# NHẬP MÔN MÃ HÓA MẬT MÃ

## TUẦN 3: NHÓM VÀ MỘT SỐ TÍNH CHẤT

Ngày 22 tháng 10 năm 2024

**Bài 1.** Cho tập số nguyên $\mathbb{Z}$ với phép toán $(*)$ được định nghĩa như sau:

- $m * n = m + n$ nếu $m$ chẵn,
- $m * n = m - n$ nếu $m$ lẻ.

Chứng minh rằng $(\mathbb{Z}, *)$ là một nhóm.

**Bài 2.** Ta định nghĩa tập $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ là tập các thặng dư không âm nhỏ nhất modulo $n$. Xét phép toán: với mọi $x, y \in \mathbb{Z}_n, x * y = (x + y) \pmod{n}$. Chứng minh rằng $(\mathbb{Z}_n, *)$ là một nhóm.

**Bài 3.** Gọi $\mathbb{Z}_n^* = \{x | \gcd(x, n) = 1\}$ là tập các thặng dư không âm nguyên tố cùng nhau với $n$. Ta định nghĩa phép toán $\circ$ trên $\mathbb{Z}_n^*$ như sau: với mọi $x, y \in \mathbb{Z}_n, x \circ y = xy \pmod{n}$ ($x$ nhân $y$ theo nghĩa phép nhân thông thường trên tập số nguyên).

a) Chứng minh rằng $(\mathbb{Z}_n, \circ)$ là một nhóm.

b) Chỉ ra cấp của nhóm $(\mathbb{Z}_n, \circ)$ là $\phi(n)$-là phi hàm Euler.

c) Dựa vào câu $b$, chỉ ra rằng với mọi số nguyên tố $p$ thì tập $\mathbb{Z}_p^*$ cùng với phép toán $\circ$ luôn luôn là một nhóm có $p - 1$ phần tử.

**Bài 4.** Chứng minh rằng $(\mathbb{Z}_6^*, \circ)$ và $(\mathbb{Z}_{17}^*, \circ)$ là các nhóm cyclic. Tìm các phần tử sinh của chúng.

**Bài 5.** Giả sử $X$ là một nhóm cyclic cấp $n$ sinh bởi phần tử $a$. Xét phần tử $b = a^k \in X$. Chứng minh rằng:

a) Cấp của $b$ là $\dfrac{n}{d}$ với $d$ là ước chung lớn nhất của $n$ và $k$.

b) $b$ là phần tử sinh của $X$ khi và chỉ khi $(n, k) = 1$.

**Bài 6.** Giả sử $a, b$ là hai phần tử của một nhóm có cấp là $r$ và $s$, $(r, s) = 1$ và $ab = ba$. Chứng minh rằng cấp của phần tử $ab$ là $rs$.

**Bài 7.** Cho $G$ là một nhóm cấp $n$ và $(n, m) = 1$. Chứng minh rằng mọi phần tử $h$ của $G$ có một căn bậc $m$, nghĩa là $h = g^m$ với một $g$ nào đó của $G$.

**Bài 8.** (**Khuyến khích sinh viên làm lấy điểm cộng**) Dựa vào định lý Lagrange và khái niệm cấp của một phần tử trong nhóm hữu hạn, hãy chứng minh định lý Fermat nhỏ và định lý Euler bằng ngôn ngữ của lý thuyết nhóm.