Universidade do Minho
Departamento de Matemática — Mestrado em Matemática e Computação

Temas de Álgebra

prova de avaliação — 21 de janeiro de 2022

A duração da prova é de duas horas e trinta minutos.

1. Considere a curva elíptica E definida por $y^2 = x^3 + 3084x + 109841$ sobre $\mathbb{Z}_{191123}$ e $P = ((123483 : 23340 : 1)) \in E$. Considere a chave pública Elgamal (E, P, Q) com $Q = rP = (130256 : 107534 : 1)$, para algum r. Cifre a mensagem `mens=112` (não se esqueça que em primeiro lugar tem que converter mens num ponto da curva elíptica P em E).

2. Considere o primo $p = 874537$. Defina uma curva elíptica E sobre os inteiros módulo p. Usando parâmetros à sua escolha, use o sistema Menezes-Vanstone para cifrar `mens=(501, 1112)` na curva elíptica E. Conhecendo a chave privada, decifre o que cifrou.

3. Factorize, usando o método de Lenstra, o número $n = 28321$, usando a curva elíptica $E : y^2 = x^3 + 17622x + 10185$ sobre $\mathbb{Z}_n$, e $P = (18640 : 5420 : 1) \in E$, tomando o parâmetro $B = 100$.

4. Seja $n \geq 3$ um natural ímpar com k factores primos $p_1, \ldots, p_k$ distintos e tal que $n = \prod_i p_i$. Mostre que existem, módulo n, exactamente 2^k raizes quadradas de 1.

***

5. Usando transformações de Householder ou rotações de Givens, construa uma base ortonormada do espaço das colunas de A, com $A = \begin{bmatrix} 4 & -3 & 4 \\ 2 & -14 & -3 \\ -2 & 14 & 0 \\ 1 & -7 & 15 \end{bmatrix}$.

6. Sejam $\mathcal{X}$ e $\mathcal{Y}$ subespaços de $\mathbb{R}^3$ com bases $B_{\mathcal{X}} = \{(1,1,1), (1,2,2)\}$ e $B_{\mathcal{Y}} = \{(1,2,3)\}$.
   (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 $v = (2, -1, 1)$ sobre $\mathcal{Y}$ ao longo de $\mathcal{X}$.

Fim