

<div>P.PORTO</div> <div>ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO</div>	Tipo de Prova Exame de Época de Recurso	Ano letivo 2016/2017	Data 06-07-2017
	Curso Licenciatura em Segurança Informática de Redes de Computadores	Hora 10:00	
	Unidade Curricular Matemática Discreta	Duração 2,5 horas	

N.º de aluno: _____ Nome: _____

Questão	1	2	3	4	5	6	7	8	9	10	11	TOTAL
Cotação	1,0+1,0+1,0	1,5	1,0+1,0	0,8+1,5	1,2	1,2	1,6	1,5	0,8+1,2	1,2+1,0	1,5	20

1. Considere o conjunto $Y = \{\emptyset, a, \{a\}, b\}$, com $a, b \in \mathbb{N}$.

a) Determine $\# Y$, $\mathcal{P}(Y)$ e $\#\mathcal{P}(\mathcal{P}(Y))$.

b) Diga, justificando, se cada uma das seguintes afirmações é verdadeira ou falsa:

$$\emptyset \in \mathcal{P}(Y) \quad \{\emptyset, a\} \subseteq \mathcal{P}(Y) \quad \mathcal{P}(Y) \subseteq \mathcal{P}(\mathcal{P}(Y)) \quad \{\{\emptyset, b\}\} \in \mathcal{P}(Y)$$

c) Dê um exemplo de uma função $f: \{a, b\} \rightarrow \mathcal{P}(Y)$, que seja injetiva não sobrejetiva.

2. Considere o conjunto universo $U = \{x \in \mathbb{Z}_0^+: 10x < 31\}$ e os seus subconjuntos

$$A = \{x \in U: x^3 \leq 10\}, B = \{x \in U: x \text{ é divisor de } 3\} \text{ e } C = \{x: x \text{ é primo e } x \text{ divide } 2\}.$$

Determine $C \times \overline{A \cap B}$ e $(A \cup B) \oplus C$.

3. Considere as seguintes relações binárias definidas sobre $\{a, b, c\}$:

$$R = \{(a, a), (b, b), (c, c), (c, a), (a, c)\} \text{ e } S = \{(a, a), (c, c), (a, c), (b, c)\} \text{ e}$$

a) Determine, caso seja possível $(R \cap S) \circ S^{-1}$ e transitivo(S).

b) Verifique, justificando, quais das relações, R ou S , é de equivalência e indique a classe de equivalência do elemento c .

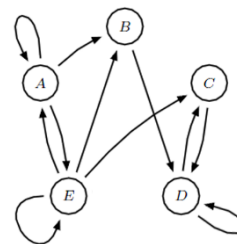
4. Relativamente ao grafo apresentado ao lado:

a) Classifique-o, indique o conjunto dos vértices e das arestas, assim como sua ordem e dimensão;

b) Determine a matriz de adjacências e, com base nesta matriz, determine:

i) o grau de cada vértice

ii) o número de caminhos de comprimento sete de D para A e, casos existam, indique dois desses caminhos.




5. Defina o *Traveling Salesman Problem* (TSP) e apresente um exemplo de aplicação.

6. Dê, justificando, um exemplo de um grafo com mais de 5 vértices que seja Semi-Euleriano e não Euleriano.

7. Usando o Algoritmo de Euclides, determine $\text{mdc}(224, 43)$, indique, justificando os coeficientes de Bézout e com base nestes indique, se possível, o inverso de $43 \bmod 224$.

8. Escreva a sequência de números pseudoaleatórios gerada por $x_{n+1} = (23x_n + 1) \bmod 11$, com raiz $x_0 = 5$.

 <small>ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO</small>	Tipo de Prova Exame de Época de Recurso	Ano letivo 2016/2017	Data 06-07-2017
	Curso Licenciatura em Segurança Informática de Redes de Computadores	Hora 10:00	
	Unidade Curricular Matemática Discreta	Duração 2,5 horas	

N.º de aluno: _____ Nome: _____

9. Considere a função encriptadora $f(n) = (7n + 1) \bmod 26$ e $A \leftrightarrow 0, \dots, Z \leftrightarrow 25$.

- Encripte a mensagem "S".
- Escreva a função de descriptação e descripte a mensagem "AH".

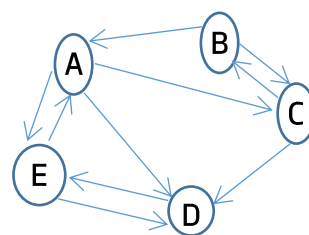
10. Considere o sistema RSA com $n = 43 \times 59 = 2537$ e $a = 13$.

- Encripte a mensagem "AS".
- Determine a chave privada.

11. Considere rede constituída por 5 páginas web A, B, C, D, E com os links mostrados na imagem ao lado.

Suponha que, em cada passo, escolhemos de forma aleatória um link da página web onde estamos.

Escreva a matriz de transição do processo Markov subjacente e calcule a probabilidade, de começando na página D, dez passos depois estar de volta à página D.



Bom Trabalho
Elia Costa e Silva