

IMO 2026 - Bài 1

Quá trình gcd/lcm, thuật toán Euclid trên số mũ và dạng chuẩn duy nhất

THÔNG TIN TÀI LIỆU

Kết quả cuối:

$$M = \prod_p p^{\gcd(v_p(x_1), \dots, v_p(x_{2026}))}.$$

Kiến trúc chứng minh: monovariant từ điển cho tính dừng, sau đó invariant theo từng số nguyên tố để xác định dạng chuẩn.

1 Đề bài

Trên bảng có 2026 số nguyên lớn hơn 1, không nhất thiết khác nhau. Trong một bước, Khổng Tử chọn hai số $m, n > 1$ ở hai vị trí khác nhau và thay chúng bằng

$$\gcd(m, n) \quad \text{và} \quad \frac{\text{lcm}(m, n)}{\gcd(m, n)}.$$

Ông tiếp tục chừng nào còn có thể.

- (a) Chứng minh rằng sau hữu hạn bước còn đúng một số $M > 1$.
 (b) Chứng minh rằng M không phụ thuộc vào các lựa chọn.

2 Bản đồ chiến lược

Phân rã nghĩa vụ

1. Chứng minh mỗi bước luôn tạo ra số nguyên dương.
2. Tìm một đại lượng sắp tốt buộc quá trình kết thúc.
3. Mô tả trạng thái cuối.
4. Tìm invariant đủ mạnh để xác định duy nhất số cuối.

Điểm then chốt là không dùng một đại lượng cho cả hai nhiệm vụ. Tính dừng được xử lý bằng một *monovariant*; tính độc lập đường đi được xử lý bằng một *invariant* khác.

3 Phép biến đổi theo số mũ nguyên tố

Cố định một số nguyên tố p . Đặt

$$a = v_p(m), \quad b = v_p(n).$$

Khi đó

$$v_p(\gcd(m, n)) = \min(a, b)$$

và

$$v_p\left(\frac{\text{lcm}(m, n)}{\gcd(m, n)}\right) = \max(a, b) - \min(a, b) = |a - b|.$$

Vì thế, ở cột số mũ của p , một bước có dạng

$$(a, b) \mapsto (\min(a, b), |a - b|).$$

Đây chính là một bước của thuật toán Euclid dạng trừ.

4 Phần (a): quá trình kết thúc

Với số nguyên dương x , ký hiệu

$$\Omega(x) = \sum_p v_p(x),$$

tức tổng các số mũ trong phân tích nguyên tố của x .

Tại một trạng thái của bảng, đặt

$$S = \sum_{i=1}^{2026} \Omega(x_i), \quad k = \#\{i : x_i > 1\}.$$

Xét cặp (S, k) theo thứ tự từ điển.

Giả sử một bước chọn m, n và đặt $d = \gcd(m, n)$. Với từng số nguyên tố p , tổng hai số mũ thay đổi từ

$$a + b$$

thành

$$\min(a, b) + |a - b| = \max(a, b).$$

Mức giảm là $\min(a, b)$. Cộng trên mọi p ,

$$S_{\text{mới}} = S_{\text{cũ}} - \Omega(d).$$

- Nếu $d > 1$, thì $\Omega(d) > 0$, nên S giảm nghiêm ngặt.
- Nếu $d = 1$, hai số mới là 1 và mn . Khi đó S không đổi nhưng k giảm đúng 1.

Do đó sau mỗi bước,

$$(S, k)_{\text{mới}} <_{\text{lex}} (S, k)_{\text{cũ}}.$$

Không tồn tại dãy giảm vô hạn trong $\mathbb{N}^2$ với thứ tự từ điển. Vậy quá trình phải kết thúc sau hữu hạn bước.

Bổ đề 4.1. Trong mọi bước, hai số mới không thể đồng thời bằng 1.

Chứng minh. Nếu $\gcd(m, n) > 1$, số thứ nhất đã lớn hơn 1. Nếu $\gcd(m, n) = 1$, số thứ hai bằng $mn > 1$. $\square$

Vì ban đầu có các số lớn hơn 1, trong suốt quá trình luôn còn ít nhất một số lớn hơn 1.

Khi quá trình dừng, không thể còn hai số lớn hơn 1, vì khi đó vẫn có thể chọn chúng để thực hiện một bước. Vậy trạng thái cuối có đúng một số $M > 1$ và tất cả các số còn lại bằng 1.

Kết luận phần (a)

Bất kể cách chọn các cặp, sau hữu hạn bước trên bảng còn đúng một số $M > 1$.

5 Phần (b): invariant xác định số cuối

Cố định số nguyên tố p . Tại một trạng thái, đặt

$$g_p = \gcd(v_p(x_1), v_p(x_2), \dots, v_p(x_{2026})).$$

Nếu một bước thay hai số mũ a, b bằng $\min(a, b), |a - b|$, thì

$$\gcd(\min(a, b), |a - b|) = \gcd(a, b).$$

Thật vậy, giả sử $a \geq b$, khi đó

$$\gcd(\min(a, b), |a - b|) = \gcd(b, a - b) = \gcd(a, b).$$

Các số mũ khác không đổi, nên g_p là invariant của toàn bộ quá trình.

Ở trạng thái cuối, chỉ còn số $M > 1$. Dãy số mũ của p có dạng

$$0, 0, \dots, 0, v_p(M), 0, \dots, 0.$$

Do đó gcd của dãy này bằng $v_p(M)$. Vì g_p không đổi,

$$v_p(M) = \gcd(v_p(x_1), \dots, v_p(x_{2026})).$$

Suy ra

$$M = \prod_p p^{\gcd(v_p(x_1), \dots, v_p(x_{2026}))}.$$

Tích chỉ chạy trên hữu hạn số nguyên tố xuất hiện trong các số ban đầu.

Công thức trên chỉ phụ thuộc trạng thái ban đầu, nên M không phụ thuộc vào thứ tự lựa chọn.

Đáp án hoàn chỉnh

$$M = \prod_p p^{\gcd_i v_p(x_i)}$$

và quá trình luôn kết thúc ở trạng thái gồm M cùng 2025 số 1.

6 Kiểm toán các bất thường gặp

Bẫy 1: gcd của các số trên bảng không bất biến

Ví dụ

$$(8, 4) \rightarrow (4, 2) \rightarrow (2, 2) \rightarrow (2, 1).$$

Số cuối là 2, trong khi $\gcd(8, 4) = 4$.

Bẫy 2: không phải mỗi bước đều làm một số mũ bằng 0

Ví dụ

$$(5, 3) \rightarrow (3, 2).$$

Phép biến đổi là Euclid dạng trừ, có thể cần nhiều bước.

Bẫy 3: tổng số mũ không luôn giảm

Nếu $\gcd(m, n) = 1$, ví dụ $(2, 3) \rightarrow (1, 6)$, tổng số mũ giữ nguyên. Vì vậy cần cập từ điển (S, k) chứ không chỉ S .

7 Góc nhìn cấu trúc

Bài toán là một hệ viết lại có nhiều đường đi. Phần (a) là bài toán *termination*. Phần (b) là bài toán *unique normal form*. Valuation v_p tách một phép toán số học phức tạp thành các bước Euclid độc lập trên từng cột, còn invariant gcd của cột ghép các kết quả trở lại thành một số duy nhất.