NHẬP MÔN MÃ HÓA MẬT MÃ

TUẦN 4: VÀNH, MIỀN NGUYÊN, TRƯỜNG VÀ MỘT SỐ TÍNH CHẤT

Ngày 29 tháng 10 năm 2024

Bài 1. Cho tập $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ là tập các thặng dư không âm nhỏ nhất theo modulo n.Với mọi $x, y \in \mathbb{Z}_n$, định nghĩa hai phép toán:

- $x * y = (x + y) \pmod n$,
- $x \circ y = xy \pmod n$ (x nhân y theo nghĩa phép nhân thông thường trên tập số nguyên).

Hãy chứng minh rằng $(\mathbb{Z}_n, *, \circ)$ là một vành.

Bài 2. Chỉ ra rằng x là phần tử khả nghịch (có phần tử nghịch đảo) trên vành $(\mathbb{Z}_n, *, \circ)$ khi và chỉ khi x nguyên tố cùng nhau với n.

Bài 3. Gọi $\mathbb{Z}[x] = \{a_0 + a_x + a_2x + \ldots + a_nx^n : n \geq 0$ và $a_0, a_1, \ldots, a_n \in \mathbb{Z}\}$ là tập các đa thức với hệ số là số nguyên. Chứng minh rằng $\mathbb{Z}[x]$ với phép cộng và phép nhân hai đa thức thông thường là một vành giao hoán có đơn vị.

Bài 4. Hãy chỉ ra rằng phương trình $x^2 + 14 = 0$ có bốn nghiệm trên vành $\mathbb{Z}_{15}$.

Bài 5. Hãy chứng tỏ rằng $(\mathbb{Z}_{17}, *, \circ)$ là một miền nguyên nhưng $(\mathbb{Z}_{16}, *, \circ)$ thì không phải là một miền nguyên.

Bài 6. Cho p, q là các số nguyên tố. Hãy chứng minh rằng $(\mathbb{Z}_p, *, \circ)$ là một miền nguyên nhưng $(\mathbb{Z}_{pq}, *, \circ)$ thì không phải là một miền nguyên.

Bài 7. Chứng minh rằng $(\mathbb{Z}_n, *, \circ)$ với các phép toán được định nghĩa như ở Bài 1 là một trường khi và chỉ khi n là số nguyên tố.