

# Phương pháp chứng minh

Trần Vĩnh Đức

HUST

Ngày 6 tháng 9 năm 2018

## Bài tập

- ▶ GS Mc Brain và vợ là bà April tới một bữa tiệc ở đó có 4 đôi vợ chồng khác.
- ▶ Có một vài cặp bắt tay nhau nhưng không ai bắt tay với vợ hoặc chồng mình.
- ▶ GS hỏi mọi người khác xem họ bắt tay bao nhiêu người và ông ấy nhận được 9 con số khác nhau.
- ▶ Hỏi có bao nhiêu người đã bắt tay April?

# Tài liệu tham khảo

- ▶ Eric Lehman, F Thomson Leighton & Albert R Meyer, *Mathematics for Computer Science*, 2013 (Miễn phí)
- ▶ K. Rosen, *Toán học rời rạc ứng dụng trong tin học* (Bản dịch Tiếng Việt)

## Định nghĩa

Chứng minh toán học của một **mệnh đề** là một dãy **suy luận logic** dẫn đến mệnh đề này từ một tập **tiên đề**.

# Nội dung

Mệnh đề, tiên đề, và suy luận logic

Phương pháp chứng minh

Nguyên lý sắp thứ tự tốt

## Định nghĩa

Mệnh đề là một khẳng định hoặc đúng hoặc sai.

- ▶ Mệnh đề  $2 + 3 = 5$  ✓
- ▶ Mệnh đề  $1 + 1 = 3$  ✗

# Khẳng định không phải mệnh đề

- ▶ “Đưa tôi cái bánh!”
- ▶ “Bây giờ là 5 giờ”

## Mệnh đề

Với mọi số nguyên dương  $n$ , giá trị

$$p(n) ::= n^2 + n + 41$$

là số nguyên tố.

▶  $p(0) = 41$  ✓

▶  $p(1) = 43$  ✓

▶  $p(2) = 47$  ✓

▶  $p(3) = 53$  ✓

▶ ...

▶  $p(39) = 1601$  ✓

nhưng

$$p(40) = 40^2 + 40 + 41 = 41 \times 41 \quad \times$$



## Mệnh đề (Giả thuyết Euler, 1769)

Phương trình

$$a^4 + b^4 + c^4 = d^4$$

không có nghiệm khi  $a, b, c, d$  là số nguyên dương.

Năm 1988, Noam Elkies đã chứng minh là sai với phản ví dụ

$$\begin{array}{ll} a = 95800, & b = 217519, \\ c = 414560, & d = 422481 \end{array}$$

## Mệnh đề

Phương trình

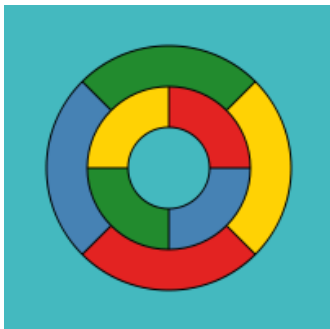
$$313(x^3 + y^3) = z^3$$

không có nghiệm nguyên dương.

Mệnh đề này cũng sai nhưng phản ví dụ nhỏ nhất có nhiều hơn 1000 chữ số.

## Mệnh đề (Định lý bốn màu)

Mọi bản đồ đều có thể tô được chỉ bằng bốn màu sao cho hai vùng kề nhau có màu khác nhau.



Hình: Bản đồ tô 5 màu

## Mệnh đề (Định lý bốn màu)

Mọi bản đồ đều có thể tô được chỉ bằng bốn màu sao cho hai vùng kề nhau có màu khác nhau.

Appel & Hakel đã phân loại các bản đồ và dùng máy tính để kiểm tra xem chúng có tô được bằng 4 màu. Họ đã hoàn tất chứng minh năm 1976. Tuy nhiên

- ▶ Chứng minh quá dài để có thể kiểm tra mà không dùng máy tính.
- ▶ Không ai đảm bảo rằng chương trình máy tính này chạy đúng.
- ▶ Không ai đủ nhiệt tình để kiểm tra hết hàng nghìn trường hợp đã được chứng minh.

## Mệnh đề (Định lý cuối cùng của Fermat)

Phương trình

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

không có nghiệm nguyên với  $n \geq 3$ .

- ▶ Bài toán được viết trong một quyển sách Fermat đọc năm 1630.
- ▶ Andrew Wiles chứng minh là đúng năm 1994.

## Mệnh đề (Giả thuyết Goldbach)

Mọi số nguyên chẵn lớn hơn 2 đều là tổng của hai số nguyên tố.

- ▶ Được giả thuyết năm 1742
- ▶ Đã được khẳng định là đúng với mọi số không lớn hơn  $10^{16}$ .
- ▶ ✓ hay ✗ ?

## Định nghĩa

Vị từ là một mệnh đề mà giá trị chân lý phụ thuộc vào một hoặc nhiều biến.

$p(n) ::= "n \text{ là số bình phương hoàn hảo}"$

$p(4) = "4 \text{ là số bình phương hoàn hảo}"$

$p(4) = \checkmark$

$p(5) = \times$

# Phương pháp tiên đề

- ▶ Thủ tục chuẩn để thiết lập các giá trị chân lý trong toán học đã được phát triển khoảng từ 300 BC bởi Euclid.
- ▶ Bắt đầu từ 5 “giả sử” để xây dựng hình học Euclid. Ví dụ:  
*Qua một điểm nằm ngoài một đường thẳng ta vẽ được một và chỉ một đường thẳng song song với đường thẳng đã cho.*
- ▶ Các mệnh đề như thế này được thừa nhận là đúng được gọi là tiên đề.
- ▶ Bắt đầu từ các tiên đề này, Euclid thiết lập giá trị chân lý của các mệnh đề khác bằng cách đưa ra “chứng minh”.
- ▶ Chứng minh là một dãy các lập luận logic từ tập tiên đề dẫn đến mệnh đề cần chứng minh.



# Một số thuật ngữ cho mệnh đề

- ▶ Mệnh đề đúng và quan trọng gọi là *định lý*.
- ▶ *Bổ đề* là mệnh đề chuẩn bị có ích để chứng minh các mệnh đề khác.
- ▶ *Hệ quả* là một mệnh đề mà chứng minh nó chỉ cần vài bước từ một định lý.

# Hệ tiên đề của chúng ta

- ▶ Về cơ bản, toán học hiện đại dựa trên hệ tiên đề ZFC (Zermelo-Fraenkel with Choice) cùng với một vài quy tắc suy luận logic.
- ▶ Tuy nhiên, chúng quá tối giản. Ví dụ, một chứng minh hình thức trong ZFC cho  $2 + 2 = 4$  cần nhiều hơn 20,000 bước lập luận!
- ▶ Trong môn học này, ta thừa nhận mọi sự kiện trong toán “phổ thông” như tiên đề.

# Suy luận logic

- ▶ Luật Modus Ponens:

$$\frac{P, \quad P \Rightarrow Q}{Q}$$

(Một chứng minh của  $P$  và một chứng minh  $P$  suy ra  $Q$  là một chứng minh của  $Q$ )

- ▶ Luật

$$\frac{P \Rightarrow Q, \quad Q \Rightarrow R}{P \Rightarrow R}$$

- ▶ Luật

$$\frac{\neg P \Rightarrow \neg Q}{Q \Rightarrow P}$$

# Không phải luật

$$\frac{\neg P \Rightarrow \neg Q}{P \Rightarrow Q} \quad \times$$

## Ví dụ

- ▶ Nếu 4 là số nguyên tố, thì “tôi không biết bay”. ✓
- ▶ Nếu 4 không phải số nguyên tố, thì “tôi biết bay”. ✗.

# Nội dung

Mệnh đề, tiên đề, và suy luận logic

Phương pháp chứng minh

Nguyên lý sắp thứ tự tốt

# Chứng minh mệnh đề “Nếu ... thì”

Để chứng minh mệnh đề  $P \Rightarrow Q$ :

1. Viết, “Giả sử  $P$ ”.
2. Chỉ ra bằng lập luận logic rằng  $Q$  đúng.

## Định lý

Nếu  $0 \leq x \leq 2$  thì  $-x^3 + 4x + 1 > 0$ .

## Chứng minh.

Giả sử  $0 \leq x \leq 2$ . Vậy các số

$$x, \quad 2 + x, \quad 2 - x$$

đều lớn hơn hoặc bằng 0. Vậy

$$x(2 - x)(2 + x) \geq 0$$

Thêm 1 vào tích trên ta được

$$x(2 - x)(2 + x) + 1 > 0$$

Khai triển tích ta được  $-x^3 + 4x + 1 > 0$ .



# Chứng minh bằng phản đảo

- ▶ Phản đảo của mệnh đề  $P \Rightarrow Q$  là mệnh đề  $\neg Q \Rightarrow \neg P$ .
- ▶ Ta chứng minh như sau:
  1. Viết “Ta chứng minh mệnh đề phản đảo:” và đưa ra mệnh đề phản đảo.
  2. Làm như phương pháp chứng minh “Nếu ... thì”.



## Định lý

Nếu  $r$  là số vô tỷ, vậy  $\sqrt{r}$  cũng là số vô tỷ.

## Chứng minh.

- ▶ Ta chứng minh mệnh đề phản đảo: Nếu  $\sqrt{r}$  là số hữu tỉ, vậy  $r$  là số hữu tỉ.
- ▶ Giả sử rằng  $\sqrt{r}$  là số hữu tỉ. Có nghĩa rằng có hai số nguyên  $p, q$  sao cho  $\sqrt{r} = p/q$ .
- ▶ Bình phương hai vế ta được

$$\frac{p^2}{q^2} = r$$

- ▶ Vì  $p^2, q^2$  đều là số nguyên nên  $r$  là số hữu tỉ. □

# Chứng minh mệnh đề “Nếu và chỉ nếu”

Có hai cách chứng minh:

## 1. Chứng minh

$P \Leftrightarrow Q$  tương đương với hai chứng minh  $\begin{cases} P \Rightarrow Q \\ Q \Rightarrow P \end{cases}$

## 2. Xây dựng dãy “nếu và chỉ nếu”.

# Chứng minh bằng cách chia trường hợp

## Định lý

Mọi nhóm gồm 6 người đều có 3 người hoặc đôi một quen nhau, hoặc đôi một lạ nhau.

## Chứng minh.

Xét  $x$  là một trong 6 người. Có hai trường hợp tương tự nhau:

1. Trong 5 người khác  $x$ , có ít nhất 3 người đều quen  $x$ .
2. Trong 5 người khác  $x$ , có ít nhất 3 người đều lạ  $x$ .

Tại sao?

# Chứng minh bằng cách chia trường hợp

## Định lý

Mọi nhóm gồm 6 người đều có 3 người hoặc đôi một quen nhau, hoặc đôi một lạ nhau.

## Chứng minh trường hợp 1.

Trong 5 người khác  $x$ , có ít nhất 3 người đều quen  $x$ .

Có hai trường hợp con:

1. Không có cặp nào trong số 3 người này quen nhau. ✓
2. Có một cặp trong 3 người này quen nhau. Vậy cặp này cùng với  $x$  tạo thành 3 người quen nhau từng đôi một. ✓



# Chứng minh phản chứng

Để chứng minh mệnh đề  $P$  bằng phản chứng:

1. Viết “Ta chứng minh dùng phản chứng”.
2. Viết “Giả sử  $P$  sai.”
3. Dẫn ra một sự kiện đã biết là sai (một phản chứng).
4. Viết “Điều này mâu thuẫn. Vậy  $P$  phải đúng.”

## Định lý

$\sqrt{2}$  là số vô tỉ.

## Chứng minh.

- ▶ Ta chứng minh dùng phản chứng.
- ▶ Giả sử  $\sqrt{2}$  là số hữu tỉ.
- ▶ Vậy ta có thể viết  $\sqrt{2} = p/q$  ở dạng phân số tối giản.
- ▶ Ta có

$$\sqrt{2} = \frac{p}{q} \Rightarrow 2 = \frac{p^2}{q^2} \Rightarrow 2q^2 = p^2$$

- ▶ Vậy  $p$  chia hết cho 2. Tại sao? Nên  $p^2$  chia hết cho 4.
- ▶ Vậy  $q^2$  chia hết cho 2. Nên  $q$  chia hết cho 2.
- ▶ Vậy  $p/q$  không tối giản. ✗



# Nội dung

Mệnh đề, tiên đề, và suy luận logic

Phương pháp chứng minh

Nguyên lý sắp thứ tự tốt

## Nguyên lý sắp thứ tự tốt (STTT)

Mọi tập số nguyên **không âm khác rỗng** đều có phần tử nhỏ nhất.

- ▶ Tập rỗng không có phần tử nhỏ nhất.
- ▶ Không đúng với tập số âm. Ví dụ tập

$$\{\dots, -3, -2, -1\}$$

- ▶ Không đúng với mọi tập số hữu tỉ. Ví dụ tập

$$\left\{ \frac{1}{1}, \frac{1}{2}, \frac{1}{3}, \dots \right\}$$



## Định lý

Mọi số hữu tỉ  $m/n$  đều viết được dưới dạng  $x/y$  sao cho  $x, y$  không có ước chung nguyên tố.

## Chứng minh.

- ▶ Giả sử ngược lại có  $m, n$  không viết được như trên.
- ▶ Xét  $C$  là tập **tử số** của các phân số như vậy. Vậy  $C \neq \emptyset$  vì  $m \in C$ .
- ▶ Theo nguyên lý STTT, có số nhỏ nhất  $m_0 \in C$ .
- ▶ Theo định nghĩa của tập  $C$ , có số  $n_0$  để  $m_0/n_0$  không viết được ở dạng trên.

## Chứng minh (tiếp).

- ▶ Có nghĩa rằng  $m_0, n_0$  có ước chung nguyên tố  $p > 0$ . Vậy

$$\frac{m_0/p}{n_0/p} = \frac{m_0}{n_0}$$

- ▶ Vì  $m_0/n_0$  không thể viết ở dạng trên. Vậy  $\frac{m_0/p}{n_0/p}$  cũng không viết được ở dạng trên.
- ▶ Vậy ta có

$$\frac{m_0}{p} \in C \quad \text{và} \quad \frac{m_0}{p} < m_0 \quad \text{X}$$



# Chứng minh dùng STTT

Để chứng minh  $P(n)$  đúng với mọi số nguyên không âm  $n$ , ta làm như sau

- ▶ Định nghĩa tập phản ví dụ của  $P$  :

$$C ::= \{n \in \mathbb{N} \mid \neg P(n) \text{ đúng} \}$$

- ▶ Giả sử phản chứng rằng  $C \neq \emptyset$ .
- ▶ Bởi nguyên lý STTT có phần tử nhỏ nhất  $c \in C$ .
- ▶ Đưa ra phản chứng: thường bằng cách chỉ ra  $P(c)$  đúng hoặc chỉ ra một phần tử  $d \in C$  và  $d < c$ .
- ▶ Kết luận rằng  $C$  rỗng, có nghĩa rằng không có phản ví dụ.

## Định lý

Mọi số nguyên dương lớn hơn một đều phân tích được thành tích các số nguyên tố.

## Chứng minh bằng STTT.

- ▶ Giả sử tập phản ví dụ của định lý  $C \neq \emptyset$ .
- ▶ Có phần tử  $n$  nhỏ nhất thuộc  $C$ . Vậy  $n$  không nguyên tố. Có nghĩa rằng

$$n = a \cdot b \quad \text{với} \quad a, b > 1$$

- ▶ Hơn nữa  $a, b$  phải phân tích được thành tích các số nguyên tố. Tại sao?

$$a = p_1 \cdots p_k \quad \text{và} \quad b = q_1 \cdots q_m$$

- ▶ Vậy  $n = p_1 \cdots p_k \cdot q_1 \cdots q_m$ .



## Định lý

Mọi số nguyên dương đều thú vị.

## Chứng minh.

- ▶ Xét  $S$  là tập các số nguyên dương **không** thú vị.
- ▶ Nếu  $S$  **khác** rỗng,  $S$  chứa phần tử nhỏ nhất  $n$ .
- ▶ Nhưng là phần tử nhỏ nhất của một tập phải là một tính chất thú vị.
- ▶ Vậy  $n$  không thuộc  $S$ . **X**

