
 <small>ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO</small>	Tipo de Prova Teste 2	Ano letivo 2018/2019	Data 29-05-2019
	Curso Licenciatura em Segurança Informática de Redes de Computadores Licenciatura em Engenharia Informática	Hora 15:10	
	Unidade Curricular Matemática Discreta	Duração 1,5 horas	

N.º de aluno: _____ Nome: _____

Observações:

Responda às questões que se seguem na folha do enunciado da prova.

Nas perguntas assinaladas com  recorra ao software para evitar os cálculos morosos. Nos restantes exercícios não são admitidas justificações obtidas com o software.

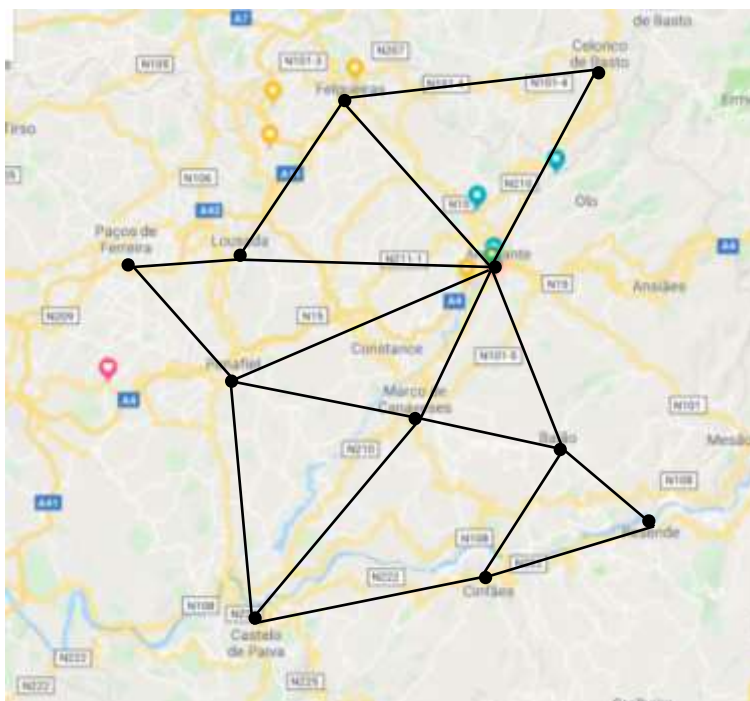
Submeta no moodle um ficheiro com os cálculos que efetue no .

Questão	1	2	3	4	5	6	TOTAL
Cotação	3,0	3,0	5,5	2,0	2,0	4,5	31

1. A empresa **PC-You** dá assistência nos seus clientes com instalações localizadas em cada um dos 11 Concelhos da Região do Tâmega e Sousa, denominados por:

Concelhos	Vértice
Amarante	A
Baião	B
Castelo de Paiva	CP
Celorico de Basto	CB
Cinfães	C
Felgueiras	F
Lousada	L
Marco de Canaveses	MC
Paços de Ferreira	PF
Penafiel	P
Resende	R

Os concelhos estão ligados por estradas ilustradas no grafo ao lado. Para atender os clientes o mais rapidamente possível ele precisa de visitar cada concelho uma única vez e no fim voltar a sua sede em **A/B/P/R**.



- 1.1. [1,5] Indique um possível circuito para responder a esta situação e classifique-o.

Temos que ter um circuito de Hamilton, por exemplo

A/CB/F/L/PF/P/MC/CP/C/R/B/A

B/A/CB/F/L/PF/P/MC/CP/C/R/B

P/MC/CP/C/R/B/A/CB/F/L/PF/P

R/B/A/CB/F/L/PF/P/MC/CP/C/R

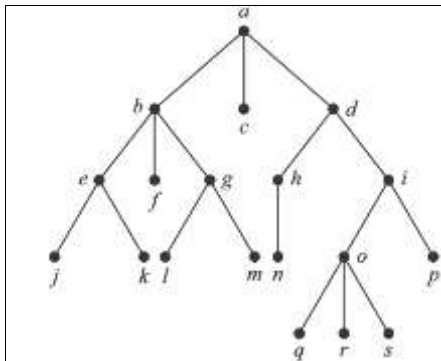
- 1.2. [1,5] Por questões de manutenção a estrada que liga **A a CB/ L a PF/ B a R/ CB a F** está interdita. Ainda é possível efetuar um circuito que passe por todos os concelhos? Justifique.

Não. Porque o circuito deixa de ser um circuito de Hamilton, já que fica com um vértice de grau 1

<p>P.PORTO</p> <p>ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO</p>	Tipo de Prova Teste 2	Ano letivo 2018/2019	Data 29-05-2019
	Curso Licenciatura em Segurança Informática de Redes de Computadores Licenciatura em Engenharia Informática	Hora 15:10	
	Unidade Curricular Matemática Discreta	Duração 1,5 horas	

N.º de aluno: _____ Nome: _____

2. Considere a árvore:



2.1. [1,5] Indique:

Versão 1

a raiz a
 um vértice interno b, d, e, g, d, i, o ou h
 um descendente de b e, f, g, j, k, l ou m
 um filho de d h, i
 a profundidade do vértice q 4

Versão 2

a raiz a
 uma folha j, k, l, m, f, c, n, p, q, r ou s
 um ascendente de b a
 um pai de d a
 a altura 4

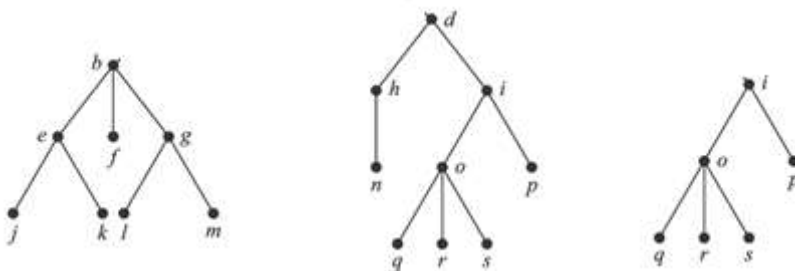
Versão 3


a raiz a
 um vértice interno b, e, g, d, i, o ou h
 um descendente de i o, p, q, r, s
 o pai de d a
 a profundidade 4

Versão 4

a raiz a
 uma folha j, k, l, m, f, c, n, p, q, r ou s
 um ascendente de d a
 um irmão de p o
 a altura 4

2.2. [1,5] Desenhe uma subárvore com raiz em b/d/i



 <small>ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO</small>	Tipo de Prova Teste 2	Ano letivo 2018/2019	Data 29-05-2019
	Curso Licenciatura em Segurança Informática de Redes de Computadores Licenciatura em Engenharia Informática		Hora 15:10
	Unidade Curricular Matemática Discreta		Duração 1,5 horas

N.º de aluno: _____ Nome: _____

3. Considere $a=205$ e $b=95$. Determine:

	A	b
V1	205	95
V2	234	48
V3	210	75
V4	235	75
	210	68
	235	80

3.1. o $\text{mdc}(a,b)$.


V1: $\text{mdc}(205,95)$ Temos que: $205 = 95 \times 2 + 15$, $95 = 15 \times 6 + 5$ e $15 = 5 \times 3 + 0$ Portanto, $\text{mdc}(205,95) = \text{mdc}(95,15) = \text{mdc}(15,5) = 5$	V2: $\text{mdc}(234,48)$ Temos que: $234 = 48 \times 4 + 42$, $48 = 42 \times 1 + 6$ e $42 = 6 \times 7 + 0$ Portanto, $\text{mdc}(234,48) = \text{mdc}(48,42) = \text{mdc}(42,6) = 6$
V3: $\text{mdc}(210,75)$ Temos que: $210 = 75 \times 2 + 60$, $75 = 60 \times 1 + 15$ e $60 = 15 \times 4 + 0$ Portanto, $\text{mdc}(210,75) = \text{mdc}(75,60) = \text{mdc}(60,15) = 15$	V4: $\text{mdc}(235,75)$ Temos que: $235 = 75 \times 3 + 10$, $75 = 10 \times 7 + 5$ e $10 = 5 \times 2 + 0$ Portanto, $\text{mdc}(235,75) = \text{mdc}(75,10) = \text{mdc}(10,5) = 5$

3.2. usando o Algoritmo de Euclides, os inteiros s e t (coeficientes de Bézout) tais que $\text{mdc}(a,b) = a \times s + b \times t$.

V1: Pretende-se determinar s e t tais que $\text{mdc}(205,95) = 5 = 205 \times s + 95 \times t$. Temos que: $5 = 95 - 15 \times 6 = 95 - (205 - 95 \times 2) \times 6$ $= 95 - 6 \times 205 + 95 \times 12$ $= 95 \times 13 - 6 \times 205$ Logo, os coeficientes de Bézout são: $s = -6$ e $t = 13$.	V2: Pretende-se determinar s e t tais que $\text{mdc}(234,48) = 6 = 234 \times s + 48 \times t$. Temos que: $6 = 48 - 42 \times 1 = 48 - (234 - 48 \times 4) \times 1$ $= 5 \times 48 - 234$ Logo, os coeficientes de Bézout são: $s = -1$ e $t = 5$.
V3: Pretende-se determinar s e t tais que $\text{mdc}(210,75) = 15 = 210 \times s + 75 \times t$. Temos que: $15 = 75 - 60 = 75 - (210 - 95 \times 2) \times 6 = 3 \times 75 - 1 \times 210$ Logo, os coeficientes de Bézout são: $s = -1$ e $t = 3$.	V4: Pretende-se determinar s e t tais que $\text{mdc}(235,75) = 5 = 235 \times s + 75 \times t$. Temos que: $5 = 75 - 10 \times 7 = 75 - 7 \times (235 - 75 \times 3)$ $= 22 \times 75 - 7 \times 235$ Logo, os coeficientes de Bézout são: $s = -7$ e $t = 22$.

3.3. se possível, o inverso de a mod b .

Como $\text{mdc}(a,b) \neq 1$ os números a e b não são primos entre si, portanto não é possível calcular o inverso de a módulo b .


 <small>ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO</small>	Tipo de Prova Teste 2	Ano letivo 2018/2019	Data 29-05-2019
	Curso Licenciatura em Segurança Informática de Redes de Computadores Licenciatura em Engenharia Informática		Hora 15:10
	Unidade Curricular Matemática Discreta		Duração 1,5 horas

N.º de aluno: _____ Nome: _____

4. Resolva, se possível, a congruência $10x \equiv 2 \pmod{11}$, $9x \equiv 3 \pmod{11}$, $8x \equiv 4 \pmod{11}$, $7x \equiv 2 \pmod{11}$, $6x \equiv 3 \pmod{11}$, $5x \equiv 4 \pmod{11}$.

V1: $10x \equiv 2 \pmod{11}$ $\text{mdc}(10,11) = 1$, logo existe inverso de 10 modulo 11. Pelo algoritmo da divisão $11 = 1 \times 10 + 1 \Leftrightarrow 1 = 11 - 1 \times 10$, logo (-1) é inverso de 10 modulo 11, então $10x \equiv 2 \pmod{11} \Leftrightarrow (-1) \cdot 10x \equiv (-1) \cdot 2 \pmod{11}$ $\Leftrightarrow x \equiv -2 \pmod{11} \Leftrightarrow x \equiv 9$ Então $x = 9 + 11k, k \in \mathbb{Z}$.	V2: $9x \equiv 3 \pmod{11}$ $\text{mdc}(9,11) = 1$, 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 $x = 4 + 11k, k \in \mathbb{Z}$.
V3: $8x \equiv 4 \pmod{11}$ $\text{mdc}(8,11) = \text{mdc}(3,2) = 1$, logo existe inverso de 8 modulo 11. Pelo algoritmo da divisão $11 = 8 \times 1 + 3 \Leftrightarrow 3 = 11 - 8$ $8 = 3 \times 2 + 2 \Leftrightarrow 2 = 8 - 3 \times 4$ $3 = 2 \times 1 + 1 \Leftrightarrow 1 = 3 - 2 \times 1$ $1 = 3 - 2 \times 1 = 3 - (8 - 3 \times 2) = 3 \times 3 - 8 = 3 \times (11 - 8 \times 1) - 8 = 3 \times 11 - 4 \times 8$, logo (-4) é inverso de 8 modulo 11, então $8x \equiv 4 \pmod{11} \Leftrightarrow (-4) \times 8x \equiv (-4) \cdot 4 \pmod{11} \Leftrightarrow x \equiv -16 \pmod{11} \Leftrightarrow x \equiv 6$ Então $x = 6 + 11k, k \in \mathbb{Z}$.	V4: $7x \equiv 2 \pmod{11}$ $\text{mdc}(7,11) = \text{mdc}(4,3) = 1$, logo existe inverso de 7 modulo 11. Pelo algoritmo da divisão $11 = 7 \times 1 + 4 \Leftrightarrow 4 = 11 - 7$ $7 = 4 \times 1 + 3 \Leftrightarrow 3 = 7 - 1 \times 4$ $4 = 3 \times 1 + 1 \Leftrightarrow 1 = 3 - 2 \times 1$ $1 = 4 - 3 \times 1 = 4 - (7 - 4 \times 1) = 4 \times 2 - 7 = (11 - 7 \times 1) \times 2 - 7 = 2 \times 11 - 3 \times 7$, logo (-3) é inverso de 7 modulo 11, então $7x \equiv 2 \pmod{11} \Leftrightarrow (-3) \times 7x \equiv (-3) \times 2 \pmod{11} \Leftrightarrow x \equiv -6 \pmod{11} \Leftrightarrow x \equiv 5$ Então $x = 5 + 11k, k \in \mathbb{Z}$.

$ax \equiv b \pmod{11}$	a	inverso de a	b	inv a * b	$x = \text{inv}(a) * b \pmod{11}$
$10x \equiv 2 \pmod{11}$	10	10	2	20	9
$9x \equiv 3 \pmod{11}$	9	5	3	15	4
$8x \equiv 4 \pmod{11}$	8	7	4	28	6
$7x \equiv 2 \pmod{11}$	7	8	2	16	5
$6x \equiv 3 \pmod{11}$	6	2	3	6	6
$5x \equiv 4 \pmod{11}$	5	9	4	36	3

5.  Escreva a sequência de números pseudo-aleatórios gerada por

V1: $x_{n+1} = (5x_n + 7) \pmod{13}$, com raiz $x_0 = 4$.


V2, V4: $x_{n+1} = (6x_n + 2) \pmod{13}$, com raiz $x_0 = 1$.

V3: $x_{n+1} = (7x_n + 2) \pmod{13}$, com raiz $x_0 = 2$.

$x_{n+1} = (5x_n + 7) \pmod{13}$, com raiz $x_0 = 3$.

$x_{n+1} = (6x_n + 2) \pmod{13}$, com raiz $x_0 = 4$.

$x_{n+1} = (7x_n + 2) \pmod{13}$, com raiz $x_0 = 5$.

 <small>ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO</small>	Tipo de Prova Teste 2	Ano letivo 2018/2019	Data 29-05-2019
	Curso Licenciatura em Segurança Informática de Redes de Computadores Licenciatura em Engenharia Informática		Hora 15:10
	Unidade Curricular Matemática Discreta		Duração 1,5 horas

N.º de aluno: _____ Nome: _____

	V1	V2,V4	V3			
a	5	6	7	5	6	7
b	7	2	2	7	2	2
m	13	13	13	13	13	13
x_0	4	1	2	3	4	5
	1	8	3	9	0	11
	12	11	10	0	2	1
	2	3	7	7	1	9
	4	7	12	3	8	0
	1	5	8	9	11	2
	12	6	6	0	3	3
	2	12	5	7	7	10
	4	9	11	3	5	7
	1	4	1	9	6	12
	12	0	9	0	12	8
	2	2	0	7	9	6
	4	1	2	3	4	5

6. Considere a função de encriptação $V1: f(n) = (15n + 1) \bmod 29$. Considere ainda que:

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

$$V1: f(n) = (15n + 1) \bmod 29.$$

$$V2: f(n) = (10n + 1) \bmod 29$$

$$V3: f(n) = (22n + 1) \bmod 29$$


$$V4: f(n) = (6n + 1) \bmod 29$$

$$f(n) = (11n + 1) \bmod 29$$

$$f(n) = (25n + 1) \bmod 29$$

6.1. Encripte a mensagem "WIKI", "HASH", "LIKE", "WORD", "SPAM", "BLOB".



5.1						f(n)=an+b mod 29						
Encripte						a	b					
W	I	K	I		v1	15	1	M	F	G	F	20%
22	8	10	8	20%				12	5	6	5	60%
H	A	S	H		v2	10	1	N	B	H	N	20%
7	0	18	7	20%				13	1	7	13	60%
L	I	K	E		v3	22	1	L	D	S	C	20%
11	8	10	4	20%				11	3	18	2	60%
W	O	R	D		v4	6	1	R	#	Q	T	20%
22	14	17	3	20%				17	27	16	19	60%
S	P	A	M		v5	11	1	Z	V	B	R	20%
18	15	0	12	20%				25	21	1	17	60%
B	L	O	B		v6	25	1	_	P	D	_	20%
1	11	14	1	20%				26	15	3	26	60%

 <small>ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO</small>	Tipo de Prova Teste 2	Ano letivo 2018/2019	Data 29-05-2019
	Curso Licenciatura em Segurança Informática de Redes de Computadores Licenciatura em Engenharia Informática	Hora 15:10	
	Unidade Curricular Matemática Discreta	Duração 1,5 horas	

N.º de aluno: _____ Nome: _____

6.2. Escreva a função de descriptação f^{-1} .

<p>V1: $f(n) = (15n + 1) \bmod 29$</p> <p>Como $\text{mdc}(15,29) = 1$ os números 15 e 29 são primos entre si, portanto é possível calcular o inverso de 15 módulo 29.</p> <p>Pelo algoritmo da divisão temos que</p> $29 = 1 \times 15 + 14 \quad \text{e} \quad 15 = 14 \times 1 + 1$ <p>Donde,</p> $1 = 15 - 1 \times 14 = 15 - 29 + 15 \Leftrightarrow$ $1 = 2 \times 15 - 29 \times 1$ <p>Portanto, $x = 2$ é o inverso de 15 módulo 29.</p> $f(p) = (15p + 1) \bmod 29 \Leftrightarrow c = (15p + 1) \bmod 29$ $\Leftrightarrow c - 1 = 15p \bmod 29 \Leftrightarrow$ $15p = (c - 1) \bmod 29 \Leftrightarrow$ $2 \times 15p = 2(c - 1) \bmod 29 \Leftrightarrow$ $p = 2(c - 1) \bmod 29$ <p>Logo, $f^{-1}(p) = 2(p - 1) \bmod 29 = (2p + 27) \bmod 29$</p>	<p>V2: $f(n) = (10n + 1) \bmod 29$</p> <p>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.</p> <p>Pelo algoritmo da divisão temos que</p> $29 = 2 \times 10 + 9 \quad \text{e} \quad 10 = 1 \times 9 + 1$ <p>Donde,</p> $1 = 10 - 1 \times 9 = 10 - 29 + 2 \times 10 \Leftrightarrow 1$ $= 3 \times 10 - 29 \times 1$ <p>Portanto,</p> <p>$x = 3$ é o inverso de 10 módulo 29.</p> $f(p) = (10p + 1) \bmod 29 \Leftrightarrow c = (10p + 1) \bmod 29$ $\Leftrightarrow c - 1 = 10p \bmod 29$ $\Leftrightarrow 10p = (c - 1) \bmod 29 \Leftrightarrow 3 \times 10p$ $= 3(c - 1) \bmod 29 \Leftrightarrow 1 \times p$ $= 3(c - 1) \bmod 29$ $\Leftrightarrow p = 3(c - 1) \bmod 29 = 3(c + 28) \bmod 29$ <p>Logo, $f^{-1}(p) = 3(p - 1) \bmod 29$</p> $= 43(p + 28) \bmod 29$
<p>V3: $f(n) = (22n + 1) \bmod 29$</p> <p>Como $\text{mdc}(22,29) = 1$ os números 22 e 29 são primos entre si, portanto é possível calcular o inverso de 22 módulo 29.</p> <p>Pelo algoritmo da divisão temos que</p> $29 = 1 \times 21 + 7 \quad \text{e} \quad 22 = 7 \times 3 + 1$ <p>Donde,</p> $1 = 22 - 7 \times 3 = 22 - (29 - 22) \times 3$ $= 22 - 29 \times 3 + 22 \times 3$ $= 4 \times 22 - 29 \times 3$ <p>Portanto, $x = 4$ é o inverso de 22 módulo 29.</p> $f(p) = (22p + 1) \bmod 29 \Leftrightarrow c = (22p + 1) \bmod 29$ $\Leftrightarrow c - 1 = 22p \bmod 29 \Leftrightarrow$ $22p = (c - 1) \bmod 29 \Leftrightarrow$ $4 \times 22p = 4(c - 1) \bmod 29 \Leftrightarrow$ $p = 4(c - 1) \bmod 29$ <p>Logo, $f^{-1}(p) = 4(p - 1) \bmod 29 = (4p + 25) \bmod 29$</p>	<p>V4: $f(n) = (6n + 1) \bmod 29$</p> <p>Como $\text{mdc}(6,29) = 1$ os números 6 e 29 são primos entre si, portanto é possível calcular o inverso de 6 módulo 29.</p> <p>Pelo algoritmo da divisão temos que</p> $29 = 6 \times 4 + 5 \quad \text{e} \quad 6 = 5 \times 1 + 1$ <p>Donde,</p> $1 = 6 - 5 \times 1 = 6 - (29 - 6 \times 4)$ $= 6 - 29 + 6 \times 4$ $= 6 \times 5 - 29$ <p>Portanto, $x = 5$ é o inverso de 6 módulo 29.</p> $f(p) = (6p + 1) \bmod 29 \Leftrightarrow c = (6p + 1) \bmod 29$ $\Leftrightarrow c - 1 = 6p \bmod 29 \Leftrightarrow$ $6p = (c - 1) \bmod 29 \Leftrightarrow$ $5 \times 6p = 5(c - 1) \bmod 29 \Leftrightarrow$ $p = 5(c - 1) \bmod 29$ <p>Logo, $f^{-1}(p) = 5(p - 1) \bmod 29 = (5p + 24) \bmod 29$</p>

 	Tipo de Prova Teste 2	Ano letivo 2018/2019	Data 29-05-2019
	Curso Licenciatura em Segurança Informática de Redes de Computadores Licenciatura em Engenharia Informática		Hora 15:10
	Unidade Curricular Matemática Discreta		Duração 1,5 horas

N.º de aluno: _____ Nome: _____

6.3. Desencrpte a mensagem "FIZ", "BWO", "DUB", "NDU", "CTG", "TDQ".

				5.2 $f(n)=an+b \bmod 29$			
				Desencrpte			
					a	b	
I	O	T		F	I	Z	2 28
8	14	19		5	8	25	
A	F	K		B	W	O	3 28
0	5	10		1	22	14	
I	M	O		D	U	B	4 28
8	12	14		3	20	1	
C	K	I	10%	N	D	U	5 28
2	10	8	40%	13	3	20	
I	S	A		C	T	G	8 28
8	18	0		2	19	6	
K	O	S		T	D	Q	7 28
10	14	18		19	3	16	