 <div> <div>ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO</div> </div>	Tipo de Prova Teste 2	Ano letivo 2021/2022	Data 13-06-2022
	Curso LSIRC+LEI	Hora 14:00	
	Unidade Curricular Matemática Discreta	Duração 1,5 horas + 15 min	

Nome: \_\_\_\_\_ Número: \_\_\_\_\_

#### Observações:

A avaliação desta Unidade Curricular, na modalidade de avaliação durante o período letivo, contempla os três elementos e respetivas ponderações: 35% Teste 1 + 35% Teste 2 + 30% Trabalho Prático.

Para a realização desta prova pode usar um formulário manuscrito e criado pelo próprio, com até **uma página A4** (ou 2 páginas A5).

**Responda às questões neste enunciado.**

Nas **questões 1 a 6 não apresente justificações. Nas restantes apresente todas as justificações.**


As cotações de cada questão estão identificadas entre parêntesis [ ].

No final da prova, **têm de ser entregues** o enunciado, as folhas de resposta e de rascunho, assim como o formulário, **TODOS devidamente identificados** com o nome e número de estudante.

Bom trabalho!

Eliana Costa e Silva e Isabel Cristina Duarte

#### Responda às questões 1 a 6 sem apresentar justificações.

1. [1.0] Considere o fragmento de código  onde são definidas as matrizes de adjacência M1 e M2 de dois grafos de vértices {a,b,c,d,e,f} e {A,B,C,D}, respetivamente. Com base no output, responda às questões seguintes.

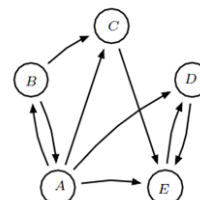
Podemos afirmar que:

- |  |   |
|--|---|
| <input type="checkbox"/> os dois grafos são de Hamilton  | <input type="checkbox"/> apenas o grafo de vértices {a,b,c,d,e,f} é de Hamilton |
| <input type="checkbox"/> nenhum dos grafos é de Hamilton | <input type="checkbox"/> apenas o grafo de vértices {A,B,C,D} é de Hamilton     |


--> M1=[1 0 0 1 0 1; > 1 0 0 0 0 0; > 1 1 0 0 0 1; > 0 0 1 0 1 0; > 0 0 1 0 0 1; > 1 1 0 1 1 0];	--> M2=[1 0 2 1; > 0 0 1 0; > 2 1 1 0; > 1 0 0 1];
---	---

2. [1.0] Relativamente ao grafo apresentado ao lado, A, B, C, E, D, A:

- |  |   |
|--|---|
| <input type="checkbox"/> é um circuito de Hamilton | <input type="checkbox"/> é um caminho de Hamilton |
| <input type="checkbox"/> não é caminho             | <input type="checkbox"/> nenhuma das anteriores   |



3. [1.0] O produto de dois números é 12 e o seu máximo divisor comum é 2, então o seu mínimo múltiplo comum é: ☐ 2 ☐ 4 ☐ 6 ☐ 12

4. Com base no fragmento de código  abaixo, podemos afirmar que:

```
--> factor(55), factor(150), factor(539), factor(1287)
ans =
  5. 11.
ans =
  2. 3. 5. 5.
ans =
  7. 7. 11.
ans =
  3. 3. 11. 13.
```

4.1 [1.0] mdc(150, 1287) é:

- |                            |                            |                             |   |
|----------------------------|----------------------------|-----------------------------|---|
| <input type="checkbox"/> 3 | <input type="checkbox"/> 5 | <input type="checkbox"/> 11 | <input type="checkbox"/> nenhuma das anteriores |
|----------------------------|----------------------------|-----------------------------|---|

4.2 [1.0] não são primos entre si:

- |  |   |  |                                    |
|--|---|--|------------------------------------|
| <input type="checkbox"/> 55, 150 e 539 | <input type="checkbox"/> 55, 539 e 1287 | <input type="checkbox"/> 150, 539 e 1287 | <input type="checkbox"/> 150 e 539 |
|--|---|--|------------------------------------|

4.3 [1.0] existe o inverso de 539 modulo:

- |                             |                              |                               |   |
|-----------------------------|------------------------------|-------------------------------|---|
| <input type="checkbox"/> 55 | <input type="checkbox"/> 150 | <input type="checkbox"/> 1287 | <input type="checkbox"/> nenhuma das anteriores |
|-----------------------------|------------------------------|-------------------------------|---|

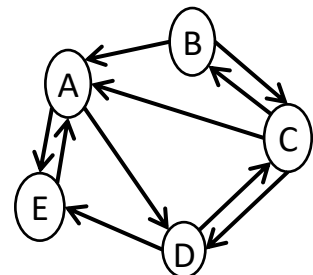
<div>P.PORTO</div> <div>ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO</div>	Tipo de Prova Teste 2	Ano letivo 2021/2022	Data 13-06-2022
	Curso LSIRC+LEI	Hora 15:00	
	Unidade Curricular Matemática Discreta	Duração 1,5 horas+15 min	

5. [1.0] Um inverso de 3 modulo 7 é:

☐ 2      ☐ 3      ☐ 4      ☐ 5

6. Considere a rede constituída por cinco páginas web A, B, C, D e E com os links mostrados na imagem apresentada na figura ao lado.

6.1. [1.0] Considere que, em cada passo, escolhemos de forma aleatória um link da página web onde estamos. A matriz de transição (definida no Scilab) do processo Markov subjacente é:



☐

T =

```

0.    0.5    0.3333333    0.    1.
0.    0.    0.3333333    0.    0.
0.    0.5    0.    0.5    0.
0.5    0.    0.3333333    0.    0.
0.5    0.    0.    0.5    0.

```

☐

T =

```

0.    0.    0.    0.5    0.5
0.5    0.    0.    0.5    0.
0.3333333    0.3333333    0.    0.3333333    0.
0.    0.    0.5    0.    0.5
1.    0.    0.    0.    0.

```

☐

T =

```

0.41    0.59    0.39    0.73    0.54
0.88    0.69    0.92    0.26    0.12
0.11    0.89    0.95    0.5    0.23
0.2    0.5    0.34    0.26    0.63
0.56    0.35    0.38    0.53    0.76

```

☐

T =

```

0.    0.5    0.33    0.    1.
0.    0.    0.33    0.    0.
0.    0.5    0.    0.5    0.
0.5    0.    0.33    0.    0.
0.5    0.    0.    0.5    0.

```

6.2. [1.0] Considere os cálculos apresentados no fragmento de código Scilab apresentado abaixo, sendo T a matriz de transição definida na alínea 6.1 .

```

--> T^6
ans =

0.2916667    0.3935185    0.3217593    0.337963    0.4027778
0.0277778    0.0601852    0.0462963    0.025463    0.0694444
0.1423611    0.1111111    0.1134259    0.1736111    0.0833333
0.2291667    0.1956019    0.2384259    0.1712963    0.2152778
0.3090278    0.2395833    0.2800926    0.2916667    0.2291667

```

<pre> --&gt; T^6*[0 1 0 0 0]' ans =  0.3935185 0.0601852 0.1111111 0.1956019 0.2395833 </pre>	<pre> --&gt; T^6*[0 0 0 0 1]' ans =  0.4027778 0.0694444 0.0833333 0.2152778 0.2291667 </pre>	<pre> --&gt; T^6*[1 0 0 0 0]' ans =  0.2916667 0.0277778 0.1423611 0.2291667 0.3090278 </pre>
---	---	---

A probabilidade, de começando na página B, seis passos depois estar na página D é aproximadamente:

☐ 0,2      ☐ 0,4      ☐ 0,03      ☐ 0,3

<div>P.PORTO</div> <div>ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO</div>	Tipo de Prova Teste 2	Ano letivo 2021/2022	Data 13-06-2022
	Curso LSIRC+LEI	Hora 14:00	
	Unidade Curricular Matemática Discreta	Duração 1,5 horas + 15 min	

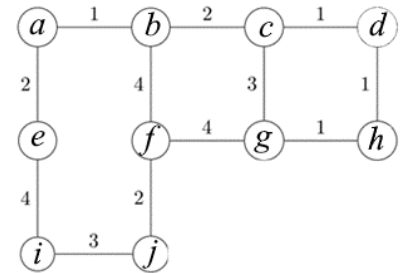
Nome: \_\_\_\_\_ Número: \_\_\_\_\_

Nas questões que seguem apresente todas as justificações.

7. Considere o grafo ponderado apresentado ao lado.


7.1 [1.5] Use o algoritmo de *Dijkstra* para encontrar o caminho de menor custo entre  $a$  e  $f$ .

Observação: Apresente a sua resolução na tabela abaixo.



It.	$v_d$ (M)	Mc	A	$v_i, \dots, v_d, v_j$ e $L(v_j)$	X e $X_d$	R: Caminhos mínimos




 <small>ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO</small>	Tipo de Prova Teste 2	Ano letivo 2021/2022	Data 13-06-2022
	Curso LSIRC+LEI	Hora 14:00	
	Unidade Curricular Matemática Discreta	Duração 1,5 horas + 15 min	

**Nome:** \_\_\_\_\_ **Número:** \_\_\_\_\_

**8 [1.5]** Determine, recorrendo ao Algoritmo de Euclides, os inteiros  $s$  e  $t$  (coeficientes de Bézout) tais que  $\text{mdc}(234,48) = 234 \times s + 48 \times t$ , e se possível, indique o inverso de  $48 \bmod 234$ .

**9 [1.5]** Resolva, se possível, a congruência  $9x \equiv 3 \bmod 11$ .

**10 [1.5]** Escreva a sequência de números pseudo-aleatórios gerada por  $x_{n+1} = (5x_n + 7) \bmod 11$  com raiz  $x_0 = 7$ .

 <small>ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO</small>	Tipo de Prova Teste 2	Ano letivo 2021/2022	Data 13-06-2022
	Curso LSIRC+LEI	Hora 15:00	
	Unidade Curricular Matemática Discreta	Duração 1,5 horas+15 min	


**11** Considere a função de encriptação  $f(n) = (10n + 1) \bmod 29$  e ainda as correspondências seguintes:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	_	#	@
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28

**11.1 [1.0]** Encripte a mensagem “HASH”.

**11.2 [1.0]** Escreva a função de desencriptação  $f^{-1}$ , sabendo que 3 é o inverso de 10 módulo 29.

**12** Considere o sistema RSA com  $a = 13$  e  $m = 43 \times 59 = 2537$ .

Responda às seguintes questões usando os outputs do  que considerar necessários.

**12.1 [0.75]** Encripte a mensagem “CS”.

**12.1[0.75]** Sendo  $b = 937$  a chave privada, desencripte a mensagem “1005”.

<pre>--&gt; pmodulo(218,2537) ans =     218.  --&gt; pmodulo(218^13,2537) ans =      0.</pre>	<pre>--&gt; x=13 x =     13.  --&gt; x_new=1; --&gt; for k=1:218,     &gt; x_new=pmodulo(x*x_new,2537);     &gt; end --&gt; x_new x_new =     1672.</pre>
<pre>--&gt; x=218 x =     218.  --&gt; x_new=1; --&gt; for k=1:13,     &gt; x_new=pmodulo(x*x_new,2537);     &gt; end --&gt; x_new x_new =     1259.</pre>	<pre>--&gt; x=1005; --&gt; x_new=1; --&gt; for k=1:2537,     &gt; x_new=pmodulo(x*x_new,937);     &gt; end --&gt; x_new x_new =     225.</pre>
<pre>--&gt; x=1005; --&gt; x_new=1; --&gt; for k=1:13,     &gt; x_new=pmodulo(x*x_new,2537);     &gt; end --&gt; x_new x_new =     2056.</pre>	<pre>--&gt; x=1005; --&gt; x_new=1; --&gt; for k=1:937,     &gt; x_new=pmodulo(x*x_new,2537);     &gt; end --&gt; x_new x_new =     2400.</pre>