




## Temas de Álgebra

prova de avaliação


4 de janeiro de 2023

1.  Factorize, usando o método de Lenstra, o número  $n = 63109$ , usando a curva elíptica  $E : y^2 = x^3 + 618x + 19471$  sobre  $\mathbb{Z}_n$ , e  $P = (60863 : 27581 : 1) \in E$ .
2.  Alice e Bob acordaram na curva elíptica  $E$  definida por  $y^2 = x^3 + 47356x + 58368$  sobre  $\mathbb{Z}_{92627}$  e em  $P = (4274 : 62891 : 1) \in E$ . Irão usar o protocolo de Massey-Omura. Explique como pode Alice enviar a mensagem  $(63813 : 3598 : 1)$  a Bob. Determine o texto cifrado e descreva todos os passos que seguiu.
3.  Considere a curva elíptica  $E : y^2 = x^3 + 1164x + 4366$  sobre  $\mathbb{Z}_{6151}$ . Para  $P = (497 : 4447 : 1) \in E$ ,
  - (a) mostre que  $E = \langle P \rangle$  (ou seja, que  $E$  é grupo cíclico e que  $P$  é gerador de  $E$ );
  - (b) para  $(k, a) = (4917, 1933)$ , use o sistema Menezes-Vanstone para cifrar  $\text{mens} = (213, 981)$ ;
  - (c) conhecendo a chave privada, decifre o que obteve na alínea anterior.
4. Calcule, usando (pelo menos uma vez) a Lei da Reciprocidade Quadrática,  $\left(\frac{761067}{1000033}\right)$ .

\*\*\*

5.  Usando reflexões elementares, obtenha a fatorização QR de  $A$ , com

$$A = \begin{bmatrix} 0.8147 & 0.0975 & 0.1576 \\ 0.9058 & 0.2785 & 0.9706 \\ 0.1270 & 0.5469 & 0.9572 \\ 0.9134 & 0.9575 & 0.4854 \\ 0.6324 & 0.9649 & 0.8003 \end{bmatrix}.$$

6.  Usando rotações de Givens, obtenha a fatorização QR de  $\begin{bmatrix} 3 & 1 & 0 \\ 0 & 2 & 0 \\ 4 & 0 & 5 \end{bmatrix}$ .
7. A norma de Frobenius de uma matriz  $X$  está definida como  $\|X\|_F = \sqrt{\text{tr}(X^*X)}$ , onde  $\text{tr}(\cdot)$  denota o traço (ou seja, a soma dos elementos diagonais).
  - (a) Mostre que  $\|X\|_F = 0 \Leftrightarrow X = 0$ .
  - (b) Dada a fatorização QR de  $A = QR$ , mostre que  $\|A\|_F = \|R\|_F$ .
8. Dado um subespaço  $W$  de um espaço vetorial  $V$  de dimensão finita, mostre que  $(W^\perp)^\perp = W$ .

Fim