BÀI TẬP BỔ SUNG

Bài 1

Xét tập hợp M gồm các ma trận vuông 2x2 có dạng $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}$ với a, b, c $\in \mathbb{Z}_8$. Tập M là một vành với phép cộng và nhân ma trận, phần tử 0 là $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ và phần tử 1 là $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Gọi $\mathbf{U}(M)$ là tập các ma trận của M khả nghịch với phép nhân.

a) Tính $\varphi(8)$.

b) Giả sử $a, c \in \mathbb{Z}_8$. Tính $(a-c)(a^3 + a^2c + ac^2 + c^3)$.

c) Giả sử $a, c \in \mathbf{U}(\mathbb{Z}_8)$. Chứng minh: $(a-c)(a^3 + a^2c + ac^2 + c^3) = \overline{0}$.

Ghi chú: Lưu ý rằng từ giả thiết $a - c \neq \overline{0}$ và $(a-c)(a^3 + a^2c + ac^2 + c^3) = \overline{0}$ ta không thể suy ra $a^3 + a^2c + ac^2 + c^3 = \overline{0}$. Bạn hãy cho ví dụ.

d) Giả sử $a, c \in \mathbf{U}(\mathbb{Z}_8)$. Chứng minh:

$$a^{31} + a^{30}c + a^{29}c^2 + a^{28}c^3 + \ldots + a^2c^{29} + ac^{30} + c^{31} = \overline{0}.$$

Nếu không thể lý luận thì bạn có thể viết chương trình kiểm tra, chạy thử dựa vào tính chất $\mathbf{U}(\mathbb{Z}_8)$ chỉ có vài phần tử. Nhưng cách thức này sẽ khó nâng tổng quát.

e) Tìm điều kiện cần và đủ mà a, b, c phải thỏa mãn để $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \in \mathbf{U}(M)$.

f) Đếm số lượng các phần tử của $\mathbf{U}(M)$.

g) Tìm công thức cho $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}^m$ và tính $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}^{8\varphi(8)}$.

h) Chứng minh $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}^{8\varphi(8)} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ với mọi ma trận $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \in \mathbf{U}(M)$.

Bài 2

Luyện tập nhờ làm lại Bài 1, thay $n = 8$ bởi 11, 15, 27, 33.

Bài 3. Dựa vào ý tưởng của Bài 1 để giải trường hợp tổng quát hơn như sau. Trường hợp không thể giải quyết trường hợp n tổng quát, bạn hãy viết chương trình máy tính để khảo sát kết quả.

Giả sử n là số nguyên dương lớn hơn 1. Xét tập hợp M_n gồm các ma trận vuông 2x2 có dạng $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}$ với $a, b, c \in \mathbb{Z}_n$. Tập M_n là một vành với phép cộng và nhân ma trận. Gọi $\mathbf{U}(M_n)$ là tập các phần tử đơn vị (phần tử khả nghịch với phép nhân) của M_n.

a) Tìm điều kiện cần và đủ mà a, b, c phải thỏa mãn để $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \in \mathbf{U}(M_n)$.

b) Chứng minh $|U(M_n)| = n\,[\varphi(n)]^2$. Trong đó $\varphi(n)$ là hàm phi Euler.

c) Chứng minh $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}^{n[\varphi(n)]^2} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ với mọi ma trận $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \in \mathbf{U}(M)$.

d) Có thể thay lũy thừa $n\,[\varphi(n)]^2$ nói trên bởi một số m nhỏ hơn hay không? Bạn có thể thử nghiệm bằng chương trình máy tính trước khi khảo sát kết quả lý thuyết.

e) Chứng minh nếu $D, E \in \mathbb{Z}_{1100}$ thỏa mãn $D\,.\,E = \overline{1}$ thì $(\boldsymbol{x}^E)^D = \boldsymbol{x}$ với mọi ma trận $\boldsymbol{x} \in \boldsymbol{U}(M_{11})$. Nhờ đó ta có thể mã hóa ma trận trong $\mathbf{U}(M_{11})$ bằng E và giải mã bằng D.

f) Cho ví dụ về 5 cặp khóa (E, D) để mã hóa các phần tử của $\mathbf{U}(M_{11})$.

g) Các ma trận nào trong $M_{11} \setminus \mathbf{U}(M_{11})$ mà có thể mã hóa và giải mã như trên. Có bao nhiêu ma trận như vậy?

h) Thực tế có thể mã hóa các phần tử của $\mathbf{U}(M_{11})$ nhờ một sơ đồ mã hóa thu gọn hơn theo nghĩa là có thể tìm được số nguyên dương $m<1100$ sao cho nếu $E, D \in \mathbb{Z}_m$ thỏa mãn $(\boldsymbol{x}^E)^D = \boldsymbol{x}$ với mọi ma trận $\boldsymbol{x} \in \boldsymbol{U}(M_{11})$. Hãy khảo sát vấn đề này xem tồn tại m như vậy hay không, tìm m nhỏ nhất có thể được.

LỜI GIẢI ĐỀ ÔN THI CUỐI KỲ 2019
MÔN "PHƯƠNG PHÁP TOÁN CHO TIN HỌC"

Bài 1. Xét tập hợp M gồm các ma trận vuông 2×2 có dạng $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}$ với $a,b,c \in \mathbb{Z}_8$. Tập M là một vành với phép cộng và phép nhân ma trận, phần tử 0 là $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, còn phần tử 1 là $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Gọi $U(M)$ là tập hợp các ma trận của M khả nghịch với phép nhân.

a) Tính $\varphi(8)$.

Ta có $\varphi(8)=4$ vì có 4 số $1,3,5,7$ nguyên tố cùng nhau với 8 và không vượt quá 8.

b) Giả sử $a,c \in U(\mathbb{Z}_8)$. Tính $(a-c)(a^3+a^2c+ac^2+c^3)$.

Ta có $(a-c)(a^3+a^2c+ac^2+c^3)=a^4-c^4$.

c) Giả sử $a,c \in U(\mathbb{Z}_8)$. Chứng minh rằng $(a-c)(a^3+a^2c+ac^2+c^3)=\overline{0}$.

Lưu ý nếu giả thiết là $a-c\neq\overline{0}$ và $(a-c)(a^3+a^2c+ac^2+c^3)=\overline{0}$, ta không thể suy ra được $a^3+a^2c+ac^2+c^3=\overline{0}$. Hãy cho ví dụ.

Vì $a,c\in U(\mathbb{Z}_8)$ nên $a^{\varphi(8)}=a^4=\overline{1}$, $c^{\varphi(8)}=c^4=\overline{1}$, suy ra $a^4-c^4=\overline{0}$.

Ví dụ cho ý sau: Lấy $a=1, c=5$ là hai số thỏa mãn điều kiện $a,c\in U(\mathbb{Z}_8)$ và $a-c\neq\overline{0}$ nhưng tính toán trực tiếp cho thấy $a^3+a^2c+ac^2+c^3=\overline{4}$.

d) Giả sử $a,c\in U(\mathbb{Z}_8)$. Chứng minh

$$a^{31}+a^{30}c+\cdots+ac^{30}+c^{31}=\overline{0}.$$

Gọi T là vế trái của biểu thức trên.

Ta có $a^4=\overline{1}$ nên với mọi $n\in\mathbb{Z}^+$, nếu đặt $n=4k+r$ với r là số dư của n khi chia cho 4 thì $a^n=a^{4k+r}=a^{4k}\cdot a^r=\overline{1}\cdot a^r=a^r$, tức là lũy thừa của a trong $\mathbb{Z}_8$ là tuần hoàn chu kỳ 4.

Ta thấy rằng T là tổng của các số hạng có dạng $a^m\cdot c^n$ với $m+n=31$ là số chia 4 dư 3.

Nếu m chia hết cho 4 thì n chia 4 dư 3 và $a^m\cdot c^n=\overline{1}\cdot c^3=c^3$. Từ 0 đến 31 có tất cả 32 số và trong đó, có đúng 8 số m chia hết cho 4 nên tổng tất cả các số hạng như thế (đó là $a^0c^{31},a^4c^{27},a^8c^{23},\ldots,a^{28}c^3$) đều có thể viết thành c^3 trong $\mathbb{Z}_8$, thế nên tổng của chúng là $8c^3=\overline{0}$ trong $\mathbb{Z}_8$. Tương tự nếu m chia 4 dư $1,2,3$ thì theo thứ tự n chia 4 dư $2,1,0$ và các biểu thức có dạng này lần lượt được viết thành ac^2,a^2c,a^3. Ngoài ra, mỗi biểu thức xuất hiện đúng 8 lần nên tổng của mỗi nhóm đều là $\overline{0}$. Từ đó suy ra $T=\overline{0}$.

e) Tìm điều kiện cần và đủ của a,b,c để $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \in U(M)$.

Để $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \in U(M)$ thì nó khả nghịch với phép nhân. Theo giả thiết thì phần tử đơn vị của $U(M)$ là $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ nên cần có $\begin{pmatrix} a' & 0 \\ b' & c' \end{pmatrix} \in U(M)$ sao cho $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}\begin{pmatrix} a' & 0 \\ b' & c' \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ hay

$$aa' = 1, ba' + cb' = 0, cc' = 1.$$

Do $aa' = cc' = \bar{1}$ nên $a, c, a', c' \in U(\mathbb{Z}_8)$ (là các phần tử khả nghịch trong $\mathbb{Z}_8$). Khi đó, với mọi $b \in \mathbb{Z}_8$, ta có $ba' + cb' = 0 \Leftrightarrow c'(ba' + cb') = 0 \Leftrightarrow bc'a' + b' = 0$ nên chọn $b' = -bc'a'$ là được.

Vì thế nên điều kiện cần và đủ là $a, c \in U(\mathbb{Z}_8)$ và $b \in \mathbb{Z}_8$.

f) Đếm số lượng các phần tử của $U(M)$.

Theo câu e thì có 4 cách chọn cho a,c vì $\varphi(8) = 4$, và 8 cách chọn b nên số lượng ma trận trong $U(M)$ là $4^2 \cdot 8 = 128$.

g) Tìm công thức cho $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}^m$ và tính $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}^{8\varphi(8)}$.

Bằng quy nạp, ta sẽ chứng minh công thức $\boxed{\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}^m = \begin{pmatrix} a^m & 0 \\ b \cdot \dfrac{a^m - c^m}{a - c} & c^m \end{pmatrix}}$ với mọi $m = 1, 2, 3, \ldots$

Ghi chú. Công thức này dự đoán được nhờ tính thử vài giá trị m nhỏ.

Thật vậy, với $m = 1$ thì đẳng thức trên đúng.

Giả sử ta đã có kết quả trên với m, xét lũy thừa $m+1$ thì theo công thức nhân ma trận:

$$\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}^{m+1} = \begin{pmatrix} a^m & 0 \\ b \cdot \dfrac{a^m - c^m}{a - c} & c^m \end{pmatrix}\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} = \begin{pmatrix} a^{m+1} & 0 \\ b \cdot \dfrac{a(a^m - c^m)}{a - c} + b \cdot c^m & c^{m+1} \end{pmatrix}.$$

Chú ý rằng $b \cdot \dfrac{a(a^m - c^m)}{a - c} + b \cdot c^m = \dfrac{b}{a - c}\left(a(a^m - c^m) + (a - c)c^m\right) = b \cdot \dfrac{a^{m+1} - c^{m+1}}{a - c}$. Do đó, khẳng định cũng đúng với $m+1$ và theo quy nạp thì nó đúng với mọi m.

Từ đó suy ra $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}^{8\varphi(8)} = \begin{pmatrix} a & 0 \\ b & c \end{pmatrix}^{32} = \begin{pmatrix} a^{32} & 0 \\ b \cdot \dfrac{a^{32} - c^{32}}{a - c} & c^{32} \end{pmatrix}$.

h) Chứng minh rằng $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}^{8\varphi(8)} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ với mọi ma trận $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \in U(M)$.

Theo công thức đã tính được ở trên thì $a^{32} = (a^4)^8 = \bar{1}$ vì $a \in U(\mathbb{Z}_8)$. Tương tự thì $c^{32} = \bar{1}$.

Ta cũng có $b \cdot \dfrac{a^{32} - c^{32}}{a - c} = b(a^{31} + a^{30}c + \cdots + ac^{30} + c^{31})$. Ngoài ra, theo câu d thì biểu thức trong dấu ngoặc bằng $\bar{0}$ trong $\mathbb{Z}_8$ nên ta có được $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}^{8\varphi(8)} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Giải mẫu bài 2 với các câu hỏi $a \to h$ sẽ được đổi số tương ứng cho phù hợp.

Bài 2. Giải mẫu với $n = 11$.

a) Tính $\varphi(11)$.

Ta có $\varphi(11) = 10$ vì có 10 số $1, 2, 3, \ldots, 10$ nguyên tố cùng nhau với 11 và không vượt quá 11.

b) Giả sử $a, c \in U(\mathbb{Z}_{11})$. Tính $(a - c)(a^9 + a^8c + \cdots + ac^8 + c^9)$.

Ta có $(a - c)(a^9 + a^8c + \cdots + ac^8 + c^9) = a^{10} - b^{10}$.

c) Giả sử $a, c \in U(\mathbb{Z}_{11})$. Chứng minh rằng $(a - c)(a^9 + a^8c + \cdots + ac^8 + c^9) = \bar{0}$.

Vì $a, c \in U(\mathbb{Z}_{11})$ nên $a^{\varphi(11)} = a^{10} = \bar{1}$, $c^{\varphi(11)} = c^{10} = \bar{1}$, suy ra $a^{10} - c^{10} = \bar{0}$.

<u>Ghi chú quan trọng</u>: ở đây 11 là số nguyên tố nên nếu $a \neq c$ thì có thể suy ra dấu ngoặc thứ hai là $\bar{0}$. Điều này sẽ dùng cho câu <u>3(h) ở trang cuối</u>!

Ở bài gốc, đề cho số 8 không phải là số nguyên tố nên không thể loại bỏ hiệu $a - c$ đi được, và vì thế cần có $8\varphi(8)$ thay vì $\varphi(8)$ thì đề bài mới đúng.

d) Giả sử $a, c \in U(\mathbb{Z}_{11})$. Chứng minh $a^9 + a^8c + \cdots + ac^8 + c^9 = \bar{0}$.

Điều này đúng theo ghi chú quan trọng ở trên.

e) Tìm điều kiện cần và đủ của a, b, c để $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \in U(M)$.

Tương tự câu e, điều kiện cần và đủ là $a, c \in U(\mathbb{Z}_{11})$ và $b \in \mathbb{Z}_{11}$.

f) Đếm số lượng các phần tử của $U(M)$.

Kết quả là $10^2 \times 11 = 1100$.

g) Tìm công thức cho $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}^{m}$ và tính $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}^{\varphi(11)}$.

Ghi chú: cách chứng minh công thức tương tự bài 1.

Từ công thức suy ra $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}^{\varphi(11)} = \begin{pmatrix} a & 0 \\ b & c \end{pmatrix}^{10} = \begin{pmatrix} a^{10} & 0 \\ b\cdot\dfrac{a^{10}-c^{10}}{a-c} & c^{10} \end{pmatrix}$.

h) Chứng minh rằng $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}^{\varphi(11)} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ với mọi ma trận $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \in U(M)$.

Theo công thức đã tính được ở trên thì $a^{10} = \bar{1}$ vì $a \in U(\mathbb{Z}_{11})$. Tương tự thì $c^{10} = \bar{1}$.

Ta cũng có $b\cdot\dfrac{a^{10}-c^{10}}{a-c} = b(a^9 + a^8c + \cdots + ac^8 + c^9)$. Ngoài ra, theo câu d thì biểu thức trong dấu ngoặc bằng $\bar{0}$ trong $\mathbb{Z}_{11}$ nên ta có được $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}^{\varphi(11)} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Bài 2. Giải mẫu với $n = 15$.

a) Tính $\varphi(15)$.

Ta có $\varphi(15) = \varphi(3)\varphi(5) = 2\cdot 4 = 8$.

Ghi chú. ở trên là cách tính dùng công thức của hàm φ, nếu cẩn thận ta có thể liệt kê các số nguyên tố cùng nhau với 15 ra bằng cách nhẩm hoặc tra bảng.

b) Giả sử $a, c \in U(\mathbb{Z}_{15})$. Tính $(a-c)(a^7 + a^6c + \cdots + ac^6 + c^7)$.

Ta có $(a-c)(a^7 + a^6c + \cdots + ac^6 + c^7) = a^8 - b^8$.

c) Giả sử $a, c \in U(\mathbb{Z}_{15})$. Chứng minh rằng $(a-c)(a^7 + a^6c + \cdots + ac^6 + c^7) = \bar{0}$.

Lưu ý nếu giả thiết là $a - c \neq \bar{0}$ và $(a-c)(a^7 + a^6c + \cdots + ac^6 + c^7) = \bar{0}$. ta không thể suy ra được $a^7 + a^6c + \cdots + ac^6 + c^7 = \bar{0}$. Bạn hãy cho ví dụ.

Vì $a, c \in U(\mathbb{Z}_{11})$ nên $a^{\varphi(11)} = a^8 = \bar{1}$, $c^{\varphi(11)} = c^8 = \bar{1}$, suy ra $a^8 - c^8 = \bar{0}$.

Ví dụ cho ý sau: Lấy $a = 1, c = 4$ là hai số thỏa mãn điều kiện $a, c \in U(\mathbb{Z}_{15})$ và $a - c \neq \bar{0}$ nhưng tính tính trực tiếp cho thấy $a^7 + a^6c + \cdots + ac^6 + c^7 = \dfrac{a^8 - c^8}{a-c} = 21845 = \bar{5} \neq \bar{0}$.

Ghi chú. Mẹo ở đây là chỉ cần chọn các số a,c sao cho $a-c\notin U(\mathbb{Z}_{15})$ là có ngay ví dụ; ở trên ta chọn $a=1,c=4$ thì $a-c=3$; có thể chọn $a=1,c=6$ cũng được.

d) Giả sử $a,c\in U(\mathbb{Z}_{15})$. Chứng minh

$$a^{119}+a^{118}c+\cdots+ac^{118}+c^{119}=\overline{0}.$$

Ghi chú: 119 được tính bằng cách lấy $15\times\varphi(15)=120$ rồi trừ đi 1.

Ta có $a^8=\overline{1}$ nên với mọi $n\in\mathbb{Z}^+$, nếu đặt $n=8k+r$ với r là số dư của n khi chia cho 8 thì $a^n=a^{8k+r}=a^{8k}\cdot a^r=\overline{1}\cdot a^r=a^r$, tức là lũy thừa của a trong $\mathbb{Z}_{15}$ là tuần hoàn chu kỳ 8.

Ta thấy rằng T là tổng của các số hạng có dạng $a^m\cdot c^n$ với $m+n=119$ chia 8 dư 7.

Nếu m chia hết cho 8 thì n chia 8 dư 7 và $a^m\cdot c^n=\overline{1}\cdot c^7=c^7$. Từ 0 đến 119 có tất cả 120 số và trong đó, có đúng 15 số m chia hết cho 8 nên tổng tất cả các số hạng như thế (đó là $a^0c^{119},a^8c^{111},\ldots,a^{112}c^7$) đều có thể viết thành c^7 trong $\mathbb{Z}_{15}$, thế nên tổng của chúng là $15c^7=\overline{0}$ trong $\mathbb{Z}_{15}$. Tương tự nếu m chia 8 dư $1,2,\ldots,7$ thì theo thứ tự n chia 8 dư $6,5,\ldots,0$ và các biểu thức có dạng này lần lượt được viết thành $ac^6,a^2c^5,\ldots,a^7$. Ngoài ra, mỗi biểu thức xuất hiện đúng 15 lần nên tổng của mỗi nhóm đều là $\overline{0}$. Từ đó suy ra $T=\overline{0}$.

e) Tìm điều kiện cần và đủ của a,b,c để $\begin{pmatrix} a & 0\\ b & c\end{pmatrix}\in U(M)$.

Tương tự câu e, điều kiện cần và đủ là $a,c\in U(\mathbb{Z}_{15})$ và $b\in\mathbb{Z}_{15}$.

f) Đếm số lượng các phần tử của $U(M)$.

Kết quả là $8^2\times 15=960$.

g) Tìm công thức cho $\begin{pmatrix} a & 0\\ b & c\end{pmatrix}^m$ và tính $\begin{pmatrix} a & 0\\ b & c\end{pmatrix}^{15\varphi(15)}$.

Ghi chú: cách chứng minh công thức tương tự bài 1.

Từ công thức suy ra $\begin{pmatrix} a & 0\\ b & c\end{pmatrix}^{15\varphi(15)}=\begin{pmatrix} a & 0\\ b & c\end{pmatrix}^{120}=\begin{pmatrix} a^{120} & 0\\ b\cdot\dfrac{a^{120}-c^{120}}{a-c} & c^{120}\end{pmatrix}$.

h) Chứng minh rằng $\begin{pmatrix} a & 0\\ b & c\end{pmatrix}^{15\varphi(15)}=\begin{pmatrix} 1 & 0\\ 0 & 1\end{pmatrix}$ với mọi ma trận $\begin{pmatrix} a & 0\\ b & c\end{pmatrix}\in U(M)$.

Theo công thức đã tính được ở trên thì $a^{120}=(a^8)^{15}=\overline{1}$ vì $a\in U(\mathbb{Z}_{15})$. Tương tự thì $c^{120}=\overline{1}$.

Ta cũng có $b\cdot\dfrac{a^{120}-c^{120}}{a-c}=b(a^{119}+a^{118}c+\cdots+ac^{118}+c^{119})=\overline{0}$ nên $\begin{pmatrix} a & 0\\ b & c\end{pmatrix}^{15\varphi(15)}=\begin{pmatrix} 1 & 0\\ 0 & 1\end{pmatrix}$.

Bài 2. Giải mẫu với $n = 27$.

a) Tính $\varphi(27)$.

Ta có $\varphi(27) = 3^2\varphi(3) = 18$.

Ghi chú. ở trên là cách tính dùng công thức của hàm φ, nếu cẩn thận ta có thể liệt kê các số nguyên tố cùng nhau với 27 ra bằng cách nhẩm hoặc tra bảng.

b) Giả sử $a, c \in U(\mathbb{Z}_{27})$. Tính $(a-c)(a^{17} + a^{16}c + \cdots + ac^{16} + c^{17})$.

Ta có $(a-c)(a^{17} + a^{16}c + \cdots + ac^{16} + c^{17}) = a^{18} - b^{18}$.

c) Giả sử $a, c \in U(\mathbb{Z}_{27})$. Chứng minh rằng $(a-c)(a^{17} + a^{16}c + \cdots + ac^{16} + c^{17}) = \overline{0}$.

Lưu ý nếu giả thiết là $a - c \neq \overline{0}$ và $(a-c)(a^{17} + a^{16}c + \cdots + ac^{16} + c^{17}) = \overline{0}$ ta không thể suy ra được $a^{17} + a^{16}c + \cdots + ac^{16} + c^{17} = \overline{0}$. Bạn hãy cho ví dụ.

Vì $a, c \in U(\mathbb{Z}_{27})$ nên $a^{\varphi(27)} = a^{18} = \overline{1}$, $c^{\varphi(27)} = c^{18} = \overline{1}$, suy ra $a^{18} - c^{18} = \overline{0}$.

Ví dụ cho ý sau: Lấy $a = 1, c = 7$ là hai số thỏa mãn điều kiện $a, c \in U(\mathbb{Z}_{27})$ và $a - c \neq \overline{0}$ nhưng tính tính trực tiếp cho thấy $(a-c)(a^{17} + a^{16}c + \cdots + ac^{16} + c^{17}) = \dfrac{a^{18} - c^{18}}{a - c} = 18 \pmod{27}$.

d) Giả sử $a, c \in U(\mathbb{Z}_{27})$. Chứng minh

$$a^{485} + a^{484}c + \cdots + ac^{484} + c^{485} = \overline{0}.$$

Ghi chú: 485 được tính bằng cách lấy $27 \times \varphi(27) = 486$ rồi trừ đi 1.

Ta có $a^{18} = \overline{1}$ nên với mọi $n \in \mathbb{Z}^+$, nếu đặt $n = 18k + r$ với r là số dư của n khi chia cho 18 thì $a^n = a^{18k+r} = a^{18k} \cdot a^r = \overline{1} \cdot a^r = a^r$, tức là lũy thừa của a trong $\mathbb{Z}_{27}$ là tuần hoàn chu kỳ 18.

Ta thấy rằng T là tổng của các số hạng có dạng $a^m \cdot c^n$ với $m + n = 485$ chia 18 dư 17.

Nếu m chia hết cho 18 thì n chia 18 dư 17 và $a^m \cdot c^n = \overline{1} \cdot c^{17} = c^{17}$. Từ 0 đến 485 có tất cả 486 số và trong đó, có đúng 27 số m chia hết cho 18 nên tổng tất cả các số hạng như thế (đó là $a^0c^{485}, a^{18}c^{467}, \ldots, a^{468}c^{17}$) đều có thể viết thành c^{17} trong $\mathbb{Z}_{27}$, thế nên tổng của chúng là $27c^{17} = \overline{0}$ trong $\mathbb{Z}_{27}$. Tương tự nếu m chia 18 dư $1, 2, \ldots, 17$ thì theo thứ tự n chia 18 dư $16, 15, \ldots, 0$ và các biểu thức có dạng này lần lượt được viết thành $ac^{16}, a^2c^{15}, \ldots, a^{17}$. Ngoài ra, mỗi biểu thức xuất hiện đúng 27 lần nên tổng của mỗi nhóm đều là $\overline{0}$. Từ đó suy ra $T = \overline{0}$.

e) Tìm điều kiện cần và đủ của a, b, c để $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \in U(M)$.

Tương tự câu e, điều kiện cần và đủ là $a, c \in U(\mathbb{Z}_{27})$ và $b \in \mathbb{Z}_{27}$.

f) Đếm số lượng các phần tử của $U(M)$.

Kết quả là $18^2 \times 27 = 8748$.

g) Tìm công thức cho $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}^m$ và tính $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}^{27\varphi(27)}$.

Ghi chú: cách chứng minh công thức tương tự bài 1.

Từ công thức suy ra $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}^{27\varphi(27)} = \begin{pmatrix} a & 0 \\ b & c \end{pmatrix}^{486} = \begin{pmatrix} a^{486} & 0 \\ b\cdot\dfrac{a^{486}-c^{486}}{a-c} & c^{486} \end{pmatrix}$.

h) Chứng minh rằng $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}^{27\varphi(27)} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ với mọi ma trận $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \in U(M)$.

Theo công thức đã tính được ở trên thì $a^{486} = (a^{18})^{27} = \bar{1}$ vì $a \in U(\mathbb{Z}_{27})$. Tương tự thì $c^{486} = \bar{1}$.

Ta cũng có $b\cdot\dfrac{a^{486}-c^{486}}{a-c} = b(a^{485} + a^{484}c + \cdots + ac^{484} + c^{485})$. Ngoài ra, theo câu d thì biểu thức trong dấu ngoặc bằng $\bar{0}$ trong $\mathbb{Z}_{27}$ nên ta có được $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}^{27\varphi(27)} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Bài 2. Giải mẫu với $n = 33$, câu này tương tự $n = 15$, ở dưới chỉ tóm tắt kết quả.

a) Tính $\varphi(33) = 20$.

b,c,d) Đổi thành $(a-c)(a^{19} + a^{18}c + \cdots + ac^{18} + c^{19})$. Ở ý ví dụ của câu c, chọn $a = 1, c = 4$ thì sẽ có $a^{19} + a^{18}c + \cdots + ac^{18} + c^{19} = \overline{11} \neq \bar{0}$.

f) Đếm số lượng các phần tử của $U(M)$ là $20^2 \times 33 = 13200$.

Bài 3. Giả sử n là số nguyên dương lớn hơn 1, xét tập hợp M_n gồm các ma trận vuông 2×2 có dạng $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}$ với $a,b,c \in \mathbb{Z}_n$. Tập M_n là một vành với phép cộng và phép nhân ma trận, phần tử 0 là $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, còn phần tử 1 là $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Gọi $U(M_n)$ là tập hợp các ma trận của M_n khả nghịch.

a) Tìm điều kiện cần và đủ của a,b,c để $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \in U(M_n)$.

Để $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \in U(M_n)$ thì nó khả nghịch với phép nhân. Theo giả thiết thì phần tử đơn vị của $U(M_n)$ là $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ nên cần có $\begin{pmatrix} a' & 0 \\ b' & c' \end{pmatrix} \in U(M_n)$ sao cho $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}\begin{pmatrix} a' & 0 \\ b' & c' \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ hay

$$aa' = \bar{1}, ba' + cb' = \bar{0}, cc' = \bar{1}.$$

Do $aa' = cc' = \bar{1}$ nên $a, c, a', c' \in U(\mathbb{Z}_n)$ (là các phần tử khả nghịch trong $\mathbb{Z}_n$). Khi đó, với mọi $b \in \mathbb{Z}_n$, ta có $ba' + cb' = 0 \Leftrightarrow c'(ba' + cb') = 0 \Leftrightarrow bc'a' + b' = 0$ nên chọn $b' = -bc'a'$ là được.

Vì thế nên điều kiện cần và đủ là $a, c \in U(\mathbb{Z}_n)$ và $b \in \mathbb{Z}_n$.

b) Chứng minh $|U(M_n)| = n[\varphi(n)]^2$.

Do $a, c \in U(\mathbb{Z}_n)$ nên có $\varphi(n)$ cách chọn a, c và có n cách chọn b. Do đó, số lượng phần tử có trong $U(M_n)$ là $n[\varphi(n)]^2$.

c) Chứng minh $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}^{n[\varphi(n)]^2} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ với mọi $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \in U(M_n)$.

Ghi chú. Thực ra ở đây chỉ cần lũy thừa $n\varphi(n)$ như bài 1 là đủ.

Tiếp tục dùng công thức $\boxed{\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}^m = \begin{pmatrix} a^m & 0 \\ b \cdot \dfrac{a^m - c^m}{a - c} & c^m \end{pmatrix}}$ với mọi $m = 1, 2, 3, \ldots$

Ta có $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}^{n\varphi(n)} = \begin{pmatrix} a^{n\varphi(n)} & 0 \\ b \cdot \dfrac{a^{n\varphi(n)} - c^{n\varphi(n)}}{a - c} & c^{n\varphi(n)} \end{pmatrix}$ và $a^{n\varphi(n)} = (a^{\varphi(n)})^n = 1^n = \bar{1}$, tương tự với số c. Chú ý rằng lũy thừa của a, c trong $\mathbb{Z}_n$ tuần hoàn với chu kỳ $\varphi(n)$. Gọi T là biểu thức

$$\frac{a^{n\varphi(n)} - c^{n\varphi(n)}}{a - c} = \sum_{x+y=n\varphi(n)-1} a^x c^y = a^{n\varphi(n)-1} + a^{n\varphi(n)-2}c + \cdots + c^{n\varphi(n)-1}.$$

Bằng cách giống như bài 1, ta xét số dư của lũy thừa x, y khi chia cho $\varphi(n)$.

Nếu x chia hết cho $\varphi(n)$ thì y chia $\varphi(n)$ dư $\varphi(n) - 1$ và $a^x \cdot c^y = \bar{1} \cdot c^{\varphi(n)-1} = c^{\varphi(n)-1}$. Từ 0 đến $n\varphi(n) - 1$ có tất cả $n\varphi(n)$ số và trong đó, có đúng n số x chia hết cho $\varphi(n)$ nên tổng tất cả các số hạng như thế đều có thể viết thành $c^{\varphi(n)-1}$ trong $\mathbb{Z}_n$, thế nên tổng của chúng là $nc^{\varphi(n)-1} = \bar{0}$ trong $\mathbb{Z}_n$. Tương tự nếu x chia $\varphi(n)$ dư $1, 2, \ldots$ thì theo thứ tự y chia $\varphi(n)$ dư $\varphi(n) - 2, \ldots, 1, 0$ và các biểu thức có dạng này lần lượt được viết thành $ac^{\varphi(n)-2}, a^2c^{\varphi(n)-3}, \ldots, a^{\varphi(n)-1}$. Ngoài ra, mỗi biểu thức xuất hiện đúng n lần nên tổng của mỗi nhóm đều là $\bar{0}$. Từ đó suy ra $T = \bar{0}$.

Do đó, $b\cdot\dfrac{a^m-c^m}{a-c}=0$ và $\begin{pmatrix}a&0\\b&c\end{pmatrix}^{n\varphi(n)}=\begin{pmatrix}1&0\\0&1\end{pmatrix}$. Điều này kéo theo

$$\begin{pmatrix}a&0\\b&c\end{pmatrix}^{n[\varphi(n)]^2}=\begin{pmatrix}1&0\\0&1\end{pmatrix}^{\varphi[n]}=\begin{pmatrix}1&0\\0&1\end{pmatrix}.$$

Ghi chú. Đẳng thức trên đúng vì lũy thừa của ma trận đơn vị thì bằng chính nó.

d) Có thể thay lũy thừa $n[\varphi(n)]^2$ ở trên bằng số m nào nhỏ hơn không?

Ở câu c, ta đã chỉ ra có số $n\varphi(n)<n[\varphi(n)]^2$. Do đó, câu trả lời là khẳng định.

Ghi chú. Nếu đề đổi thành có số m nào nhỏ hơn $n\varphi(n)$ thỏa mãn không thì sẽ thành câu khó! Điều này liên quan đến việc tìm n để $\varphi(n)$ là số nguyên dương nhỏ nhất mà $\forall d\in U(\mathbb{Z}_n)$ thì $d^m=\bar{1}$. Mọi người quan tâm có thể xem thêm tại:

https://vi.wikipedia.org/wiki/C%C4%83n_nguy%C3%AAn_th%E1%BB%A7y_modulo_n

e) Chứng minh nếu $D,E\in\mathbb{Z}_{1100}$ thỏa mãn $D\cdot E=\bar{1}$ thì $(x^E)^D=x$ với mọi ma trận $x\in U(M_{11})$. Từ đó ta có thể mã hóa ma trận trong $U(M_{11})$ bằng E và giải mã bằng D.

Vì $D\cdot E=\bar{1}$ nên $DE=1100k+1$ với $k\in\mathbb{Z}$. Theo bài 2, ta đã chứng minh được

$$x^{\varphi(11)}=x^{10}=\begin{pmatrix}1&0\\0&1\end{pmatrix} \text{ với mọi } x\in U(M_{11}).$$

Do đó $x^{1100k+1}=(x^{10})^{110k}\cdot x=\begin{pmatrix}1&0\\0&1\end{pmatrix}^{110k}\cdot x=\begin{pmatrix}1&0\\0&1\end{pmatrix}\cdot x=x$. Vì thế nên khi dùng lũy thừa E, ta đã biến đổi ma trận ban đầu sang một ma trận khác (mã hóa), và sau đó lũy thừa lần nữa bằng D để đưa nó về ma trận ban đầu (giải mã).

f) Cho ví dụ về 5 khóa (E,D) để mã hóa các phần tử của $U(M_{11})$.

Ghi chú. Thực ra ở câu e, f, ta cũng chỉ cần $\mathbb{Z}_{110}$ là đủ ($110=11\cdot\varphi(11)$), không cần xét $\mathbb{Z}_{1100}$, điều này gây khó khăn khi cần chỉ ra ví dụ cho câu f vì số quá lớn.

Nếu đề vẫn giữ $\mathbb{Z}_{1100}$ thì ta có thể dùng các cặp số sau:

$$(3,367),(7,943),(9,489),(13,677),(31,71).$$

Nếu đề đổi thành $\mathbb{Z}_{110}$ thì ta có thể dùng các cặp số sau:

$$(3,37),(7,63),(9,49),(13,17),(19,29),(23,67),(27,53),(31,71),(39,79),(41,51).$$

g) Các ma trận nào trong $M_{11}\setminus U(M_{11})$ có thể mã hóa và giải mã như trên. Có bao nhiêu ma trận như vậy?

Chú ý rằng $|M_{11}| = 11^3 = 1331$, còn $|U(M_{11})| = 1100$ nên $|M_{11} \setminus U(M_{11})| = 231$.

Để thực hiện được mã hóa, giải mã như trên đối với $x \in M_{11} \setminus U(M_{11})$ thì phải có m sao cho

$$x^m = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ và } x^{m+1} = x.$$

Ta có $U(\mathbb{Z}_{11}) = 1, 2, \ldots, 10$ và ta biết $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \in U(M_{11}) \Leftrightarrow a, c \in U(\mathbb{Z}_{11}), b \in \mathbb{Z}_{11}$. Mà 11 là số nguyên tố nên $U(\mathbb{Z}_{11}) = \{\bar{1}, \bar{2}, \ldots, \overline{10}\}$. Vì thế nên ma trận trong $M_{11} \setminus U(M_{11})$ sẽ có a hoặc c là $\bar{0}$. Nhưng khi đó tính lũy thừa m lên, các số a^m, c^m không thể cùng bằng $\bar{1}$ được, vô lý.

Vậy không tồn tại ma trận thỏa mãn đề bài.

h) Thực tế có thể mã hóa $x \in U(M_{11})$ bằng sơ đồ mã hóa thu gọn hơn theo nghĩa có thể tìm được số $m < 1100$ sao cho nếu $E, D \in \mathbb{Z}_m$ và $(x^E)^D = x$. Hãy khảo sát xem có tồn tại số m như thế hay không, tìm m nhỏ nhất có thể được.

Ta sẽ chứng minh rằng $m = 10 < 1100$ là số nhỏ nhất thỏa mãn.

Trước hết, theo ghi chú ở trang 3, ta đã chứng minh được

$$\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}^{10} = \begin{pmatrix} a^{10} & 0 \\ b\dfrac{a^{10} - c^{10}}{a - c} & c^{10} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ với mọi } \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \in U(M_{11}).$$

Giả sử có số $k < 10$ thỏa mãn, nghĩa là trước hết ta phải có $a^k = c^k = \bar{1}$ trong $\mathbb{Z}_{11}$ với mọi số $a, c \in U(\mathbb{Z}_{11})$.

Xét $a = \bar{2}$, ta thấy $a^2 = \bar{4}, a^3 = \bar{8}, a^4 = \bar{5}, a^5 = \overline{10}, a^6 = \bar{9}, a^7 = \bar{7}, a^8 = \bar{3}, a^9 = \bar{6}, a^{10} = \bar{1}$ thì không có lũy thừa k nào nhỏ hơn 10 để cho $a^k = \bar{1}$. Do đó không tồn tại k như thế.

Vì thế nên $m = 10$ là số nhỏ nhất thỏa mãn đề bài.

Ghi chú. Nếu bài toán này thay 11 bởi bất kỳ số nguyên tố p nào thì kết quả sẽ là $\varphi(p) = p - 1$, còn nếu thay bởi số n không nguyên tố thì kết quả sẽ là $n\varphi(n)$.