





Temas de Álgebra

exame

8 de fevereiro de 2023

1.  Factorize, usando o método de Lenstra, o número $n = 2059$, usando a curva elíptica $E : y^2 = x^3 + 1464x + 747$ sobre \mathbb{Z}_n , e $P = (1000 : 1738 : 1) \in E$.
 2.  Considere a curva elíptica $E : y^2 = x^3 + 2585x + 9201$ sobre \mathbb{Z}_{209887} . Para $P = (36630 : 104122 : 1) \in E$,
 - (a) mostre que $E = \langle P \rangle$ (ou seja, que E é grupo cíclico e que P é gerador de E);
 - (b) para $(k, a) = (1758, 1728)$, use o sistema Menezes-Vanstone para cifrar $\text{mens} = (314, 159)$;
 - (c) conhecendo a chave privada, decifre o que obteve na alínea anterior.
 3. Calcule, usando (pelo menos uma vez) a Lei da Reciprocidade Quadrática, $\left(\frac{12345}{543211} \right)$.
 4. Seja p um primo tal que $p \equiv 3 \pmod{4}$, e suponha que $x^2 \equiv y \pmod{p}$.
 - (a) Mostre que $(y^{\frac{p+1}{2}})^2 \equiv y^2 \pmod{p}$.
 - (b) Mostre que $y^{\frac{p+1}{2}} \equiv \pm y \pmod{p}$.
 - (c) Mostre que $(x^{\frac{p+1}{4}})^2 \equiv x \pmod{p}$.
 - (d) Mostre que -1 é um não resíduo quadrático módulo p .
 - (e) Supondo que z é um não resíduo quadrático módulo p , mostre que $-z$ é um resíduo quadrático módulo p .
 - (f) Mostre que $z^{\frac{p+1}{4}}$ é uma raiz quadrada de $-z$ módulo p .
- ***
5.  Usando transformações de Householder ou rotações de Givens, obtenha a factorização QR de A , com $A = \begin{bmatrix} 6 & 5 & 0 \\ 5 & 1 & 4 \\ 0 & 4 & 3 \end{bmatrix}$.
 6.  Sejam \mathcal{X} e \mathcal{Y} subespaços de \mathbb{R}^3 com bases $B_{\mathcal{X}} = \{(1, 0, 1), (0, 1, 2)\}$ e $B_{\mathcal{Y}} = \{(0, 1, 1)\}$.
 - (a) Mostre que \mathcal{X} e \mathcal{Y} são complementares.
 - (b) Calcule o projector P sobre \mathcal{X} ao longo de \mathcal{Y} , assim como o seu projector complementar Q .
 - (c) Determine a projecção de $v = (1, 1, 1)$ sobre \mathcal{Y} ao longo de \mathcal{X} .

Fim