BÀI TẬP TUẦN 3

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.

Xét: $(m * n) * z$ $(\forall m, n, z \in \mathbb{Z})$

Trường hợp 1: $(m * n)$ chẵn
ta có: $(m * n) * z = (m + n) * z$

- Nếu $(m + n)$ chẵn thì: $(m + n) * z = m + n + z$
- Nếu $(m + n)$ lẻ thì: $(m + n) * z = m + n - z$

Trường hợp 2: $(m * n)$ lẻ
ta có: $(m * n) * z = (m - n) * z$

- Nếu $(m - n)$ chẵn thì: $(m - n) * z = m - n + z$ $(\forall m, n, z \in \mathbb{Z})$
- Nếu $(m - n)$ lẻ thì: $(m - n) * z = m - n - z$ $(\forall m, n, z \in \mathbb{Z})$

Xét: $m * (n * z)$ $(\forall m, n, z \in \mathbb{Z})$

Trường hợp 1: m chẵn
ta có: $m * (n * z) = m + (n * z)$

- Nếu n chẵn $\Rightarrow (m + n)$ chẵn
  do đó: $m + (n * z) = m + n + z$ $(\forall m, n, z \in \mathbb{Z})$
- Nếu n lẻ $\Rightarrow (m + n)$ lẻ
  do đó: $m + (n * z) = m + n - z$ $(\forall m, n, z \in \mathbb{Z})$

Trường hợp 2: m lẻ
ta có: $m * (n * z) = m - (n * z)$

- Nếu n lẻ $\Rightarrow (m - n)$ chẵn
  do đó: $m - (n * z) = m - n + z$ $(\forall m, n, z \in \mathbb{Z})$
- Nếu n chẵn $\Rightarrow (m - n)$ lẻ
  do đó: $m - (n * z) = m - n - z$ $(\forall m, n, z \in \mathbb{Z})$

Vậy suy ra được $(m * n) * z = m * (n * z)$ $(\forall m, n, z \in \mathbb{Z})$ thỏa mãn tính chất kết hợp.

Ta có: $e = 0$ thỏa mãn:

- nếu m chẵn: $m * e = m + 0 = m$
- nếu m lẻ: $m * e = m - 0 = m$

Vậy $e = 0$ là phần tử đơn vị của $(\mathbb{Z}, *)$

Ta có: $\forall m \in \mathbb{Z}$ luôn tồn tài m' thỏa:

- nếu m chẵn: $m + m' = e = 0 \Rightarrow m' = -m$
- nếu m lẻ: $m - m' = e = 0 \Rightarrow m' = m$

Vậy $(\mathbb{Z}, *)$ là 1 nhóm.

Bài 2. Ta định nghĩa tập $\mathbb{Z}_n = \{0, 1, 2, ..., n-1\}$ 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.

Ta có:

- $(x * y) * z = ((x + y) \pmod{n} + z) \pmod{n}$
- $x * (y * z) = (x + (y + z) \pmod{n}) \pmod{n}$

Vậy suy ra được $(x * y) * z = x * (y * z)$ $(\forall x, y, z \in \mathbb{Z})$ thỏa mãn tính chất kết hợp.

Ta có: $e = 0 \in \mathbb{Z}_n$ là phần tử đơn vị thỏa mãn:

- $x * 0 = (x + 0) \pmod{n} = x$
- $0 * x = (0 + x) \pmod{n} = x$

Ta có: $\forall x \in \mathbb{Z}$ luôn tồn tài $x' = n - x$ vì:

$$x * x' = (x + n - x) \equiv 0 \pmod{n}$$

Vậy $(\mathbb{Z}, *)$ là 1 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.

a) Ta có:

$$(x \circ y) \circ z = ((xy \pmod{n}) \circ z) \pmod{n} = (x(yz)) \pmod{n} = x \circ (y \circ z)$$

Vậy suy ra được $(x \circ y) \circ z = x \circ (y \circ z)$ $(\forall x, y, z \in \mathbb{Z^*}_n)$ thỏa mãn tính chất kết hợp.

Ta có: $e = 1 \in \mathbb{Z}_n$ là phần tử đơn vị thỏa mãn:

- $x \circ 1 = (x.1) \pmod{n} = x$
- $0 \circ x = (1.x) \pmod{n} = x$

Ta có: $\forall x \in \mathbb{Z^*}_n$ luôn tồn tài $x \circ x' = 1$ vì $gcd(x, n) = 1$ theo định lý euclid mở rộng luôn tồn tại $x^{-1} \in \mathbb{Z^*}_n$

$$x.x^{-1} \equiv 1 \pmod{n}$$

Vậy $(\mathbb{Z^*}_n, \circ)$ là 1 nhóm.

b) Tập $\mathbb{Z^*}_n$ bao gồm các số nguyên $\{1, 2, 3, .., n-1\}$ sao cho $gcd(x, n) = 1$.
Theo định nghĩa của phi hàm euler: $\phi(n)$ chính là số lượng phần của tập $\mathbb{Z^*}_n$
Do đó cấp của $(\mathbb{Z^*}_n, \circ)$ là $\phi(n)$

c) vì p không chia hết cho bất kì số nào trong tập $\mathbb{Z}_p$
Do đó: $\mathbb{Z^*}_p = \mathbb{Z}_p = \{1, 2, 3, .., p-1\}$
Suy ra: $(\mathbb{Z^*}_n, \circ) = \phi(p) = p - 1$

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.

Ta có:

- $\mathbb{Z}^*{}_6 = \{1, 5\}$
- $\mathbb{Z}^*{}_{17} = \{1, 2, 3, ..16\}$

+) Bậc của $(\mathbb{Z}^*{}_6, \circ)$ có 2 phần tử nên $(\mathbb{Z}^*{}_6, \circ)$ là nhóm cyclic và được sinh bởi $g = 5$.
+) với $g = 3$ sinh ra được tập $\mathbb{Z}^*{}_{17}$ nên $(\mathbb{Z}^*{}_{17}, \circ)$ là 1 nhóm cyclic.

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 $\frac{n}{d}$ với d là ước chung lớn nhất của n và k.
b) b là phần tử sinh của X khi và chỉ khi $(n, k) = 1$.

a) vì $b = a^k \Leftrightarrow b^m = a^{km}$
Ta cần tìm m sao $b^m = a^{km} = e$ mà a là phần tử sinh của nhóm X cấp n.
nên suy ra được:

$$km \equiv 0 \pmod{n}$$

nhận thấy được km là bội của n hay $m = \frac{n}{d}$
Vậy cấp của b là $\frac{n}{d}$ với d là ước chung lớn nhất của n và k.

b) ta có $b = a^k$ là phần tử sinh khi $gcd(n, k) = 1$ và cấp của b là $\frac{n}{d} = \frac{n}{1} = n$.
vì cấp của b là n hay $b^n = (a^{kn}) = e$ và không có phần tử nào có cấp lớn hơn n trong nhóm X cấp n nên b là phần tử sinh của nhóm X.

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.

ta có: $(ab)^{rs} = a^{rs}b^{rs}$
do $a^r = e, b^s = e$ nên

$$(ab)^{rs} = e$$

Giả sử $k < rs$ sao cho $(ab)^k = e$
mà $a^r = e$ và $b^s = e$ ta thấy rằng k phải chia hết cho cả r và s.
vì $gcd(r, s) = 1$ do đó

$$k = rs$$

điều này mâu thuẫn với $k < rs$
Vậy 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.

với $h \in G$ là phần tử bất kì, ta có:

$$g = h^x (g \in G)$$
$$\Leftrightarrow g^m = (h^x)^m = h^{mx}$$

do $gcd(n, m) = 1$ hay $mx + ny = 1$ nên

$$g^m = h^{mx} = h^{1-ny} = h^1 h^{-ny}$$

vì nhóm G có cấp n nên

$$h^n = e \Rightarrow h^{-ny} = (h^n)^{-y} = e^{-y} = e \Rightarrow g^m = h^1.e = h$$

Vậy với mọi phần tử $h \in G$ ta có thể tìm được $g \in G$ sao cho $g^m = h$.

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.

+) Chứng minh định lý Euler:

Ta có: cấp của nhóm ${\mathbb{Z}^*}_n = \phi(n)$
Theo định lý lagrange, với mọi phần tử $a \in {\mathbb{Z}^*}_n$ cấp của a phải chia hết cho cấp của nhóm tức là:

$$a^{\phi(n)} = e$$

trong đó $e = 1$ là phần tử đơn vị. do đó:

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

+) Chứng minh định lý Fermat:

với p là số nguyên tố và phép nhân modulo p trên ${\mathbb{Z}^*}_n$ tạo thành một nhóm cyclic với cấp của ${\mathbb{Z}^*}_n = p - 1$

vì $gcd(a, p) = 1$ $(a \neq 0 \pmod{p})$ $a \in {\mathbb{Z}^*}_p$
Theo định lý euler đã chứng minh ở trên ta có được:

$$a^{\phi(p)} \equiv 1 \pmod{p}$$

với p là số nguyên tố, $\phi(p) = p - 1$ do đó:

$$a^{p-1} \equiv 1 \pmod{p}$$