 <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: _____

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.

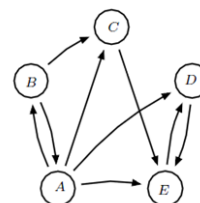
Podemos afirmar que:

- ☐ os dois grafos são de Hamilton
☒ apenas o grafo de vértices {a,b,c,d,e,f} é de Hamilton
☐ nenhum dos grafos é de Hamilton
☐ 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:

- ☐ é um circuito de Hamilton
☐ é um caminho de Hamilton
☒ não é caminho
☐ 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:

- ☒ 3
☐ 5
☐ 11
☐ nenhuma das anteriores

4.2 [1.0] não são primos entre si:

- ☐ 55, 150 e 539
☒ 55, 539 e 1287
☐ 150, 539 e 1287
☐ 150 e 539

4.3 [1.0] existe o inverso de 539 modulo:


- ☐ 55
☒ 150
☐ 1287
☐ nenhuma das anteriores

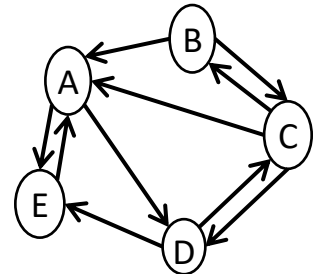
<div>P.PORTO</div> <div>ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO</div>	Tipo de Prova Teste 2	Ano letivo 2021/2022	Data 13-06-2022
	Curso LSIRC+LEI	Hora 15:00	
	Unidade Curricular Matemática Discreta	Duração 1,5 horas+15 min	

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 ) do processo Markov subjacente é:



X

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.    0.5    0.    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  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> --> T^6*[0 1 0 0 0]' ans = 0.3935185 0.0601852 0.1111111 0.1956019 0.2395833 </pre>	<pre> --> T^6*[0 0 0 0 1]' ans = 0.4027778 0.0694444 0.0833333 0.2152778 0.2291667 </pre>	<pre> --> 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	

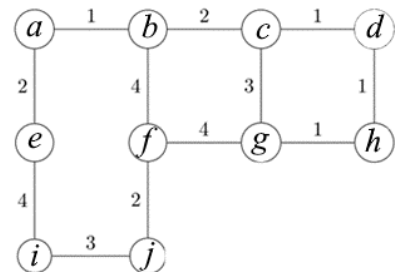
Nome: _____ Número: _____

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
0		a	{b, e}	$a, b \rightarrow L(b)=1$ $a, e \rightarrow L(e)=2$	{b, e} {1, 2}	a,b a,e
1	b	a, b	{c, f}	$a, b, c \rightarrow L(c)=1+2=3$ $a, b, f \rightarrow L(f)=1+4=5$	{e, c, f,} {2, 3, 5}	a,e a,b,c a,b,f
2	e	a, e	{i}	$a, e, i \rightarrow L(i)=2+4=6$	{c, f, i} {3, 5, 6}	a,b,c a,b,f a,e,i
3	c	a, b, c	{d, g}	$a, b, c, d \rightarrow L(d)=3+1=4$ $a, b, c, g \rightarrow L(g)=3+3=6$	{d, f, g, i} {4, 5, 6, 6}	a,b,c,d a,b,f a,b,c,g a,e,i
4	d	a, b, c, d	{h}	$a, b, c, d, h \rightarrow L(h)=4+1=5$	{h, f, i, g} {5, 5, 6, 6}	a,b,c,d,h a,b,f a,e,i a,b,c,g
5	h	a, b, c, d, h	{g}	$a, b, c, d, h, g \rightarrow L(g)=5+1=6$	{f, g, i} {5, 6, 6}	a,b,f a,b,c,g a,e,i a,b,c,g

O caminho de menor custo entre a e f é: a,b,f

 <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: _____

5	(a,e)	1	3	(a,e)	a,b ,e	c,d, g,h	f	i	j						5
6	(b,c)	1	2	(b,c)	a,b ,c,d ,e,g ,h	f	i	j							6
7	(f,j)	2	4	(f,j)	a,b ,c,d ,e,g ,h	f,j	i								7
8	(c,g)	1	1												
9	(i,j)	2	3	(i,j)	a,b ,c,d ,e,g ,h	f,i,j									8
10	(b,f)	1	2	(b,f)	a,b ,c,d ,e,f ,g, h,i, j										9

 <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	

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 mod 234.

$$\text{mdc}(234,48)$$

Temos que:

$$234 = 48 \times 4 + 42, 48 = 42 \times 1 + 6 \text{ e} \\ 42 = 6 \times 7 + 0$$

Portanto,

$$\text{mdc}(234,48) = \text{mdc}(48,42) = \text{mdc}(42,6) = 6$$

Não existe inverso de 48 mod 234 porque 48 e 234 não são primos entre si. De facto, $\text{mdc}(234,48) = 6 \neq 1$

9 [1.5] Resolva, se possível, a congruência $9x \equiv 3 \pmod{11}$.

$\text{mdc}(9,11) = 1$, logo existe inverso de 9 modulo 11.

Pelo algoritmo da divisão

$$11 = 9 \times 1 + 2 \Leftrightarrow 2 = 11 - 9 \\ 9 = 2 \times 4 + 1 \Leftrightarrow 1 = 9 - 2 \times 4$$

$1 = 9 - 2 \times 4 = 9 - (11 - 9) \times 4 = 5 \times 9 - 4 \times 11$, logo 5 é inverso de 9 modulo 11, então

$$9x \equiv 3 \pmod{11} \Leftrightarrow 5 \times 9x \equiv 5 \times 3 \pmod{11} \Leftrightarrow x \equiv 4$$

Então $x = 4 + 11k, k \in \mathbb{Z}$.

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


$$x_0 = 7$$

$$x_1 = (5 \times 7 + 7) \pmod{11} = 42 \pmod{11} = 9$$

$$x_2 = (5 \times 9 + 7) \pmod{11} = 52 \pmod{11} = 8$$

$$x_3 = (5 \times 8 + 7) \pmod{11} = 47 \pmod{11} = 3$$

$$x_4 = (5 \times 3 + 7) \pmod{11} = 22 \pmod{11} = 0$$

 <div> <div>ESCOLA</div> <div>SUPERIOR</div> <div>DE TECNOLOGIA</div> <div>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: _____

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”.

As letras da mensagem a encriptar correspondem às posições 7, 0, 18 e 7

$$f(7) = (10 \times 7 + 1) \bmod 29 = 71 \bmod 29 = 13 \rightarrow N$$

$$f(0) = (10 \times 0 + 1) \bmod 29 = 1 \bmod 29 = 1 \rightarrow B$$

$$f(18) = (10 \times 18 + 1) \bmod 29 = 181 \bmod 29 = 7 \rightarrow H$$

$$f(7) = (10 \times 7 + 1) \bmod 29 = 71 \bmod 29 = 13 \rightarrow N$$

Logo, a mensagem encriptada será: NBHN

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

Proposta de Resolução:

VERSÃO 1: $f(n) = (10n + 1) \bmod 29$

Como $\text{mdc}(10, 29) = 1$ os números 10 e 29 são primos entre si, portanto é possível calcular o inverso de 10 módulo 29.

Pelo algoritmo da divisão temos que

$$29 = 2 \times 10 + 9 \quad \text{e} \quad 10 = 1 \times 9 + 1$$

Donde,

$$1 = 10 - 1 \times 9 = 10 - 29 + 2 \times 10 \Leftrightarrow 1 = 3 \times 10 - 29 \times 1$$

Portanto,

$x = 3$ é o inverso de 10 módulo 29.

$$f(n) = (10n + 1) \bmod 29 \Leftrightarrow c = (10n + 1) \bmod 29 \Leftrightarrow c + 28 = (10n + 1 + 28) \bmod 29$$

$$\Leftrightarrow c + 28 = 10n \bmod 29 \Leftrightarrow 10n = (c + 28) \bmod 29 \Leftrightarrow 3 \times 10 n = 3 \times (c + 28) \bmod 29$$

$$\Leftrightarrow n = (3c + 26) \bmod 29$$


```
--> pmodulo(3*28,29)
```

```
ans =
```


```
26.
```

Logo,

$$f^{-1}(n) = (3n + 26) \bmod 29$$

 <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	

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”.

Como $C \rightarrow 02$ e $S \rightarrow 18$, CS corresponde a 0218.

Encriptação: $u(x) = x^a \bmod m$, com $m = p \times q = 2537$

Assim como

$$u(\text{CS}) = u(0218) = 218^{13} \bmod (2537) = 1259$$

A mensagem “CS” encriptada é: 1259

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

$$v(1005) = 1005^{937} \bmod (2537) = 2400$$

Como $24 \rightarrow Y$ e $00 \rightarrow A$, a mensagem original é YA.

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