MỘT SỐ BÀI TẬP KHÁC (2 ĐỀ CÒN LẠI)

Đề 2.

Bài 1

Xét vành $\mathbb{Z}_3[x]$ gồm các đa thức trên trường $\mathbb{Z}_3$.

a) Vành $\mathbb{Z}_3[x]$ có bao nhiêu đa thức bất khả qui bậc 2? Liệt kê hết các đa thức như vậy.

b) Tìm tất cả các đa thức bậc 3 có nghiệm trong $\mathbb{Z}_3$.

c) Tìm và liệt kê tất cả các đa thức bậc 3 bất khả qui của $\mathbb{Z}_3[x]$.

Lời giải. a) Trên $\mathbb{Z}_3[x]$ thì các đa thức có dạng ax^2+bx+c, và để nó bất khả quy thì nó phải vô nghiệm, khi đó $c \neq 0$. Thay $x=1, x=2$ vào, ta có $a+b+c \neq 0, a+2b+c \neq 0$.

- Nếu $a=1$ thì có x^2+x+2, x^2+2x+2, x^2+1 thỏa mãn.
- Nếu $a=2$ thì có $2x^2+2x+1, 2x^2+x+1, 2x^2+2$ thỏa mãn.

Vậy nên tổng cộng có 6 đa thức.

b) Xét đa thức ax^3+bx^2+cx+d với $a \in \{1,2\}, b,c,d \in \{0,1,2\}$.

- Nếu $d=0$ thì đa thức có nghiệm là $x=0$, và có $2\cdot 3^2=18$ đa thức như thế.

- Nếu $d=1$ thì đa thức chỉ có thể có nghiệm là 1 hoặc 2.

+ Nếu có nghiệm bằng 1 thì: $a+b+c+1=0 \pmod 3$, chọn a có 2 cách, chọn b có 3 cách, khi đó c có 1 cách nên có $2\times 3=6$ đa thức.

+ Nếu có nghiệm bằng 2 thì: $8a+4b+2c+1=0 \pmod 3 \Leftrightarrow 2a+b+2c+1=0 \pmod 3$, chọn a có 2 cách, chọn b có 3 cách, khi đó c có 1 cách nên vẫn có $2\times 3=6$ đa thức.

Trường hợp này có $6+6=12$ đa thức.

- Nếu $d=2$ thì chỉ cần lấy các đa thức ở trên gấp đôi lên là được, nên số lượng vẫn là 12.

Tổng cộng có $18+12\times 2=42$ đa thức.

c) Số đa thức bậc 3 là $2\cdot 3^3=54$ nên số đa thức bất khả quy là $54-42=12$. Cụ thể là

$$\begin{aligned}
&x^3+2x+1,\ x^3+2x+2,\ x^3+2x^2+1,\ x^3+x^2+2,\\
&2x^3+x+1,\ 2x^3+x+2,\ 2x^3+x^2+2,\ 2x^3+2x^2+1,\\
&x^3+x^2+x+2,\ x^3+2x^2+2x+2,\\
&2x^3+2x^2+2x+1,\ 2x^3+x^2+x+1.
\end{aligned}$$

Có thể kiểm tra trực tiếp bằng cách thay $x=0,1,2$ vào, ta thấy chúng đều vô nghiệm (không chia hết cho 3) nên bất khả quy trên $\mathbb{Z}_3[x]$.

Bài 2

Xét xem đa thức h(x) = $\bar{2}x^4 + x^3 + \bar{1} \in \mathbb{Z}_3[x]$ có bất khả qui hay không.

Giả sử $h(x)$ khả quy. Kiểm tra trực tiếp ta thấy $h(0), h(1), h(2)$ đều khác 0 nên $h(x)$ không thể chia hết chi nhân tử bậc 1. Khi đó, $h(x)$ phải là tích của hai đa thức bậc 2.

Ta có $2x^4 + x^3 + 1 = (x^2 + ax + b)(2x^2 + cx + d)$. Khai triển và đồng nhất, ta có

$$\begin{cases} 2a + c = 1 & (1) \\ 2b + d + ac = 0 & (2) \\ bc + ad = 0 & (3) \\ bd = 1 & (4) \end{cases}$$

Từ (4) suy ra $b = d \neq 0$. Từ (2) và $b = d$ thì $ac = 0$. Theo (3) thì $b(a + c) = 0$ nên $a + c = 0$, do đó $a = c = 0$, mâu thuẫn với (1). Hệ này vô nghiệm trên $\mathbb{Z}_3$ nên đa thức bất khả quy.

Bài 3

Xét đa thức *p(x)* = $\bar{2}x^3 + x + \bar{1} \in \mathbb{Z}_3[x]$.

a) Đa thức *p(x)* có bất khả qui hay không?

b) Xét cấu trúc thương **F**=$\mathbb{Z}_3$[x]/<p(x)> với phép toán cộng và nhân. Cấu trúc (**F**, +, .) thuộc loại cấu trúc đại số nào? **F** có bao nhiêu phần tử?

c) Tìm cách biểu diễn các phần tử của **F** như là các số trong hệ đếm cơ số 3. Hãy thiết lập công thức để thực hiện phép nhân của cấu trúc **F**.

Giả sử A = 112 ∈ **F**. Tìm nghịch đảo A^{-1} của A.

d) Tìm tất cả những cặp số K1, K2 (K1 < K2) thỏa mãn $(x^{K1})^{K2}$ = x với mọi x∈**F**.

e) Có thể dùng hàm *E(x)* = x^{43} để thực hiện phép mã hóa (trong **F**) hay không?

f) Giải phương trình X^{41} = B trên **F**, với B∈**F**. Cụ thể hãy tìm tất cả các nghiệm của phương trình X^{41} = 112.

Lời giải. Các câu a, b, c, d tham khảo câu 3 trong file hoặc lý thuyết của thầy đã giảng:

https://drive.google.com/file/d/1tQS4ILc8dqbrCUzNaBVUoVjoNJrCcl5P/view

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

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

$$x^{DE} = x$$

e) Theo câu e ở link trên thì có thể sử dụng được hàm đó vì $x^{43} \neq x$ và tồn tại $k > 43$ để $43k \equiv 1 \pmod{26}$. Câu trả lời là khẳng định.

f) Giải phương trình $X^{41} = 112$. Ta có $41 \cdot 7 = 26 + 1$ nên từ $X^{41} = x^2 + x + 2$, ta suy ra

$$(x^2 + x + 2)^7 = (X^{41})^7 = X^{11 \cdot 26 + 1} = (X^{26})^{11} \cdot X = X .$$

Từ đó suy ra

$$\begin{aligned} X &= (x^2 + x + 2)^7 = \left[(x^2 + x + 2)^2\right]^3 (x^2 + x + 2) = x^3(x^2 + x + 2) \\ &= (x+1)(x^2 + x + 2) = x^3 + 2x^2 + 3x + 2 \\ &= (x+1) + 2x^2 + 2 = 2x^2 + x \end{aligned}$$

chính là đa thức cần tìm. Chú ý rằng ở đây ta dùng kết quả $x^3 \equiv x + 1$ ở bài trong link.

Tổng quát nếu thay $x^2 + x + 2 \to B$ bất kỳ thì ta vẫn có đáp số là $X = B^7$.

Đề 3.

Bài 1

a) Một đa thức bậc nhất trong vành đa thức $\mathbb{Z}_6[x]$ có chắc chắn là một đa thức bất khả qui hay không? Lập luận hoặc cho phản ví dụ.

b) Đa thức *f(x)* = *x* có bất khả qui trong vành đa thức $\mathbb{Z}_6[x]$ hay không?

Lời giải.

Cả hai đều là phủ định. Phản ví dụ: $(2x+3)(3x+2) = x$.

Bài 2

Xét vành $\mathbb{Z}_2[x]$ gồm các đa thức trên trường $\mathbb{Z}_2$.

a) Vành $\mathbb{Z}_2[x]$ có bao nhiêu đa thức bất khả qui bậc 2?

b) Tìm dạng của tất cả các đa thức bậc 4 có nghiệm trong $\mathbb{Z}_2$. Có tất cả bao nhiêu đa thức như vậy?

c) Tìm tất cả các đa thức bậc 4 không có nghiệm trong $\mathbb{Z}_2$ và có thể phân tích thành tích của hai đa thức bậc 2.

d) Từ hai câu trên, hãy lập luận để tìm được tất cả các đa thức bậc 4 bất khả qui của $\mathbb{Z}_2[x]$.

Lời giải. a) Các đa thức bậc hai là $x^2, x^2 + x, x^2 + 1, x^2 + x + 1$, trong đó ba đa thức đầu đã có nghiệm, chỉ còn lại mỗi $x^2 + x + 1$ là vô nghiệm và hiển nhiên bất khả quy trên $\mathbb{Z}_2[x]$.

b) Xét đa thức bậc 4 có dạng $x^4 + ax^3 + bx^2 + cx + d$.

- Nếu nó có nghiệm $x = 0$ thì $d = 0$. Có $2^3 = 8$ đa thức.
- Nếu nó có nghiệm $x = 1$ và $d = 1$ thì $a + b + c = 0$ hay $a + b + c$ chẵn, tức là trong đó sẽ có 3 số chẵn hoặc 1 số chẵn. Có $1 + 3 = 4$ đa thức như vậy.

Suy ra số đa thức thỏa mãn là $8+4=12$.

c) Đa thức duy nhất thỏa mãn là $(x^2+x+1)^2 = x^4+x^2+1$.

d) Tổng số đa thức bậc 4 trên $\mathbb{Z}_2$ là $2^4=16$. Số đa thức vô nghiệm là $16-12=4$, trong đó loại đi một đa thức ở câu c, còn $4-1=3$ đa thức bất khả quy. Cụ thể là

$$x^4+x^3+1,\ x^4+x^3+x^2+x+1,\ x^4+x+1.$$

Bài 3

Xét đa thức $p(x) = x^4 + x^3 + 1 \in \mathbb{Z}_2[x]$.

a) Chứng minh $p(x)$ là một đa thức bất khả qui.

b) Đặt $F=\mathbb{Z}_2[x]/<p(x)>$. Trường F có tất cả bao nhiêu phần tử? Nếu lưu mỗi phần tử của F như một dãy bit, hãy liệt kê tất cả các phần tử của F.

c) Thiết lập công thức (hay mô tả thuật toán) để thực hiện các phép tính trên trường F:

- Phép cộng ;
- Phép nhân ;
- Phép lấy nghịch đảo.

Giả sử A = 1101 $\in$ F. Tìm nghịch đảo A^{-1} của A.

d) Tìm tất cả những cặp số K1, K2 (K1 $\neq$ K2) thỏa mãn $(x^{K1})^{K2} = x$ với mọi $x \in F$.

e) Có thể dùng hàm $E(x) = x^2$ để thực hiện phép mã hóa hay không?

f) Giải phương trình X^{23} = B trên F, với B$\in$F. Cụ thể hãy tìm tất cả các nghiệm của phương trình X^{23} = 1101.

Lời giải.

a, b, c) tương tự trong link:

https://drive.google.com/file/d/1tQS4ILc8dqbrCUzNaBVUoVjoNJrCcl5P/view

Với $A=1101\in F$, để tìm nghịch đảo, ta chú ý $A^{15}=1$ nên nghịch đảo của nó là $A^{-1}=A^{14}$.

d) Đây là trường $GF(2^4)$ nên điều kiện là $K_1K_2=1(\text{mod}15)$.

e) Khẳng định.

f) Ta có $X^{23}=B \to X^{46}=B^2$, mà $X^{46}=X^{15\cdot 3+1}=X$ nên $X=B^2$.

Từ đó $X^{23}=1101$ thì $X=1101^2=(x^3+x^2+1)^2=x^6+x^4+1$.

Xét trong trường sinh bởi $f(x)=x^4+x^3+1$ thì $x^4\equiv x^3+1$. Do đó

$$\begin{aligned} x^6+x^4 &\equiv (x^2+1)(x^3+1) = x(x^3+1)+x^3+x^2+1 \\ &= x^4+x^3+x^2+x+1 \\ &= x^2+x \end{aligned}.$$

Suy ra $X=x^2+x+1$.