

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This document is not up to date and may contain several errors or outdated information.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: 2023-04-07

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: 2023-04-07



Creative Commons Attribution-ShareAlike 4.0 International

- Trình bày lời giải vào các khoảng trống sau đề bài. Sử dụng mặt sau nếu thiếu khoảng trống.
- Không sử dụng tài liệu. Không trao đổi, bàn bạc khi làm bài.

Họ và Tên: _____

Mã Sinh Viên: _____ Lớp: _____

Câu:	1	Tổng
Điểm tối đa:	10	10
Điểm:		

1. Cho các số nguyên dương m_1, m_2, \dots, m_n thỏa mãn $m_i \geq 2$ và $\gcd(m_i, m_j) = 1$ với mọi $i \neq j$ và $1 \leq i, j \leq n$ với số nguyên $n \geq 2$ nào đó. Bằng cách sử dụng các gợi ý dưới đây, chứng minh rằng

nếu $a \equiv b \pmod{m_i}$ với mọi $1 \leq i \leq n$, thì $a \equiv b \pmod{m}$ với $m = m_1 m_2 \dots m_n$.

- (a) (5 điểm) Chứng minh phát biểu cho $n = 2$.
(b) (2 điểm) Chứng minh rằng $\gcd(m_i, m/m_i) = 1$ với mọi i , $1 \leq i \leq n$.
(c) (3 điểm) Chứng minh phát biểu với mọi $n \geq 2$.

Lời giải:

- (a) Giả sử các số nguyên dương m_1, m_2 thỏa mãn $m_1, m_2 \geq 2$ và $\gcd(m_1, m_2) = 1$. Ta chứng minh nếu $a \equiv b \pmod{m_1}$ và $a \equiv b \pmod{m_2}$ thì $a \equiv b \pmod{m_1 m_2}$. Do $a \equiv b \pmod{m_1}$, tồn tại $k_1 \in \mathbb{Z}$ sao cho $a - b = k_1 m_1$. Do $a \equiv b \pmod{m_2}$, tồn tại $k_2 \in \mathbb{Z}$ sao cho $a - b = k_2 m_2$. Từ Định lý Bézout, tồn tại $s, t \in \mathbb{Z}$ sao cho $\gcd(m_1, m_2) = 1 = sm_1 + tm_2$. Ta có

$$\begin{aligned} a - b &= k_1 m_1 \\ &= k_1 m_1 (sm_1 + tm_2) \\ &= (k_1 m_1)(sm_1) + (k_1 m_1)(tm_2) \\ &= (k_2 m_2)(sm_1) + (k_1 m_1)(tm_2) \\ &= m_1 m_2 (k_2 s + k_1 t). \end{aligned}$$

Do đó, $a \equiv b \pmod{m_1 m_2}$.

- (b) Ta sử dụng phương pháp phản chứng. Giả sử tồn tại $i \in \{1, 2, \dots, n\}$ sao cho $\gcd(m_i, m/m_i) = d > 1$. Gọi $p > 1$ là một ước nguyên tố của d . Theo định nghĩa, $p \mid (m/m_i)$, do đó $p \mid m_1 m_2 \dots m_{i-1} m_{i+1} \dots m_n$. Do đó, tồn tại $j \in \{1, 2, \dots, n\} - \{i\}$ thỏa mãn $p \mid m_j$. Do $p \mid m_i$ và $p \mid m_j$, p là một ước chung của m_i và m_j . Thêm vào đó, $p > 1 = \gcd(m_i, m_j)$. Điều này mâu thuẫn với định nghĩa ước chung lớn nhất. Do đó, với mọi $i \in \{1, 2, \dots, n\}$, $\gcd(m_i, m/m_i) = 1$.

- (c) Giả sử $a \equiv b \pmod{m_i}$ với mọi i thỏa mãn $1 \leq i \leq n$ với số nguyên $n \geq 2$ nào đó, trong đó $m_i \geq 2$ và $\gcd(m_i, m_j) = 1$ với mọi $i \neq j$ và $1 \leq i, j \leq n$. Ta chứng minh phát biểu $P(n)$ sau đúng với mọi $n \geq 2$ bằng phương pháp quy nạp.

$$a \equiv b \pmod{m}, \text{ trong đó } m = m_1 m_2 \dots m_n.$$

- **Bước cơ sở:** $P(2)$ đúng do (a).
- **Bước quy nạp:** Giả sử $P(k)$ đúng với số nguyên $k \geq 2$ nào đó. Ta chứng minh $P(k+1)$ đúng. Thật vậy, từ giả thiết quy nạp, ta có $a \equiv b \pmod{m_1 m_2 \dots m_k}$. Theo giả thiết, ta cũng có $a \equiv b \pmod{m_{k+1}}$. Thêm vào đó, từ phần (b), ta có $\gcd(m_{k+1}, m_1 m_2 \dots m_k) = 1$. Áp dụng phần (a), ta có $a \equiv b \pmod{m_1 m_2 \dots m_k m_{k+1}}$, nghĩa là $P(k+1)$ đúng.