3) Para añadir redundancia a una información dada por un vector fila $\vec{v} \in \mathbb{Z}_3 \times \mathbb{Z}_3$, lo codificamos como $c(\vec{v}) = [\vec{v}, \vec{v}A, \vec{v}A^2, \ldots, \vec{v}A^k]$ módulo 3, donde $A \in \mathcal{M}_{2\times 2}(\mathbb{Z})$ con $\det(A) = 1$ y k se escoge de forma que $\vec{v}A^{k+1} = \vec{v}$. ¿Cuántas coordenadas puede tener como máximo el resultado?

Ejemplo:

$$\vec{v} = (1,0), \quad A = \begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix} \quad \Rightarrow \quad c(\vec{v}) = [1,0,2,2,0,1]$$

porque $(0,1)A = \vec{v}$. Entonces el máximo es mayor o igual que 6.

El tercer problema del primer parcial era difícil y nadie lo ha sacado por completo. Equivalía a hallar el máximo orden de una matriz A en $\mathcal{M}_{2\times 2}(\mathbb{Z}_3)$ con determinante 1. Si N es el orden máximo, $A^N = I$, la solución es $2N$. Por explicar esto, que es casi inmediato, sólo daba 1 punto de 9, en un par de casos excepcionales algo más.

A continuación doy varias demostraciones con diferentes niveles de dificultad. Todos deberían entender alguna de ellas. Claramente hay una gran diferencia entre seguirlas y crearlas. Como avisé en el examen, a mi juicio este problema era más difícil que el resto. Los resultados han probado que lo era más de lo que suponía.

1. Con álgebra lineal un poco avanzada. [Más bien difícil pero asequible]

El polinomio característico de A (en $\mathbb{Z}_3$) puede ser[1] $\lambda^2 + 1$ ó $\lambda^2 \pm \lambda + 1 = (\lambda \mp 1)^2$. En el primer caso se tiene[2] $A^2 + I = O$ y por tanto el orden es 4. En el segundo caso, los autovalores son iguales, ± 1. Tras escribir la forma canónica de Jordan[3], sólo hay que considerar los casos:

$$I, \qquad -I, \qquad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad \text{y} \qquad \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}$$

que tienen órdenes 1, 2, 3 y 6, respectivamente.

2. Combinatoria (casos) y muy poca álgebra lineal. [Medio fácil pero trabajosa]

Como $\det(A) = 1$, si fuera diagonal, $A = \pm I$ que da órdenes 1 y 2. En otro caso, empleando que las matrices

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \qquad A^t = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \qquad \text{y} \qquad A^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

tienen el mismo orden, es fácil ver que podemos suponer $b = 1$ (p.ej., si fuera -1, aplicaríamos la inversa). Si $b = 1$ entonces $c = ad - 1$. Dando todos los valores $a, d \in \mathbb{Z}_3$ se obtiene que basta con que estudiemos el orden de

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

[1] El último coeficiente es el determinante.

[2] La matriz siempre resuelve su polinomio característico. Aparte de que esto sea un teorema que se ve en primero (Cayley-Hamilton), pensándolo después de diagonalizar, es muy creíble.

[3] Es muy fácil ver que A y $P^{-1}AP$ tienen el mismo orden, incluso si uno no lo recuerda de Estructuras Algebraicas.

y de

$$\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix},\quad \begin{pmatrix}-1 & 1\\ -1 & 0\end{pmatrix},\quad \begin{pmatrix}-1 & 1\\ 1 & 1\end{pmatrix},\quad \begin{pmatrix}-1 & 1\\ 0 & -1\end{pmatrix},$$

lo cual es un rollo pero factible en un tiempo razonable si uno ha terminado rápido los otros problemas.

3. Combinatoria (casos) y más álgebra lineal. [Más ingeniosa y mucho menos trabajosa]

Como dijimos en la prueba anterior, el caso con A diagonal es muy fácil. También lo es si la diagonal secundaria es nula ($c = d = 0$, una matriz, salvo el signo, de orden 4). Con ello, quizá invirtiendo o trasponiendo (como en la prueba anterior) se puede suponer $a, b \neq 0$. Además

$$A = \begin{pmatrix}a & b\\ c & d\end{pmatrix}, \qquad \text{y} \qquad \begin{pmatrix}a & -b\\ -c & d\end{pmatrix} = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}^{-1} (A^{-1})^t \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$$

tienen el mismo orden (ver la última nota a pie de página). Así pues podemos suponer $a = b \neq 0$. Si $a = b = 1$ se tienen

$$\begin{pmatrix}1 & 1\\ -1 & 0\end{pmatrix}, \qquad \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix} \qquad \text{y} \qquad \begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix},$$

con órdenes 6, 3 y 4. Si $a = b = -1$ saldrán las negativas de estas matrices y como cambiar de signo conmuta con la multiplicación de matrices, $(-A)B = -(AB)$, y tiene orden 2, entonces las otras matrices tendrán órdenes que no superan 6.

4. Con álgebra avanzada. [Difícil, requiere teoría de Galois, pero generalizable]

Si el polinomio característico no es irreducible en $\mathbb{Z}_3[x]$ sus raíces son iguales (porque el determinante es 1), lo que da los casos, como en la primera prueba,

$$I, \qquad -I, \qquad \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix} \qquad \text{y} \qquad \begin{pmatrix}-1 & 1\\ 0 & -1\end{pmatrix}$$

de órdenes 1, 2, 3 y 6. Si fuera irreducible, su cuerpo raíz es $\mathbb{F}_9$ y A tendrá sus autovalores allí, digamos $\lambda_1 = \alpha$, $\lambda_2 = \alpha^{-1}$ y será diagonalizable en $\mathbb{F}_9$ (raíces distintas). Además $\lambda_1 = \lambda_2^3$ (por el automorfismo de Frobenius), entonces $\alpha^4 = 1$ y el orden es a lo más 4 en este caso.