ĐẠI HỌC KHOA HỌC TỰ NHIÊN HÀ NỘI
KHOA TOÁN-CƠ-TIN
(Đề gồm 1 câu/1 trang)

ĐỀ KIỂM TRA THƯỜNG XUYÊN 2
Môn: Toán rời rạc (MAT3500 3, 2022-2023)
Thời gian: 30 phút

- 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. Chứng minh Định lý cơ bản của số học dựa trên các gợi ý sau:

Định lý 1 (Định lý cơ bản của số học)**.** *Mọi số nguyên dương $n > 1$ có thể được viết một cách duy nhất dưới dạng một số nguyên tố hoặc tích của các ước nguyên tố của nó theo thứ tự tăng dần.*

(a) (5 điểm) Chứng minh bằng quy nạp mạnh: Mọi số nguyên dương $n > 1$ có thể được biểu diễn dưới dạng một số nguyên tố hoặc tích của các ước nguyên tố của n theo thứ tự tăng dần.

(b) (4 điểm) Chứng minh rằng nếu $n \geq 1$ và p là một số nguyên tố thỏa mãn $p \mid a_1 a_2 \dots a_n$, trong đó $a_i \in \mathbb{Z}$ với $1 \leq i \leq n$, thì $p \mid a_j$ với j nào đó thỏa mãn $1 \leq j \leq n$.

(c) (1 điểm) Sử dụng phần (b) để chứng minh rằng nếu một số nguyên $n > 1$ được biểu diễn dưới dạng một số nguyên tố hoặc tích của các ước nguyên tố của n theo thứ tự tăng dần thì biểu diễn đó là duy nhất.

Lời giải:

(a) Ta chứng minh phát biểu $P(n)$ sau đúng với mọi $n \geq 2$ bằng phương pháp quy nạp

n có thể được biểu diễn dưới dạng tích của các ước nguyên tố của n theo thứ tự tăng dần.

- **Bước cơ sở:** $P(2)$ đúng, do $2 = 2$.
- **Bước quy nạp:** Giả sử $P(j)$ đúng với mọi số nguyên j thỏa mãn $2 \leq j \leq k$ với $k \geq 2$ nào đó. Ta chứng minh $P(k+1)$ đúng. Thật vậy, nếu $k+1$ là số nguyên tố thì hiển nhiên $P(k+1)$ đúng. Ngược lại, nếu $k+1$ là hợp số, ta có $k+1 = a \cdot b$ với $2 \leq a, b \leq k$. Theo giả thiết quy nạp, $a = p_1^{a_1} p_2^{a_2} \dots p_h^{a_h}$ với $a_i \geq 0$ và p_i $(1 \leq i \leq h)$ là các số nguyên tố thỏa mãn $p_1 \leq p_2 \leq \dots \leq p_h$ và tương tự $b = q_1^{b_1} q_2^{b_2} \dots q_m^{b_m}$ với $b_i \geq 0$ và q_i $(1 \leq i \leq m)$ là các số nguyên tố thỏa mãn $q_1 \leq q_2 \leq \dots \leq q_m$, trong đó $m, h \geq 1$ là các số nguyên dương nào đó. Do đó, ta có thể viết $k+1 = a \cdot b = (p_1^{a_1} p_2^{a_2} \dots p_h^{a_h}) \cdot (q_1^{b_1} q_2^{b_2} \dots q_m^{b_m})$. Bằng cách sắp xếp lại các thừa số nguyên tố $p_1, \dots, p_h, q_1, \dots, q_m$ theo thứ tự tăng dần, ta có điều phải chứng minh.

(b) Ta chứng minh phát biểu $Q(n)$ sau đúng với mọi $n \geq 1$ bằng phương pháp quy nạp

Nếu p là một số nguyên tố thỏa mãn $p \mid a_1 a_2 \dots a_n$, trong đó $a_i \in \mathbb{Z}$ với $1 \leq i \leq n$, thì tồn tại $j \in \{1, 2, \dots, n\}$ sao cho $p \mid a_j$.

- **Bước cơ sở:** $Q(1)$ đúng, do nếu $p \mid a_1$ thì hiển nhiên $j = 1$ thỏa mãn điều kiện đề ra. Ta chứng minh $Q(2)$ đúng, nghĩa là, nếu p là một số nguyên tố thỏa mãn $p \mid a_1 a_2$, trong đó $a_1, a_2 \in \mathbb{Z}$, thì $p \mid a_1$ hoặc $p \mid a_2$. Thật vậy, giả sử $p \nmid a_1$ và $p \nmid a_2$. Theo Định lý Bézout, tồn tại $s, t \in \mathbb{Z}$ thỏa mãn $\gcd(p, a_1) = 1 = sp + ta_1$. Nhân cả hai vế của đẳng thức trên với a_2 cho ta $a_2 = spa_2 + ta_1 a_2$. Do $p \mid a_1 a_2$, ta cũng có $p \mid (ta_1 a_2)$. Thêm vào đó, $p \mid (spa_2)$. Do đó, $p \mid (spa_2 + ta_1 a_2)$, nghĩa là $p \mid a_2$, mâu thuẫn với giả thiết ban đầu. Tóm lại, ta có $Q(2)$ đúng.
- **Bước quy nạp:** Giả sử $Q(j)$ đúng với mọi j thỏa mãn $1 \leq j \leq k$ với số nguyên $k \geq 2$ nào đó. Ta chứng minh $Q(k+1)$ đúng. Thật vậy, giả sử $p \mid a_1 a_2 \dots a_k a_{k+1}$ với số nguyên tố p nào đó. Nếu $p \mid a_{k+1}$ thì hiển nhiên $Q(k+1)$ đúng. Nếu $p \nmid a_{k+1}$, do $Q(2)$ đúng, ta có $p \mid a_1 a_2 \dots a_k$. Theo giả thiết quy nạp, tồn tại $j \in \{1, 2, \dots, k\} \subseteq \{1, 2, \dots, k, k+1\}$ sao cho $p \mid a_j$. Do đó, $Q(k+1)$ đúng.

(c) Ta sử dụng phương pháp phản chứng. Giả sử với các tập số nguyên tố $A = \{p_1, p_2, \dots, p_h\}$ $(p_1 \leq \dots \leq p_h)$ và $B = \{q_1, \dots, q_m\}$ $(q_1 \leq \dots \leq q_m)$ với $A \neq B$, ta có $(\star)$ $n = p_1^{a_1} \dots p_h^{a_h} = q_1^{b_1} \dots q_m^{b_m}$. Nếu $A \cap B = \emptyset$ thì không làm gì. Ngược lại, ta chia cả hai vế của $(\star)$ cho tích các số nguyên tố trong $A \cap B$. Giả sử kết quả thu được là

$$r_1^{c_1} \dots r_u^{c_u} = s_1^{d_1} \dots s_v^{d_v}$$

trong đó $\{r_1, \dots, r_u\} = A - B$ và $\{s_1, \dots s_v\} = B - A$. Do $r_1 \mid (r_1^{c_1} \dots r_u^{c_u})$, ta cũng có $r_1 \mid (s_1^{d_1} \dots s_v^{d_v})$. Theo phần (b), tồn tại $j \in \{1, 2, \dots, v\}$ thỏa mãn $r_1 \mid s_j^{d_j}$. Do cả r_1 và s_j đều là số nguyên tố, ta có $r_1 = s_j$. Điều này mâu thuẫn với giả thiết $r_1 \in A - B$ và $s_j \in B - A$. Do đó, ta có điều phải chứng minh.