 <div> <div>ESCOLA</div> <div>SUPERIOR</div> <div>DE TECNOLOGIA</div> <div>E GESTÃO</div> </div>	Tipo de Prova Teste 2	Ano letivo 2016/2017	Data 09-06-2017
	Curso Licenciatura em Segurança Informática de Redes de Computadores	Hora 13:10	
	Unidade Curricular Matemática Discreta	Duração 1,5 horas	

N.º de aluno: \_\_\_\_\_ Nome: Proposta de Resolução

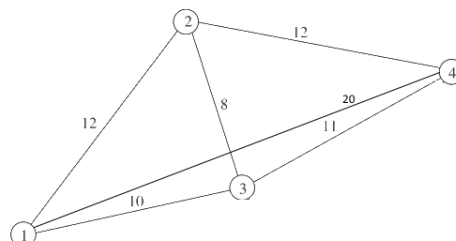
Questão	1	2	3	4	5	6	TOTAL
Cotação	1,5+1,5+1,5	1,5+1,5+1,5	1,5	1,5+1,7	1,5+1,8	1,5+1,5	20

1. Considere o grafo representado ao lado:

a) Classifique o grafo e indique o grau de cada um dos seus vértices.

O grafo é não orientado, simples, ponderado, conexo e completo.

$\text{grau}(1)=\text{grau}(2)=\text{grau}(3)=\text{grau}(4)=3$ .



b) Justifique que o grafo é de Hamilton.

O grafo B é de Hamilton, uma vez que um grafo simples que possui  $n=4$  vértices e todos os seus vértices têm grau 3, portanto, maior ou igual a  $n/2=2$ .

c) Indique todos circuitos de Hamilton possíveis e o respetivo custo.

O grafo tem  $\frac{(n-1)!}{2} = \frac{3!}{2} = 3$  circuitos de Hamilton que são:

- 1, 2, 3, 4, 1 com custo  $12+8+11+20=51$
- 1, 3, 2, 4, 1 com custo  $10+8+12+20=50$
- 1, 3, 4, 2, 1 com custo  $10+11+12+12=45$

2. Usando o Algoritmo de Euclides, determine:

a)  $\text{mmc}(252,113)$ ;

Temos que:

- $252 = 113 \times 2 + 26$
- $113 = 26 \times 4 + 9$
- $26 = 9 \times 2 + 8$
- $9 = 8 \times 1 + 1$

Portanto,

$$\text{mdc}(252,113)=\text{mdc}(113,26)=\text{mdc}(26,9)=\text{mdc}(8,1)=\text{mdc}(9,8)=1$$

Por outro lado,

$$\text{mdc}(252,113) \times \text{mmc}(252,113) = 252 \times 113$$

$$\Leftrightarrow 28476 = 1 \times \text{mmc}(252,113)$$

$$\Leftrightarrow \text{mmc}(252,113) = 28476$$

b) os inteiros  $s$  e  $t$  (coeficientes de Bézout) tais que  $\text{mdc}(252,113) = 252s + 113t$ ;

Temos que:

$$\begin{aligned} 1 &= 9 - 8 \times 1 \\ &= 9 - (26 - 9 \times 2) \times 1 = 9 \times 3 - 26 \times 1 \\ &= (113 - 26 \times 4) \times 3 - 26 \times 1 = 113 \times 3 - 26 \times 13 \\ &= 113 \times 3 - (252 - 113 \times 2) \times 13 = 113 \times 29 - 252 \times 13 \end{aligned}$$

Logo, os coeficientes de Bézout são  $s = -13$  e  $t = 29$ .


c) resolva, se possível a congruência,  $113x \equiv 1 \pmod{252}$ .

Como  $\text{mdc}(113,252)=1$  temos que 113 admite inverso modulo 252.

Pela alínea anterior temos que

$$113 \times 29 - 252 \times 13 = 1 \Leftrightarrow 113 \times 29 = 252 \times 13 + 1 \Leftrightarrow 113 \times 29 \equiv 1 \pmod{252}$$

A solução é  $x = 29$ .

 <small>ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO</small>	Tipo de Prova Teste 2	Ano letivo 2016/2017	Data 09-06-2017
	Curso Licenciatura em Segurança Informática de Redes de Computadores	Hora 13:10	
	Unidade Curricular Matemática Discreta	Duração 1,5 horas	

N.º de aluno: \_\_\_\_\_ Nome: Proposta de Resolução

3. Escreva a sequência de números pseudo-aleatórios gerada por  $x_{n+1} = (7x_n + 3) \bmod 11$ , com raiz  $x_0 = 1$ .  
A sequência de números pseudo-aleatórios gerada é: 1, 10, 7, 8, 4, 9, 0, 3, 2, 6.

$$x_1 = (7x_0 + 3) \bmod 11 = (7 \times 1 + 3) \bmod 11 = 10 \bmod 11 = 10$$

$$x_2 = (7x_1 + 3) \bmod 11 = (7 \times 10 + 3) \bmod 11 = 73 \bmod 11 = 7$$

$$x_3 = (7x_2 + 3) \bmod 11 = (7 \times 7 + 3) \bmod 11 = 52 \bmod 11 = 8$$

$$x_4 = (7x_3 + 3) \bmod 11 = (7 \times 8 + 3) \bmod 11 = 4$$

$$x_5 = (7x_4 + 3) \bmod 11 = (7 \times 4 + 3) \bmod 11 = 9$$

$$x_6 = (7x_5 + 3) \bmod 11 = (7 \times 9 + 3) \bmod 11 = 0$$

$$x_7 = (7x_6 + 3) \bmod 11 = (7 \times 0 + 3) \bmod 11 = 3$$

$$x_8 = (7x_7 + 3) \bmod 11 = (7 \times 3 + 3) \bmod 11 = 2$$

$$x_9 = (7x_8 + 3) \bmod 11 = (7 \times 2 + 3) \bmod 11 = 6$$

$$x_{10} = (7x_9 + 3) \bmod 11 = (7 \times 6 + 3) \bmod 11 = 1$$

-->x=1; x=pmodulo(7*x+3,11) x =  10.  -->x=pmodulo(7*x+3,11) x =  7. -->x=pmodulo(7*x+3,11) x =  8.	-->x=pmodulo(7*x+3,11) x =  4. -->x=pmodulo(7*x+3,11) x =  9. -->x=pmodulo(7*x+3,11) x =  0.	-->x=pmodulo(7*x+3,11) x =  3.  -->x=pmodulo(7*x+3,11) x =  2.	-->x=pmodulo(7*x+3,11) x =  6.  -->x=pmodulo(7*x+3,11) x =  1.
---	---	--	--

4. Considere a função encriptadora  $f(n) = (7n + 3) \bmod 26$  e  $A \leftrightarrow 0, \dots, Z \leftrightarrow 25$ .

a) Encripte a mensagem "MD".

$$f(M) = f(12) = (7 \times 12 + 3) \bmod 26 = 9 \rightarrow J$$

$$f(D) = f(3) = (7 \times 3 + 3) \bmod 26 = (21 + 3) \bmod 26 = 24 \rightarrow Y$$

A mensagem encriptada é JY.

-->pmodulo((7*12+3),26) ans =  9.	-->pmodulo((7*3+3),26) ans =  24.
--	--

- b) Sabendo que  $x = 15$  é a solução de  $7x \equiv 1 \bmod 26$ , escreva a função de desencriptação e desencripte a mensagem "ZA".

$$p = (7n + 3) \bmod 26 \Leftrightarrow 7n = (p - 3) \bmod 26 \Leftrightarrow 15 \times 7n = 15(p - 3 + 26) \bmod 26$$

$$\Leftrightarrow n = 15(p + 23) \bmod 26$$


$$\text{Logo, } f^{-1}(n) = 15(n + 23) \bmod 26.$$

$$f^{-1}(Z) = f^{-1}(25) = 15(25 + 23) \bmod 26 = 15 \times 48 \bmod 26 = 720 \bmod 26 = 18 \rightarrow S$$

$$f^{-1}(A) = f^{-1}(0) = 15(0 + 23) \bmod 26 = 15 \times 23 \bmod 26 = 345 \bmod 26 = 7 \rightarrow H$$

A mensagem encriptada é SH.

-->pmodulo(15*(25+23),26) ans =  18.	-->pmodulo(15*(0+23),26) ans =  7.
---	---

 <small>ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO</small>	Tipo de Prova Teste 2	Ano letivo 2016/2017	Data 09-06-2017
	Curso Licenciatura em Segurança Informática de Redes de Computadores	Hora 13:10	
	Unidade Curricular Matemática Discreta	Duração 1,5 horas	

N.º de aluno: \_\_\_\_\_ Nome: Proposta de Resolução

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

a) Encripte a mensagem "AZ".

$$u(AZ) = u(0025) = 0025^{13} \bmod 2537 = 1433$$

A mensagem encriptada é 1433.

```
-->x=0025;
-->x_new=1;
-->for k=1:13
-->x_new=pmodulo(x*x_new,2537);
-->end
-->x_new
x_new =
1433.
```

b) Desencripte a mensagem "1105".

Determinar  $b$  tal que  $ab \bmod n = 1$ :

$$13b \bmod (43 \times 59) = 1 \Leftrightarrow 13b \bmod 2537 = 1 \Leftrightarrow \exists k \in \mathbb{Z}: 13b - 1 = 2537k$$

$$\Leftrightarrow \exists k \in \mathbb{Z}: 13b - 2537k = 1$$

Temos

$$2537 = 187 \times 13 + 5$$

$$13 = 5 \times 2 + 3$$

$$5 = 3 \times 1 + 2$$

$$3 = 2 \times 1 + 1$$

Então

$$1 = 3 - 2 \times 1$$

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

$$\Leftrightarrow 1 = (13 - 5 \times 2) \times 2 - 5 \times 1 = 13 \times 2 - 5 \times 5$$

$$\Leftrightarrow 1 = 13 \times 2 - 5 \times (2537 - 13 \times 187) = 13 \times 937 + 2537 \times (-5)$$

Logo  $b=937$

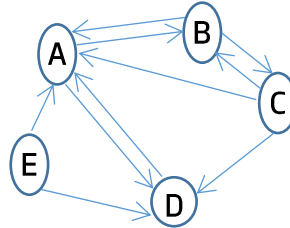
$$1105^{937} \bmod 2537 = 69$$

```
-->x=1105
x =
1105.
-->x_new=1
x_new =
1.
-->for k=1:(937)
--> x_new=pmodulo(x*x_new,2537);
-->end
-->x_new
x_new =
69.
```

<p><b>P.PORTO</b></p> <p>ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO</p>	Tipo de Prova Teste 2	Ano letivo 2016/2017	Data 09-06-2017
	Curso Licenciatura em Segurança Informática de Redes de Computadores	Hora 13:10	
	Unidade Curricular Matemática Discreta	Duração 1,5 horas	

N.º de aluno: \_\_\_\_\_ Nome: Proposta de Resolução

6. Considere rede constituída por 5 páginas web A, B, C, D, E com os links mostrados na imagem abaixo:



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

a) Escreva a matriz de transição do processo Markov subjacente.

A matriz de transição é:

$$T = \begin{bmatrix} 0 & \frac{1}{2} & \frac{1}{3} & 1 & \frac{1}{2} \\ \frac{1}{2} & 0 & \frac{1}{3} & 0 & 0 \\ 0 & \frac{1}{2} & 0 & 0 & 0 \\ \frac{1}{2} & 0 & \frac{1}{3} & 0 & \frac{1}{2} \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

```
-->T=zeros(5,5); T(1,2)=0.5;T(1,4)=0.5; T(2,1)=0.5;T(2,3)=0.5;
```

```
-->T(3,1)=1/3;T(3,2)=1/3;T(3,4)=1/3; T(4,1)=1;  
T(5,1)=0.5;T(5,4)=0.5;
```

```
-->T=T'
```

```
T =
```

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

b) Calcule a probabilidade, de começando na página A, 5 passos depois estar na página D, A e C?

É necessário calcular  $T^5 \times \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$ . Usando o Scilab obteve-se  $\begin{bmatrix} 0.1388889 \\ 0.4201389 \\ 0.0208333 \\ 0.4201389 \\ 0 \end{bmatrix}$

A probabilidade de estar:

- em D é aproximadamente 42%,
- em A é aproximadamente 14%
- e em C é aproximadamente 2%.

```
-->T^5  
ans =
```

```
0.1388889 0.5868056 0.3217593 0.6875 0.3854167  
0.4201389 0.1111111 0.2939815 0.0416667 0.25  
0.0208333 0.1909722 0.0902778 0.2291667 0.1145833  
0.4201389 0.1111111 0.2939815 0.0416667 0.25  
0. 0. 0. 0. 0.
```

```
-->T^5*[1 0 0 0 0]'  
ans =
```

```
0.1388889  
0.4201389  
0.0208333  
0.4201389  
0.
```

Bom Trabalho  
Elia Costa e Silva  
Flora Ferreira