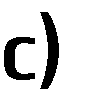
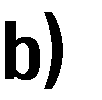
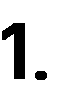
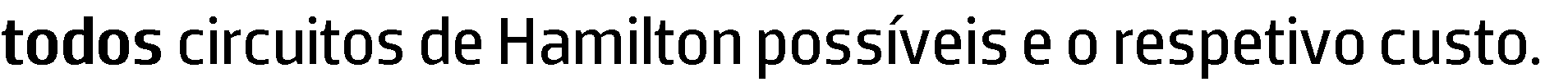
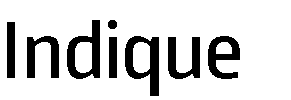
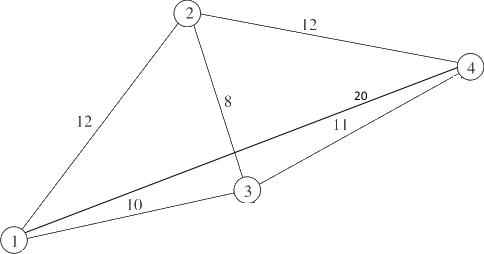
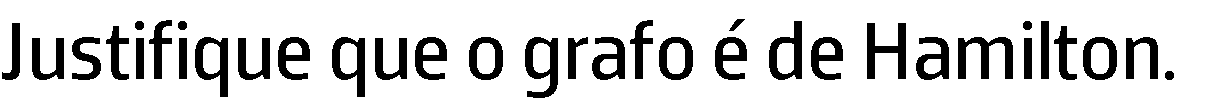
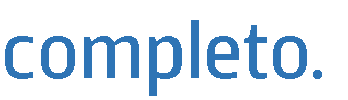
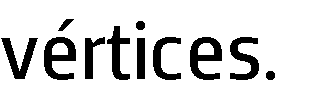
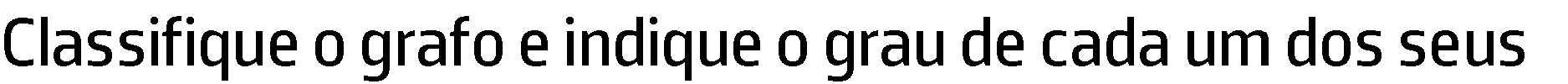
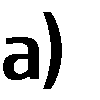
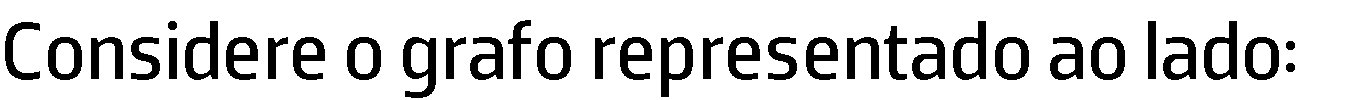
|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |





= 3! = 3

2



(𝑛−1)!

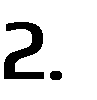
2

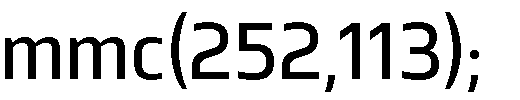
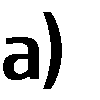
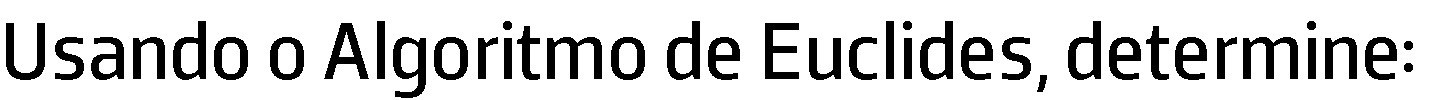








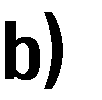




* 252 = 113 × 2 + 26
* 113 = 26 × 4 + 9
* 26 = 9 × 2 + 8
* 9 = 8 × 1 + 1

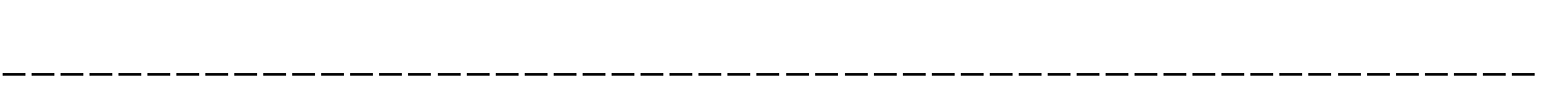
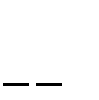
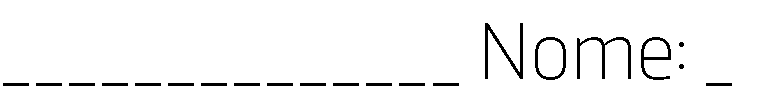
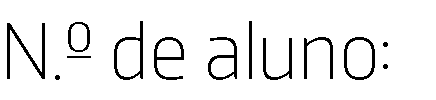
⟺ 28476 = 1 ×

⟺ 28476

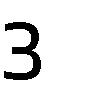
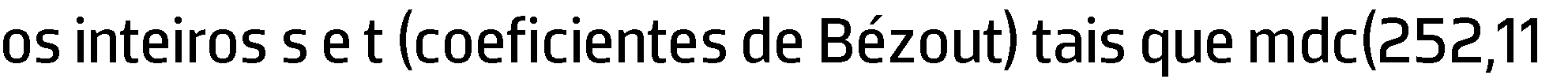
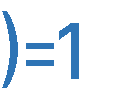
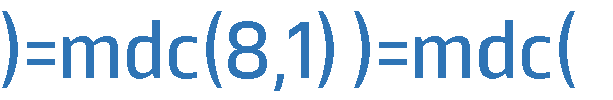


× 252 × 113

= 252 𝑠 + 113 𝑡

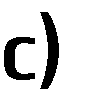


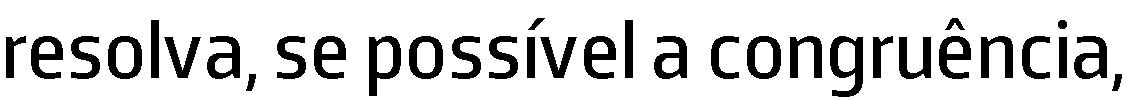
1 = 9 − 8 × 1



= 9 − (26 − 9 × 2) × 1 = 9 × 3 − 26 × 1

= (113 − 26 × 4) × 3 − 26 × 1 = 113 × 3 − 26 × 13

= 113 × 3 − (252 − 113 × 2) × 13 = 113 × 29 − 252 × 13



𝑠 = −13 = 29

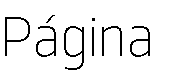
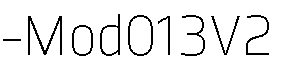
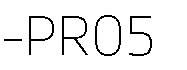
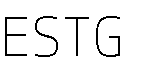
113𝑥 ≡ 1 mod 252



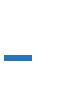
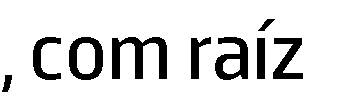
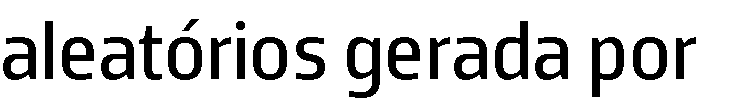
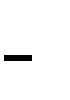
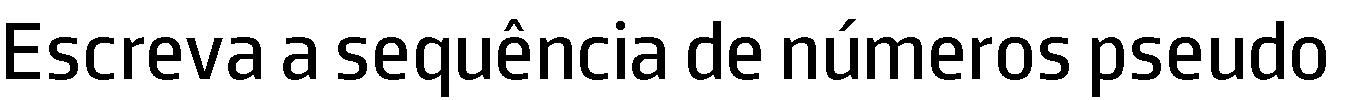
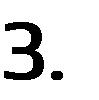
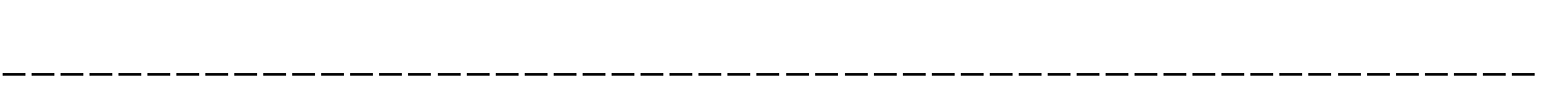
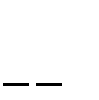
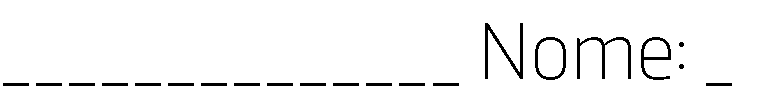
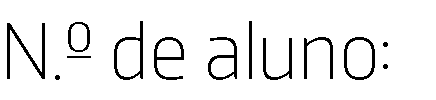
𝑡

113 × 29 − 252 × 13 = 1 ⇔ 113 × 29 = 252 × 13 + 1 ⇔ 113 × 29 ≡ 1 mod 252

𝑥 = 29







𝑥𝑛+1 = (7𝑥𝑛 + 3)mod 11

𝑥0 = 1

𝑥1 = (7𝑥0 + 3)mod 11 = (7 × 1 + 3)mod 11 = 10 mod 11 = 10

𝑥2 = (7𝑥1 + 3)mod 11 = (7 × 10 + 3)mod 11 = 73 mod 11 = 7

𝑥3 = (7𝑥2 + 3)mod 11 = (7 × 7 + 3)mod 11 = 52 mod 11 = 8

𝑥4 = (7𝑥3 + 3)mod 11 = (7 × 8 + 3)mod 11 = 4

𝑥5 = (7𝑥4 + 3)mod 11 = (7 × 4 + 3)mod 11 = 9

𝑥6 = (7𝑥5 + 3)mod 11 = (7 × 9 + 3)mod 11 = 0

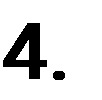
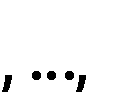
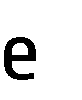
𝑥7 = (7𝑥6 + 3)mod 11 = (7 × 0 + 3)mod 11 = 3

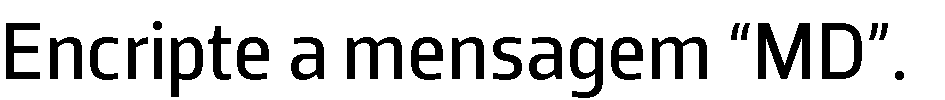
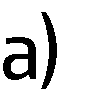
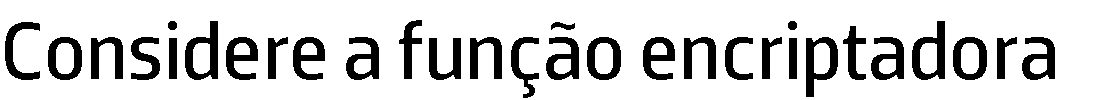
𝑥8 = (7𝑥7 + 3)mod 11 = (7 × 3 + 3)mod 11 = 2

𝑥9 = (7𝑥8 + 3)mod 11 = (7 × 2 + 3)mod 11 = 6

𝑥10 = (7𝑥9 + 3)mod 11 = (7 × 6 + 3)mod 11 = 1

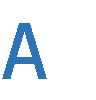
|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |

 𝑓(𝑛) = (7𝑛 + 3) mod 26 𝐴 ⟷ 0 𝑍 ⟷ 25

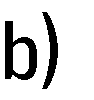
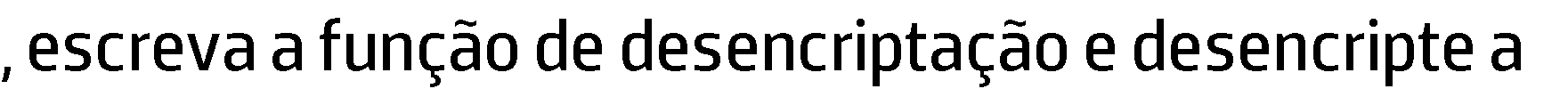


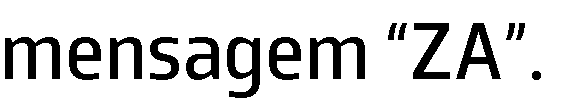
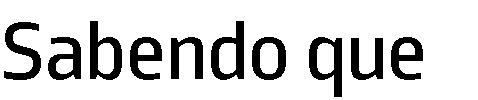
𝑓(𝑀) = 𝑓(12) = (7 × 12 + 3)mod26 = 9 ⟶ 𝐽

𝑓(𝐷) = 𝑓(3) = (7 × 3 + 3)mod26 = (21 + 3)mod 26 = 24 ⟶ 𝑌

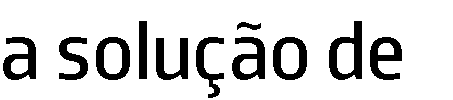
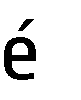


|  |  |
| --- | --- |
|  |  |

 7𝑥 ≡ 1 mod 26



𝑥 = 15



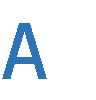
𝑝 = (7𝑛 + 3)mod26 ⇔ 7𝑛 = (𝑝 − 3)mod 26 ⇔ 15 × 7 𝑛 = 15(𝑝 − 3 + 26)mod 26

⇔ 𝑛 = 15(𝑝 + 23)mod 26

𝑓−1(𝑛) = 15(𝑛 + 23) mod 26

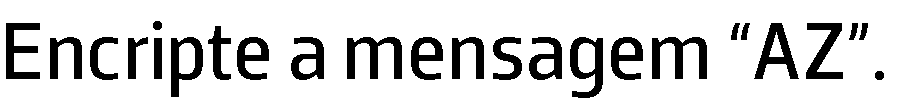
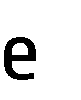
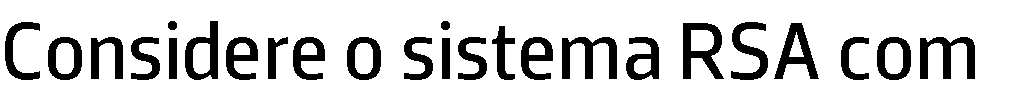
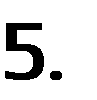
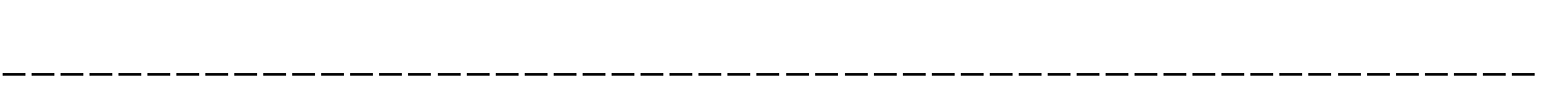
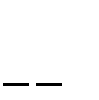
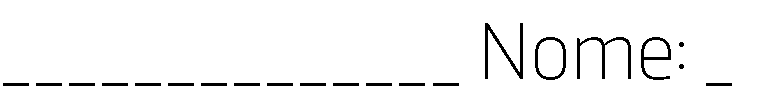
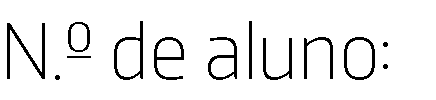
𝑓−1(𝑍) = 𝑓−1(25) = 15(25 + 23)mod26 = 15 × 48 mod 26 = 720 mod 26 = 18 ⟶ 𝑆

𝑓−1(𝐴) = 𝑓−1(0) = 15(0 + 23)mod26 = 15 × 23 mod 26 = 345 mod 26 = 7 ⟶ 𝐻



|  |  |
| --- | --- |
|  |  |

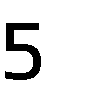
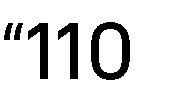
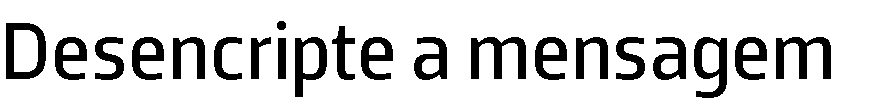
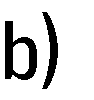
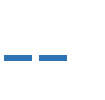
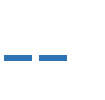
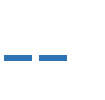
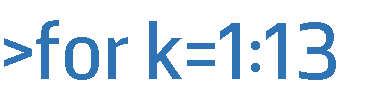
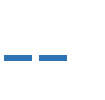
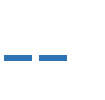
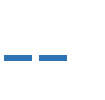
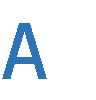




𝑚 = 43 × 59 = 2537 𝑎 = 13

𝑢(𝐴𝑍) = 𝑢(0025) = 002513mod 2537 = 1433

𝑎𝑏 mod 𝑛 = 1



13𝑏 mod (42 × 58) = 1 ⇔ 13𝑏 mod 2436 = 1 ⇔ ∃𝑘 ∈ 𝑍: 13𝑏 − 1 = 2436𝑘

⇔ ∃𝑘 ∈ ℤ: 13𝑏 − 2436𝑘 = 1



2436 = 187 × 13 + 5

13 = 5 × 2 + 3

5 = 3 × 1 + 2

3 = 2 × 1 + 1

1 = 3 − 2 × 1

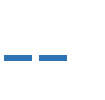
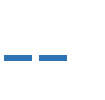
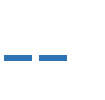
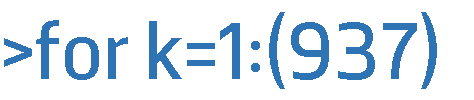
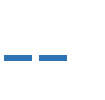
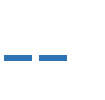
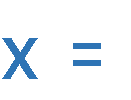
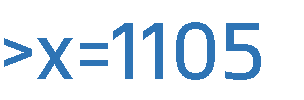
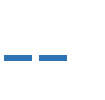
⇔ 1 = 3 − (5 − 3 × 1) × 1 = 3 × 2 − 5 × 1

⇔ 1 = (13 − 5 × 2) × 2 − 5 × 1 = 13 × 2 − 5 × 5

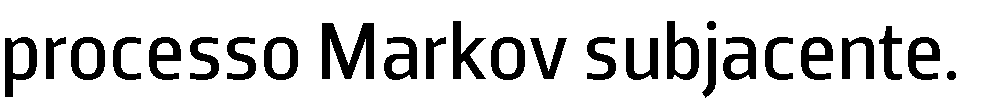
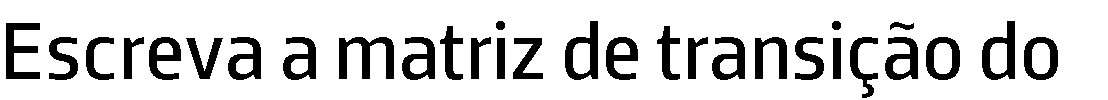
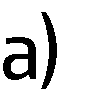
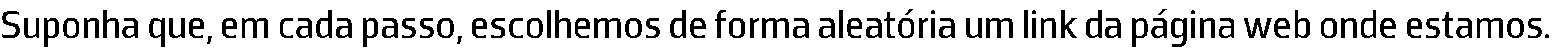
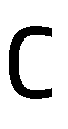
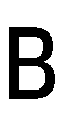
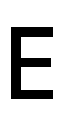
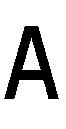
⇔ 1 = 13 × 2 − 5 × (2436 − 13 × 187) = 13 × 937 + 2436 × (−5)



1105937mod 2537 = 69



|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  | |  |
|  | |  |



1 1 1

0 1

2 3 2

1

2

𝑇 =

0 1 0 0

3

1

0 0 0 0

2

1 1

0

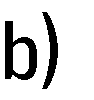
2 3

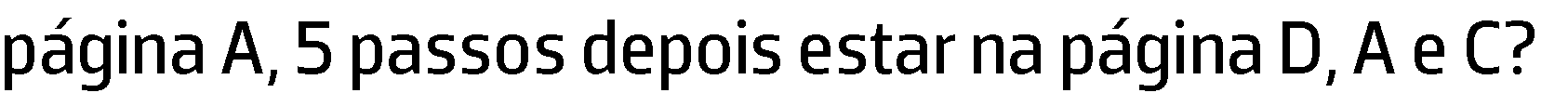
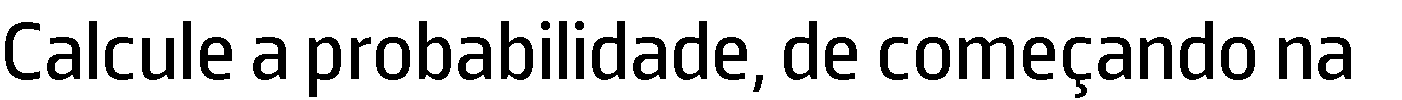
0 1

2

[ 0 0 0 0 0 ]

|  |  |
| --- | --- |
|  |  |

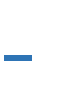




𝑇5 ×

1

0 0



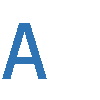
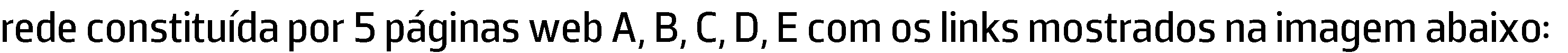
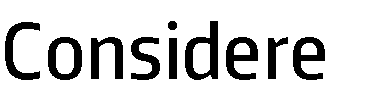
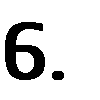
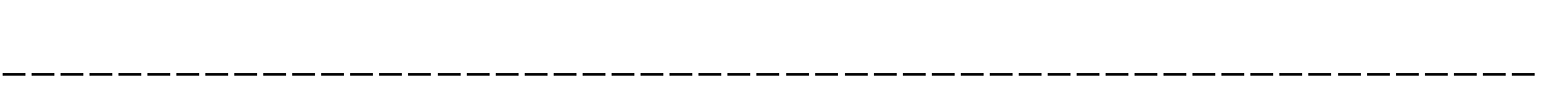
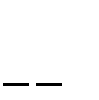
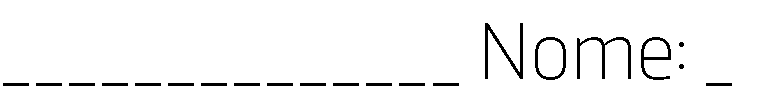
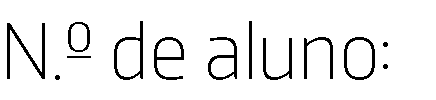
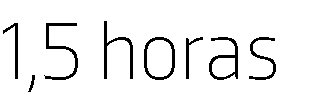
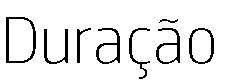
0

0.1388889

0.4201389 0.0208333

0.4201389

[0] [ 0 ]









|  |  |
| --- | --- |
|  |  |

