```
--> M = [1 0 0 1 0;
  > 1 0 0 0 0;
  > 1 1 0 0 0;
  > 0 0 1 0 1;
  > 0 0 1 0 0];
```

Figura 1

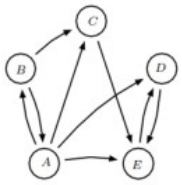
1. **[0.8]** Considere o código *Scilab*, apresentado na **Figura 1**, relativo à matriz de adjacência de um grafo. Podemos afirmar que o grafo:

☐ é de Hamilton ☐ é semi-Hamiltoniano
☐ não é nem semi-Hamiltoniano nem Hamiltoniano ☐ não é fortemente conexo

ou

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



Ps: tem uma pergunta sobre caminhos

5. Considere que a letra A corresponde a 0, a letra B corresponde a 1, e assim sucessivamente até à letra Z que corresponde a 25. Considere ainda um sistema RSA com $a = 13$ e $m = 43 \times 59 = 2537$ e os outputs do Scilab:

```
--> pmodulo(1904,2537)
 ans  =
   1904.
--> pmodulo(1904^13,2537)
 ans  =
   0.
--> pmodulo(194^13,2537)
 ans  =
  -7.037D+13
```

```
--> x=194; x_new=1;
--> for k=1:13
  > x_new=pmodulo(x*x_new,2537);
  > end
--> x_new
 x_new  =
   1077.
```

```
--> x=1904; x_new=1;
--> for k=1:13
  > x_new=pmodulo(x*x_new,2537);
  > end
--> x_new
 x_new  =
   1723.
```

Podemos afirmar que:

5.1. [0.8] a encriptação de "TE" é:

☐ "RX" ☐ "BFCD" ☐ "BAFF" ☐ "AA"

5.2. [0.8] sabendo que $b = 937$ é a chave privada, a desencriptação da mensagem "1206" consiste em calcular:

☐ $1206^{937} \bmod 2537$ ☐ $937^{1206} \bmod 2537$ ☐ $1206^{937} \bmod 2536$ ☐ $937^{1206} \bmod 2536$

4. Com base no fragmento de código Scilab 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

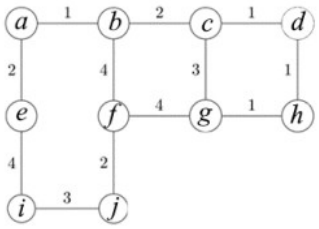
4.3 [1.0] existe o inverso de 539 modulo:

☐ 55 ☐ 150 ☐ 1287 ☐ nenhuma das anteriores

5. [1.0] Um inverso de 3 modulo 7 é:

☐ 2 ☐ 3 ☐ 4 ☐ 5

7.2 [1.5] 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.



---

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

162 * t + 372 * t

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 raíz $x_0 = 7$.

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.

11.1Encriptar “WIFI” f(n) = (15n+1) mod 29

11.2 Desincriptar “FIZ”

- F → 5
- I → 8
- Z → 25

---

2. Aplicar a função de desencriptação:

A função de desencriptação é:

E−1(y)=2(y−1)mod 29E^{-1}(y) = 2(y - 1) \mod 29E−1(y)=2(y−1)mod29

Para F → 5:

E−1(5)=2(5−1)mod 29=2×4=8mod 29=8E^{-1}(5) = 2(5 - 1) \mod 29 = 2 × 4 = 8 \mod 29 = 8E−1(5)=2(5−1)mod29=2×4=8mod29=8

Para I → 8:

E−1(8)=2(8−1)=2×7=14mod 29=14E^{-1}(8) = 2(8 - 1) = 2 × 7 = 14 \mod 29 = 14E−1(8)=2(8−1)=2×7=14mod29=14

Para Z → 25:

E−1(25)=2(25−1)=2×24=48mod 29=48−29=19E^{-1}(25) = 2(25 - 1) = 2 × 24 = 48 \mod 29 = 48 - 29 = 19E−1(25)=2(25−1)=2×24=48mod29=48−29=19

---

3. Converter os números de volta para letras:

- 8 → I
- 14 → O
- 19 → T

✅ **Resultado da desencriptação de “FIZ”:**

IOT