P.PORTO ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO	Tipo de Prova Exame de Época Normal – Proposta de Resolução	Ano letivo 2021/2022	Data 01-07-2022
	Curso LSIRC+LEI		Hora 10:00
	Unidade Curricular Matemática Discreta		Duração 3,0 horas

Nome: ____ **Número:** ________

Observações:

A avaliação desta Unidade Curricular, na modalidade de avaliação durante o período de exames, contempla dois elementos com as ponderações: **70% Exame + 30% Trabalho Prático**.

Para a realização desta prova o estudante pode usar um formulário (com até duas páginas A4) manuscrito e criado pelo próprio. 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, Isabel Cristina Duarte e Glória Carvalho

PARTE 1

RESPONDA À QUESTÃO 1 NESTA FOLHA. NÃO PRECISA DE JUSTIFICAR A SUA RESPOSTA.

1. Considere os conjuntos $X = \{x^2 + 1 : x \in \{0, 1\}\}$ e $Y = \{\emptyset, 0, 1, 2, \{1,2\}\}$.

1.1. [0.6] Complete os espaços abaixo com $\in$ ou $\subseteq$ por forma a obter afirmações verdadeiras.

$\emptyset \in Y$ $\quad\quad$ $\{0,1\} \subseteq Y$ $\quad\quad$ $\{1,2\} \subseteq X$ $\quad\quad$ $\{1,2\} \in \mathcal{P}(Y)$

$X = \{1,2\}$, uma vez que para $x = 0$ temos $x^2 + 1 = 0^2 + 1 = 1$ e para $x = 1$ temos $x^2 + 1 = 1^2 + 1 = 2$

1.2. [0.6] Complete os espaços abaixo por forma a obter afirmações verdadeiras.

A função $f: \{0,1\} \longrightarrow Y$, definida por $f(x) = \{x\} \cap X$ é injetiva (injetiva/não injetiva) e não sobrejetiva (sobrejetiva/não sobrejetiva), portanto é não bijetiva (bijetiva/não bijetiva).

1.3. [0.8] Determine:

$X \times Y = \{(1,\emptyset), (1,0), (1,1), (1,2), (1,\{1,2\}), (2,\emptyset), (2,0), (2,1), (2,2), (2,\{1,2\})\}$

$X^2 = X \times X = \{(1,1), (1,2), (2,1), (2,2)\}$

$\mathcal{P}(X) - \mathcal{P}(Y) = \{\ \}$ uma vez que, todos os subconjunto de X também são subconjuntos de Y.

$\#(X \oplus Y) = 3$ porque $X \oplus Y = (X \cup Y) - (X \cap Y) = Y - X = \{\emptyset, 0, \{1,2\}\}$

PARA AS QUESTÕES 2 ATÉ 6, APRESENTE TODAS AS JUSTIFICAÇÕES E CÁLCULOS NA FOLHA DE RESPOSTA.

2. [1.2] Tendo em conta as igualdades apresentadas ao lado, determine:

$$\sum_{i=1}^{76} \left(\frac{3}{5}\right)^i$$

$$7\sum_{i=8}^{45} (i^3 - i^2)$$

$$\frac{5}{3}\prod_{i=97}^{101} 2$$

$\sum_{i=0}^{n} ar^i, r \neq 0$ (PG)	$a \times \dfrac{1 - r^{n+1}}{1-r}, r \neq 1$
$\sum_{i=1}^{n} i$ (PA)	$\dfrac{n(n+1)}{2}$
$\sum_{i=1}^{n} i^2$	$\dfrac{n(n+1)(2n+1)}{6}$
$\sum_{i=1}^{n} i^3$	$\dfrac{n^2(n+1)^2}{4}$

Proposta de Resolução:

$$\sum_{i=1}^{76} \left(\frac{3}{5}\right)^i = \sum_{i=0}^{75} \left(\frac{3}{5}\right)\left(\frac{3}{5}\right)^i = \left(\frac{3}{5}\right) \times \frac{1 - \left(\frac{3}{5}\right)^{75+1}}{1 - \frac{3}{5}} = \frac{3}{5} \times \frac{5}{2}\left(1 - \left(\frac{3}{5}\right)^{76}\right) = \frac{3}{2}\left(1 - \left(\frac{3}{5}\right)^{76}\right)$$

$$7\sum_{i=8}^{45}(i^3-i^2)=7\sum_{i=8}^{45}i^3-7\sum_{i=8}^{45}i^2=7\left(\sum_{i=1}^{45}i^3-\sum_{i=1}^{7}i^3\right)-7\left(\sum_{i=1}^{45}i^2-\sum_{i=1}^{7}i^2\right)$$

$$=7\times\frac{45^2\times(45+1)^2-7^2\times(7+1)^2}{4}-7\times\frac{45\times(45+1)\times(2\times45+1)-7\times(7+1)\times(2\times7+1)}{6}$$

$$=7\times\frac{45^2\times46^2-7^2\times8^2}{4}-7\times\frac{45\times46\times\ 91-7\times8\times15}{6}=7493087-218785=7274302$$

$$\frac{5}{3}\prod_{i=97}^{101}2=\frac{5}{3}\times2^{101-97+1}=\frac{5}{3}\times2^5=\frac{160}{3}$$

3. **[1.2]** Considere a fórmula de recorrência dada por:

$$\begin{cases} S(1)=5 \\ S(n)=3\,S(n-1)+4, & n\geq 2\end{cases}$$

Recorrendo ao algoritmo EGV (*Expand*, *Guess*, *Verify*), encontre a fórmula fechada correspondente.

Proposta de Resolução:

Expand

Temos que

$$\begin{aligned} S(n) &= 3\,S(n-1)+4 \\ &= 3\times(\mathbf{3\,S(n-2)+4})+4=3^2\times S(n-2)+3\times4+4 \\ &= 3^2\times(\mathbf{3\,S(n-3)+4})+3\times4+4=3^3\times S(n-3)+3^2\times4+3\times4+4 \\ &= \cdots \\ &= 3^k\,S(n-k)+3^{k-1}\times4+\cdots+3\times4+4=3^k\,S(n-k)+4\times(3^{k-1}+3^{k-2}+\cdots+3^0) \\ &= 3^k\,S(n-k)+4\times\sum_{i=0}^{k-1}3^i \end{aligned}$$

Cálculos auxiliares

$$\sum_{i=0}^{k-1}3^j=1\times\frac{1-3^{(k-1)+1}}{1-3}=\frac{1-3^k}{-2}=\frac{3^k-1}{2}$$

Guess

A fórmula fechada para a fórmula de recorrência será:

$$S(n)=3^k\,S(n-k)+2\times(3^k-1)$$

Para $n-k=1$, ou seja, $k=n-1$ temos

$$S(n)=3^{n-1}\times S(1)+2\times(3^{n-1}-1)=3^{n-1}\times5+2\times(3^{n-1}-1)=3^{n-1}\times(5+2)-2=7\times3^{n-1}-2$$

Verify – Indução Matemática

Passo base: P(1) verifica-se pois, se aplicarmos a fórmula fechada $S(n)=7\times3^{n-1}-2$ para $n=1$ obtemos $S(1)=5$ tal como é dado na fórmula de recorrência, i.e.:

$$S(1)=7\times3^{1-1}-2=5$$

Passo indutivo $P(k) \Longrightarrow P(k+1)$

Hipótese de Indução P(k): $S(k) = 7 \times 3^{k-1} - 2$

Tese P(k+1): $S(k+1) = 7 \times 3^{k} - 2$

Temos que,

$S(k+1) = 3\,S(k) + 4$, pela fórmula de recorrência

$= 3 \times \left(\mathbf{7} \times \mathbf{3}^{\boldsymbol{k-1}} - \mathbf{2}\right) + 4$, assumindo como verdadeira a Hipótese de Indução P(k): $S(k) = 7 \times 3^{k-1} - 2$

$= 7 \times 3 \times\ 3^{k-1} - 3 \times 2 + 4 = 7 \times 3^{k} - 2$, efetuando os cálculos

Portanto,

$$P(k) \Longrightarrow P(k+1)$$

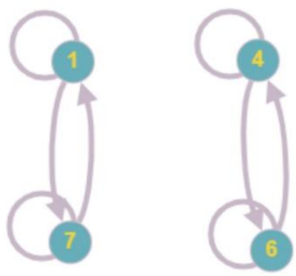
Visto que P(1) é verificado e $P(k) \Longrightarrow P(k+1)$, temos por indução matemática que, para todo $n \in I\!N$

$$S(n) = 7 \times 3^{n-1} - 2$$

4. Considere o conjunto $A = \{1,4,6,7\}$, e as duas relações seguintes definidas em A:

$$R = \{(x,y) : |x-y| \text{é divisível por } 2\} \text{ e } S = \{(1,1),(1,4),(1,7),(4,6)\}$$

4.1. [0.4] Represente a relação R graficamente na figura ao lado;



Proposta de resolução:

Seja $R = \{(x,y) : |x-y| \text{é divisível por } 2\}$ definida em $A = \{1,4,6,7\}$.

|x-y|	1	4	6	7
1	|1-1|=0	|1-4|=3	|1-6|=5	|1-7|=6
4	|4-1|=3	|4-4|=0	|4-6|=2	|4-7|=3
6	|6-1|=5	|6-4|=2	|6-6|=0	|6-7|=1
7	|7-1|=6	|7-4|=3	|7-6|=1	|7-7|=0

Logo,

$$R = \{(1,1),(1,7),(4,4),(4,6),(6,4),(6,6),(7,1),(7,7)\}$$

4.2. [0.8] Indique, justificando, se a relação R é de equivalência e em caso afirmativo escreva o seu conjunto quociente;

Proposta de resolução:

Para que uma relação seja de equivalência tem de ser: reflexiva, simétrica e transitiva.

Comecemos por considerar a relação $R = \{(x,y) : |x-y| \text{é divisível por } 2\}$

- Para qualquer $x \in A = \{1,4,6,7\}$, temos que $|x-x| = 0$, portanto $(x,x) \in R$.

  Logo, R é reflexiva.

- Para quaisquer $x, y \in A = \{1,4,6,7\}$, se $(x,y) \in R$ temos que $|x-y|$ é divisível por 2. Mas, $|x-y| = |y-x|$, donde $|y-x|$ é divisível por 2, e portanto $(y,x) \in R$.

  Logo, R é simétrica.

- Para quaisquer $x, y, z \in A = \{1,4,6,7\}$,

  se $(x, y) \in R$ e $(y, z) \in R$ temos que $|x - y|$ é divisível por 2 e $|y - z|$ é divisível por 2
  - Se $x = y$ então $|x - z| = |y - z|$ é divisível por 2, donde $(x, z) \in R$
  - Se $z = y$ então $|x - z| = |x - y|$ é divisível por 2, donde $(x, z) \in R$
  - O caso $x \neq y \neq z$ não ocorre em nenhum dos elementos de R.

  Logo, R é transitiva.

Concluímos assim que R é uma relação de equivalência.

O conjunto quociente é $[A]_R = \{[a]_R : a \in A\} = \{\{1,7\}, \{4,6\}\}$, porque

$[1]_R = \{xR1 : x \in A\} = \{1,7\}$, pois $(1,1) \in R$ e $(7,1) \in R$

$[7]_R = \{xR7 : x \in A\} = [1]_R$

$[4]_R = \{xR4 : x \in A\} = \{4,6\}$, pois $(4,4) \in R$ e $(6,4) \in R$

$[6]_R = \{xR6 : x \in A\} = [4]_R$

4.3. **[1.2]** Calcule:

- $S^{-1} \cup R =$
- $S^2 \ =$
- $S \cap R =$

Proposta de resolução:

Temos que $S^{-1} = \{(1,1), (4,1), (7,1), (6,4)\}$. Assim,

$$S^{-1} \cup R = \{(1,1), (4,1), (7,1), (6,4)\} \cup \{(1,1), (1,7), (4,4), (4,6), (6,4), (6,6), (7,1), (7,7)\}$$
$$= \{(1,1), (1,7), (4,1), (4,4), (4,6), (6,4), (6,6), (7,1), (7,7)\}$$

$S^2 \ = \{(1,1), (1,4), (1,7), (1,6)\}$ pois

$(1,1) \in S$ e $(1,1) \in S$ então $(1,1) \in S^2$
$(1,1) \in S$ e $(1,4) \in S$ então $(1,4) \in S^2$
$(1,1) \in S$ e $(1,7) \in S$ então $(1,7) \in S^2$
$(1,4) \in S$ e $(4,6) \in S$ então $(1,6) \in S^2$

$$S \cap R = \{(\mathbf{1}, \mathbf{1}), (1,4), (\mathbf{1}, \mathbf{7}), (\mathbf{4}, \mathbf{6})\} \cap \{(\mathbf{1}, \mathbf{1}), (\mathbf{1}, \mathbf{7}), (4,4), (\mathbf{4}, \mathbf{6}), (6,4), (6,6), (7,1), (7,7)\}$$
$$= \{(1,1), (1,7), (4,6)\}$$

5. Considere o fragmento de código Scilab onde são definidas as matrizes de adjacência M1 e M2 de dois grafos com vértices V1={a,b,c,d,e,f} e V2={A,B,C,D}, respetivamente. Com base no *output*, responda às questões seguintes.

```
--> 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];
```

```
--> M1^4
 ans  =
   16.    9.    6.    10.    8.    12.
   5.     2.    4.    3.     3.    5.
   13.    7.    7.    9.     8.    11.
   10.    2.    5.    7.     5.    7.
   11.    5.    5.    8.     6.    9.
   17.    7.    7.    11.    9.    11.
```

```
--> M2^4
 ans  =
   60.    18.    54.    24.
   18.    6.     15.    6.
   54.    15.    57.    24.
   24.    6.     24.    12.
--> M2+M2^2+M2^3+M2^4
 ans  =
   83.    24.    78.    35.
   24.    8.     23.    8.
   78.    23.    79.    32.
   35.    8.     32.    19.
```

5.1. Relativamente ao grafo definido pela matriz M1, indique:

i) [0.6] todos os caminhos de comprimento 4 do segundo para o quinto vértice;

Proposta de resolução:

Por observação da matriz M1^4, mais concretamente 2.ª linha e 5.ª coluna, temos que existem três caminhos de comprimento 4 do segundo para o quinto vértice;

Os caminhos são: b,a,a,d,e ; $b,a,a,f,e;$ b,a,f,d,e

ii) [0.2] o número de caminhos de comprimento 4 do quinto para o quarto vértice;

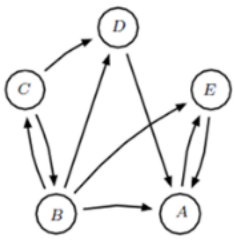
Proposta de resolução:

Por observação da matriz M1^4, mais concretamente 5.ª linha e 4.ª coluna, temos que existem oito caminhos de comprimento 4 do quarto para o quinto vértice;

5.2. [0.4] Relativamente ao grafo definido pela matriz M2, indique **justificando** se se trata de um grafo conexo;

Proposta de resolução:

A matriz M2 é simétrica pelo que o seu grafo é não orientado. A matriz de fecho `M2+M2^2+M2^3+M2^4` não tem nenhuma entrada nula, pelo que o grafo é conexo.



6. Relativamente ao grafo apresentado ao lado:

6.1. [0.6] indique a ordem, a dimensão, o conjunto dos vértices e das arestas;

Ordem: 5

Dimensão: 9

Conjunto das arestas: {(A,E), (B,A),(B,D),(B,C),(B,E),(C,B),(C,D),(D,A),(E,A)}

Conjunto dos Vértices: {A,B,C,D,E}

6.2. [1.0] determine a matriz de adjacências e determine o grau de cada vértice.

Proposta de resolução:

Matriz de adjacências:

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$grau^e(A) = 0+1+0+1+1 = 3 \qquad grau^s(A) = 0+0+0+0+1 = 1$$
$$grau^e(B) = 0+0+1+0+0 = 1 \qquad grau^s(B) = 1+0+1+1+1 = 4$$
$$grau^e(C) = 0+1+0+0+0 = 1 \qquad grau^s(C) = 0+1+0+1+0 = 2$$
$$grau^e(D) = 0+1+1+0+0 = 2 \qquad grau^s(D) = 1+0+0+0+0 = 1$$
$$grau^e(E) = 1+1+0+0+0 = 2 \qquad grau^s(E) = 1+0+0+0+0 = 1$$

6.3. [0.4] averigue, **justificando**, se se trata de um grafo euleriano ou semi-euleriano, e, se possível, determine um circuito ou caminho de Euler, recorrendo ao Algoritmo de Fleury.

Proposta de resolução:

Um multigrafo orientado admite um circuito de Euler se e só se for conexo e se cada vértice tem o mesmo grau de entrada e saída. Como no grafo em estudo os graus de entrada e saída de cada vértice não coincidem, concluímos que o grafo não admite um circuito de Euler. Logo, o grafo não é euleriano.

Por outro lado, um multigrafo orientado admite um caminho euleriano, mas não tem um circuito de Euler, se e só se for conexo e todos os vértices têm o mesmo grau de entrada e saída, exceto dois vértices que têm graus de entrada e de saída que diferem de 1, sendo que um dos vértices tem um grau de entrada a mais do que o grau de saída e o outro vértice tem um grau de saída a mais do que o grau de entrada. Como no grafo em estudo todos os vértices têm graus de entrada e saídas diferentes, não admite um caminho de Euler. Podemos então concluir que o grafo também não é semi-euleriano.

PARTE 2

<u>RESPONDA ÀS QUESTÕES 7 ATÉ 10 NESTA FOLHA. NÃO PRECISA DE JUSTIFICAR A SUA RESPOSTA.</u>

7. [0.5] Considere o fragmento de código Scilab 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, podemos afirmar que:

- [ ] os dois grafos são de Hamilton
- [x] 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=[0 0 0 0 1 0;
  > 1 0 1 0 0 0;
  > 0 0 0 1 0 0;
  > 1 0 1 0 0 0;
  > 0 0 0 0 0 1;
  > 0 1 0 0 0 0];
```

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

8. Com base no fragmento de código Scilab ao lado, podemos afirmar que:

```
--> factor(22), factor(126), factor(294), factor(525)
 ans  =
   2.   11.
 ans  =
   2.   3.   3.   7.
 ans  =
   2.   3.   7.   7.
 ans  =
   3.   5.   5.   7.
```

8.1. [0.5] mdc(294, 525) é:

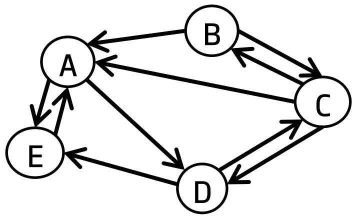
[ ] 3 [ ] 7 [x] 21 [ ] nenhuma das anteriores

8.2. [0.5] existe o inverso de 525 modulo:

[x] 22 [ ] 126 [ ] 294 [ ] nenhuma das anteriores

9. [0.5] Um inverso de 5 modulo 7 é: [ ] 2 [x] 3 [ ] 4 [ ] 5

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



10.1. [0.5] 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:

[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^6*[1 0 0 0 0]'
 ans  =

   0.2916667
   0.0277778
   0.1423611
   0.2291667
   0.3090278
```

```
--> T^6*[0 1 0 0 0]'
 ans  =

   0.3935185
   0.0601852
   0.1111111
   0.1956019
   0.2395833
```

```
--> T^6*[0 0 0 0 1]'
 ans  =

   0.4027778
   0.0694444
   0.0833333
   0.2152778
   0.2291667
```

[ ]

```
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.
```

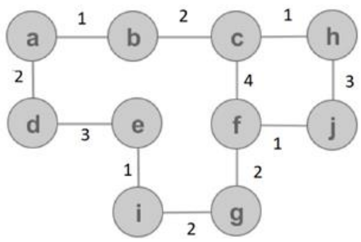
10.2. [0.5] Considere os cálculos apresentados no fragmento de código Scilab, sendo T a matriz de transição definida na alínea anterior.

A probabilidade, de começando na página B, seis passos depois não estar nem na página A nem na página C é aproximadamente:

[ ] 0,39 [ ] 0,11 [x] 0,50 [ ] 0,56

Nome: ________________________________ **Número:** ________

11. Considere o grafo ponderado apresentado ao lado.



11.1. **[1.2]** Use o algoritmo de *Dijkstra* para encontrar o caminho de menor custo entre ***a*** e ***g***.

***Observação**: Apresente a sua resolução na tabela abaixo.*

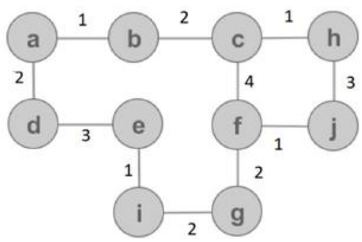
Proposta de resolução:

O caminho de menor custo é ***a,d,e,i,g*** O custo é 2+3+1+2=8

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,d}	a,b → L(b)=1 a,d → L(d)=2	{b,d} {1,2}	**a,b** a,d
1	b	a,b	{c}	a,b,c → L(c)=1+2=3	{d,c} {2,3}	**a,d** a,b,c
2	d	a,d	{e}	a,d,e → L(e)=2+3=5	{c,e} {3,5}	**a,b,c** a,d,e
3	c	a,b,c	{f,h}	a,b,c,f → L(f)=3+4=7 a,b,c,h → L(h)=3+1=4	{h,e,f} {4,5,7}	a,b,c,h a,d,e a,b,c,f
4	h	a,b,c,h	{j}	a,b,c,h,j → L(j)=4+3=7	{e,f,j} {5,7,7}	**a,d,e** a,b,c,f a,b,c,h,j
5	e	a,d,e	{i}	a,d,e,i → L(i)=5+1=6	{i,f,j} {6,7,7}	**a,d,e,i** a,b,c,f a,b,c,h,j
6	i	a,d,e,i	{g}	a,d,e,i,g → L(g)=6+2=8	{f,j,g} {7,7,8}	**a,b,c,f** a,b,c,h,j a,d,e,i,g
7	f	a,b,c,f	{j,g}	a,b,c,f,g → L(g)=7+2=9	{j,g} {7,8}	a,b,c,h,j a,d,e,i,g

11.2. **[1.2]** Usando o Algoritmo de *Kruskal*, determine uma árvore geradora de custo mínimo do grafo, e indique o seu comprimento.

***Observação**: Apresente a sua resolução na tabela abaixo.*



Proposta de resolução:

(a, b) → 1 (e, i) → 1 (a, d) → 2 (f, g) → 2 (d, e) → 3 (c, f)
(c, h) → 1 (f, j) → 1 (b, c)→ 2 (i, g) → 2 (h, j) → 3 → 4

T={(a,b),(c,h)(e,i)(f,j)(a,d),(b,c),(f,g),(i,g),(d,e)} Custo =15

It	(vi,vj)	Si	Sj	T	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	Nr
					a	b	c	d	e	f	g	h	i	j	
1	(a, b)	S1	S2	(a, b)	a, b	c	d	e	f	g	h	i	j		1
2	(c, h)	S2	S7	(c, h)	a ,b	c, h	d	e	f	g	i	j			2
3	(e, i)	S4	S7	(e, i)	a, b	c, h	d	e, i	f	g	j				3
4	(f, j)	S5	S7	(f, j)	a, b	c ,h	d	e, i	f, j	g					4
5	(a, d)	S1	S3	(a, d)	a, b, d	c, h	e, i	f, j	g						5
6	(b, c)	S1	S2	(b, c)	a, b, c, d, h	e, i	f, j	g							6
7	(f, g)	S3	S4	(f, g)	a, b, c, d, h	e, i	f, g, j								7
8	(i, g)	S2	S3	(i, g)	a, b, c, d, h	e, i, f, g, j									8
9	(d, e)	S1	S2	(d, e)	a, b, c, d, e, f, g, h, i, j										9

PARA AS QUESTÕES SEGUINTES, APRESENTE TODAS AS JUSTIFICAÇÕES E CÁLCULOS NA FOLHA DE RESPOSTA.

12. [1.0] Determine, recorrendo ao Algoritmo de Euclides, os inteiros s e t (coeficientes de Bézout) tais que mdc(32,105) $= 105 \times s + 32 \times t$, e se possível, indique o inverso de $32 \bmod 105$.

Proposta de resolução:

Temos que:

$$105 = 32 \times 3 + 9$$
$$32 = 9 \times 3 + 5$$
$$9 = 5 \times 1 + 4$$
$$5 = 4 \times 1 + 1$$
$$4 = 1 \times 4 + 0$$

Portanto,

$$\mathrm{mdc}(105{,}32) = \mathrm{mdc}(32{,}9) = \mathrm{mdc}(9{,}5) = mdc(5{,}4) = 1$$

Como mdc(105,32)=1 então existe o inverso de 32 mod 105.

Vamos determinar os coeficientes de Bézout

$$\begin{aligned}\mathrm{mdc}(105{,}32) = 1 &= 5 - 4 \times 1 \\ &= 5 - (9 - 5 \times 1) = 5 - 9 + 5 = 2 \times 5 - 1 \times 9 \\ &= 2 \times (32 - 9 \times 3) - 1 \times 9 = 2 \times 32 - 6 \times 9 - 1 \times 9 = 2 \times 32 - 7 \times 9 \\ &= 2 \times 32 - 7 \times (105 - 32 \times 3) = 2 \times 32 - 7 \times 105 + 21 \times 32 = -7 \times 105 + 23 \times 32\end{aligned}$$

Logo,

os coeficientes de Bézout são s=-7, t=23 e, portanto, 23 é o inverso de 32 mod 105.

13. [0.6] Resolva, se possível, a congruência $7x \equiv 2 \bmod 12$, sabendo que 7 é inverso de 7 modulo 12.

Proposta de resolução:

$$7x \equiv 2 \bmod 12 \Leftrightarrow 7 \times 7x \equiv 7 \times 2 \bmod 12 \Leftrightarrow 1 \times x \equiv 14 \bmod 12 \Leftrightarrow x \equiv 2 \bmod 12$$

Então,

$$x = 2 + 12k, k \in \mathbb{Z}.$$

14. [1.0] Escreva a sequência de números pseudo-aleatórios gerada por $x_{n+1} = (6x_n + 2) \bmod 13$, com raíz $x_0 = 1$.

Proposta de resolução:

$$\begin{aligned}
x_0 &= 1 \\
x_1 &= (6 \times 1 + 2) \bmod 13 = 8 \bmod 13 = 8 \\
x_2 &= (6 \times 8 + 2) \bmod 13 = 50 \bmod 13 = 11 \\
x_3 &= (6 \times 11 + 2) \bmod 13 = 68 \bmod 13 = 3 \\
x_4 &= (6 \times 3 + 2) \bmod 13 = 20 \bmod 13 = 7 \\
x_5 &= (6 \times 7 + 2) \bmod 13 = 44 \bmod 13 = 5 \\
x_6 &= (6 \times 5 + 2) \bmod 13 = 32 \bmod 13 = 6 \\
x_7 &= (6 \times 6 + 2) \bmod 13 = 38 \bmod 13 = 12 \\
x_8 &= (6 \times 12 + 2) \bmod 13 = 74 \bmod 13 = 9 \\
x_9 &= (6 \times 9 + 2) \bmod 13 = 56 \bmod 13 = 4 \\
x_{10} &= (6 \times 4 + 2) \bmod 13 = 26 \bmod 13 = 0 \\
x_{11} &= (6 \times 0 + 2) \bmod 13 = 2 \bmod 13 = 2 \\
x_{12} &= (6 \times 2 + 2) \bmod 13 = 14 \bmod 13 = 1
\end{aligned}$$

Logo, a sequência de números pseudo-aleatórios gerada por $x_{n+1} = (6x_n + 2) \bmod 13$, com raíz $x_0 = 1$ é:

1, 8, 11, 3, 7, 5, 6, 12, 9, 4, 0, 2, 1, ...

15. Considere a função de encriptação $f(n) = (8n + 1) \bmod 29$ 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

15.1. [0.4] Mostre que a função de desencriptação é definida por $f^{-1}(n) = (11n + 18) \bmod 29$.

Proposta de resolução:

Como $\text{mdc}(8, 29) = 1$ os números 8 e 29 são primos entre si, portanto é possível calcular o inverso de 8 módulo 29.

Pelo algoritmo da divisão temos que

$$29 = 3 \times 8 + 5\,, \qquad 8 = 5 \times 1 + 3, \qquad 5 = 3 \times 1 + 2 \quad \text{e} \quad 3 = 2 \times 1 + 1$$

Donde,

$$1 = 3 - 1 \times 2 = 3 - 1 \times (5 - 3 \times 1) = 2 \times 3 - 1 \times 5 = 2 \times (8 - 5 \times 1) - 5 = 2 \times 8 - 3 \times 5$$

$$= 2 \times 8 - (8 - 5)53 = -3 \times 8 + 5 \times 5 = -3 \times 8 + 5 \times (29 - 8 \times 3) = -18 \times 8 + 5 \times 29$$

Portanto, -18 é um inverso de 8 módulo 29. Como -18+29=11 temos que $x = 11$ é o inverso de 8 módulo 29.

$$f(n) = (8n + 1) \bmod 29 \iff c = (8n + 1) \bmod 29 \iff c + 28 = (8n + 1 + 28) \bmod 29$$

$$\iff c + 28 = 8n \bmod 29 \iff 8n = (c + 28) \bmod 29 \iff 11 \times 8\, n = 11 \times (c + 28) \bmod 29$$

$$\iff 11 \times 8\, n = (11c + 308) \bmod 29 \iff n = (11c + 18) \bmod 29$$

Logo, a função de desencriptação é definida por

$$f^{-1}(n) = (11n + 18) \bmod 29$$

15.2. [0.8] Desencripte a mensagem "@ECC_".

Proposta de resolução:

As letras da mensagem a encriptar correspondem às posições @ →28, E →4, C→2 e _ → 26.

Aplicando a função de desencriptação temos:

$$f^{-1}(28) = (11 \times 28 + 18) \bmod 29 = 326 \bmod 29 = 7 \to H$$

$$f^{-1}(4) = (11 \times 4 + 18) \bmod 29 = 62 \bmod 29 = 4 \to E$$

$$f^{-1}(2) = (11 \times 2 + 18) \bmod 29 = 40 \bmod 29 = 11 \to L$$

$$f^{-1}(26) = (11 \times 26 + 18) \bmod 29 = 304 \bmod 29 = 14 \to 0$$

Logo, a mensagem encriptada é "HELLO".

16. [0.8] Considere o sistema RSA com $a = 13$ e $m = 43 \times 59 = 2537$. Sendo b=937 a chave privada, desencripte a mensagem "1590".

Use os outputs do Scilab que considerar necessários.

```
--> pmodulo(1408,2537)
 ans  =
   1408.
--> pmodulo(1408^13,2537)
 ans  =
   0.
```

```
--> x=13;
--> x_new=1;
--> for k=1:1408,
  >      x_new=pmodulo(x*x_new,2537);
  > end
--> x_new
 x_new  =
   271.
```

```
--> x=1048;
--> x_new=1;
--> for k=1:13,
  >
x_new=pmodulo(x*x_new,2537);
  > end
--> x_new
 x_new  =
     1673.
```

```
--> x=1590;
--> x_new=1;
--> for k=1:2537,
  >      x_new=pmodulo(x*x_new,937);
  > end
--> x_new
 x_new  =
   664.
```

```
--> x=1590;
--> x_new=1;
--> for k=1:13,
  >    x_new=pmodulo(x*x_new,2537);
  > end
--> x_new
 x_new  =
   1332.
```

```
---> x=1590;
--> x_new=1;
--> for k=1:937,
  >    x_new=pmodulo(x*x_new,2537);
  > end
--> x_new
 x_new  =
   1203.
```

<u>Proposta de resolução:</u>

$v(1590) = 1590^{937} \mathrm{mod}(2537) = 1203$

Como 12 → M e 03→D,
a mensagem original é "MD".

Observação:
Dos outputs apresentados seria usado apenas o indicado a azul.