COPYRIGHT NOTICE
THÔNG BÁO BẢN QUYỀN

Nhận xét Bài kiểm tra thường xuyên 2

Toán rời rạc (MAT3500 2, 2022-2023)

Hoàng Anh Đức
BMTH, ĐHKHTN, ĐHQG Hà Nội
hoanganhduc@hus.edu.vn

Ngày 13 tháng 4 năm 2023

- Với câu (a),
  - Một số bạn chứng minh như sau. Từ $a \equiv b \pmod{m_1}$, ta có $a - b$ chia hết cho m_1, nghĩa là tồn tại $k_1 \in \mathbb{Z}$ thỏa mãn $a - b = k_1 m_1$. Tương tự, tồn tại $k_2 \in \mathbb{Z}$ thỏa mãn $a - b = k_2 m_2$. Do đó, $k_1 m_1 = k_2 m_2$, nghĩa là $k_1 m_1$ chia hết cho m_2. Do $\gcd(m_1, m_2) = 1$, k_1 phải chia hết cho m_2. Nghĩa là tồn tại $h \in \mathbb{Z}$ sao cho $k_1 = hm_2$. Do đó, $a - b = k_1 m_1 = hm_1 m_2$. Suy ra $a - b$ chia hết cho $m_1 m_2$ và do đó $a \equiv b \pmod{m_1 m_2}$. Lời giải này là hoàn toàn chính xác.
  - Một số bạn chứng minh như sau. Từ $a \equiv b \pmod{m_1}$ suy ra $m_1 \mid (a - b)$ và do đó tồn tại $k \in \mathbb{Z}$ sao cho $a - b = km_1$. Tương tự, tồn tại $p \in \mathbb{Z}$ sao cho $a - b = m_2 p$. Suy ra $(a - b)m_2 = m_1 k m_2 = (m_1 m_2)k$. Do đó, $m_1 m_2 \mid (a - b)m_2$. Kết hợp với $\gcd(m_1, m_2) = 1$, ta có $m_1 m_2 \mid (a - b)$. Suy ra $a \equiv b \pmod{m_1 m_2}$.

    Ở bước suy luận ra $m_1 m_2 \mid (a-b)$, có thể là các bạn đã áp dụng mệnh đề sau: "Cho các số nguyên dương a, b, c thỏa mãn $\gcd(a, b) = 1$ và $a \mid bc$. Ta có $a \mid c$". Tuy nhiên, để áp dụng mệnh đề này, ta cần $\gcd(m_1 m_2, m_2) = 1$, và điều này không phải luôn đúng. Do đó, chứng minh trên của các bạn không chính xác.
- Với câu (b),
  - Một số bạn lý luận như sau. Giả sử $\gcd(m_i, m/m_i) = d \neq 1$ với $i \in \{1, 2, \dots, n\}$ nào đó. Do đó, $d \mid m_i$ và $d \mid (m/m_i)$. Do đó, ta có thể viết $m_i = dx$ và $m/m_i = dy$ với các số nguyên dương x, y nào đó. Khi đó $m = m_i(m/m_i) = d^2xy$. Do đó $d \mid m$. Do $\gcd(m_i, m_j) = 1$ với mọi $i \neq j$, $1 \leq i, j \leq n$, ta có d phải bằng 1. Một số bạn viết $\gcd(m, m_i) = 1$ thay vì $\gcd(m_i, m_j) = 1$. Trong cả hai trường hợp, tại sao các bạn suy ra được $d = 1$?
  - Một số bạn lý luận như sau. Giả sử $\gcd(m_i, m/m_i) = \alpha > 1$ với $i \in \{1, 2, \dots, n\}$ nào đó. Do đó, tồn tại $k_1, k_2 \in \mathbb{N}$ sao cho $m_i = k_1\alpha$ và $m/m_i = k_2\alpha$. Do đó, $m_1 m_2 \dots m_{i-1} m_{i+1} \dots m_n = k_2\alpha$. Suy ra có ít nhất một số trong $m_1, m_2, \dots, m_{i-1}, m_{i+1}, \dots, m_n$ chia hết cho một ước α_i khác một của α. Không mất tính tổng quát, giả sử m_k chia hết cho α_i. Suy ra $\gcd(m_i, m_k) = \alpha_i > 1$, mâu thuẫn với giả thiết $\gcd(m_i, m_k) = 1$.

    Tại sao các bạn suy ra được có ít nhất một số trong $m_1, m_2, \dots, m_{i-1}, m_{i+1}, \dots, m_n$ chia hết cho một ước α_i khác một của α? Chú ý rằng điều này đúng với một ước nguyên tố nào đó của α, nhưng **không đúng với mọi ước lớn hơn một của** α. Các bạn xem lại các Bài tập 4 và 5 của slides Lý thuyết số cơ bản I.
- Với câu (c),
  -