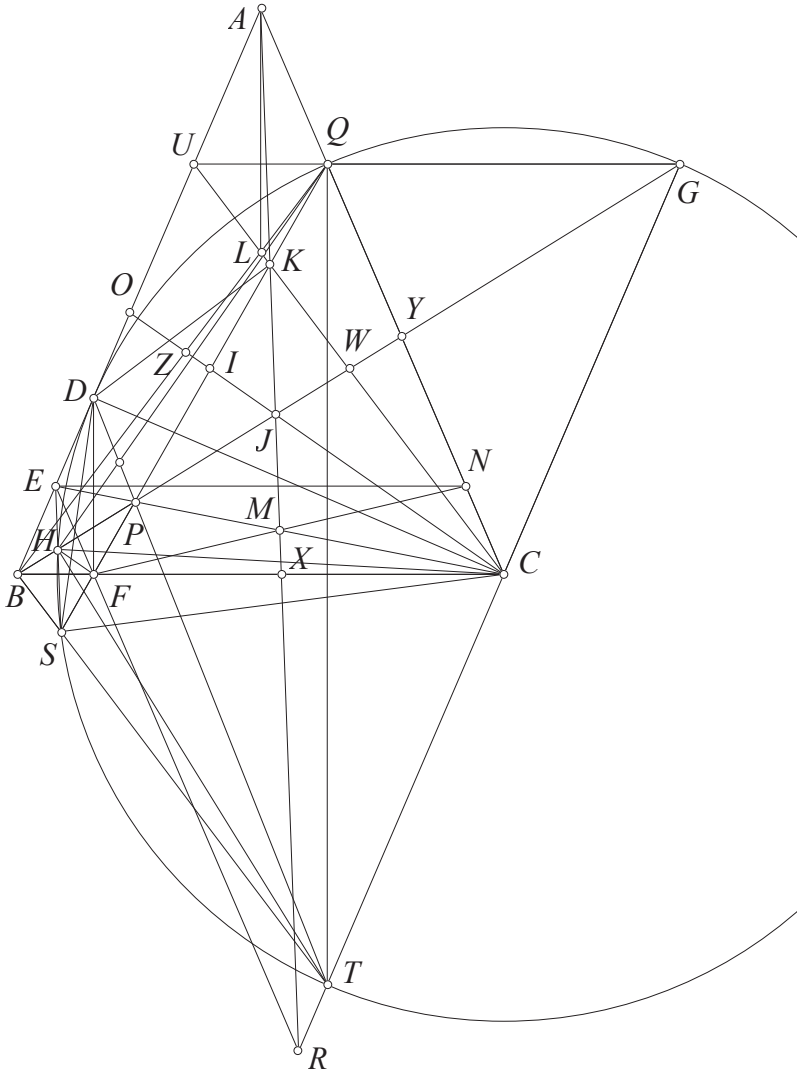
Đây là bài toán thú vị trên một mô hình không đối xứng. Bài toán được giải trên THTT số 469 [1] bởi tác giả **Nguyễn Đức Bảo**. Chúng tôi sẽ đưa ra thêm các khai thác và lời giải trên mô hình của bài toán này. Ta xét bài toán sau

Bài toán 2. Cho tam giác ABC cân tại A có đường cao CD. Gọi E là trung điểm của BD, M là trung điểm CE, phân giác của $\angle BDC$ cắt CE tại P. Đường tròn tâm C bán kính CD cắt AC tại Q. Gọi K là giao điểm của PQ và AM. F là hình chiếu vuông góc của D lên BC.

a) Chứng minh rằng tam giác CKD vuông.

b) Lấy S thuộc PF sao cho $ES \parallel AM$. Chứng minh rằng $CS = CD$.

c) Chứng minh rằng BP và ES cắt nhau trên (C).



Hình 2.

Lời giải. a) Gọi T là giao của DP với đường tròn tâm C bán kính CD. Do DT là phân giác $\angle CDE$ và BD là tiếp tuyến của đường tròn tâm (C) nên $\angle DCT = 2\angle DBT = 90^\circ$ nên

$CT \perp DC$. Lại có tam giác CDQ cân tại C nên ta có biến đổi góc

$$\angle CQT = \angle DQC - 45^\circ = 90^\circ - \frac{\angle DCQ}{2} - 45^\circ = 45^\circ - \frac{90^\circ - \angle BAC}{2} = \frac{\angle BAC}{2}$$

do đó $QT \perp BC$. Tam giác DEF và tam giác TCQ có các cạnh tương ứng song song nên DT, FQ và CE đồng quy tại P. Mặt khác do $EF \parallel AC$ nên nếu N là đối xứng của F qua M thì N thuộc AC. Áp dụng định lí Menelaus cho tam giác QFN với M, K, A thẳng hàng, ta có

$$\frac{KQ}{KF} \cdot \frac{AN}{AQ} \cdot \frac{MF}{MN} = 1 \text{ từ đó } \frac{KQ}{KF} = \frac{AQ}{AN}$$

Gọi BQ cắt CK tại L. Áp dụng định lí Menelaus cho tam giác QBF với L, K, C thẳng hàng thì

$$\frac{LB}{LQ} \cdot \frac{KQ}{KF} \cdot \frac{CF}{CB} = 1$$

với chú ý $EF \parallel AC$ nên $\frac{CF}{CB} = \frac{AE}{AB}$ và $AN = AE$ ta thu được

$$\frac{LB}{LQ} = \frac{KF}{KQ} \cdot \frac{CB}{CF} = \frac{AN}{AQ} \cdot \frac{AB}{AE} = \frac{AB}{AQ}$$

Do vậy AL là phân giác $\angle QAB$ nên $LB = LC$. Theo hệ thức lượng trong tam giác vuông thì $CQ^2 = CD^2 = CF.CB$ suy ra $\triangle CQF \sim \triangle CBQ$(cạnh - góc - cạnh) nên $\angle FQC = \angle QBC = \angle LCB$. Từ đó $\triangle CFQ \sim \triangle KFC$ (góc - góc) suy ra $\angle FKC = \angle FCQ = \angle DBC = \angle FDC$, vậy $KCFD$ là tứ giác nội tiếp hay $\angle CKD = 90^\circ$.

b) Lấy R đối xứng A qua M, do $EF \parallel AC$ và $AE \parallel CT$ nên dễ thấy R nằm trên EF và CT.

$$\frac{FS}{FK} = \frac{FE}{FR} = \frac{FB}{FC} \Rightarrow SB \parallel CK$$

Từ chứng minh trên ta có $\triangle KFC \sim \triangle CFQ \sim \triangle CQB$. Do đó $\frac{KF}{KC} = \frac{CQ}{CB} = \frac{CD}{CB}$

$$\frac{KF^2}{KC^2} = \frac{CD^2}{CB^2} = \frac{CF}{CB} = \frac{KF}{KS}$$

Suy ra $KC^2 = KF.KS$ nên $\angle KSC = \angle KCF = \angle CBS$. Vậy $CS^2 = CF.CB = CD^2$ nên ta kết luận $CS = CD$.

c) AM cắt BC tại X. Áp dụng định lý Menelaus cho tam giác BCE với A, M, X thẳng hàng, ta suy ra $\frac{XB}{XC} = \frac{AB}{AE} = \frac{BC}{CF}$. Gọi TG là đường kính của (C, CD). Dễ thấy B, P, G thẳng hàng và tam giác CGQ cân tại C lại có $CG \parallel AB$ nên $QG \parallel BC$. BG cắt CA tại Y.

$$\frac{YQ}{YC} = \frac{QG}{BC} = \frac{CQ}{CA} = \frac{CD}{AC}$$

$$\Rightarrow \frac{QC}{YC} = \frac{CD + AC}{AC} \Rightarrow \frac{YC}{AC} = \frac{CD}{CD + AC}$$

Do vậy $\frac{YC}{YA} = \frac{CD}{AC}$. Gọi I là trung điểm của FQ. CI cắt BQ tại Z. Áp dụng định lý Menelaus cho tam giác QBF với Z, I, C thẳng hàng thì $\frac{ZQ}{ZB} = \frac{CF}{CB}$. CZ cắt AB tại O, áp dụng Menelaus cho tam giác AQB với O, I, C thẳng hàng thì

$$\frac{OB}{OA} = \frac{CQ}{CA} \cdot \frac{ZB}{ZQ} = \frac{CD}{AC} \cdot \frac{CF}{CB}$$

$$\Rightarrow \frac{XB}{XC}\cdot\frac{YC}{YA}\cdot\frac{OA}{OB}=\frac{BC}{CF}\cdot\frac{CD}{AC}\cdot\frac{CD.CF}{AC.CB}=1$$

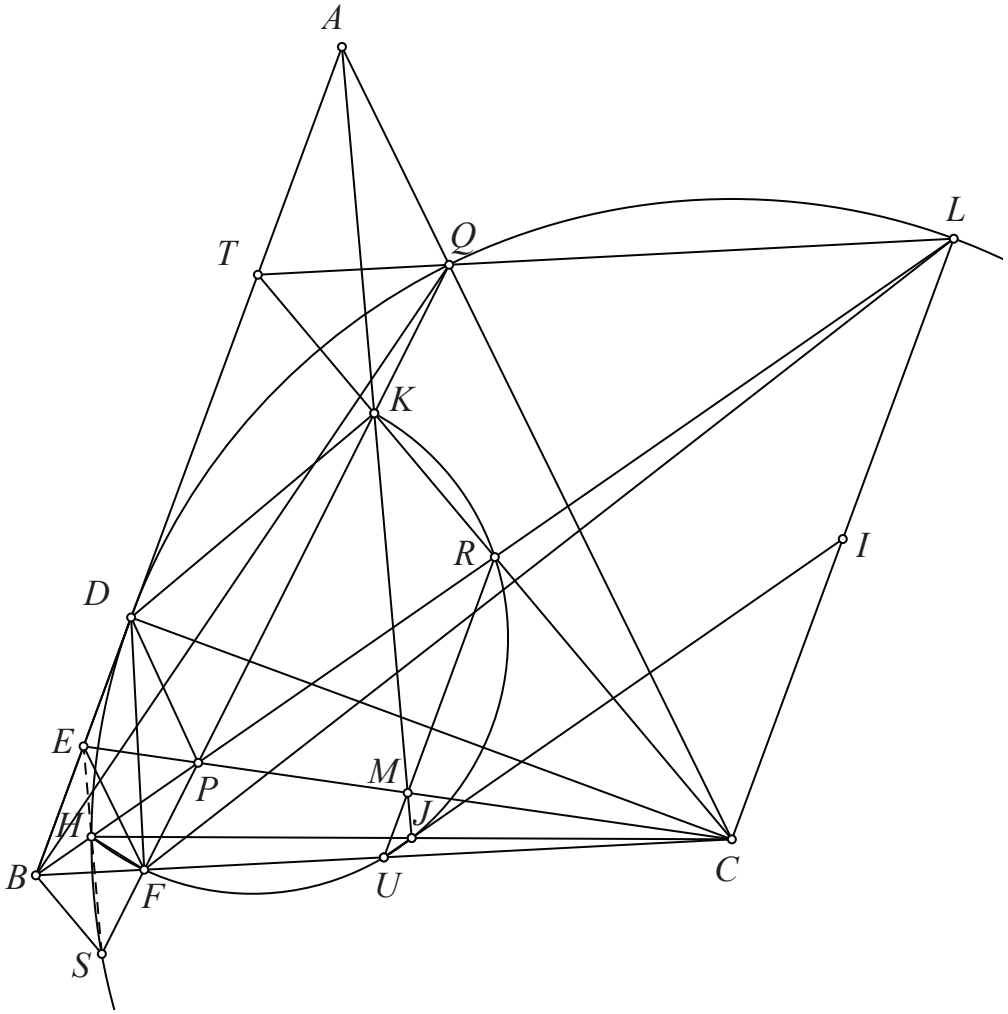
Nên AX, BY, CZ đồng quy tại J. CL cắt AB tại U. Dễ thấy $QU \parallel BC$ nên $BUGC$ là hình bình hành nên BG đi qua trung điểm W của UC. Ta chú ý các tam giác đồng dạng và bằng nhau $\triangle CFQ \sim \triangle CQB = \triangle BUC$. Mà CI, BW là trung tuyến tương ứng của hai tam giác CFQ và BUC nên $\angle ICQ = \angle WBC = \angle WGQ \Rightarrow$ tứ giác $CGQJ$ nội tiếp. Cùng với

$$\angle KQU = \angle QFC = \angle BQC = \angle QBA + \angle QAB = \angle KCA + \angle QCG = \angle KCG$$

nên tứ giác $QKCG$ nội tiếp. Vậy C, J, K, Q, G đồng viên. BG cắt (C, CD) tại H khác G. Ta có $\angle HSQ = \angle HGQ = \angle SKJ$. Từ đó $HS \parallel AM \parallel ES$ nên H thuộc ES.

Bạn **Đỗ Xuân Long** lớp 10 Toán, THPT chuyên KHTN đề xuất một lời giải khác cho ý c) như sau

Qua C vẽ $CL \parallel AB$, không khó để thấy rằng L thuộc BP và $QL \parallel BC$. Gọi QL cắt KC ở T thì vì tam giác DKC vuông tại K và ta có $\angle TKQ = \angle QCB = \angle CQL = \angle CLQ$ nên K thuộc AB suy ra trung điểm R của BL nằm trên (KMF). Gọi H là giao điểm của BP với (C), ta sẽ chứng minh E, H, S thẳng hàng. Vì $HFCL$ là tứ giác nội tiếp và chú ý rằng $BS \parallel CK$ ở đây ta coi S là điểm sao cho $ES \parallel AM$ thì theo phần b) ta có S thuộc (C) nên $BHFS$ là tứ giác nội tếp, do vậy ta quy về chứng minh $\angle CBH = \angle DKP$. Sử dụng định lí Pascal đảo cho P, M, C thẳng hàng ta có AK và CH cắt nhau tại J thuộc đường tròn $(KRUFH)$, suy ra $\angle JKF = \angle JHF = \angle FLC = \angle CBL$ và ta có điều phải chứng minh.



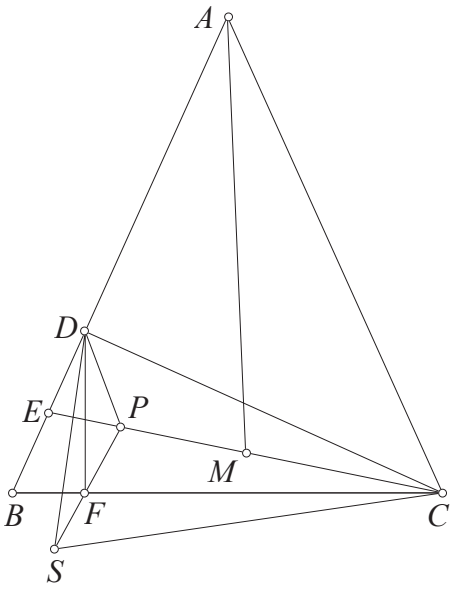
Hình 3.

□

Nhận xét. Cả ba ý của bài toán này thực chất là các bài toán chứng minh cắt nhau trên đường tròn mà hai đường thẳng không xuất phát từ hai điểm nằm trên đường tròn này. Đây là một dạng toán khó đòi hỏi phải dựng thêm các điểm nằm trên đường tròn mà hai đường thẳng đó đi qua.

Như vậy ngoài bài toán 1 là phần a), chúng ta có thể tách riêng các phần b), c) thành các bài toán dưới đây

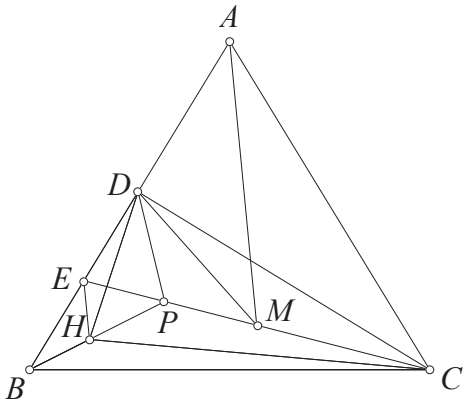
Bài toán 3. Cho tam giác ABC cân tại A có đường cao CD. Gọi E là trung điểm của BD, M là trung điểm CE, phân giác của $\angle BDC$ cắt CE tại P. F là hình chiếu của D trên BC. Lấy S thuộc PF sao cho $ES \parallel AM$. Chứng minh rằng $CS = CD$.



Hình 4.

Cách phát biểu sau của phần c) cũng có trong [3]

Bài toán 4. Cho tam giác ABC cân tại A và đường cao CD. E, M là trung điểm của BD, CE. DP là phân giác của tam giác CDE. H thuộc BP sao cho $EH \parallel AM$. Chứng minh rằng $CH = CD$.



Hình 5.

Trong [3] có đưa ra một cách tiếp cận khá đơn giản cho bài toán 4 này là dùng phương pháp tọa độ. Tuy nhiên chúng tôi không đưa lời giải này vào vì lời giải tọa độ không đẹp. Cũng như vậy với với các bài toán 1 và bài toán 3, chúng tôi cũng có nhận xét rằng phương pháp tọa độ là khá hữu dụng trong việc chứng minh trực tiếp các bài toán này. Nếu so sánh chúng với các lời giải thuần túy hình học mà chúng tôi đã trình bày trong bài toán 2 thì độ phức tạp của lời giải với phương pháp tọa độ giảm đi đáng kể. Những ví dụ này làm cho chúng ta phần nào thấy được những lợi thế rất lớn từ phương pháp tọa độ, tuy nhiên vì tính đẹp mắt của lời giải thì chúng tôi vẫn ưu tiên trình bày các cách tiếp cận thuần túy hình học.

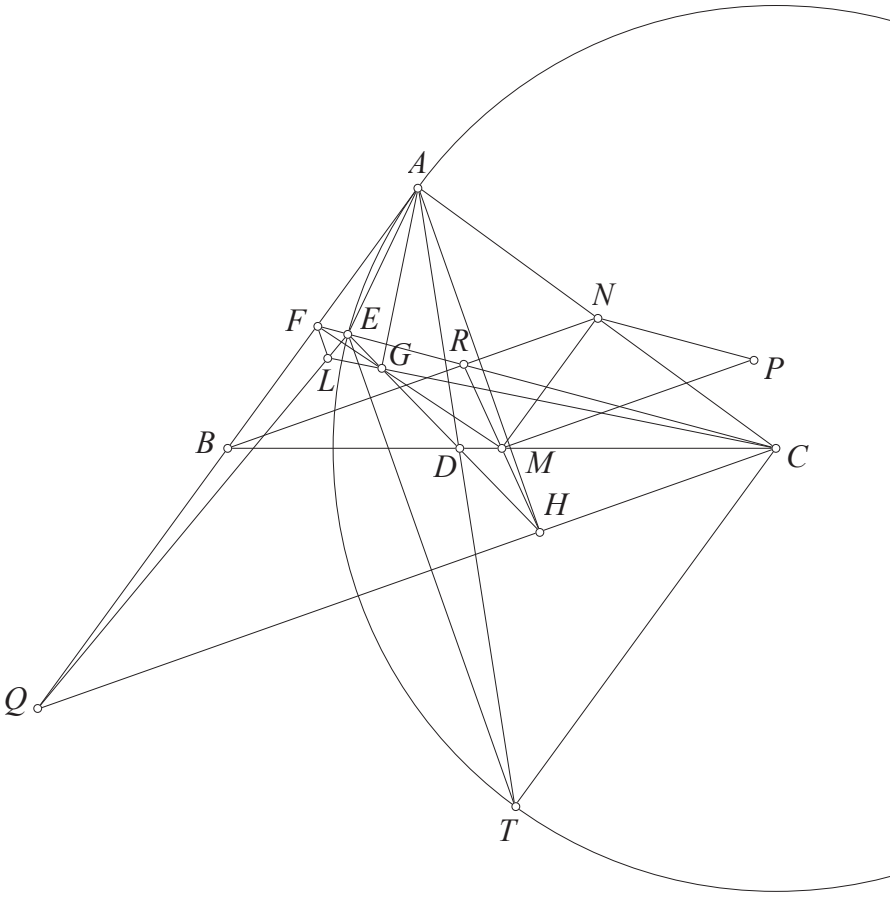
2. Một số ứng dụng

Phần này sẽ ứng dụng chủ yếu là các bài toán 1, 3, 4 và cách chứng minh tường minh của ba bài toán này đã có trong bài toán 2.

Khi thay đổi cách phát biểu của bài toán 1, ta thu được bài toán sau

Bài toán 5. Cho tam giác ABC vuông tại A và phân giác AD. M, N là trung điểm của BC, AC. Dựng điểm P sao cho $NM = NP$ và $MP \parallel BN$. F thuộc AB sao cho $CF \parallel NP$. E thuộc CF sao cho $CE = AC$. DE cắt FM tại G. Chứng minh rằng $\angle AGC = 90^\circ$.

Lời giải sau mô phỏng cách làm của tác giả **Nguyễn Đức Bảo**.



Hình 6.

Lời giải 1. Lấy Q đối xứng A qua B. Ta thấy tam giác QFC và MNP có cạnh tương ứng song song nên tam giác QFC cân tại F. Gọi T là giao của AD với đường tròn tâm C bán kính CA. Do AT là phân giác $\angle CAB$ và QA là tiếp tuyến của đường tròn tâm (C) nên $\angle ACT = 2\angle AQT = 90^\circ$ nên $CT \perp AC$. Lại có tam giác CAE cân tại C nên ta có biến đổi góc

$$\angle CET = 135^\circ - \angle AEC = 135^\circ - \frac{90^\circ - \angle ACE}{2} = 45^\circ + \frac{\angle QFC - 90^\circ}{2} = 90^\circ - \angle FCQ$$

do đó $ET \perp QC$. Gọi H là hình chiếu của A lên QC dễ thấy tam giác BQH cân nên $BH \parallel FC$, khi đó tam giác ABH và tam giác TCE có các cạnh tương ứng song song nên AT, HE và CB đồng quy tại D. Mặt khác do $BH \parallel FC$ nên nếu R là đối xứng của H qua M thì R thuộc FC. Áp dụng định lí Menelaus cho tam giác EHR với M, G, F thẳng hàng, ta thu được

$$\frac{GE}{GH} \cdot \frac{FR}{FE} \cdot \frac{MH}{MR} = 1 \Rightarrow \frac{GE}{GH} = \frac{FE}{FR}$$

Gọi QE cắt CG tại L. Áp dụng định lí Menelaus cho tam giác EQH với L, G, C thẳng hàng thì

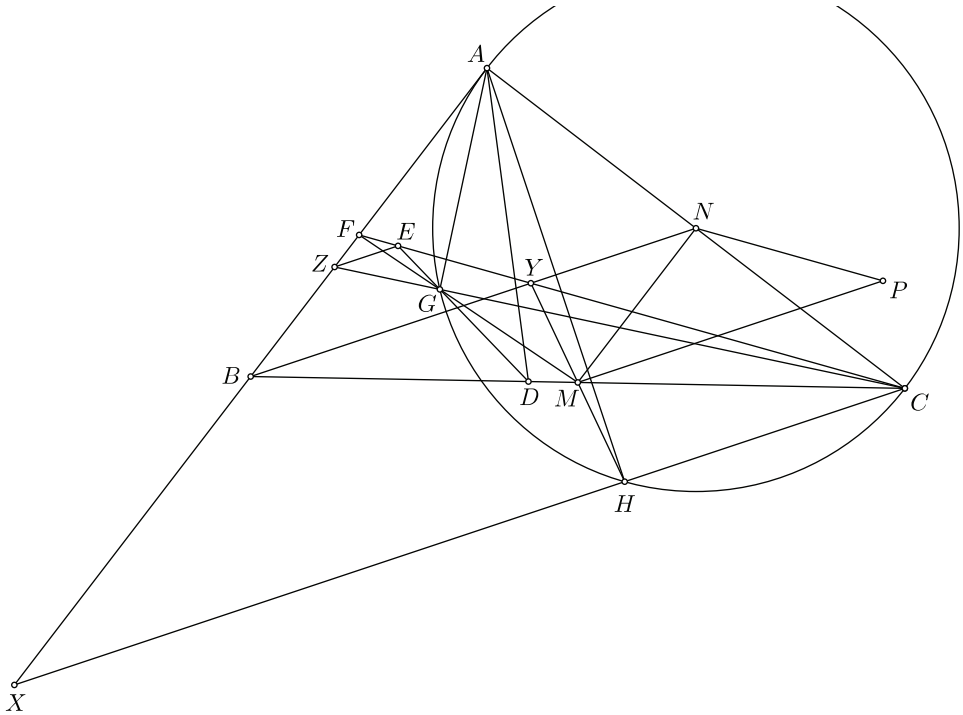
$$\frac{LQ}{LE} \cdot \frac{GE}{GH} \cdot \frac{CH}{CQ} = 1$$

với chú ý $BH \parallel FC$ nên $\frac{CH}{CQ} = \frac{FB}{FQ}$ và $FR = FB$ ta thu được

$$\frac{LQ}{LE} = \frac{GH}{GE} \cdot \frac{CQ}{CH} = \frac{FR}{FE} \cdot \frac{FQ}{FB} = \frac{FQ}{FE}$$

Do đó FL là phân giác $\angle EFQ$ nên $LQ = LC$. Theo hệ thức lượng trong tam giác vuông thì $CE^2 = CA^2 = CH.CQ$ suy ra $\angle HEC = \angle EQC = \angle LCQ$. Từ đó $\triangle CHE \sim \triangle GHC$(góc - góc) suy ra $\angle HGC = \angle HCE = \angle AQC = \angle HAC$, vậy $GCHA$ là tứ giác nội tiếp hay $\angle CGA = 90^\circ$. □

Lời giải trực tiếp sau của nickname **PSJL** sử dụng phép nghịch đảo, tham khảo [2]



Hình 7.

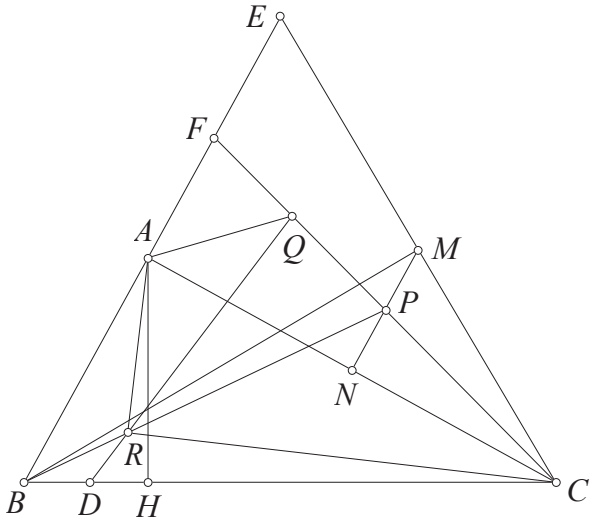
Lời giải 2. Đường thẳng qua C song song với BN cắt AB tại X. Dễ thấy $\triangle FCX \sim \triangle NPM$ do đó $FC = FX$. Gọi H là hình chiếu của A lên CX, do $BA = BX = BH$ nên $BH \parallel FC$ suy ra,

$$\frac{BH}{CE} = \frac{BA}{CA} = \frac{BD}{CD}$$

Do đó H, D, E thẳng hàng. Gọi Y là giao điểm của BN và CF, Z là giao điểm của đường thẳng qua E song song CX với FX. Do $BH = BX = CY$, $BH \parallel CY$ nên $BHCY$ là hình bình hành suy ra H, M, Y thẳng hàng. Từ đó áp dụng định lí Dersagues cho hai tam giác thấu xạ HMC và EFZ ta suy ra C, G, Z thẳng hàng. Xét phép nghịch đảo cực C, bán kính CA nên $(CA) \to FX$, $HE \to (CXE)$ qua Z do đó $G \mapsto Z$ suy ra G thuộc (CA) hay $\angle AGC = 90^\circ$. □

Cũng tương tự cách làm trên, nếu phát biểu bài toán 1 theo cách khác ta có bài toán sau

Bài toán 6. Cho tam giác ABC vuông tại A với đường cao AH. AD là phân giác của tam giác AHB. Trung trực CA cắt phân giác $\angle ABC$ tại M. N, P là trung điểm AC, MN. CP cắt phân giác ngoài góc A tại Q. DQ cắt BP tại R. Chứng minh rằng $\angle ARC = 90^\circ$.

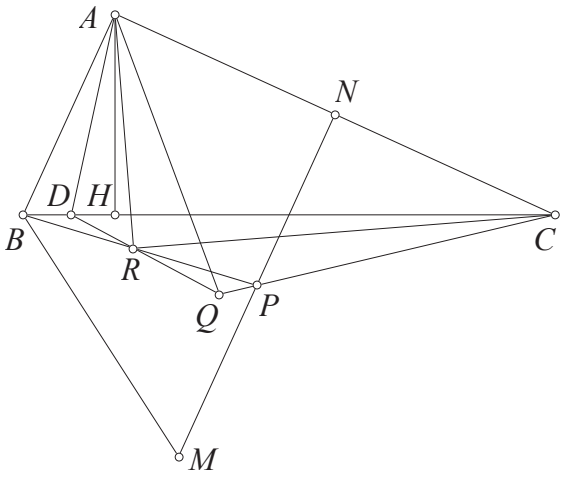


Hình 8.

Lời giải. Dễ thấy M nằm trên đường tròn ngoại tiếp tam giác ABC nên $\angle AMC = 90^\circ$. Gọi CM cắt AB tại E khi đó tam giác BEC cân tại B có đường cao CA và CP đi qua trung điểm F của AE. P cũng là trung điểm CF. Áp dụng trực tiếp bài toán 1 vào tam giác BEC cân tại B thì ta thu được $\angle ARC = 90^\circ$. □

Đến đây ta lại thấy rằng ta hoàn toàn có thể phát biểu bài toán cho phân giác trong góc A với cách chứng minh hoàn toàn tương tự

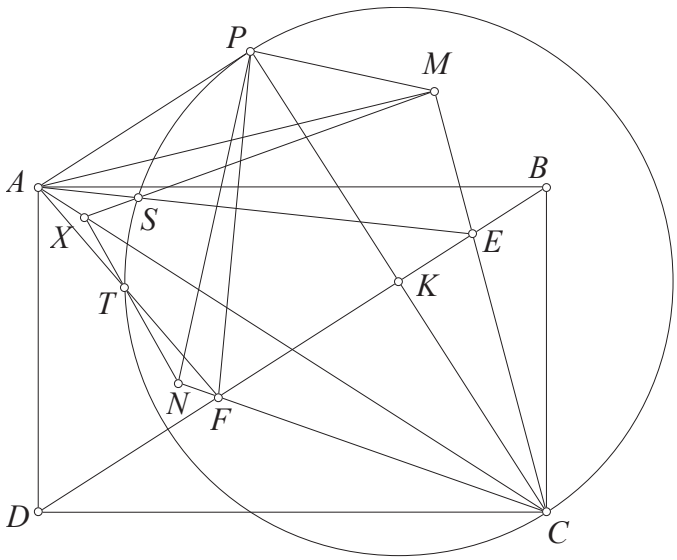
Bài toán 7. Cho tam giác ABC vuông tại A với đường cao AH. AD là phân giác của tam giác AHB. Trung trực CA cắt phân giác ngoài góc $\angle ABC$ tại M. N, P là trung điểm AC, MN. CP cắt phân giác góc $\angle BAC$ tại Q. DQ cắt BP tại R. Chứng minh rằng $\angle ARC = 90^\circ$.



Hình 9.

Đến đây việc kết hợp cả hai bài toán 6, 7 này sẽ cho ta một bài toán đồng quy thú vị sau

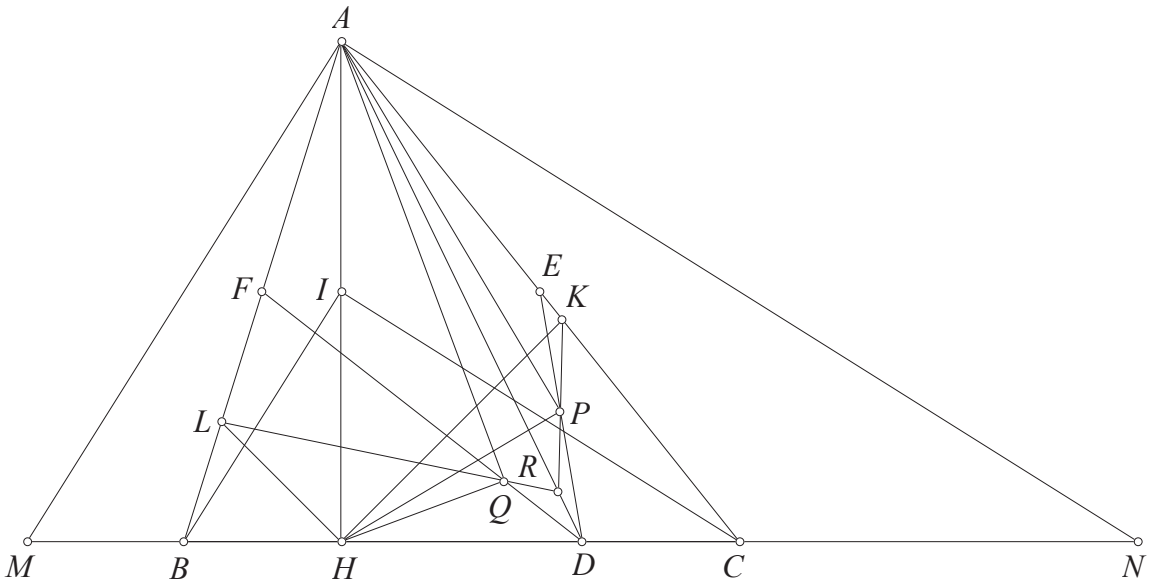
Bài toán 8. Cho hình chữ nhật $ABCD$. P đối xứng với C qua BD. (K) là đường tròn đường kính PC. E, F là trung điểm của KB, KD. CE, CF lần lượt cắt phân giác ngoài và phân giác trong $\angle BPC$ tại M, N. Đoạn thẳng AE, AF lần lượt cắt đường tròn (K) tại S, T. Chứng minh rằng MS, NT và AC đồng quy.



Hình 10.

Bài toán sau có thể coi là một ứng dụng được rút ra từ bài toán 1, tuy nhiên nếu chưa được biết bài toán 1 thì bài toán này cũng là một thách thức lớn

Bài toán 9. Cho tam giác ABC nhọn với đường cao AH sao cho trung điểm của AH nhìn BC dưới một góc vuông. Lấy D đối xứng H qua trung điểm BC. E, F là trung điểm của CA, AB. Các điểm P, Q lần lượt thuộc đoạn DE, DF sao cho $\angle APH = \angle AQH = 90^\circ$. HK, HL là phân giác của các tam giác HCA, HAB. Chứng minh rằng KP, LQ và AD đồng quy.

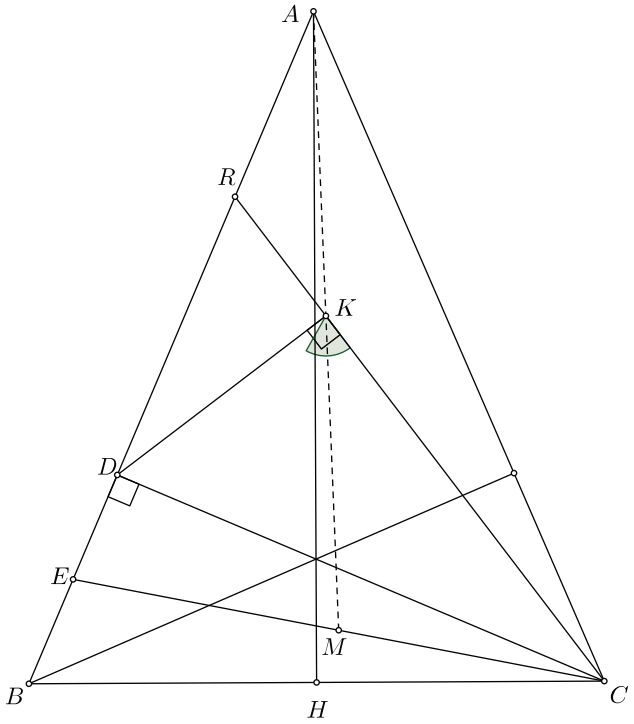


Hình 11.

Lời giải. Gọi I là trung điểm AH thì $\angle BIC = 90^\circ$. Từ đó gọi M, N là các điểm nằm trên đường thẳng BC sao cho $AM \parallel IB$, $AN \parallel IC$. Từ đó tam giác AMN vuông tại A và B, C lần lượt là trung điểm HB, HC nên $DN = DC + CN = BH + HC = MB + BD = DM$. Từ đó D là trung điểm MN nên các tam giác DAM và DAN cân tại D. Áp dụng trực tiếp bài toán 2 phần a) vào các tam giác cân DAM, DAN ta thấy LQ, KP cùng đi qua điểm R thuộc AD thỏa mãn $AR = AH$. □

Bài toán sau có thể được coi là một hệ quả bài toán 1 nhưng được giải độc lập như sau

Bài toán 10. Cho tam giác ABC cân tại A có đường cao CD. Gọi E, M là trung điểm của BD, CE. R thuộc AB sao cho $BR = CD$. CR cắt AM tại K. Chứng minh rằng $\angle CKD = 90^\circ$.



Hình 12.

Lời giải. Áp dụng định lí Menelaus cho tam giác REC với ba điểm M, K, A thẳng hàng, ta suy ra

$$\frac{MC}{ME}\cdot\frac{KR}{KC}\cdot\frac{AE}{AR}=1 \text{ từ đó } \frac{KR}{KC}=\frac{AR}{AE}$$

Ta cần chứng minh

$$\frac{KR}{KC}=\frac{DR^2}{DC^2} \text{ tức là chứng minh } \frac{DR^2}{DC^2}=\frac{AR}{AE}$$

Gọi H là chân đường vuông góc kẻ từ A xuống BC, chú ý $\triangle BDC\sim\triangle BHA$ (góc - góc) ta suy ra

$$AR=AB-CD=AB-\frac{BC.AH}{AB}=\frac{AB^2-BC.AH}{AB}$$

$$AE=AB-\frac{BD}{2}=AB-\frac{BH^2}{AB}=\frac{AB^2-BH^2}{AB}$$

Chú ý đẳng thức trên thu được do $2BH=BC$. Nên ta suy ra

$$\frac{AR}{AE}=\frac{AB^2-BC.AH}{AB^2-BH^2}$$

Mặt khác

$$\frac{DR^2}{DC^2}=\frac{(CD-DB)^2}{DC^2}=\frac{(AH-BH)^2}{AH^2}$$

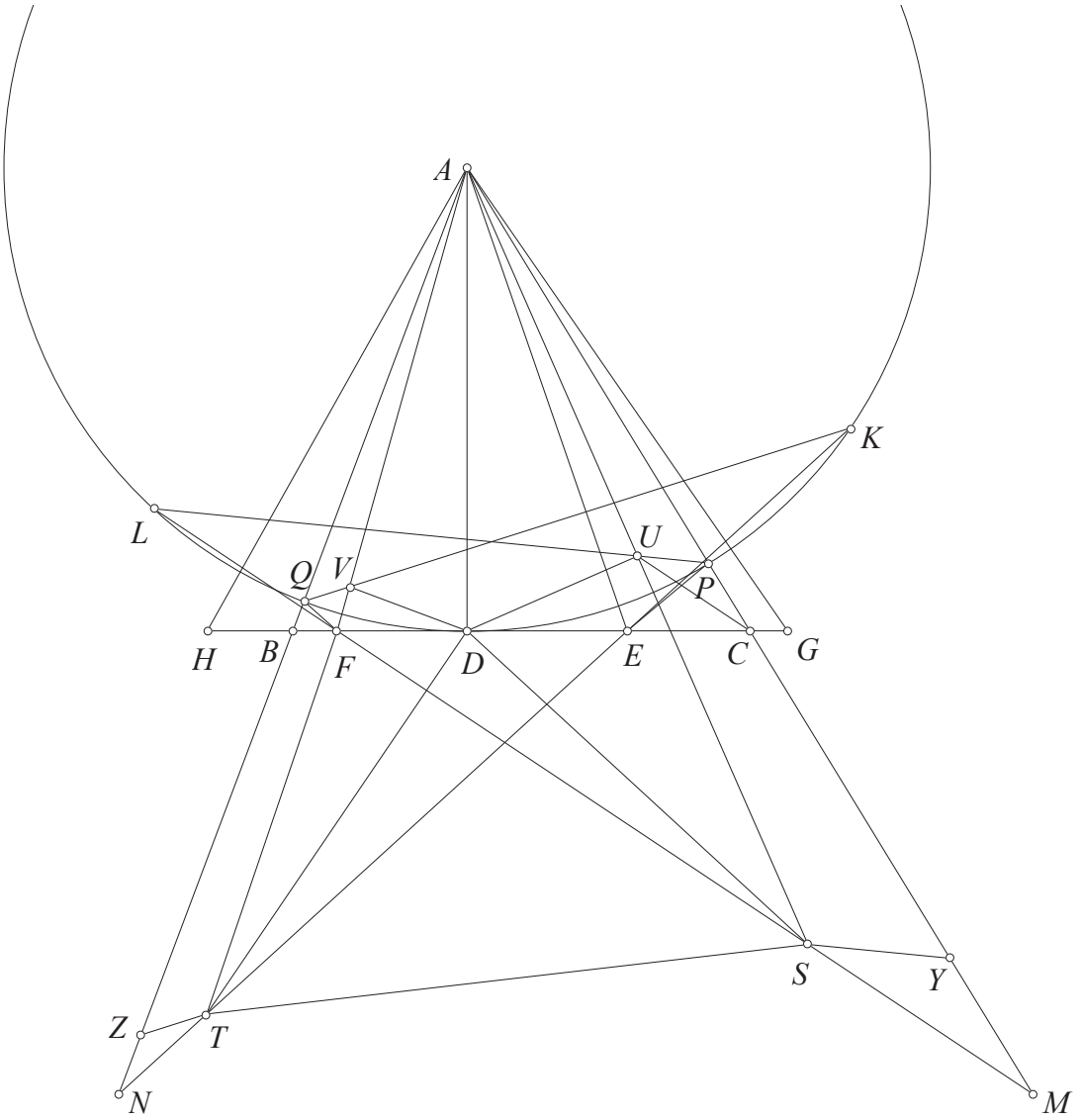
Do vậy chỉ cần chứng minh

$$\frac{AB^2-BC.AH}{AB^2-BH^2}=\frac{(AH-BH)^2}{AH^2}=\frac{AH^2+BH^2-2AH.BH}{AH^2}$$

Điều này tương đương với chứng minh $(AB^2-BC.AH).AH^2 = (AH^2+BH^2-2AH.BH)(AB^2-BH^2)$. Đẳng thức trên hiển nhiên đúng do $AB^2 - BH^2 = AH^2$. Vậy $\angle CKD = 90^\circ$. □

Bài toán sau được xây dựng dựa trên phần b) của bài toán 2

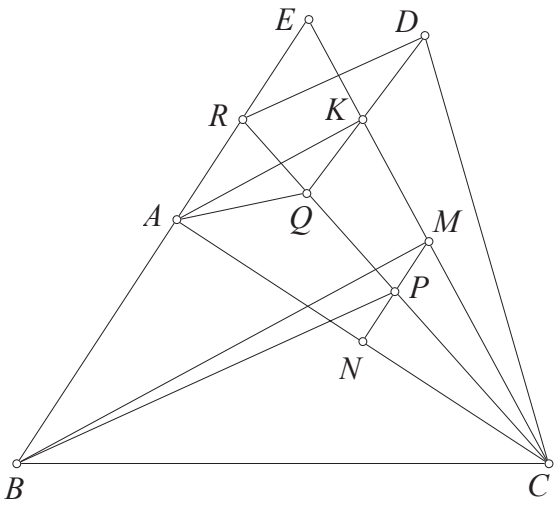
Bài toán 11. Cho tam giác ABC có đường cao AD. Trên tia BC, CB lấy các điểm G, H sao cho $BG = BA$, $CH = CA$. E, F là trung điểm của DG, DH. Đường tròn (A, AD) cắt CA, AB tại P, Q. M, N, Y, Z lần lượt đối xứng A qua C, B, P, Q. NE cắt đường tròn (A, AD) tại K sao cho K, N khác phía đường thẳng qua A vuông góc KN. MF cắt đường tròn (A, AD) tại L sao cho L, M khác phía đường thẳng qua A vuông góc LM. Lấy S, T thuộc MF, NE sao cho $YS \parallel PL$ và $ZT \parallel QK$. Chứng minh rằng $DS = DT$.



Hình 13.

Lời giải. Gọi U, V là trung điểm của AS, AT. Như vậy U thuộc LP để $MF \parallel CU$, áp dụng bài toán 2 phần b) trên vào tam giác cân CAH thì $\angle AUD = 90^\circ$. Tương tự $\angle AVD = 90^\circ$. Vậy $DA = DS = DT$. □

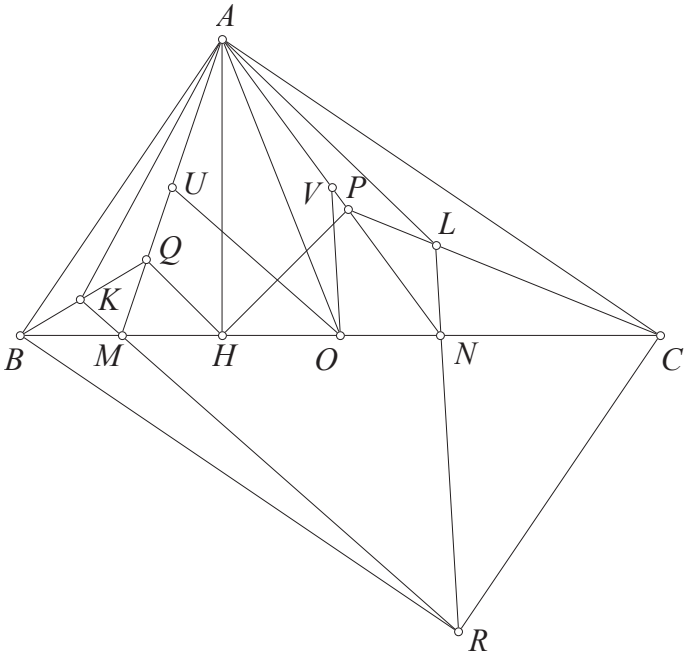
Bài toán 12. Cho tam giác ABC vuông tại A. Trung trực CA cắt phân giác ngoài góc $\angle ABC$ tại M. N, P là trung điểm AC, MN. CP cắt phân giác góc $\angle BAC$ tại Q. CQ cắt AB tại R. K là hình chiếu của A trên CM. D thuộc QK sao cho $RD \parallel BM$. Chứng minh rằng $CD = CA$.



Hình 14.

Lời giải. Gọi CK cắt AB tại E dễ thấy tam giác BCE cân tại B và có đường cao CA đồng thời R, P là trung điểm của AE và CR. Từ đó áp dụng bài toán 3 vào tam giác cân BCE ta thu được $CD = CA$. □

Bài toán 13. Cho tam giác ABC vuông tại A với đường cao AH. M, N là trung điểm của HB, HC. HP, HQ là phân giác của tam giác HAC, HAB. Trên đoạn BQ, CP lấy các điểm K, L sao cho $AK = AH = AL$. LN cắt KM tại R. Chứng minh rằng $ABRC$ là hình chữ nhật.



Hình 15.

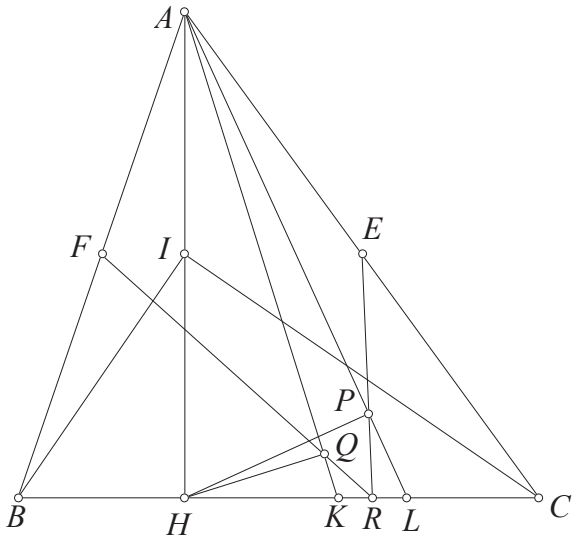
Lời giải. Gọi O là trung điểm BC thì các tam giác OCA, OAB cân tại O và đều có đường cao AH. Gọi khi đó nếu U, V là trung điểm của AM, AN thì theo bài toán 3 ta có $LN \parallel OV$ và $KM \parallel OU$. Từ đó theo tính chất phép vị tự tâm A tỷ số 2 thì LN, KM đi qua đối xứng của A qua O nên R là đối xứng của A qua O. Từ đó $ABRC$ là hình chữ nhật. □

3. Một số bài toán luyện tập

Bài toán 14. Cho tam giác ABC cân tại A, đường cao CD. E, M lần lượt là trung điểm BD, CE. DP là phân giác trong của tam giác CDE. H thuộc BP sao cho $EH \parallel AM$. Gọi F là hình chiếu của D lên BC. R, Q lần lượt là giao điểm của FP với DH và AC. Chứng minh rằng BR, DP và đường thẳng qua Q song song với BC đồng quy.

Bài toán 15. Cho tam giác ABC cân tại A, đường cao CD. E, M lần lượt là trung điểm BD, CE. DP là phân giác trong của tam giác CDE. Gọi F là đối xứng của D qua BC. S thuộc PF sao cho $ES \parallel AM$. SP cắt AC tại Q. R là giao của DS và đường thẳng qua Q song song với BC. Chứng minh rằng RP, ES và đường thẳng qua Q vuông góc với BC đồng quy.

Bài toán 16. Cho tam giác ABC nhọn có đường cao AH sao cho trung điểm AH nhìn BC dưới góc vuông. E, F là trung điểm CA, AB. Trên đoạn BC lấy các điểm K, L sao cho $BK = AH - BH$ và $CL = AH - CH$. P, Q là hình chiếu của H lên AL, AK. Chứng minh rằng EP, QF và BC đồng quy.



Hình 16.

Tài liệu

[1] Tạp chí toán học và tuổi trẻ số 465 và số 469

[2] Topic Right angle
http://artofproblemsolving.com/community/q1h1276419p6696477

[3] Topic Equal segments in isosceles triangle
http://artofproblemsolving.com/community/q1h1280275p6732257

MỘT BỔ ĐỀ VỀ PHÂN GIÁC

Nguyễn Trần Hữu Thịnh
Trường THPT chuyên Lý Tự Trọng, Cần Thơ

TÓM TẮT

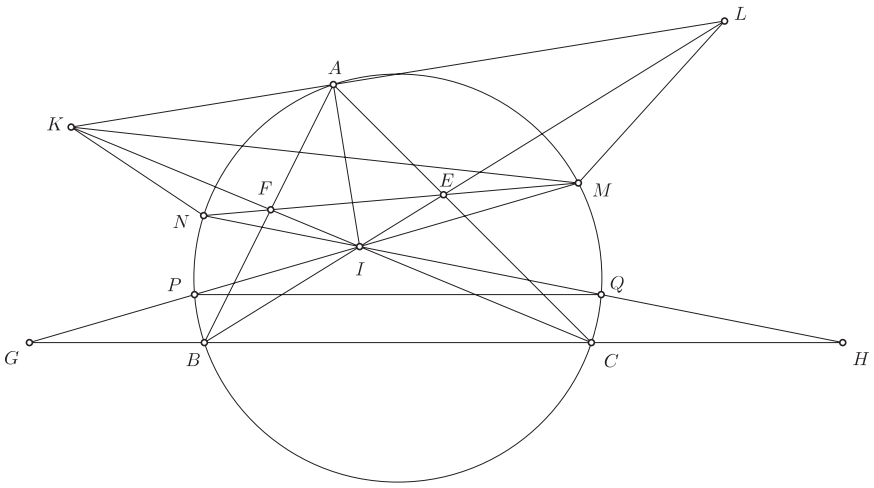
Bài viết xoay quanh một bổ đề hay có nhiều mở rộng với cách giải quyết bằng các công cụ hình học phẳng thuần túy.

1. Mở đầu

Khi tìm hiểu về vấn đề phân giác trong tam giác, tác giả phát hiện được một cấu hình khá đẹp và có nhiều ứng dụng, cụ thể ta có bài toán sau [1]

Bài toán 1. *$\triangle ABC$ nội tiếp đường tròn (O) có các phân giác trong BE, CF cắt nhau tại I. EF cắt (O) tại M, N. Các đường thẳng MI, NI cắt (O) lần lượt tại P, Q khác M, N. Khi đó PQ song song BC.*

Bài toán trên có nhiều lời giải, sau đây tác giả xin nêu ba cách:



Biên tập: Ngô Quang Dương

Lời giải 1. Đường phân giác ngoài của góc A trong $\triangle ABC$ cắt BI, CI theo thứ tự tại L, K nên ta có L, K lần lượt là tâm đường tròn bàng tiếp góc B, C của $\triangle ABC$. Với chú ý rằng tứ giác $AICL$ nội tiếp, ta có:

$$\overline{EN} \cdot \overline{EM} = \overline{EA} \cdot \overline{EC} = \overline{EI} \cdot \overline{EL}$$

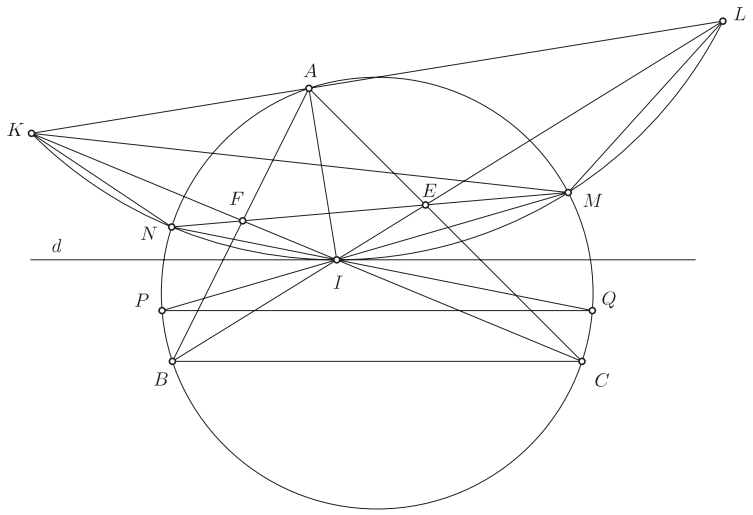
Do đó tứ giác $NIML$ nội tiếp. Tương tự $NIMK$ nội tiếp nên năm điểm K, N, I, M, L cùng thuộc một đường tròn.
Kéo dài MP, NQ cắt BC lần lượt tại G, H. Ta có:

$$(CK, CG) = (CA, CI) = (LA, LI) = (LK, LI) = (MK, MI)$$

Suy ra tứ giác $KMCG$ nội tiếp, từ đó:

$$(GI, GH) = (KM, KI) = (NM, NI) = (PI, PQ)$$

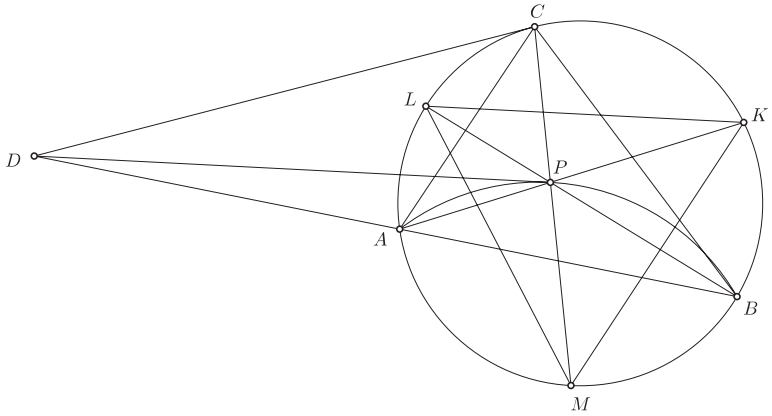
Như vậy PQ song song BC. Ta có điều phải chứng minh. □



Lời giải 2. Cũng như **Lời giải 1**, ta có đa giác $KLMIN$ nội tiếp đường tròn ω. Gọi d là tiếp tuyến tại I của ω. Ta có $(IK, Id) = (LK, LI) = (CI, CB)$ nên d song song BC. Mặt khác $(QI, QP) = (MN, MI) = (IN, Id)$ suy ra d song song PQ. Như vậy PQ song song BC. Vậy bài toán đã được giải xong. □

Ở **Lời giải 3** tác giả xét bổ đề sau:

Bổ đề. (IMO 2010) $\triangle ABC$ nội tiếp đường tròn Γ, P là một điểm nằm trong đường tròn. AP, BP, CP lần lượt cắt Γ tại K, L, M. Tiếp tuyến tại C của Γ cắt AB tại D. Chứng minh rằng nếu $DC = DP$ khi và chỉ khi $MK = ML$.



Chứng minh bổ đề. Do $\triangle LPM \sim \triangle CPB$ và $\triangle KPM \sim \triangle CPA$ nên:

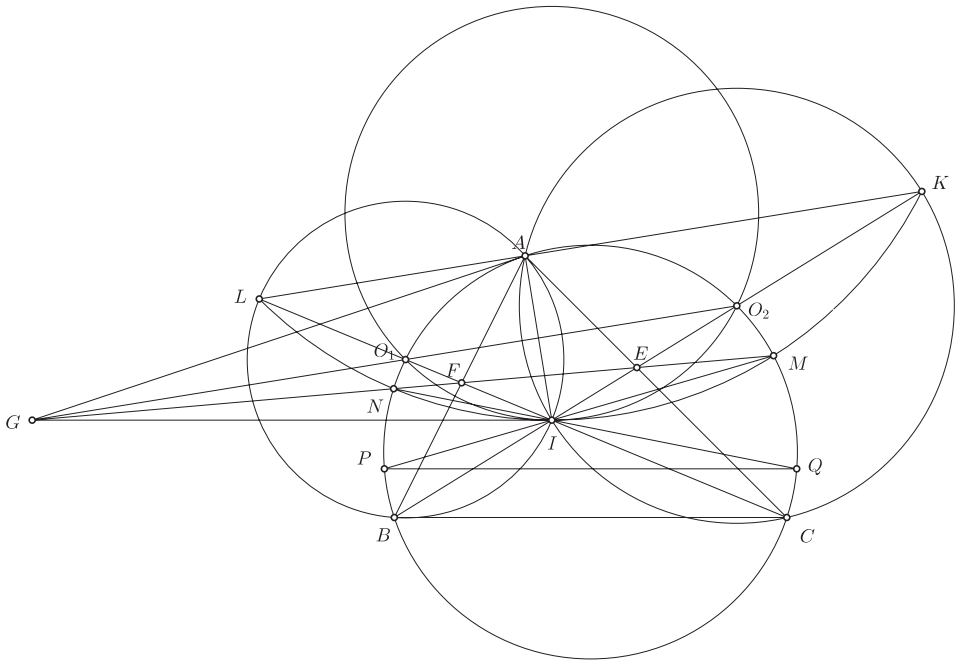
$$\frac{ML}{MP} = \frac{BC}{BP} \text{ và } \frac{MK}{MP} = \frac{AC}{AP}$$

Suy ra:

$$MK = ML \Leftrightarrow \frac{BC}{BP} = \frac{AC}{AP} \Leftrightarrow \frac{BC}{AC} = \frac{BP}{AP}$$

Do đó P thuộc đường tròn Apollonius tỉ số $\dfrac{CA}{CB}$ dựng trên đoạn AB. Hơn nữa D chính là tâm của đường tròn này nên $MK = ML$ khi và chỉ khi $DC = DP$. □

Quay trở lại bài toán,



Lời giải 3. Gọi O_1, O_2 lần lượt là tâm đường tròn ngoại tiếp $\triangle ABI$ và $\triangle ACI$. Ta đã biết O_1, O_2 nằm trên (O). Gọi K, L lần lượt là tâm đường tròn bàng tiếp góc B, C của $\triangle ABC$. Do O_1,

O_2 theo thứ tự là trung điểm của LI, KI nên (IO_1O_2) tiếp xúc $(IKL) \equiv (IMN)$. Gọi G là giao điểm của O_1O_2 và MN. Do O_1NMO_2 nội tiếp nên:

$$\mathcal{P}_{G/(IO_1O_2)} = \overline{GO_1} \cdot \overline{GO_2} = \overline{GM} \cdot \overline{GN} = \mathcal{P}_{G/(IMN)}$$

Tức là G nằm trên trục đẳng phương của (IO_1O_2) và (IMN), suy ra GI là tiếp tuyến chung của hai đường tròn này. Mặt khác G thuộc O_1O_2 là đường trung trực của AI nên $GA^2 = GI^2 = \overline{GM} \cdot \overline{GN} = \mathcal{P}_{G/(O)}$, suy ra GA là tiếp tuyến của (O). Áp dụng bổ đề cho $\triangle AMN$ với AI, MI, NI cắt (O) theo thứ tự tại D, P, Q được $PD = QD$, suy ra $PB = QC$, như vậy PQ song song BC.
Vậy bài toán đã được giải xong. □

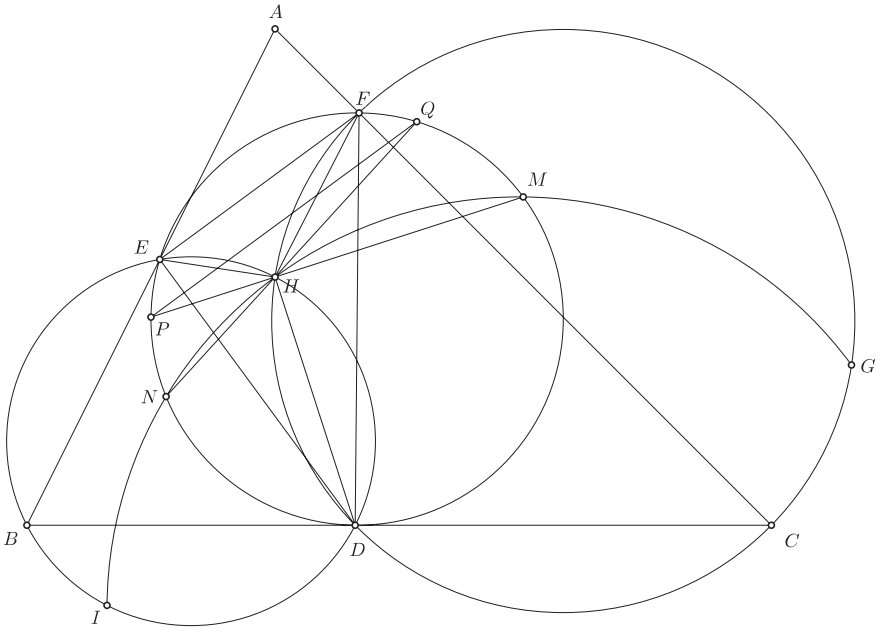
Từ **Lời giải 1** của **Bài toán 1**, ta có thể phát biểu bài toán lại như sau

Bài toán 2. *Cho $\triangle ABC$ và tâm đường tròn nội tiếp I. Gọi I_b, I_c lần lượt là tâm đường tròn bàng tiếp góc B, C của $\triangle ABC$. (II_bI_c) cắt (ABC) tại M, N. MI, NI cắt (ABC) lần thứ hai theo thứ tự tại P, Q. Chứng minh rằng PQ song song BC.*

Bài toán 3. *Cho $\triangle ABC$, đường cao AD, BE, CF đồng quy tại H. (BHC) cắt (DEF) tại M, N. MH, NH cắt (DEF) lần thứ hai theo thứ tự tại P, Q. Chứng minh rằng PQ song song EF.*

Ta có thể phát triển **Bài toán 3** thành bài toán sau:

Bài toán 4. *Cho $\triangle ABC$, trực tâm H. Lấy D là một điểm nằm trên cạnh BC. (BHD) cắt AB tại E. (CHD) cắt AC tại F. Đường thẳng HE cắt (CHD) tại G, đường thẳng HF cắt (BHD) tại I. (HGI) cắt (DEF) tại M, N. Kéo dài MH, NH cắt (DEF) lần thứ hai lần lượt tại P, Q. Chứng minh rằng PQ song song EF.*



Chứng minh. Áp dụng định lý Miquel trong $\triangle ABC$ ta được $AEHF$ nội tiếp. Từ đây dễ dàng suy ra H là tâm đường tròn nội tiếp $\triangle DEF$. Áp dụng bài toán đầu cho $\triangle DEF$ ta kết luận PQ song song EF. Vậy bài toán đã được giải xong. □

Hoặc từ **Lời giải 3** của **Bài toán 1**, bài toán có thể trở thành:

Bài toán 5. *Cho $\triangle ABC$ nội tiếp đường tròn (O), đường phân giác trong AD. I là một điểm di chuyển trên đướng thẳng AD. Tiếp tuyến tại A của (O) cắt đường trung trực của AI tại X. Một đường thẳng qua X cắt (O) tại M, N. Các tia MI, NI theo thứ tự cắt (O) tại P, Q. Chứng minh PQ song song BC.*

Sau đây ta xét một số mở rộng và ứng dụng của bài toán này.

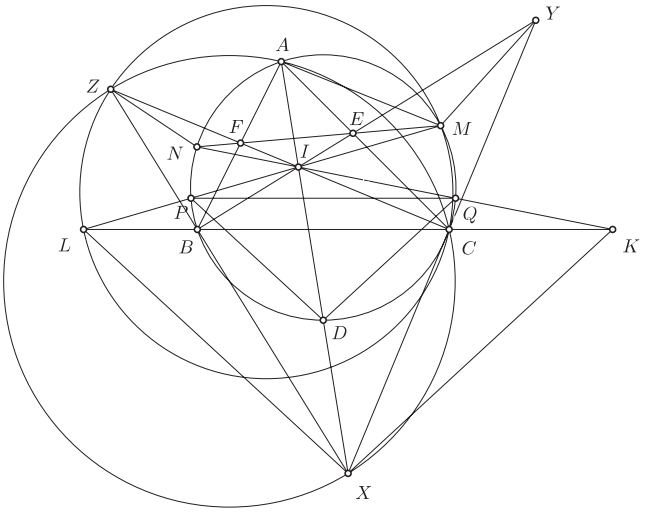
2. Khai thác bài toán

Bài toán gốc là một cấu hình đẹp và có nhiều tính chất thú vị. Bài toán sau là một kết quả về việc chia đôi đoạn thẳng.

Bài toán 6. *Cho $\triangle ABC$ nội tiếp đường tròn (O) có các phân giác BE, CF cắt nhau tại I. EF cắt (O) tại M, N. Các đường thẳng MI, NI cắt (O) lần lượt tại P, Q. Khi đó PQ chia đôi BI và CI.*

Tính chất này được phát hiện khi tác giả tìm thêm những lời giải khác cho **Bài toán 1**. Chia đôi đoạn thẳng cũng là một kiểu bài toán đang phổ biến hiện nay, lời giải sau được đề xuất bởi anh **Nguyễn Lê Phước**.

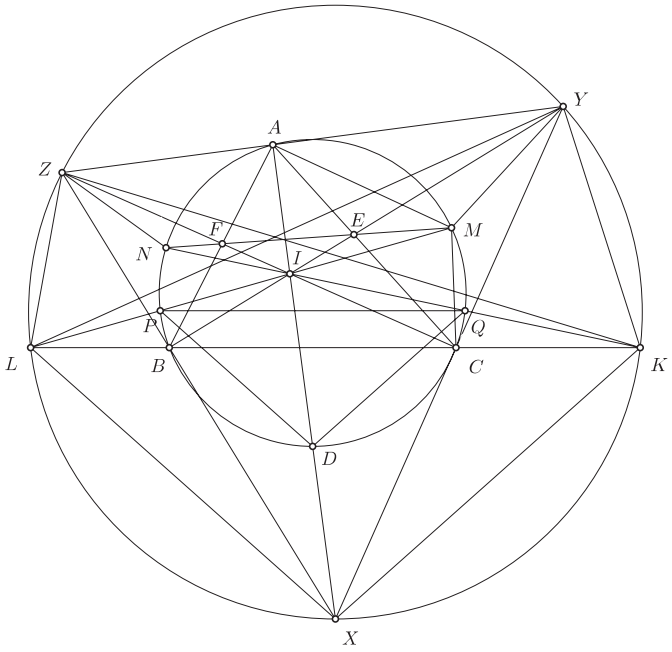
Chứng minh. Gọi X, Y, Z lần lượt là tâm đường tròn bàng tiếp góc A, B, C của $\triangle ABC$. Kéo dài IP, IQ cắt BC theo thứ tự tại L, K. Gọi D là giao điểm của AI với (O).
Như đã chứng minh ở tính chất 1, ta có tứ giác $ZMCL$ nội tiếp, kết hợp với việc bốn điểm A, C, X, Z cùng nằm trên một đường tròn, ta có $\overline{IL} \cdot \overline{IM} = \overline{IZ} \cdot \overline{IC} = \overline{IA} \cdot \overline{IX}$. Do đó tứ giác $AMXL$ nội tiếp, suy ra $(LI, LX) = (AM, AI) = (PI, PD)$. Như vậy PD song song LX. Mà D là trung điểm của IX nên P là trung điểm của IL. Tương tự Q là trung điểm của IK hay PQ là đường trung bình của $\triangle ILK$. Từ đó ta suy ra PQ chia đôi IB và IC.



Vậy bài toán đã được giải xong. □

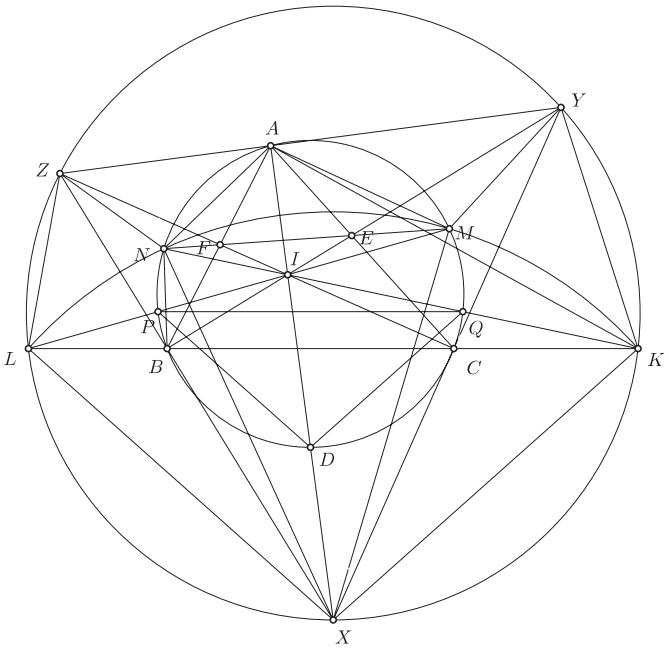
Chia đôi đoạn thẳng là một tính chất hay, thậm chí ta có thể mở rộng bài toán thành chia đoạn thẳng theo tỉ số k, sau đây ta có một khai thác nhiều bài toán khá đẹp như sau:

Bài toán 7. *Cho $\triangle ABC$ nội tiếp đường tròn (O) có các phân giác BE, CF cắt nhau tại I. EF cắt (O) tại M, N. Các đường thẳng MI, NI cắt (O) lần lượt tại P, Q. Gọi X, Y, Z lần lượt là tâm đường tròn bàng tiếp góc A, B, C của $\triangle ABC$. IP, IQ theo thứ tự cắt đường thẳng BC tại L, K. Chứng minh rằng năm điểm X, Y, Z, L, K cùng nằm trên một đường tròn.*



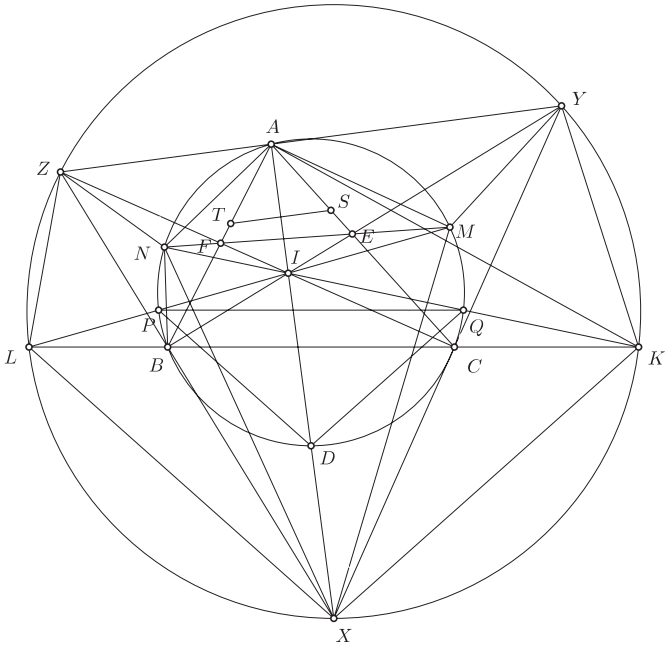
Bài toán 7 được suy ra trực tiếp từ **Bài toán 6** cùng với tính chất: *Phép vị tự tâm I tỉ số $\dfrac{1}{2}$ biến (XYZ) thành (ABC).*

Bài toán 8. *Cho $\triangle ABC$ nội tiếp đường tròn (O) có các phân giác BE, CF cắt nhau tại I. EF cắt (O) tại M, N. Các đường thẳng MI, NI cắt (O) lần lượt tại P, Q. Gọi X, Y, Z lần lượt là tâm đường tròn bàng tiếp góc A, B, C của $\triangle ABC$. IP, IQ theo thứ tự cắt đường thẳng BC tại L, K. Chứng minh rằng tứ giác $MNLK$ nội tiếp đường tròn tâm X.*



Chứng minh. Như ta thấy, để chứng minh một điểm là tâm của tứ giác thì hai hướng thường gặp nhất là biến đổi góc hoặc biến đổi cạnh, ở đây tác giả sử dụng phương pháp biến đổi cạnh thông qua việc chứng minh AN và AK là hai đường đẳng giác, vì để chứng minh $LX = NX = MX = KX$ thì đầu tiên ta có thể chứng minh $KX = NX$ và $LX = MX$ sau đó kết hợp việc $LX = KX$ đã chứng minh ở hệ quả trên ta suy ra bốn cạnh bằng nhau. Từ đó ta nghĩ đến việc chứng minh các tam giác cân thông qua việc biến đổi góc, chú ý do tứ giác $NAKX$ nội tiếp nên $(AN, AX) = (KN, KX)$ và $(NX, NK) = (AX, AK)$. Nếu tam giác NKX cân tại X thì $(KN, KX) = (NX, NK)$, do đó ta phải chứng minh $(AN, AX) = (AX, AK)$ hay AN và AK là hai đường đẳng giác của $\triangle ABC$.
Chú ý tứ giác $ANXK$ nội tiếp nên, mà $(AN, AX) = (AX, AK)$ nên $XN = XK$. Hoàn toàn tương tự, $XM = XL$. Vị tự tâm I tỉ số 2 biến D, P, Q thành X, L, K nên $XL = XK$. Vậy K, L M, N thuộc đường tròn tâm X. □

Bài toán 9. *Cho $\triangle ABC$ nội tiếp đường tròn (O) có các phân giác BE, CF cắt nhau tại I. EF cắt (O) tại M, N. Các đường thẳng MI, NI cắt (O) lần lượt tại P, Q. Gọi X, Y, Z lần lượt là tâm đường tròn bàng tiếp góc A, B, C của $\triangle ABC$. Tia IP, IQ theo thứ tự cắt đường thẳng BC tại L, K. Gọi S là điểm đối xứng của K qua XY, T là điểm đối xứng của L qua XZ. Chứng minh rằng các bộ ba điểm (Z, T, K), (A, T, B), (A, S, C), (Y, L, S) thẳng hàng.*

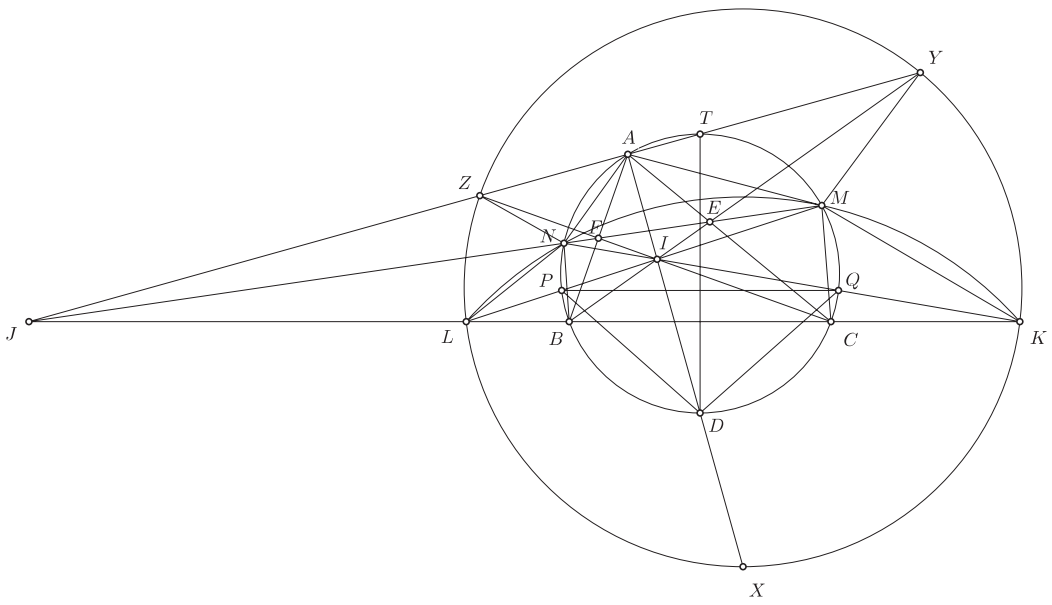


Chứng minh. Ta có $(ZB, ZT) = (ZL, ZB) = (ZB, ZK)$ nên Z, T, K thẳng hàng.
Ta có $(BZ, BT) = (BL, BZ) = (BC, BX) = (BZ, BA)$ nên A, T, B thẳng hàng.
Tương tự A, S, C và Y, S, L thẳng hàng. □

Bài toán sau là một tính chất thú vị về hai đường thẳng cắt nhau trên đường tròn:

Bài toán 10. *Cho $\triangle ABC$ nội tiếp đường tròn (O) có các phân giác BE, CF cắt nhau tại I. EF cắt (O) tại M, N. Các đường thẳng MI, NI cắt đường thẳng BC theo thứ tự tại L, K. LN, KM cắt (O) lần thứ hai tại T. Chứng minh rằng T là điểm chính giữa cung BAC.*

Lời giải sau được phát hiện khi tác giả cố suy nghĩ tìm một ứng dụng cho định lý Brokard:



Chứng minh. Gọi X, Y, Z lần lượt là tâm đường tròn bàng tiếp góc A, B, C của $\triangle ABC$. Gọi J là giao điểm của đường thẳng YZ và BC. Theo bài toán gốc có $YMINZ$ nội tiếp đường tròn ω và $YZBC$ nội tiếp. Theo bài toán 8 còn có $KLNM$ nội tiếp nên trục đẳng phương của các cặp trong ba đường tròn (O), $(KLMN)$, $(YZMN)$ đồng quy nên MN đi qua J.
Ta dễ dàng chứng minh $JLNA$ và $JKMA$ nội tiếp nên A là điểm Miquel của bộ bốn đường thẳng (MN, LK, MK, LN). Mặt khác T là giao điểm của MK và LN nên A cũng thuộc (TMN) hay T thuộc $(AMN) \equiv (O)$. Áp dụng định lý Brokard cho tứ giác $MNLK$ nội tiếp (X) ta được $IA \equiv IX \perp JT$. Mà $IA \perp YZ \equiv \overline{JZY}$ nên T nằm trên đường thẳng YZ. Vậy bài toán đã được giải quyết. □

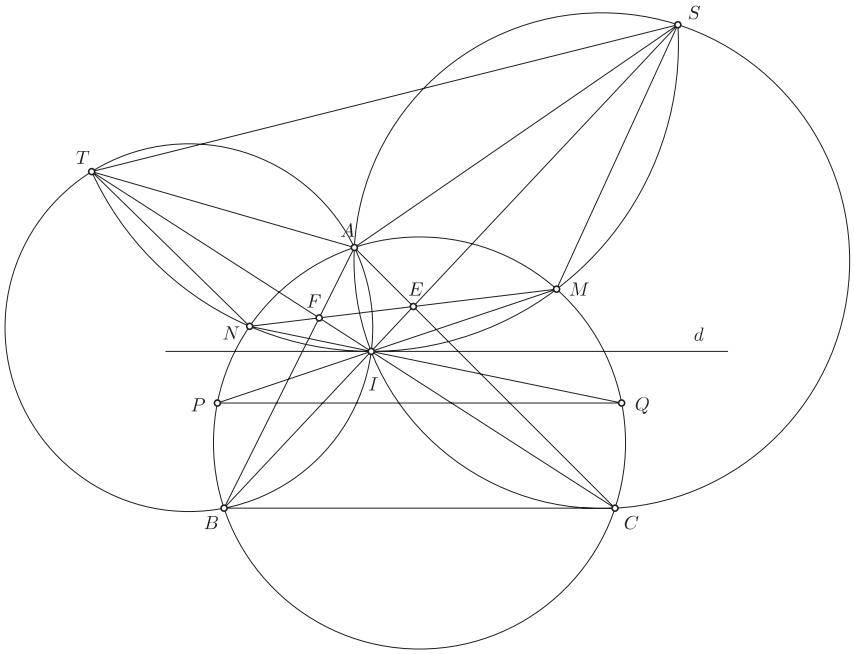
Từ bài toán gốc ban đầu ta đã thu được nhiều kết quả đẹp, phần tiếp theo tác giả sẽ mở rộng bài toán gốc ra tổng quát hơn.

3. Mở rộng bài toán

Bài toán gốc là một kết quả rất đẹp của hình học phẳng về vấn đề phân giác. **Lời giải 2** ta chỉ sử dụng tính chất của đường phân giác ở góc A của $\triangle ABC$. **Lời giải 3** lại liên quan đến vấn đề tiếp tuyến tại điểm A của (ABC) nên ở các bài toán tiếp theo ta sẽ có những mở rộng cho **Bài toán 1**.

Bài toán 11. *$\triangle ABC$ nội tiếp đường tròn (O), đường phân giác trong AD. I là một điểm di chuyển trên AD sao cho I, A cùng nằm trên một mặt phẳng bờ BC. Gọi E, F là giao điểm của BI với AC, CI với AB. EF cắt (O) tại M, N. MI, NI theo thứ tự cắt (O) tại P, Q. Chứng minh rằng PQ song song BC.*

Trường hợp này ta thấy khi vẽ đường phân giác ngoài của góc A cắt BI, CI thì cho hai điểm không còn đặc biệt nữa. Nhưng để ý thấy BI, CI cắt lần lượt các đường tròn (ACI) và (ABI) thì quan hệ giữa các góc sẽ rõ ràng hơn.



Chứng minh. Gọi S, T lần lượt là giao điểm của BI và (ACI), CI và (ABI), từ đây:

$$\overline{FI} \cdot \overline{FT} = \overline{FA} \cdot \overline{FB} = \overline{FN} \cdot \overline{FM}$$

Nên tứ giác $NIMT$ nội tiếp. Tương tự tứ giác $NIMS$ nội tiếp.
Ta có:

$$(TB, TC) = (TB, TI) = (AB, AI) = (AI, AC) = (SI, SC) = (SB, SC)$$

Do đó tứ giác $TBCS$ nội tiếp.
Gọi d là tiếp tuyến tại I của đường tròn đi qua các điểm N, I, M, S, T, ta có:

$$(BC, BI) = (TI, TS) = (Id, IS)$$

Suy ra d song song BC. Mặt khác:

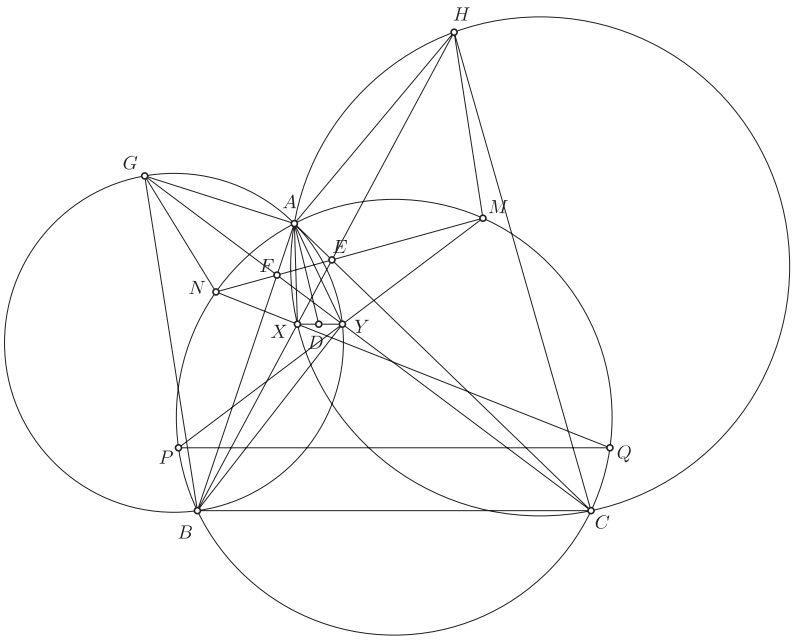
$$(PI, PQ) = (NM, NI) = (IM, Id)$$

Suy ra d song song PQ. Do đó ta kết luận PQ song song BC.
Vậy bài toán đã được giải xong. □

Nhận xét. Lời giải trên vẫn sử dụng kỹ thuật biến đổi góc cùng với phương tích. Tuy nhiên rõ ràng trong bài toán mở rộng nó đã được dùng khéo léo để vận dụng hết các dữ kiện mở của bài toán.

Bài toán tiếp theo là một mở rộng của bài toán trên khi khai thác dữ kiện hai đường tròn ngoại tiếp $\triangle ABI$ và $\triangle ACI$:

Bài toán 12. *Cho $\triangle ABC$, điểm D nằm trên phân giác trong d của góc A. Trong $\triangle ABC$, gọi d_1, d_2 là hai đường thẳng đi qua A đối xứng nhau qua d sao cho d_1 nằm trên mặt phẳng chứa B bờ d. Qua D kẻ đường thẳng song song với BC cắt d_1, d_2 lần lượt tại X, Y. BX cắt AC tại E, CY cắt AB tại F. Đường thẳng EF cắt (ABC) tại M, N. Tia MY, NX cắt (ABC) lần thứ hai tại P, Q. Chứng minh PQ song song BC.*



Chứng minh. Kéo dài BE cắt (AXC) tại H, CF cắt (ABY) tại G. Khi đó do:

$$(GB, GC) = (AB, AY) = (AX, AC) = (HB, HC)$$

Nên tứ giác $GHCB$ nội tiếp. Từ đây suy ra $GHYX$ nội tiếp. Mặt khác do:

$$\overline{FG} \cdot \overline{FY} = \overline{FA} \cdot \overline{FB} = \overline{FN} \cdot \overline{FM}$$

Nên $GNYM$ nội tiếp, tương tự $HMXN$ nội tiếp. Do đó sáu điểm G, N, X, Y, M, H cùng thuộc một đường tròn. Từ điều này ta có:

$$(XY, XQ) = (MP, MN) = (QP, QX)$$

Như thế XY song song PQ. Mà XY song song BC nên PQ song song BC.
Vậy bài toán đã được giải xong. □

Ngoài ra, **Bài toán 12** còn một khai thác về đường thẳng song song với BC nữa ở bài toán sau:

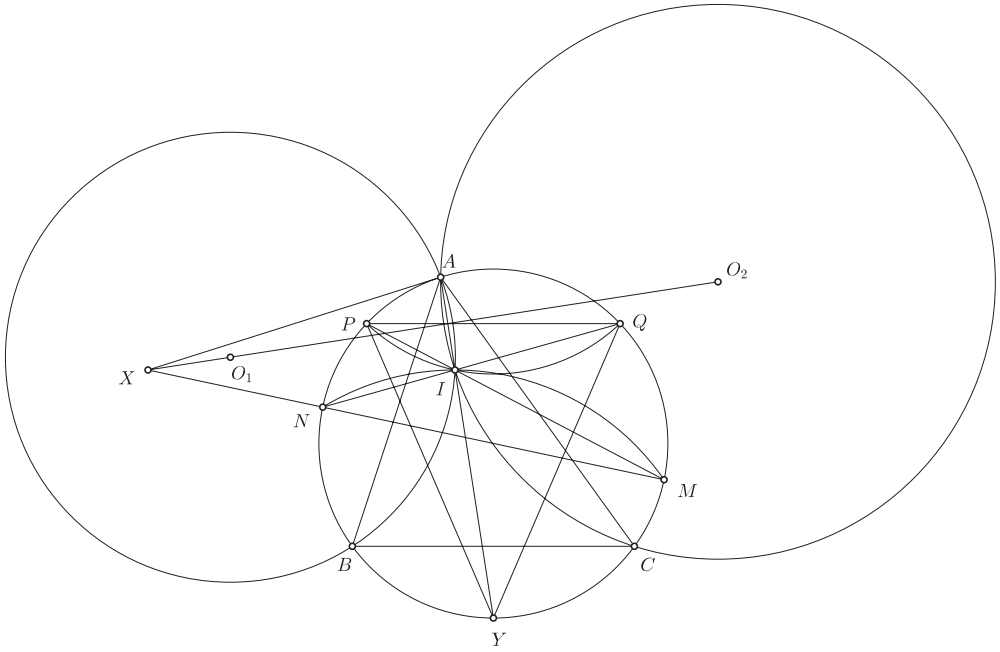
Bài toán 13. *Cho $\triangle ABC$, điểm D nằm trên phân giác trong d của góc A. Trong $\triangle ABC$, gọi d_1, d_2 là hai đường thẳng đi qua A đối xứng nhau qua d sao cho d_1 nằm trên mặt phẳng chứa B bờ d. Qua D kẻ đường thẳng song song với BC cắt d_1, d_2 lần lượt tại X, Y. BX cắt AC tại E, CY cắt AB tại F. Đường thẳng EF cắt (ABC) tại M, N. Tia MD, ND cắt (ABC) lần thứ hai tại P, Q. Chứng minh PQ song song BC.*

Trong **Bài toán 11**, ta lần lượt có B, I, E và C, I, F thẳng hàng và ta để ý thấy đường nối tâm của (ABI) và (ACI), đường thẳng EF, tiếp tuyến tại A của (ABC) đồng quy. Vậy trong trường hợp B, I, E và C, I, F không còn thẳng hàng nhưng vẫn giữ nguyên tính chất ba đường thẳng ấy đồng quy thì như thế nào? Ta có bài toán thú vị như sau:

Bài toán 14. *Cho $\triangle ABC$ nội tiếp đường tròn (O), đường phân giác trong AD. I là một điểm di chuyển trên đướng thẳng AD. Gọi O_1, O_2 lần lượt là tâm của (ABI) và (ACI). Tiếp tuyến tại A của (O) cắt đường thẳng O_1O_2 tại X. Một đường thẳng qua X cắt (O) tại M, N. Các tia MI, NI theo thứ tự cắt (O) tại P, Q. Chứng minh PQ song song BC.*

Ở bài toán này ta thấy rõ ràng không thể sử dụng việc kéo dài BI, CI được nữa vì M, N di chuyển tùy ý nên khó định hướng được việc xài phương tích, nhưng với bổ đề đã được nêu ở **Lời giải 3** của bài toán gốc thì bài toán trở nên rõ ràng hơn.

Chứng minh. Không mất tính tổng quát, giả sử N nằm giữa X và M. Ta có X nằm trên đường trung trực của AI nên $XA = XI$. Áp dụng **Bổ đề** của **Bài toán 1** cho tam giác AMN với AI, MI, NI cắt (ABC) lần lượt tại Y, P, Q và chú ý $BY = CY$.



được $PY = QY$ suy ra $PB = QC$. Từ đây dễ dàng suy ra PQ song song BC.
Vậy bài toán đã được giải xong. □

Cuối cùng, tác giả xin đưa ra một số bài tập để bạn đọc rèn luyện thêm về các tính chất thú vị này:

Bài toán 15. *Cho $\triangle ABC$ nội tiếp đường tròn (O). I là một điểm di chuyển trên phân giác trong ℓ của góc A sao cho I, A cùng nằm trên một mặt phẳng bờ BC. Gọi E, F là giao điểm của BI với AC, CI với AB. EF cắt (O) tại M, N. MI, NI theo thứ tự cắt (O) tại P, Q, cắt đường thẳng BC tại L, K.*
a) Gọi Y, Z lần lượt là giao điểm của BI và (ACI), CI và (ABI). Chứng minh rằng bốn điểm L, K, Y, Z cùng nằm trên đường tròn tâm X.
b) Gọi D là giao điểm của ℓ và (O). Chứng minh rằng khi P, Q lần lượt chia IL, IK theo cùng tỉ số k thì D cũng chia IX theo tỉ số k.

Từ **Bài toán 15** ta có một khai thác như sau:

Bài toán 16. *Cho $\triangle ABC$, đường phân giác trong AD của góc A (D thuộc BC). I là một điểm di chuyển trên cạnh AD với I khác A và D. BI cắt AC tại E, CI cắt AB tại F. Đường thẳng EF cắt (ABC) tại M, N. MI, NI cắt đường thẳng BC lần lượt tại L, K. Chứng minh rằng các đường thẳng MK, NL giao nhau tại một điểm cố định khi I thay đổi.*

Bài toán 17. *Cho $\triangle ABC$, đường phân giác trong BE, CF. EF cắt (O) tại M, N. Chứng minh rằng M, N là tiếp điểm của hai tiếp tuyến chung của (ABC) và đường tròn bàng tiếp góc A của $\triangle ABC$.*

Bài toán 18. *Cho $\triangle ABC$, hai tiếp tuyến chung ngoài ℓ_1, ℓ_2 của (ABC) và đường tròn bàng tiếp góc A. Đường thẳng BC cắt ℓ_1, ℓ_2 lần lượt tại D, E. Chứng minh rằng AD, AE là hai đường đẳng giác của $\triangle ABC$.*

Bài toán 17 và **Bài toán 18** có thể tham khảo ở [3].

Tài liệu

[1] Two parallels
http://www.artofproblemsolving.com/community/c6h550786

[2] Two parallels generalization problem.
http://www.artofproblemsolving.com/community/c6h1147664p5418246

[3] Common tangents problem.
http://www.artofproblemsolving.com/community/c6h385175p3753324

[4] Bisects segment problem.
https://www.facebook.com/groups/Loicenter/permalink/982284725178035

CÁC ĐƯỜNG TRÒN CÓ HAI ĐIỂM CHUNG TRONG TỨ GIÁC NỘI TIẾP

Trần Minh Ngọc, TP.HCM

1. Giới thiệu

Trong quá trình dạy đội tuyển trường THPT chuyên Hạ Long, tôi đã phát hiện bài toán sau:

Bài toán 1. *Cho tứ giác $ABCD$ nội tiếp (O). Một đường thẳng d lần lượt cắt AC, BD, AB, CD, AD, BC tại M, N, P, Q, R, S. Chứng minh rằng với mọi điểm X nằm trên (O) thì (XMN), (XPQ), (XRS), (O) có một điểm chung khác X.*

Trong bài viết này, tôi sẽ giới thiệu ba lời giải bài toán và một số tính chất khác trong cấu hình của nó. Trong phần cuối cùng, tôi sẽ giới thiệu về ứng dụng của những tính chất vừa tìm được trong việc giải những bài toán khác.

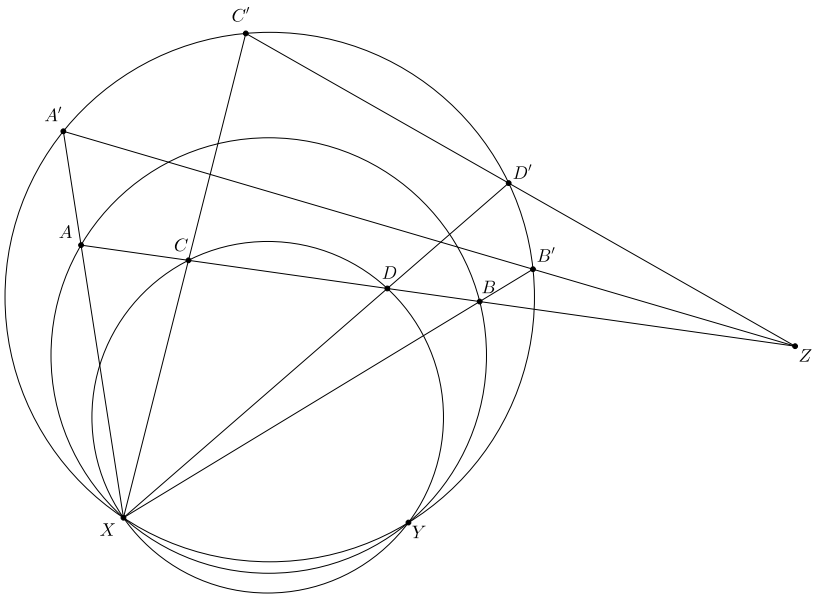
2. Lời giải

2.1. Lời giải 1

Ta phát biểu và chứng minh bổ đề sau:

Bổ đề 1. *Cho đường tròn (O) và đường thẳng d. Trên (O) lấy X, trên d lấy A, B, C, D rồi lần lượt cho XA, XB, XC, XD cắt (O) tại điểm thứ hai là A', B', C', D'. Khi đó $A'B'$, $C'D'$, d đồng quy khi và chỉ khi (XAB), (XCD), (O) có một điểm chung khác X.*

Biên tập: Ngô Quang Dương



Hình 1. Bổ đề 1

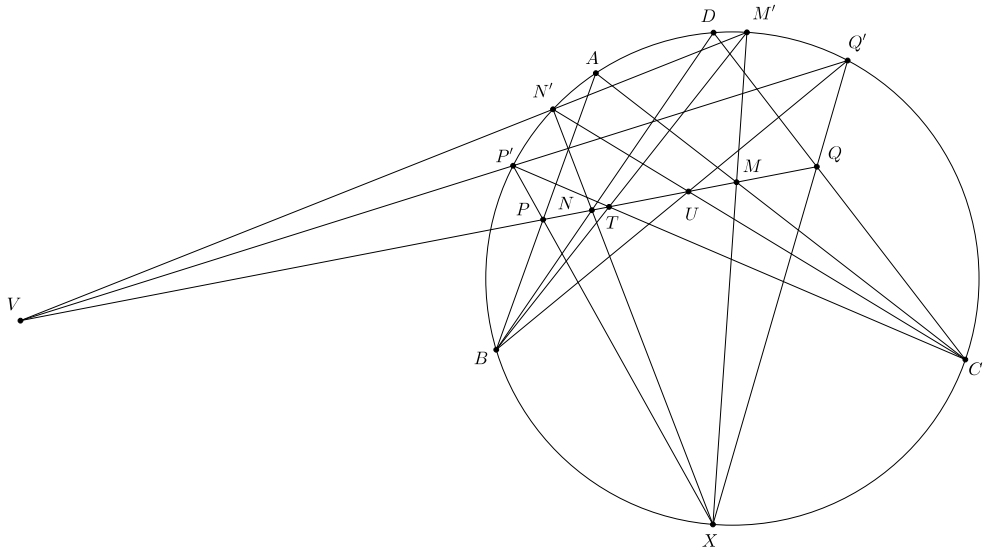
Chứng minh. Chứng minh hai chiều.

- Chiều thuận. Giả sử $A'B'$, $C'D'$, d đồng quy tại Z. Áp dụng định lý Miquel cho tứ giác toàn phần tạo bởi bốn đường thẳng AA', BB', AB, $A'B'$, ta được (XAB), $(XA'B') \equiv (O)$, (ZAA'), (ZBB') đồng quy tại một điểm Y. Do $\angle DZY = \angle BZY = \angle BB'Y = \angle DD'Y$ nên tứ giác $DD'ZY$ nội tiếp. Suy ra $\angle YDZ = \angle YD'Z = \angle CXY$. Do đó theo định lý Miquel, tứ giác $CDYX$ nội tiếp.
  Vậy (XAB), (XCD), (O) có chung điểm $Y \neq X$.

- Chiều nghịch. Giả sử (XAB), (XCD), (O) có chung điểm $Y \neq X$. Gọi Z là giao điểm của $A'B'$, d.
  D_1 là giao điểm thứ hai của ZC', (O).
  D_2 là giao điểm của XD_1, d.
  Theo chiều thuận, (XAB), (XCD), (O) đồng quy. Suy ra $D_2 \equiv D$, $D_1 \equiv D'$.
  Vậy $A'B'$, $C'D'$, d đồng quy tại Z.

□

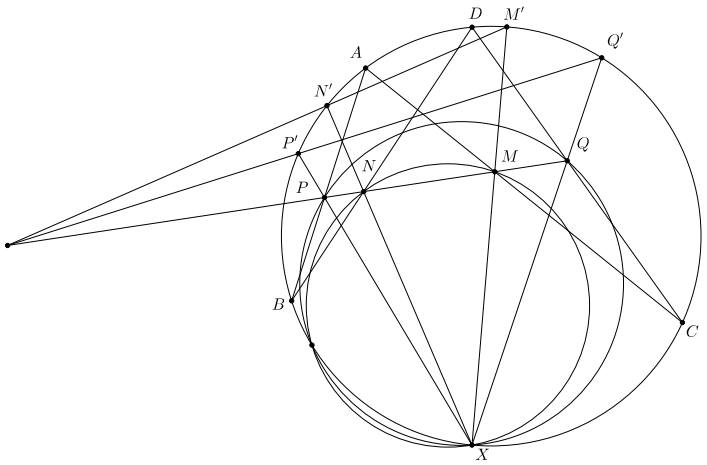
Bổ đề 2. *Cho tứ giác $ABCD$ nội tiếp đường tròn (O). Một đường thẳng d lần lượt cắt AC, BD, AB, CD, AD, BC tại M, N, P, Q, R, S. Trên (O) lấy X rồi lần lượt cho XM, XN, XP, XQ, XR, XS cắt (O) tại M', N', P', Q', R', S'. Khi đó $M'N'$, $P'Q'$, $R'S'$, d đồng quy.*



Hình 2. Bổ đề 2

Chứng minh. Áp dụng định lý Pascal cho lục giác $CABM'XP'$, ta được $CA \cap M'X = M$, $AB \cap XP' = P$, $BM' \cap CP' = T$ thẳng hàng, hay $T \in d$. Chứng minh tương tự $BQ' \cap CN' = U \in d$.
Áp dụng định lý Pascal cho lục giác $M'N'C'P'Q'B'$, ta được $M'N' \cap P'Q' = V$, $N'C \cap Q'B = U$, $CP' \cap BM' = T$ thẳng hàng, hay $V \in d$, hay $M'N'$, $P'Q'$, d đồng quy. Chứng minh tương tự $M'N'$, $R'S'$, d đồng quy.
Vậy $M'N'$, $P'Q'$, $R'S'$, d đồng quy. □

Trở lại bài toán.



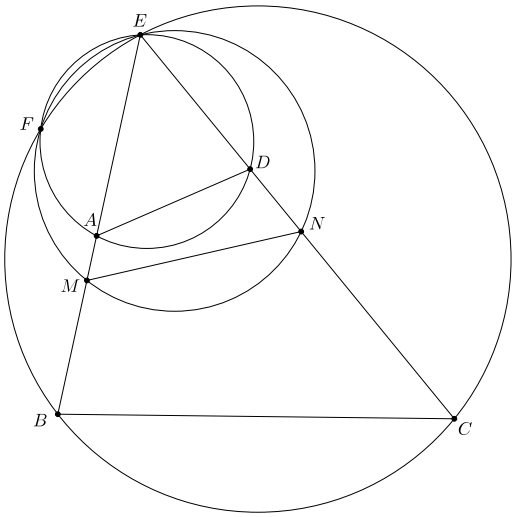
Hình 3

Với M', N', P', Q', R', S' định nghĩa như trong bổ đề 2.
Theo bổ đề 2: $M'N'$, $P'Q'$, $R'S'$, d đồng quy.
Theo bổ đề 1: (XMN), (XPQ), (XRS), (O) có một điểm chung khác X.

2.2. Lời giải 2

Ta phát biểu và chứng minh bổ đề sau:

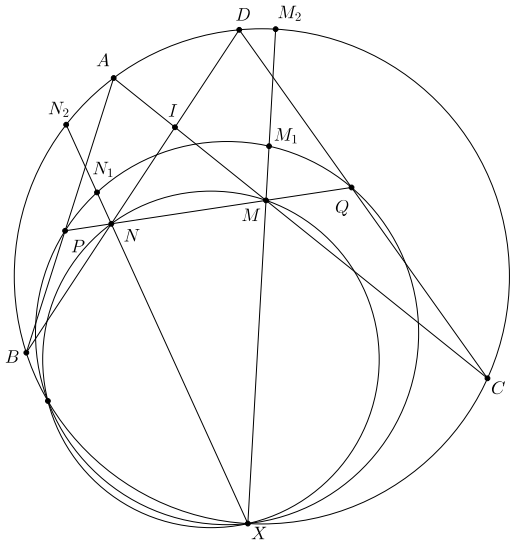
Bổ đề 3. *Cho tứ giác $ABCD$. Trên AB, CD lần lượt lấy M, N sao cho $\dfrac{\overline{AM}}{\overline{AB}} = \dfrac{\overline{DN}}{\overline{DC}}$. Gọi E là giao điểm của AB, CD. Khi đó (EAD), (EBC), (EMN) có một điểm chung khác E.*



Hình 4. Bổ đề 3

Chứng minh. Gọi F là giao điểm thứ hai của (EAD) và (EBC).
Do $\angle FAB = 180^o - \angle FAE = 180^o - \angle FDE = \angle FDC$, $\angle FBA = \angle FCD$ nên $\triangle FAB \sim \triangle FDC$. Suy ra $\dfrac{FA}{FD} = \dfrac{AB}{DC} = \dfrac{AM}{DN}$. Do đó $\triangle FAM \sim \triangle FDN$. Suy ra $\angle EMF = \angle ENF$ nên $ENMF$ nội tiếp. Vậy (EAD), (EBC), (EMN) có điểm chung khác E. □

Trở lại bài toán.



Hình 5

XM, XN lần lượt cắt (XPQ), (O) tại điểm thứ hai là M_1, M_2, N_1, N_2.
Áp dụng định lý Menelaus cho $\triangle IMN$ với A, P, B thẳng hàng, ta được $\dfrac{AI}{AM} \cdot \dfrac{PM}{PX} \cdot \dfrac{BN}{BI} = 1$.
Tương tự $\dfrac{DI}{DN} \cdot \dfrac{QN}{QM} \cdot \dfrac{CM}{CI} = 1$. Do đó

$$\frac{AI}{AM} \cdot \frac{PM}{PX} \cdot \frac{BN}{BI} = \frac{DI}{DN} \cdot \frac{QN}{QM} \cdot \frac{CM}{CI}$$

Đẳng thức này tương đương :

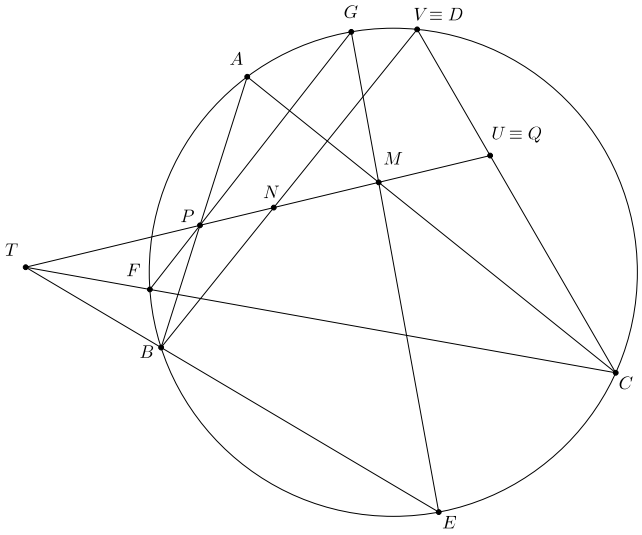
$$\frac{PM \cdot QM}{AM \cdot CM} \cdot \frac{CI}{BI} = \frac{PN \cdot QN}{DN \cdot BN} \cdot \frac{DI}{AI}$$

Mà $\dfrac{CI}{BI} = \dfrac{DI}{AI}$ (do $\triangle CBI \sim \triangle DAI$). Nên $\dfrac{PM \cdot QM}{AM \cdot CM} = \dfrac{PN \cdot QN}{DN \cdot BN}$. Suy ra $\dfrac{MM_1}{MM_2} = \dfrac{MM_1 \cdot MX}{MM_2 \cdot MX} = \dfrac{NN_1 \cdot NX}{NN_2 \cdot NX} = \dfrac{NN_1}{NN_2}$. Theo hình vẽ, ta được $\dfrac{\overline{MM_1}}{\overline{MM_2}} = \dfrac{\overline{NN_1}}{\overline{NN_2}}$. Theo bổ đề 2.3, ta được (XMN), $(XM_1N_1) \equiv (XPQ)$, $(XM_2N_2) \equiv (O)$ có điểm chung khác X. Chứng minh tượng tự (XMN), (XRS), (O) có điểm chung khác X.
Vậy (XMN), (XMN), (XRS), (O) có điểm chung khác X.

2.3. Lời giải 3

Ta phát biểu và chứng minh bổ đề sau:

Bổ đề 4. *Cho tứ giác $ABCD$ nội tiếp đường tròn (O). Một đường thẳng lần lượt cắt AC, BD, AB, CD tại M, N, P, Q. Khi đó tồn tại duy nhất điểm T sao cho $\overline{TM}.\overline{TN} = \overline{TP}.\overline{TQ} = \mathcal{P}_{T/(O)}$.*



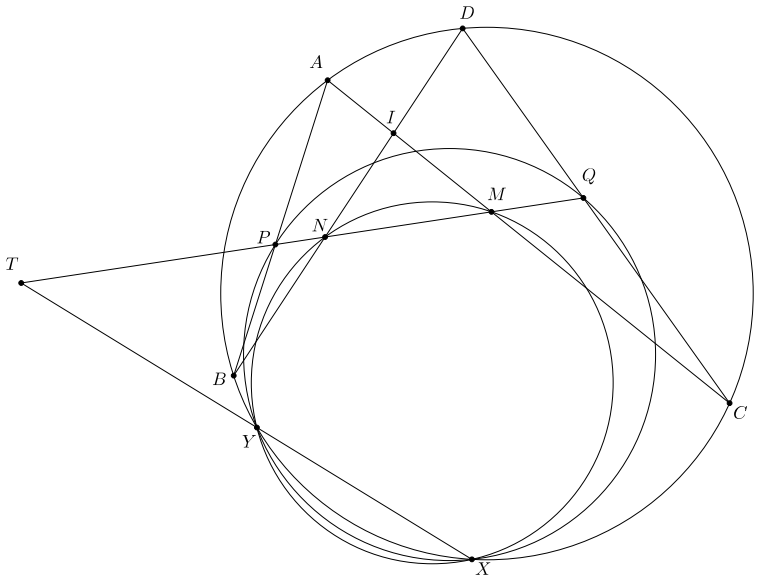
Hình 6. Bổ đề 4

Chứng minh. Gọi T là điểm mà $\overline{TM}.\overline{TN} = \mathcal{P}_{T/(O)}$, U là điểm mà $\overline{TP}.\overline{TU} = \mathcal{P}_{T/(O)}$. Khi đó T, U là duy nhất.
V là giao điểm của BN, CU. E, F lần lượt là giao điểm thứ hai của TB, TC với (O).
Do $\overline{TM}.\overline{TN} = \overline{TP}.\overline{TU} = \mathcal{P}_{T/(O)} = \overline{TB}.\overline{TE} = \overline{TC}.\overline{TF}$ nên các tứ giác $BEMN$, $CFPU$ nội tiếp. Hơn nữa, nếu gọi G là giao điểm của EM, FP và áp dụng định lý Pascal đảo cho lục giác $BACFGE$ với $BA \cap FG = P$, $AC \cap GE = M$, $CF \cap EB = T$ thẳng hàng và $A, B, C, E, F \in (O)$, ta được $G \in (O)$. Từ đó, ta có biến đổi góc sau:

$$\begin{aligned}\angle BVC &= 180^o - (\angle VNU + \angle VUN) = 180^o - (\angle GEB + \angle GFC)\\ &= \frac{360^o - \overset{\frown}{GB} - \overset{\frown}{GC}}{2} = \frac{\overset{\frown}{BC}}{2}\end{aligned}$$

Suy ra $V \in (O)$. Do đó $V \equiv D$, $U \equiv Q$. Vậy tồn tại duy nhất điểm T sao cho $\overline{TM}.\overline{TN} = \overline{TP}.\overline{TQ} = \mathcal{P}_{T/(O)}$. □

Trở lại bài toán.



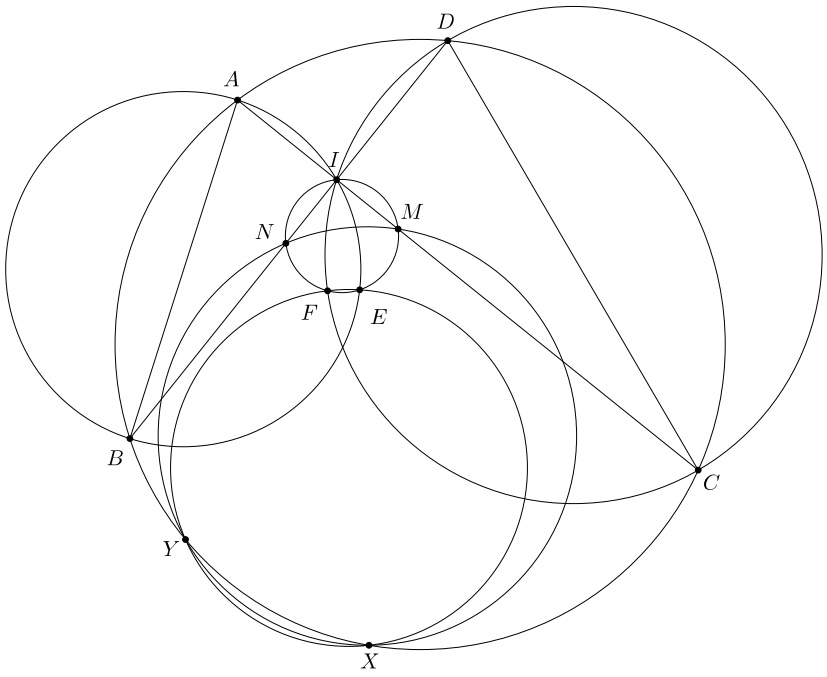
Hình 7

Gọi Y là giao điểm thứ hai của TX và (O). Theo bổ đề 2.4, tồn tại duy nhất điểm T sao cho $\overline{TM}.\overline{TN} = \overline{TP}.\overline{TQ} = \mathcal{P}_{T/(O)} = \overline{TX}.\overline{TY}$. Suy ra các tứ giác $MNYX$, $PQXY$ nội tiếp. Do đó (XMN), (XPQ), (O) đồng trục. Chứng minh tương tự (XMN), (XRS), (O) có điểm chung khác X.
Vậy (XMN), (XPQ), (XRS), (O) có điểm chung khác X.

3. Các tính chất khác

Gọi Y là điểm chung khác X của (XMN), (XPQ), (XRS), (O).

Tính chất 1. *Gọi I là giao điểm của AC, BD. (IMN) lần lượt cắt (IAB), (ICD), (IAD), (IBC) tại E, F, G, H . Khi đó (XEF), (XGH) qua Y.*

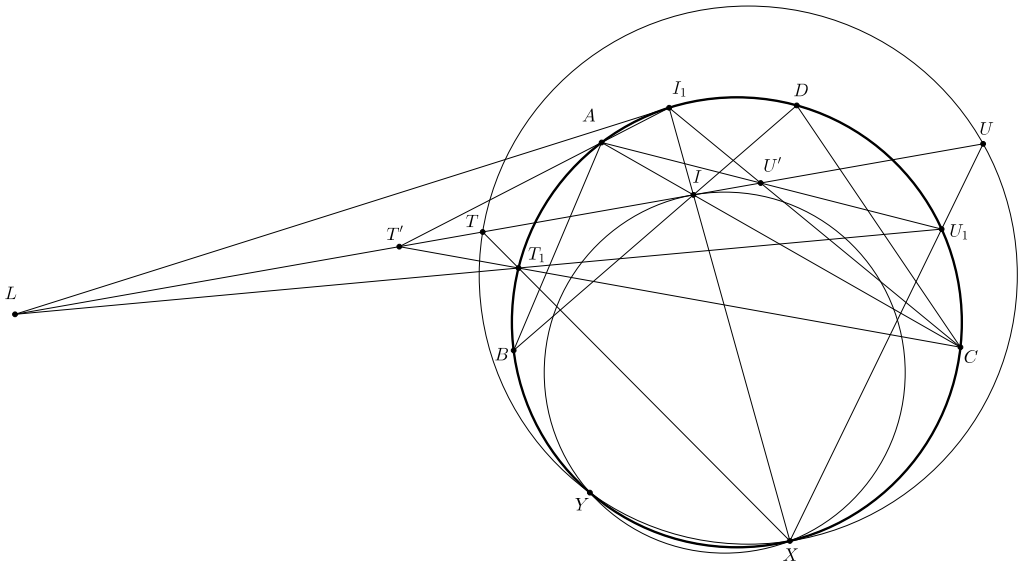


Hình 8. Tính chất 1

Chứng minh. Phép nghịch đảo cực I , phương tích $k \neq 0$ biến A, B, C, D, M, N, E, F, X thành A', B', C', D', M', N', E', F', X' . Khi đó AC, BD, (IAB), (ICD), (IMN) biến thành $A'C'$, $B'D'$, $A'B'$, $C'D'$, $M'N'$. Suy ra $M'N'$ lần lượt cắt $A'C'$, $B'D'$, $A'B'$, $C'D'$ tại M', N', E', F' . Mà A', B', C', D', X' đồng viên. Nên theo bài toán 1, $(A'B'C'D')$, $(X'M'N')$, $(X'E'F')$ có điểm chung khác X'. Do đó (O), (XMN), (XEF) có điểm chung khác X , hay (XEF) qua Y . Chứng minh tương tự (XGH) qua Y. □

Chú ý 1. *Ta có kết quả tương tự với J, K lần lượt là giao điểm của AB và CD, AD và BC. Khi d qua một trong ba điểm I, J, K , kết quả chỉ còn đúng với hai điểm còn lại.*

Tính chất 2. *Giả sử d qua I và lần lượt cắt tiếp tuyến tại A, C, B, D của (O) tại T, U, V, W. Khi đó đường tròn qua X và tiếp xúc d tại I, (XTU), (XVW) qua Y.*



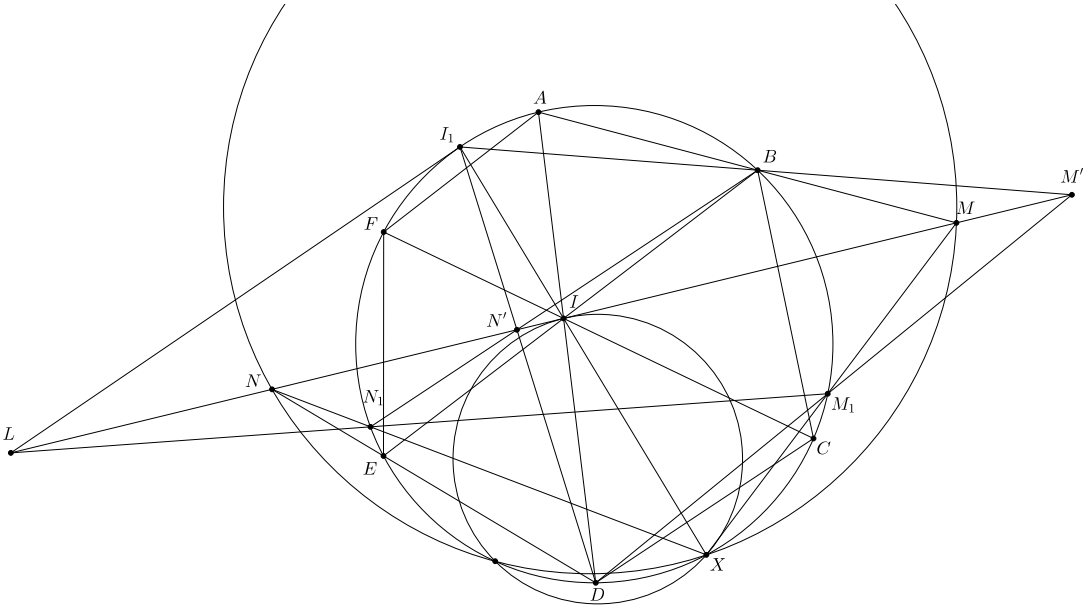
Hình 9. Tính chất 2

Chứng minh. Đường tròn qua X và tiếp xúc d tại I qua Y chỉ là trường hợp đặc biệt của (XMN) qua Y. Thật vậy, khi d qua I thì $M \equiv N \equiv I$, (XMN) suy biến thành đường tròn qua X và tiếp xúc d tại I . Ta chỉ chứng minh (XTU), (XVW) qua Y.
Kí hiệu ZZ là tiếp tuyến tại Z của (O)
Gọi I_1, T_1, U_1 lần lượt là giao điểm thứ hai của XI, XT, XU với (O).
Áp dụng định lý Pascal cho lục giác U_1XI_1CCA nội tiếp (O), ta được $U_1X \cap CC = U$, $XI_1 \cap CA = I$, $I_1C \cap U_1A = U'$ thẳng hàng, hay $U' \in d$. Chứng minh tương tự $I_1A \cap T_1C = T' \in d$.
Áp dụng định lý Pascal cho lục giác $U_1AI_1I_1CT_1$ nội tiếp (O), ta được $U_1A \cap I_1C = U'$, $AI_1 \cap CT_1 = T'$, $I_1I_1 \cap U_1T_1 = L$ thẳng hàng, hay $L \in U'T' = d$. Do đó I_1I_1, U_1T_1, d đồng quy tại L. Từ đó, áp dụng bổ đề 1 cho $X \in (O)$ và $T,\ U,\ I,\ I \in d$, ta được đường tròn qua X và tiếp xúc d tại I, (XTU), (O) có điểm chung khác X, hay (XTU) qua Y. Chứng minh tương tự (XVW) qua Y. □

Chú ý 2. *Ta có kết quả tương tự với J, K.*

Tính chất 2 được mở rộng cho lục giác như sau.

Tính chất 3. *Cho lục giác $ABCDEF$ nội tiếp (O) có AD, BE, CF đồng quy tại I. Một đường thẳng d qua I, lần lượt cắt AB, DE, BC, EF, CD, FA tại M, N, P, Q, R, S. Khi đó với mọi điểm X nằm trên (O), đường tròn qua X tiếp xúc với d tại I, (XMN), (XPQ), (XRS), (O) có một điểm chung khác X.*



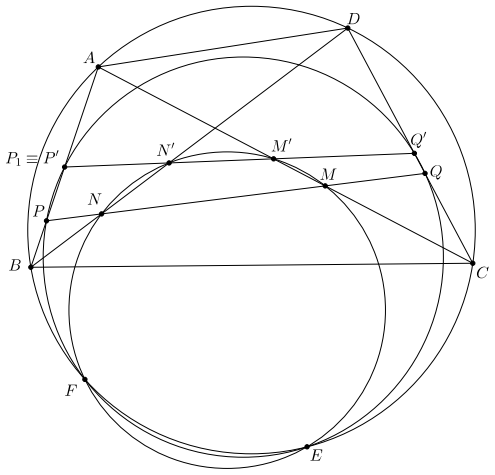
Hình 10. Tính chất 3

Chứng minh. Áp dụng định lý Pascal cho lục giác M_1XI_1BAD, ta được $M_1X \cap AB = M$, $XI_1 \cap AD = I$, $I_1B \cap DM_1 = M'$ thẳng hàng, hay $M' \in d$. Chứng minh tương tự, ta được $I_1D \cap BN_1 = N' \in d$.
Áp dụng định lý Pascal cho lục giác $BI_1I_1DM_1N_1$, ta được $BI_1 \cap DM_1 = M'$, $I_1I_1 \cap M_1N_1 = L$, $I_1D \cap N_1B = N'$, hay $L \in M'N' = d$. Do đó M_1N_1, I_1I_1, d đồng quy tại L. Từ đó, áp dụng bổ đề 1 cho $X \in (O)$ và $M,\ N,\ I,\ I \in d$, ta được đường tròn qua X và tiếp xúc d tại I, (XMN), (O) có điểm chung khác X. Chứng minh tương tự đường tròn qua X và tiếp xúc d tại I, (XPQ), (XRS), (O) có điểm chung khác X. Ta đi đến kết luận bài toán! □

Chú ý 3. *Tính chất 2 có thể được mở rộng cho $2n-$giác nội tiếp đường tròn có các đường chéo đồng quy theo cách tương tự.*

4. Ứng dụng

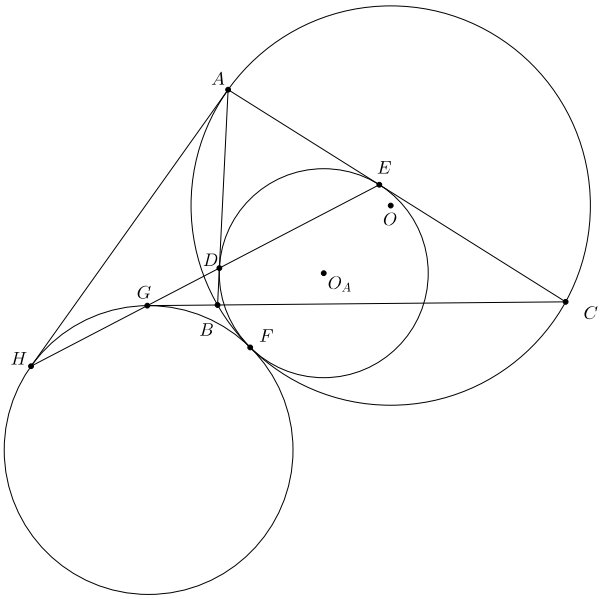
Bài toán 2. *Cho ngũ giác $ABCDE$ nội tiếp (O). Một đường thẳng d cắt AC, BD, AB, CD tại M, N, P, Q. (EMN) lần lượt cắt AC, BD tại điểm thứ hai là M', N'. (EPQ) lần lượt cắt AB, CD tại điểm thứ hai là P', Q'. Chứng minh rằng M', N', P', Q' thẳng hàng.*



Hình 11. Bài toán 2

Chứng minh. Áp dụng bài toán 1 cho tứ giác $ABCD$ nội tiếp (O) và đường thẳng d lần lượt cắt AC, BD, AB, CD tại M, N, P, Q, ta được (EMN), (EPQ), (O) có điểm chung khác $F \neq E$.
Áp dụng bài toán 1 cho tứ giác $MNN'M'$ nội tiếp và đường thẳng AB lần lượt cắt MM', NN', MN, $M'N'$ tại A, B, P, P_1, ta được $(EAB) \equiv (O_1)$, (EPP_1), $(MNN'M')$ có điểm chung khác E. Suy ra $F \in (EPP_1)$. Do đó $P_1 \equiv P$ là giao điểm thứ hai của AB, (PEF), hay M', N', P' thẳng hàng. Chứng minh tương tự M', N', Q' thẳng hàng. Vậy M', N', P', Q' thẳng hàng. □

Bài toán 3. *Cho $\triangle ABC$ nội tiếp (O). Một đường tròn (O_A) lần lượt tiếp xúc với AB, AC tại D, E và tiếp xúc trong với (O) tại F. DE lần lượt cắt BC và tiếp tuyến tại A của (O) tại G, H. Chứng minh rằng (FGH) tiếp xúc với (O), BC và tiếp tuyến tại A của (O).*



Hình 12. Bài toán 3

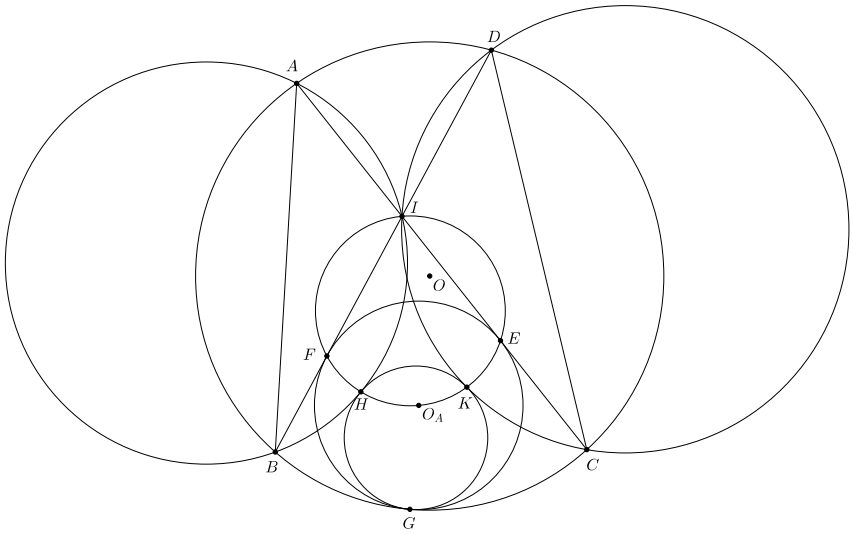
Chứng minh. Áp dụng bài toán 1 cho tứ giác $AABC$ nội tiếp (O) và đường thẳng DE lần lượt cắt AB, AC, BC, AA tại D, E, G, H , ta được với mọi điểm X nằm trên (O), (XDE), (XGH), (O) có điểm chung Y, X.
Khi (XDE) tiếp xúc với (O) tại F thì $X \equiv Y \equiv F$. Suy ra (FGH) tiếp xúc với (O) tại F.
Áp dụng bài toán 2 cho tứ giác $AABC$ nội tiếp (O) và đường thẳng d lần lượt cắt AB, AC, BC, AA tại D_1, E_1, G_1, H_1, ta được D_2, E_2, G_2, H_2 thẳng hàng, trong đó D_2, E_2, G_2, H_2 lần lượt là giao điểm thứ hai của (FD_1E_1) với AB, AC; (FG_1H_1) với BC, AA.
Khi (FD_1E_1) lần lượt tiếp xúc với AB, AC tại D, E thì $D_1 \equiv D_2 \equiv D$, $E_1 \equiv E_2 \equiv E_2 \equiv E$. Suy ra $G_1 \equiv G_2 \equiv G$, $H_1 \equiv H_2 \equiv H$. Do đó (FGH) lần lượt tiếp xúc với BC, AA tại G, H. □

Bài toán 4. *Cho tứ giác $ABCD$ nội tiếp (O). Một đường tròn (O_A) lần lượt tiếp xúc với AC, BD tại E, F và tiếp xúc trong với (O) tại G. Gọi I là giao điểm của AC, BD. (IEF) lần lượt cắt (IAB), (ICD) tại điểm thứ hai là H, K. Chứng minh rằng (GHK) tiếp xúc với (O), (IAB), (ICD).*

Chứng minh. Ta phát biểu và chứng minh bổ đề sau.

Bổ đề 5. *Cho ngũ giác $ABCDE$ nội tiếp (O). Gọi I là giao điểm của AC, BD. Trên AC, BD lần lượt lấy M, N rồi vẽ đường tròn (IMN) lần lượt cắt (IAB), (ICD) tại P, Q. (EMN) lần lượt cắt AC, BD tại điểm thứ hai là M', N'. (EPQ) lần lượt cắt (IAB), (ICD) tại điểm thứ hai là P', Q'. Khi đó M', N', P', Q' đồng viên.*

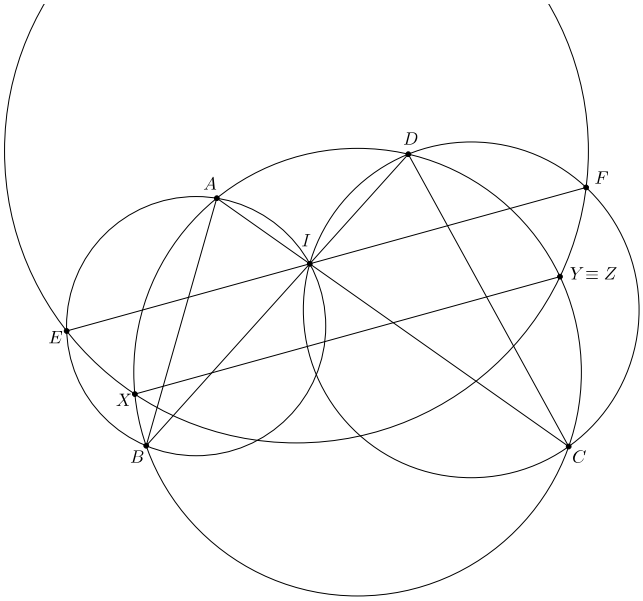
Chứng minh bổ đề: Qua phép nghịch đảo cực I, phương tích $k \neq 0$, ta nhận được cấu hình bài toán 2.



Hình 13. Bài toán 4

Trở lại bài toán.
Áp dụng tính chất 1 cho tứ giác $ABCD$ nội tiếp (O) và đường thẳng EF lần lượt cắt AC, BD tại E, F và (IEF) lần lượt cắt (IAB), (ICD) tại điểm thứ hai là H, K, ta được với mọi điểm X nằm trên (O), (XEF), (XHK), (O) có điểm chung $Y \neq X$.
Khi (XMN) tiếp xúc với (O) tại G thì $X \equiv Y \equiv G$. Suy ra (GHK) tiếp xúc với (O) tại G.
Áp dụng bổ đề cho tứ giác $ABCD$ nội tiếp (O) và đường thẳng E_1F_1 lần lượt cắt AC, BD tại E_1, F_1 và (IE_1F_1) lần lượt cắt (IAB), (ICD) tại điểm thứ hai là H_1, K_1, ta được E_2, F_2, H_2, K_2 đồng viên, trong đó E_2, F_2, H_2, K_2 lần lượt là giao điểm thứ hai của (GE_1F_1) với AC, BD; (GH_1K_1) với AB, CD.
Khi (GE_1F_1) lần lượt tiếp xúc với AC, BD tại E, F thì $E_1 \equiv E_2 \equiv E$, $F_1 \equiv F_2 \equiv F$. Suy ra $H_1 \equiv H_2 \equiv H$, $K_1 \equiv K_2 \equiv K$. Do đó (GHK) lần lượt tiếp xúc với (IAB), (ICD) tại H, K. □

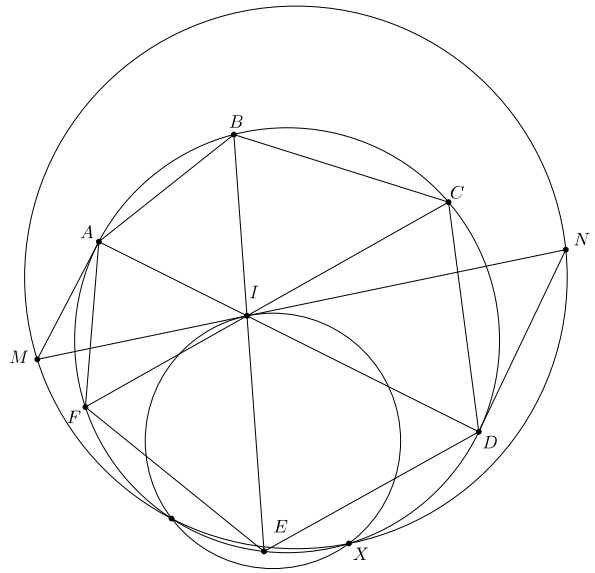
Bài toán 5. *Cho tứ giác $ABCD$ nội tiếp (O). Gọi I là giao điểm của AC, BD. Một đường thẳng d qua I lần lượt cắt (IAB), (ICD) tại E, F. Chứng minh rằng dây cung XY của (O) song song với d khi và chỉ khi tứ giác $XYFE$ nội tiếp.*



Hình 14. Bài toán 5

Chứng minh. Phép nghịch đảo cực I, phương tích $k \neq 0$, biến A, B, C, D, E, F, X, Y thành A', B', C', D', E', F', X', Y'. Khi đó AC, BD, (IAB), (ICD), d, XY lần lượt biến thành $A'C'$, $B'D'$, $A'B'$, $C'D'$, d, $(IX'Y')$ và A', B', C', D', X', Y' đồng viên.
Chiều thuận. Giả sử dây cung XY của (O) song song với d. Suy ra $(IX'Y')$ tiếp xúc với d tại I.
Áp dụng tính chất 2 cho tứ giác $A'B'C'D'$ nội tiếp và đường thẳng d qua I, lần lượt cắt $A'B'$, $C'D'$ tại E', F', ta được đường tròn qua X' và tiếp xúc với d tại I, $(X'E'F')$, $(A'B'C'D')$ có điểm chung khác X'. Suy ra $Y' \in (X'E'F')$. Do đó $XYFE$ nội tiếp.
Chiều nghịch. Giả sử $XYFE$ nội tiếp.
Vẽ dây cung $XZ \parallel d$. Theo chiều thuận, $XZFE$ nội tiếp. Suy ra $Z \equiv Y$, hay $XY \parallel d$. □

Bài toán 6. *Cho lục giác $ABCDEF$ nội tiếp (O) có AD, BE, CF đồng quy tại I. Một đường thẳng d qua I, lần lượt cắt tiếp tuyến tại A, D, B, E, C, F của (O) tại M, N, P, Q, R, S. Khi đó với mọi điểm X nằm trên (O) thì (XMN), (XPQ), (XRS), (O) có một điểm chung khác X.*



Hình 15. Bài toán 6

Chứng minh. Áp dụng tính chất 2 cho tứ giác $ACDF$ và đường thẳng d qua I cắt AA, DD tại M, N, ta được đường tròn qua X và tiếp xúc d tại I, (XMN), (O) có điểm chung khác X. Chứng minh tương tự đường tròn qua X và tiếp xúc d tại I, (XPQ), (XRS), (O) có điểm chung khác X. Ta đi đến kết luận bài toán ! □

Tổng quát của bài toán 1 đó là bổ đề Poncelet mở rộng (tham khảo [1]). Sử dụng bổ đề 4, ta có một lời giải cho nó. Ta cũng có thể tổng quát tính chất 1, 2, 3 và bài toán 1, 5 theo cách tương tự. Một khía cạnh khác, các bài toán 2, 3, 4 đều có lời giải ngắn gọn hơn, tác giả xin dành cho bạn đọc. Nhưng với cách tiếp cận thông qua bài toán 1 và một số tính chất khác trong cấu hình của nó, ta thấy được mối liên quan giữa các bài toán trên.

Tài liệu

[1] Trần Minh Ngọc, Bổ đề Poncelet mở rộng và ứng dụng, Geometry Blog
https://tranminhngocctlhp.wordpress.com/

[2] Nguyễn Văn Linh, Ứng dụng của tỉ số phương tích, Euclidean Geometry Blog
https://nguyenvanlinh.wordpress.com/

[3] Lachlan, "Coaxal Circles", Ch. 13 in An Elementary Treatise on Modern Pure Geometry. London: Macmillian, pp. 199-217, 1893

Email: tranminhngoc.ctlhp@gmail.com

Epsilon
Tạp chí online của cộng đồng những người yêu toán

ĐỊNH LÝ CAUCHY - DAVENPORT VÀ ỨNG DỤNG

Trần Minh Hiền
(Trường THPT chuyên Quang Trung, Bình Phước)

GIỚI THIỆU

Nội dung của chuyên đề này trình bày một số cách chứng minh định lý Cauchy - Davenport và nêu một số ứng dụng của nó. Để có được sự so sánh sự khác nhau giữa các kết quả trên $\mathbb{Z}$ và trên $\mathbb{Z}_p$ (tập các số dư theo modulo p, p nguyên tố), trong phần 1 trình bày một số kết quả khá quen thuộc của các tập tổng trên $\mathbb{Z}$. Bạn đọc quan tâm đến các kết quả sâu hơn về nội dung này có thể tham khảo tài liệu [3]. Về các kết quả hay trên $\mathbb{Z}_p$ bạn đọc có thể tham khảo các kết quả trong [1], [2]. Trong toàn bộ chuyên đề này, thống nhất ký hiệu

$$A + A = \{a + b \,|\, a \in A, b \in B\},\ c \cdot A = \{c \cdot a \,|\, a \in A\}.$$

Lời giải của một số bài tập có thể tương đối dài, nhưng trong đó chứa nhiều giải thích quan trọng để bạn đọc hiểu rõ hơn về ý tưởng.

1. Một số đánh giá tập tổng trên $\mathbb{Z}$

Định lý 1. *Cho A là một tập gồm k số nguyên. Khi đó $|2A| \geqslant 2k-1$. Nếu A là một tập gồm k số nguyên và nếu $|2A| = 2k-1$ thì A phải là một* ***cấp số cộng****.*

Lời giải. Đặt $A = \{a_0, a_1, \ldots, a_{k-1}\}$ với $a_0 < a_1 < a_2 < \cdots < a_{k-1}$. Khi đó tập $2A$ sẽ chứa k số nguyên $2a_i$, với $i = 0, 1, 2, \ldots, k-1$ và $k-1$ số nguyên $a_{i-1} + a_i$, với $i = 1, 2, \ldots, k-1$.

Do

$$2a_{i-1} < a_{i-1} + a_i < 2a_i, \quad \forall i = 1, 2, \ldots, 2k-1.$$

Từ đây suy ra $|2A| \geqslant 2k-1$.

Nếu $|2A| = 2k-1$, khi đó **mọi phần tử của** $2A$ **hoặc có dạng** $2a_i$ **hoặc** $a_{i-1} + a_i$. Do

$$a_{i-1} + a_i < a_{i-1} + a_{i+1} < a_i + a_{i+1}, \quad a_{i-1} + a_i < 2a_i < a_i + a_{i+1}, \quad \forall i = 1, 2, \ldots, k-1$$

nên suy ra

$$2a_i = a_{i-1} + a_{i+1} \Rightarrow a_i - a_{i-1} = a_{i+1} - a_i, \forall i = 1, 2, \ldots, k-1.$$

Điều này chứng tỏ A là một cấp số cộng. Định lý được chứng minh. □

Tổng quát hơn, ta có đánh giá sau đây.

Định lý 2. *Cho $n \geqslant 2$ và $A_1, A_2, \ldots, A_n$ là các tập hợp hữu hạn số nguyên. Khi đó*

$$|A_1| + |A_2| + \cdots + |A_n| - (n-1) \leqslant |A_1 + A_2 + \cdots + A_n| \leqslant |A_1| \cdot |A_2| \cdots |A_n|.$$

Lời giải. Bất đẳng thức $|A_1 + A_2 + \cdots + A_n| \leqslant |A_1| \cdot |A_2| \ldots |A_n|$ là hiển nhiên, do số biểu diễn dạng $a_1 + a_2 + \cdots + a_n (a_i \in A_i)$ là $|A_1| \cdot |A_2| \ldots |A_n|$.

Ta chứng minh bất đẳng thức còn lại bằng quy nạp. Với $n = 2$, đặt

$$A_1 = \{a_0, a_1, \ldots, a_{k-1}\}, \quad A_2 = \{b_0, \ldots, b_{l-1}\}$$

với $a_0 < a_1 < \cdots < a_{k-1}, b_0 < b_1 < \cdots < b_{l-1}$. Giả sử $|A_1| = k \leqslant l = |A_2|$. Khi đó tập $A_1 + A_2$ chứa $2k - 1 + (l-k)$ các phần tử phân biệt sau

$$\begin{aligned} a_0 + b_0 &< a_0 + b_1 < a_1 + b_1 < a_1 + b_2 < \cdots \\ &< a_i + b_i < a_i + b_{i+1} < a_{i+1} + b_{i+1} < \cdots \\ &< a_{k-1} + b_{k-1} < a_{k-1} + b_k < a_{k-1} + b_{k+1} < \cdots < a_{k-1} + b_{l-1}. \end{aligned}$$

Do đó

$$|A_1 + A_2| \geqslant (2k-1) + (l-k) = |A_1| + |A_2| - 1.$$

Vậy $n = 2$ định lý đúng. Giả sử kết luận đúng cho mọi $\leqslant n-1$ tập hữu hạn các số số. Khi đó với n tập thì

$$\begin{aligned} |A_1| + |A_2| + \cdots + |A_n| &= |(A_1 + A_2 + \cdots + A_{n-1}) + A_n| \\ &\geqslant |A_1 + A_2 + \cdots + A_{n-1}| + |A_n| - 1 \\ &\geqslant |A_1| + |A_2| + \cdots + |A_{n-1}| - (n-2) + |A_n| - 1 \\ &= |A_1| + |A_2| + \cdots + |A_n| - (n-1). \end{aligned}$$

Chứng tỏ kết luận đúng với n. Theo phương pháp quy nạp thì bài toán đúng cho với mọi n tập hữu hạn các số nguyên. □

Bổ đề 1. *Cho A, B là hai tập hợp hữu hạn các số nguyên và $|A| = |B| = k$. Nếu $|A + B| = |A| + |B| - 1$ thì A và B là **hai cấp số cộng có cùng công sai**.*

Lời giải. Đặt $A = \{a_0, a_1, a_2, \ldots, a_{k-1}\}$ và $B = \{b_0, b_1, b_2, \ldots, b_{k-1}\}$ với $a_0 < a_1 < \cdots < a_{k-1}, b_0 < b_1 < \cdots < b_{k-1}$. Khi đó $A + B$ chứa một dãy gồm $2k-1$ số nguyên tăng dần sau

$$\begin{aligned} a_0 + b_0 &< a_0 + b_1 < a_1 + b_1 < a_1 + b_2 < \cdots \\ &< a_{i-1} + b_i < a_i + b_i < a_i + b_{i+1} + a_{i+1} + b_{i+1} < \cdots \\ &< \cdots < a_{k-1} + b_{k-1}. \end{aligned}$$

Do $|A| + |B| = 2k - 1$, suy ra dãy số nguyên trên chứa toàn bộ các phần tử của tập $A + B$. Do

$$a_{i-1} + b_i < a_i + b_i < a_i + b_{i+1}$$

và

$$a_{i-1} + b_i < a_{i-1} + b_{i+1} < a_i + b_{i+1}$$

dẫn đến

$$a_{i-1} + b_{i+1} = a_i + b_i \Rightarrow a_i - a_{i-1} = b_{i+1} - b_i, \forall i = 1, 2, \ldots, k-2 \quad (1).$$

Tương tự, bất đẳng thức

$$a_{i-1} + b_{i-1} < a_{i-1} + b_i < a_i + b_i$$

và

$$a_{i-1} + b_{i-1} < a_i + b_{i-1} < a_i + b_i$$

dẫn đến

$$a_{i-1} + b_i = a_i + b_{i-1} \Rightarrow a_i - a_{i-1} = b_i - b_{i-1}, \forall i = 1, 2, \ldots, k-1 \quad (2).$$

Từ (1) và (2), đặt $q = a_1 - a_0$ thì

$$a_i - a_{i-1} = b_i - b_{i-1} = q, \forall i = 1, 2, \ldots, k-1.$$

Chứng tỏ A, B là hai cấp số cộng có cùng công sai q. □

Tổng quát hơn ta có kết quả sau. Bạn đọc quan tâm chứng minh của nó tham khảo bổ đề 1.3, trang 10, tài liệu tham khảo [3].

Định lý 3. *Cho A, B là hai tập hữu hạn các số nguyên, với $|A| = k \geqslant 2, |B| = l \geqslant 2$. Nếu $|A + B| = k + l - 1$ thì A, B là hai cấp số cộng có cùng công sai.*

2. Định lý cauchy - davenport

Trong phần này, nếu không chú thích gì thêm thì tất cả các tập hợp được lấy là các tập con trong trường $\mathbb{Z}_p$, tập chứa hệ thặng dư đầy đủ modulo p.

Định lý 4 (**Định lý Cauchy - Davenport**). *Cho p là số nguyên tố và A, B là hai tập con của $\mathbb{Z}_p$. Khi đó*

$$|A + B| \geqslant \min\{p, |A| + |B| - 1\}.$$

2.1. Chứng minh thông qua phép biến đổi Davenport

Cho B là tập con của $\mathbb{Z}_p$, $\boxed{0 \in B, |B| \geqslant 2 \text{ và } A + B \neq \mathbb{Z}_p}$. Khi đó ta có một số nhận xét sau:

- $\boxed{A + B \text{ là tập con } \textbf{thực sự} \text{ của } A + 2B}$. Thật vậy, với $x \in A + B$, khi đó

$$x = a + b (a \in A, b \in B) \Rightarrow x = \underbrace{a}_{\in A} + \underbrace{b}_{\in B} + \underbrace{0}_{\in B} \in A + 2B.$$

  Vậy $A + B \subseteq A + 2B$. Mặt khác nếu $A + B = A + 2B$ thì ta sẽ có $A + 2B = A + 3B$. Thật vậy:

- $x \in A + 2B$ thì $x = a + b_1 + b_2 (a \in A, b_1, b_2 \in B)$ nên

$$x = \underbrace{a}_{\in A} + \underbrace{b_1}_{\in B} + \underbrace{b_2}_{\in B} + \underbrace{0}_{\in B} \in A + 3B.$$

  Do đó $x \in A + 3B$ nên $A + 2B \subset A + 3B$.

- $x \in A+3B$ thì $x = a+b_1+b_2+b_3 (a \in A, b_1, b_2, b_3 \in B)$. Do $a+b_1+b_2 \in A+2B$ mà $A + 2B = A + B$ nên xảy ra

$$a + b_1 + b_2 = a' + b' (a' \in A, b' \in B).$$

  Khi đó $x = a + b_1 + b_2 + b_3 = \underbrace{a'}_{\in A} + \underbrace{b'}_{\in B} + \underbrace{b_3}_{\in B} \in A + 2B$. Do đó $A + 3B \subset A + 2B$.

Và hoàn toàn tương tự ta có $A + B = A + 2B = A + 3B = \cdots$. Nhưng khi đó với $a \in A$ và $0 \neq b \in B$ (b tồn tại do $|B| \geqslant 2$) thì $a + nb \in A + B, \forall n = 0, 1, 2, \ldots$. Điều này phải xảy ra $A + B = \mathbb{Z}_p$, trái với giả thiết.

- Đặt $X = (A + 2B) \backslash (A + B)$, khi đó $X \neq \emptyset$. Đặt

$$\boxed{B_x^* = \{b \in B | x - b \in A + B\}, \quad B_x = B \backslash B_x^*}.$$

  Khi đó tập B_x được gọi là **biến đổi Davenport** của tập B.

  - Khi đó $0 \notin B_x^* \neq \emptyset$. Thật vậy, nếu $0 \in B_x^*$ thì $x - 0 \in A + B$ hay $x \in A + B$, mâu thuẫn do $x \in X$. Ngoài ra $B_x^* \neq \emptyset$ vì với $x \in X$, khi đó

$$x = \underbrace{a}_{\in A} + \underbrace{b_1}_{\in B} + \underbrace{b_2}_{\in B},$$

    do đó

$$x - b_1 = a + b_2 \in A + B \Rightarrow b_1 \in B_x^*.$$

  - Ta có $0 \in B_x \subset B$, và $(A + B_x) \cup (x - B_x^*) \subset A + B \quad (1)$ (tính chất này hiển nhiên do định nghĩa của hai tập B_x, B_x^*). Ngoài ra ta có $(A + B_x) \cap (x - B_x^*) = \emptyset \quad (2)$. Thật vậy, giả sử có

$$a + \underbrace{b_x}_{\in B_x} = x - \underbrace{b_x^*}_{\in B_x^*} \Rightarrow x - b_x = \underbrace{a}_{\in A} + \underbrace{b_x^*}_{\in B_x^* \subset B} \in A + B.$$

    Do đó $x - b_x \in A + B \Rightarrow b_x \in B_x^*$ (theo định nghĩa của B_x^*), mâu thuẫn với $b_x \in B_x$.

  - Từ (1) và (2) ta có

$$|A + B| \geqslant |A + B_x| + |x - B_x^*|.$$

    Vì $|x - B_x^*| = |B_x^*| = |B| - |B_x|$ nên ta được

$$\boxed{|A + B| \geqslant |A + B_x| + |B| - |B_x| \quad (*)}.$$

Chứng minh định lý 2.1. Giả sử định lý không đúng, khi đó tồn tại hai tập con A, B của $\mathbb{Z}_p$ mà $A + B \neq \mathbb{Z}_p$ (3) và

$$|A + B| \leqslant |A| + |B| - 2 \quad (4).$$

Kết quả (3), và (4) sẽ không thay đổi nếu thay B bởi $-b + B$ (với $b \in B$ tùy ý) (*Thật vậy, (3) suy ra các phần tử của $A + B$ không lập thành một hệ thặng dư modulo p, khi đó các phần tử của tập $A + (-b + B)$ chẳng qua là các phần tử của tập $A + B$ tịnh tiến sang trái $-b$ đơn vị nên cũng không thể lập thành một hệ thặng dư đầy đủ modulo p. Còn tính chất* (4) *hiển nhiên khi thay B bởi $-b + B$ vì $|-b + B| = |B|$*).

Do đó, ta có thể **giả sử** $0 \in B$. Trong tất cả các cặp A, B thỏa mãn (3), (4) ta chọn cặp A, B mà $|B|$ **nhỏ nhất**. Khi đó $|B| \geqslant 2$ (*vì nếu $|B| \leqslant 1$, khi đó $|A+B| = |A|$, còn $|A|+|B|-2 \leqslant |A|-1$ thì (4) không xảy ra.*) Vậy ta đã có $0 \in B, |B| \geqslant 2, A + B \neq \mathbb{Z}_p$. Do đó tồn tại phép biến đổi Davenport B_x của B để (*) xảy ra. Do $1 \leqslant |B_x| < |B|$. Do $B_x \subset B$ nên $A + B_x \subset A + B$, suy ra $|A + B_x| < |A + B| < p$. Kết hợp (*) và (4) ta có

$$|A + B_x| \leqslant |A + B| - |B| + |B_x| \leqslant |A| + |B_x| - 2,$$

tức (4) lại đúng cho B_x, mà $B_x \subset B$, mâu thuẫn với tính nhỏ nhất của $|B|$. Vậy điều phản chứng là sai. Định lý được chứng minh hoàn toàn. □

2.2. Chứng minh bằng đa thức nhiều biến

Bổ đề 2. *Cho đa thức $P(x_1, x_2, \ldots, x_n)$ là một đa thức n biến hệ số thực với bậc của P theo biến x_i lớn nhất là t_i, $1 \leqslant i \leqslant n$. Gọi $S_1, S_2, \ldots, S_n$ là các tập con của $\mathbb{R}$ và $|S_i| = t_i + 1, \forall i = 1, 2, \ldots, n$. Nếu $P(s_1, s_2, \ldots, s_n) = 0$ với mọi $(s_1, s_2, \ldots, s_n) \in S_1 \times S_2 \times \cdots \times S_n$ thì $P \equiv 0$.*

Lời giải. Ta chứng minh bằng quy nạp theo n, số các biến của đa thức P. Với $n = 1$, $P(x_1)$ là đa thức một biến x_1, có bậc là t_1. Vì $P(x_1) = 0$ tại $|S_1| = t_1 + 1$ điểm, nên theo tính chất của đa thức một biến thì $P \equiv 0$. Vậy bổ đề đúng cho $n = 1$. Giả sử bổ đề đúng cho mọi đa thức $n - 1$ biến, $n \geqslant 2$. Xét đa thức $P(x_1, x_2, \ldots, x_n)$ là đa thức n biến. Ta viết là đa thức này **như là đa thức một biến** x_n:

$$P_n(x_n) = P(x_1, x_2, \ldots, x_n) = \sum_{i=0}^{t_n} Q_i(x_1, \ldots, x_{n-1}) x_n^i.$$

Vì đa thức P_n là đa thức một biến x_n, có bậc t_n và bằng 0 tại $t_n + 1$ điểm trong S_n. Do đó lại theo tính chất đa thức một biến ta được

$$P_n \equiv 0 \Rightarrow Q_i(x_1, x_2, \ldots, x_{n-1}) = 0, \forall i = 0, 1, \ldots, t_n.$$

(*đến đây mới chứng tỏ được các đa thức $n - 1$ biến $Q_i (i = 1, 2, \ldots, t_n)$ bằng 0 tại các điểm của $S_1 \times S_2 \times \cdots \times S_{n-1}$. Tiếp theo phải chứng minh các đa thức này đồng nhất 0*) Nhưng với mỗi $i = 0, 1, \ldots, t_n$ thì

$$Q_i(x_1, x_2, \ldots, x_{n-1}) = 0, \forall (x_1, x_2, \ldots, x_{n-1}) \in S_1 \times S_2 \times \cdots \times S_{n-1}$$

nên theo giả thiết quy nạp thì $Q_i \equiv 0, \forall i = 0, 1, \ldots, t_n$. Từ đó chứng tỏ $P \equiv 0$. Kết luận bài toán đúng với n. Theo phương pháp quy nạp, thì bổ đề đúng cho mọi đa thức n biến.

□

Định lý 5. *Cho đa thức $P(x_1, x_2, \ldots, x_n)$ là một đa thức n biến hệ số thực. Gọi $S_1, S_2, \ldots, S_n$ là các tập con của $\mathbb{R}$. Định nghĩa đa thức*

$$Q_i(x_i) = \prod_{s \in S_i} (x_i - s).$$

Nếu $P(s_1, s_2, \ldots, s_n) = 0$ với mọi $(s_1, s_2, \ldots, s_n) \in S_1 \times S_2 \times \cdots \times S_n$, thì tồn tại các đa thức $R_1, \ldots, R_n \in \mathbb{R}[x_1, \ldots, x_n]$ với $\deg R_i \leqslant \deg P - \deg Q_i$ sao cho

$$P = R_1 Q_1 + R_2 Q_2 + \cdots + R_n Q_n.$$

Lời giải. Đặt $t_i = |S_i| - 1$. Ta xét thuật toán sau đây: "Nếu có một đơn thức $c x_1^{m_1} \ldots x_n x_n^{m_n}$ trong P mà $m_i > t_i$, với một chỉ số i nào đó, thì ta thay thế đại lượng $x_i^{m_i}$ bởi $x_i^{m_i} - x_i^{m_i - (i+1).Q_i(x_i)}$".

- Do $\deg Q_i = t_i + 1$ và Q_i là đa thức monic, khi đó đơn thức $x_1^{m_1} \ldots x_n x_n^{m_n}$ sẽ được thay thế bởi **một số đơn thức khác, nhưng tất cả các đơn thức đó đều có bậc nhỏ hơn** $m_1 + m_2 + \cdots + m_n$.
- Do đó, sau mỗi bước của thuật toán này, thì tổng các bậc của tất cả các đơn thức trong P **sẽ giảm thực sự**. Nhưng do tổng ban đầu là hữu hạn, nên thuật toán này sẽ kết thúc sau một số hữu hạn lần thực hiện.

Gọi $\overline{P}$ là đa thức cuối cùng nhận được sau mỗi lần thực hiện thuật toán trên. Khi đó phép biến đổi

$$c x_1^{m_1} \cdots x_i^{m_i} \cdots x_n x_n^{m_n} \mapsto c x_1^{m_1} \cdots \left(x_i^{m_i} - x_i^{m_i - (i+1)} Q_i(x_i) \right) \cdots x_n^{m_n}$$

tương ứng là **một phép trừ** của đa thức P cho một đa thức có dạng $R_i'.Q_i$, với

$$R_i' = c x_1^{m_1} \cdots x_i^{m_i - (i+1)} \ldots x_n^{m_n}$$

và

$$\deg R_i' = m_1 + \cdots + m_n - (t_i + 1) \leqslant \deg P - \deg Q_i.$$

Do đó quá trình này thực hiện cho tất cả các đơn thức trong P, khi đó

$$\overline{P} = P - R_1 \cdot Q_1 + \cdots + R_n \cdot Q_n$$

(*ở đây R_i là tổng của các đa thức R_i' ở trên (mỗi đơn thức trong P có $m_i > t_i$ ta đều có một R_i'. Thực hiện thuật toán cho tất cả các đơn thức này, ta sẽ được các R_i' khác nhau). Vì R_i' có bậc đều $\leqslant \deg P - \deg Q_i$ nên*) ta có

$$\deg R_i \leqslant \deg P - \deg Q_i.$$

Vì $\overline{P}$ nhận được cuối cùng của thật toán trên, nên **mỗi biến x_i trong $\overline{P}$ có lũy thừa cao nhất là** t_i. Vì

$$Q_i(x_i) = 0, \forall x_i \in S_i$$

nên suy ra

$$\overline{P}(s_1, s_1, \ldots, s_n) = P(s_1, s_2, \ldots, s_n), \quad \forall (s_1, s_2, \ldots, s_n) \in S_1 \times S_2 \times \cdots \times S_n.$$

Theo bổ đề 2.2 thì $\overline{P} \equiv 0$, do đó

$$P = R_1 Q_1 + R_2 Q_2 + \cdots + R_n Q_n.$$

□

Định lý 6 (**Combinatorial Nullstellensatz**). *Cho đa thức $P(x_1, \ldots, x_n) \in \mathbb{R}[x_1, \ldots, x_n]$ có bậc* $\deg P = t_1 + \cdots + t_n$*, với t_i là các số nguyên không âm và hệ số của đơn thức $x_1^{t_1} \cdots x_n^{t_n}$ khác 0. Nếu $S_1, \ldots, S_n$ là các tập con của $\mathbb{R}$ thỏa $|S_i| > t_i$, khi đó tồn tại một bộ $(s_1, \ldots, s_n) \in S_1 \times S_2 \times \cdots \times S_n$ sao cho*

$$\boxed{P(s_1, s_2, \ldots, s_n) \neq 0}.$$

Lời giải. Ta chỉ cần chứng minh kết luận bài toán trong trường hợp $|S_i| = t_i + 1$ (vì nếu $|S_i| > t_i + 1$ thì hiển nhiên kết luận bài toán đúng, nếu ta chứng minh được khẳng định với $|S_i| = t_i + 1$). Giả sử kết luận bài toán **không đúng**, tức là

$$P(s_1, s_2, \ldots, s_n) = 0, \forall (s_1, \ldots, s_n) \in S_1 \times S_2 \times \cdots \times S_n.$$

Khi đó, theo định lý 2.3 thì

$$P = R_1 \cdot Q_1 + R_2 \cdot Q_2 + \cdots + R_n \cdot Q_n$$

với $\deg R_i \leqslant \deg P - \deg Q_i, \forall i = 1, 2, \ldots, n$. Theo giả thiết, hệ số của $x_1^{t_1} \cdots x_n^{t_n}$ ở vế phải khác 0. Tuy nhiên, do $\deg R_i \cdot Q_i \leqslant \deg P$ và một đơn thức trong $R_i \cdot Q_i$ mà có bậc $t_1 + \cdots + t_n$ khi và chỉ khi (theo cách xây dựng trong 2.3), chúng ta lấy R_i nhân với $x_i^{t_i+1}$ trong khai triển

$$Q_i(x_i) = \prod_{s \in S_i} (x - s_i) = x_i^{t_i+1} + \underbrace{\cdots}_{\text{các thừa số còn lại có bậc} \leqslant t_i}.$$

Từ đây suy ra **mọi đơn thức trong $R_1.Q_1 + \cdots + R_nQ_n$ mà có tổng bậc bằng $t_1 + \cdots + t_n$ đều phải chia hết cho $x_i^{t_i+1}$, với một chỉ số $i \in \{1, 2, \ldots, n\}$**. Do đó đơn thức $x_1^{t_1} \cdots x_n^{t_n}$ nằm trong $R_1 \cdot Q_1 + \cdots + R_nQ_n$ có tổng bậc bằng $t_1 + \cdots + t_n$ cũng phải chia hết cho $x_i^{t_i+1}$. Điều này chỉ xảy ra được khi hệ số của $x_1^{t_1} \cdots x_n^{t_n}$ bằng 0. Điều này trái với giả thiết. Vậy điều phản chứng là sai. Định lý được chứng minh. □

Chú ý: Các định lý trên đúng cho đa thức trên trường $\mathbb{R}$, nó cũng vẫn đúng trên trường $\mathbb{Z}_p$.
Trước khi áp dụng định lý 2.4 để chứng minh định lý 2.1 ta sẽ thấy một ứng dụng đẹp của nó trong bài toán khá nổi tiếp sau: IMO 2007.

Ví dụ 1 (**IMO 2007**). *Cho n là một số nguyên dương. Đặt*

$$S = \{(x, y, z) \mid x, y, z \in \{0, 1, \ldots, n\}, x + y + z > 0\}$$

là một tập chứa $(n + 1)^3 - 1$ điểm trong không gian ba chiều. Xác định số mặt phẳng ít nhất, sao cho hợp của chúng chứa S, nhưng không chứa điểm $(0, 0, 0)$.

Lời giải. Dễ dàng nhận thấy $3n$ mặt phẳng có phương trình $x + y + z = i, \forall i = 1, 2, \ldots, 3n$ là đạt được yêu cầu bài toán. Ta chứng minh $3n$ chính là số mặt phẳng nhỏ nhất cần tìm. Giả sử ngược lại, tồn tại các mặt phẳng $P_1, P_2, \ldots, P_k (k \leqslant 3n - 1)$ mà hợp của chúng phủ hết tập S và không chứa điểm $(0, 0, 0)$. Mỗi mặt phẳng P_i xác định bởi một phương trình

$$a_i x + b_i y + c_i z + d_i = 0.$$

Nhận thấy $d_i \neq 0$ do $(0,0,0) \notin P_i$. Hợp của các mặt phẳng P_i phủ hết các điểm của S nếu và chỉ nếu

$$P(x,y,z) = \prod_{i=1}^{k}(a_i x + b_i y + c_i z + d_i) = 0, \forall (x,y,z) \in S.$$

Vì $0 \notin P_i$ nên $P(0,0,0) \neq 0$. Đặt $S_1 = S_2 = S_3 = \{0,1,2,\ldots,n\}$. Khi đó

$$S \cup \{(0,0,0)\} = S_1 \times S_2 \times S_3.$$

Xét đa thức

$$Q(x,y,z) = P(x,y,z) - c.\prod_{i=1}^{k}(x-i)(y-i)(z-i),$$

với c là hằng số và bằng $c = \dfrac{P(0,0,0)}{(-1)^{3n}(n!)^3}$.

- Nhận thấy $Q(x,y,z) = 0, \forall (x,y,z) \in S_1 \times S_2 \times S_3 \quad (*)$.
- Lại do $k < 3n$ nên deg $Q = 3n$. Hệ số của $x^n y^n z^n$ trong Q là $-c \neq 0$. Theo định lý 2.4, tồn tại một điểm $(x_0, y_0, z_0) \in S_1 \times S_2 \times S_3$ để $Q(x_0, y_0, z_0) \neq 0$, mâu thuẫn với (*).

Từ đó chứng tỏ điều phản chứng sai. Bài toán được chứng minh. □

Chứng minh định lý 2.1 bằng định lý 2.4. Nếu $|A| + |B| - 1 \geqslant p$. Khi đó $A + B = \mathbb{Z}_p$. Thật vậy, do $|A| + |B| > p$ nên với mọi $x \in \mathbb{Z}_p$ thì tập $A \cap (x - B) \neq \emptyset$ (vì nếu $A \cap (x - B) = \emptyset$ thì $A, e - B$ đều là tập con của $\mathbb{Z}_p$ nên $p \geqslant |A| + |x - B| = |A| + |B| > p$, vô lý). Từ đó mọi phần tử $x \in \mathbb{Z}_p$ đều có thể viết dưới dạng $x = a + b, a \in A, b \in B$ hay $x \in A + B$. Chứng tỏ $\mathbb{Z}_p \subset A + B$, suy ra $A + B = \mathbb{Z}_p$, định lý đúng trong trường hợp này.

Nếu $|A| + |B| < p$. Giả sử kết luận bài toán không đúng, tức là $|A + B| \leqslant |A| + |B| - 2$. Đặt C là tập hợp sao cho $A + B \subset C$ và $|C| = |A| + |B| - 2$. Xét đa thức

$$P(x,y) = \prod_{c \in C}(x + y - c)$$

thì deg $P = |A| + |B| - 2$. Vì $A + B \subset C$ nên

$$P(a,b) = 0, \forall (a,b) \in A \times B. \quad (*)$$

Mặt khác, hệ số của $x^{|A|-1}y^{|B|-1}$ trong P là $\binom{|A|+|B|-2}{|A|-1}$. Vì $|A| + |B| - 2 < p$ nên hệ số này khác trong trong $\mathbb{Z}_p$. Do đó theo định lý 2.4 tồn tại $(a,b) \in A \times B$ sao cho $P(a,b) = 0$, mâu thuẫn với (*). Vậy điều phản chứng không đúng. Chứng tỏ kết luận đúng trong trường hợp này. □

Định lý 7. *Cho p là số nguyên tố, A, B là hai tập con khác rỗng của $\mathbb{Z}_p$. Định nghĩa*

$$A \oplus B = \{a + b | a \in A, b \in B, a \neq b\}.$$

Khi đó

$$|A \oplus B| \geqslant \min\{p, |A| + |B| - 3\}. \quad (1)$$

Nếu $|A| \neq |B|$ thì ta có kết quả mạnh hơn

$$|A \oplus B| \geqslant \min\{p, |A| + |B| - 2\}. \quad (2)$$

Lời giải. • Nếu $|A| = 1$ hoặc $|B| = 1$, khi đó bất đẳng thức (2) hiển nhiên. Xét $|A|, |B| \geqslant 2$. Trong trường hợp $|A = |B|$, khi đó ta lấy tập $B' = B\backslash\{b\}$, với b là một phần tử bất kỳ của B. Khi đó áp dụng (2) cho hai tập A và B' ta được bất đẳng thức (1).

- Từ đó ta chỉ cần chứng minh (2).
  - Trường hợp $|A| + |B| - 2 \geqslant p$. Nếu $p \geqslant 2$ hiển nhiên. Xét $p > 2$ thì p lẻ. Ta sẽ chứng minh $A + B = \mathbb{Z}_p$. Thật vậy, xét $g \in \mathbb{Z}_p$ là một phần tử tùy ý. Đặt $C = g - B$, thì $|C| = |B|$. Khi đó $|A| + |C| = |A| + |B| \geqslant p + 2$. Theo công thức
  $$|X \cup Y| + |X \cap Y| = |X| + |Y|$$
  ta có
  $$\left|\mathbb{Z}_p\right| + |A \cap C| \geqslant |A \cup C| + |A \cap C| = |A| + |C| \geqslant p + 2 \Rightarrow |A \cap C| \geqslant 2.$$
  Gọi x, y là hai phần tử phân biệt của $A \cap C$. Vì $C = g - B$, nên tồn tại hai phần tử $b_x, b_y \in B$ sao cho
  $$x + b_x = y + b_y = g.$$
  Ta sẽ có được kết luận bài toán nếu chỉ ra được $x \neq b_x$ **hoặc** $y \neq b_y$ (khi đó $g \in A \oplus B$). Giả sử cả hai điều trên đều không xảy ra, khi đó $x + x = y + y = g \Rightarrow 2(x - y) = 0$. Suy ra $2 \vdots p$, vô lý do p nguyên tố lẻ.
  - Xét trường hợp $|A| + |B| - 2 < p$. Giả sử kết luận của định lý không đúng, tức là $|A \oplus B| < |A| + |B| - 2$. Gọi C là một tập hợp trong $\mathbb{Z}_p$ có $|A| + |B| - 3$ phần tử và $A + \oplus B \subset C$. Xét đa thức
  $$P(x, y) = (x - y) \prod_{c \in C} (x + y - c).$$
  Nhận thấy rằng với mọi $a \in A, b \in B$ thì $P(a, b) = 0$. Mặt khác, ta có $\deg P = |C| + 1 = |A| + |B| - 2$. Do $|A| \neq |B|$, nên hệ số của $x^{|A|-1} y^{|B|-1}$ trong P là
  $$\binom{m+n-3}{m-2} - \binom{m+n-3}{m-1} = \frac{(m+n-3)!}{(m-2)!(n-1)!} - \frac{(m+n-3)!}{(m-1)!(n-2)!}$$
  $$= \frac{(m+n-3)!}{(m-1)!(n-2)!}(m-n),$$
  là khác 0 (theo modulo p) do $m + n - 3 < p$ và $m \neq n$. Do đó theo định lý 2.4 tồn tại $(a, b) \in A \times B$ sao cho $P(a, b) \neq 0$, mâu thuẫn. Vậy điều giả sử là sai. Trường hợp này đã được chứng minh.

Vậy định lý được chứng minh hoàn toàn. □

Định lý 8 (**Định lý Cauchy - Davenport tổng quát**). *Giả sử p là số nguyên tố và $A_1, A_2, \ldots, A_n$ là các tập con của $\mathbb{Z}_p$ ($n \geqslant 2$). Khi đó*

$$|A_1 + A_2 + \cdots + A_n| \geqslant \min\{p, |A_1| + |A_2| + \cdots + |A_n| - (n-1)\}.$$

Lời giải. Ta chứng minh bằng phương pháp quy nạp. Với $n = 2$, thì kết quả trên là định lý 2.1. Giả sử định lý đúng với $n-1$. Khi đó, với n tập $A_1, \ldots, A_n$ thì

$$\begin{aligned}
&|A_1 + A_2 + \cdots + A_n| = |(A_1 + \ldots + A_{n-1}) + A_n)| \\
&\geqslant \min\{p, |A_1 + \ldots + A_{n-1}| + |A_n| - 1\} \quad \text{(áp dụng cho } n = 2 \text{ tập)} \\
&\geqslant \min\{p, \min\{p, |A_1| + |A_2| + \ldots + |A_{n-1}| - (n-2)\} + |A_n| - 1\} \quad \textit{(giả thiết quy nạp cho } n-1 \textit{ tập)}.
\end{aligned}$$

- Nếu $\min\{p, |A_1| + |A_2| + \cdots + |A_{n-1}| - (n-2)\} = p (*)$, khi đó

$$\min\{p, \min\{p, |A_1|+|A_2|+\cdots+|A_{n-1}|-(n-2)\}+|A_n|-1\} = \min\{p, p+|A_n|-1\} = p (1) (\text{do } |A_n| \geqslant 1).$$

Mặt khác từ (*) thì $|A_1| + |A_2| + \cdots + |A_{n-1}| - (n-2) \geqslant p$ nên

$$|A_1| + |A_2| + \cdots + |A_{n-1}| + |A_n| - (n-1) \geqslant p + |A_n| - 1 \geqslant p$$

$$\Rightarrow \min\{p, |A_1| + |A_2| + \cdots + |A_n| - (n-1)\} = p. \quad (2)$$

Từ (1) và (2) suy ra

$$\min\{p, \min\{p, |A_1|+|A_2|+\cdots+|A_{n-1}|-(n-2)\}+|A_n|-1\} = \min\{p, |A_1|+|A_2|+\cdots+|A_n|-(n-1)\} (3).$$

- Nếu $\min\{p, |A_1| + |A_2| + \cdots + |A_{n-1}| - (n-2)\} = |A_1| + |A_2| + \cdots + |A_{n-1}| - (n-2)$ thì

$$\begin{aligned}
&\min\{p, \min\{p, |A_1| + |A_2| + \cdots + |A_{n-1}| - (n-2)\} + |A_n| - 1\} \\
&= \min\{p, |A_1| + |A_2| + \cdots + |A_{n-1}| + |A_n| - (n-1)\}. \quad (4)
\end{aligned}$$

Trong cả hai trường hợp (3) và (4) ta đều có

$$|A_1 + A_2 + \cdots + A_n| \geqslant \min\{p, |A_1| + |A_2| + \cdots + |A_n| - (n-1)\}$$

tức định lý đúng cho n. Theo phương pháp quy nạp ta có điều phải chứng minh. □

Định lý 9 (**Định lý Vosper**). *Cho p là số nguyên tố và A, B là hai tập con của $\mathbb{Z}_p$ sao cho $|A|, |B| \geqslant 2$ và $|A + B| \leqslant p - 2$. Khi đó $|A + B| = |A| + |B| - 1$ khi và chỉ khi A, B là hai cấp số cộng có cùng công sai.*

Chú ý: Bạn đọc cần tìm hiểu chứng minh định lý này, có thể tham khảo một chứng minh khá sơ cấp trong định lý 3.2 tài liệu tham khảo [4]. Ngoài ra trong tài liệu này, định lý 3.1 cũng cung cấp thêm một cách chứng minh sơ cấp bằng quy nạp, theo qua phép biến đổi e. Chính cách chứng minh này cho ta một lời giải cho bài tập 4.11.

3. Một số ứng dụng

Ví dụ 2 (**Poland 2003**). *Chứng minh rằng với mọi số nguyên tố $p > 3$, tồn tại các số nguyên x, y, k sao cho $0 < 2k < p$ và $x^2 + y^2 = kp + 3$.*

Lời giải. Kết quả của bài toán không thay đổi nếu thay x, y bởi $p-x, p-y$. Do đó ta sẽ chỉ ra các số x, y trong miền $0 \leqslant x, y < \dfrac{p}{2}$ thỏa mãn điều kiện bài toán. Khi x, y nằm trong miền này thì hiển nhiên phần thương k sẽ thỏa $2k < p$, vì

$$x^2 + y^2 < \frac{p^2}{4} + \frac{p^2}{4} = \frac{p^2}{2}.$$

Đặt S là tập chứa tất cả **bình phương theo modulo** p. Chú ý $x^2 \equiv (p-x)^2 \pmod{p}, \forall x \in \left\{1, 2, \ldots, \left[\frac{p}{2}\right]\right\}$. Do đó $|S| = \dfrac{p+1}{2}$. Theo định lý 2.1 thì

$$|S+S| \geqslant \min\{p, 2|S|-1\} = \min\left\{p, 2.\frac{p+1}{2} - 1\right\} = p \Rightarrow |S+S| = p.$$

Điều này chứng tỏ mọi thặng dư modulo p đều có thể viết được thành tổng của hai số chính phương. Và bài toán là trường hợp đặc biệt với kết quả bằng 3. □

Ví dụ 3. *Cho p là số nguyên tố. Cho trước $p-1$ số nguyên sao cho không có số nào chia hết cho p. Chứng minh rằng ta có thể đổi dấu một vài số trong chúng để tổng của các số thu được chia hết cho p.*

Lời giải. Gọi $p-1$ số nguyên là $a_1, a_2, \ldots, a_{p-1}$. Với mỗi $i = 1, 2, \ldots, p-1$, đặt

$$A_i = \{a_i, -a_i\} \pmod{p}.$$

Khi đó $|A_i| = 2, \forall i = 1, 2, \ldots, p-1$ vì $a_i \not\equiv -a_i \pmod{p}$. Áp dụng định lý 2.6 ta có

$$|A_1 + A_2 + \cdots + A_{p-1}| \geqslant \min\{p, |A_1| + \cdots + A_{p-1} - (p-2)\} = \min\{p, p\} = p.$$

Từ đây suy ra

$$|A_1 + A_2 + \cdots + A_{p-1}| = p$$

hay tập $A_1 + A_2 + \cdots + A_{p-1}$ chứa một hệ thặng dư đầy đủ modulo p. Đây chính là kết luận của bài toán. □

Ví dụ 4. *Giả sử $p > 2$ là số nguyên tố và cho $p-1$ số nguyên $a_1, a_2, \ldots, a_{p-1}$ thỏa mãn $a_1 \cdots a_{p-1} \not\vdots p$ và $a_1 + a_2 + \cdots + a_{p-1} \not\vdots p$. Chứng minh rằng có thể chia tập này thành hai nhóm rời nhau để tổng các phần tử của hai nhóm đồng dư với nhau theo modulo p.*

Lời giải. Đặt $A_i = \{0, a_i\} \pmod{p}$. Thì do $a_i \not\vdots p, \forall i = 1, 2, \ldots, p-1$ nên $|A_i| = 2, \forall i = 1, 2, \ldots, p-1$. Theo định lý 2.6 thì

$$|A_1 + A_2 + \cdots + A_{p-1}| \geqslant \min\{p, |A_1| + \cdots + |A_{p-1}| - (p-2)\} = \min\{p, 2(p-1) - (p-2)\} = p.$$

Do đó $A_1 + A_2 + \cdots + A_{p-1} = \mathbb{Z}_p$. Khi đó tồn tại $b_i \in A_i, i = 1, 2, \ldots, p-1$ sao cho

$$b_1 + b_2 + \cdots + b_{p-1} \equiv \frac{a_1 + a_2 + \cdots + a_{p-1}}{2} \pmod{p}.$$

Vì mỗi phần tử $b_i \in A_i$ thì b_i hoặc bằng 0, hoặc bằng a_i. Tuy nhiên do $a_1+a_2+\cdots+a_{p-1} \not\equiv 0 \pmod p$ nên tồn tại một số phần tử b_i khác 0. Gọi các phần tử đó là $a_{j_1},\ldots,a_{j_k}$, thì thay vào ta có

$$a_{j_1}+\cdots+a_{j_k} \equiv \frac{a_1+a_2+\cdots+a_{p-1}}{2} \pmod p$$

hay

$$2\left(a_{j_1}+\cdots+a_{j_k}\right) \equiv a_1+\cdots+a_{p-1} \pmod p$$

hay

$$a_{j_1}+\cdots+a_{j_k} \equiv (a_1+\cdots+a_{p-1})-(a_{j_1}+\cdots+a_{j_k}) \pmod p$$

bài toán được chứng minh. □

Ví dụ 5 (**USAMO 2009**). *Cho n là số nguyên dương. Xác định tập con A lớn nhất của tập $\{-n,-n+1,\ldots,n-1,n\}$ sao cho trong A **không** tồn tại ba phần tử a,b,c (không nhất thiết phân biệt) mà $a+b+c=0$.*

Phân tích và hướng dẫn giải. Nhận xét $0 \notin A$ (vì nếu $0 \in A$ thì $0=0+0+0$, mâu thuẫn với tính chất của tập A). Đặt

$$A^+ = A \cap \{1,2,\ldots,n\}, \quad A^- = A \cap \{-n,-n+1,\ldots,-1\}.$$

- Nhận xét $A^+ + A^-$ và $-A$ là hai tập con **rời nhau** của $\{-n,-n+1,\ldots,n-1,n\}$. Thật vậy, nếu $(A^+ + A^-) \cap (-A) \neq \emptyset$, khi đó tồn tại số c mà

  $$c = i+j = -k \quad (i \in \{1,2,\ldots,n\}\cap A, \quad j \in \{-n,-n+1,\ldots,-1\}\cap A, \quad k \in A) \Rightarrow i+j+k=0,$$

  mâu thuẫn với định nghĩa của tập A.

- Vì $A^+ + A^-$ và $-A$ là hai tập con rời nhau của tập $\{-n,-n+1,\ldots,n-1,n\}$ (tập này có $2n+1$ phần tử) nên

  $$|A^+ + A^-| + \underbrace{|-A|}_{=|A|} \leqslant 2n+1 \Rightarrow 2n+1 \geqslant |A^+ + A^-| + |A|.$$

  Ngoài ra theo định lý 1.2 thì

  $$|A^+ + A^-| \geqslant |A^+| + |A^-| - 1.$$

  Do đó

  $$2n+1 \geqslant \underbrace{|A^+|+|A^-|}_{=|A|} - 1 + |A| = 2|A| - 1 \Rightarrow |A| \leqslant n+1.$$

Đến đây dự đoán tập A lớn nhất có $n+1$ phần tử. Việc tiếp theo cần chỉ ra một tập A có $n+1$ phần tử. Để thỏa mãn bài toán, ta chỉ cần lấy tập A các phần tử lớn nhất và nhỏ nhất của tập đề bài. Đó là tập

$$A = \left\{ \underbrace{-n,-n+1,\ldots,-\left[\frac{n}{2}\right]-1}_{\text{phần âm}}, \underbrace{\left[\frac{n}{2}\right]+1,\ldots,n}_{\text{phần dương}} \right\}.$$

Lấy ba phần tử a, b, c tùy ý của tập A này. Nếu cả ba phần tử cùng thuộc phần âm, hoặc phần dương của tập A thì hiển nhiên $a+b+c \neq 0$. Nếu hai số thuộc phần dương, giả sử a, b, và một số c thuộc phần âm, khi đó $c \geqslant -n$ và

$$a+b \geqslant \left[\frac{n}{2}\right]+1+\left[\frac{n}{2}\right]+1 = 2\left(\left[\frac{n}{2}+1\right]\right) > 2\cdot\frac{n}{2} = n \geqslant c \Rightarrow a+b+c > 0.$$

Tương tự kiểm tra nếu hai số thuộc phần âm, một số thuộc phần dương thì tập A này thỏa mãn đề bài. ***Trở ngại duy nhất còn lại là tập A này có $n+1$ phần tử chỉ khi n lẻ. Còn nếu n chẵn, thì tập A này chỉ có n phần tử, không đạt được tới $n+1$ phần tử.*** *Tuy nhiên ta sẽ chỉ ra nếu n chẵn thì tập A không thể có $n+1$ phần tử được như dưới đây.* Thật vậy, giả sử $|A| = n+1$ vẫn đúng với n chẵn. Do $A^- \subset \{-n, \ldots, -1\}$ và $A^+ \subset \{1, 2, \ldots, n\}$ nên

$$A^+ + A^- \subseteq \{-n+1, -n+2, \ldots, n-2, n-1\}.$$

Lại vì $A^+ + A^-$ và $-A$ là hai tập hợp **rời nhau** của tập $2n+1$ phần tử $\{-n, -n+1, \ldots, n-1, n\}$ nên $2n+1 = |A^+ + A^-| + |-A|$ chỉ có thể xảy ra khi $-n, n \in -A$, tức là $-n, n \in A$. Vì $-n \in A$, theo cấu trúc tập A và định nghĩa tập A^+, thì trong mỗi cặp phần tử sau đây (n chẵn)

$$\{1, n-1\}, \quad \{2, n-2\}, \quad \ldots \quad , \left\{\frac{n}{2}-1, \frac{n}{2}+1\right\}, \quad \left\{\frac{n}{2}\right\}$$

chỉ có **nhiều nhất một phần tử trong mỗi cặp** thuộc vào A^+. Dẫn đến $|A|^+ \leqslant \dfrac{n}{2}$, tương tự $|A^-| \leqslant \dfrac{n}{2}$. Do đó

$$|A| = |A^+| + |A^-| \leqslant \frac{n}{2} + \frac{n}{2} = n$$

mâu thuẫn với $|A| = n+1$. Vậy bài toán được chứng minh hoàn toàn. □

Ví dụ 6 (**Việt Nam TST 2012**). *Cho số nguyên tố $p \geqslant 17$. Chứng minh rằng $t = 3$ là số nguyên dương lớn nhất thỏa mãn điều kiện: Với các số nguyên bất kỳ a, b, c, d sao cho số abc không chia hết cho p và $a+b+c$ chia hết cho p thì tồn tại các số nguyên x, y, z thuộc tập $\left\{0, 1, 2, \ldots \left[\dfrac{p}{t}\right]-1\right\}$ sao cho $ax+by+cz+d \vdots p$.*

Lời giải. **Nhận xét** Nếu $\{u_1, \ldots, u_k\}$ chứa một hệ thặng dư đầy đủ modulo p thì tập $d + \{u_1, \ldots, u_k\}$ cũng chứa một hệ thặng dư đầy đủ modulo p.
Đặt $k = \left[\dfrac{p}{t}\right]-1$, và $A = \{0, 1, 2, \ldots, k\}$. Đặt

$$S = \{ax+by+cz | 0 \leqslant x, y, z \leqslant k\} = aA + bA + cA \pmod{p}.$$

- Với $t = 3$, theo yêu cầu bài toán và nhận xét ở trên thì **bài toán tương đương với việc chứng minh nếu $t = 3$ thì S chứa một hệ thặng dư đầy đủ modulo p, tức cần chứng minh** $|S| = p$. Đặt $C = \{ax+by+cz | -1 \leqslant x, y, z \leqslant 1\}$. Do $a+b+c \equiv 0 \pmod{p}$ nên với mỗi bộ $(x, y, z \in A)$ thì

$$ax+by+cz \equiv a(x-k)+b(y-k)+c(z-k) \pmod{p}.$$

Tức là mỗi bộ $(x, y, z) \in A$ tương ứng với bộ $(x-k, y-k, z-k)$, nên ta **thực hiện đối xứng tập A để sử dụng tập C**, bằng cách đặt $L = \left[\frac{k}{2}\right]$ và xét tập

$$S' = \{ax + by + cz | -L \leqslant x, y, z \leqslant L\}$$

thì

$$|S| \geqslant |S'| \quad \text{(dấu bằng xảy ra khi và chỉ khi } k \text{ chẵn).}$$

- Khi đó tập S' viết được dưới dạng

$$S' = \underbrace{C + C + \cdots + C}_{L \text{ lần}}.$$

Theo định lý 2.6 ta có

$$|S'| \geqslant \min\{p, L.|C| - (L-1)\}. \quad (*)$$

Để có được kết luận bài toán là $|S| = p$, ta cần chỉ ra $|S'| = p$, do đó theo (*) ta sẽ cần chứng minh

$$L|C| - (L-1) \geqslant p \quad (**).$$

- Với chú ý a, b, c không chia hết cho p nên tập $\{0, a, b, c, -a, -b, -c, a-b, b-c, c-a\}$ gồm 10 phần tử đôi một phân biệt theo modulo p nằm trong tập C. Do đó $|C| \geqslant 10$. Vậy để có (**) ta sẽ chứng minh

$$10L - (L-1) \geqslant 0 \Leftrightarrow 9L + 1 \geqslant p. \quad (***)$$

Vì p nguyên tố, nên xét hai trường hợp

  - p dạng $p = 6a + 1$. Do $p \geqslant 17$ nên $a \geqslant 3$. Khi đó $k = \left[\frac{p}{3}\right] - 1 = 2a - 1$, nên $L = \left[\frac{k}{2}\right] = \left[a - \frac{1}{2}\right] = a - 1$. Do đó (***) tương đương

$$9(a-1) + 1 \geqslant 6a + 1 \Rightarrow a \geqslant 3 \quad \text{(đúng).}$$

  - p dạng $p = 6a + 5$. Do $p \geqslant 17$ nên $a \geqslant 2$. Khi đó $k = \left[\frac{p}{3}\right] - 1 = 2a$, nên $L = \left[\frac{k}{2}\right] = a$. Do đó (***) tương đương

$$9(a) + 1 \geqslant 6a + 5 \Leftrightarrow a \geqslant \frac{4}{3} \Rightarrow a \geqslant 2 \quad \text{(đúng, do } a \text{ nguyên).}$$

Vậy trong mọi trường hợp của p thì (***) đều đúng. Vậy bài toán được chứng minh trong trường hợp $t = 3$.

- Ta chứng minh $t = 4$ không thỏa mãn. Thật vậy, chọn $a = b = 1, c = -2$ và $d = \frac{p-1}{2}$. Khi đó với $x, y, z \in A = \left\{0, 1, 2, \ldots, \left[\frac{p}{4}\right] - 1\right\}$ thì

$$\underbrace{-2\left(\left[\frac{p}{4}\right] - 1\right) + \frac{p-1}{2}}_{x=y=0, z=\left[\frac{p}{4}\right]-1} \leqslant x + y - 2z + \frac{p-1}{2} \leqslant \underbrace{2\left(\left[\frac{p}{4}\right] - 1\right) + \frac{p-1}{2}}_{x=y=\left[\frac{p}{4}\right]-1, z=0}$$

hay

$$\frac{3}{2} \leqslant x + y - 2z + \frac{p-1}{2} \leqslant p - \frac{5}{2}.$$

Trong khoảng giá trị $\left(\frac{3}{2}, p - \frac{5}{2}\right)$ không có số nào chia hết cho p, tức không tồn tại x, y, z thỏa mãn.

Bài toán được chứng minh. □

Ví dụ 7 (**IMO Shortlist 2007**). *Cho X là tập hợp gồm 10000 số nguyên, không có số nào trong chúng chia hết cho 47. Chứng minh rằng tồn tại một tập con Y của X gồm 2007 phần tử sao cho $a - b + c - d + e \not\vdots 47, \forall a, b, c, d, e \in Y$.*

Phân tích và hướng dẫn giải.

- Một tập M gồm các số nguyên được gọi là **tốt** nếu $47 \not| \ a - b + c - d + e, \forall a, b, c, e, d \in M$.

- Nhận thấy tập $J = \{-9, -7, -5, -3, -1, 1, 3, 5, 7, 9\}$ là một tập tốt. Thật vậy, với mọi phần tử $a, b, c, d, e \in J$ thì số $a - b + c - d + e$ là số lẻ và

  $$-45 = (-9) - 9 + (-9) - 9 + (-9) \leqslant a - b + c - d + e \leqslant 9 - (-9) + 9 - (-9) + 9 = 45$$

  nhưng không có **số nguyên lẻ nào chia hết cho 47 nằm trong tập** $\{-45, -43, \ldots, 43, 45\}$.

- Với mỗi $k = 1, 2, \ldots, 46$, thì các tập hợp $A_k = \{x \in X | \exists j \in J : kx \equiv j \pmod{47}\}$ đều là tập tốt. Thật vậy, giả sử tồn tại một tập A_k không tốt ($k \in \{1, 2, \ldots, 46\}$). Khi đó tồn tại 5 phần tử $x_1, x_2, x_3, x_4, x_5 \in A_k$ sao cho

  $$x_1 - x_2 + x_3 - x_4 + x_5 \equiv 0 \pmod{47} \Rightarrow k(x_1 - x_2 + x_3 - x_4 + x_5) \equiv 0 \pmod{47}.$$

  Dẫn đến $kx_1 - kx_2 + kx_3 - kx_4 + kx_5 \equiv 0 \pmod{47}$. Theo định nghĩa của $x_1, \ldots, x_5$, thì tồn tại $j_1, \ldots, j_5 \in J$ sao cho

  $$j_1 - j_2 + j_3 - j_4 + j_5 \equiv kx_1 - kx_2 + kx_3 - kx_4 + kx_5 \equiv 0 \pmod{47}$$

  chứng tỏ J là tập không tốt, mâu thuẫn.

- Mỗi phần tử $x \in X$ thuộc **đúng 10 tập** A_k. Thật vậy, vì 47 là số nguyên tố, tập $\{1, 2, \ldots, 46\}$ lập thành một hệ thặng dư thu gọn modulo 47, do $x \in X$ nên $(x, 47) = 1$, do đó $\{x, 2x, \ldots, 46x\}$ cũng lập thành một hệ thặng dư thu gọn modulo 47. Do đó với $j \in J$ (gồm có 10 giá trị j) thì tương ứng sẽ tồn tại 10 chỉ số $k \in \{1, 2, \ldots, 46\}$ (các j khác nhau thì k cũng khác nhau) để $kx \equiv j \pmod{47}$. Do đó x sẽ thuộc vào đúng 10 tập $A_k (k \in \{1, 2, \ldots, 47\})$.

- Do đó

  $$\sum_{k=1}^{4} 6|A_k| = 10|X| = 100000.$$

  Theo nguyên lý trung bình, tồn tại một chỉ số k sao cho

  $$|A_k| \geqslant \frac{100000}{46} > 2173 > 2007,$$

tức tập A_k này chính là tập cần tìm.

Ta có điều phải chứng minh. □

Trong lời giải trên, ta không thấy sử dụng định lý Cauchy - Davenport. Hãy nhìn kỹ lời giải trên, thì bước đầu tiên chỉ ra tập J là quan trọng nhất. Tập J là tập tốt có đúng 10 phần tử. ***Thực sự thì tập chứa các số dư khác nhau khi chia cho 47 mà là tập tốt thì chỉ chứa tối đa 10 phần tử****. Thật vậy, nếu $|J| \geqslant 11$, thì theo định lý 2.6 thì, do $5|J| - 4 \geqslant 5 \times 11 - 4 = 51 > 47$*

$$|J + J + J + (-J) + (-J)| \geqslant \min\{5|J| - 4, 47\} = 47$$

do đó sẽ tồn tại $a, b, c, d, e \in J$ sao cho $a - b + c - d + e \vdots 47$, suy ra tập J không tốt. Vậy $|J| \leqslant 10$. Để $|J| = 10$ thì theo định lý 2.7, J phải là một cấp số cộng.

Ví dụ 8 (**Định lý Erdos - Ginzburg - Ziv**). *Cho $n \geqslant 1$ và $a_0, a_2, \ldots, a_{2n-2}$ là một dãy gồm $2n-1$ số nguyên (không nhất thiết phân biệt). Chứng minh rằng tồn tại một dãy con gồm n số $a_{i_1}, \ldots, a_{i_n}$ sao cho*

$$a_{i_1} + a_{i_2} + \cdots + a_{i_n} \equiv 0 \pmod{n}.$$

Phân tích và hướng dẫn giải. • Trước tiên ta chứng minh kết luận bài toán trong trường hợp $n = p$ là **số nguyên tố**. Gọi $a_i' \in \mathbb{Z}, 0 \leqslant a_i' < p$ sao cho $a_i \equiv a_i' \pmod{p}$ (*thực hiện lấy modulo các phần tử của dãy*). Ta có thể đánh lại chỉ số cho các số a_i để

$$0 \leqslant a_0' \leqslant a_1' \leqslant \ldots \leqslant a_{2p-2}' \leqslant p - 1.$$

– Nếu $a_i' \equiv a_{i+p-1}'$ với một chỉ số $i \in [1, p-1]$ thì theo thứ tự trên xảy ra

$$a_i' \equiv a_{i+1}' \equiv \cdots \equiv a_{i+p-1}' \pmod{p}$$

dẫn đến

$$a_i + a_{i+1} + \cdots + a_{i+p-1} \equiv pa_i \equiv 0 \pmod{p}.$$

– Nếu $a_i' \equiv a_{i+p-1}'$ với mọi $i \in [1, p-1]$. Khi đó đặt $\boxed{A_i = \{a_i', a_{i+p-1}'\}}$ thì $|A_i| = 2, \forall i = 1, 2, \ldots, p-1$. Áp dụng định lý 2.6 ta có

$$|A_1 + A_2 + \cdots + A_{p-1}| \geqslant \min\{p, |A_1| + \cdots + |A_{p-1}| - (p-2)\} = \min\{p, 2(p-1) - (p-2)\} = p.$$

Từ đây suy ra

$$A_1 + A_2 + \cdots + A_{p-1} = \mathbb{Z}_p.$$

Từ đó tồn tại một lớp các đồng dư $a_{j_i}' \in A_i, i = 1, 2, \ldots, p-1$, với $j_i \in \{i, i+p-1\}$ sao cho

$$-a_0 \equiv a_{j_1}' + a_{j_2}' + \cdots + a_{j_{p-1}}' \pmod{p}.$$

Suy ra

$$a_{j_1} + a_{j_2} + \cdots + a_{j_{p-1}} + a_0 \equiv 0 \pmod{p}.$$

Vậy bài toán đúng trong trường hợp n nguyên tố.

- Ta chứng minh kết luận bài toán trong trường hợp tổng quát bằng phương pháp quy nạp. Nếu $n = 1$, bài toán hiển nhiên đúng. Giả sử với $n > 1$ và *kết luận bài toán đúng cho mọi số nguyên dương nhỏ hơn n*. Ta sẽ chứng minh bài toán đúng với n. Nếu n nguyên tố, bài toán đúng theo ý trên. Nếu n hợp số, đặt

$$n = uv \quad (1 < u \leqslant v < n).$$

Khi đó theo giả thiết quy nạp, bài toán đúng cho u và v.

  - Từ dãy số $a_0, \ldots, a_{2n-2}$ có độ dài $2n - 1 = 2uv - 1$, theo giả thiết quy nạp, luôn tồn tại một dãy con $a_{1,i_1}, \ldots, a_{1,i_v}$ sao cho

$$a_{1,i_1} + \cdots + a_{1,i_v} \equiv 0 \pmod{v}.$$

  - Khi đó còn lại $2n - 1 - v = (2u - 1)v - 1$ số nguyên **nằm trong dãy ban đầu, nhưng không thuộc vào dãy con ở trên**. Do $2u - 1 \geqslant 2$, lại áp dụng giả thiết quy nạp, từ dãy độ dài $(2u - 1)v - 1 \geqslant 2v - 1$ số nguyên, luôn tồn tại một dãy con $a_{2,i_1}, \ldots, a_{2,i_v}$ sao cho

$$a_{2,i_1} + \cdots + a_{2,i_v} \equiv 0 \pmod{v}.$$

  - Khi đó còn lại $2n - 1 - 2v = (2u - 2)v - 1$ số nguyên trong dãy và không thuộc vào hai dãy con ở trên. Cứ tiếp tục quá trình trên, với $j = 1, 2, \ldots, 2u - 1$, ta nhận được $2u - 1$ **các dãy con đôi một rời nhau** $a_{j,i_1}, \ldots, a_{j,i_v}$ độ dài v sao cho

$$a_{j,i_1} + \cdots + a_{j2,i_v} \equiv 0 \pmod{v}.$$

    Khi đó

$$a_{j,i_1} + \cdots + a_{j2,i_v} = b_j v (b_j \in \mathbb{Z}), \quad \forall j = 1, 2, \ldots, 2u - 1.$$

  - Do giả thiết đúng cho u, nên từ một dãy $b_1, b_2, \ldots, b_{2u-1}$ độ dài $2u - 1$ sẽ có một dãy con $b_{j_1}, \ldots, b_{j_u}$ sao cho

$$b_{j_1} + b_{j_2} + \cdots + b_{j_u} \equiv 0 \pmod{u},$$

    tức là

$$b_{j_1} + b_{j_2} + \cdots + b_{j_u} = cu \ (c \in \mathbb{Z}).$$

Khi đó

$$\sum_{r=1}^{u} \sum_{s=1}^{v} a_{j_r,i_s} = \sum_{r=1}^{u} b_{j_r} v = cuv = cn \equiv 0 \pmod{n}.$$

Định lý được chứng minh hoàn toàn. □

Ví dụ 9 (**China TST 2016**). *Cho m, n là các số nguyên dương thỏa mãn $n \geqslant m \geqslant 1$ và S là một tập hợp gồm có n số tự nhiên. Chứng minh rằng S chứa ít nhất 2^{n-m+1} tập con phân biệt, mà mỗi tập đó có tổng các phần tử chia hết cho m (tập rỗng xem như là tập con thỏa mãn).*

Trước khi chứng minh, ta cần sử dụng một số kết quả quen thuộc cho bởi các nhận xét sau:

Nhận xét 1: Trong n số nguyên tùy ý, luôn tồn tại một số hoặc một vài số mà tổng của chúng chia hết cho n. Đây là một tính chất quen thuộc chứng minh bằng Dirichlet.

Nhận xét 2: Cho p là số nguyên tố và $Q = \{a_1, a_2, \ldots, a_{p-1}\}$ là tập hợp chứa các số nguyên không chia hết cho p. Khi đó tập

$$R = \{S(A) = \sum_{x \in A} x | A \subset Q\}$$

chứa một hệ thặng dư đầy đủ modulo p. Ở đây $S(\emptyset) = 0$.

Chứng minh. Ta có thể lấy các phần tử của Q theo modulo p mà không làm thay đổi bài toán. Xét các tập

$$A_1 = \{0, a_1\}, \quad A_2 = \{0, a_2\}, \ldots, A_{p-1} = \{0, a_{p-1}\}$$

thì do $a_i \not\vdots p, \forall i = 1, 2, \ldots, p-1$ nên $|A_i| = 2, i = 1, 2, \ldots, p-1$. Theo định lý 2.6 thì

$$|A_1 + A_2 + \cdots + A_{p-1}| \geqslant \min\{p, |A_1| + \cdots + |A_{p-1}| - (p-2)\} = \min\{p, 2(p-1) - (p-2)\} = p.$$

Chứng tỏ $A_1 + \cdots + A_{p-1} = \mathbb{Z}_p$. Mặt khác, các phần tử trong $A_1 + A_2 + \cdots + A_{p-1}$ là các phần tử trong R (phần tử $0 + 0 + \cdots + 0$ trong $A_1 + \cdots + A_{p-1}$ ứng với việc chọn tập $A = \emptyset \subset Q$).

Lời giải. *Ý tưởng của bài toán là ta sẽ chia tập S thành hai tập A, B. Mỗi tập con A' trong A đều tìm được một tập con B' trong B mà tổng các số của hai tập con này chia hết cho m. Đồng nghĩa với việc $S(A') \equiv -S(B') \pmod m$.*

- Trước tiên ta chứng minh nếu $m = p$ nguyên tố, bài toán hiển nhiên đúng. Thật vậy:
  - Nếu trong S có ít nhất $p-1$ số nguyên không chia hết cho m. Gọi $Q = \{a_1, a_2, \ldots, a_{p-1}\}$ là tập chứa $p-1$ số nguyên không chia hết cho p. Khi đó

    $$S = Q \cup (S \setminus Q).$$

    Tập $S \setminus Q$ có $n - (p-1) = n - p + 1$ phần tử nên có 2^{n-p+1} tập con. Mỗi tập con $A \subset (S \setminus Q)$, do nhận xét 2, tồn tại một tập con $B \subset Q$ sao cho

    $$S(A) \equiv -S(B) \pmod p \Rightarrow S(A) + S(B) \equiv 0 \pmod p \Rightarrow S(A \cup B) \equiv 0 \pmod p.$$

    Vậy cứ một tập con $A \subset (S \setminus Q)$, luôn tìm được một tập dạng $A \cup B \subset S$ để $S(A \cup B) \vdots p$. Mà có 2^{n-p+1} tập A nên tương ứng có 2^{n-p+1} tập con trong S thỏa mãn đề bài.
  - Nếu trong S có $< p-1$ số nguyên không chia hết cho m. Dẫn đến trong S có $\geqslant n - p + 1$ số chia hết cho m. Trong trường hợp này hiển nhiên mọi tập con của tập chứa $n - p + 1$ số này đều chia hết cho p, tức là cũng có ít nhất 2^{n-p+1} tập thỏa mãn bài toán.

- Trong trường hợp m tùy ý. Ta chứng minh khẳng định bài toán bằng quy nạp. Với $m = 1$ bài toán hiển nhiên đúng. Giả sử bài toán đúng cho mọi giá trị nguyên dương $< m$. Xét với số nguyên dương m. Đặt $m = p.k$, với p nguyên tố và $k \geqslant 1$. Một tập $A \subset S$ được gọi là tập "gần tốt tối thiểu" nếu $S(A) \vdots k$ nhưng $S(A) \not\vdots m$ và $|A|$ nhỏ nhất. Khi đó theo nhận xét 1 thì một tập A là *gần tốt tối thiểu* thì $|A| \leqslant k$.

  - Nếu trong tập S **chỉ có tối đa** $t < p-1$ tập gần tốt tối thiểu. Gọi các tập này là $S_1, \ldots, S_t$. Khi đó xét phân hoạch của S

    $$S = S_1 \cup S_2 \cup \cdots \cup S_t \cup N \quad (N = S \backslash (S_1 \cup S_2 \cup \cdots \cup S_t)).$$

    Vì mỗi tập $|S_i|$ chỉ có tối đa k phần tử. Nên tập N có

    $$|N| \geqslant n - tp > n - (p-1)k = n - m + k \geqslant k.$$

    Áp dụng giả thiết quy nạp, thì tập N chứa

    $$2^{|N|-k+1} \geqslant 2^{n-m+1}$$

    tập con phân biệt chia hết cho k. Tuy nhiên vì có tốt đa t tập *gần tốt tối thiểu*, do đó 2^{n-m+1} tập con này mặc dù chia hết cho k, không không thể là tập *gần tốt tối thiểu*, tức mỗi tập con này có tổng chia chết cho m. Kết luận bài toán được chứng minh trong trường hợp này.
  - Nếu trong tập S có $\geqslant p-1$ tập *gần tốt tối thiểu*. Chọn ra $p-1$ tập *gần tốt tối thiểu* phân biệt, ký hiệu là $B_1, \ldots, B_{p-1}$. Khi đó xét phân hoạch của S

    $$S = B_1 \cup B_2 \cup \cdots \cup B_{p-1} \cup M \quad (M = S \backslash (S_1 \cup S_2 \cup \cdots \cup S_t)).$$

    Vì mỗi tập $|S_i|$ chỉ có tối đa k phần tử. Nên tập M có

    $$|M| \geqslant n - (p-1)k = n - m + k \geqslant k.$$

    Áp dụng giả thiết quy nạp, thì tập M chứa

    $$2^{|M|-k+1} \geqslant 2^{n-m+1}$$

    tập con phân biệt chia hết cho k. Do định nghĩa của $B_1, \ldots, B_{p-1}$, đặt

    $$S(B_1) = r_1 k, \quad S(B_2) = r_2, \quad \ldots, \quad S(B_{p-1}) = r_{p-1}.k \quad (r_i \in \mathbb{Z}^+, i = 1, 2, \ldots, p-1)$$

    và các $r_i \not\vdots p, \forall i = 1, 2, \ldots, p-1$. Đặt $Q = \{r_1, \ldots, t_{p-1}\}$, theo nhận xét 2, tập

    $$R = \{S(A) | A \subset Q\}$$

    chứa một hệ thặng dư đầy đủ modulo p. Do đó tập $S(B_1 + B_2 + \cdots + B_{p-1})$ sẽ chứa hệ thặng dư $\{k, 2k, \ldots, pk\} \pmod m$. Do đó lấy bất kỳ một tập con $A \subset M$ (khi đó $S(A) \vdots k$), luôn tồn tại một tập con $B \subset B_1 + \cdots + B_{p-1}$ sao cho

    $$S(B) \equiv -S(A) \pmod m \Rightarrow S(A \cup B) \equiv 0 \pmod m,$$

    tức tập $A \cup B$ thỏa mãn. Vì có $\geqslant 2^{n-m+1}$ tập $A \subset M$ mà $S(A) \vdots k$, nên có $\geqslant 2^{n-m+1}$ tập thỏa mãn yêu cầu bài toán.

Tổng hợp các kết quả trên, bài toán được chứng minh hoàn toàn. □

Lời giải cho trường hợp $m = p$ là một trường hợp riêng cho lời giải m tổng quát. Tuy nhiên tác giả vẫn trình bày ở đây, để cho thấy cách làm với m tổng quát, dựa vào cách làm với $m = p$ nguyên tố.

4. Bài tập tự luyện

Bài tập 1 (**Bosnia and herzegovina TST 2012**). Chứng minh rằng với mọi số nguyên tố p lẻ, luôn tồn tại số nguyên dương $m < p$ và các số nguyên x_1, x_2, x_3 sao cho

$$x_1^2 + x_2^2 + x_3^2 = mp.$$

Bài tập 2. Cho k, n là các số nguyên dương và p là số nguyên tố. Chứng minh rằng tồn tại các số nguyên $a_1, \ldots, a_k$ sao cho

$$a_1^k + a_2^k + \cdots + a_k^k \equiv n \pmod{p}.$$

Bài tập 3 (**Belarus MO**). Cho số nguyên tố p và gọi $x, y, z \in \{0, 1, 2, \ldots, p-1\}$ thỏa mãn $x^2 + y^2 + z^2 \vdots p$. Gọi $S(p)$ là số bộ ba (x, y, z) thỏa mãn điều kiện trên. Chứng minh rằng $S(p) \geqslant 2p - 1$.

Bài tập 4 (**Ukrainian TST 2007**). Tìm tất cả các số nguyên tố p, sao cho tồn tại số nguyên n, để phương trình sau vô nghiệm nguyên $x^3 + y^3 \equiv n \pmod{p}$.

Bài tập 5 (**Tuymaada 2008**). Cho 250 số nguyên dương không vượt quá 501. Chứng minh rằng với mọi số nguyên dương t, tồn tại bốn số nguyên a_1, a_2, a_3, a_4 trong 250 số đã cho mà $a_1 + a_2 + a_3 + a_4 - t \vdots 23$.

Bài tập 6. Cho $p > 3$ là số nguyên tố. Tập $\{1, 2, \ldots, p-1\}$ được phân hoạch thành 3 tập con rời nhau A, B, C. Chứng minh rằng tồn tại x, y, z lần lượt thuộc ba tập A, B, C sao cho $x + y - z \vdots p$.

Bài tập 7 (**APMO 2014**). Tìm tất cả các số nguyên dương n sao cho với mọi số nguyên k, tồn tại số nguyên a sao cho $a^3 + a - k \vdots n$.

Bài tập 8 (**Crux 2013, Vol 39, CC9**). Cho $k \geqslant 3$ là số nguyên. Đặt $n = \dfrac{k(k+1)}{2}$ và S là tập con của $\mathbb{Z}_n$. Chứng minh rằng $S + S \neq \mathbb{Z}_n$.

Bài tập 9 (**IMO 2003 (general)**). Cho n là số nguyên dương $\geqslant 2$. Cho A là một tập con chứa $n+1$ phần tử của tập $S = \{1, 2, \ldots, n^3\}$. Chứng minh rằng tồn tại n phần tử $t_1, t_2, \ldots, t_n$ trong S sao cho các tập

$$A_j = \{x + t_j | x \in A\}, \forall j = 1, 2, \ldots, n$$

đôi một rời nhau.

Bài tập 10 (**USA TSTST 2013**). Cho p là số nguyên tố. Cho graph G đầy đủ $1000p$ đỉnh. Trên mỗi cạnh của graph ta gán một số nguyên. Chứng minh rằng trong G tồn tại một chu trình mà tổng các số được đánh trên các cạnh nằm trong chu trình đó chia hết cho p.

Bài tập 11 (**Tomanian TST 2010**). Cho X, Y là các tập con hữu hạn của nửa khoảng $[0, 1)$ sao cho $0 \in X \cap Y$ và không tồn tại $x \in X, y \in Y$ sao cho $x + y = 1$. Chứng minh rằng tập $\{x + y - [x + y] : x \in X, y \in Y\}$ có ít nhất $|X| + |Y| - 1$ phần tử.

Tài liệu

[1] A.Frimu and M.Teleuca, *Applications of combinatorial Nullstellensatz*, Gazeta Mathematica 2011

[2] O.J.Rodseth, *Sumsets mod p*, lecture notes.

[3] M.B.Nathanson, *Additive number theory - Inverse baitapblems and the Geometry of Sumset*, Springer, 1996.

[4] H.Lee, *Combinatorial Number Theory*, lecture notes.

[5] Website: http://artofproblemsolving.com.

SỬ DỤNG MODULO TRONG PHƯƠNG TRÌNH NGHIỆM NGUYÊN VÀ BÀI TOÁN CHIA HẾT

Lê Anh Dũng
(Trường THPT chuyên Huỳnh Mẫn Đạt - Kiên Giang)

Lựa chọn modulo là một trong các kĩ năng hay dùng trong việc giải phương trình nghiệm nguyên và bài toán chia hết. Chọn modulo nào, cơ sở nào để chọn modulo? Bài viết cung cấp một số cơ sở lý thuyết và các kĩ năng nhỏ trong việc suy luận tìm modulo.

1. Các kiến thức cơ sở sử dụng

1.1. Hàm CARMICHAEL

Theo định lý Euler thì $a^{\varphi(n)} \equiv 1 \pmod{n}$ với mọi số nguyên dương a nguyên tố cùng nhau với n. Tuy nhiên, $\varphi(n)$ không phải là số nguyên dương nhỏ nhất nhỏ nhất thỏa $a^t \equiv 1 \pmod{n}$.

Định nghĩa 1. *Cho số nguyên dương n ($n \geqslant 2$). $\lambda(n)$ là số nguyên dương nhỏ nhất thỏa mãn $a^{\lambda(n)} \equiv 1 \pmod{n}$ với mọi số nguyên dương a mà $(a,n) = 1$. Hàm $\lambda(n)$ gọi là hàm Carmichael theo n.*

Định lý 1. ***(Tính chất của hàm Carmichael)***

i) Với mọi số nguyên dương a, b, ta có $\lambda(a.b) = [\lambda(a), \lambda(b)]$.

ii) $\lambda(2) = 1; \lambda(4) = 2; \lambda(2^k) = 2^{k-2}$ với mọi $k \geqslant 3$.
$\lambda(p^k) = p^{k-1}(p-1)$ với mọi số nguyên tố p, $p \geqslant 3$.
Nếu $n = p_1^{s_1}.p_2^{s_2}...p_m^{s_m}$ thì $\lambda(n) = \left[\lambda(p_1^{s_1}), \lambda(p_2^{s_2}), ..., \lambda(p_m^{s_m})\right]$

Nhận xét. Trong giải toán ta thường dùng các nhận xét sau:

- Nếu $a^2 \equiv 1 (\text{mod } p^s)$ thì hoặc $a \equiv 1 (\text{mod } p^s)$ hoặc $a \equiv -1 (\text{mod } p^s)$ với p là số nguyên tố lớn hơn 2.
- Nếu $a^2 \equiv 1 (\text{mod } 2p^s)$ thì hoặc $a \equiv 1 (\text{mod } 2p^s)$ hoặc $a \equiv -1 (\text{mod } 2p^s)$ với p là số nguyên tố lớn hơn 2.

Từ nhận xét trên, ta có các modulo hay dùng $p^s, 2p^s, 4p^s$

1.2. Số mũ đúng

Định nghĩa 2. *Cho p là số nguyên tố, a là số tự nhiên. α số mũ đúng của a theo p, kí hiệu là $v_p(a)$ nếu và chỉ nếu $p^\alpha | a$ và $p^{\alpha+1}$ không là ước của a.*

Định lý 2. *Ta có các tính chất sau*

1. $v_p(ab) = v_p(a) + v_p(b)$
2. $v_p(a^n) = nv_p(a)$
3. $v_p(a+b) \geqslant \min\{v_p(a), v_p(b)\}$ *đẳng thức xảy ra khi* $v_p(a) \neq v_p(b)$.
4. *Với số nguyên dương n, số nguyên tố p thì*
   - *Nếu $p \neq 2$ và $p|(x-y)$ thì*
   $$v_p(x^n - y^n) = v_p(x-y) + v_p(n).$$
   - *Nếu $p = 2$ và $4|(x-y)$ thì*
   $$v_2(x^n - y^n) = v_2(x-y) + v_2(n).$$
   - *Nếu $p = 2$ và $2|(x-y)$, n là số chẵn thì*
   $$v_2(x^n - y^n) = v_2(x^2 - y^2) + v_2(n) - 1.$$
   - *Nếu $p|(x+y)$ và n là số nguyên dương lẻ thì*
   $$v_p(x^n + y^n) = v_p(x+y) + v_p(n).$$

1.3. Cấp của phần tử

Định nghĩa 3. *Cho số nguyên dương $n > 1$ và số nguyên a nguyên tố cùng nhau với n, số k được gọi là cấp của a modulo n (kí hiệu là $ord_n a$) nếu k là số nguyên dương nhỏ nhất để $a^k \equiv 1 (\mathrm{mod} n)$.*

Định lý 3. *Ta có các tính chất sau*

i) $ord_n a | \lambda(n)$

ii) Nếu $a^h \equiv 1 (\mathrm{mod} n)$ *thì* $ord_n a | h$

iii) $a^x \equiv a^y (\mathrm{mod}\ n) \Leftrightarrow ord_n a | (x-y)$ *hay* $x = t.ord_n a + y$ *với* $(a,n) = 1$.

iv) $ord_n a^s = \frac{ord_n a}{(ord_n a, s)}$

v) Nếu $x \equiv 3 (\mathrm{mod}\ 8)$ *hoặc* $x \equiv 5 (\mathrm{mod}\ 8)$ *thì* $ord_{2^k} x = 2^{k-2}$ *với mọi* $k \geqslant 3$.

vi) Cho k là số nguyên dương, và p là một số nguyên tố lẻ. Xét tập $S = \{a^k | a \neq 0\} \subset \mathbb{Z}_p$. *Khi đó* $|S| = \frac{p-1}{(k,p-1)}$.

vii) Cho p là số nguyên tố và $d|(p-1)$. Khi đó phương trình $x^d \equiv 1 (\mathrm{mod}\ p)$ *có đúng $\varphi(d)$ nghiệm trong* $\mathbb{Z}_p$.

1.4. Thặng dư bình phương

Định nghĩa 4. *Giả sử m là số nguyên dương và a là số nguyên thỏa $(a,\ m) = 1$. Nếu phương trình đồng dư $x^2 \equiv a \pmod m$ có nghiệm thì ta nói a là thặng dư bình phương của m. Ngược lại, ta nói a là không thặng dư bình phương của m.*

Nếu p là số nguyên tố lẻ thì trong dãy $1,\ 2,\ ...,\ p-1$ có đúng $\dfrac{p-1}{2}$ thặng dư bình phương.
Ta thường sử dụng kí hiệu Legendre như sau:
Cho p là số nguyên tố lẻ và số nguyên a không chia hết cho p. Ta kí hiệu

$$\left[\frac{a}{b}\right] = \begin{cases} 1 & \text{nếu } a \text{ là thặng dư bình phương} \\ -1 & \text{nếu ngược lại} \end{cases}.$$

Định lý 4. *Ta có các tính chất sau*

i) ***(Tiêu chuẩn Euler)*** *Giả sử p là số nguyên tố lẻ và không là ước của số nguyên a. Khi đó:*

$$\left[\frac{a}{p}\right] \equiv a^{\frac{p-1}{2}} \pmod p.$$

ii) Nếu p là số nguyên tố lẻ và a và b không chia hết cho p thì

+) $a \equiv b \,(\mathrm{mod}\, p) \Rightarrow \left[\dfrac{a}{p}\right] = \left[\dfrac{b}{p}\right]$

+) $\left[\dfrac{ab}{p}\right] = \left[\dfrac{a}{p}\right]\left[\dfrac{b}{p}\right]$

+) $\left[\dfrac{a^2}{p}\right] = 1$

+) *Nếu p là số nguyên tố lẻ thì* $\left[\dfrac{-1}{p}\right] = \begin{cases} 1 & khi\ \ p \equiv 1 \pmod 4 \\ -1 & khi\ p \equiv -1 \pmod 4 \end{cases}$

+) *Nếu p là số nguyên tố lẻ thì* $\left[\dfrac{2}{p}\right] = (-1)^{\frac{p^2-1}{8}}$

+) $\left[\dfrac{2}{p}\right] = 1$, *nếu* $p \equiv \pm 1 (\mathrm{mod} 8)$; $\left[\dfrac{2}{p}\right] = -1$, *nếu* $p \equiv \pm 3 (\mathrm{mod} 8)$

iii) ***(Luật thuận nghịch bình phương)*** *Nếu p, q là các số nguyên tố lẻ khác nhau thì*

$$\left[\frac{p}{q}\right].\left[\frac{q}{p}\right] = (-1)^{\frac{p-1}{2}.\frac{q-1}{2}}.$$

Do đó, $\left[\dfrac{p}{q}\right] = \left[\dfrac{q}{p}\right]$, *nếu* $p \equiv 1 \vee q \equiv 1 (\mathrm{mod} 4)$ *và* $\left[\dfrac{p}{q}\right] = \left[\dfrac{q}{p}\right]$, *nếu* $p \equiv q \equiv 3 (\mathrm{mod} 4)$.

2. Một số bài toán áp dụng

Bài toán 1. ***(IMO Shortlist 2002)*** *Tìm số nguyên dương t nhỏ nhất sao cho tồn tại các số nguyên $x_1, x_2, ..., x_t$ thỏa*

$$x_1^3 + x_2^3 + ... + x_t^3 = 2002^{2002}.$$

Phân tích và lời giải. Ta thấy

$$3 = \frac{1}{2}.6 = \frac{1}{2}\lambda(7) = \frac{1}{2}\lambda(9) = \frac{1}{2}\lambda(14) = \frac{1}{2}\lambda(18),$$

đó là các modulo đầu tiên ta xét tới.
Theo nhận xét trên, trước hết ta khảo sát các modulo 9 của x^3,2002^{2002}.
Nếu $3|x$ thì $x^3 \equiv 0(mod\,9)$.
Nếu $(x,\ 3) = 1$ thì x^3 đồng dư 1 hoặc -1 modulo 9.
Như vậy, $x_1^3 + x_2^3 + ... + x_t^3$ đồng dư từ $-t$ đến t modulo 9.

$$2002^{2002} \equiv 4^{2002} \equiv 4^{6.333}.4^4 \equiv 4^4 \equiv 4 \pmod 9.$$

Như vậy, nếu $t \leqslant 3$ thì $x_1^3 + x_2^3 + ... + x_t^3$ không đồng dư 4 modulo 9 nên đẳng thức sau

$$x_1^3 + x_2^3 + ... + x_t^3 = 2002^{2002}$$

không xảy ra.
Với $t = 4$, ta thử tìm 1 nghiệm của phương trình

$$x_1^3 + x_2^3 + x_3^3 + x_4^3 = 2002^{2002}.$$

Để ý $2002^{2002} = \left(2002^{667}\right)^3.2002$, như vậy ta chỉ cần thử xây dựng các nghiệm dạng $x_i = m_i 2002^{667}$, với

$$m_1^3 + m_2^3 + m_3^3 + m_4^3 = 2002.$$

Ta chọn $m_1 = m_2 = 10; m_3 = m_4 = 1$ thỏa yêu cầu này.

Bài toán 2. ***(USAMO)*** *Xác định tất cả nghiệm không âm $(x_1,\ x_2, ...,\ x_{14})$ của phương trình*

$$x_1^4 + x_2^4 + ... + x_{14}^4 = 15999.$$

Phân tích và giải. Lũy thừa 4, gợi cho ta xét modulo nào? $\lambda(n) = 4 = 2^2 \to n = 16$.
Ta có x^4 đồng dư 0 hoặc 1 modulo 16.
Do đó $x_1^4 + x_2^4 + ... + x_{14}^4$ đồng dư $1,\ 2,\ ...,\ 14$ modulo 16.
Mà $15999 \equiv -1 (\text{mod } 16)$ (mâu thuẫn).
Vậy phương trình trên vô nghiệm.

Bài toán 3. ***(USAMO 2005)*** *Chứng minh rằng hệ phương trình*

$$\begin{cases} x^6 + x^3 + x^3y + y = 147^{157} \\ x^3 + x^3y + y^2 + y + z^9 = 157^{147} \end{cases}$$

không có ngiệm nguyên $x,\ y,\ z$.

Phân tích và lời giải. Cộng hai phương trình ta được

$$(x^3+y+1)^2+z^9=147^{157}+157^{147}+1.$$

Đối với lũy thừa 9, ta xét modulo nào? Để ý

$$9=\frac{1}{2}18=\frac{1}{2}\lambda(19)=\frac{1}{2}\lambda(27)=\frac{1}{2}\lambda(54),$$

nên ta có thể xét theo các mođulo này trước tiên.
Lũy thừa 2, ta xét các modulo 3, 4, 5, 8; sử dụng thặng dư bình phương để kiểm tra nghiệm.
Ta bắt đầu với modulo $p=19$. Ta có

$$\begin{aligned}
&z^9\equiv 0,\ \pm 1 \pmod{19}\\
&147^{157}\equiv(-5)^{18.8+13}\equiv -5^{13}\equiv 2 \pmod{19}\\
&157^{147}\equiv(5)^{18.8+3}\equiv 5^3\equiv 11 \pmod{19}.
\end{aligned}$$

Suy ra

$$(x^3+y+1)^2=147^{157}+157^{147}+1-z^9\equiv 13,\ 14,\ 15 \pmod{19}.$$

Áp dụng tính chất ta tính được

$$\left[\frac{13}{19}\right]=-1;\ \left[\frac{14}{19}\right]=-1;\ \left[\frac{15}{19}\right]=-1$$

nên điều này không xảy ra.

Bài toán 4. ***(USAJMO 2013)*** *Tìm tất cả các số nguyên a, b sao cho a^5b+3 và ab^5+3 đều là lập phương của một số nguyên.*

Phân tích và lời giải. Giả sử

$$\begin{cases} a^5b+3=x^3\\ ab^5+3=y^3 \end{cases}.$$

với $x,\ y\in\mathbb{N}$. Suy ra

$$(ab)^6=(a^5b)(ab^5)=(x^3-3)(y^3-3). \qquad (*)$$

Lũy thừa 6, 3 gợi ý cho ta xét các modunlo 9 và 18. $\lambda(9)=6$ nên $(ab)^6\equiv 0,\ 1 \pmod 9$. $x^3,\ y^3\equiv 0,\ \pm 1 \pmod 9$. Kết hợp (*) ta có

$$\begin{cases} x^3\equiv 0 \pmod 9\\ y^3\equiv 0 \pmod 9\\ (ab)^6\equiv 0 \pmod 9 \end{cases}\Rightarrow\begin{cases} 3|\,x\\ 3|\,y\\ 3|\,ab \end{cases}$$

Nếu $3|\,a$ thì từ $a^5b+3=x^3$ ta được điều vô lý vì $27|\,x^3;\ 27|\,a^5b$.
Nếu $3|\,b$ thì từ $ab^5+3=y^3$ ta được điều vô lý vì $27|\,y^3;\ 27|\,ab^5$.
Vậy không tồn tại các số nguyên a, b thỏa điều kiện bài toán.

Bài toán 5. ***(MOP 2002)*** *Chứng minh rằng phương trình $x^6=y^5+24$ không có nghiệm nguyên.*

Phân tích và lời giải. Ta tìm một modulo chung cho hai lũy thừa 5, 6. Với mong muốn số đồng dư hai vế là tối thiểu. Như vậy, $5.6|(p-1)$, $p=31$ là trường hợp đầu tiên ta xét.
x^6 có $1+\dfrac{30}{(6,30)}=6$ đồng dư; y^5 có $1+\dfrac{30}{(5,30)}=7$ đồng dư, như vậy khả năng các đồng dư của hai vế không bằng nhau
y^5 có các đồng dư $0,\ 1,\ 5,\ 6,\ 25,\ 26,\ 30$ theo modulo 31.
Suy ra y^5+24 có các đồng dư $24,\ 25,\ 29,\ 30,\ 18,\ 19,\ 23$ theo modulo 31.
x^6 có các đồng dư $0,\ 1,\ 2,\ 4,\ 8,\ 16$ theo modulo 31.
Vậy phương trình trên không có nghiệm nguyên. Tiếp theo, ta phân tích một số kĩ năng chọn modulo với các phương trình dạng lũy thừa chứa biến trên mũ.

Bài toán 6. *Tìm các nghiệm nguyên dương của phương trình*

$$2^x+3^y=5^z.$$

Phân tích và lời giải.
+ Dự đoán nghiệm phương trình $(x;\ y;\ z)=(1;\ 1;\ 1),\ (4;\ 2;\ 2)$.
+ Đối với lũy thừa có cơ số đã xác định, thường phương án đầu tiên ta thử phân tích nhân tử về dạng $A.B=a^x$, xét ước chung của A, B để đưa về hệ. Để phân tích nhân tử, thường ta quan tâm đến các hàng đẳng thức cùng số mũ.
+ Các modulo thường dùng trước hết để xét lũy thừa là a^{n+1}với n là nghiệm lớn nhất của phương trình, các modulo có đồng dư 1.
+ Để ý $5\equiv 1 \pmod 2^2$; $3\equiv -1 \pmod 2^2$, $3^2\equiv 1 \pmod 2^3$. Do đó, ta có thể xét các modulo 4, 8. Để xét các modulo này ta chia thành 2 trường hợp.

TH1: $x=1$, phương trình trở thành

$$2+3^y=5^z.$$

Phương trình có nghiệm $(1;\ 1;\ 1)$.
Xét $z\geqslant 2$, suy ra $3^y\equiv 5^z-2\equiv -2 \pmod{25}$.

r	$3^r \pmod{25}$
1	3
2	9
3	2
4	6
5	18
6	4
7	12
8	11

r	$3^r \pmod{25}$
9	11
10	8
11	24
12	22
13	16
14	-2
15	-6
16	21

$\lambda(25)=20$ do đó $ord_3 25|\ 20$, suy ra $ord_3 25=20$.
$3^y\equiv -2\equiv 3^13 \pmod{25}$, theo tính chất cấp phần tử suy ra $y=13+20k$.
$3^y=3^{13+20k}=3^{13}.\left(3^{20}\right)^k$ ta xét modulo nào? Modulo 11 là modulo xét trước để cố định số đồng dư của 3^y.

$$5^z\equiv 2+\left(3^{10}\right)^{1+2k}.3^3\equiv 7 \pmod{11}.$$

z	$5^z \pmod{11}$
1	5
2	3
3	4
4	9
5	1

Do đó không có giá trị nào của z để

$$5^z \equiv 7 \pmod{11}.$$

TH2. $x = 2$, phương trình trở thành

$$4 + 3^y = 5^z,$$

suy ra $z \geqslant 2$. Suy ra

$$3^y \equiv 5^z - 4 \equiv 21 \equiv 3^{16} \pmod{25} \Rightarrow y = 16 + 20k.$$

Khi đó

$$5^z \equiv 4 + \left(3^{10}\right)^{1+2k}.3^6 \equiv 7 \pmod{11} \text{ vô lí.}$$

TH3: $x \geqslant 3$. Khi đó

$$1^z - (-1)^y \equiv 5^z - 3^y \equiv 2^x \equiv 0 (\text{mod } 4) \Rightarrow y = 2n.$$

Nên

$$5^z \equiv 3^y + 2^x \equiv 9^n \equiv 1 \pmod{8},$$

mà $ord_8 5 = 2$ suy ra $z = 2m$. Suy ra

$$2^x = 5^{2m} - 3^{2n} = (5^m + 3^n)(5^m - 3^n)$$

Suy ra

$$\begin{cases} 5^m - 3^n = 2^s \\ 5^m + 3^n = 2^r \end{cases}$$

hay

$$\begin{cases} 2.5^m = 2^r + 2^s \\ 2.3^n = 2^r - 2^s \end{cases}$$

với $r > s$, $r + s = x$. Nên $s = 1$,ta có

$$\begin{cases} 5^m = 2^{r-1} + 1 \\ 3^n = 2^{r-1} - 1 \end{cases}$$

và $5^m - 3^n = 2$.
Phương trình có nghiệm $m = n = 1$ (đã giải ở TH1).
Vậy phương trình đã cho chỉ có 2 nghiệm $(x;\ y;\ z)$ là $(1;\ 1;\ 1)$ và $(4;\ 2;\ 2)$.

Bài toán 7. *Tìm nghiệm nguyên dương của phương trình*

$$2^x + 3 = 11^y.$$

Phân tích và lời giải.
Phương trình có nghiệm $(x;\ y) = (3;\ 1)$.
Trong phương trình modulo đầu tiên ta có thể sử dụng là modulo 11.
Vì $2^5 \equiv 32 \equiv -1 \pmod{11}$ nên $ord_2 11 = 10$.
$2^3 \equiv -3 \pmod{11}$ nên $2^x \equiv -3 \equiv 2^3 \pmod{11}$. Suy ra $x = 3 + 10n$.
Điều này chưa sử dụng được.
Với $x \geqslant 4$,

$$11^y \equiv 2^x + 3 \equiv 3 \pmod{2^x}.$$

và $11 \equiv 3 (\text{mod } 8)$ nên $ord_{2^4} 11 = 2^2 = 4$; $11^3 \equiv 3 (\text{mod } 2^4)$ do đó $y = 4k + 3$, dạng modulo này nhỏ sẽ dễ "trùng lặp đồng dư".
Ta tăng modulo lên 2^5.
Ta chứng minh phương trình không có nghiệm $x \geqslant 5$ bằng cách lựa chọn modulo theo sơ đồ như bài trên.
Bước 1: Sử dụng modulo 2^5 tìm dạng của y:

$$11^y \equiv 2^x + 3 \equiv 3 \pmod{32}.$$

Từ $ord_{2^5} 11 = 2^{5-2} = 8$; $11^7 \equiv 3 \pmod{32}$; $11^y \equiv 11^7 \pmod{32}$ suy ra $y = 8k + 7$.
Phương trình trở thành

$$2^x = 11^{8y+7} - 3 = \left(11^8\right)^y .11^7 - 3.$$

Bước 2: Tìm số nguyên tố p sao cho hai vế không cùng đồng dư, muốn vậy cách dễ nhất là chọn modulo p sao cho $11^8 \equiv \pm 1 \pmod{p}$ và $ord_2 p$ là nhỏ.
Chú ý $8 = \frac{1}{2}(17 - 1)$ và $2^4 = 16 \equiv -1 \pmod{17}$, ta xét mod 17.
2^x có $4.2 = 8$ đồng dư; vế phải có 2 đồng dư, vậy khả năng không trùng là lớn.
$11^2 \equiv 6^2 \equiv 2 (\text{mod } 17)$; $11^4 \equiv 4 (\text{mod } 17)$; $11^8 \equiv -1 (\text{mod } 17)$; $11^7 \equiv 3 (\text{mod } 17)$
Suy ra $2^x \equiv (11^8)^y .11^7 - 3 \equiv 0 (\text{mod } 17)$ hoặc $2^x \equiv (11^8)^y .11^7 - 3 \equiv -6 (\text{mod } 17)$.
Ta khảo sát các đồng dư modulo 17 của 2^x với $x = 3 + 10n$.

x	$2^x \pmod{17}$
1	2
3	8
5	-2
7	-8

Vậy hai vế không cùng đồng dư với modulo 17.

Bài toán 8. ***(Ấn Độ)*** *Tìm nghiệm nguyên dương của phương trình*

$$7^x = 3^y + 4.$$

Phân tích và lời giải.
Phương trình có nghiệm $(1;\ 1)$ và $y = 2$ không thỏa phương trình.
Ta có $3^y \equiv 7^x - 4 \equiv 3 \pmod 7$ mà $3^3 \equiv -1 (\text{mod } 7)$, $ord_7 3 = 6$ nên $y = 1 + 6t$.
Ta chứng minh $y \geqslant 3$, không thỏa.

Bước 1: Từ phương trình suy ra

$$7^x \equiv 3^y + 4 \equiv 4 (\text{mod } 3^3).$$

Trước hết ta xác định $ord_{3^n} 7$. Đặt $ord_{3^n} 7 = 3^i.k$ với $(k, 3) = 1$, $i \leqslant n - 1$.
Ta có

$$v_3\left(7^{3^i.k} - 1\right) = v_3(7 - 1) + v_3\left(3^i.k\right) = i + 1 \geqslant n.$$

Suy ra $i \geqslant n - 1$ nên $i = n - 1$.
Vậy $ord_{3^n} 7 = 3^{n-1}$, do đó $ord_{3^3} 7 = 9$.
Lại có $7^8 \equiv 4 \equiv 7^x \pmod{27}$, suy ra $x = 9q + 8$.
Phương trình trở thành

$$\left(7^9\right)^q.7^8 - 4 = 3^y.$$

Bước 2: Tìm số nguyên tố p sao cho $7^9 \equiv \pm 1 (mod\ \text{p})$ và $ord_p 3$ là nhỏ. Vì

$$7^9 - 1 = (7^3 - 1)(7^6 + 7^3 + 1).(7^3 - 1).3.37.1063$$

nên ta chọn $p = 37$.
Ta có:

$$7^2 \equiv 12 \pmod{37};\ 7^4 \equiv 12^2 \equiv -4 \pmod{37};\ 7^8 \equiv 16 \pmod{37}.$$

Vậy $\left(7^9\right)^q.7^8 - 4 \equiv 12 \pmod{37}$.
Ta khảo sát các đồng dư modulo 37 của 3^y với $y = 1 + 6t$

y	$3^y \pmod{37}$
1	3
7	4
13	30
19	25
25	21
31	28

Vậy hai vế không cùng đồng dư với modulo 37.

*Đối với các phương trình lũy thừa có biểu thức $a^u \pm 1$ thì các bổ đề **LTE** và kiến thức về cấp là thực sự hữu dụng. Ta xét các ví dụ sau đây.*

Bài toán 9. ***(1995 Czech – Slovak Match)*** *Giải phương trình nghiệm nguyên dương $p^x - y^p = 1$ với p là số nguyên tố lẻ.*

Phân tích và lời giải.
Phương trình được viết lại $p^x = y^p + 1$, suy ra $p | (y+1)$.
Áp dụng bổ đề LTE ta có

$$x = v_p(y^p + 1) = v_p(y+1) + v_p(p) = 1 + v_p(y+1).$$

Suy ra $y + 1 = p^{x-1}$ và $\dfrac{y^p + 1}{y+1} = p$.
Ta có

$$y^3 + 1 - (y+1)^2 = y^3 - y^2 - 2y = y(y^2 - y - 2) > 0 \ \forall y \geqslant 3.$$

Hay

$$y + 1 < \frac{y^3 + 1}{y+1} \leqslant \frac{y^p + 1}{y+1}.$$

với mọi $y \geqslant 3$.
Vậy ta phải có $y = 2$, suy ra $p^{x-1} = 3 \Leftrightarrow \left[\begin{array}{l} x = 2 \\ p = 3 \end{array}\right.$
Vậy phương trình có nghiệm $x = 2,\ y = 2,\ p = 3$.

Bài toán 10. ***(IMO lần 31)*** *Giải phương trình nghiệm nguyên dương*

$$2^x + 1 = x^2 y.$$

Phân tích và lời giải.
Phương trình có nghiệm $(x; y) = (1;\ 3),\ (3;\ 1)$.
Xét $x \geqslant 3$, từ phương trình suy ra x, y là các số lẻ.
Phương trình có lũy thừa có $a^u \pm 1$ có thể sử dụng cấp để xét. Một trong các modulo hay dùng là ước nguyên tố của nhân tử.
Ta thử xét theo modulo p, với p là ước của x. $2^x = x^2 y - 1 \equiv -1 \pmod p$ nên $2^2 \equiv 1 \pmod p$.
Đặt $u = ord_p 2 > 1$, ta có $u | (p-1)$. Suy ra $u | 2x$.
Vậy p chọn như thế nào?
+ Nếu $p = 3$ thì hai điều này là như nhau. Vậy ta phải xét tới số mũ chính xác của 3 trong x là bao nhiêu ?
+ Nếu $p > 3$, thì chọn p như thế nào trong số các ước của x, để các ước không trùng nhau, ta sẽ chọn p là ước nguyên tố nhỏ nhất khác 3 của x.

$$v_3(x^2 y) = v_3(2^x + 1^x) = v_3(2+1) + v_3(x).$$

Suy ra $2v_3(x) + v_3(y) = 1 + v_3(x)$ từ đây ta được $v_3(x) + v_3(y) = 1$.
Đặt $x = 3^k.d$ với $k = 0$ hoặc 1; $(d, 3) = 1$. Ta sẽ chứng minh $d = 1$.
Vì $2^x = x^2 y - 1 \equiv -1 \pmod x$, gợi ta có thể sử dụng định lý về cấp của 2.
Nếu $d > 1$, gọi p là ước nguyên tố nhỏ nhất của d, cũng là ước nguyên tố khác 3 nhỏ nhất của x. Do $(d, 3) = 1$ nên $p \geqslant 5$.
Đặt $u = ord_p 2 > 1$, $u | (p-1)$. $2^x = x^2 y - 1 = 3^{2k} d^2 y - 1 \equiv -1 \pmod p$ nên $2^{2x} \equiv 1 \pmod p$. Suy ra $u | 2x$.
Vì p là ước nguyên tố khác 3 nhỏ nhất của x và $(x, p-1) = 1$ nên $u \in \{2; 3; 6\}$.
Mà $p | 2^u - 1$ nên $p = 7$.
Suy ra $2^x + 1 \equiv 0 \pmod 7$ điều này mâu thuẫn vì bảng đồng dư sau.

x	$2^x \pmod 7$
1	2
2	4
3	1

Bài toán 11. ***(Trung Quốc 2009)*** *Tìm tất cả các cặp số nguyên tố p, q thỏa*

$$pq \mid 5^p + 5^q.$$

Phân tích và lời giải.
Các lũy thừa cùng cơ số có thể tạo dạng $a^u \pm 1$:

$$a^m \pm a^n = a^n \left(a^{m-n} \pm 1\right).$$

Nếu $p = q$, ta được $p^2 \mid 2.5^p$, suy ra $p = q = 5$.
Nếu trong hai số p, q có 1 số bằng 5, giả sử $p = 5 \neq q$, suy ra $q \mid 5^5 + 5^q$.
Theo Fermat $5^p \equiv 5 \pmod q$, suy ra $0 \equiv 5^5 + 5^q \equiv 5^5 + 5 \pmod q$, suy ra $q \mid 5^5 + 5$ nên $q = 2$ hoặc 313.
Nếu trong hai số p, q có 1 số bằng 2, giả sử $p = 2 \neq q$, suy ra $q \mid 5^2 + 5^q$.
Theo Fermat $5^p \equiv 5 (\text{mod } q)$, suy ra $0 \equiv 5^2 + 5^q \equiv 5^2 + 5 \pmod q$, suy ra $q \mid 5^2 + 5$ nên $q = 3$ hoặc 5.
Nếu $p \neq q$ và p, q khác 5, khác 2. Ta có $0 \equiv 5^p + 5^q \equiv 5 + 5^q \pmod p$, suy ra $5^{q-1} \equiv -1 \pmod p$.
Tương tự $5^{p-1} \equiv -1 \pmod q$. Suy ra

$$\begin{cases} 5^{2p-2} \equiv 1 \pmod q \\ 5^{2q-2} \equiv 1 \pmod p \end{cases} \Rightarrow \begin{cases} ord_q 5 \mid 2p-2 \\ ord_p 5 \mid 2q-2 \end{cases}.$$

Mặt khác $5^{p-1} \equiv -1 \neq 1 \pmod q$ nên $ord_q 5$ không là ước của $p-1$.
Suy ra $v_2(ord_q 5) = v_2(2p-2) = 1 + v_2(p-1)$.
Tương tự

$$v_2(ord_p 5) = v_2(2q-2) = 1 + v_2(q-1).$$

Mặt khác từ

$$\begin{cases} ord_q 5 \mid q-1 \\ ord_p 5 \mid p-1 \end{cases},$$

suy ra

$$\begin{cases} v_2(ord_q 5) \leqslant v_2(q-1) \\ v_2(ord_p 5) \leqslant v_2(p-1) \end{cases}.$$

Kết hợp điều trên suy ra

$$\begin{cases} 1 + v_2(p-1) \leqslant v_2(q-1) \\ 1 + v_2(q-1) \leqslant v_2(p-1) \end{cases} \text{(vô lý)}.$$

Bài toán 12. ***(Bulgaria)*** *Tìm tất cả các số nguyên tố p, q thỏa mãn*

$$pq \mid (5^p - 2^p)(5^q - 2^q).$$

Phân tích và lời giải.
Ta tạo dạng $a^u \pm 1$ như thế nào ? Hai lũy thừa cùng số mũ, thường ta nhân phần tử nghịch đảo. $5^p \equiv 2^p \pmod q$, ta nhân vào hai vế phần tử nghịch đảo của 2 sẽ tạo ra dạng $a^u \pm 1$. Rõ ràng, $p,\ q \notin \{2,5\}$.
* Nếu $p \mid 5^p - 2^p$, theo Fermat ta có

$$5^p - 2^p \equiv 5 - 2 \equiv 3 \pmod p,$$

suy ra $p = 3$. Lúc này

$$3q \mid \left(5^3 - 2^3\right)\left(5^q - 2^q\right)$$

hay

$$q \mid 39\left(5^q - 2^q\right),$$

tương tự như trên suy ra $q = 3$ hoặc $q = 13$.
* Nếu $q \mid 5^q - 2^q$, ta cũng được $p = 3$ hoặc $q = 13$.
* Xét $\begin{cases} q \mid 5^p - 2^p \\ p \mid 5^q - 2^p \end{cases}$, $p, q \neq 3$.
Do $(2,q) = 1$ nên tồn tại m, n sao cho $2m + nq = 1$ hay $2m \equiv 1 \pmod q$.
Suy ra $(5.m)^p \equiv (2m)^p \equiv 1 \pmod q$, do đó $ord_q(5m) \in \{1, p\}$ và $ord_q(5m) \Big| p - 1$.
Nếu $ord_q(5m) = 1$, hay $5m \equiv 1 \pmod q$. Suy ra $2 \equiv 2(5m) \equiv 5.2m \equiv 5 \pmod q$, do đó $q = 3$ (mâu thuẫn).
Vậy $ord_q(5m) = p$, suy ra $p \mid q - 1$ (*).
Tương tự cũng từ $5^q \equiv 2^q \pmod p$, ta có $q \mid p - 1$ điều này mâu thuẫn với (*).
Vậy $(p,\ q) = (3;\ 3),\ (3;\ 13),\ (13;\ 3)$.

Bài toán 13. ***(USA TST 2003)*** *Tìm tất cả các số nguyên tố p, q, r sao cho*

$$p \mid q^r + 1,\ q \mid r^p + 1,\ r \mid p^q + 1. \qquad (*)$$

Phân tích và lời giải.
Nếu p, q, r đều khác 2. Từ (*) suy ra

$$\begin{cases} p \mid q^{2r} - 1 \\ q \mid r^{2p} - 1 \\ r \mid p^{2q} - 1 \end{cases}, \text{ do đó } \begin{cases} ord_p q \in \{1, 2, r\} \\ ord_q r \in \{1, 2, p\} \\ ord_r p \in \{1, 2, q\} \end{cases}.$$

+ Nếu $ord_p q,\ ord_q r,\ ord_r p \in \{1, 2\}$ thì

$$\begin{cases} q^2 \equiv 1 \pmod p \\ p^2 \equiv 1 \pmod r \\ r^2 \equiv 1 \pmod q \end{cases} \Rightarrow \begin{cases} q \equiv \pm 1 \pmod p \\ p \equiv \pm 1 \pmod r \\ r \equiv \pm 1 \pmod q \end{cases}.$$

Suy ra $\begin{cases} q \pm 1 \geqslant 2p \\ p \pm 1 \geqslant 2r \\ r \pm \geqslant 2q \end{cases}$, điều này vô lí vì $p,\ q,\ r \geqslant 3$.
+ Vậy trong 3 số $ord_p q,\ ord_q r,\ ord_r p$ phải có ít nhất một số lớn hơn 2, giả sử $ord_p q = 2r$.
Suy ra $2r \mid p - 1$, do đó $p \equiv 1 \pmod r$, $p^q + 1 \equiv 2 \pmod r$ trái giả thiết.
* Vậy trong 3 số p, q, r phải có ít nhất một số bằng 2. Giả sử $p = 2$. Suy ra q, r là các số

nguyên tố lẻ, do đó tương tự chứng minh trên ta cũng có $ord_r 2 \in \{2,\ 2q\}$.
Nếu $ord_r 2 = 2$ thì $r = 3$ và $q | 3^2 + 1$ nên $q = 5$.
Nếu $ord_r 2 = 2q$ suy ra $2q | r - 1$, do đó $r \equiv 1 \pmod 1$, vì vậy $r^2 + 1 \equiv 2 \pmod q$ mâu thuẫn giả thiết).
Vậy $(p,\ q,\ r) = (2,\ 3,\ 5)$ và các hoán vị của nó.

Các bài tập sau ta phân tích một số kĩ năng chọn modulo "không có sẵn". Các modulo thường là các nhân tử nguyên tố nào đó.

Bài toán 14. *Cho $p \geqslant 5$ là số nguyên tố, n là số nguyên dương sao cho các số $p-1, pn, n+1$ đôi một không có chung ước lớn hơn 2. Chứng minh rằng phương trình sau không có nghiệm nguyên dương x, y*

$$2 + x + x^2 + \ldots + x^{p-1} = y^{n+1}.$$

Phân tích và lời giải.
Giả sử tồn tại các số nguyên dương x, y thỏa phương trình

$$2 + x + x^2 + ... + x^{p-1} = y^{n+1}.$$

Viết lại (1) :

$$1 + x + x^2 + ... + x^{p-1} = y^{n+1} - 1.$$

Nếu $x = 1$, ta có

$$p = y^{n+1} - 1 = (y-1)(y^n + y^{n-1} + ... + y + 1),$$

suy ra $y - 1 = 1$ và $p = 2^{n+1} - 1$.
Đặt $ord_p 2 = u$, $u \geqslant 3$, $u | (p-1)$ Mà $2^{n+1} \equiv 1 \pmod p$ nên $u | (n+1)$.
Vậy $(n+1, p-1) \geqslant u > 2$ mâu thuẫn giả thiết.
• $x \geqslant 2$, ta có

$$\begin{aligned} x^{p-1} + x^{p-2} + ... + x + 1 = \frac{x^p - 1}{x - 1} &= y^{n+1} - 1 \\ &= (y-1)(y^n + y^{n-1} + ... + y + 1). \end{aligned}$$

Ta khảo sát các ước nguyên tố của $\dfrac{x^p - 1}{x - 1}$.
Xét q là một ước nguyên tố bất kì của $\dfrac{x^p - 1}{x - 1}$.
Nếu $x \equiv 1 \pmod q$ thì

$$0 \equiv \frac{x^p - 1}{x - 1} = 1 + x + x^2 + ... + x^{p-1} \equiv p \pmod q$$

suy ra $p = q$.
Nếu $x \not\equiv 1 \pmod q$, từ $x^p \equiv 1 \pmod q$ và p là số nguyên tố thì $p = ord_q x$.
Mặt khác $x^{q-1} \equiv 1 \pmod q$ suy ra $p | (q-1)$.
Vậy tất cả các ước nguyên tố q của $\dfrac{x^p - 1}{x - 1}$ thì $q = p$ hoặc $q = 1 \pmod p$.
Dẫn tới hai số $y - 1$ và $y^n + y^{n-1} + ... + y + 1$ hoặc chia hết cho p hoặc có số dư là 1 khi chia cho p. (*)

TH1: $y-1\equiv 0 \pmod p \Leftrightarrow y\equiv 1 \pmod p$, suy ra

$$y^n+y^{n-1}+...+y+1\equiv n+1 \pmod p.$$

Theo (*) suy ra $n+1\equiv 1 \pmod p$ hoặc $p|(n+1)$ điều này mâu thuẫn giải thiết các số $p-1,\ pn,\ n+1$ đôi một không có chung ước lớn hơn 2.

TH2: $y-1\equiv 1 \pmod p \Leftrightarrow y\equiv 2 \pmod p$. Khi đó

$$y^n+y^{n-1}+...+y+1\equiv 2^{n+1}-1 \pmod p.$$

Theo (*) suy ra hoặc

$$2^{n+1}-1\equiv 0 \pmod p \tag{1}$$

hoặc

$$2^{n+1}-1\equiv 1 \pmod p.$$

Mà $2^{n+1}-1\equiv 1 \pmod p$ cho ta $2^{n+1}-2\equiv 0 \pmod p$, suy ra

$$2^n\equiv 1 \pmod p. \tag{2}$$

Đặt $ord_p 2=u, u\geqslant 3,\ u|(p-1)$.
Từ (1) suy ra $u|(n+1)$; $u|(p-1)$ mâu thuẫn giả thiết.
Từ (2) suy ra $u|n$; $u|(p-1)$ mâu thuẫn giả thiết.
Tóm lại trong các trường hợp ta đều có điều giả sử ban đầu là sai. Bài toán được chứng minh.

Bài toán 15. ***(Turkey TST 2013)*** *Kí hiệu $\varphi(n)$ là phi hàm Euler của n. Giải phương trình nghiệm nguyên dương ($n\geqslant 2$) sau*

$$2^n+(n-\varphi(n)-1)!=n^m+1.$$

Phân tích và lời giải.
Ta có:

$$2^n-1=n^m-(n-\varphi(n)-1)!.$$

Ta chọn số nguyên tố ước của n, để đảm bảo $p|(n-\varphi(n)-1)!$ ta phải xét xem khi nào $n-\varphi(n)-1\geqslant p$.
Đặt $n=p_1^{r_1}...p_s^{r_s}$, với $p_1<p_2<...<p_s$, xét $p=p_1$.

$$n-\varphi(n)-1=p_1^{r_1}...p_s^{r_s}-n=p_1^{r_1-1}...p_s^{r_s-1}[p_1...p_s-(p_1-1)...(p_s-1)]-1.$$

Nếu $s\geqslant 2$ thì

$$p_1...p_s-(p_1-1)...(p_s-1)>p_1...p_s-p_1p_2...p_{s-1}(p_s-1)>p_1$$

do đó $n-\varphi(n)-1\geqslant p$.
Nếu $s=1, n-\varphi(n)-1=p^{r-1}(p-1)-1<p$ khi $\left[\begin{array}{c} r=1 \\ r=2, p=2 \end{array}\right.$

TH1 : $n=p$ là số nguyên tố, $2^p+1=p^m+1$ suy ra $p=2, m=2$.

TH2: $n=2^2$, suy ra $2^4+1=4^m+1$ suy ra $m=2$.

TH3: n không phải là số nguyên tố và $n > 4$.
Gọi p là ước nguyên tố nhỏ nhất của n, gọi lại chứng minh trên ta được $n - \varphi(n) - 1 \geqslant p$, suy ra

$$p \mid (n - \varphi(n) - 1)!$$

$$2^n = n^m + 1 - (n - \varphi(n) - 1)! \equiv 1 \pmod{p}.$$

Đặt $ord_p 2 = u$, $u \geqslant 2$, $u \mid (p-1)$, mà $2^n \equiv 1 (mop\ \text{p})$ nên $u \mid n$ điều này vô lý vì p là ước nguyên tố nhỏ nhất của n.
Vậy phương trình có 2 nghiệm $(n, m) = (2; 2), (4; 2)$.

Bài toán 16. ***(IMO SL 2012)*** *Cho x, y là các số nguyên dương. Chứng minh rằng nếu $x^{2^n} - 1$ chia hết cho $2^n y + 1$ với mọi số nguyên dương n thì $x = 1$.*

Phân tích và lời giải.
Nếu $x \neq 1$ và p là một ước nguyên tố của $2^n y + 1$ thì $p \mid x^{2^n} - 1$. Suy ra $ord_p x \mid UCLN(2^n,\ p-1)$.
Mà $UCLN(2^n,\ p-1)$ xác định trong trường hợp đặc biệt $p = 4h+3$ và $UCLN(2^n,\ p-1) = 2$.
Lúc này

$$x^2 - 1 \equiv 0 \pmod{p}$$

Như vậy, ta sẽ đi khảo sát các ước nguyên tố dạng $4h + 3$ của $2^n y + 1$. Khi n thay đổi, liệu có vô số số p dạng $4h + 3$ không ?
Ta chứng minh với m là số lẻ, có vô số số ước nguyên tố dạng $4h + 3$của $2^n m + 1$ với n nào đó.
Vì $2m + 1 = 2(2s + 1) + 1 = 4s + 3$ do đó $2m + 1$ có ước nguyên tố dạng $4h + 3$.
Giả sử chỉ có hữu hạn số nguyên tố $p_1, p_2, ..., p_k$ dạng $4h + 3$ mà $p_i \mid 2^n m + 1$, trong đó $p_1, p_2, ...p_s$ là tất cả các ước nguyên tố dạng $4h + 3$ của $2m + 1$.
Đặt

$$2m + 1 = p_1^{r_1} p_2^{r_2} ... p_s^{r_s} . q_1^{\alpha_1} ... q_t^{\alpha_t}.$$

Từ các số $2^n m + 1$, ta có thể tạo dạng lũy thừa quen thuộc $2^s - 1$ bằng phép hiệu để đặt nhân tử chung:

$$2^n . m + 1 - (2m + 1) = 2m(2^{n-1} - 1),$$

để chia hết số w, ta chỉ cần chọn $n - 1 = \varphi(w)$, vậy w là số nào?
Ta có

$$w \mid 2^n . m + 1 - (2m + 1) \Leftrightarrow 2^n . m + 1 \equiv 2m + 1 \pmod{w},$$

như vậy trong w nếu có nhân tử $p_{s+1}, ...p_k$ thì $p_{s+1}, ...p_k$ không là ước của $2^n m + 1$, do đó $2^n m + 1$ chỉ có các ước nguyên tố dạng $4h + 1$ và p_i, q_j, $(1 \leqslant i \leqslant s)$. Vậy ta chọn

$$w = (2m + 1).p_1 p_2 ... p_s . p_{s+1} ... p_k . q_1 q_2 ... q_t > 2m + 1.$$

Xét $w = (2m + 1).p_{s+1} ... p_k$ và $n = \varphi(w) + 1$. Suy ra

$$2^n . m + 1 \equiv 2m + 1 \pmod{(2m + 1).p_1 p_2 ... p_s . p_{s+1} ... p_k . q_1 q_2 ... q_t} \qquad (*)$$

Suy ra $p_{s+1}, ...p_k$không là ước của $2^n m + 1$, do đó $2^n m + 1$ chỉ có các nhân tử nguyên tố dạng $4h + 1$ và p_i, q_j, $(1 \leqslant i \leqslant s)$.
Cũng từ (*) suy ra $2^n . m + 1 = (2m + 1)M$, trong đó M chỉ gồm các nhân tử nguyên tố dạng $4h + 1$. Suy ra

$$2^n m + 1 \equiv 2m + 1 \equiv 3 \pmod{4} \text{ (vô lý).}$$

Vậy có vô số số nguyên tố p dạng $4h+3$ mà p là ước của $2^n m+1$ với n nào đó.
Nếu y chẵn ta cũng có được điều này bằng cách đặt $y=2^u.m$.
Vậy có vô số số nguyên tố p để $p|\, x^2-1$, do đó $x=1$.

Bài toán 17. *Tìm tất cả các số nguyên dương n sao cho với mọi số nguyên dương k đều tồn tại một số nguyên dương a sao cho a^3+a-k chia hết cho n.*

Phân tích và giải.
Với $n=1$ hiển nhiên thỏa yêu cầu đề bài.
Nếu $n>1$, gọi p là một ước nguyên tố của n. Khi đó, cho k chạy từ 0 đến $p-1$ ta được

$$\left\{a^3+a\middle|\, 0\leqslant a\leqslant p-1\right\}$$

là hệ thặng dư đầy đủ modulo p (*).
Do a^3+a là số chẵn nên $p>2$.
Nếu $p=3$,thì

$$a^3+a\equiv a+a\equiv 2a \pmod 3$$

nên

$$\left\{a^3+a\middle|\, 0\leqslant a\leqslant 2\right\}$$

là hệ thặng dư đầy đủ modulo p.
Xét $p>3$. Do (*) nên phương trình

$$a^3+a\equiv 0^3+0 \pmod p$$

không có nghiệm $a\neq 0 \pmod p$, hay phương trình

$$x^2\equiv -1 \pmod p$$

vô nghiệm. Vậy tập

$$\left\{-x^2\middle|\, 1\leqslant x\leqslant p-1\right\}$$

là tập tất cả các không thặng dư bậc hai modulo p.
Do (*) nên phương trình

$$a^3+a\equiv (ka)^3+ka \pmod p$$

vô nghiệm với mọi $1\leqslant a,k\leqslant p-1$ hay phương trình

$$a^2\left(k^2+k+1\right)+1\equiv 0 \pmod p. \tag{1}$$

Hay

$$k^2+k+1\equiv -1(a^{-1})^2 \pmod p.$$

Vậy phương trình

$$k^2+k+1\equiv -c^2 \pmod p$$

vô nghiệm $(k,\ c)$. Suy ra k^2+k+1 là thặng dư bậc hai với mọi k.
Xét tập

$$A=\left\{f(x)_{\bmod p}\middle|\, 0\leqslant x\leqslant \frac{p-1}{2}\right\}$$

với $f(x) = x^2 + x + 1$.
Vì $f(x) - f(y) = (x-y)(x+y+1)$, và $x+y+1 < p$ với $0 \leqslant x, y \leqslant \dfrac{p-1}{2}, x \neq y$ nên $f(x) \bmod p \neq f(y) \bmod p$.
Vậy $|A| = \dfrac{p+1}{2}$, suy ra A là tập tất cả thặng dư bậc hai modulo p và 0.
Với mỗi $b = z^2 \in A$, do p lẻ nên tồn tại w sao cho $z \equiv 2w+1 \pmod p$. Vậy $4w^2+4w+1 \in A$.
Ta có $b+3 = 4(w^2+w+1) = 2^2(w^2+w+1)$ là thặng dư bình phương nên $b+3 \in A$.
Vậy A có tính chất

$$\forall b, b \in A \Rightarrow b+3 \in A.$$

Do $0,\ 1 \in A$ nên $|A| \geqslant \dfrac{2}{3}(p-1) > \dfrac{p+1}{2}$ vô lí.
Vậy $p = 3$, do đó $n = 3^r$.
* Với $n = 3^r$, ta chứng minh

$$\left\{a^3 + a \,\middle|\, 0 \leqslant a \leqslant 3^r\right\}$$

là hệ thặng dư đầy đủ modulo 3^r.
Với $0 \leqslant a, b \leqslant 3^r - 1, a \neq b$ ta có

$$(a^3+a) - (b^3+b) = (a-b)(a^2+b^2+ab+1)$$
$$4(a^2+ab+b^2+1) = (2a+b)^2 + 3b^2 + 4 \equiv (2a+b)^2 + 1 \neq 0 \pmod 3.$$

Vậy

$$(a^3+a) - (b^3+b) = (a-b)(a^2+b^2+ab+1) \neq 0 (\bmod\ 3^r).$$

Suy ra

$$\left\{a^3 + a \,\middle|\, 0 \leqslant a \leqslant 3^r\right\}$$

là hệ thặng dư đầy đủ modulo 3^r.
Vậy giá trị cần tìm n là $n = 3^r$. Cuối cùng chúng tôi đưa ra một số bài tập để bạn đọc luyện tập.

Bài tập 1. **(Bosnhia TST 2015)** Chứng minh rằng có vô số số nguyên dương n, n không là số nguyên tố sao cho

$$n \mid 3^{n-1} - 2^{n-1}.$$

Bài tập 2. **(Bosnhia TST 2014)** Tìm tất cả các số nguyên không âm x, y sao cho $7^x - 2.5^y = -1$.

Bài tập 3. **(Pháp TST 2012)** Cho p là số nguyên tố. Tìm tất cả các số nguyên dương a, b, c thỏa

$$a^p + b^p = p^c.$$

Bài tập 4. **(Đức TST 2010)** Tìm tất cả các số nguyên dương m, n thỏa

$$3^m - 7^n = 2.$$

Bài tập 5. **(Iran TST 2012)** Tìm tất cả các số nguyên dương a, b, c sao cho $a^2+b^2+c^2$ chia hết cho $2013(ab+bc+ca)$.

Bài tập 6. **(Romanian Master in Mathematics 2012)** Chứng minh rằng tồn tại vô số số nguyên dương n sao cho $2^{2^n+1}+1$ chia hết cho n, nhưng 2^n+1 không chia hết cho n.

Tài liệu

[1] Olympiad Number Theory, Justin Stevens.

[2] http://www.artofproblemsolving.com

CHỨNG MINH BẤT ĐẲNG THỨC BẰNG PHƯƠNG PHÁP PHÂN TÍCH BÌNH PHƯƠNG VỚI SỰ TRỢ GIÚP CỦA MÁY VI TÍNH

Nguyễn Quốc Anh
(Thành phố Hồ Chí Minh)

GIỚI THIỆU

Với khả năng hiện nay, máy tính đã giúp ta giải được rất nhiều bài toán khó mà trước kia thường bó tay. Mặc dù vậy, vẫn còn một số lớn các bài toán rất thú vị nhưng chưa có "thuật giải" hợp lý để giải chúng. Trong số đó, bài toán phân tích về dạng tổng bình phương trong chứng minh bất đẳng thức là bài toán thường xuyên gặp phải. Trong bài viết này, tác giả sẽ giới thiệu về việc ứng dụng các lệnh có sẵn trong phần mềm Maple [a] (http://www.maplesoft.com/, một công cụ đã khá quen thuộc với mọi người, để xử lý một số bài bất đẳng thức; trên cơ sở đó, xây dựng một chương trình dùng Maple để giải quyết một số bài toán phức tạp hơn. [b]

[a] Maple, cùng với các ngôn ngữ lập trình khác như Mathematica, Mathlab, ... thuộc thế hệ thứ tư (Fourth-generation Programming Language) với các hàm buildin vô cùng mạnh mẽ có thể hỗ trợ, giải quyết hầu hết các tính toán cần thiết, từ đơn giản cho đến phức tạp.

[b] Email của tác giả: bdtilove@live.com)

1. Bài toán mở đầu.

Ta sẽ bắt đầu với bài toán sau đây. Cho các số thực a, b chứng minh rằng:

$$a^2 + b^2 \geq 2ab.$$

Ta có ngay: $a^2 + b^2 - 2ab = (a - b)^2 \geq 0$.
Xuất phát từ bất đẳng thức hiển nhiên đúng: $x^2 \geq 0$, lời giải này là vô cùng dễ hiểu với mọi người. Tuy nhiên, việc quy một đa thức nhiều biến bất kỳ về dạng tổng bình phương không phải là điều dễ dàng chút nào, kể cả với một đa thức đối xứng thuần nhất ba biến.

2. Một vài bài toán hai biến số.

Để hiểu rõ vai trò của máy vi tính trong việc phân tích các bất đẳng thức về dạng bình phương ta sẽ bắt đầu với các bài toán bất đẳng thức hai biến số, nơi máy tính mang một sức mạnh "áp đảo" gần như tuyệt đối.

Ví dụ 1 *Cho a, b là các số thực dương. Chứng minh rằng:*

$$f(a,b) = \frac{1}{a^2} + \frac{1}{b^2} + \frac{4}{a^2+b^2} - \frac{32(a^2+b^2)}{(a+b)^4} \geq 0$$

Lời giải. Chỉ với lệnh $factor$ đơn giản $Maple$ cho ta phân tích như sau:

$$f(a,b) = \frac{(a^4 + 8\,a^3b + 6\,a^2b^2 + 8\,ab^3 + b^4)\,(a-b)^4}{a^2b^2\,(a^2+b^2)\,(a+b)^4} \geq 0$$

Ví dụ 2 *Cho a, b là các số thực dương và $ab \geq 1$. Chứng minh rằng:*

$$f(a,b) = \frac{1}{1+a^2} + \frac{1}{1+b^2} - \frac{2}{1+ab} \geq 0$$

Lời giải. Bằng lệnh $factor$ ta thu được kết quả sau:

$$f(a,b) = \frac{(ab-1)\,(a-b)^2}{(a^2+1)\,(b^2+1)\,(ab+1)}$$

Để ý với $ab \leq 1$ ta có:

$$f(a,b) = \frac{1}{1+a^2} + \frac{1}{1+b^2} - \frac{2}{1+ab} \leq 0$$

Ví dụ 3 *Cho a, b là các số thực dương. Chứng minh rằng:*

$$f(a,b) = \frac{6}{(a+b)^2} - \frac{2}{a^2+b^2} - \frac{1}{ab + \dfrac{(a+b)^2}{4}} \geq 0$$

Lời giải. Ta có:

$$f(a,b) = 12\,.\frac{ab\,(a-b)^2}{(a+b)^2\,(a^2+b^2)\,(a^2+6\,ab+b^2)} \geq 0$$

Ví dụ 4 *Cho các số thực dương a, b. Chứng minh rằng:*

$$f(a,b)=\frac{a^2b}{2\,a^3+b^3}+\frac{2}{3}-\frac{a^2+2\,ab}{2\,a^2+b^2}\geq 0$$

Lời giải. Ta có phân tích như sau:

$$f(a,b)=\frac{2}{3}\cdot\frac{(a+b)\,(a-b)^4}{(2\,a^3+b^3)\,(2\,a^2+b^2)}$$

Ví dụ 5 *Cho các số thực a, b thỏa mãn $a+b=1$. Chứng minh rằng:*

$$ab(a^4+b^4)\leq\frac{5\sqrt{10}-14}{27}$$

Lời giải. Nếu giữ nguyên như thế, ta sẽ không thể nào phân tích được, ta sẽ có một bước chuyển nho nhỏ là đồng bậc hóa để có thể phân tích bài toán, sử dụng điều kiện đầu bài $a+b=1$ ta có phép đồng bậc và phân tích như sau:

$$\begin{aligned}f(a,b)&=\frac{\left(5\sqrt{10}-14\right)}{27}(a+b)^6-ab\left(a^4+b^4\right)\\&=\frac{\left(5\sqrt{10}-14\right)\left[2\,a^2+\left(6-\sqrt{10}\right)ab+2b^2\right]\left[a^2-\left(\sqrt{10}+2\right)ab+b^2\right]^2}{54}\end{aligned}$$

Trong phần tiếp theo, ta quy ước ký hiệu $\sum f(a,b,c)$ là tổng đối xứng tính theo biến a, b, c đối với hàm số f.

3. Phân tích bình phương cho các bài toán ba biến số.

Như đã thấy ở mục trên, máy tính có sức mạnh áp đảo đối với lớp các bài toán hai biến số. Nhưng với lớp các bài toán ba biến số thì sao?

3.1. Phân tích trực tiếp

Với một số bài toán tương đối đơn giản ta có thể phân tích bằng hàm $factor$ như đối với các bài toán hai biến số ở trên.

Ví dụ 6 *Cho các số thực a, b, c. Chứng minh rằng:*

$$\sum a^4+\sum a^3b+\sum ab^3\geq 3\sum a^2bc$$

Lời giải. Ta có thể chứng minh dễ dàng bằng bất đẳng thức $AM-GM$, tuy nhiên ở đây là các biến thực. Với sự trợ giúp của Maple ta có phân tích như sau:

$$\sum a^4+\sum a^3b+\sum ab^3-3\sum a^2bc=\left(a^2+b^2+c^2-ab-bc-ca\right)(a+b+c)^2\geq 0$$

Đẳng thức xảy ra khi $a=b=c$ hoặc $a+b+c=0$.

Ví dụ 7 *Cho các số thực a,b,c thỏa mãn $a+b+c\geq 0$. Chứng minh rằng:*

$$\sum a^3b^2+\sum a^2b^3\geq \sum a^3bc+\sum a^2b^2c$$

Lời giải. Lại là một bài toán với các biến thực "khó chịu" khiến ta không thể áp dụng $AM-GM$ như thường lệ. Ta có phân tích như sau với sự trợ giúp của Maple:

$$\sum a^3b^2+\sum a^2b^3-\sum a^3bc+\sum a^2b^2c=\left(\sum a^2b^2-\sum a^2bc\right)(a+b+c)\geq 0$$

Đẳng thức xảy ra khi $a=b=c$ hoặc $a+b+c=0$.
Tuy nhiên ta sẽ không bàn nhiều về các bất đẳng thức dạng này.

3.2. Một vài kiểu phân tích hỗn hợp

Nếu cứ sử dụng một hàm $factor$ và có ngay kết quả sẽ gây nhàm chán và trên thực tế khi chứng minh một bất đẳng thức không bao giờ đơn giản như những bài toán trên.

Ví dụ 8 *Cho các số thực không âm x,y,z thỏa mãn $x+y+z=32$. Tìm giá trị lớn nhất của biểu thức sau:*

$$f(x,y,z)=x^3y+y^3z+z^3x$$

Phân tích. Cho $x=24,y=8,z=0$ ta có $f(x,y,z)=110592$ ta sẽ chứng minh đây là giá trị lớn nhất của $f(x,y,z)$. Tuy nhiên nếu cứ để nguyên và cố chứng minh thì rất khó, ta sẽ có một bước chuyển nho nhỏ là đồng bậc hóa bất đẳng thức này thành:

$$\frac{27}{256}(x+y+z)^4\geq x^3y+y^3z+z^3x$$

Tới đây, liệu bạn đã có ý tưởng hé mở? Rõ ràng cách phân tích trực tiếp sẽ không hiệu quả với bài toán có dấu bằng lệch tại biên như thế này. Nhưng hãy để ý lại dấu đẳng thức $x=3y,z=0$. Từ đây gợi cho ta phân tích bài toán về dạng:

$$(x-3y)^{2n}\,g(x,y,z)+z\,h(x,y,z)\geq 0.$$

Lời giải và thao tác máy tính.
Không mất tính tổng quát giả sử $x = \max\{x, y, z\}$
> `f:=27 (x + y + z)^4 - 256 (x^3y + y^3z + z^3x);`

$$f := 27(x + y + z)^4 - 256(x^3y + y^3z + z^3x)$$

Để dễ thao tác với bất đẳng thức này ta sẽ khai triển hoàn toàn bất đẳng thức với lệnh $expand$.
> `g:=expand(f);`

$$g := 27\,x^4 - 148\,x^3y + 108\,x^3z + 162\,x^2y^2 + 324\,x^2yz + 162\,x^2z^2 + 108\,xy^3 + 324\,xy^2z + 324\,xyz^2 - 148\,z^3x + 27\,y^4 - 148\,y^3z + 162\,y^2z^2 + 108\,yz^3 + 27\,z^4$$

Như trong bài ta đã biết đẳng thức xảy ra khi $z = 0$, thay $z = 0$ vào g bằng lệnh $subs$.
> `h:=subs(z=0,g);`

$$h := 27\,x^4 - 148\,x^3y + 162\,x^2y^2 + 108\,xy^3 + 27\,y^4$$

> `h1:=factor(h);`

$$h1 := (27\,x^2 + 14\,xy + 3\,y^2)\,(-3\,y + x)^2$$

Vậy là dự đoán của chúng ta đã đúng được một nữa. Ta sẽ tiếp tục với nữa còn lại.
> `g1:=g-h;`

$$g1 := 108\,x^3z + 324\,x^2yz + 162\,x^2z^2 + 324\,xy^2z + 324\,xyz^2 - 148\,z^3x - 148\,y^3z + 162\,y^2z^2 + 108\,yz^3 + 27\,z^4$$

> `factor(g1);`

$$z\,(108\,x^3 + 324\,x^2y + 162\,x^2z + 324\,xy^2 + 324\,xyz - 148\,xz^2 - 148\,y^3 + 162\,y^2z + 108\,yz^2 + 27\,z^3)$$

Dễ thấy bất đẳng thức này luôn đúng. Thật vậy do:

$$324x^2y \geq 148y^3 \text{ và } 162x^2z^2 \geq 148xz^3.$$

Ta có thể viết lại lời giải ngắn gọn như sau:
Không mất tính tổng quát giả sử $x = \max\{x, y, z\}$, ta có:

$$\begin{aligned} f :=& 27(x + y + z)^4 - 256(x^3y + y^3z + z^3x) \\ =& \left(27\,x^2 + 14\,xy + 3\,y^2\right)(-3\,y + x)^2 + \\ &+ z\big[108x^3 + 176x^2y + 14x^2z + 176xy^2 + 324xyz + (148x^2z - 148xz^2) + \\ &+ (148xy^2 - 148y^3) + 162y^2z + 108yz^2 + 27z^3\big] \geq 0 \end{aligned}$$

Đúng do $x = \max\{x, y, z\}$. Đẳng thức xảy ra khi $x = 24, y = 8, z = 0$.

Ví dụ 9 *Cho các số thực dương x, y, z. Chứng minh rằng:*

$$\left[\left(x^2+y^2+z^2\right)(x+y+z)+3xyz\right]^2 \geq 2\left[x^2+y^2+z^2+(x+y+z)^2\right]\left[x^3y+y^3z+z^3x+xyz(x+y+z)\right]$$

Lời giải. Việc phân tích cụm đa thức cồng kềnh này thành tổng các bình phương tương đối khó vì sự xuất hiện của cụm đại lượng $x^3y+y^3z+z^3x$ trong vế phải khiến khiến việc phân tích trở nên khó khăn và gần như "phá sản". Tuy nhiên với một chút khéo léo ta có phân tích như sau:

$$\begin{aligned}&\left[\left(x^2+y^2+z^2\right)(x+y+z)+3xyz\right]^2 \\ &\quad -2\left[x^2+y^2+z^2+(x+y+z)^2\right]\left[x^3y+y^3z+z^3x+xyz(x+y+z)\right] \\ &\quad =\left(x^3-x^2y+x^2z-xy^2+xyz+xz^2-y^3-y^2z-yz^2+z^3\right)^2+ \\ &\quad +4(x-y)(y-z)(y+z)z\left(x^2+xy+xz+y^2+yz+z^2\right)\geq 0\end{aligned}$$

Với y là số nằm giữa x và z. Còn về làm sao phân tích được, xin dành lại cho bạn đọc như một bài tập rèn luyện.

Qua hai ví dụ minh họa ở trên, hẳn bạn sẽ có chút khó chịu vì không có điểm chung giữa hai bài toán trên?

4. Phương pháp S.O.S, một tiêu chuẩn chung

Trong phần này ta sẽ nói khái quát về phương pháp S.O.S. Có thể xem là một tiêu chuẩn "chung" cho việc phân tích các bất đẳng thức về dạng tổng các bình phương.

4.1. Dạng chính tắc và một vài tiêu chuẩn của phương pháp S.O.S

4.1.1. Dạng chính tắc

Về cơ bản khi đứng trước một bất đẳng thức bất kì của ba biến a, b, c ta sẽ tìm cách đưa chúng về dạng tổng của các bình phương $(a-b)^2, (b-c)^2, (c-a)^2$ kí hiệu:

$$S_c(a-b)^2+S_a(b-c)^2+S_b(c-a)^2\geq 0.$$

Phần đưa về dạng chính tắc trên là bước đầu tiên trong cách sử dụng phương pháp S.O.S. Nếu may mắn có được S_a, S_b và S_c đều dương thì bài toán được chứng minh. Tuy nhiên không phải lúc nào ta cũng may mắn như thế.

4.1.2. Định lý S.O.S

Xét biểu thức:

$$S = f(a,b,c) = S_a(b-c)^2 + S_b(c-a)^2 + S_c(a-b)^2,$$

Trong đó $S_a,\ S_b,\ S_c$ là các hàm số của a, b, c, khi đó

1. Nếu $S_a,\ S_b,\ S_c \geq 0$ thì $S \geq 0$.
2. Nếu $a \geq b \geq c$ và $S_b,\ S_b + S_c,\ S_b + S_a \geq 0$ thì $S \geq 0$.
3. Nếu $a \geq b \geq c$ và $S_a,\ S_c, S_a + 2S_b,\ S_c + 2S_b$ thì $S \geq 0$.
4. Nếu $a \geq b \geq c$ và $S_b,\ S_c \geq 0,\ a^2S_b + b^2S_a \geq 0$ thì $S \geq 0$.
5. Nếu $S_a + S_b + S_c \geq 0$ và $S_a\,S_b + S_b\,S_c + S_c\,S_a \geq 0$ thì $S \geq 0$

4.2. Một vài bài toán minh họa

Tiếp theo, tác giả xin giới thiệu một số bài toán khá thú vị, có kết hợp dùng chương trình *hsos* mà tác giả đã tự xây dựng trên nền Maple để giải quyết. Ý tưởng thực hiện và cách vận hành của nó sẽ giới thiệu ở mục sau.

Bài toán 1 *Cho các số thực a, b, c không âm sao cho $ab + bc + ca > 0$. Chứng minh rằng:*

$$\sqrt{\frac{a^2+bc}{b^2+bc+c^2}} + \sqrt{\frac{b^2+ca}{c^2+ca+a^2}} + \sqrt{\frac{c^2+ab}{a^2+ab+b^2}} \geq \sqrt{6}$$

Lời giải. Đặt

$$A = \sqrt{\frac{a^2+bc}{b^2+bc+c^2}} + \sqrt{\frac{b^2+ca}{c^2+ca+a^2}} + \sqrt{\frac{c^2+ab}{a^2+ab+b^2}},$$

$$B = (a^2+bc)^2(b^2+bc+c^2)(2a+b+c)^3 + (b^2+ca)(c^2+ca+a^2)(2b+c+a)^3 + (c^2+ab)(a^2+ab+b^2)(2c+a+b)^3$$

Áp dụng bất đẳng thức Holder ta có

$$A^2B \geq \left[(a^2+bc)(2a+b+c) + (b^2+ca)(2b+c+a) + (c^2+ab)(2c+a+b)\right]^3$$

Do đó ta chỉ cần chứng minh

$$\left[\sum (a^2+bc)(2a+b+c)\right]^3 \geq 6\sum (a^2+bc)^2(b^2+bc+c^2)(2a+b+c)^3$$

Đến đây bậc của bất đẳng thức khá cao và khá khó xử lí, và một lần nữa máy tính lại chứng tỏ được sức mạnh. Sử dụng chương trình $hsos$, ta có thể phân tích bất đẳng thức trên thành dạng S.O.S như sau:

$$S_c(a-b)^2 + S_b(c-a)^2 + S_a(b-c)^2 \geq 0$$

Trong đó

$$S_c = 2(a^7+b^7) + 9c(a^6+b^6) + 7ab(a^5+b^5) + 36abc(a^4+b^4) + \left(9a^2b^2 + 27abc^2\right)(a^3+b^3)$$
$$+ 60a^2b^2c(a^2+b^2) + 3a^3b^3(a+b) + 72a^2b^2c^2(a+b) + 72a^3b^3c + 6a^2b^2c^3$$

Tương tự với S_a, S_b.
Máy tính đưa ra phân tích này trong $1.484s$[1], mặt khác dễ thấy $S_a,\ S_b,\ S_c \geq 0$ do $a,\ b,\ c \geq 0$.
Chứng minh hoàn tất. Đẳng thức xảy ra khi $a = b = c$.

Bài toán 2 *Cho các số thực dương a, b, c hãy chứng minh bất đẳng thức sau luôn đúng:*

$$f(a,b,c) = a^3 + b^3 + c^3 + 3\,abc - ab\,(a+b) - bc\,(b+c) - ca\,(c+a) \geq 0$$

Lời giải. Sử dụng phần mềm $hsos$ được viết trên nền Maple ta thu được phân tích như sau:

$$f(a,b,c) = (a+b-c)\,(a-b)^2 + (b+c-a)\,(b-c)^2 + (c+a-b)\,(c-a)^2$$

Máy tính đưa ra phân tích này trong $0.188s$, mặt khác không phải $S_a,\ S_b,\ S_c$ luôn dương.
Không mất tính tổng quát giả sử $a \geq b \geq c$, ta có

$$S_b = a + c - b \geq 0 \text{ và } S_b + S_c = 2a \geq 0 \text{ và } S_b + S_a = 2c \geq 0$$

nên bất đẳng thức này đúng theo tiêu chuẩn 2.
Đẳng thức xảy ra khi $a = b = c$ hoặc $a = b, c = 0$ cùng các hoán vị tương ứng.

4.3. Vài dòng về chương trình $hsos$

Trong mục này ta sẽ tìm hiểu sơ lược về chương trình $hsos$ và ý tưởng thuật toán vận hành nó như thế nào.

4.3.1. Giới thiệu khái quát về chương trình $hsos$

Chương trình $hsos$ được viết bằng ngôn ngữ lập trình Maple bởi tác giả và một số "đồng nghiệp" người Trung Quốc vào năm 2009. Phiên bản 1.0 của chương trình chỉ hoạt động đối với các bất đẳng thức dạng đa thức, đến phiên bản 2.0 mới hoạt động được với các bất đẳng thức dạng phân thức. Phiên bản hoàn chỉnh 3.0 hoàn chỉnh vào năm 2011. Hiện chương trình vẫn còn trong giai đoạn phát triển, phiên bản tiếp theo tập trung vào việc phát triển thuật toán cho các bài toán dạng căn. Tuy nhiên, vẫn còn trong giai đoạn kiểm thử nên tác giả chưa thể công bố rộng rãi.

[1]Tất cả các tính toán có liên quan đến thời gian đều được thực hiện trên cùng một máy tính sử dụng bộ xử lý Intel(R) Core(TM) i7-4510U 2.00GHz, bộ nhớ Ram 8Gb.

4.3.2. Thuật toán

Bước một: Kiểm tra điều kiện cần và đủ của $f(a,b,c)$:

+ Điều kiện cần: $f(a,a,a)=0$.
+ Điều kiện đủ: $f(a,b,c)$ là đa thức đồng bậc và đối xứng.

Nếu thỏa mãn cả hai điều kiện ta đi đến bước hai. Nếu không kết thúc.
Bước hai: Khai sinh đa thức có bậc $n-2$, với n là bậc của đa thức $f(a,b,c)$ cần phân tích gắn kèm với hệ số tự do.
Bước ba: Giải hệ tự do, sau đó đưa ra kết quả nếu hệ tự do có nghiệm.

4.3.3. Ví dụ minh họa

Ví dụ. Hãy thực hiện phép phân tích S.O.S cho các đa thức sau đây:

1. $a^3+b^3+c^3-(a^2b+b^2c+c^2b)$
2. $a^2+b^3+c^4-ab-a^2b-a^3c$
3. $a^3+b^3+c^3-a^2b-b^2c-c^2a$

Phân tích.

1. Bước một: Đa thức không có dạng hoán vị vòng quanh. Phân tích kết thúc.
2. Bước một: Đa thức không có dạng hoán vị vòng quanh. Phân tích kết thúc.
3. Bước một: Đa thức này thỏa mãn cả điều kiện cần và đủ, nên ta sẽ thực hiện phân tích S.O.S cho nó:

   Bước hai: Sinh đa thức tự do $f(a,b,c)$ có bậc $n=3-2=1$ là

   $$f_1(a,b,c)=m_1a+m_2b+m_3c$$

   Từ đây ta có dạng S.O.S cần tìm là:

   $$f_{sos}=(am_1+bm_2+cm_3)(a-b)^2+(am_3+bm_1+cm_2)(b-c)^2+(am_2+bm_3+cm_1)(c-a)^2$$

   Giải phương trình $f(a,b,c)=f_{sos}$ ta có nghiệm $(m_1,m_2,m_3)=(2,1,0)$.
   Vậy ta được

   $$a^3+b^3+c^3-a^2b-b^2c-c^2a=(2a+b)(a-b)^2+(2b+c)(b-c)^2+(2c+a)(c-a)^2$$

5. Lại vẫn là các phép phân tích bình phương?

Bạn cảm thấy có chút chán nản về các phép phân tích bình phương này? Chúng đều mơ hồ và rất khó để nắm bắt, thậm chí với phương pháp S.O.S ta vẫn phải chứng minh những bất đẳng thức trung gian cực kỳ phức tạp dù đã giảm đi hai bậc so với ban đầu. Nhưng vẫn không thể phủ nhận sự hấp dẫn của phép phân tích bình phương trong chứng minh bất đẳng thức. Đẹp, hoàn hảo, trong sáng và dễ hiểu. Bài toán phân tích về các dạng tổng bình phương bài toán thứ 17 trong số 23 bài toán của Hilbert:

Cho một đa thức nhiều biến luôn nhận giá trị không âm trên trường số thực, liệu nó có thể được biểu diễn dưới dạng tổng các bình phương của các hàm hữu tỉ?

Lời giải khẳng định đã được chứng minh năm 1927 bởi Emil Artin. Sau đó Charles Delzell đã tìm ra một thuật toán cho bài toán này. Tuy nhiên lời giải lại sử dụng các kiến thức về toán cao cấp, không tiện trình bày trong bài báo này. Bù lại ta sẽ nghiên cứu một "giải thuật" khác đơn giản hơn nhưng đều hiệu quả. Phần này của bài báo xin trình bày sơ lược về công trình nghiên cứu của giáo sư SUI Zhen-lin tính [2] cho việc phân tích một đa thức bất kì về dạng tổng các bình phương dựa trên thuật toán "sinh đa thức tổ hợp".

5.1. Vài dòng về *lpsos* và *sosany*

Chương trình *lpsos* do giáo sư SUI Zhen-lin tự xây dựng thuật toán và viết trên nền ngôn ngữ lập trình Maple, còn *sosany* do tác giả xây dựng lại dựa trên thuật toán của giáo sư SUI Zhen-lin cung cấp. Tuy hai chương trình đều được viết trên nền ngôn ngữ lập trình Mapple tuy nhiên hiệu năng tính toán và độ hiệu quả của hai chương trình là khác nhau do "trình độ" và kỹ năng "lập trình" của hai tác giả là khác nhau.

5.2. Một vài bài toán minh họa

Bài toán 1 *Cho các số thực x, y, z chứng minh rằng:*

$$(x-y)^4+(y-z)^4+(z-x)^4+\frac{9}{2}yz(y-z)^2\geq 0$$

Lời giải. Ta có phân tích sau:

$$\sum(x-y)^4+\frac{9}{2}yz(y-z)^2=\frac{9}{8}(y-z)^2(y+z)^2+\frac{3}{4}(y-z)^2(2x-y-z)^2+\frac{1}{8}(2x-y-z)^4\geq 0.$$

[2] Hiện đang giảng dạy tại Cao đẳng dầu mỏ nâng cao Shengli, Đông Dinh, Sơn Đông.

Chương trình $lpsos$ cho ra kết quả sau $3.812s$.
Chương trình $sosany$ cho ra kết quả sau $6.12s$.

Bài toán 2 *Cho các số thực dương a, b, c chứng minh rằng:*

$$\frac{a}{b}+\frac{b}{c}+\frac{c}{a}+1 \geq \sqrt{\frac{11(a^2+b^2+c^2)}{ab+bc+ca}+5}$$

Lời giải. Ta có phân tích như sau:

$$\left(\frac{a}{b}+\frac{b}{c}+\frac{c}{a}+1\right)^2-\frac{11\left(a^2+b^2+c^2\right)}{ab+ca+bc}-5$$

$$=\frac{1}{4}\left[\frac{a\left(12ac+3b^2+4bc\right)(b-c)^2}{bc^2\left(ab+ac+bc\right)}+\frac{b\left(12ab+4ac+3c^2\right)(c-a)^2}{ca^2\left(ab+ac+bc\right)}+\frac{c\left(3a^2+4ab+12bc\right)(a-b)^2}{ab^2\left(ab+ac+bc\right)}\right]$$
$$+\frac{1}{4}\left[\frac{a\left(2ac-b^2-bc\right)^2}{bc^2\left(ab+ac+bc\right)}+\frac{b\left(2ab-ac-c^2\right)^2}{ca^2\left(ab+ac+bc\right)}+\frac{c\left(-a^2-ab+2bc\right)^2}{ab^2\left(ab+ac+bc\right)}\right]\geq 0$$

Chương trình $lpsos$ cho ra kết quả sau $4.344s$.
Chương trình $sosany$ cho ra kết quả sau $12.364s$.

Bài toán 3 *Cho các số thực dương x, y, z, chứng minh rằng:*

$$\left(x^2+2z+1\right)\left(y^2+2x+1\right)\left(z^2+2y+1\right)\geq\frac{64}{9}.(x+y+z)(xy+zx+yz)$$

Lời giải. Ta có phân tích như sau:

$$\begin{aligned}&\left(x^2+2z+1\right)\left(y^2+2x+1\right)\left(z^2+2y+1\right)-\frac{64}{9}.(x+y+z)(xy+zx+yz)\\&=2x\left(z^2+1\right)(x-1)^2+2y\left(x^2+1\right)(y-1)^2+2z\left(y^2+1\right)(z-1)^2+\\&+\frac{4}{9}.z(9y+2)(x-y)^2+\frac{4}{9}.x(9z+2)(y-z)^2+\frac{4}{9}.y(9x+2)(z-x)^2+\\&+(xyz-1)^2+3(xy+xz+yz-x-y-z)^2+\\&+(x-1)^2(y-z)^2+(y-1)^2(z-x)^2+(z-1)^2(x-y)^2\geq 0\end{aligned}$$

Chương trình $lpsos$ cho ra kết quả sau $0.75s$.
Chương trình $sosany$ cho ra kết quả sau $2.422s$.

Bài toán 4 *Cho các số thực dương a, b, c thỏa mãn $a+b+c=3$. Chứng minh rằng:*

$$\sqrt{\frac{a}{2+b}}+\sqrt{\frac{b}{2+c}}+\sqrt{\frac{c}{2+a}}\leq\sqrt{3}$$

Lời giải. Sử dụng bất đẳng thức Cauchy-Schwarz ta có:

$$\left(\sum\sqrt{\frac{a}{2+b}}\right)^2\leq\sum\frac{a}{1+a}.\sum\frac{1+a}{2+b}$$

Từ đây ta sẽ cố gắng chứng minh:

$$\sum\frac{a}{1+a}.\sum\frac{1+a}{2+b}\leq 3$$

Thật vậy ta có:

$$3-\sum\frac{a}{1+a}\cdot\sum\frac{1+a}{2+b}=$$
$$\sum\frac{\sum[a(7c^2+3c+2)(ab-1)^2+(bc+2a+4)(a-1)^2(b-c)^2]}{\prod(1+a).\prod(2+a)}\geq 0$$

Chương trình $lpsos$ cho ra kết quả sau $2.01s$.
Chương trình $sosany$ cho ra kết quả sau $3.12s$.

Bài toán 5 *Cho các số thực $x, y, z>0$. Chứng minh rằng:*

$$\sum\frac{(z+x)(x+y)}{(y+z)(3x^2+4yz)}\geq\frac{18}{7(x+y+z)}$$

Lời giải. Ta có phân tích sau:

$$\sum\frac{(z+x)(x+y)}{(y+z)(3x^2+4yz)}-\frac{18}{7(x+y+z)}=$$
$$\frac{1}{126}\cdot\frac{1}{(x+y+z)\prod(x+y)\cdot\prod(3x^2+4yz)}\sum z(1008x^3y+1191x^2y^2+19x^2yz$$
$$+1008xy^3+19xy^2z+420xyz^2+66z^4)(x-y)^4$$
$$+\frac{1}{63}\cdot$$
$$\frac{1}{(x+y+z)\prod(x+y)\cdot\prod(3x^2+4yz)}\sum z(420x^2z^2+254xz^3+19y^4)(x-y)^2(x-2z)^2$$
$$+\frac{1}{63}\cdot$$
$$\frac{1}{(x+y+z)\prod(x+y)\cdot\prod(3x^2+4yz)}\sum z(19x^4+420y^2z^2+254yz^3)(x-y)^2(y-2z)^2\geq$$
$$0$$

Chương trình $lpsos$ cho ra kết quả sau $8s$.
Chương trình $sosany$ cho ra kết quả sau $842.12s$.
Trước khi chuyển qua phần tiếp theo của bài viết là phân tích kỹ hơn về cách xử lý đằng sau các dòng biến đổi ở trên, liệu bạn có chút ấn tượng gì với các bài toán và lời giải trình bày ở trên?

5.3. Thuật toán SUI

Về cơ bản mà nói thuật toán của SUI gồm có 5 bước cơ bản:

1. Bước 1: Phỏng đoán đa thức.
2. Bước 2: Khai sinh tập biến.
3. Bước 3: Tạo nhân tử.
4. Bước 4: Tổ hợp nhân tử và gắn hệ số.
5. Bước 5: Giải hệ và đưa ra kết quả.

Khác với thuật toán của *hsos* vốn chỉ áp dụng cho các đa thức đối xứng thuần nhất, thuật toán SUI áp dụng cho một đa thức bất kì nên không cần điều kiện cần và đủ như hsos.

5.4. Áp dụng vào bài toán phân tích bình phương

Để cho dễ hiểu ta sẽ thao tác trực tiếp trên một bài toán cụ thể, xét đa thức:

$$f(x,y,z) = (x-y)^4 + (y-z)^4 + (z-x)^4 + \frac{9}{2}yz(y-z)^2$$

Bước 1: Đây là một đa thức bậc 4 nếu muốn phân tích bài toán này về dạng tổng các bình phương không âm ta có thể dễ dàng phỏng đoán được dạng của phân tích mà ta cần hướng đến có dạng:

$$\sum_{n=1}^{\infty}(f_n(x,y,z))^4 + \sum_{n=1}^{\infty}(i_n(x,y,z))^2(k_n(x,y,z))^2$$

Bước 2: Khai sinh tập biến:
Như đã thu được ở bước 1, tổng bình phương của đa thức này là tích của các đại lượng bậc một tạo nên, cho nên tập biến của chúng ta sẽ đơn giản chỉ gồm:

$$x, y, z$$

Bước 3: Dễ thấy đẳng thức xảy ra khi và chỉ khi $x = y = z$. Ta ước lượng nhân tử của phép phân tích có khả năng sẽ chứa các đại lượng sau:

$$x, y, z, x-y, y-z, z-x$$

Bước 4: Tổ hợp và tạo các nhân tử, với sự trợ giúp của Maple ta có tổ hợp sau đây:
$tohop := [x, y, z, -x, -y, -z, -2x+y, -2x+z, -x-y, -x+y, -x-z, x-y, x+y, x-z, x+z, 2x-y, 2x-z, -2y+x, -2y+z, -y-z, -y+z, y-z, y+z, 2y-x, 2y-z, -2z+$

$x, -2z+y, z-x, 2z-x, 2z-y, -2x+y+z, -x-y+z, -x+y-z, -x+2y-z, x-2y+z, x-y+z, x+y-z, 2x-y-z, -y+x-z, -y+2z-x, y-2z+x, y+z-x]$
Với vài dòng code đơn giản Maple cho ta một đa thức được tạo nên từ *tohop* như sau:

$$M_{55}\big((y+z-x)\big)^2(x+y)^2 + M_{56}\big((y+z-x)\big)^2(x-z)^2 + M_{57}\big((y+z-x)\big)^2(x+z)^2$$
$$+ M_{58}\big((y+z-x)\big)^2(2\,x-y)^2 + M_{59}\big((y+z-x)\big)^2(2\,x-z)^2 + \cdots$$
$$+ M_{79}\big((-y+x-z)\big)^2(-y+2\,z-x)^2 + M_{80}\big((-y+x-z)\big)^2(y-2z+x)^2$$
$$+ M_{81}\big((-y+x-z)\big)^2(y+z-x)^2 + \cdots$$
$$+ M_{10}\big((y)\big)^2(-2x+z)^2 + M_{11}\big((y)\big)^2(-x-y)^2$$

Bước 5: Bằng việc giải hệ trên và chọn kết quả phù hợp ta đưa ra được kết quả như sau:

$$\sum (x-y)^4 + \frac{9}{2}yz(y-z)^2 = \frac{9}{8}(y-z)^2(y+z)^2 + \frac{3}{4}(y-z)^2(2x-y-z)^2 + \frac{1}{8}(2x-y-z)^4 \geq 0$$

Như các bạn đã thấy ở trên đa thức được tạo ra có $(42^2-42)/2 = 861$ phần tử khác nhau, nói nôm na ta phải giải một hệ có 861 biến số khác nhau. Một con số khủng khiếp, tuy nhiên nói đi thì cũng phải nói lại, biến số tuy nhiều nhưng chỉ là hệ bậc nhất thuần nhất - "một mảnh đất" đã được khai thác triệt để.

6. Nhận xét

6.1. Lợi thế đến từ máy tính và phần mềm

Sử dụng một ít kiến thức Toán học cơ bản và tận dụng lợi thế số một của máy tính là khả năng tính toán nhanh và chính xác, ta đã có thể giải quyết được một bài toán khó, đó là phân tích một đa thức không âm trên trường thực về các dạng tổng bình phương không âm.

Ngoài máy tính thì các phần mềm toán học cũng đóng vai trò cực kì quan trọng. Kể từ sau khi các thế hệ máy tính cá nhân ra đời, rồi đến hệ thống World Wide Web thì việc ra đời của bộ phần mềm: Maple, Mathematica, Matlab và các phần mềm tính toán tương tự đã ảnh hưởng không hề nhỏ đến việc học và làm toán trên toàn thế giới. Với thư viện các hàm toán học phong phú và không ngừng phát triển qua từng năm, các phần mềm nói trên ngày càng hoàn thiện hơn không chỉ ứng dụng trong toán học mà còn là công cụ đắc lực cho các nhà khoa học thuộc nhiều lĩnh vực khác nhau như vật lý, hóa học, điện...

Với chúng, ta có thể tiết kiệm rất nhiều thời gian vì không phải viết các hàm riêng cho mình nữa mà có thể áp dụng trực tiếp thuật toán theo ý của mình. Tất nhiên, nó vẫn đòi hỏi phải có một kiến thức tương đối về lập trình.

6.2. Những hạn chế

Dù có tốc độ tính toán nhanh và chính xác, tuy nhiên nếu "thuật toán" không tối ưu vẫn không thể tận dụng được hết sức mạnh của máy tính. Mặt khác, các phần mềm toán học đều được phát triển dựa trên một ngôn ngữ lập trình trung gian như Java, nên tốc độ thực thi vẫn còn chậm.

Khi bài toán này được giải quyết thì một bài toán khác lại ra đời, giờ ta có thể viết được một đa thức không âm trên trường thực về các dạng tổng bình phương, nhưng làm sao ta biết được liệu đa thức đó có luôn dương trên trường thực để mà viết? Thật may mắn, bài toán này đã được giải quyết hoàn toàn bởi Wen-Tsun Wu và các đồng nghiệp. Giáo sư Yang Lu và các đồng nghiệp của mình đã dựa trên "giải thuật" của Wu và viết nên chương trình $bottema2009$" cũng là phần mềm hoạt động trên nền Maple. Tuy nhiên do viết trên nền Maple cũ chương trình không tương thích trên các phiên bản Maple mới hiện nay do có sự thay đổi về cú pháp lập trình ở các phiên bản. Đến năm 2014 thì được chính tác giả viết lại toàn bộ mã nguồn và hoạt động trên tất cả các phiên bản của Maple[3]. Tuy nhiên do khuôn khổ bài báo có hạn, tác giả sẽ trình bày về chương trình này trong một bài báo khác.

Một trong những hạn chế khác nữa chính là Bùng nổ tổ hợp[4] như đã thấy ở trên một đa thức bậc bốn ta đã phải làm việc với 861 biến tự do. Bài toán số 5 có bậc 9 ngốn của máy tính tận $14p30$ mới cho ra kết quả. Rõ ràng trong tương lai ta cần cải thiện thuật toán nhiều hơn nữa. Tổng hợp các khuyết điểm ở trên ta thấy chương trình có sự chậm trễ đến từ ba nguồn khác nhau:

Độ trễ = Time(Thuật toán chưa tối ưu) + Time(Ngôn ngữ trung gian) + Time(Bùng nổ tổ hợp)

Nếu khắc phục được những lỗi này trong tương lai chương trình sẽ hiệu quả và hoạt động nhanh hơn rất nhiều.

Mặt khác xuyên suốt bài báo ta chỉ làm việc với các bất đẳng thức dạng đa thức và phân thức, chỉ có một ví dụ dạng căn, nhưng chúng ta đã xử lý theo hướng bình phương để phá căn. Việc phát triển thuật toán cho bất đẳng thức dạng căn là vô cùng phức tạp, tuy nhiên trong tương lai sẽ có những thuật toán cho vấn đề này.

7. Giới thiệu một chương trình cùng loại

Vì lý do đã nêu ở trên nên tác giả chưa thể giới thiệu mã nguồn của chương trình $hsos$. Thay vào đó, tác giả xin giới thiệu mã nguồn của chương trình cùng loại (cũng viết trên nền Maple) do tác giả xây dựng để giải quyết các bài về các bất đẳng thức đa thức bậc bốn ba biến:

[3]Phiên bản Maple mới nhất cho đến khi bài báo được viết là 2016.1

[4]Bùng nổ tổ hợp là thuật ngữ dùng để mô tả sự tăng nhanh và đột biến của một hàm số do phải tính toán hết các trường hợp tổ hợp khác nhau.

```
print("=================================================");
print("prove4");
print("Chuong trinh duoc viet boi Nguyen Quoc Anh");
print("Day la mot chuong trinh ma nguon mo. (Open source code.)");
print("bdtilove@live.com");
print("[[[[3.0]]]]");
print("Copyright(C) 2013-2016");
print("[xprove4,yprove4]");
print("=================================================");
#################################################################
sgm:=proc(expr)
  local rap,ex2,ex3,ex:
    rap:={a=b,b=c,c=a}:
  ex2:=subs(rap,expr):
  ex3:=subs(rap,ex2):
  ex:=expr+ex2+ex3:
  RETURN(ex)
end:
#################################################################
pro:=proc(expr)
  local rap,ex2,ex3,ex:
    rap:={a=b,b=c,c=a}:
  ex2:=subs(rap,expr):
  ex3:=subs(rap,ex2):
  ex:=expr*ex2*ex3:
  RETURN(ex)
end:
#################################################################
prove4:=proc(ineq)
 local exp,i,sj,ff,tt,ff1,g,f:
 if whattype(ineq)= `=` then print("This is not an inequality!")
    else
 g:=rhs(ineq)-lhs(ineq):f:=convert(g,`+`):sj:=time():exp:={}:tt:=0:
 ff1:=unapply(f,a,b,c):
 for i from 2 to nops([op(expand(numer(f)))]) do
  if degree([op(expand(numer(f)))][i]/subs(a=1,b=1,c=1,
  [op(expand(numer(f)))][i]))<>degree([op(expand(numer(f)))][1]
  /subs(a=1,b=1,c=1,[op(expand(numer(f)))][1])) then tt:=tt+1:fi:od:

      if   tt>0 then print("ERROR, this polynomial is not
         homonegeous!"):
      elif tt=0 and nops(expand({ff1(a,b,c),ff1(a,c,b)
         ,ff1(b,c,a),ff1(c,a,b),ff1(c,b,a),ff1(b,a,c)}))>2 then
```

```
        print("ERROR,This form is not circle symmetric!")
      elif tt=0 and
        nops(expand({ff1(a,b,c),ff1(b,c,a),ff1(c,a,b)}))=1 then if
        type(f,symmfunc(a,b,c)) then print("This is a symmetric
        polynomial!"):check1(ineq):else print("This is a cyclic
        symmetric polynomial!"):check2(ineq):fi:fi:fi:
end:
#################################################################
solve01:=proc(ff1)
 local m,n,p,g,gg:
  m:=coeff(subs({a=a,b=1,c=1},ff1),a^4);
  n:=coeff(subs({a=a,b=1,c=0},ff1),a^2);
  p:=coeff(subs({a=a,b=1,c=0},ff1),a^3);
  g:=coeff(subs({a=a,b=0,c=1},ff1),a^3);
  if subs({a=a,b=a,c=a},ff1)=0 and 3*m*(m+n)-p^2-p*g-g^2>=0 and m>0
     and p^2+p*g+g^2<>0 then
   gg:=sgm((3*m*(a^2-b^2)+(p-g)*a*b-(2*p+g)*b*c+(p+2*g)*c*a)^2/(18*m))
   +sgm((3*m*(m+n)-p^2-p*g-g^2)*((p-g)*a*b-(2*p+g)*b*c
   +(p+2*g)*c*a)^2/(18*m*(p^2+p*g+g^2))):
  else print("Cant give a solution."):fi;
end:
#################################################################
solve02:=proc(ff1)
 local k,l,o,ff7,ff6,Mm,i,j,gg:
 ff7:=sgm((k*a+l*b+o*c)^4);
 Mm:=solve(subs(a=1,b=1,c=1,
 {op(collect(ff1-ff7,[a,b,c],distributed))}),{k,l,o});
 gg:=remove(hastype, {Mm}, {And(complexcons, Not(realcons)),
    specfunc(anything, RootOf)});
 if gg<>{} then subs(gg[1], ff7) else print("Cant give a
    solution."):fi
end:
#################################################################
solve03:=proc(ff2)
 local m1,m2,m3,m4,m5,deg2,g,amu4,amu3b,amu3c,amu2bmu2,amu2bc,gg:
 m1 := simplify(coeff(subs({a = a, b = 1, c = 1}, ff2), a^4));
 m2 := simplify(coeff(subs({a = a, b = 1, c = 0}, ff2), a^2));
 m3 := simplify(coeff(subs({a = a, b = 1, c = 0}, ff2), a^3));
 m4 := simplify(coeff(subs({a = a, b = 0, c = 1}, ff2), a^3));
 m5 := simplify(coeff(subs({a = a, b = 1, c = 1}, ff2), a^2)-2*m2);
 amu4 :=(x^2+y^2+z^2);
 amu3b :=2*(x*m+z*p+y*n);
 amu3c :=2*(x*p+z*n+y*m);
```

```
 amu2bmu2 :=(2*x*y+2*y*z+2*z*x+m^2+n^2+p^2);
 amu2bc := 2*(x*n+m*p+z*m+n*p+y*p+m*n);
 g := sgm((x*a^2+y*b^2+z*c^2+m*a*b+n*b*c+p*c*a)^2);
 deg2 := solve({x=1,amu2bc = m5, amu3b = m3, amu3c = m4, amu4 = m1,
    amu2bmu2 = m2}, {m, n, p, x, y, z});
 gg:=remove(hastype, {deg2}, {And(complexcons, Not(realcons)),
    specfunc(anything, RootOf)});
  if gg<>{} then subs(gg[1], g) else print("Cant give a
     solution."):fi:
 end:
#####################################################################
solve04:=proc(ff)
 local k,l,ff7,ff5,Mm,gg:
 ff7:=k*(sgm(a^2)-l*sgm(a*b))^2;
 Mm:=solve(subs(a=1,b=1,c=1,
 {op(collect(ff-ff7,[a,b,c],distributed))}),{k,l});
 gg:=remove(hastype, {Mm}, {And(complexcons, Not(realcons)),
    specfunc(anything, RootOf)});
 if gg<>{} then subs(gg[1], ff7) else print("Cant give a
    solution."):fi:
end:
#####################################################################
check1:=proc(ineq)
 local ff1;
 ff1:=convert(rhs(ineq)-lhs(ineq),`+`);
   if solve(subs(b=1,c=1,ff1)>=0,a)=a and
      solve(subs(b=0,c=0,ff1)>=0,a)=a then print("This inequality is
      true! Try to solving:
      "):solve01(ff1),solve02(ff1),solve03(ff1),solve04(ff1);
     else print("This inequality is false!"):fi:
end:
#####################################################################
check2:=proc(ineq)
 local m,r,p,q,s,ff2,ff1:
   ff1:=convert(rhs(ineq)-lhs(ineq),`+`);
   m:=coeff(subs({a=a,b=1,c=1},ff1),a^4);
   ff2:=expand(ff1/m);
   r:=coeff(subs({a=a,b=1,c=0},ff2),a^2);
   p:=-coeff(subs({a=a,b=1,c=0},ff2),a^3);
   q:=-coeff(subs({a=a,b=0,c=1},ff2),a^3);
   s := simplify(coeff(subs({a = a, b = 1, c = 1}, ff2), a^2)-2*r);
   if s>=p+q-r-1 and s<=2*(r+1)+p+q-p^2-p*q-q^2 then print("This
      inequality is true! Try to solving:
```

```
      "):solve01(ff1),solve02(ff1),solve03(ff1),solve04(ff1);
  else print("This inequality is false!"):fi:
end:
```

8. Lời cảm ơn

Cuối cùng tác giả xin gửi lời cảm ơn sâu sắc đến giáo sư SUI-Zhen Lin vì đã cung cấp thuật giải để tác giả viết bài báo này. Cám ơn em Lê Hoàng Long, THPT Võ Nguyên Giáp, Quảng Bình vì đã chỉnh sửa $Latex$ cho bài báo này. Cám ơn anh Hoàng Ngọc Thế và anh Nguyễn Ngọc Giang cùng các anh, em ở Diễn đàn Toán học VMF đã dành thời gian đọc và góp ý cho bài báo hoàn thiện hơn.

Tài liệu

[1] Yang Lu, *Recent advances in automated theorem proving on inequalities*, Journal of Computer Science and Technology, September 1999, Volume 14, Issue 5, pp 434-446.

[2] SHUI-Zhen Lin, *Squares polynomial decomposition.*, Shengli Oilfield Advanced Training College,Dongying,Shandong,257000,P.R.China

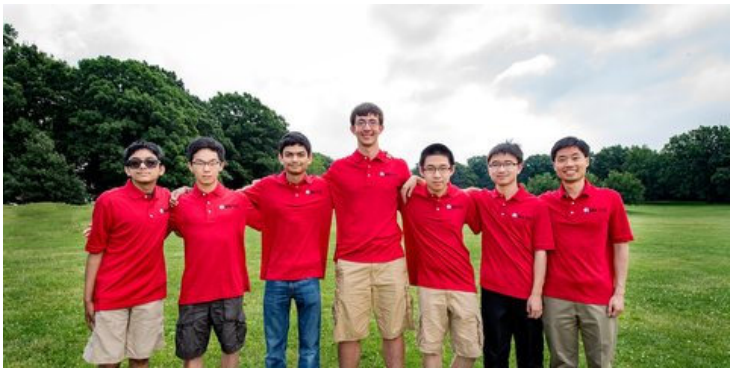
[3] http://diendantoanhoc.net/topic/157829-ch%E1%BB%A9ng-minh-c%C3%A1c-b%C4%91t-%C4%91a-th%E1%BB%A9c-b%E1%BA%ADc-4-ba-bi%E1%BA%BFn-th%E1%BB%B1c-tr%C3%AAn-m%C3%A1y-t%C3%ADnh

[4] Trang web http://mathlinks.ro.

MỘT VÀI ĐIỂM ĐẶC BIỆT CỦA PHONG TRÀO OLYMPIC TOÁN CỦA MỸ

Gary Antonick, người dịch Nguyễn Vũ Duy Linh

Trong giới IMO, từ vài chục năm nay, vị trí số 1 của đội tuyển Trung Quốc tại các kỳ IMO gần như không còn phải bàn cãi. Thậm chí có người còn nói nửa đùa, nửa thật "*Nếu Trung Quốc đem theo* 40 *học sinh thì họ cũng được* 40 *huy chương vàng*". Vì vậy, những năm nào mà Trung Quốc không xếp thứ nhất thì đội tuyển chiếm vị trí của họ luôn có được một sự quan tâm đặc biệt. Ví dụ như Bulgaria vào năm 2003, Nga vào năm 2007, Hàn Quốc vào năm 2012 hay Mỹ vào năm 2015. Các chuyên gia đều tìm một cách nào đó để giải thích kết quả đột biến của đội đã soán ngôi Trung Quốc. Thế nhưng, tại IMO 2016, khi đoàn Mỹ lần thứ hai liên tiếp đoạt ngôi quán quân tại IMO, người ta bắt đầu phải suy nghĩ một cách nghiêm túc: Dường như đội tuyển Mỹ không xếp thứ nhất do đột biến. Chúng ta cùng theo dõi cuộc trò chuyện giữa nhà báo Gary Antonick với TS Po-Shen-Loh, trưởng đoàn Mỹ tại IMO 2015 và IMO 2016.



Hình 1: Đội tuyển IMO Mỹ: Ankan Bhattacharya, Allen Liu, Ashwin Sah, Michael Kural, Yuan Yao, Junyao Peng, và huấn luyện viên Po-Shen Loh - Ảnh của đại học Carnegie Mellon.

Mỹ đã giành thắng lợi tại kỳ thi Olympic Toán Học Quốc Tế (IMO) lần thứ 57, cuộc tranh tài giải toán uy tín nhất thế giới dành cho học sinh trung học.

Cuộc thi được tổ chức từ ngày 6 đến ngày 16 tháng 7 tại Hong Kong, bao gồm các đoàn dự thi của hơn 100 nước tham gia. Đoàn Mỹ giành thắng lợi với số điểm 214 trên điểm tối đa là 252 vượt qua Hàn Quốc (207) và Trung Quốc (204). Ba đoàn trên cùng với Singapore (196), Đài Loan (175), Bắc Triều Tiên (168), Liên bang Nga (165), Anh (165), Hong Kong (161) và Nhật Bản (156) là mười đoàn dẫn đầu.

Chúc mừng đoàn Mỹ: Các sinh viên Ankan Bhattacharya, Michael Kural, Allen Liu, Junyao Peng, Ashwin Sah, and Yuan Yao, huấn luyện viên trưởng Po-Shen Loh, và huấn luyện viên phó Razvan Gelca.

Tuần này chúng ta sẽ điểm qua hai bài toán đặc sắc trong số sáu bài của năm nay. Cuộc thảo luận của chúng ta sẽ được dẫn dắt bởi chính Po-Shen Loh.

Đây là hai bài toán – thử thách tuần này của chúng ta.

Thách đố thứ nhất là Bài 2 của IMO 2016:

Tìm tất cả số nguyên dương n sao cho mỗi ô của một bảng $n \times n$ có thể được điền bằng một trong ba chữ cái I, M và O theo cách sau đây:

- *Trên mỗi hàng và mỗi cột, một phần ba các ô là I, một phần ba là M và một phần ba là O.*
- *Trên mỗi đường chéo, nếu số ô trên đường chéo là bội số của ba thì một phần ba là I, một phần ba là M và một phần ba là O.*

Thử thách thứ hai của chúng ta khó một chút. Đây là phần bình luận của tiến sĩ Loh:

Điểm đặc sắc của IMO năm nay là số lượng lớn các bài toán không chuẩn mực kết hợp nhiều lãnh vực của toán học vào trong cùng một vấn đề. Bài toán khó nhất hóa ra là bài số 3, một bài kết hợp giữa đại số, hình học và lý thuyết số. Về bài này, Hoa Kỳ đạt được số điểm tổng cộng cao nhất so với các nước khác, góp phần quyết định trong chiến thắng cuối cùng, hai lần liên tiếp đoạt ngôi quán quân (2015 và 2016), chấm dứt 21 năm không đoạt giải nhất kể từ lần cuối đoạt giải nhất vào năm 1994. Và đây là lần đầu tiên đội tuyển Mỹ đoạt giải nhất 2 năm liên tiếp.

Chúng ta hãy thử xem qua bài này. Đây là bài số 3 của IMO 2016:

Cho $P = A_1A_2\cdots A_k$ là một đa giác lồi trên mặt phẳng. Các đỉnh $A_1, A_2, \ldots, A_k$ có tọa độ nguyên và nằm trên một đường tròn.Gọi S là diện tích của P. Bình phương độ dài các cạnh của P chia hết cho n (n là một số nguyên dương lẻ). Chứng minh rằng $2S$ là một số nguyên chia hết cho n.

Đó là các thách thức cho tuần này. Nếu muốn, bạn có thể thử sức với bốn bài còn lại của cuộc thi IMO năm nay. (Đề thi, lời giải và bình luận có thể xem ở bài của Nguyễn Tiến Dũng ở số báo này, TS). Để đạt điểm cao, bạn phải trả lời đúng mỗi câu hỏi và đồng thời chứng minh câu trả lời của mình là đúng.

Cuộc trò chuyện ngắn với huấn luyện viên đoàn Mỹ Po-Shen Loh

Tôi có may mắn hiện diện tại Hong Kong tuần rồi nhân cuộc thi IMO, và được gặp huấn luyện viên đoàn Mỹ sau sự kiện này. Sau đây là trích dẫn từ cuộc hội thoại của chúng tôi:

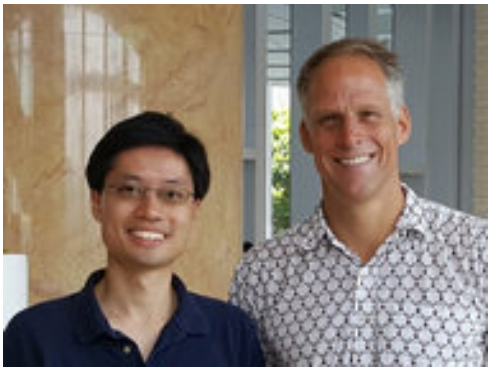
Gary Antonick (G.A): Chúc mừng chiến thắng của anh. Anh có bất ngờ khi giành chiến thắng?

Po-Shen Loh (P-S.L): Chiến thắng là một bất ngờ và giờ đây nó có nghĩa là Hoa Kỳ sẽ mạnh hơn trong tương lai. Một vài điều thú vị đã xảy ra trong năm nay: Các học sinh theo học chương trình bồi dưỡng của Mỹ được đánh giá khả năng giành thắng lợi tại cuộc thi IMO. Đánh giá của

họ là 40%. Đối với tôi, con số đó rất lớn. Nếu anh đánh giá khả năng này ba năm trước đây, anh sẽ không được con số phần trăm cao đến như vậy. Có rất nhiều đội mạnh tại các cuộc thi này. Điều đáng nói là chiến thắng năm ngoái đã mang lại một tác động tự tin rất lớn.

Anh hoàn tất một điều gì đó như thế nào không chỉ là một hàm số của cái mà anh biết mà là anh tham gia một hoạt động mạnh mẽ như thế nào. Năm nay, đoàn Mỹ đi thi với một thái độ nồng nhiệt CHÚNG TA SẼ LÀM ĐƯỢC ĐIỀU ĐÓ. Hoa Kỳ đã thắng trước đó, do đó giành chiến thắng là điều có thể.

Năm nay đúng là năm tái kiến thiết cho Hoa Kỳ - cả bốn thành viên của đoàn đều không phải là học sinh năm cuối của trường – nhưng họ vẫn có thể chiến thắng.



Hình 2: Nói chuyện với huấn luyện viên đoàn Mỹ Po-Shen Loh tại Hong Kong sau cuộc thi Olympic Toán Học Quốc Tế 2016.

G.A: Có vẻ như bài thi năm nay mang nhiều tính sáng tạo hơn những năm trước. Theo anh các bài thi sáng tạo thế nào?

P-S.L: Các bài thi năm nay – đặc biệt là bài số 3 mà chúng tôi chia sẻ ở trên – kết hợp nhiều lãnh vực khác nhau một cách sáng tạo. Bất cứ nơi nào mà chúng ta có sự kết hợp, như là trong nhà bếp, thì nơi đó có sự sáng tạo.

G.A: Đoàn Mỹ được chọn lọc và bồi dưỡng như thế nào?

P-S.L: Các học sinh được chọn từ vài trăm ngàn học sinh thông qua một chuỗi những bài kiểm tra chọn lọc do Hiệp Hội Toán Học Mỹ (MAA), tổ chức chính thức của Mỹ tham gia IMO, chịu trách nhiệm. Đội gồm sáu học sinh được tập hợp lại trước kỳ thi IMO để được bồi dưỡng trong ba tuần rưỡi tại đại học Carnegie Mellon, cũng do chính MAA tổ chức.

Tham gia vào trại bồi dưỡng là sáu em thi năm nay cùng với năm mươi bốn học sinh khác có thể tham dự vào các năm sau. Năm nay, chúng ta cũng bồi dưỡng những học sinh quốc tế - học sinh trong các đoàn IMO của các quốc gia khác. Chúng ta trả chi phí máy bay, khách sạn, ăn uống và học hành cho họ.

G.A: Xem nào, các anh đã bồi dưỡng học sinh của các đoàn IMO khác?

P-S.L: Mười trong số họ, bao gồm một vài học sinh đoạt huy chương vàng. Chẳng hạn như hai trong số bốn huy chương vàng của đội Singapore được bồi dưỡng cùng với đoàn Mỹ. Một trong số họ bình luận rằng một trong số những kỹ thuật anh ta dùng để giải các bài thi năm nay là học từ lớp bồi dưỡng. Thành công lớn là năm sau chúng tôi sẽ mời 30 học sinh quốc tế.

G.A: Những nước khác có làm như vậy không?

P-S.L: Không với mức độ như vậy. Điều này là khác thường. Thứ nhất, cho những học sinh quốc tế vào học mang đến cho những học sinh đứng đầu của Mỹ những người bạn bằng vai phải vế. Người ta luôn luôn nói với anh rằng – nếu anh là người tài ba nhất trong lớp học thì anh đang học nhầm lớp. Nên chúng tôi mang đến những người ngang mức với sáu em dẫn đầu.

Thứ hai, khi những học sinh đến dự thi IMO, họ sẽ không bị sốc về văn hóa. Bất thình lình anh đáp xuống và anh nhìn chung quanh - lạy chúa tôi. Đó là đoàn Hàn Quốc. Đó là đoàn Trung Quốc. Đó là đoàn Singapore. Bọn họ phải rất lạ lùng.

Tôi nhớ lại khi tôi tham dự IMO, đó chính là cảm giác mà tôi đã trải qua. Nhưng nếu anh bồi dưỡng chung với nhau, anh sẽ có cái kinh nghiệm quốc tế đó ba tuần rưỡi.

G.A: Ai đã nghĩ ra cái ý tưởng bồi dưỡng nhiều thành viên của nhiều đoàn khác nhau?

P-S.L: Ý tưởng của tôi. Tôi nghĩ ra một vài điều khá kỳ lạ.

G.A: Việc bồi dưỡng thi IMO trông như thế nào?

P-S.L: Chúng tôi có lớp toán từ 8 : 30 sáng đến 3 : 00 chiều, tính luôn giờ ăn trưa. Sau đó chúng tôi có seminar vào lúc 7 : 30 PM khoảng một giờ.

Cứ cách một ngày, chúng tôi lại làm việc đến 6 : 00 vì chúng tôi có một bài kiểm tra.

Đây là một video về khóa bồi dưỡng này: An Inside Look at the MAA's Mathematical Olympiad Summer Program.

Tại sự kiện mà chúng tôi tổ chức – đó là một bầu không khí khác hẳn. Anh ở đó không phải để đánh một ai đó. Các anh chỉ làm việc với nhau trong 3 tuần rưỡi.

G.A: Chương trình bồi dưỡng của đoàn Mỹ khác với những chương trình khác như thế nào?

P-S.L: Chương trình bồi dưỡng của đoàn Mỹ không chú trọng đến những kỹ thuật. Điều thật sự làm vài người lo lắng là – nếu bạn đến với chương trình bồi dưỡng của đoàn Mỹ, bạn có thể không được huấn luyện đầy đủ.

G.A: Điều gì tách biệt giữa những em giỏi nhất của IMO so với những em còn lại?

P-S.L: Tôi không muốn nói đó là di truyền. Rất nhiều người nói rằng anh phải sinh ra với một cái gì đó rất đặc biệt. Trong một lúc nào đó, bạn có thể thấy một điều gì như vậy. Nhưng mọi người căn bản mà nói đều như nhau.

Đây là một ví dụ. Giả sử tôi bảo bạn nhớ câu sau đây: *First of all, what is gravity?*

Bây giờ, với câu tiếp theo. Bạn có thể nhớ và viết lại y chang như vậy? Không thể được.

প্রথমসব, মাধ্যাকর্ষণকি ?

Nhưng điều này không có gì là không thể được. Tất cả mọi người ở Bangladesh có thể làm được. Điều mà tôi muốn nói là – bạn có vài khái niệm trong bộ óc của bạn gọi là chữ cái và từ. Khi bạn nhìn ở phiên bản Anh văn của câu hỏi này về hấp dẫn, bộ não của bạn không nhớ những đường ngoằn ngoèo ở đâu. Bộ não của bạn đã sẵn sàng với các khái niệm và sau đó nén thông tin lại. Đối với bạn, không có vấn đề gì đáng kể.

Vậy thì đâu là chỗ khác biệt giữa những em giỏi nhất và những em còn lại? Nếu bạn xem lại toán học – nếu bạn xây dựng cấu trúc khái niệm, khi bạn lý giải vấn đề, bạn đang lý luận với những khái niệm lớn. Bạn làm việc với những khái niệm lớn và sắp đặt chúng với nhau.

Đó không phải là điều kỳ diệu. Đó là liệu bộ não của anh phân chia bản đồ khái niệm, và anh có thể làm việc với toàn bộ các khái niệm như những đối số nguyên thủy như thể áp đặt làm việc với từng chữ cái nhỏ bé trong từng lúc.

G.A: Cám ơn anh, Po.

Để giới thiệu những khái niệm của kỳ thi IMO năm nay, Huấn Luyện Viên Quốc Gia Po-Shen Loh nhấn mạnh một vài câu đố vui của anh tuần này trên Expii, xem tại đây.

Quan tâm đến kỳ thi Olympic Toán năm sau? Mỗi tuần, Po-Shen Loh cho đăng năm câu hỏi trên Expii, với mức độ từ dễ tới khó. Cộng tác với bộ phim gần đây The Man Who Knew Infinity về thiên tài toán học Srinivasa Ramanujan, người đã vượt qua tính lập dị không thể ngờ được để thay đổi tương lai của toán học, họ đã lùng sục thế giới tìm kiếm những tài năng toán học chưa được phát hiện, trong Spirit of Ramanujan Talent Search.

Tuần này như vậy đến đây là hết. Như thường lệ, một khi bạn có thể đọc bình luận cho những bài đăng này, hãy sử dụng Gary Hewitt's Enhancer để xem công thức và hình ảnh một cách đúng đắn nhất và gởi đến các câu đố của bạn đến: gary.antonick@NYTimes.com.

Lời giải

Xem bình luận của độc giả vào thứ sáu về lời giải và tóm tắt của Po-Shen Loh.

BÌNH LUẬN ĐỀ THI OLYMPIC TOÁN QUỐC TẾ (IMO) 2016

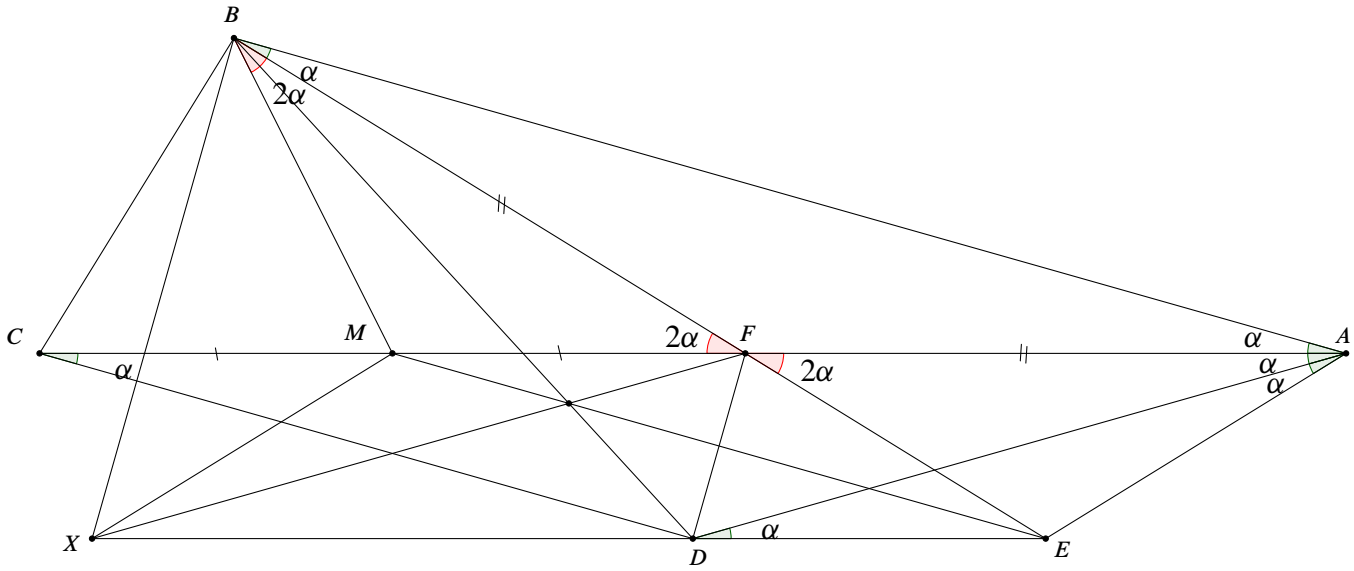
Nguyễn Tiến Dũng
(Đại học Toulouse, Pháp)

Đề thi ngày thứ nhất có 3 bài: Bài 1 là hình phẳng, bài 2 dạng tổ hợp và bài 3 là hình tổ hợp. Như vậy trong một ngày mà có đến 2 bài liên quan đến tổ hợp, là kiểu toán "vừa dễ vừa khó" không cần kiến thức gì nhiều, nhưng cần nhận định và tìm chiến lược giải cho tốt.

Bài 1 được đánh giá là tương đối dễ, nói chung học sinh nào của Việt Nam cũng phải giải được.

Bài toán 1. *Cho tam giác BCF vuông tại B. Gọi A là điểm nằm trên đường thẳng CF sao cho $FA = FB$ và F nằm giữa A và C. Lấy điểm D sao cho $DA = DC$ và AC là phân giác của $\angle DAB$. Lấy điểm E sao cho $EA = ED$ và AD là phân giác của $\angle EAC$. Gọi M là trung điểm của CF. Gọi X là điểm sao cho $AMXE$ là hình bình hành ($AM//EX$ và $AE//MX$). Chứng minh rằng các đường thẳng BD, FX và ME đồng qui.*

Lời giải. Dễ thấy E, D, X thẳng hàng và $\angle CDA = 180^\circ - 2\alpha$, $\angle CBA = 90^\circ + \alpha$ suy ra D là tâm nội tiếp tam giác ABC.



Do đó

$$DB = DC = DA \Rightarrow \angle DBF = \angle DFA = \alpha \Rightarrow D \in (BCF) \Rightarrow \angle CDF = 90^\circ.$$

Suy ra $\angle DFA = 90^\circ + \alpha$ mà $\angle DEA = 180^\circ - 2\alpha$ nên E là tâm nội tiếp tam giác DFA. Do đó È $+ EA$ nên tam giác EFA cân tại E suy ra $\angle EFA = \angle EAF = 2\alpha = CFB$. Cho nên ba điểm B, E, F thẳng hàng. Từ đó dễ dàng chứng minh được $BMEA$ là hình thang cân, suy ra $EB = MA + EX$ và

$$FB = FA = MA - MF = EX - MB = EX - EA = EX - ED = DX$$

kết hợp với $MB = EA = MX$ ta suy ra điều phải chứng minh. □

Bài toán 2. *Cho một bảng ô vuông $n \times n$. Người ta muốn điền các chữ cái I, M, O vào các ô của bảng (mỗi ô một chữ cái) sao cho trong mỗi hàng, mỗi cột thì số lượng của mỗi chữ cái đúng bằng $\frac{1}{3}$ tổng số, và trong mỗi đường chéo có độ dài chia hết cho 3 thì cũng như vậy. Hỏi với những số n nào thì có thể làm được việc đó?*

(Đường chéo hiểu theo nghĩa như những đường chéo của bàn cờ).

Bài này lời giải không dài, nhưng tìm được lời giải không dễ lắm. Nhận xét hiển nhiên đầu tiên là n phải chia hết cho 3, thì mới có $\frac{1}{3}$ của n là số nguyên. Ngoài ra còn những điều kiện gì?

Thử xét trường hợp đơn giản nhất $n = 3$ thấy không thể được.

Trường hợp $n = 6$ thì sao? Sau khi thử xếp nhiều lần không được, thì ta đưa ra giả thuyết là $n = 6$ không được và sẽ thử chứng minh.

Trường hợp $n = 9$ thì sao? Khi đó n chia hết cho 9. Và có thể xếp được, thậm chí chứng minh được là với mọi số $n = 9k$ chia hết cho 9 đều xếp được.

Một cách xếp như sau: Thay vì viết I, M, O ta sẽ viết $0, 1, -1$ (modulo 3) cho tiện. Đánh số các ô bằng cặp số (i, j) để chỉ hàng i, cột j (i, j đi từ 1 đến n).

Số viết ở ô (i, j) là số $\left[\frac{i}{3}\right] + j$ modulo 3 (ở đây $[x]$ là ký hiệu chỉ phần nguyên).

Quay lại các trường hợp n chia hết cho 3 nhưng không chia hết cho 9. Muốn chứng minh rằng không thể xếp được.

Tương tự như trường hợp n chia hết cho 9, ta muốn dùng đồng dư theo 3 để chứng minh. Ký hiệu các chữ thành $0, 1, -1$ như lúc nãy.

Giả sử xếp được, thế thì tổng tất cả các số bằng 0 (thực sự bằng 0, chứ không chỉ đồng dư với 0 modulo 3). Bây giờ chú ý tất cả các ô với chỉ số có dạng $(3i + 2, 3j + 2)$. Có tổng cộng $\left(\frac{n}{3}\right)^2$ các ô như vậy, và con số này là một số nguyên không chia hết cho 3.

Qua bất kỳ một ô nào khác thì có đúng 1 đường hoặc là chéo với độ dài chia hết cho 3 hoặc là ngang hoặc là dọc mà sẽ đi qua một trong các ô trên. Tổng các số trên các đường đó, có tính cả lặp bằng 0 (trên mỗi đường đều bằng 0) đồng thời nó bằng tổng tất cả các số của bảng vuông cộng thêm 3 lần tổng tất cả các số trên các ô được đánh dấu phía trên. Suy ra tổng các số trên các ô được đánh dấu bằng 0.

Cho đến đây thì mọi thứ OK. Nhưng mâu thuẫn nằm ở chỗ này: Bây giờ chỗ nào ghi 0 thì thay bằng 1, chỗ nào ghi 1 thì thay bằng -1, chỗ nào ghi -1 thì thay bằng 0 (hoán vị tuần hoàn). Khi đó bảng mới vẫn thỏa mãn các điều kiện nêu ra, và như vậy tổng các số của các ô được đánh dấu trên bảng mới cũng phải bằng 0.

Mặt khác, khi làm như vậy thì mỗi số được thay đi $+1$ modulo 3, và như vậy tổng theo modulo 3 phải thành $\left(\frac{n}{3}\right)^2$ modulo 3, và khác 0. Mâu thuẫn này cho thấy không tồn tại cách xếp khi n không chia hết cho 9.

Bài toán 3. *Cho đa giác lồi nội tiếp đường tròn với các đỉnh đều là điểm nguyên và độ dài bình phương của các cạnh đều chia hết cho một số tự nhiên lẻ N nào đó. Chứng minh rằng 2 lần diện tích của đa giác cũng chia hết cho N.*

Bài này được coi là khó nhất của ngày 1. Thực ra lời giải cũng không dài nếu tìm được đúng hướng (về nguyên tắc chung, không có bài thi nào đòi hỏi lời giải quá dài, vì nếu quá dài thì học sinh không làm nổi trong thời gian thi).

Để giải, đầu tiên làm trường hợp tam giác. Trong trường hợp này có thể chứng minh trực tiếp bằng cách vận dụng một công thức nào đó để tính diện tích tam giác khi biết tọa độ cách đỉnh (điều kiện nội tiếp đường tròn là tự thỏa mãn và không có tác dụng gì đối với tam giác).

Trường hợp đa giác: Tìm cách quy về trường hợp tam giác bằng quy nạp. Tức là tìm cách chia đa giác thành nhiều tam giác, và làm sao vận dụng được điều kiện nội tiếp.

Có lời giải rất hay và ngắn gọn của Phạm Ngọc Mai như sau

Với $n = 3$ ta có

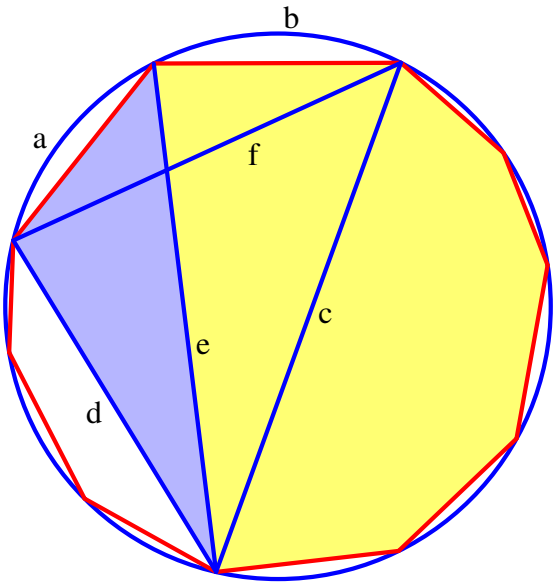
$$16S^2 = 2(a^2b^2 + b^2c^2 + c^2a^2) - a^4 - b^4 - c^4.$$

Từ bình phương của a, b, c đều chia hết cho n ta suy ra $16S^2 \vdots n$ cho nên $2S \vdots n$ ($2S$ nguyên).

Xét $k \geqslant 4$. Rõ ràng ta chỉ cần xét trường hợp $n = p^m$ ($m \geqslant 1$) với p là một số nguyên tố lẻ.

Ta chứng minh khẳng định sau: "*Tồn tại một đường chéo có bình phương chia hết cho p.*"

Lấy đường chéo e chia đa giác đã cho thành hai đa giác có vô số cạnh nhỏ hơn k. Gọi a, b là hai cạnh liên tiếp tại đầu mút của e (xem hình vẽ)



Theo định lý Ptolemy, ta có

$$ac + bd = ef \Rightarrow (abcd)^2 = \left(\frac{e^2f^2 - c^2a^2 - b^2d^2}{2}\right)^2. \tag{1}$$

Từ cách chọn e nên ta có c^2, d^2 đều chia hết cho p^α do đó vế trái của (1) chia hết cho $p^{2m+2\alpha}$. Suy ra $e^2f^2 - c^2a^2 - b^2d^2$ chia hết cho $p^{m+\alpha}$. Theo giả thiết ta có a^2, b^2 chia hết cho p^m. Vì vậy ta nhận được e^2f^2 chia hết cho $p^{m+\alpha}$. Suy ra f^2 chia hết cho p^m. Như vậy khẳng định được chứng minh.

Áp dụng mệnh đề này bằng cách sử dụng phương pháp quy nạp theo số cạnh k của đa giác ta dễ dàng suy ra kết luận của bài toán.

Bài toán 4. *Đặt $P(n) = n^2 + n + 1$. Tìm số tự nhiên $b > 1$ nhỏ nhất sao cho tồn tại dãy số liên tiếp với b phần tử $P(a+1)$, $P(a+2)$, ..., $P(a+b)$ (a là số tự nhiên) sao cho bất kỳ số nào trong dãy đó cũng có một ước số chung khác 1 với một số khác trong dãy.*

Lời giải. Lời giải bài này thuộc loại "bổ củi", tương đối dễ nhưng có khá nhiều trường hợp cần phải xét.

Trước hết, để ý rằng với mọi n thì $P(n)$ là số lẻ, và $P(n)$ và $P(n+1)$ nguyên tố cùng nhau

$$\begin{aligned}\gcd(n^2 + n + 1, (n+1)^2 + (n+1) + 1) &= \gcd(n^2 + n + 1, 2n + 2)\\ &= \gcd(n^2 + n + 1, n + 1)\\ &= \gcd(n^2, n + 1) = 1.\end{aligned}$$

Từ đó suy ra b không thể bằng 2, b cũng không thể bằng 3, vì nếu dãy 3 số thì số ở giữa sẽ nguyên tố cùng nhau với 2 số còn lại. Vậy $b = 4$ được không?

Nếu $b = 4$ thì số thứ 3 phải có ước chung khác 1 với số thứ 1, số thứ 2 phải có ước chung khác 1 với số thứ 4. Như vậy cần xét $\gcd(P(n), P(n+2))$. Làm tương tự như trên thì tính ra (thuật

toán Euclid) ước chung lớn nhất là 1 hoặc 7, và là 7 khi và chỉ khi n đồng dư với 2 modulo 7. Nhưng không thể cả $a+1$ và $a+3$ đều đồng dư với 7 modulo 7, nên $b=4$ cũng không được.

Để xem $b=5$ có được không, phải xét đến $\gcd(P(n), P(n+3))$ nó khác 0 khi và chỉ khi n đồng dư 1 modulo 3. Từ đó, làm tương tự như trên, suy ra cũng không được.

Đến $b=6$ thì được. Khi đó a sẽ phải thỏa mãn các điều kiện sau:

- $a+1$ đồng dư với 1 modulo 3 (để cho $P(a+1)$, $P(a+4)$ đều chia hết cho 3).
- $a+2$ đồng dư với 7 modulo 19 (để cho $P(a+2)$ và $P(a+6)$ đều chia hết cho 19).
- $a+3$ đồng dư với 2 modulo 7 (để cho $P(a+3)$ và $P(a+5)$ đều chia hết cho 7).

Theo định lý thặng dư thì tồn tại a như vậy. □

Bài toán 5. *Cho đồng nhất thức*

$$(x-1)(x-2)\cdots(x-2016) = (x-1)(x-2)\cdots(x-2016).$$

Xóa đi N nhân tử bậc nhất từ hai bên của đồng nhất thức này, để sao cho mỗi bên còn ít nhất 1 nhân tử, và được một phương trình không có nghiệm thực. Hỏi số N nhỏ nhất để làm được như vậy là bao nhiêu?

Lời giải. Dễ thấy là $N \geqslant 2016$, vì nếu chẳng hạn để lại $x-1$ ở bên trái thì phải xóa nó đi ở bên phải, nếu không sẽ có nghiệm $x=1$.

Phần khó hơn là chứng minh rằng chỉ cần xóa đúng 2016 nhân tử là đủ. Cách xóa có vẻ không duy nhất. Một cách xóa để lại hai bên $P(x)$ và $Q(x)$ như sau

$$P(x) = (x-2)(x-3)(x-6)(x-7)\cdots(x-2014)(x-2015),$$

$$Q(x) = (x-1)(x-4)(x-5)(x-8)\cdots(x-2013)(x-2016).$$

Có thể chứng minh $P(x) > Q(x)$ với mọi số thực x.

Thật vậy, trường hợp $P(x) > 0$ và $Q(x) < 0$ (ví dụ như $3 < x < 4$) thì hiển nhiên $P(x) > Q(x)$. Trong trường hợp mà $P(x)$ và $Q(x)$ đều dương (ví dụ như là $4 < x < 5$), thì ta có các bất đẳng thức

$$(x-2)(x-3) > (x-1)(x-4) > 0,$$

$$(x-6)(x-7) > (x-5)(x-8) > 0,$$

$$\cdots\cdots$$

Nhân vào với nhau ta được $P(x) > Q(x)$.

Trường hợp mà cả $P(x)$ và $Q(x)$ đều âm, ví dụ $2 < x < 3$, khi đó nhóm lại theo kiểu khác

$$(x-4)(x-5) > (x-3)(x-6) > 0,$$

$$(x-8)(x-9) > (x-7)(x-10) > 0,$$

$$\cdots\cdots$$

$$(x-2012)(x-2013) > (x-2011)(x-2014) > 0,$$

$$(x-1)(2016-x) > (x-2)(2015-x) > 0.$$

Nhân vào với nhau ta được $-Q(x) > -P(x)$, tức là $P(x) > Q(x)$ (không có trường hợp nào mà $P(x) < 0 < Q(x)$ vì các "đoạn âm" của $P(x)$ nằm trọn trong các "đoạn âm" của $Q(x)$).

Xin mời thử kiểm tra với hai đa thức khác

$$P(x) = (x-506)(x-507)(x-508)\cdots(x-5113),$$
$$Q(x) = \text{tích của các nhân tử còn lại.}$$

Bài này thuộc diện "khó vừa phải", nhiều bạn giải được. □

Bài toán con ếch (bài số 6) được coi là bài khó nhất của ngày thứ hai, và là bài "chém" đội tuyển Việt Nam. Nếu như phần lớn các bạn trong đoàn giải được hai bài số 4 và số 5, thì bài số 6 không bạn nào giải được: Chỉ có một bạn được 3 điểm trên 7, và các bạn còn lại đều 0 điểm.

Bài toán 6. *Có N đoạn thẳng cắt nhau từng đôi một trên mặt phẳng sao cho không có 3 đoạn nào đồng quy. Như vậy trên mỗi đoạn có $N-1$ điểm nút cắt và hai nút đầu đuôi. Thầy Minh (Nguyễn Khắc Minh) chơi trò sau: Đặt N con ếch vào N đầu của N đoạn thẳng đó (mỗi đoạn 1 con). Rồi thầy vỗ tay N lần. Cứ mỗi lần thầy vỗ tay thì con ếch nhảy từ một nút đến nút tiếp theo trên đoạn thẳng của nó (theo hướng cố định từ đầu đặt ếch đến đầu kia). Chứng minh rằng*

i) Nếu N lẻ thì luôn có thể đặt ếch sao cho khi nhảy như vậy, không có lần nào mà 2 con ếch đều nhảy cùng vào 1 nút.

ii) Nếu N chẵn thì đặt ếch kiểu gì cũng có lúc hai con ếch nhảy cùng vào 1 nút ở một lần vỗ tay nào đó.

Bài này khó ở chỗ nó lạ, và học sinh của ta chỉ giỏi giải các bài thuộc những dạng quen thuộc đã "cày đi bừa lại" còn gặp bài lạ nói chung là ngơ ngác không biết phải làm thế nào. Nếu có được chiến lược tốt để đối mặc với các bài toán lạ như bài này, thì chúng sẽ không còn phức tạp quá nữa (nếu quá phức tạp người ta đã không chọn làm bài thi). Lời giải thực ra cũng khá ngắn gọn, thậm chí có khi còn ngắn hơn những bài khác của đề thi. Một lời giải như sau:

Lời giải. Gồm có 4 bước:

Bước 1: Lấy 1 vòng tròn đủ to để chứa tất cả các điểm cắt nhau của các đoạn thẳng bên trong. Kéo dài các đoạn thẳng sao cho các điểm đầu đuôi của chúng nằm trên vòng tròn. Sau khi làm thế ta có thể đánh số thứ tự các điểm đầu đuôi này theo vòng tròn (chẳng hạn theo chiều kim đồng hồ): Ta đánh số ký hiệu chúng từ A_1 đến A_{2N}. Dễ thấy là các điểm A_i và A_{N+i} là cùng thuộc về một đoạn thẳng với mọi i (điều này suy ra từ tính chất các đoạn thẳng đều cắt nhau).

Bước 2: Quan sát rằng nếu ếch đặt ở A_i và A_{i+1} (hai điểm sát nhau trên vòng tròn) thì thể nào chúng cũng cụng đầu nhau sau một số bước nhảy, vì số nút tính từ hai đầu đó đến giao điểm của hai đường thứ i và thứ $i+1$ là bằng nhau. Đây là quan sát then chốt của bài toán.

Bước 3: Giả sử ta muốn xếp ếch sao cho chúng không bị nhảy vào nhau và không mất tính tổng quát, giả sửa con đều tiên xếp ở A_1. Khi đó không được xếp ở A_2, suy ra phải xếp ở A_{n+2} cho đường thứ 2, suy ra không được xếp ở A_{n+3}, suy ra phải xếp ở A_3 cho đường thứ 3. Tức là cứ phải xếp cách một điểm $1 \to 3 \to 5 \to \cdots$

Nếu $N = 2k$ là số chẵn thì $1 \to 3 \to 5 \to \cdots \to 2k+1 = N+1$, tức là thành ra xếp 2 con ở 2 đầu đoạn thẳng thứ nhất, vô lý. Suy ra là không thể xếp ếch sao cho chúng không nhảy vào nhau trong trường hợp này.

Bước 4: $N = 2k+1$ lẻ thì sao? Có mỗi 1 cách xếp như trên

$$1,\ 3,\ \ldots,\ 2k+1 = N,\ N+2,\ N+2,\ \ldots,\ N+2k = 2N-1.$$

Cần chứng minh rằng cách này OK. Để chứng minh, ta dùng tính chẵn lẻ. Để ý rằng số điểm đầu - đuôi giữa hai con ếch bất kỳ theo cách xếp này là một số lẻ. Từ đó suy ra nếu số bước đi từ một con ếch đến một nút nào đó là số chẵn thì số bước đi từ con ếch ở đường còn lại đến nút đó là số lẻ và ngược lại. Do đó chúng không thể nào nhảy đến nút cắt tại cùng một thời điểm. □

Nhận xét. Làm sao tìm được lời giải?

Cần có những chiến lược chung để áp dụng với những bài toán lạ như thế này, gồm những bước như:

- Tạo ra cái gì đó để mà bấu víu vào (như trong bước 1, xếp thứ tự các đường để mà bấu víu vào thứ tự đó, phân tích trở nên dễ hơn).
- Xét các trường hợp riêng đơn giản để tìm quy luật chung (xét với 3, 4, 5, 6 con).
- Tạo ra các giả thuyết trung gian và tìm cách chứng minh các giả thuyết đó. Ví dụ, để chứng minh có thể xếp được ếch khi N lẻ, tạo giả thuyết về chẵn - lẻ, tức là xếp sao cho tính chẵn lẻ của hai con đến 1 đầu mút là khác nhau. Giả thuyết này thực ra có thể chứng minh trực tiếp được mà không cần đến bước 2 quan sát phía trên.

  Có một giả thuyết khác cũng khá thú vị (để chứng minh là khi N chẵn thì không xếp được): Tồn tại một điểm mút mà số bước từ đó đến cả 4 điểm đầu đuôi của 2 đoạn cắt tại nó đều bằng $\frac{N}{2}$. Nếu giả thuyết này đúng, thì có nghĩa là sau $\frac{N}{2}$ bước sẽ có 2 con đụng đầu. Rất tiếc là giả thuyết này thực ra không đúng, có phản ví dụ khi $N = 6$. Bởi vậy khi có các giả thuyết, thì cũng cần thử kiểm tra (với N nhỏ) xem có đúng không nếu không chứng minh được cho N tổng quát.
- Quan sát để tìm quy luật. Như là bước 2 phía trên là một bước mấu chốt, làm cho bài toán trở nên đơn giản hẳn.
- Quy nạp đối với các bài tổ hợp trong đó có "N" tùy ý. Trong bài toán con ếch này, nếu quy nạp theo số đoạn thẳng, bằng cách mỗi lần bỏ bớt đi 1 hay 2 đoạn, thì rất khó khăn, vì các số bước nhảy đến từ điểm đầu đuôi đến điểm mút thay đổi khá phức tạp mỗi khi thêm 1 đoạn. Tuy nhiên các điều nêu trong bước 2 và bước 3 phía trên, để viết ra một cách tỉ mỉ, thì đều có thể viết bằng quy nạp.

BÀI TOÁN HAY LỜI GIẢI ĐẸP

Trần Nam Dũng
(Đại học Khoa học Tự nhiên - ĐHQG TP.HCM)

GIỚI THIỆU

Chuyên mục này được lấy cảm hứng từ bài viết của thầy Nguyễn Duy Liên về bài toán số 6 trong kỳ thi IMO 2001 với 5 cách giải khác nhau. Mục này sẽ để dành viết về những bài toán hay, lời giải đẹp và những câu chuyện thú vị xung quanh những bài toán và lời giải đó.

Tên của chuyên mục được mượn từ tên của một nhóm những người yêu toán trên Facebook do anh Nguyễn Văn Lợi sáng lập "*Bài toán hay – Lời giải đẹp – Đam mê toán học*". Chuyên mục ghi nhận các đề cử của bạn đọc và sẽ chọn đăng mỗi kỳ 1, 2 bài toán.

Số này chúng tôi giới thiệu buổi trò chuyện của TS Trần Nam Dũng tại Trại hè Phương Nam năm 2016 nhân một bài toán khá dễ của kỳ thi này, bài số 1.

Bài toán 1 (Olympic Trại hè Phương Nam 2016). *Giải phương trình*

$$\frac{13(1-2x^2)}{\sqrt{1-x^2}}+\frac{9(1+2x^2)}{\sqrt{1+x^2}}=0. \tag{1}$$

Bài toán này rất đơn giản, vì nhìn kỹ, nó chỉ là một phương trình bậc ba của x^2, và phương trình đó lại có nghiệm đặc biệt. Nhiều bạn học sinh đã giải được bài này, và đây là lời giải mà đại đa số học sinh đã tìm ra:

Điều kiện $|x|<1$. Ta thực hiện biến đổi tương đương

$$\frac{13(2x^2-1)}{\sqrt{1-x^2}}=\frac{9(1+2x^2)}{\sqrt{1+x^2}}\Leftrightarrow\begin{cases}2x^2-1\geqslant 0\\ 169(2x^2-1)^2(1+x^2)=81(1+2x^2)^2(1-x^2)\end{cases}$$

$$\Leftrightarrow\begin{cases}2x^2-1\geqslant 0\\ 1000x^6-750x^2+88=0\end{cases}\Leftrightarrow\begin{cases}2x^2-1\geqslant 0\\ 2(5x^2-4)(100x^4+80x^2-11)=0\end{cases}$$

Ta thấy trong điều kiện $2x^2-1\geqslant 0$ thì $100x^4+80x^2-11>0$ nên từ đây suy ra phải có $5x^2-4=0$, tức là $x=\pm\frac{2}{\sqrt{5}}$.[1]

[1]Khi được giới thiệu bài này, bạn Võ Quốc Bá Cẩn cũng có đề xuất thêm lời giải sau đây:

Câu chuyện có lẽ đã dừng lại vì cũng không có gì để bình luận. Một phương trình vô tỷ bình thường được giải bằng một phương pháp bình thường không có gì đặc biệt. Thế nhưng tôi (Trần Nam Dũng) đặt câu hỏi.

"Bài toán được giải xong rồi. Nhưng bây giờ mới là câu hỏi khó: Bài toán này liên quan đến một bài toán quen thuộc nào?"

Do các em học sinh không đoán được (quá khó để đoán), tôi đã gợi ý: Đó là bài toán bất đẳng thức trong đề thi Olympic 30/4 năm 1996, khối lớp 10.

Bài toán 2 (Olympic 30/4, 1996, khối lớp 10). *Cho* $0 \leqslant x \leqslant 1$. *Chứng minh rằng*

$$x\left(13\sqrt{1-x^2}+9\sqrt{1+x^2}\right) \leqslant 16. \tag{2}$$

Tôi đặt câu hỏi: "Biết là liên quan rồi đó, nhưng liên quan thế nào?"

Sau vài giây, một bạn học sinh trả lời "Dạ thưa thầy, nếu gọi vế trái của bất đẳng thức là $f(x)$ thì phương trình $f'(x)=0$ chính là phương trình ở bài toán của chúng ta ạ".

Đúng là như vậy. Để chứng minh (2), ta chỉ cần chứng minh giá trị lớn nhất của hàm số ở vế trái bằng 16. Nếu biết đạo hàm, điều này sẽ quy về việc giải phương trình $f'(x)=0$ rồi xét dấu $f'(x)$ để tìm cực tiểu. Sơ đồ giải quen thuộc này nêu lên ý nghĩa quan trọng của đạo hàm và cũng giải thích các phương trình xuất hiện từ đâu và vì sao ta phải học giải phương trình.

Tôi lại đặt tiếp câu hỏi "Giải bằng đạo hàm thì đơn giản rồi, nhưng đây là bài toán cho khối lớp 10. Vậy làm sao các bạn ấy giải được. Tại sao BTC lại chọn bài toán này? Tôi xin bật mí cho các bạn là bài toán được chọn do lời giải chỉ có 1 dòng, và không cần dùng đến đạo hàm. Các bạn đã biết điểm rơi tại $x=\frac{2}{\sqrt{5}}$, các bạn có thể phục dựng lại lời giải 1 dòng của đáp án không?".

Sau vài phút, có một bạn học sinh đã lên trình bày lời giải sau: Theo bất đẳng thức AM-GM,

$$13x\sqrt{1-x^2}=\frac{13}{2}\left(x\cdot 2\sqrt{1-x^2}\right)\leqslant\frac{13}{4}\left[x^2+4(1-x^2)\right],$$
$$9x\sqrt{1+x^2}=\frac{3}{2}\left(3x\cdot 2\sqrt{1+x^2}\right)\leqslant\frac{3}{4}\left[9x^2+4(1+x^2)\right]$$

Cộng tác bất đẳng thức trên lại, ta có điều phải chứng minh. Dấu bằng xảy ra khi và chỉ khi $x>0$, $x^2=4(1-x^2)$ và $9x^2=4(1+x^2)$ tức là khi $x=\frac{2}{\sqrt{5}}$.

Ta biến đổi phương trình về dạng

$$\frac{13(2x^2-1)}{2x^2+1}=9\sqrt{\frac{1-x^2}{1+x^2}}\Leftrightarrow 13\left(1-\frac{2}{1+2x^2}\right)=9\sqrt{\frac{2}{1+x^2}-1}.$$

Đến đây, chỉ cần để ý rằng vế trái là hàm liên tục và tăng theo ẩn x^2, còn vế phải là hàm liên tục và giảm theo x^2, ta chứng minh được x^2 phải bằng $\frac{4}{5}$.

Tôi nói rằng đó chính là lời giải của đáp án, chỉ khác là đáp án viết gộp lại nên chứng minh chính chỉ có một dòng!

Có lẽ vì lời giải ngắn gọn đó mà bài toán đã được chọn, lại được xếp vào vị trí bài toán... dễ. Sự thật diễn ra cho thấy đó là một nhận định sai lầm: chỉ có duy nhất một thí sinh của kỳ thi giải được bài này, đó là em Vũ Đức Phú. Em đã giải bằng bất đẳng thức Cauchy-Schwarz.

Lời giải đó như sau: Ta có

$$\left(13\sqrt{1-x^2}+9\sqrt{1+x^2}\right)^2 \leqslant (13+27)\left[13(1-x^2)+3(1+x^2)\right] = 80(8-5x^2).$$

Từ đó suy ra

$$x^2\left(13\sqrt{1-x^2}+9\sqrt{1+x^2}\right)^2 \leqslant 80x^2(8-5x^2) \leqslant 4(5x^2+8-5x^2)^2 = 256.$$

Lấy căn bậc hai hai vế, ta dễ có điều phải chứng minh.

Trong khi đó 3 học trò cưng của tôi là Lê Quang Nẫm, Nguyễn Lê Lực, Lưu Minh Đức đã bó tay. Nẫm còn nói "Em đã thử dùng đạo hàm mà cũng không được". Chắc cậu ấy tính sai, chứ nếu tính đúng sẽ dẫn đến phương trình (1) và đã giải được rồi.

Quay trở lại với hai lời giải trên, một bạn học sinh lại thắc mắc: Có được các lời giải này là do ta biết điểm rơi $x = \frac{2}{\sqrt{5}}$ và tìm cách cân bằng hệ số thích hợp khi áp dụng AM-GM. Nhưng giá trị này đâu dễ đoán ra. Vậy phải làm thế nào?

Tôi nói: Đây chính là câu hỏi mà tôi muốn nghe. Lời giải 1 dòng ở đáp án tuy đẹp và đáng ngưỡng mộ, có thể vỗ tay nhưng ta chưa học nhiều được ở đó, vì các hằng số khi áp dụng AM-GM vẫn là bí ẩn. Làm sao để tìm ra các hằng số này với điều kiện chưa biết điểm rơi. Đây là câu trả lời: ta dùng phương pháp hệ số bất định. Với hai số dương $\alpha,\ \beta$ bất kỳ, ta có

$$13x\sqrt{1-x^2} = \frac{13}{\alpha}\left(\alpha x\cdot\sqrt{1-x^2}\right) \leqslant \frac{13}{2\alpha}(\alpha^2x^2+1-x^2),$$
$$9x\sqrt{1+x^2} = \frac{9}{\beta}\left(\beta x\cdot\sqrt{1+x^2}\right) \leqslant \frac{9}{2\beta}(\beta^2x^2+1+x^2).$$

Cộng các bất đẳng thức vế theo vế, ta được

$$13x\sqrt{1-x^2}+9x\sqrt{1+x^2} \leqslant \frac{13}{2\alpha}(\alpha^2x^2+1-x^2)+\frac{9}{2\beta}(\beta^2x^2+1+x^2). \qquad (3)$$

Dấu bằng xảy ra khi và chỉ khi $\alpha^2x^2 = 1-x^2,\ \beta^2x^2 = 1+x^2$.

Để tìm giá trị lớn nhất của vế trái, ta cần chọn $\alpha,\ \beta$ sao cho

i) Vế phải của (3) không phụ thuộc vào x;

ii) Tồn tại x sao cho $\alpha^2x^2 = 1-x^2,\ \beta^2x^2 = 1+x^2$.

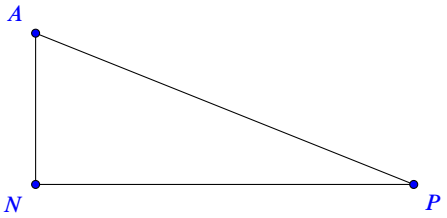
Từ đây ta dễ dàng tìm được điều kiện đối với α, β là hệ phương trình

$$\begin{cases} \dfrac{13}{2\alpha}(\alpha^2-1)+\dfrac{9}{2\beta}(\beta^2+1)=0 \\ \alpha^2+1=\beta^2-1 \end{cases}$$

Giải hệ này ra, ta được (cũng là một phương trình bậc ba của α) $\alpha=\frac{1}{2}$, $\beta=\frac{3}{2}$. Từ đó mà có lời giải như trên. Chú ý hệ phương trình rất giống hay chính xác hơn là tương đương với phương trình (1). Một lần nữa lý do để ta phải học giải phương trình, hệ phương trình được giải thích.

Cuối cùng, tôi đề nghị các bạn học sinh áp dụng các phương pháp tương tự để giải quyết bài toán 3 của kỳ thi:

Bài toán 3 (Olympic Trại hè Phương Nam 2016). *Một nhà địa chất đang ở vị trí A trong sa mạc, cách con đường thẳng* 10 km ($AN=10$ km). *Trên con đường thì xe của nhà địa chất có thể chạy với vận tốc* 50 km/h *nhưng trên sa mạc thì nó chỉ chạy được với vận tốc* 30 km/h. *Nhà địa chất đang rất khát nước và ông biết rằng có một trạm xăng P ở vị trí xuôi theo đường* 25 km ($NP=25$ km) *và ở đó có xá xị Chương Dương ướp lạnh.*



a) *Nhà địa chất tốn bao nhiêu phút để đi từ A đến P theo đường sa mạc?*

b) *Nếu nhà địa chất đi từ A đến N, sau đó sử dụng con đường để đến P thì có nhanh hơn đi từ A đến P theo đường sa mạc không?*

c) *Hãy tìm một cách đi nhanh hơn cho nhà địa chất. Cách của bạn đã là nhanh nhất chưa?*

Các bạn học sinh ở Tiền Giang đã giải quyết rất tốt bài toán (ý nói câu cuối – tìm phương án tối ưu) mà không dùng đến đạo hàm. Còn các bạn thì sao?

LỜI GIẢI ĐỀ THI TOÁN QUỐC TẾ FORMULA OF UNITY - THE THIRD MILLENNIUM (TIẾP THEO)

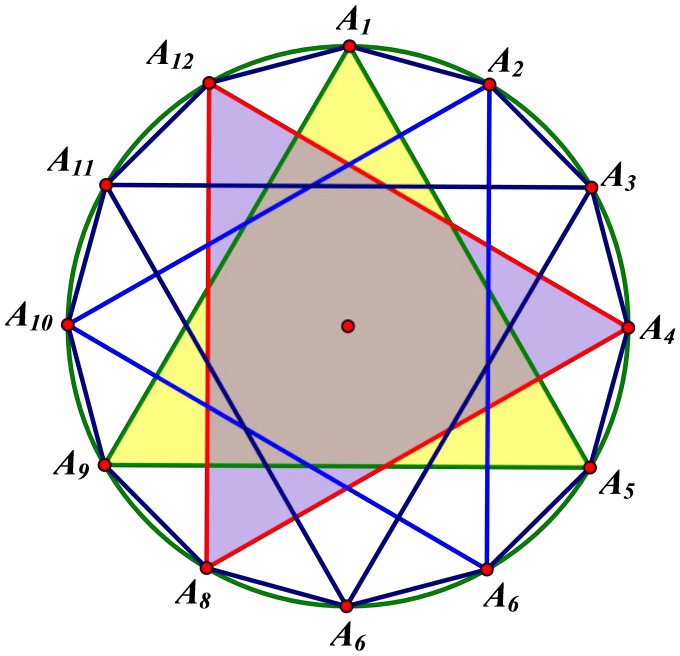
Ban biên tập Epsilon

Tiếp theo Epsilon số 9, Ban biên tập xin giới thiệu với bạn đọc lời giải của đề thi của kỳ thi Formula of Unity. Phần 2 gồm các đề của khối lớp 9, 10, 11.

1. Đề thi dành cho Khối lớp R9

Bài 1 *Các đỉnh của một đa giác đều* 12 *cạnh được tô màu xanh và đỏ. Biết rằng trong* 3 *đỉnh bất kì tạo thành một tam giác đều, có ít nhất* 2 *đỉnh màu đỏ. Chứng minh rằng ta có thể chọn* 4 *đỉnh tạo thành một hình vuông với ít nhất* 3 *đỉnh đỏ.*

Lời giải.



Ta thấy có tất cả 4 tam giác đều rời nhau và 3 hình vuông rời nhau trong đa giác đã cho.

Giả sử rằng không tồn tại hình vuông nào thỏa mãn đề bài thì với mỗi hình vuông, có không quá 2 đỉnh đỏ. Do đó, tổng cộng có không quá 6 đỉnh đỏ.

Trong khi đó, mỗi tam giác đều đóng góp ít nhất 2 đỉnh đỏ nên sẽ có tổng cộng ít nhất 8 đỉnh đỏ. Điều mâu thuẫn này cho ta đpcm.

Bài 2 *Ta nói một số nguyên dương là đẹp nếu nó là tích các giai thừa của các số nguyên tố (không nhất thiết phải phân biệt). Ta gọi một số hữu tỉ dương là tốt nếu nó là tỉ số giữa hai số nguyên dương đẹp. Chứng minh rằng tất cả các số hữu tỉ dương đều tốt.*

Lời giải. Trước hết, ta thấy rằng nếu một số hữu tỉ dương là tốt thì tích và thương của chúng cũng đều tốt.

Ngoài ra, mỗi số nguyên dương n đều có thể viết thành $\frac{n!}{(n-1)!}$.

Từ đó, ta đưa bài toán về chứng minh mọi số nguyên dương đều tốt và ta sẽ thực hiện điều này bằng quy nạp.

Với $n = 1$, ta có $1 = \frac{2!}{2!}$ là số tốt.

Với $n = 2$, ta có $2 = \frac{2!2!}{2!}$ cũng là số tốt.

Với $n = 3$, ta có $3 = \frac{3!}{2!}$ cũng là số tốt.

Khi đó, với $n \geq 4$, nếu nó là hợp số, ta có thể viết nó thành tích của các số nguyên tố nhỏ hơn và theo giả thiết quy nạp, nó cũng là số tốt.

Nếu $n \geq 4$ là số nguyên tố, ta viết $n = \frac{n!}{(n-1)!}$ và $n - 1$ là hợp số, khi đó nó cũng là số tốt nên suy ra n là số tốt.

Theo nguyên lý quy nạp thì nhận xét được chứng minh. Bài toán được giải quyết.

Chẳng hạn $5 = \frac{5!}{4!} = \frac{5!}{2 \cdot 3 \cdot 4} = \frac{5!}{2^3 \cdot 3} = \frac{5!}{(2!)^3 \cdot \frac{3!}{2!}} = \frac{5!}{(2!)^2 \cdot 3!}$.

Bài 3 *Có 27 con gián tham gia một cuộc chạy đua. Trong mỗi vòng sẽ có ba con gián chạy. Mỗi con gián chạy với tốc độ cố định, không đổi giữa các vòng đua, và tốc độ của các con gián là đôi một khác nhau. Sau mỗi vòng, người ta ghi lại thứ tự về đích của các con gián tham gia vòng đua đó. Hỏi 14 vòng đua có đủ để xác định chính xác theo thứ tự hai con gián chạy nhanh nhất không?*

Lời giải. Câu trả lời là khẳng định.

Ta dùng 9 vòng đầu loại 9 con chậm nhất. 3 vòng tiếp theo chọn ra con nhanh nhất trong 9 con nhanh nhất và loại 3 con chậm nhất. Vòng 13 chọn ra con nhanh nhất (vô địch) trong 3 con nhanh nhất. Lúc này chỉ còn 3 con có thể đứng nhì là con đứng nhì ở vòng 13, con đứng nhì trong cuộc đua với con vô địch ở vòng 3 trận và con đứng nhì ở cuộc đua với con vô địch ở 9 vòng đầu. Dùng trận 14 để tìm ra con thứ nhì từ 3 con này.

Bài 4 *Cho tam giác ABC với $\angle B = 30^\circ, \angle C = 105^\circ$ và D là trung điểm đoạn thẳng BC. Tìm góc $\angle BAD$?*

Lời giải. Hạ CH vuông góc với AB thì suy ra CHD là tam giác đều và AHC là tam giác vuông cân tại H. Từ đây suy ra tam giác AHD cân tại H và

$$\angle BAD = \angle HAD = 15^\circ.$$

Bài 5 *John có 12 que gỗ với độ dài mỗi que là một số nguyên dương không vượt quá 56. Chứng minh rằng John có 3 que có thể tạo thành một tam giác.*

Lời giải. Giả sử ngược lại, không có 3 que tạo thành tam giác. Xếp thứ tự chiều dài các que gỗ $a_1 \leq a_2 \leq ... \leq a_{12}$ thì từ giả thiết, ta sẽ suy ra $a_{n+2} \geq a_{n+1} + a_n$. Từ đây lần lượt suy ra

$$a_3 \geq a_2 + a_1 \geq 2, a_4 \geq a_3 + a_2 \geq 3, a_5 \geq a_4 + a_3 \geq 5.$$

Cứ như thế

$$a_6 \geq 8, a_7 \geq 13, a_8 \geq 21, a_9 \geq 34, a_{10} \geq 55, a_{11} \geq 89.$$

Điều này mâu thuẫn, suy sẽ John sẽ luôn tạo được tam giác.

Bài 6 *Hãy tìm một số nguyên dương sao cho tích các ước tự nhiên của nó là 10^{90}.*

Lời giải. Ta tìm số dưới dạng $2^m 5^n$. Các ước của số này có dạng

$$2^a \cdot 5^b \text{ với } 0 \leq a \leq m, 0 \leq b \leq n.$$

Từ đó tích các ước bằng $10^{\frac{mn(m+1)(n+1)}{4}}$ nên ta đưa về

$$mn(m+1)(n+1) = 360.$$

Chọn $m = 3, n = 5$ thì ta được một số thỏa mãn yêu cầu bài toán là $2^3 \cdot 5^5 = 25000$.

Bài 7 *Tất cả chúng ta đều biết* $3^2 + 4^2 = 5^2$. *Bên cạnh đó, không phải ai cũng biết rằng* $10^2 + 11^2 + 12^2 = 13^2 + 14^2$. *Liệu có tồn tại hay không* 2015 *số nguyên dương liên tiếp sao cho tổng bình phương của* 1008 *số đầu tiên bằng tổng bình phương của* 1007 *số sau đó?*

Lời giải. Câu trả lời là khẳng định, khi thay $1007, 1008$ bởi các số liên tiếp tùy ý.

Giả sử số đầu tiên của dãy là $n + 1$. Ta có:

$$\sum_{i=1}^{1008} (n+i)^2 = 1008n^2 + 2n\sum_{i=1}^{1008} i + \sum_{i=1}^{1008} i^2 \text{ và}$$

$$\sum_{i=1009}^{2015} (n+i)^2 = 1007n^2 + 2n\sum_{i=1009}^{2015} i + \sum_{i=1009}^{2015} i^2.$$

Để có đẳng thức $\sum_{i=1}^{1008} (n+i)^2 = \sum_{i=1009}^{2015} (n+i)^2$, ta cần xét phương trình:

$$\begin{aligned}
&1008n^2 + 2n\sum_{i=1}^{1008} i + \sum_{i=1}^{1008} i^2 = 1007n^2 + 2n\sum_{i=1009}^{2015} i + \sum_{i=1009}^{2015} i^2 \\
\Leftrightarrow\ &n^2 + 2n\left(\sum_{i=1}^{1008} i - \sum_{i=1009}^{2015} i\right) + \sum_{i=1}^{1008} i^2 - \sum_{i=1009}^{2015} i^2 = 0 \\
\Leftrightarrow\ &n^2 - 2n\left(\sum_{i=1}^{2015} i - 2\sum_{i=1}^{1008} i\right) - \left(\sum_{i=1}^{2015} i^2 - 2\sum_{i=1}^{1008} i^2\right) = 0
\end{aligned}$$

Thay $1008 = a$, ta có

$$\sum_{i=1}^{2015} i - 2\sum_{i=1}^{1008} i = \frac{(2a-1)2a - 2a(a+1)}{2} = a(a-2) \text{ và}$$

$$\sum_{i=1}^{2015} i^2 - 2\sum_{i=1}^{1008} i^2 = \frac{(2a-1)2a(4a-1) - 2a(a+1)(2a+1)}{6} = a^2(2a-3).$$

Do đó, ta có phương trình $n^2 - a(2a-4)n - a^2(2a-3) = 0$. Phương trình này có 2 nghiệm cố định là $n = -a, n = 2a^2 - 3a$. Vậy ta tìm được nghiệm dương là $n = 2029104$.

2. Đề thi dành cho Khối lớp R10

Bài 1 *Hai chú thỏ Bugs và Roger cá cược xem ai nhanh hơn. Để xác định người chiến thắng, hai bạn quyết định tổ chức một cuộc thi. Mỗi bạn thỏ sẽ nhảy* 50 *mét theo một hướng và sau đó quay lại để nhảy ngược lại. Biết rằng, độ dài mỗi bước nhảy của Bugs là* 50 *cm và của Roger là* 60*cm, nhưng thỏ Bugs nhảy được* 6 *bước trong khi Roger chỉ nhảy được* 5 *bước. Hỏi ai sẽ giành được chiến thắng?*

Lời giải. Giả sử rằng thời gian nhảy một bước của thỏ Bugs là 5 thì theo giả thiết, thời gian để nhảy được một bước của thỏ Roger là 6.

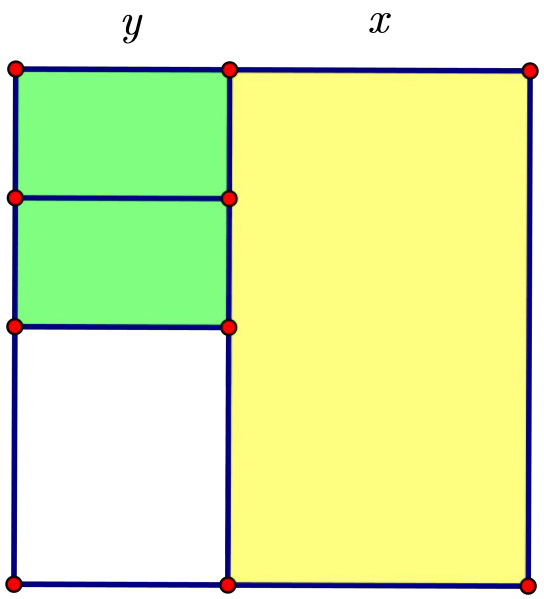
Để nhảy được hết $50 \times 2 = 100$ mét (đổi ra là 10000 cm) trong hai lượt, Bugs cần thời gian là: $10000 : 50 \times 5 = 1000$.

Trong khi đó, thỏ Roger cần phải thực hiện $\left\lceil \frac{10000}{60} \right\rceil = 168$ bước (vì 10000 không chia hết cho 60 nên thỏ cần nhảy thêm 1 bước). Thời gian thỏ Roger cần dùng là $168 \times 6 = 1008$.

Do đó, thỏ Bugs chiến thắng.

Bài 2 *Với những giá trị nào của n thì ta có thể chia một hình vuông thành n hình chữ nhật đồng dạng sao cho có ít nhất hai trong số chúng là không bằng nhau?*

Lời giải. Rõ ràng $n = 2$ không thỏa mãn. Ta sẽ chứng minh rằng mọi $n \geq 3$ đều thỏa mãn.



Trước hết, ta chia hình vuông thành 2 phần, một phần hình chữ nhật lớn bên phải và phần còn lại chia thành $n - 1$ hình chữ nhật nhỏ đồng dạng với nhau.

Tỷ lệ cạnh của hình chữ nhật màu vàng là $\frac{x+y}{x}$, tỷ lệ cạnh của hình chữ nhật màu xanh là $\frac{x+y}{(n-1)y}$. Để các hình chữ nhật đồng dạng thì phải có

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

Tỷ lệ này chọn được nên luôn tồn tại cách chia thỏa mãn đề bài.

Bài 3 *Có tồn tại hay không các số nguyên dương a và b sao cho*

$$lcm(a,b) = lcm(a+2015, b+2016)?$$

Ở đây, $lcm(a,b)$ được kí hiệu cho bội chung nhỏ nhất của hai số a và b.

Lời giải. Câu trả lời là khẳng định. Chẳng hạn, ta chọn $a = 2015$ thì cần tìm b sao cho

$$lcm(2015, b) = lcm(4030, b+2016)$$

Ta thấy rằng $2015 = 5 \cdot 13 \cdot 31$ và $2016 = 2^5 \cdot 3^2 \cdot 7$ nên có thể chọn b là ước của 2016 với dạng $2^a 3^b 7$ để có tổng $b + 2016$ cũng chỉ có ước nguyên tố thuộc $\{5, 13, 31, 2, 3, 7\}$.

Ta chọn được $b = 168$. Khi đó bội chung nhỏ nhất của cả hai cặp số đều là 338520.

Bài 4 *Cho tam giác ABC với $\angle B = 30^\circ, \angle C = 105^\circ$ và D là trung điểm đoạn thẳng BC. Tìm góc $\angle BAD$?*

Lời giải. Xem lời giải ở phần trước.

Bài 5 *Người ta điền vào các ô của bảng vuông 10×10 các số nguyên dương phân biệt sao cho tổng các số trên mỗi hàng, mỗi cột là bằng nhau và nhỏ nhất có thể. Biết rằng, các số $1, 2, \ldots, 9$ và 2015 đã được điền trước trên một đường chéo. Hỏi tổng đó có thể nhỏ nhất là bao nhiêu?*

Lời giải. Ta xét mô hình sau:

1									b_1
	2								b_2
		3							b_3
			4						b_4
				5					b_5
					6				b_6
						7			b_7
							8		b_8
								9	b_9
a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	2015

Đặt các số ở hàng cuối (trừ 2015) là $a_1, a_2, \ldots, a_9$ và các số ở cột cuối (trừ 2015) là $b_1, b_2, \ldots, b_9$. Ta cần có

$$\sum_{i=1}^{9} a_i = \sum_{i=1}^{9} b_i.$$

Chú ý rằng

$$\sum_{i=1}^{9} a_i + \sum_{i=1}^{9} b_i \geq 10 + 11 + 12 + \cdots + 27 = 333.$$

Tuy nhiên, tổng này phải chẵn nên ta có thể chọn

$$\sum_{i=1}^{9} a_i + \sum_{i=1}^{9} b_i = 334$$

và

$$\sum_{i=1}^{9} a_i = \sum_{i=1}^{9} b_i = 167.$$

Ta xây dựng được trường hợp $\sum\limits_{i=1}^{9} a_i = 10 + 11 + 12 + 13 + 24 + 25 + 26 + 28 + 18 = 167$ còn

$$\sum_{i=1}^{9} b_i = 14 + 15 + 16 + 17 + 19 + 20 + 21 + 22 + 23 = 167.$$

Tổng của hàng cuối và cột cuối là $167 + 2015 = 2182$. Khi đó, ta có thể không quá khó khăn để điền thêm vào các ô còn lại các số lớn hơn 28 và thỏa mãn điều kiện bài toán.

Vậy tổng nhỏ nhất là 2182.

Bài 6 *Đường tròn nội tiếp tam giác ABC tiếp xúc với các cạnh AB, BC và AC tại các điểm C_1, A_1 và B_1 tương ứng. Chứng minh rằng*

$$\frac{AC}{AB_1} + \frac{CB}{CA_1} + \frac{BA}{BC_1} > 4.$$

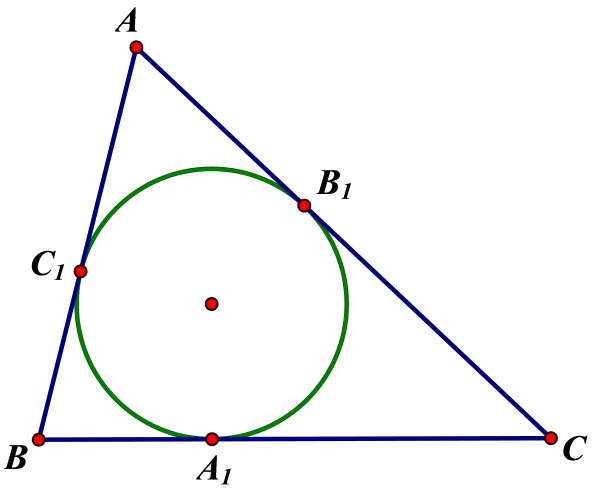
Lời giải.

Đặt $BC = a, CA = b, AB = c$ thì $AB_1 = \frac{b+c-a}{2}, CA_1 = \frac{a+b-c}{2}, BC_1 = \frac{c+a-b}{2}$. Ta cần chứng minh rằng

$$\begin{aligned} &\frac{2b}{b+c-a} + \frac{2a}{a+b-c} + \frac{2c}{c+a-b} > 4 \\ \Leftrightarrow\ &\frac{b}{b+c-a} + \frac{a}{a+b-c} + \frac{c}{c+a-b} > 2 \end{aligned}.$$

Theo BĐT Cauchy-Schwarz thì

$$\frac{b^2}{b(b+c-a)} + \frac{a^2}{a(a+b-c)} + \frac{c^2}{c(c+a-b)} \geq \frac{(a+b+c)^2}{a^2+b^2+c^2}.$$



Ta cần có

$$\frac{(a+b+c)^2}{a^2+b^2+c^2} > 2 \Leftrightarrow 2(ab+bc+ca) > a^2+b^2+c^2.$$

BĐT cuối đúng vì có thể viết thành $a(b+c-a)+b(c+a-b)+c(a+b-c)>0$.

Bài 7 *Tất cả chúng ta đều biết* $3^2+4^2=5^2$. *Bên cạnh đó, không phải ai cũng biết rằng* $10^2+11^2+12^2=13^2+14^2$. *Khẳng định sau đúng hay sai: Với mọi số nguyên dương* k, *có* $2k+1$ *số nguyên dương liên tiếp sao cho tổng bình phương của* $k+1$ *số đầu tiên bằng tổng bình phương của* k *số còn lại?*

Lời giải. Xem lời giải ở phần trước.

3. Đề thi dành cho Khối lớp R11

Bài 1 *Hai chú thỏ Bugs và Roger cá cược xem ai nhanh hơn. Để xác định người chiến thắng, hai bạn quyết định tổ chức một cuộc thi. Mỗi bạn thỏ sẽ nhảy* 50 *mét theo một hướng và sau đó quay lại để nhảy ngược lại. Biết rằng, độ dài mỗi bước nhảy của Bugs là* 50 *cm và của Roger là* 60*cm, nhưng thỏ Bugs nhảy được* 6 *bước trong khi Roger chỉ nhảy được* 5 *bước. Hỏi ai sẽ giành được chiến thăng?*

Lời giải. Xem lời giải ở phần trước.

Bài 2 *Với những giá trị nào của* n *thì ta có thể chia một hình vuông thành* n *hình chữ nhật đồng dạng sao cho có ít nhất hai trong số chúng là không bằng nhau?*

Lời giải. Xem lời giải ở phần trước.

Bài 3 *Có tồn tại hay không các số nguyên dương a và b sao cho*

$$lcm(a,b) = lcm(a+2015, b+2016)?$$

Ở đây, $lcm(a,b)$ được kí hiệu cho bội chung nhỏ nhất của hai số a và b.

Lời giải. Xem lời giải ở phần trước.

Bài 4 *Cho tam giác ABC với $\angle B = 30^\circ, \angle C = 105^\circ$ và D là trung điểm đoạn thẳng BC. Tìm góc $\angle BAD$?*

Lời giải. Xem lời giải ở phần trước.

Bài 5 *Tại mỗi điểm có tọa độ nguyên trên mặt phẳng tọa độ trồng một cây với đường kính 10^{-6}. Một bác tiều phu đốn cây tại gốc tọa độ $(0,0)$ và đứng trên gốc cây. Hỏi phần mặt phẳng mà anh ta nhìn thấy có bị giới hạn hay không? Ở đây, các cây được coi như là một cột hình trụ vô hạn với các trục chứa các điểm nguyên của mặt phẳng tọa độ.*

Lời giải. Giả sử anh tiều phu nhìn theo hướng của đường thẳng $\Delta : y = ma$ với $m \in (0; +\infty)$ (trường hợp còn lại chứng minh tương tự).

Khoảng cách từ một điểm $K(a,b)$ với $a, b \in \mathbb{Z}^+$ thì

$$d(K, \Delta) = \frac{|b - ma|}{\sqrt{1^2 + m^2}}$$

. Do đó, nếu như hướng nhìn bị che bởi gốc cây tại K thì

$$\frac{|b-ma|}{\sqrt{1+m^2}} < \frac{1}{10^6} \Leftrightarrow |b - ma| < \frac{\sqrt{1+m^2}}{10^6}.$$

Ta có bổ đề sau: Với mọi số vô tỷ dương m và với số $\varepsilon > 0$ nhỏ tùy ý, luôn tồn tại hai số nguyên dương a, b sao cho $|b - ma| < \varepsilon$.

Do đó, nếu m là số vô tỷ thì sẽ luôn tồn tại điểm K che hướng nhìn ở trên.

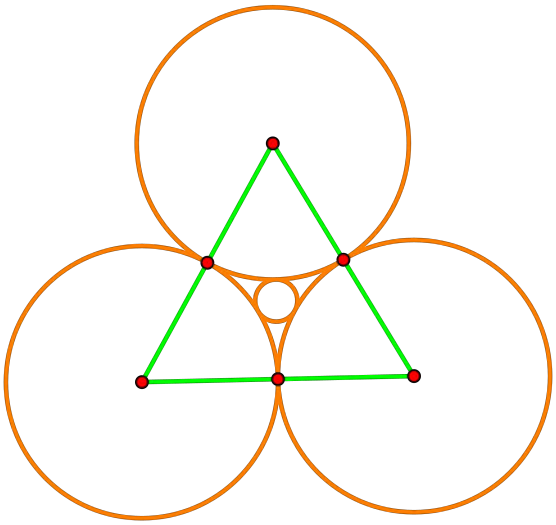
Xét m là số hữu tỷ và đặt $m = \frac{p}{q}$ với $p, q \in \mathbb{Z}^+, (p,q) = 1$. Khi đó đường thẳng này sẽ đi qua điểm $K(q,p)$, cũng không thỏa.

Vậy phần mặt phẳng mà anh ta nhìn thấy luôn bị giới hạn.

Bài 6 *Hãy chỉ ra một bộ* 4 *số dương không thể là bán kính của bốn hình cầu đôi một tiếp xúc.*

Lời giải. Gọi R_1, R_2, R_3, R_4 là bán kính của các hình cầu. Trước hết, ta chọn $R_1 = R_2 = R_3 = 1$ thì các hình cầu đều phải đôi một tiếp xúc ngoài.

Mặt phẳng đi qua các tâm của 3 hình cầu cắt chúng tạo thành mô hình như bên dưới:



Hình cầu thứ 4 muốn tiếp xúc được với các hình cầu đã có thì chỉ có hai khả năng là tiếp xúc về bên ngoài hoặc tiếp xúc phía trong. Ta sẽ chọn R_4 đủ nhỏ để nó không thể tiếp xúc trong.

Dễ dàng tính được tỷ số giữa bán kính đường tròn nhỏ so với các đường tròn lớn là $\dfrac{2\sqrt{3}}{3} - 1 \approx 0.155$. Ta chọn $R_4 = \dfrac{1}{10}$ thì bộ (R_1, R_2, R_3, R_4) thỏa mãn bài toán.

Bài 7 *Tất cả chúng ta đều biết* $3^2 + 4^2 = 5^2$. *Bên cạnh đó, không phải ai cũng biết rằng* $10^2 + 11^2 + 12^2 = 13^2 + 14^2$. *Khẳng định sau đúng hay sai: Với mọi số nguyên dương* k, *có* $2k + 1$ *số nguyên dương liên tiếp sao cho tổng bình phương của* $k + 1$ *số đầu tiên bằng tổng bình phương của* k *số còn lại?*

Lời giải. Xem lời giải ở phần trước.

CÁC VẤN ĐỀ CỔ ĐIỂN VÀ HIỆN ĐẠI

Ban biên tập

GIỚI THIỆU

Chuyên mục này dành cho các vấn đề cổ điển và hiện đại được trình bày dưới dạng các bài toán xâu chuỗi. Đó có thể là chuỗi các bài để giải bài toán đẳng chu, chứng minh đẳng thức Euler kỳ diệu $1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots = \frac{\pi^2}{6}$, một chuỗi bài toán vận trù ... Cách trình bày xuất phát từ những vấn đề đơn giản, dễ hiểu, những khái niệm mới sẽ được định nghĩa luôn trong bài để có thể đọc tương đối độc lập. Và mỗi một chuỗi bài sẽ nêu ra những vấn đề nhất định, có thể là giải quyết một bài toán kinh điển hay nêu ra những giả thuyết mới, những vấn đề mới. Lời giải và thảo luận về các bài toán sẽ được đăng ở số $N + 3$.

GIỚI THIỆU CUỘC THI HỌC THUẬT "ENTROPY – KHAI PHÁ DỮ LIỆU"

Lần I, Năm 2016

1. Mục đích

Với mục tiêu khai phá tiềm năng tri thức của thế hệ trẻ Việt Nam về lĩnh vực khoa học dữ liệu (Data Science), viện John von Neumann (JVN), đại diện khối ĐHQG Tp. HCM tổ chức cuộc thi Entropy lần 1 năm 2016 nhằm tạo cơ hội cho các bạn sinh viên, học viên cao học được phát huy năng lực chuyên môn và tư duy sáng tạo. Đây là một sân chơi học thuật chuyên nghiệp, giúp các bạn sinh viên, học viên cao học có cơ hội thực hành, phát triển khả năng nghiên cứu cũng như tích luỹ thêm kinh nghiệm trong chuyên ngành về lĩnh vực khoa học máy tính và phân tích dữ liệu.

Bên cạnh đó, cuộc thi Entropy lần đầu tiên tổ chức tại Việt Nam sẽ là cơ hội để các bạn trẻ yêu khoa học được biết đến lĩnh vực khoa học dữ liệu đang rất "nóng" tại các nước trên thế giới. Từ đó, cuộc thi tìm kiếm và mang đến những nguồn nhân lực tiềm năng cho nền kinh tế xã hội Việt Nam trong tương lai. Đây cũng chính là cơ hội để viện JVN giới thiệu về môi trường học tập, nghiên cứu cùng các cơ hội về học bổng du học tại các trường danh tiếng trên thế giới.

2. Thể lệ cuộc thi và giải thưởng

Đối tượng tham gia cuộc thi là các sinh viên, học viên cao học từ tất cả các trường đại học tại Việt Nam với độ tuổi từ 20 – 35 tuổi. Cuộc thi được chia là hai bảng: **Bảng A** dành cho đối tượng là các sinh viên năm cuối và **bảng B** dành cho các học viên cao học. Các thí sinh tham dự có thể đăng ký trực tiếp tại viện JVN hoặc đăng ký trực tiếp thông qua website của viện trong thời gian từ ngày **08/03/2016** đến ngày **31/05/2016**.

Thời gian tổ chức cuộc thi là từ ngày **02/04/2016** đến ngày **03/07/2016** và trải qua ba vòng: *Vòng loại (*04/06/2016*), vòng bán kết (*18/06/2016*) và vòng chung kết (*02/07/2016 *và* 03/07/2016*)*.* Những thí sinh xuất sắc nhất sẽ có cơ hội nhận được phần thưởng là các học bổng toàn phần tại viện **JVN** và tại các trường đại học danh tiếng trên thế giới (**ParisTech, France và Trinity College, Dublin, Ireland**).

3. Diễn biến cuộc thi

Chính thức được phát động vào tháng 03 năm 2016. Cuộc thi đã thu hút trên 250 thí sinh (cả bảng A và bảng B) từ các trường Đại học trên cả nước và cả thí sinh đang học tập và nghiên cứu tại nước ngoài.

a) Vòng sơ loại: Được diễn ra vào ngày 04/06/2016

Hình thức thi: Online.

Tổng số bài thi nhận được qua hệ thống : 173 bài làm.

Sau khi nhận được kết quả Ban Tổ chức chọn ra 150 thí sinh để tiếp tục vào vòng bán kết.

b) Vòng bán kết: Vòng bán kết của cuộc thi được tổ chức tại Viện John von Neumann

Thời gian: 18/06/2016

Hình thức thi: Gồm có 2 phần thi.

- Phần 1 : Thí sinh làm bài thi trên giấy bằng cách trả lời những câu trắc nghiệm giải toán và câu hỏi Story Telling nhằm đánh giá khả năng phân tích và suy luận của thí sinh.
- Phần 2 : Phần thi Coding, nhằm kiểm tra các kiến thức cơ bản về lập trình cũng như khả năng giải quyết vấn đề.

Sau vòng thi Bán kết Ban Tổ chức chọn ra 10 thí sinh bảng A và 6 thí sinh bảng B tranh tài tại vòng chung kết.

c) Vòng thi chung kết:

Thời gian : 02 và 03/07/2016

Hình thức thi: Trình bày trước hội đồng Ban giám khảo và bảo vệ đề tài.

Các thi sinh vào vòng chung kết được nhận một bộ dữ liệu và có 01 tuần để tiến hành phân tích và giải quyết các yêu cầu theo đề bài đưa ra dựa trên bộ dữ liệu được cung cấp.

Các thí sinh có 30 phút (bảng A) và 40 phút (Bảng B) để trình bày cũng như trả lời các câu hỏi đưa ra từ các thành viên Ban Giám khảo.

4. Kết quả cuộc thi

Bảng A

Giải nhất: Lý Quốc Thắng – Đại học Khoa học Tự nhiên (ĐHQG TP.HCM).

Giải nhì: Lê Tạ Đăng Khoa – Đại học FPT.

Giải ba:

- Lê Văn Duyệt – Đại học Công nghệ Thông tin (ĐHQG TP.HCM).
- Phan Trường Bửu – Đại học Quốc tế (ĐHQG TP.HCM).

- Nguyễn Đức Trí – Đại học Bách khoa (ĐHQG TP.HCM).

Giải khuyết khích:

- Phạm Thượng Hải – Đại học Khoa học Tự nhiên (ĐHQG TP.HCM).
- Nguyễn Nhật Nam – Đại học Bách khoa (ĐHQG TP.HCM).
- Phạm Minh Châu – Đại học Bách khoa (ĐHQG TP.HCM).
- Phạm Thị Thu Phương – Viện John von Neumann.
- Phó Ngọc Đăng Khoa – Đại học Khoa học Tự nhiên (ĐHQG TP.HCM).

Bảng B

Giải nhất: Lê Vũ Hoàng – Viện John von Neumann.

Giải nhì: Hoàng Như Thịnh – Đại học Kinh tế TP.HCM.

Giải ba: Nguyễn Ngọc Tuấn – Đại học Bách khoa (ĐHQG TP.HCM).

Giải khuyến khích:

- Hoàng Thanh Tùng – Đại học Công nghệ - ĐHQG HN.
- Đỗ Phúc Hảo – Đại học Bách Khoa Đà Nẵng.
- Trần Anh Duy – Đại học Khoa học Tự nhiên (ĐHQG TP.HCM).

5. Đề thi

Bảng A

Phần I – phân tích dữ liệu phi cấu trúc

Một công ty A hoạt động trong lĩnh vực nghiên cứu thị trường đã tiến hành thu thập dữ liệu từ các trang báo điện tử Việt Nam để khảo sát xem thị hiếu của người dân về các chủ đề xã hội và đời sống như thế nào. Từ đó hỗ trợ cho các công ty bán hàng làm chiến lược marketing hiệu quả hơn. Dữ liệu được lấy về, lưu trên một cơ sở dữ liệu dưới định dạng file văn bản (.txt) mà chưa qua bất kỳ khâu xử lý nào. Do trong quá trình lấy dữ liệu, các kỹ thuật viên của công ty A đã sơ suất quên ghi nhớ chủ đề cho từng bài viết khi được tải về. Những gì công ty A hiện có là một thư mục chứa hơn 28.000 file văn bản (text), mỗi file văn bản là nội dung một bài viết trên một trang báo nào đó.

Câu hỏi: Với số lượng bài viết lớn như vậy (hơn 28.000 bài viết), bạn hãy tìm cách nào đó để nhóm các bài viết theo những chủ đề khác nhau. Bạn hãy đề xuất một phương pháp để có thể đặt tên cho từng chủ đề một cách hợp lý nhất. Kết quả công ty A mong đợi sẽ là một file dạng csv gồm 2 cột: Cột 1 là tên bài báo, cột 2 là tên chủ đề tương ứng.

File dữ liệu được gửi kèm (Tên file: phan1.zip).

Phần II – Phân tích dữ liệu có cấu trúc

Phần kiến thức chuẩn bị

Công ty QK là một công ty chuyên sản xuất các loại thực phẩm ở Mỹ, trong đó có sản phẩm thịt trộn. Sản phẩm thịt trộn được đóng gói trong một lớp giấy bạc chứa bì lợn giòn kèm bột và các gia vị khác nhau. Người mua có thể trộn lẫn các thành phần như trứng và thịt bò để tạo ra phần thịt trộn. Sự trộn lẫn này có tác dụng làm tăng hương vị của sản phẩm.

QK là một thương hiệu có uy tín, mặc dù doanh thu của công ty không quá lớn nhưng công ty luôn có lợi nhuận ổn định. Giả sử bạn là giám đốc thương mại của QK, và phải xem xét lại kế hoạch sản xuất mặt hàng thịt trộn. Nhiệm vụ đầu tiên của bạn là chuẩn bị dự đoán doanh thu bán hàng, và kinh phí cho khuyến mãi và quảng cáo cho năm sau. Bạn có dữ liệu lịch sử của công ty. Dữ liệu này bao gồm doanh số bán hàng cũng như là các chi phí dành cho phần khuyến mãi và quảng cáo trong 24 quý vừa qua (đơn vị một ngàn USD). Ngoài ra, dữ liệu cũng bao gồm chỉ số index kinh tế trong thị trường bán thịt trộn. Giá trị chỉ số này cao thể hiện thời kì kinh tế tốt. Sản phẩm thịt trộn được bán thông qua các đại lý thực phẩm tại Texas, Ohio, Utah, và New York. Chi phí quảng cáo thường được dùng để trả các tạp chí về thực phẩm và sức khỏe. Chi phí khuyến mãi thì tập trung chi trả cho các đại lý phân phối và các quản lý cửa hàng. Các chi phí này bao gồm các khuyến mãi đặc biệt, ví dụ như mua bốn tặng một, tặng hoa hồng cho đại lý với doanh thu cao hay các cuộc thi bán hàng giữa các đại lý với giải thưởng là một chuyến đi du lịch ở Hawaii.

Bạn sẽ xem xét dữ liệu lịch sử và có thể thấy những biến đổi lớn trong doanh số bán hàng giữa các quý, và sự khác nhau cho các chi phí quảng cáo và khuyến mãi. Trong một cuộc họp, phó chủ tịch bán hàng giải thích rằng trước đây có một chính sách chung là chỉ nên chi trả cho quảng cáo hoặc khuyến mãi. Tuy nhiên, đã có một tranh cãi lâu dài trong công ty về hiệu quả tương tác giữa khuyến mãi và quảng cáo đối với doanh số thịt trộn. Người tiền nhiệm đã cố gắng thử nhiều phương pháp so sánh khác nhau nhưng chưa thể xác định được quảng cáo hay khuyến mãi là tốt hơn.

Một số ý kiến hoài nghi rằng việc dành chi tiêu cho khuyến mãi và quảng cáo là lãng phí bởi vì chúng không ảnh hưởng lắm đến vệc bán hàng. Một số người khác lại cảm thấy rằng việc khuyến mãi có tác động làm giảm doanh số bán hàng trong tương lai. Nghĩa là, họ cảm thấy các đại lý và quản lý cửa hàng mua rất nhiều trong thời gian khuyến mãi và sau đó không đặt hàng ở các giai đoạn tiếp theo cho đến khi họ cần. Tác động của quảng cáo cũng không rõ rệt, vì doanh số bán hàng thường thay đổi rất nhiều trong các giai đoạn mà chi phí quảng cáo như nhau. Ví dụ, trong hai quý 23 và 24 (xem bảng dữ liệu), chi phí quảng cáo gần bằng nhau (36, 000 USD và 39, 000 USD) nhưng doanh thu tương ứng là 648, 000 USD và 343, 000 USD.

Ngoài ra, một chuyên viên thuộc phòng tài chính nhấn mạnh rằng thị trường thịt trộn là thị trường "phản chu kỳ" (counter-cyclical) kinh tế, nghĩa là sản phẩm bán tốt hơn trong thời kỳ kinh tế đi xuống, và ngược lại. Anh ta cho rằng thịt trộn rẻ tiền hơn các loại thực phẩm khác, cho nên người ta thường mua nhiều hơn trong thời kỳ khó khăn. Hơn nữa, anh ta cho rằng doanh thu bán hàng có tính chất mùa vụ, với nhiều sản phẩm bán được trong những tháng lạnh hơn là những tháng nóng như mùa hè. Mùa lạnh ở Mỹ là Quý 4 và Quý 1, mùa nóng rơi vào Quý 2 và Quý 3.

Obs	**Sales**	**Prom**	**Adv.**	**Index**
1	504.72	15.6	30	100
2	406.59	22.2	36	102
3	398.55	0.0	45	104
4	587.76	0.0	57	104
5	598.92	0.0	39	104
6	703.62	31.8	21	100
7	387.24	21.3	12	98
8	365.67	3.9	6	96
9	388.71	0.0	6	98
10	372.96	8.4	30	103
11	603.30	45.3	30	105
12	614.73	50.1	33	107
13	484.38	39.6	6	107
14	227.76	4.2	33	107
15	329.13	0.0	6	108
16	308.25	0.0	3	105
17	433.86	0.0	45	103
18	514.98	13.8	48	108
19	404.70	17.7	0	110
20	245.43	0.0	15	112
21	433.20	17.4	9	113
22	627.24	37.8	54	112
23	647.61	42.3	36	113
24	342.81	11.4	39	114
Mean	455.51	16.0	26.6	105.5

Chú thích

- Obs (Observation) là dữ liệu thu thập từng quý, bắt đầu từ Quý 1.
- Sales là doanh số bán hàng của thịt trộn theo quý của QK (ngàn USD).
- Prom là chi tiêu dùng trong các hoạt động khuyến mãi trong từng quý (ngàn USD).
- Adv là chi tiêu dùng trong việc quảng cáo trong từng quý (ngàn USD).
- Index là chỉ số kinh tế của thị trường.

Phần câu hỏi

1. Đề xuất một mô hình hồi quy tuyến tính (linear regression) để dự đoán doanh số bán thịt trộn cho QK.

2. Nếu bạn có $1.000 để dành cho một trong hai việc quảng cáo và khuyến mãi, thì bạn nên chọn cái nào và tại sao? Có những tác động như thế nào đến việc sử dụng $1.000 trong mỗi việc quảng cáo hoặc khuyến mãi?

3. Bạn có đồng ý với ý kiến của chuyên viên phòng tài chính rằng thị trường thịt trộn có tính chất "phản chu kỳ" (counter-cyclical) so với chỉ số kinh tế? Tại sao?

4. Bạn có nghĩ rằng có tính chất mùa vụ trong doanh số bán hàng hay không? Tại sao?

Gợi ý trả lời câu hỏi: Các bạn thử cân nhắc các yếu tố sau đây:

- Mùa nóng tương ứng với quý 2 và 3, mùa lạnh tương ứng với quý 1 và 4.
- Điều kiện kinh tế thay đổi như thế nào.
- Ảnh hưởng của Khuyến mãi và Quảng cáo có kéo dài hay không.

Bảng B

Phần I – phân tích dữ liệu phi cấu trúc

Một công ty A hoạt động trong lĩnh vực nghiên cứu thị trường đã tiến hành thu thập dữ liệu từ các trang báo điện tử Việt Nam để khảo sát xem thị hiếu của người dân về các chủ đề xã hội và đời sống như thế nào. Từ đó hỗ trợ cho các công ty bán hàng làm chiến lược marketing hiệu quả hơn. Dữ liệu được lấy về, lưu trên một cơ sở dữ liệu dưới định dạng file văn bản (.txt) mà chưa qua bất kỳ khâu xử lý nào. Do trong quá trình lấy dữ liệu, các kỹ thuật viên của công ty A đã sơ suất quên ghi nhớ chủ đề cho từng bài viết khi được tải về. Những gì công ty A hiện có là một thư mục chứa hơn 28.000 file văn bản (text), mỗi file văn bản là nội dung một bài viết trên một trang báo nào đó.

Câu hỏi:

1. Với số lượng bài viết lớn như vậy (hơn 28.000 bài viết), bạn hãy tìm cách nào đó để nhóm các bài viết theo những chủ đề khác nhau. Bạn hãy đề xuất một phương pháp để có thể đặt tên cho từng chủ đề một cách hợp lý nhất. Kết quả công ty A mong đợi sẽ là một file dạng csv gồm 2 cột: Cột 1 là tên bài báo, cột 2 là tên chủ đề tương ứng.

2. Ngoài ra, công ty A muốn bạn chọn ra một chủ đề nào đó và nhờ bạn đề xuất một phương pháp tự động để đánh giá một bài báo bất kì trong chủ đề đó theo ba mức độ khác nhau (tích cực, tiêu cực và trung hòa). Bạn sẽ làm một chương trình hoàn chỉnh để giúp công ty giải quyết vấn đề này. Kết quả công ty A mong đợi sẽ là một file dạng csv gồm 2 cột: Cột 1 là tên bài báo, cột 2 là đánh giá tương ứng với bài báo đó.

Gợi ý: Các bạn xem xét sử dụng kỹ thuật "Sentiment Analysis" để giải quyết vấn đề này.

File dữ liệu được gửi kèm (Tên file: phan1.zip).

Phần II – Phân tích dữ liệu có cấu trúc

Phần kiến thức chuẩn bị

Công ty QK là một công ty chuyên sản xuất các loại thực phẩm ở Mỹ, trong đó có sản phẩm thịt trộn. Sản phẩm thịt trộn được đóng gói trong một lớp giấy bạc chứa bì lợn giòn kèm bột và các gia vị khác nhau. Người mua có thể trộn lẫn các thành phần như trứng và thịt bò để tạo ra phần thịt trộn. Sự trộn lẫn này có tác dụng làm tăng hương vị của sản phẩm.

QK là một thương hiệu có uy tín, mặc dù doanh thu của công ty không quá lớn nhưng công ty luôn có lợi nhuận ổn định. Giả sử bạn là giám đốc thương mại của QK, và phải xem xét lại kế hoạch sản xuất mặt hàng thịt trộn. Nhiệm vụ đầu tiên của bạn là chuẩn bị dự đoán doanh thu bán hàng, và kinh phí cho khuyến mãi và quảng cáo cho năm sau. Bạn có dữ liệu lịch sử của công ty. Dữ liệu này bao gồm doanh số bán hàng cũng như là các chi phí dành cho phần khuyến mãi và quảng cáo trong 24 quý vừa qua (đơn vị một ngàn USD). Ngoài ra, dữ liệu cũng bao gồm chỉ số index kinh tế trong thị trường bán thịt trộn. Giá trị chỉ số này cao thể hiện thời kì kinh tế tốt. Sản phẩm thịt trộn được bán thông qua các đại lý thực phẩm tại Texas, Ohio, Utah, và New York. Chi phí quảng cáo thường được dùng để trả các tạp chí về thực phẩm và sức khỏe. Chi phí khuyến mãi thì tập trung chi trả cho các đại lý phân phối và các quản lý cửa hàng. Các chi phí này bao gồm các khuyến mãi đặc biệt, ví dụ như mua bốn tặng một, tặng hoa hồng cho đại lý với doanh thu cao hay các cuộc thi bán hàng giữa các đại lý với giải thưởng là một chuyến đi du lịch ở Hawaii.

Bạn sẽ xem xét dữ liệu lịch sử và có thể thấy những biến đổi lớn trong doanh số bán hàng giữa các quý, và sự khác nhau cho các chi phí quảng cáo và khuyến mãi. Trong một cuộc họp, phó chủ tịch bán hàng giải thích rằng trước đây có một chính sách chung là chỉ nên chi trả cho quảng cáo hoặc khuyến mãi. Tuy nhiên, đã có một tranh cãi lâu dài trong công ty về hiệu quả tương tác giữa khuyến mãi và quảng cáo đối với doanh số thịt trộn. Người tiền nhiệm đã cố gắng thử nhiều phương pháp so sánh khác nhau nhưng chưa thể xác định được quảng cáo hay khuyến mãi là tốt hơn.

Một số ý kiến hoài nghi rằng việc dành chi tiêu cho khuyến mãi và quảng cáo là lãng phí bởi vì chúng không ảnh hưởng lắm đến vệc bán hàng. Một số người khác lại cảm thấy rằng việc khuyến mãi có tác động làm giảm doanh số bán hàng trong tương lai. Nghĩa là, họ cảm thấy các đại lý và quản lý cửa hàng mua rất nhiều trong thời gian khuyến mãi và sau đó không đặt hàng ở các giai đoạn tiếp theo cho đến khi họ cần. Tác động của quảng cáo cũng không rõ rệt, vì doanh số bán hàng thường thay đổi rất nhiều trong các giai đoạn mà chi phí quảng cáo như nhau. Ví dụ, trong hai quý 23 và 24 (xem bảng dữ liệu), chi phí quảng cáo gần bằng nhau (36, 000 USD và 39, 000 USD) nhưng doanh thu tương ứng là 648, 000 USD và 343, 000 USD.

Ngoài ra, một chuyên viên thuộc phòng tài chính nhấn mạnh rằng thị trường thịt trộn là thị trường "phản chu kỳ" (counter-cyclical) kinh tế, nghĩa là sản phẩm bán tốt hơn trong thời kỳ

kinh tế đi xuống, và ngược lại. Anh ta cho rằng thịt trộn rẻ tiền hơn các loại thực phẩm khác, cho nên người ta thường mua nhiều hơn trong thời kỳ khó khăn. Hơn nữa, anh ta cho rằng doanh thu bán hàng có tính chất mùa vụ, với nhiều sản phẩm bán được trong những tháng lạnh hơn là những tháng nóng như mùa hè. Mùa lạnh ở Mỹ là Quý 4 và Quý 1, mùa nóng rơi vào Quý 2 và Quý 3.

Obs	**Sales**	**Prom**	**Adv.**	**Index**
1	504.72	15.6	30	100
2	406.59	22.2	36	102
3	398.55	0.0	45	104
4	587.76	0.0	57	104
5	598.92	0.0	39	104
6	703.62	31.8	21	100
7	387.24	21.3	12	98
8	365.67	3.9	6	96
9	388.71	0.0	6	98
10	372.96	8.4	30	103
11	603.30	45.3	30	105
12	614.73	50.1	33	107
13	484.38	39.6	6	107
14	227.76	4.2	33	107
15	329.13	0.0	6	108
16	308.25	0.0	3	105
17	433.86	0.0	45	103
18	514.98	13.8	48	108
19	404.70	17.7	0	110
20	245.43	0.0	15	112
21	433.20	17.4	9	113
22	627.24	37.8	54	112
23	647.61	42.3	36	113
24	342.81	11.4	39	114
Mean	455.51	16.0	26.6	105.5

Chú thích

- Obs (Observation) là dữ liệu thu thập từng quý, bắt đầu từ Quý 1.
- Sales là doanh số bán hàng của thịt trộn theo quý của QK (ngàn USD).
- Prom là chi tiêu dùng trong các hoạt động khuyến mãi trong từng quý (ngàn USD).
- Adv là chi tiêu dùng trong việc quảng cáo trong từng quý (ngàn USD).
- Index là chỉ số kinh tế của thị trường.

Phần câu hỏi

1. Đề xuất một mô hình hồi quy tuyến tính (linear regression) để dự đoán doanh số bán thịt trộn cho QK.

2. Nếu bạn có $1.000 để dành cho một trong hai việc quảng cáo và khuyến mãi, thì bạn nên chọn cái nào và tại sao? Có những tác động như thế nào đến việc sử dụng $1.000 trong mỗi việc quảng cáo hoặc khuyến mãi?

3. Bạn có đồng ý với ý kiến của chuyên viên phòng tài chính rằng thị trường thịt trộn có tính chất "phản chu kỳ" (counter-cyclical) so với chỉ số kinh tế? Tại sao?

4. Bạn có nghĩ rằng có tính chất mùa vụ trong doanh số bán hàng hay không? Tại sao?

Gợi ý trả lời câu hỏi: Các bạn thử cân nhắc các yếu tố sau đây:

- Mùa nóng tương ứng với quý 2 và 3, mùa lạnh tương ứng với quý 1 và 4.
- Điều kiện kinh tế thay đổi như thế nào.
- Ảnh hưởng của Khuyến mãi và Quảng cáo có kéo dài hay không.

Yêu cầu của ban tổ chức

1. Phần I đánh giá về khả năng chuyên môn trong lĩnh vực khoa học dữ liệu và khả năng trình bày báo cáo. Phần II đánh đánh giá cả về khả năng chuyên môn trong lĩnh vực khoa học dữ liệu, khả năng sáng tạo, khả năng trình bày (bằng powerpoint) và khả năng phản biện trước Ban Giám khảo.

2. Phần I và II: Thí sinh làm và viết báo cáo dạng word (hoặc chuyển thành file dạng pdf) gửi về BTC Cuộc thi để chấm năng lực chuyên môn và trình bày, gửi về BTC trước 17 giờ ngày 30/6/2016 qua email TS.Nguyễn Minh Trung – trung.nguyenminh@jvn.edu.vn.

3. Phần II: Thí sinh chuẩn bị báo cáo này trên file dạng powerpoint để trình bày và trả lời câu hỏi của Ban Giám khảo trong ngày thi chung kết. Bảng A thi ngày 02/07/2016. Bảng B thi ngày 03/07/2016.