

MATH AND SCIENCE SUMMER PROGRAM 2021

Tuyển sinh môn Toán

Câu hỏi 1

Ông già Noel muốn tặng n phần quà cho n em bé. Ông có m chú tuần lộc, với $m \geq n$. Chiếc xe của ông chỉ có thể được kéo bởi một chú tuần lộc và chỉ mang được một phần quà. Như vậy, ông sẽ phải mang từng phần quà đến cho từng em bé, sau đó lại quay về để lấy quà. Mỗi chú tuần lộc chỉ đủ sức cho một chuyến đi (cả đi lẫn quay về), nghĩa là ông phải thay một chú tuần lộc mới (chưa từng đi chuyến nào trước đó) mỗi lần quay về lấy quà. Quãng đường từ nhà ông già Noel đến nhà của n em bé lần lượt là $a_1, \dots, a_n$, với $a_1 > \dots > a_n > 0$. Vận tốc của m chú tuần lộc lần lượt là $b_1, \dots, b_m$, với $0 < b_1 < \dots < b_m$. Ông già Noel nên sắp xếp các chú tuần lộc cho n chuyến đi của mình như thế nào để xong việc nhanh nhất?

Câu hỏi 2

Trong mặt phẳng tọa độ, xét hình vuông bị giới hạn bởi các đường thẳng $\{x = 0\}$, $\{x = 1\}$, $\{y = 0\}$ và $\{y = 1\}$. Một chú bọ xấu số nằm ở một điểm bên trong hình vuông (không nằm trên cạnh). Chú bọ bắt đầu di chuyển theo một đường thẳng với hệ số góc α . Tuy nhiên, đây là một hình vuông kỳ quặc, nó tuần hoàn theo cả hai phương ngang và dọc. Nói cách khác,

1. khi chú bọ di chuyển đến điểm $(a, 1)$ thì sẽ lập tức bị dịch chuyển về điểm $(a, 0)$ (vẫn giữ nguyên hướng di chuyển lúc đầu), và ngược lại, khi di chuyển đến điểm $(a, 0)$ thì sẽ lập tức bị dịch chuyển về điểm $(a, 1)$.
2. Tương tự, khi chú bọ di chuyển đến điểm $(1, b)$ thì sẽ lập tức bị dịch chuyển về điểm $(0, b)$, và ngược lại.

Tìm điều kiện của α để chú bọ trở về vị trí ban đầu sau một khoảng thời gian nào đó (nói cách khác, quỹ đạo chuyển động là tuần hoàn).

Câu hỏi cộng điểm. Em có nhận xét gì về quỹ đạo chuyển động khi quỹ đạo chuyển động là không tuần hoàn?

Câu hỏi 3

Mục tiêu của câu hỏi này là tìm hiểu về một phương pháp mã hóa trong mật mã học. Nó gồm 12 bài tập nhỏ. Trước hết, ta gán cho mỗi chữ cái trong bảng chữ cái tiếng Anh một con số từ 0 đến 25 theo đúng thứ tự. Vậy

$$\begin{aligned} A \mapsto 0, \quad B \mapsto 1, \quad C \mapsto 2, \quad D \mapsto 3, \quad E \mapsto 4, \quad F \mapsto 5, \quad G \mapsto 6, \quad H \mapsto 7, \quad I \mapsto 8, \quad J \mapsto 9, \\ K \mapsto 10, \quad L \mapsto 11, \quad M \mapsto 12, \quad N \mapsto 13, \quad O \mapsto 14, \quad P \mapsto 15, \quad Q \mapsto 16, \quad R \mapsto 17, \\ S \mapsto 18, \quad T \mapsto 19, \quad U \mapsto 20, \quad V \mapsto 21, \quad W \mapsto 22, \quad X \mapsto 23, \quad Y \mapsto 24, \quad Z \mapsto 25. \end{aligned}$$

Để mã hóa một văn bản cho trước, ta thực hiện như sau: Chia văn bản thành các khối nhỏ, mỗi khối gồm 2 chữ cái liên tiếp (bỏ qua dấu cách). Nếu số chữ cái là lẻ thì ta thêm một ký tự tùy ý vào cuối văn bản (chẳng hạn là A). Với mỗi khối văn bản thu được, ta sẽ mã hóa nó thành một khối văn bản mới, vẫn gồm 2 chữ cái, theo quy tắc như sau. Gọi $x, y \in \{0, 1, \dots, 25\}$ lần lượt là con số ứng với hai ký tự cần mã hóa. Hai ký tự sau khi mã hóa sẽ lần lượt ứng với các con số $X, Y \in \{0, 1, \dots, 25\}$ được cho bởi quy tắc như sau

$$\begin{cases} X &= 3x + 2y \pmod{26} \\ Y &= 4x + y \pmod{26} \end{cases}$$

(ta làm phép nhân và cộng như bình thường, rồi lấy số dư khi chia cho 26).
Chẳng hạn, văn bản gốc I LOVE YOU sẽ được mã hóa theo các bước như sau.

1. Tách thành 4 khối IL, OV, EY và OU.
2. Chuyển từng khối trên thành các cặp số $(8, 11)$, $(14, 21)$, $(4, 24)$ và $(14, 20)$.

3. Mã hóa các cặp số trên theo quy tắc đã cho

$$\begin{cases} 3 \cdot 8 + 2 \cdot 11 = 20 \pmod{26} \\ 4 \cdot 8 + 11 = 17 \pmod{26}, \end{cases} \quad \begin{cases} 3 \cdot 14 + 2 \cdot 21 = 6 \pmod{26} \\ 4 \cdot 14 + 21 = 25 \pmod{26}, \end{cases}$$

$$\begin{cases} 3 \cdot 4 + 2 \cdot 24 = 8 \pmod{26} \\ 4 \cdot 4 + 24 = 14 \pmod{26}, \end{cases} \quad \begin{cases} 3 \cdot 14 + 2 \cdot 20 = 4 \pmod{26} \\ 4 \cdot 14 + 20 = 24 \pmod{26}. \end{cases}$$

Ta thu được các cặp số $(20, 17)$, $(6, 25)$, $(8, 14)$ và $(4, 24)$.

4. Chuyển từng cặp khối trên thành các khối chữ cái UR, GZ, IO và EY.

5. Ghép các khối chữ cái đã mã hóa lại, ta thu được văn bản mã hóa URGZIOEY.

Bài 1. Giải mã văn bản mã hóa sau, biết rằng nó được mã hóa theo quy tắc nêu trên

KWTFANTEWQMDOM

(hãy giải thích cách giải mã ít nhất 6 chữ cái đầu tiên).

Bây giờ ta xét quy tắc mã hóa tổng quát. Cho trước các số $a, b, c, d \in \{0, 1, \dots, 25\}$ thỏa mãn điều kiện sau.

$$ad - bc \text{ là một số lẻ và không chia hết cho } 13. \quad (1)$$

Một cặp số (x, y) (đại diện cho một khối 2 chữ cái) sẽ được mã hóa thành cặp số (X, Y) theo quy tắc

$$\begin{cases} X = ax + by \pmod{26} \\ Y = cx + dy \pmod{26}. \end{cases} \quad (2)$$

Chẳng hạn, ở ví dụ ở đầu bài, ta có $a = 3$, $b = 2$, $c = 4$ và $d = 1$. Ta gọi bảng vuông sau đây

$$K = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

là *khóa* của quy tắc mã hóa (2). Ta viết lại (2) ở dạng gọn hơn như sau

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} X \\ Y \end{bmatrix} \quad \text{hay} \quad K \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} X \\ Y \end{bmatrix}.$$

Chẳng hạn, như trong ví dụ ở đầu bài

$$\begin{bmatrix} 3 & 2 \\ 4 & 1 \end{bmatrix} \begin{bmatrix} 8 \\ 11 \end{bmatrix} = \begin{bmatrix} 20 \\ 17 \end{bmatrix}, \quad \begin{bmatrix} 3 & 2 \\ 4 & 1 \end{bmatrix} \begin{bmatrix} 14 \\ 21 \end{bmatrix} = \begin{bmatrix} 6 \\ 25 \end{bmatrix}, \quad \begin{bmatrix} 3 & 2 \\ 4 & 1 \end{bmatrix} \begin{bmatrix} 4 \\ 24 \end{bmatrix} = \begin{bmatrix} 8 \\ 14 \end{bmatrix}, \quad \begin{bmatrix} 3 & 2 \\ 4 & 1 \end{bmatrix} \begin{bmatrix} 14 \\ 20 \end{bmatrix} = \begin{bmatrix} 4 \\ 24 \end{bmatrix}.$$

Bài 2. Giải thích điều kiện (1). *Gợi ý: Một quy tắc mã hóa chỉ có ý nghĩa khi ta có thể giải mã mọi văn bản một cách duy nhất. Nói một cách toán học, một quy tắc mã hóa là một ánh xạ*

$$\{0, 1, \dots, 25\} \times \{0, 1, \dots, 25\} \rightarrow \{0, 1, \dots, 25\} \times \{0, 1, \dots, 25\},$$

và ta yêu cầu rằng ánh xạ này phải là song ánh.

Bài 3. Nếu tổng số chữ cái không phải là 26 mà là n , ta điều chỉnh lại các quy tắc ở trên một cách thích hợp. Khi đó điều kiện (1) sẽ là gì?

Bài 4. Ở bài này, ta thừa nhận khẳng định sau: Tồn tại duy nhất khóa $K' = \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix}$ (đương nhiên, K' là một

khóa nên nó phải thỏa mãn điều kiện (1) khi thay a, b, c, d lần lượt bởi a', b', c', d') sao cho quy tắc mã hóa tương ứng chính là quy tắc giải mã ứng với khóa K , nói cách khác là

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} X \\ Y \end{bmatrix} \iff \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} \begin{bmatrix} X \\ Y \end{bmatrix} = \begin{bmatrix} x \\ y \end{bmatrix}$$

Ta gọi khóa K' là *khóa ngược* của khóa K . Tìm khóa ngược của khóa $\begin{bmatrix} 3 & 2 \\ 4 & 1 \end{bmatrix}$ ở đầu bài.

Bài 5. Chứng minh khẳng định đã thừa nhận ở Bài 4, và tìm công thức cho các số a', b', c', d' trong khóa K' theo a, b, c, d . *Chú ý: Điều kiện (1) sẽ đóng một vai trò then chốt.*

Phá mã là thao tác tìm khóa K ban đầu (từ đó, ta có thể dễ dàng tìm được khóa ngược K' theo **Bài 4**, và giải mã tất cả văn bản đã mã hóa theo quy tắc này).

Bài 6. Giả sử ta có một chiếc máy mã hóa (khi nhập vào một văn bản, máy cho ra văn bản đã mã hóa) và ta biết rằng nó hoạt động theo quy tắc (2), nhưng ta không biết khóa K của nó. Hãy đề xuất cách phá mã bằng cách nhập 4 chữ cái vào máy.

Bài 7. Tại sao ta không thể phá mã bằng ít hơn 4 chữ cái?

Bài 8. Có tất cả bao nhiêu khóa?

Bài 9. *Khóa tầm thường* là khóa I mà quy tắc mã hóa tương ứng là "giữ nguyên tất cả chữ cái". Tìm khóa tầm thường I .

Bài 10. Ta xét khóa R mà quy tắc tương ứng của nó là "đổi chỗ hai chữ cái trong mỗi khối". Tìm khóa R .

Bài 11. Chỉ ra rằng mọi khóa đều giữ nguyên khối **AA** (nghĩa là khi mã hóa khối này bằng mọi khóa thì đều thu được chính nó).

Bài 12. Chứng minh rằng nếu một khóa $K = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ giữ nguyên ít nhất hai khối (trong tổng cộng 26×26 khối hai chữ cái) thì a và d cùng tính chẵn lẻ, hoặc $1 - (a + d) + ad - bc$ chia hết cho 13.

Câu hỏi cộng điểm. Xét quy tắc mã hóa tương tự như trên, nhưng ta tách thành khối 3 chữ cái thay vì khối 2 chữ cái. Hãy cố gắng làm lại các bài tập từ 2 đến 12 (càng nhiều bài tập càng tốt). *Từ khóa: Định thức, quy tắc Sarrus.*