MỘT SỐ CÂU BỔ SUNG

15) Đặt n=63. Xét vành $\mathbb{Z}_n$ với phép cộng và nhân modulo. Gọi $U(\mathbb{Z}_n)$ là tập các phần tử đơn vị (phần tử khả nghịch với phép nhân) của $\mathbb{Z}_n$.

a) Điều kiện cần và đủ mà a phải thỏa mãn để $\overline{a} \in U(\mathbb{Z}_n)$?

b) $U(\mathbb{Z}_n)$ có bao nhiêu phần tử?

c) Tìm điều kiện cho hai số nguyên dương K1, K2 để ta có $(x^{K1})^{K2} = x$ với mọi $x \in U(\mathbb{Z}_n)$. Nhờ đó ta có thể mã hóa các phần tử trong $U(\mathbb{Z}_n)$ bằng K1 và giải mã bằng K2.

d) Liệt kê tất cả các cặp khóa (K1, K2) để mã hóa, giải mã các phần tử của $U(\mathbb{Z}_n)$.

e) Các phần tử nào trong $\mathbb{Z}_n \setminus U(\mathbb{Z}_n)$ mà có thể mã hóa và giải mã như trên? Có bao nhiêu phần tử như vậy?

a) Điều kiện cần, đủ là gcd(a,63)=1.

b) U(Z63)=phi(63)=phi(7).phi(9)=6.6=36.

c) Điều kiện K1, K2 là K1.K2=1 mod phi(63)=1 mod 36.

d) Các cặp đó thỏa mãn 1 < K2 < K1 < 36 và tích K1.K2 chia 36 dư 1. Liệt kê ra được

5	7	11	13
29	31	23	25

e) Có 63-36=27 phần tử trong $\mathbb{Z}_n \setminus U(\mathbb{Z}_n)$. Gọi x là phần tử mã hóa được như vậy thì $x^{K_1K_2} = x (\mathrm{mod}\, 63)$ hay $x\left(x^{K_1K_2} - 1\right) = 0 \,\mathrm{mod}\, 63$. Do gcd(x,63)>1 nên có 3 khả năng sau:

* Nếu gcd(x,63)=7, nghĩa là x chia hết cho 7. Chọn được K1.K2 để có x^(K1.K2)=1 mod 9 nên các số này thỏa.

* Nếu gcd(x,63)=9 thì thỏa, tương tự trên.

* Nếu gcd(x,63)=3 hoặc gcd(x,63)=21 thì không thỏa vì x chỉ chia hết cho 3 mà không chia hết cho 9, nên tích x(x^(K1.K2)-1) không thể chia hết cho 63.

Đến đây liệt kê ra được các số thỏa mãn là: 7, 9, 14, 18, 27, 28, 35, 36, 45, 49, 54, 56.

Ghi chú. Bài này nếu thay 63 bởi số nguyên tố hoặc tích các số nguyên tố thì mọi phần tử trong $\mathbb{Z}_n \setminus U(\mathbb{Z}_n)$ đều thỏa. Còn nếu nó có dạng $p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ thì các số $x \in \mathbb{Z}_n \setminus U(\mathbb{Z}_n)$ thỏa mãn câu e) phải có dạng: nếu x, n cùng chia hết cho p thì số mũ của p trong chúng là bằng nhau.

VD. Đổi $63 \to 45 = 5 \cdot 3^2$ thì đáp số câu e sẽ là 5, 9, 10, 18, 20, 25, 27, 35, 36, 40.

Phân biệt nhóm, vành, trường: chú ý quan hệ giữa giữa các khái niệm: X là nhóm thì chưa chắc là vành, còn X là vành thì chưa chắc là trường; ngược lại: X là trường thì chắc chắn là vành, X là vành thì chắc chắn là nhóm.

Nhóm (Group)

Nhóm là một tập hợp G và một phép toán 2 ngôi $\bullet$, $(G, \bullet)$ phải thỏa các tính chất sau:

- Tính đóng (Closure): Với mọi $a, b \in G$, ta có $a \bullet b \in G$
- Tính kết hợp (Associativity): Với mọi $a, b, c \in G$, ta có: $(a \bullet b) \bullet c = a \bullet (b \bullet c)$
- Phần tử đơn vị (Identity element): Tồn tại một phần tử đơn vị $e \in G$ thỏa $e \bullet a = a \bullet e = a$, với mọi $a \in G$. Nếu tồn tại, phần tử đơn vị là duy nhất.
- Phần tử nghịch đảo (Inverse element): với mỗi $a \in G$, tồn tại $b \in G$ thỏa $a \bullet b = b \bullet a = e$, với e là phần tử đơn vị của nhóm. Phần tử nghịch đảo của a thường được kí hiệu là a^{-1} hoặc $-a$, tùy theo phép toán đang sử dụng.

Ví dụ:

- Nhóm: Tập hợp số nguyên $\mathbb{Z}$ với phép toán cộng. Phần tử đơn vị là 0.
- Không phải nhóm: Tập $\mathbb{Z}$ với phép toán nhân (không có phần tử nghịch đảo).

Vành (Ring)

Xét tập hợp R với 2 phép toán + và ·, R được gọi là một vành nếu ta có các tính chất sau:

- Cộng và nhân có tính đóng
- Cộng và nhân có tính kết hợp:
  $\forall a, b, c \in R, (a + b) + c = a + (b + c), (a \cdot b) \cdot c = a \cdot (b \cdot c)$
- Tồn tại phần tử đơn vị cho phép cộng và nhân, ta kí hiệu 0 và 1 lần lượt là phần tử đơn vị của phép cộng và nhân: $\forall a \in R, a + 0 = 0 + a = a, a \cdot 1 = 1 \cdot a = a$
- Phép cộng có tính giao hoán: $a + b = b + a, \forall a, b \in R$
- Tồn tại phần tử nghịch đảo cho phép cộng, $\forall a \in R, \exists b \in R, a + b = 0$
- Tính phân phối của phép nhân đối với phép cộng:

  $$a \cdot (b + c) = (a \cdot b) + (a \cdot b)$$

  $$(b + c) \cdot a = (b \cdot a) + (c \cdot a)$$

Lưu ý là phép nhân không cần có tính giao hoán và không cần phải có phần tử nghịch đảo.

Trường (Field)

Xét tập hợp F với 2 phép toán + và ·. F được gọi là một trường nếu nó thỏa các tính chất sau:

- Cộng và nhân có tính đóng
- Cộng và nhân có tính giao hoán
- Tồn tại phần tử đơn vị cho cộng và nhân, kí hiệu lần lượt là 0 và 1.
- Tồn tại phần tử nghịch đảo $-a$ với $\forall a \in F$, thỏa $a + (-a) = 0$
- Với $\forall a \neq 0$, tồn tại a^{-1} thỏa $a \cdot a^{-1} = 1$
- Tính phân phối của phép nhân đối với phép cộng: $a \cdot (b + c) = (a \cdot b) + (a \cdot b)$

Trường hữu hạn là một trường có số phần tử là hữu hạn. Một trường hữu hạn thường gặp là $\mathbb{Z}_p$ với p nguyên tố.

1) Tập hợp $\mathbb{Z}_{41} \setminus \{ \overline{0} \}$ có tạo thành nhóm với phép nhân hay không? Tại sao?

2) Tập hợp $\mathbb{Z}_{1024} \setminus \{ \overline{0} \}$ có tạo thành nhóm với phép nhân hay không? Tại sao?

3) Chứng đa thức $f(x) = \overline{2}x + \overline{3}$ không thuộc về $U(\mathbb{Z}_6[x])$.

4) Chứng đa thức $f(x) = x$ không bất khả quy trong $\mathbb{Z}_6[x]$, nghĩa là $f(x)$ có cách rút gọn không tầm thường trong $\mathbb{Z}_6[x]$.

5) Phương trình bậc hai $\overline{3}x^2 + \overline{3}x = 0$ có bao nhiêu nghiệm trong $\mathbb{Z}_6$?

6) Giả sử $a, b \in \mathbb{Z}_6$. Phương trình $\overline{5}x^2 + \overline{4}ax + \overline{5}a^2 + \overline{3}b^2 - \overline{1} = 0$ có nghiệm trong $\mathbb{Z}_6$ hay không?

7) Tìm tất cả các đa thức bậc hai bất khả quy trong $\mathbb{Z}_2[x]$.

8) Tìm tất cả các đa thức bậc bốn vô nghiệm nhưng không bất khả quy trong $\mathbb{Z}_2[x]$.

9) Tìm tất cả các đa thức bậc hai bất khả quy trong $\mathbb{Z}_3[x]$.

10) Chứng minh $i\sqrt{3}$ là nguyên tố trong miền nguyên $(\mathbb{Z}[i\sqrt{3}], +, \cdot)$.

11) Chứng minh 2 là KTRG nhưng không nguyên tố trong miền nguyên $(\mathbb{Z}[i\sqrt{3}], +, \cdot)$.

1) Có vì tích của hai số trong Z41\{0} thì không thể ra 0 nên nó đóng với phép nhân. Xem lại định nghĩa nhóm.

2) Không, chẳng hạn lấy x = 64, y = 32 thuộc Z[1024]\{0} thì tích của nó chia hết cho 1024, tức là ra 0, nhưng tập trên không lấy số 0.

3) Cần chứng tỏ rằng không tồn tại đa thức trong $\mathbb{Z}_6[x]$ mà

$$(2x+3)f(x) = 1 (\mathrm{mod}\, 6).$$

Gọi a là hệ số tự do của $f(x)$ thì hệ số tự do của tích trên là $3a \equiv 1 (\mathrm{mod}\, 6)$, vô lý.

4) Ta có $(2x+3)(3x+2) = 6x^2 + 7x + 6 = x$ trong $\mathbb{Z}_6[x]$.

5) $3x^2 + 3x = 3x(x+1)$. Thế $x = 0,1,\ldots,5$ vào thử là được.

6) Thử các số vào để kiểm tra.

7) Chỉ có duy nhất đa thức $x^2 + x + 1$.

8) Chỉ có duy nhất $(x^2 + x + 1)^2$.

9) Có 6 đa thức: x^2+x+2, x^2+2x+2, 2x^2+2x+1, 2x^2+x+1, x^2+1 và 2x^2+2.

10) Miền $\mathbb{Z}[i\sqrt{3}]$ có dạng $x + i \cdot y\sqrt{3}$ với $x, y \in \mathbb{Z}$. Chú ý rằng $i^2 = -1$.

Giả sử $i\sqrt{3} = (x_1 + iy_1\sqrt{3})(x_2 + iy_2\sqrt{3})$, khai triển vế phải ra, ta có

$$x_1x_2 - 3y_1y_2 = 0 \text{ và } x_1y_2 + x_2y_1 = 1.$$

Từ $x_1y_2 + x_2y_1 = 1,$ suy ra $\gcd(x_1, y_1) = \gcd(x_2, y_2) = 1$, vì nếu không thì giả sử chúng có $\gcd = d > 1$ thì 1 chia hết cho $d,$ mâu thuẫn.

Từ $x_1x_2 = 3y_1y_2$, mà x_1, y_1 không có ước chung nên x_2 chia hết cho y_2, đặt $x_2 = ay_2$. Tương tự đặt $x_1 = by_1$, thay vào có $ab = 3$ và $y_1y_2(a + b) = 1.$

Đến đây dễ thấy a,b cùng lẻ, kéo theo $a + b$ chẵn, vô lý, vì 1 lẻ.

11) Không rõ chữ KTRG viết tắt của gì.

Còn để chứng minh 2 không nguyên tố trong miền $\mathbb{Z}[i\sqrt{3}],$ ta chỉ ra có

$$(a + i \cdot b\sqrt{3})(c + i \cdot d\sqrt{3}) = 2 \text{ có nghiệm } a,b,c,d \in \mathbb{Z}.$$

hay $ac - 3bd = 2,\ ad + bc = 0$. Chọn $b = d = 0, a = 1, c = 2$ là được.