

COPYRIGHT NOTICE

THÔNG BÁO BẢN QUYỀN

© 2023 Duc A. Hoang (Hoàng Anh Đức)

COPYRIGHT (English):

This document is licensed under Creative Commons Attribution-ShareAlike 4.0 International (CC-BY-SA 4.0). You are free to share and adapt this material with appropriate attribution and under the same license.

This document is not up to date and may contain several errors or outdated information.

Last revision date: 2023-04-01

BẢN QUYỀN (Tiếng Việt):

Tài liệu này được cấp phép theo Giấy phép Quốc tế Creative Commons Attribution-ShareAlike 4.0 (CC-BY-SA 4.0). Bạn được tự do chia sẻ và chỉnh sửa tài liệu này với điều kiện ghi nguồn phù hợp và sử dụng cùng loại giấy phép.

Tài liệu này không được cập nhật và có thể chứa nhiều lỗi hoặc thông tin cũ.

Ngày sửa đổi cuối cùng: 2023-04-01



Creative Commons Attribution-ShareAlike 4.0 International

VNU-HUS MAT3500: Toán rời rạc

Lời giải Bài tập 6 trong slides Lý thuyết số cơ bản I

Hoàng Anh Đức

Bộ môn Tin học, Đại học KHTN, ĐHQG Hà Nội
hoanganhduc@hus.edu.vn

Đề bài: Nếu các số nguyên dương a và b được phân tích thành tích các số nguyên tố

$$a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n} \quad b = p_1^{b_1} p_2^{b_2} \dots p_n^{b_n}$$

trong đó các số mũ là các số nguyên không âm (có thể bằng 0), thì

$$\gcd(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \dots p_n^{\min(a_n, b_n)}$$

Ta sẽ sử dụng mệnh đề sau (Bài tập 5): Nếu p là một số nguyên tố và $p \mid a_1 a_2 \dots a_n$ trong đó $a_i \in \mathbb{Z}$ với $1 \leq i \leq n$, thì $p \mid a_j$ với j nào đó ($1 \leq j \leq n$).

Chứng minh. Đặt $P = \gcd(a, b)$ và $Q = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \dots p_n^{\min(a_n, b_n)} = p_1^{m_1} p_2^{m_2} \dots p_n^{m_n}$ trong đó $m_i = \min(a_i, b_i)$ với $1 \leq i \leq n$. Để chứng minh $P = Q$, ta chứng minh $P \leq Q$ và $Q \leq P$.

- (1) **Ta chứng minh $Q \leq P$.** Do $m_i \leq a_i$ và $m_i \leq b_i$ với $1 \leq i \leq n$, ta có thể viết $a_i = m_i + k_i$ và $b_i = m_i + \ell_i$ với các số nguyên $k_i, \ell_i \geq 0$ nào đó.

$$\begin{aligned} a &= p_1^{a_1} p_2^{a_2} \dots p_n^{a_n} \\ &= p_1^{m_1 + k_1} p_2^{m_2 + k_2} \dots p_n^{m_n + k_n} \\ &= (p_1^{m_1} \cdot p_1^{k_1}) (p_2^{m_2} \cdot p_2^{k_2}) \dots (p_n^{m_n} \cdot p_n^{k_n}) \\ &= (p_1^{m_1} p_2^{m_2} \dots p_n^{m_n}) \cdot (p_1^{k_1} p_2^{k_2} \dots p_n^{k_n}) \\ &= Q \cdot (p_1^{k_1} p_2^{k_2} \dots p_n^{k_n}). \end{aligned}$$

Do đó, $Q \mid a$. Tương tự, ta cũng có $Q \mid b$. Do đó, Q là ước chung của a và b , nghĩa là $Q \leq \gcd(a, b) = P$.

- (2) **Ta chứng minh $P \leq Q$.** Cụ thể, ta sẽ chứng minh $P \mid Q$ và dễ thấy nếu điều này xảy ra thì $P \leq Q$ với $P, Q \in \mathbb{N}$. Chú ý rằng P có thể được viết dưới dạng $P = p_1^{\lambda_1} p_2^{\lambda_2} \dots p_n^{\lambda_n} k$ trong đó λ_i là các số nguyên không âm, $k \in \mathbb{N}$, và không có số nguyên tố p_i nào là ước của k , với $1 \leq i \leq n$. Ta sẽ chứng minh bằng phương pháp phản chứng rằng

(a) $k = 1$. Và do đó ta có $P = p_1^{\lambda_1} p_2^{\lambda_2} \dots p_n^{\lambda_n}$.

(b) $\lambda_i \leq m_i$ với mọi i thỏa mãn $1 \leq i \leq n$. Do đó ta sẽ kết luận $P \mid Q$ (do cùng lý do như $Q \mid a$ ở trên).

Giả sử (a) sai, nghĩa là $k \neq 1$. Do đó $k > 1$ và theo Định lý cơ bản của số học, k có một ước nguyên tố q nào đó. Do không có số nguyên tố p_i ($1 \leq i \leq n$) nào là ước của k , ta có $q \neq p_i$ với mọi i . Mặt khác, do $P = \gcd(a, b)$, $P \mid a$, và do đó $q \mid a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}$. Do đó, tồn tại i , $1 \leq i \leq n$, thỏa mãn $q \mid p_i^{a_i}$, suy ra $q = p_i$. Điều này mâu thuẫn với kết luận $q \neq p_i$ với mọi i ở trên. Do đó, $k = 1$.

Giả sử (b) sai, nghĩa là tồn tại i , $1 \leq i \leq n$, thỏa mãn $\lambda_i > m_i$. Không mất tính tổng quát, giả sử $i = 1$. (Nếu $i \neq 1$ thì đánh số lại các ước nguyên tố). Do $m_1 = \min(a_1, b_1)$, ta có $m_1 = a_1$ hoặc $m_1 = b_1$. Ta xét trường hợp $m_1 = a_1$. Trong trường hợp này $\lambda_1 > a_1$. Do $P \mid a$, tồn tại $s \in \mathbb{N}$ thỏa mãn $sP = a$. Nói cách khác

$$s \cdot p_1^{\lambda_1} p_2^{\lambda_2} \dots p_n^{\lambda_n} = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}.$$

Chia cả hai vế cho $p_1^{a_1}$, ta có

$$s \cdot p_1^{\lambda_1 - a_1} p_2^{\lambda_2} \dots p_n^{\lambda_n} = p_2^{a_2} \dots p_n^{a_n}.$$

Do $\lambda_1 - a_1 > 0$, ta có $p_1 \mid (s \cdot p_1^{\lambda_1 - a_1} p_2^{\lambda_2} \dots p_n^{\lambda_n})$ và do đó $p_1 \mid p_2^{a_2} \dots p_n^{a_n}$, nghĩa là tồn tại j thỏa mãn $2 \leq j \leq n$ và $p_1 \mid p_j^{a_j}$, suy ra $p_1 = p_j$. Đây là một mâu thuẫn. Trường hợp $m_1 = b_1$ hoàn toàn tương tự. Do đó, $\lambda_i \leq m_i$ với mọi i thỏa mãn $1 \leq i \leq n$.

Như đã đề cập ở trên, ta có $P \mid Q$ và do đó $P \leq Q$.

Do $P \leq Q$ và $Q \leq P$, ta kết luận $P = Q$. □