Nguyễn Hồ Đăng Duy - 22127085 - 22MMT

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.

+) $(\mathbb{Z}_n, *)$ là nhóm Abel

- Tính kết hợp: $\forall a, b, c \in \mathbb{Z}_n$ ta có:

$(a * b) * c = ((a + b) \pmod n) + c) \pmod n$

$= (a + b + c) \mod n$

$= (a \mod n) + ((b+c) \mod n) = a \circ (b \circ c)$

- Tính đóng: $\forall a, b \in \mathbb{Z}_n$, khi đó $0 \le a, b \le n-1$ từ đó

$0 \le a + b \le 2(n-1) < 2n$

nên $(x * y) = (x + y) \mod n$ sẽ luôn nằm trong $\mathbb{Z}_n$

- Phần tử đơn vị

Ta có, $\forall x \in \mathbb{Z}_n$ thì $x * 0 = (x + 0) \mod n = x \mod n = x$

$0 * x = (0 + x) \mod n = x \mod n = x$

Suy ra $(\mathbb{Z}_n, *)$ có phần tử đơn vị $e = 0$

- Phần tử nghịch đảo

$\forall x \in \mathbb{Z}_n$, luôn tồn tại phần tử $(n - x) \in \mathbb{Z}_n$ sao cho

$x * (n-x) = (x + (n-x)) \mod n = n \mod n = 0 = e$

$(n-x) * x = ((n-x) + x) \mod n = n \mod n = 0 = e$

Suy ra, $\forall x \in \mathbb{Z}_n$, phần tử nghịch đảo của x là $(n - x)$

+) $(\mathbb{Z}_n, \circ)$ là nhóm giao hoán

- Tính kết hợp: $\forall a, b, c \in \mathbb{Z}_n$ ta có

$(a \circ b) \circ c = (ab \mod n) c \pmod n = abc \mod n = a \circ (b \circ c)$

- Phần tử đơn vị: $\forall x \in \mathbb{Z}_n$ thì $x \circ 1 = x.1 \pmod n = x$

$1 \circ x = 1.x \pmod n = x$

- Tính giao hoán: $\forall a, b \in \mathbb{Z}_n$ thì:

$a \circ b = ab \pmod n = ba \pmod n = b \circ a$

- Phần tử nghịch đảo: $\forall a \in \mathbb{Z}_n : a \neq 0$, không tồn tại phần tử nghịch đảo $\frac{1}{\overline{a}} \in \mathbb{Z}_n$

+) Tính phân phối

$\forall a, b, c \in \mathbb{Z}_n$

$(a * b) \circ c = \big((a * b) \bmod n\big).c \pmod n = a.c * bc \pmod n$

$c \circ (a * b) = c.\big((a * b) \bmod n\big) \pmod n = c.a * c.b \pmod n$

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

* Chiều thuận

Giả sử x là phần tử khả nghịch trên vành $(\mathbb{Z}_n, *, \circ)$. Nghĩa là $\exists y \in \mathbb{Z}_n$ sao cho $x \circ y \equiv 1 \pmod n$.

Ta có: $x \circ y \equiv 1 \pmod n \Leftrightarrow xy \equiv 1 \pmod n$

$\Rightarrow \exists k \in \mathbb{Z} : xy - 1 = kn$ hay $xy - kn = 1$

Vì 1 là ước chung của xy và kn mà $\gcd(xy, kn) = \gcd(x, n)$

$\Rightarrow \gcd(x, n) = 1$ hay x và n nguyên tố cùng nhau

* Chiều nghịch

Giả sử x và n nguyên tố cùng nhau. Theo định lý Euler, vì x và n nguyên tố cùng nhau nên $x^{\varphi(n)} \equiv 1 \pmod n$

Đặt $y = x^{\varphi(n)-1}$. Khi đó: $x \cdot y = xy = x^{\varphi(n)} \equiv 1 \pmod n$

Vậy y là phần tử nghịch đảo của x trên $(\mathbb{Z}_n, *, \circ)$

Vậy ta có đpcm

Bài 3. Gọi $\mathbb{Z}[x] = \{a_0 + a_x + a_2x + \ldots + a_nx^n : n \geq 0 \text{ và } a_0, a_1, \ldots, a_n \in \mathbb{Z}\}$ 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.

1) Tính đóng

a) Phép cộng

Cho 2 đa thức $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$

và $g(x) = b_m x^m + b_{m-1}x^{m-1} + \ldots + b_1 x + b_0 \in \mathbb{Z}[x]$

Khi đó: $f(x) + g(x) = (a_n + b_n)x^n + (a_{n-1} + b_{n-1})x^{n-1} + \ldots + (a_1 + b_n)x + (a_0 + b_0)$

Vì các hệ số của đa thức mới là số nguyên $\Rightarrow f(x) + g(x) \in \mathbb{Z}[x]$

b) Phép nhân

Ta có: $f(x).g(x) = \sum_{i=0}^{n+m} a_i\, b_{n+m-i}\, x^i$

Vì các hệ số là tích của 2 số nguyên nên $f(x).g(x) \in \mathbb{Z}[x]$

2) Tính kết hợp

Vì các hệ số của đa thức là số nguyên nên tính kết hợp cũng được áp dụng lên cả phép cộng và phép nhân đa thức

3) Tính giao hoán

Tương tự như tính kết hợp. Phép nhân và phép cộng đa thức cũng có tính giao hoán

4. Phần tử đơn vị

Xét đa thức hằng $h(x) = 1$. Ta có:

$$f(x).h(x) = (a_n x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0).1$$
$$= a_n x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0 = f(x)$$

5. Phần tử đối

Cho đa thức $f(x)$ như trên, phần tử đối của $f(x)$ là $-f(x)$ vì:

$$f(x) + (-f(x))$$
$$= a_n x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0 + \left[(-a_n)x^n + (-a_{n-1})x^{n-1} + \dots + (-a_1)x + (-a_0)\right]$$
$$= 0$$

6. Tính phân phối

Vì các hệ số đều nguyên nên tính phân phối và phép cộng và phép nhân cũng được mở rộng ra cho đa thức

$\Rightarrow$ Từ các chứng minh trên, $\mathbb{Z}[x]$ 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 $\mathbb{Z}_{15}$.

Xét phương trình $x^2 + 14 = 0$ trên $\mathbb{Z}_{15}$, ta có:

$$x^2 + 14 = 0 \Leftrightarrow x^2 - 15x + 14 = 0$$
$$\Leftrightarrow (x-1)(x-14) = 0$$
$$\Leftrightarrow \left[\begin{array}{l} x = 1 \\ x = 14 \end{array}\right. \quad (\text{trên } \mathbb{Z}_{15})$$

Mặt khác: $x^2 + 14 = 0 \Leftrightarrow x^2 - 15x + 14 + 15.2 = 0$

$\Leftrightarrow \quad x^2 - 15x + 44 = 0$

$\Leftrightarrow \quad (x-4)(x-11) = 0$

$\Leftrightarrow \begin{cases} x = 4 \\ x = 11 \end{cases}$ (trên $\mathbb{Z}_{15}$)

Vậy phương trình $x^2 + 14 = 0$ có 4 nghiệm trên $\mathbb{Z}_{15}$

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.

Dựa trên kết quả bài 1 $\Rightarrow$ $(\mathbb{Z}_{17}, *, \circ)$ và $(\mathbb{Z}_{16}, *, \circ)$ là một vành nguyên

a) Để chứng minh $\mathbb{Z}_{17}$ là một miền nguyên, ta chứng minh nếu $a, b \in \mathbb{Z}_{17}$ và $ab \equiv 0 \pmod{17}$ thì $a \equiv 0 \pmod{17}$ hoặc $b \equiv 0 \pmod{17}$

Thật vậy, vì 17 là số nguyên tố nên nếu ab chia hết cho 17 thì a chia hết cho 17 hoặc b chia hết cho 17. Hay $a \equiv 0 \pmod{17}$ hoặc $b \equiv 0 \pmod{17}$

Vậy $(\mathbb{Z}_{17}, *, \circ)$ là một miền nguyên

b) Ta dễ thấy, nếu chọn $a = 2$ và $b = 8$ thì $ab = 2.8 = 16 \equiv 0 \pmod{16}$

Vì $a \not\equiv 0 \pmod{16}$ và $b \not\equiv 0 \pmod{16}$ nhưng $ab \equiv 0 \pmod{16}$ nên

$(\mathbb{Z}_{16}, *, \circ)$ không là 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.

Dựa trên kết quả bài 1 $\Rightarrow$ $(\mathbb{Z}_p, *, \circ)$ và $(\mathbb{Z}_{pq}, *, \circ)$ là một vành nguyên

*) Vành $\mathbb{Z}_p$

Giả sử $a, b \in \mathbb{Z}_p$ và $ab \equiv 0 \pmod p$

Vì p là số nguyên tố nên p phải chia hết cho ít nhất một trong 2 số a hoặc b

Do đó, $a \equiv 0 \pmod p$ hoặc $b \equiv 0 \pmod p$

Vậy $\mathbb{Z}_p$ là một miền nguyên

*) Vành $\mathbb{Z}_{pq}$

Ta chọn $a = p$, $b = q$. Rõ ràng cả p và q đều khác 0 trong $\mathbb{Z}_{pq}$.

Tuy nhiên, $ab = pq \equiv 0 \pmod{pq}$

Điều này chứng tỏ tồn tại 2 phần tử khác 0 trong $\mathbb{Z}_{pq}$ mà tích bằng 0

Vậy $\mathbb{Z}_{pq}$ không là 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.

*) $(\mathbb{Z}_n, *)$ là nhóm Abel

- Tính kết hợp: $\forall a, b, c \in \mathbb{Z}_n$ ta có:

$$(a * b) * c = ((a + b) \pmod n) + c \pmod n$$
$$= (a + b + c) \bmod n$$
$$= (a \bmod n) + ((b + c) \bmod n) = a \circ (b \circ c)$$

- Tính đóng: $\forall a, b \in \mathbb{Z}_n$, khi đó $0 \le a, b \le n - 1$ từ đó

$$0 \le a + b \le 2(n - 1) < 2n$$

nên $(x * y) = (x + y) \bmod n$ sẽ luôn nằm trong $\mathbb{Z}_n$

- Phần tử đơn vị

Ta có, $\forall x \in \mathbb{Z}_n$ thì $x * 0 = (x + 0) \bmod n = x \bmod n = x$

$0 * x = (0 + x) \bmod n = x \bmod n = x$

Suy ra $(\mathbb{Z}_n, *)$ có phần tử đơn vị $e = 0$

- Phần tử nghịch đảo

$\forall x \in \mathbb{Z}_n$, luôn tồn tại phần tử $(n - x) \in \mathbb{Z}_n$ sao cho

$x * (n - x) = (x + (n - x)) \bmod n = n \bmod n = 0 = e$

$(n - x) * x = ((n - x) + x) \bmod n = n \bmod n = 0 = e$

Suy ra, $\forall x \in \mathbb{Z}_n$, phần tử nghịch đảo của x là $(n - x)$

+) $(\mathbb{Z}_n, \cdot)$ là nhóm giao hoán

- Tính kết hợp: $\forall a, b, c \in \mathbb{Z}_n$ ta có

$(a \cdot b) \cdot c = (ab \bmod n) \cdot c \pmod n = abc \bmod n = a \cdot (b \cdot c)$

- Phần tử đơn vị: $\forall x \in \mathbb{Z}_n$ thì $x \cdot 1 = x \cdot 1 \pmod n = x$

$1 \cdot x = 1 \cdot x \pmod n = x$

- Tính giao hoán: $\forall a, b \in \mathbb{Z}_n$ thì:

$a \cdot b = ab \pmod n = ba \pmod n = b \cdot a$

- Phần tử nghịch đảo: $\forall a \in \mathbb{Z}_n : a \neq 0$, không tồn tại phần tử nghịch đảo $\frac{\overline{1}}{\overline{a}} \in \mathbb{Z}_n$

+) Tính phân phối

$\forall a, b, c \in \mathbb{Z}_n$

$(a + b) \cdot c = ((a + b) \bmod n) \cdot c \pmod n = a \cdot c + bc \pmod n$

$c \cdot (a + b) = c \cdot ((a + b) \bmod n) \pmod n = c \cdot a + c \cdot b \pmod n$

⇒ Vậy $(\mathbb{Z}_n, *, \cdot)$ là 1 vành

* Khi n là số nguyên tố

+) Giả sử $a, b \in \mathbb{Z}_n$ và $ab \equiv 0 \pmod n$

Vì n là số nguyên tố nên n phải chia hết cho ít nhất một trong 2 số a hoặc b

Do đó, $a \equiv 0 \pmod n$ hoặc $b \equiv 0 \pmod n$

+) $\forall a \in \mathbb{Z}_n, a \neq 0$. Vì n là số nguyên tố nên a và n nguyên tố cùng nhau

Theo định lý Euler ta có: $a^{\varphi(n)} \equiv 1 \pmod n$ trong đó $\varphi(n)$ là phi hàm Euler

Do đó, $a^{\varphi(n)-1}$ là nghịch đảo của a trong $\mathbb{Z}_n$

Suy ra, $\mathbb{Z}_n$ là một trường

* Khi n không là số nguyên tố

Nếu n không là số nguyên tố, ta dễ chọn được $a, b \neq 0 \pmod n$ sao cho $ab = n$

Khi đó, $ab \equiv 0 \pmod n$

Suy ra, tồn tại các ước của 0 trong $\mathbb{Z}_n$ nếu n không là số nguyên tố hay $\mathbb{Z}_n$ không là một miền khi n không là số nguyên tố

Vậy $\mathbb{Z}_n$ là một trường khi và chỉ khi n là số nguyên tố