BÀI TẬP ÔN CUỐI KỲ 2020

Bài 1. Xét vành đa thức $\mathbb{Z}_{16}[x]$ và $f(x) = 8x + 3$.

a) Tính $g(x) = [f(x)]^2$.

b) Tập hợp $\{h(x) \mid h(x) = 8x + \alpha \in \mathbb{Z}_{16}[x], \alpha \in U(\mathbb{Z}_{16})\}$ có tạo thành nhóm với phép nhân không? Vì sao?

c) Có đa thức bất khả quy nào trong $\mathbb{Z}_{16}$ không? Vì sao?

d) Liệt kê phần tử của $U(\mathbb{Z}_{16})$.

e) Tìm cấp của mỗi phần tử trong $(\mathbb{Z}_{16}, +)$.

Lời giải. a) Ta có $g(x) = (8x+3)^2 = 64x^2 + 48x + 9 = 9$.

b) Đặt G là tập hợp đã cho. Kiểm tra các tính chất của nhóm:

- Tính đóng với phép nhân: $a, b \in G$ thì $a \cdot b \in G$. Đúng vì

$$(8x+\alpha_1)(8x+\alpha_2) = 64x^2 + 8(\alpha_1+\alpha_2)x + \alpha_1\alpha_2 = 8(\alpha_1+\alpha_2)x + \alpha_1\alpha_2.$$

Để ý rằng nếu $\alpha_1, \alpha_2 \in U(\mathbb{Z}_{16})$ thì chúng cùng lẻ. Vì thế $\alpha_1 + \alpha_2$ chẵn, nên $8(\alpha_1+\alpha_2) = 0$. Do đó tích của hai đa thức trong G sẽ ra $\alpha_1\alpha_2$, không có dạng như trên. Vì thế nó không thỏa mãn tính đóng với phép nhân và không là nhóm.

Ghi chú. Tham khảo thêm lý thuyết nhóm, vành, trường và các tiêu chuẩn tại đây:

https://vietcodes.github.io/algo/group-theory

c) Chọn tùy ý một đa thức bậc nhất nào cũng sẽ có đa thức bất khả quy. Ví dụ $x+1$. Vì theo định nghĩa, muốn đa thức này khả quy thì cần có $x + 1 = f(x)g(x)$ với $\deg f, g > 1$, vô lý.

d) $U(\mathbb{Z}_{16}) = \{1, 3, 5, 7, 9, 11, 13, 15\}$.

e) Cấp của a trong $\mathbb{Z}_{16}$ là số k nhỏ nhất để $a^k \equiv 1 \bmod 16$. Ta có bảng sau (được tính đơn giản bằng cách thử dần dần các số k từ nhỏ đến lớn xem số nào thỏa):

$$\begin{array}{c|cccccccc} a = & 1 & 3 & 5 & 7 & 9 & 11 & 13 & 15 \\ \hline k = & 1 & 4 & 4 & 2 & 2 & 4 & 4 & 2 \end{array}.$$

Bài 2. a) Có tổng cộng bao nhiêu ánh xạ từ $\mathbb{Z}_7 \to \mathbb{Z}_7$?

b) Trong các ánh xạ trên, có bao nhiêu song ánh?

c) Có bao nhiêu đa thức bậc 7 trong $\mathbb{Z}_7[x]$?

d) Cho ví dụ hai đa thức khác nhau trong $\mathbb{Z}_7[x]$ mà $f(a) = g(a)$ với mọi $a \in \mathbb{Z}_7[x]$.

Lời giải. a) Số phần tử của $\mathbb{Z}_7$ là 7. Ánh xạ f có tập nguồn và tập đích đều có 7 phần tử nên số lượng ánh xạ là 7^7 (tổng quát $f: A \to B$ với $|A| = m, |B| = n$ thì $|f| = n^m$).

b) Song ánh chính là hoán vị, số lượng là $7!$.

c) Đa thức bậc 7 có dạng $a_7x^7 + a_6x^6 + \dots + a_1x + a_0$ và $a_0 \to a_6$ có 7 cách chọn, trong khi $a_7 \neq 0$ nên chỉ có 6 cách. Vì thế số đa thức thỏa mãn là $6 \cdot 7^7$.

d) Ví dụ: $f(x) = x^7 - x = x(x^6 - 1)$ và $g(x) = x^8 - x^2 = x^2(x^6 - 1)$.

Rõ ràng $f(0) = g(0) = 0$ và vì 7 là số nguyên tố nên theo định lý Fermat nhỏ thì mọi $a \in U(\mathbb{Z}_7) = \{1, 2, \dots, 6\}$ thì $a^6 - 1 \equiv 0 \bmod 7$, vì thế nên $f(a) = g(a) = 0, \forall a \in U(\mathbb{Z}_7)$.

Do đó $f(a) = g(a) = 0, \forall a \in \mathbb{Z}_7$, thỏa mãn đề bài.

Bài 3. Xét vành đa thức $\mathbb{Z}_3[x]$ và $f(x) = 2x^3 + x + 1$.

a) Chứng minh rằng $f(x)$ vô nghiệm và bất khả quy.

b) Gọi $(F, +, \cdot)$ là trường sinh bởi $f(x)$. Hỏi F có mấy phần tử, liệt kê các phần tử của F như hệ đếm cơ số 3.

c) Trong $(F, +, \cdot)$ tính $122 + 201$ và $122 \cdot 201$.

d) Tìm phần tử nghịch đảo nhân của 122 trong F.

e) Tìm tất cả cặp số (D, E) với $1 < E < D < 26$ sao cho $(x^E)^D = x$ với mọi $x \in F$. Suy ra những khả năng có thể mã hóa/giải mã với những cặp khóa thích hợp.

Lời giải.

a) Nghiệm của $f(x)$, nếu có, chỉ có thể là $x = 0, 1, 2$. Kiểm tra trực tiếp thấy

$$f(0) = 1,\ f(1) = 2 + 1 + 1 = 1,\ f(2) = 16 + 2 + 1 = 1$$

đều khác 0 nên $f(x)$ vô nghiệm. Giả sử $f(x)$ khả quy thì có phân tích $f(x) = g(x)h(x)$ với $\deg g \geq 1, \deg h \geq 1$. Vì thế, một trong hai đa thức g, h là bậc nhất, và nó có nghiệm. Nghiệm đó cũng là nghiệm của f, mâu thuẫn. Vì thế $f(x)$ bất khả quy.

Ghi chú: đa thức bậc 3 vô nghiệm thì sẽ bất khả quy; điều này không đúng với đa thức bậc 4 hoặc cao hơn.

b) Để liệt kê các phần tử của trường sinh bởi $f(x) = 2x^3 + x + 1$, ta xét phép chia của một đa thức bất kỳ trong $\mathbb{Z}_3[x]$ cho $f(x)$. Đa thức dư chính là các phần tử của trường cần tìm, và đó là mọi đa thức bậc không vượt quá 2 có dạng:

$$F = \{ax^2 + bx + c \mid a, b, c \in \mathbb{Z}_3[x]\}.$$

Rõ ràng $|F| = 3^3 = 27$ và các phần tử của nó nếu viết trong hệ tam phân có dạng:

$$000, 001, 002, 010, 011, 012, 020, \ldots, 222.$$

c) Trong $(F, +, \cdot)$ tính $122 + 201$ và $122 \cdot 201$.

Ta có $122 + 201 = (x^2 + 2x + 2) + (2x^2 + 1) = 3x^2 + 2x + 3 = 2x = \overline{020}$.

Để thực hiện phép nhân, chú ý rằng $2x^3 \equiv -x - 1 = 2x + 2 \pmod{f(x)}$ hay

$$x^3 \equiv x + 1 \pmod{f(x)}.$$

Điều này có nghĩa là kết quả của phép nhân mà bậc ≥ 3 thì ta sẽ đổi theo modulo đa thức như trên. Khi đó:

$$\begin{aligned}
&122 \cdot 201 = (x^2 + 2x + 2)(2x^2 + 1) \\
&= 2x^4 + 4x^3 + 5x^2 + 2x + 2 \\
&= 2x(x+1) + 4(x+1) + 2x^2 + 2x + 2 \\
&= 4x^2 + 8x + 6 = x^2 + 2x = \overline{120}_{(3)}
\end{aligned}$$

Ghi chú. Ta phải đổi sang vành đa thức xong rồi thực hiện phép nhân trên đó rồi mới đổi sang hệ tam phân; nếu tính toán trực tiếp trên hệ tam phân thì kết quả sẽ không giống!

d) Tìm phần tử nghịch đảo nhân của 122 trong F.

Cần tìm $ax^2 + bx + c$ để $(x^2 + 2x + 2)(ax^2 + bx + c) = 1$.

Khai triển trực tiếp ra như sau:

$$\begin{aligned}
&(x^2 + 2x + 2)(ax^2 + bx + c) \\
&= ax^4 + (2a + b)x^3 + (2a + 2b + c)x^2 + (2c + 2b)x + 2c \\
&= ax(x+1) + (2a + b)(x+1) + (2a + 2b + c)x^2 + (2c + 2b)x + 2c \\
&= (3a + 2b + c)x^2 + (3a + 3b + 2c)x + 2a + b + 2c \\
&= (2b + c)x^2 + 2cx + 2a + b + 2c
\end{aligned}$$

Giải hệ $\begin{cases} 2b + c = 0 \\ 2c = 0 \\ 2a + b + 2c = 1 \end{cases}$, ta có $a = 2, b = c = 0$. Do đó đa thức cần tìm là $2x^2$.

e) Đây là bài khó!

Để không bị trùng ký hiệu, thay $x \to g(x)$ đại diện cho một đa thức trong trường F.

Ta sẽ chọn một số đa thức cụ thể trong F để chỉ ra ràng buộc D, E (do khó giải tổng quát).
Với $g(x) = x$, ta xét bảng lũy thừa sau khi lấy x^k chia cho $f(x) = 2x^3 + x + 1$:

x^2	x^3	x^4	x^5	x^6	x^7
x^2	$x+1$	x^2+x	x^2+x+1	x^2+2x+1	$2x^2+2x+1$

và

x^8	x^9	x^{10}	x^{11}	x^{12}	x^{13}
$2x^2+2$	$x+2$	x^2+2x	$2x^2+x+1$	x^2+2	1

.

Từ đây suy ra $x^{14} = x \pmod{f(x)}$. Đồng thời, 13 đa thức trung gian sinh ra ở trên là

$$F_1 = \{x, x^2, x+1, \ldots, x^2+2, 1\}$$

đều có dạng x^k với $1 \le k \le 13$. Khi đó, nếu $DE \equiv 1$ mod 13, đặt $DE = 13a+1$ thì với mọi $g \in F_1$, ta có

$$(g)^{DE} = (x^k)^{DE} = (x^{DE})^k = (x^{13a+1})^k = (x^{13a} \cdot x)^k = x^k = g\,.$$

Xét các đa thức còn lại trong $F \setminus \{0\}$ là:

$$F_2 = \{2x^2, 2x+2, 2x^2+2x, 2x^2+2x+2, 2x^2+x+2,$$
$$x^2+x+2, x^2+1, 2x^2+x, x^2+2x+2, 2x^2+1, 2\}.$$

Rõ ràng với mỗi $g \in F_2$ thì $g = 2g'$ với $g' \in F_1$ nên $g^2 = 4(g')^2 = (g')^2$. Suy ra

$$g^{26} = (g^2)^{13} = ((g')^2)^{13} = ((g')^{13})^2 = (g')^2 = g^2\,.$$

Do đó, để có $g^{DE} = g$ với $g \in F_2$, ta cần có $DE \equiv 1$ mod 26.

Tóm lại, điều kiện của cặp số D, E thỏa mãn là $DE \equiv 1 \pmod{26}$, suy ra $D, E \in U(\mathbb{Z}_{26})$.

Sau khi tham khảo slide của thầy, mình thấy kết quả $DE = 1 \bmod 26$ ở trên được dùng luôn, xem như công thức có sẵn mà không cần chứng minh lại như trên, cụ thể là phần này:

4.3. Mô hình mã hóa trên trường hữu hạn GF(p^n)
($\mathbb{Z}_p$, đa thức BKQ biến)

$\mathbb{F}$ là trường cấp p^n

$\forall x \in \mathbb{F} \setminus \{0\}$,

$$x^{p^n-1} = \bar{1}$$

$\forall x \in \mathbb{F}$, $\forall k \in \mathbb{Z}$, $x^{k(p^n-1)+1} = x$

chọn D, E sao cho $\bar{D}.\bar{E} = \bar{1}$, $\mathbb{Z}_{p^n-1}$

$$x^{DE} = x$$