m.n.

Avaliação

Teste 1 - 18 maio	30%
Teste 2 - 1 junho	35%
Teste 3 - 15 junho	35%

dia 28 junho podemos recuperar os testes que queremos

→ Arranjar PDF do livro

Somatórios

Cálculo de formas fechadas

Cálculo finito

u_k sucessão

Definição
A derivada finita de u_k no ponto k é

$$(u_k)' = u_{k+1} - u_k$$

notação
no livro
$\Delta u_k = (u_k)'$

ex:

- $u_k = k^2$

$$(u_k)' = u_{k+1} - u_k = (k+1)^2 - k^2 = k^2 + 2k + 1 - k^2 = 2k + 1$$

$f(x) = x^2$
$f'(x) = 2x$

- $u_k = 3k$

$$(u_k)' = \underbrace{3(k+1)}_{u_{k+1}} - \underbrace{3k}_{u_k} = 3k + 3 - 3k = 3$$

$f(x) = 3x$
$f'(x) = 3$

Teorema Fundamental do Cálculo Finito (TFCF)

$n, p \in \mathbb{N}, n \geq p$

$$\sum_{k=p}^{n} (u_k)' = u_{n+1} - u_p$$

justificação

$$\sum_{k=p}^{n} (u_k)' = \sum_{k=p}^{n} (u_{k+1} - u_k) =$$

$$= (u_{p+1} - u_p) + (u_{p+2} - u_{p+1}) + (u_{p+3} - u_{p+2}) + \ldots + (u_n - u_{n-1}) + (u_{n+1} - u_n)$$

($k = p$; $k = p+1$; $k = p+2$; $k = n-1$; $k = n$)

$$= u_{n+1} - u_p$$

Potência factorial de expoente $r \in \mathbb{N}$ e base U_k

Definição

- $U_k^{\underline{0}} = 1$
- $U_k^{\underline{1}} = U_k$
- $r \in \mathbb{N}$, $U_k^{\underline{r}} = U_k \times U_{k-1} \times U_{k-2} \times \dots \times U_{k-(r-1)}$

ex:

- $U_k = 2k$

$(U_k)^{\underline{4}} = U_k \times U_{k-1} \times U_{k-2} \times U_{k-3} = 2k \times 2(k-1) \times 2(k-2) \times 2(k-3) =$

$= 2k(2k-2)(2k-4)(2k-6) = (4k^2-4k)(4k^2 - \underbrace{12k - 8k}_{-20k} + 24) =$

$= 16k^4 - 80k^3 + 96k^2 - 16k^3 + 80k^2 - 96k = 16k^4 - 96k^3 + 176k^2 - 96k$

- $U_k = k+1$

$(U_k)^{\underline{3}} = U_k \times U_{k-1} \times U_{k-2} = (k+1) \times k \times (k-1) = (k^2 - 1^2)k = k^3 - k$

Caso particular

$U_k = k$

- $k^{\underline{0}} = 1$
- $k^{\underline{r}} = k \times (k-1) \times (k-2) \times \dots \times (k-(r-1))$

$$\left.\frac{x}{x+1}\right|_a^b = \frac{b}{b+1} - \frac{a}{a+1}$$

$$\left[\frac{x}{x+1}\right]_a^b = \frac{b}{b+1} - \frac{a}{a+1}$$

notação

Teorema

$n, p \in \mathbb{N}$, $n \geq p$, $r \in \mathbb{N}$

$$\sum_{k=p}^{n-1} k^{\underline{r}} = \left[\frac{k^{\underline{r+1}}}{r+1}\right]_p^{n+1}$$

Justificação (pag. 282-283)

$U_k = k^{\underline{r+1}}$ $\quad (U_k)' = U_{k+1} - U_k = (k+1)^{\underline{r+1}} - k^{\underline{r+1}} =$

$= (k+1) \times \underbrace{k \times \dots \times (k+1-r)} - \underbrace{k(k-1) \times \dots \times (k-(r-1)) \times (k-r)} =$

$= k \times (k-1) \times \dots \times (k-(r-1)) \times ((k+1) - (k-r)) =$

$= (r+1) \times \underbrace{(K \times (K-1) \times \ldots \times (K-(r-1))}_{K^{\underline{r}}} =$

$= (r+1) \times K^{\underline{r}}$

$\therefore U_K = K^{\underline{r+1}} \Rightarrow (U_K)' = (r+1) \times K^{\underline{r}}$

$U_{n+1} - U_p \overset{TSCF}{=} \sum_{K=p}^{n} (U_K)' = \sum_{K=p}^{n} ((r+1) \times K^{\underline{r}})$

$\Downarrow$

$U_{n+1} - U_p = (r+1) \sum_{K=p}^{n} K^{\underline{r}}$

$\Downarrow$

$\frac{U_{n+1} - U_p}{r+1} = \sum_{K=p}^{n} K^{\underline{r}}$

$\Downarrow$

$\left[\frac{U_K}{r+1} \right]_p^{n+1} = \sum_{K=p}^{n} K^{\underline{r}}$

$\Downarrow$

$\left[\frac{K^{\underline{r+1}}}{r+1} \right]_p^{n+1} = \sum_{K=p}^{n} K^{\underline{r}}$

Método baseado em potências factoriais de expoente em $\mathbb{N}$

- útil para somatórios $\sum_{K=p}^{n} U_K$ onde U_K é um polinómio
- baseia-se na noção de potência factorial de expoente $r \in \mathbb{N}$
  - (i) transforma-se U_K num monómio factorial (potência factorial $K^{\underline{r}}$ com $r \in \mathbb{N}$) ou polinómio factorial (combinação linear destas potências)
  - (ii) usa-se

$$\sum_{K=p}^{n} K^{\underline{r}} = \left[\frac{K^{\underline{r+1}}}{r+1} \right]_p^{n+1}$$

ex:

- $\sum_{K=1}^{n} (K^2 - K) = \sum_{K=1}^{n} K^{\underline{2}} = \left[\frac{K^{\underline{3}}}{3} \right]_1^{n+1} = \left[\frac{K \times (K-1) \times (K-2)}{3} \right]_1^{n+1} =$

(i) $K^2 - K = K(K-1) = K^{\underline{2}}$

$= \frac{(n+1) \times n \times (n-1)}{3} - \frac{1 \times 0 \times (-1)}{3}$ (vai ser sempre 0)

- $\sum_{K=1}^{n} (5K^3 + K^2 + K) = \sum_{K=1}^{n} (5K^3 + 16K^2 + 7K^1) = \underbrace{5 \sum_{K=1}^{n} K^3}_{A} + \underbrace{16 \sum_{K=1}^{n} K^2}_{B} + \underbrace{7 \sum_{K=1}^{n} K^1}_{C}$

(i) $5K^3 + K^2 + K = K(5K^2 + K + 1) = K((K-1)(5K+6)+7) =$

	5	1	1
1		5	6
	5	6	7
2		10	
	5	16	

coef de K^1; coef de K^2; coef de K^3

$= K((K-1)(5K+6)+7K) = K^2((K-1)(5K+6)+7K^1) =$

$= K(K-1)((K-2)5 + 16) + 7K^1 =$

$= 5K(K-1)(K-2) + 16K(K-1) + 7K^1 =$

$= 5K^3 + 16K^2 + 7K^1$

arc

(*) $C = \left[\frac{K^2}{2}\right]_1^{n+1} = \left[\frac{K(K-1)}{2}\right]_1^{n+1} = \frac{(n+1)n}{2}$ - ✗

B = ver ex anterior

$A = \left[\frac{K^4}{4}\right]_1^{n+1} = \left[\frac{K(K-1)(K-2)(K-3)}{4}\right]_1^{n+1} =$

$= \frac{(n+1)n(n-1)(n-2)}{4}$

a resposta fica assim

$$\sum_{K=1}^{n}(5K^3+K^2+K+4) = \underbrace{\sum_{K=1}^{n}(5K^3+K^2+K)}_{\text{ver ex. anterior}} + \underbrace{\sum_{K=1}^{n}4}_{=4n}$$

Lista 1 ex

(4.1)

d) $\sum_{K=0}^{n-1}(4K^3-7K^2+K) = \sum_{K=0}^{n-1}(4K^3+5K^2-2K^1) = 4\underbrace{\sum_{K=0}^{n-1}K^3}_{A} + 5\underbrace{\sum_{K=0}^{n-1}K^2}_{B} - 2\underbrace{\sum_{K=0}^{n-1}K^1}_{C}$

(1) $4K^3-7K^2+K = K(4K^2-7K+1) = 4K^3+5K^2-2K^1$

	4	-7	1
1		4	-3
	4	-3	-2
2		8	
	4	5	

$A = \left[\frac{K^4}{4}\right]_0^n = \left[\frac{K(K-1)(K-2)(K-3)}{4}\right]_0^n =$

$= \frac{n(n-1)(n-2)(n-3)}{4}$ - ✗

$B = \left[\frac{K^3}{3}\right]_0^n = \left[\frac{K(K-1)(K-2)}{3}\right]_0^n = \frac{n(n-1)(n-2)}{3}$ - ✗

$C = \left[\frac{K^2}{2}\right]_0^n = \left[\frac{K(K-1)}{2}\right]_0^n = \frac{n(n-1)}{2}$ - ✗

Problemas ✦✦ Método da perturbação direta

05/05/2023

Lista 1

(2.1)

a) $\sum_{K=0}^{n}3^K$ $\quad S = \sum_{K=0}^{n}3^K + 3^{n+1}$

$\sum_{K=0}^{n+1}3^K \rightarrow 3^0 + \sum_{K=1}^{n+1}3^K \underset{K\to K-1}{=} 1 + \sum_{K=0}^{n}3^{K+1} = 1 + \sum_{K=0}^{n}3\times3^K = 1+3\underbrace{\sum_{K=0}^{n}3^K}_{S}$

$3^0 + 3^1 + \ldots + 3^n + 3^{n+1}$

$S+3^{n+1} = 1+3S \Leftrightarrow -2S = 1-3^{n+1} \Leftrightarrow S = \frac{1-3^{n+1}}{-2} = \frac{3^{n+1}-1}{2}$

$\sum_{k=0}^{n} a^k = \frac{a^{n+1}-1}{a-1}$, $a \in \mathbb{R} \setminus \{1\}$

d) $\sum_{k=0}^{n} k3^k$

$\sum_{k=0}^{n+1} k3^k = \begin{cases} \rightarrow \underbrace{\sum_{k=0}^{n} k3^k}_{S} + (n+1)3^{n+1} \\ \rightarrow 0\times 3^0 + \sum_{k=1}^{n+1} k3^k = \sum_{k=0}^{n} (k+1)3^{k+1} = 3\left[\underbrace{\sum_{k=0}^{n} k3^k}_{S} + \sum_{k=0}^{n} 3^k\right] = \end{cases}$

$0\times 3^0 + 1\times 3^1 + \ldots + n3^n + (n+1)3^{n+1}$

$= 3\sum_{k=0}^{n} k3^k + 3\times\frac{3^{n+1}-1}{2}$

$S + (n+1)3^{n+1} = 3S + 3\times\frac{3^{n+1}-1}{2} \Leftrightarrow -2S = 3\times\frac{3^{n+1}-1}{2} - (n+1)3^{n+1} \Leftrightarrow$

$\Leftrightarrow -2S = \frac{3}{2}(3^{n+1}-1) - (n+1)3^{n+1} \Leftrightarrow S = -\frac{3}{4}(3^{n+1}-1) + \frac{(n+1)3^{n+1}}{2}$ //

n vale e sem simplificar

e) $\sum_{k=0}^{n} \frac{k}{3^k}$

$\sum_{k=0}^{n+1} k3^{-k} = \begin{cases} \rightarrow \underbrace{\sum_{k=0}^{n} k3^{-k}}_{S} + (n+1)3^{-(n+1)} \\ \rightarrow 0 + \sum_{k=1}^{n+1} k3^{-k} = \sum_{k=0}^{n} (k+1)3^{-(k+1)} = \frac{1}{3}\sum_{k=0}^{n} (k3^{-k} + 3^{-k}) = \end{cases}$

$= \frac{1}{3}\left(\sum_{k=0}^{n} k3^{-k} + \sum_{k=0}^{n} 3^{-k}\right) = \frac{1}{3}\underbrace{\sum_{k=0}^{n} k3^{-k}}_{S} + \frac{1}{3}\frac{\left(\frac{1}{3}\right)^{n+1}-1}{1-\frac{1}{3}}$

$S + (n+1)3^{-(n+1)} = \frac{1}{3}S + \frac{\left(\frac{1}{3}\right)^{n+1}-1}{2} \Leftrightarrow \frac{2}{3}S = \frac{\left(\frac{1}{3}\right)^{n+1}-1}{2} - (n+1)3^{-(n+1)}$

$\Leftrightarrow S = \frac{3}{4}\left(\left(\frac{1}{3}\right)^{n+1}-1\right) - \frac{3}{2}(n+1)3^{-(n+1)}$

f) $\sum_{k=1}^{n} (-1)^k k$

$\sum_{k=1}^{n+1} (-1)^k k = \begin{cases} \rightarrow \underbrace{\sum_{k=1}^{n} (-1)^k k}_{S} + (-1)^{n+1}(n+1) \\ \rightarrow -1 + \sum_{k=2}^{n+1} (-1)^k k = -1 + \sum_{k=1}^{n} (-1)^{k+1}(k+1) = \end{cases}$

$= -1 - \sum_{k=1}^{n} ((-1)^k k + (-1)^k) = -1 - \left(\sum_{k=1}^{n} (-1)^k k + \sum_{k=1}^{n} (-1)^k\right) =$

$= -1 - \underbrace{\sum_{k=1}^{n} (-1)^k k}_{S} - \left(\frac{(-1)^{n+1}-1}{-2} - 1\right)$

$(-1)^k(k+1) = -k + (-1)^k$

$\sum_{k=1}^{n} (-1)^k = \sum_{k=0}^{n} (-1)^k - (-1)^0 = \frac{(-1)^{n+1}-1}{-2} - 1$

arc

$$S + (-1)^{n+1}(n+1) = -1 - S - \left(\frac{(-1)^{n+1}-1}{-2} - 1\right) \Leftrightarrow$$

$$\Leftrightarrow 2S = (-1)^{n+1}(n+1)\left(\cancel{-1} + \frac{(-1)^{n+1}-1}{2} + \cancel{1}\right) \Leftrightarrow S = \frac{(-1)^{n+1}(n+1)}{2} \times \frac{(-1)^{n+1}-1}{2}$$

b) $\sum_{k=2}^{n} 3^{-k}$

$$\sum_{k=2}^{n+1} 3^{-k} = \begin{cases} \sum_{k=2}^{n} 3^{-k} + 3^{-(n+1)} \\ 3^{-2} + \sum_{k=3}^{n+1} 3^{-k} = \frac{1}{9} + \sum_{k=2}^{n} 3^{-(k+1)} = \frac{1}{9} + \frac{1}{3}\underbrace{\sum_{k=2}^{n} 3^{-k}}_{S} \end{cases}$$

$$S + 3^{-(n+1)} = \frac{1}{9} + \frac{1}{3}S \Leftrightarrow \frac{2}{3}S = \frac{1}{9} - 3^{-(n+1)} \Leftrightarrow S = \frac{1}{2} - \frac{3}{2}3^{-(n+1)}$$

2.2

c) $\sum_{k=0}^{n} k^3$

$$\sum_{k=0}^{n+1} k^3 = \begin{cases} \sum_{k=0}^{n} k^3 + (n+1)^3 \quad S \\ 0^3 + \sum_{k=1}^{n+1} k^3 = \sum_{k=0}^{n} (k+1)^3 = \sum_{k=0}^{n} (k^3 + 3k^2 + 3k + 1) = \end{cases}$$

$$= \underbrace{\sum_{k=0}^{n} k^3}_{S} + 3\sum_{k=0}^{n} k^2 + 3\sum_{k=0}^{n} k + \sum_{k=0}^{n} 1 \qquad \cancel{S} + (n+1)^3 = \cancel{S} + 3\sum_{k=0}^{n} k^2 + 3\underbrace{\sum_{k=0}^{n} k}_{\frac{n(n+1)}{2}} + (n+1)$$

$$\boxed{\sum_{k=10}^{n} a^k = \sum_{k=0}^{n-10} a^{k+10} = a^{10}\sum_{k=0}^{n-10} a^k = \frac{a^{n-9}-1}{a-1}}$$

b) $\sum_{k=0}^{n} k^2$

vamos começar com k^3

$$\sum_{k=0}^{n+1} k^3 = \begin{cases} \sum_{k=0}^{n} k^3 + (n+1)^3 \quad S \\ 0^3 + \sum_{k=1}^{n+1} k^3 = \sum_{k=0}^{n} (k+1)^3 = \sum_{k=0}^{n} (k^3 + 3k^2 + 3k + 1) = \end{cases}$$

perturbação indireta
no teste a stora não pede pq dá para fazer c/ potências fatoriais

$$= \underbrace{\sum_{k=0}^{n} k^3}_{S} + 3\sum_{k=0}^{n} k^2 + 3\sum_{k=0}^{n} k + \sum_{k=0}^{n} 1$$

$$\cancel{S} + (n+1)^3 = \cancel{S} + 3\sum_{k=0}^{n} k^2 + 3\underbrace{\sum_{k=0}^{n} k}_{\frac{n(n+1)}{2}} + (n+1) \Leftrightarrow$$

$$\Leftrightarrow (n+1)^3 - 3\frac{n(n+1)}{2} - (n+1) = 3\sum_{k=0}^{n} k^2 \Leftrightarrow$$

$$\Leftrightarrow \sum_{k=0}^{n} k^2 = \frac{1}{3}\left((n+1)^3 - 3\frac{n(n+1)}{2} - (n+1)\right)$$

a) $\sum_{k=0}^{n} k$ usar perturbação indicada

usar perturbação direta aplicada a $\sum_{k=0}^{n} k^2$

$\sum_{k=0}^{n+1} k^2 \begin{cases} \to \sum_{k=0}^{n} k^2 + (n+1)^2 \\ \to 0^2 + \sum_{k=1}^{n+1} k^2 = \sum_{k=0}^{n} (k+1)^2 = \sum_{k=0}^{n} (k^2+2k+1) = \end{cases}$

$= \underbrace{\sum_{k=0}^{n} k^2}_{S} + 2\sum_{k=0}^{n} k + \sum_{k=0}^{n} 1 \quad \to n+1$

$S + (n+1)^2 = S + 2\sum_{k=0}^{n} k + (n+1) \Leftrightarrow 2\sum_{k=0}^{n} k = (n+1)^2 - (n+1) \Leftrightarrow$

$\Leftrightarrow \sum_{k=0}^{n} k = \frac{(n+1)(n+1-1)}{2} \Leftrightarrow \sum_{k=0}^{n} k = \frac{(n+1)n}{2}$ //

Recordar

U_k sucessão

$(U_k)' = U_{k+1} - U_k$

ΔU_k

TFCF

$\sum_{k=p}^{n} (U_k)' = U_{n+1} - U_p$

08/05/2023

Derivadas finitas

$\Delta k^2 \leftarrow (k^2)' = 2k+1$

$(ak)' = a \quad a \in \mathbb{R}$

$(a^k)' = \underbrace{a^{k+1}}_{U_{k+1}} - \underbrace{a^k}_{U_k} = a^k(a-1)$

$(k!)' = \underbrace{(k+1)!}_{U_{k+1}} - \underbrace{k!}_{U_k} = k!(k+1-1) = k!k$

FICHA 9

5.1

a) $\sum_{k=0}^{n} (2k+1) = \sum_{k=0}^{n} (k^2)' = (n+1)^2 - 0^2 = (n+1)^2$ (TFCF)

$\sum_{k=0}^{n} \Delta k^2$

a) $\sum_{k=0}^{n} 10^k = \sum_{k=0}^{n} \frac{9 \times 10^k}{9} = \frac{1}{9}\sum_{k=0}^{n} 9 \times 10^k = \frac{1}{9}\sum_{k=0}^{n} (10^k)' = \frac{1}{9}(10^{n+1} - 10^0)$

5.2

a) $\sum_{k=1}^{n} \frac{k^2+5k+2}{k^2(k+1)^2} = \sum_{k=1}^{n} -\left(\frac{k+2}{k^2}\right)' \overset{\text{TFCF}}{=} -\left(\frac{n+3}{(n+1)^2} - \frac{3}{1}\right)$

Seguir a sugestão $U_k = \frac{k+2}{k^2}$

$(U_k)' = \frac{k+3}{(k+1)^2} - \frac{k+2}{k^2} = \frac{k^2(k+3) - (k+1)^2(k+2)}{k^2(k+1)^2} = \frac{k^3+3k^2 - k^3 - 2k^2 - 2k^2 - 4k - k - 2}{k^2(k+1)^2} =$

$= \frac{-k^2-5k-2}{k^2(k+1)^2} = -\frac{k^2+5k+2}{k^2(k+1)^2} \Rightarrow \frac{k^2+5k+2}{k^2(k+1)^2} = -\left(\frac{k+2}{k^2}\right)'$

arc

(3.2)

b) $\underbrace{(u_n+v_n)}_{w_n}' = w_{n+1} - w_n = (u_{n+1}+v_{n+1}) - (u_n+v_n) = u_{n+1} - u_n + v_{n+1} - v_n = (u_n)' + (v_n)'$

c) $(\underbrace{u_n \times v_n}_{w_n})' = w_{n+1} - w_n = u_{n+1} \times v_{n+1} - u_n \times v_n = \underbrace{u_{n+1} \times v_{n+1} - u_n v_{n+1}}_{(u_{n+1}-u_n)v_{n+1}} + \underbrace{u_n v_{n+1} - u_n v_n}_{u_n(v_{n+1}-v_n)} =$

$= (u_n)' \times v_{n+1} + u_n \times (v_n)'$

(5.1)

i) $\sum_{k=0}^{n} 2^k (2k+1) k! = \sum_{k=0}^{n} \underbrace{(2^{k+1} k! k}_{u_{k+1}} + \underbrace{2^k k!}_{(v_k)'}) = \sum_{k=0}^{n} (k!\, 2^k)' \underset{TFC}{=} (n+1)! \, 2^{n+1} - \underbrace{0! \, 2^0}_{=1}$

$v_k = 2^k \quad (v_k)' = 2^k$

$u_k = k! \quad (u_k)' = k! \, k$

h) $\sum_{k=0}^{n} (\underbrace{(k+1)!}_{v_{k+1}} + \underbrace{k^2 k!}_{k\,k!\,k}) = \sum_{k=0}^{n} (k \times k!)' = (n+1)(n+1)! - \underbrace{0 \times 0!}_{=0} = (n+1)(n+1)!$

$v_k = k! \quad (v_k)' = k!\,k \quad v_{k+1} = (k+1)!$

$u_k = k \quad (k)' = k+1-k = 1$

Fórmula de Abel

$n, p \in \mathbb{N}$, $n \geq p$, u_k, v_k sucessões

$$\sum_{k=p}^{n} u_k (v_k)' = [u_k v_k]_p^{n+1} - \sum_{k=p}^{n} (u_k)' v_{k+1}$$

Demonstração

$(u_k \times v_k)' = (u_k)' \times v_{n+1} + u_n \times (v_n)'$

$\sum_{k=p}^{n} (u_k \times v_k)' = \sum_{k=p}^{n} ((u_k)' \times v_{k+1} + u_k (v_k)') = \sum_{k=p}^{n} (u_k)' v_{k+1} + \sum_{k=p}^{n} u_k (v_k)'$

$[u_k \times v_k]_p^{n+1}$

FICHA 1

(6.2)

b) $\sum_{k=0}^{n} k 3^k = \sum_{k=0}^{n} k \times \frac{2 \times 3^k}{2} = \frac{1}{2} \sum_{k=0}^{n} \underbrace{k}_{u_k} \times \underbrace{2 \times 3^k}_{(v_k)'} \underset{\text{fórmula de Abel}}{=} \frac{1}{2} \left([k \times 3^k]_0^{n+1} - \sum_{k=0}^{n} 1 \times 3^{k+1} \right) =$

$v_k = 3^k \quad (u_k)' = 1$

$= \frac{1}{2} \left((n+1)3^{n+1} - 3 \sum_{k=0}^{n} 3^k \right) \rightarrow \frac{3^{n+1}-1}{2}$

c) $\sum_{k=0}^{n} k^2 3^k = \frac{1}{2} \sum_{k=0}^{n} \underbrace{(k^2}_{u_k} \underbrace{2 \times 3^k)}_{(v_k)'} \underset{\text{fórmula de Abel}}{=} \frac{1}{2} \left([k^2 \times 3^k]_0^{n+1} - \sum_{k=0}^{n} \frac{(2k+1) 3^{k+1}}{2k 3^{k+1} + 3^{k+1}} \right) =$

$v_k = 3^k \quad u_k = k^2 \quad (u_k)' = 2k+1$

$= \frac{1}{2} \left((n+1)^2 3^{n+1} - 3 \left(\underbrace{2 \sum_{k=0}^{n} k 3^k}_{\text{ex. anterior}} + \underbrace{\sum_{k=0}^{n} 3^k}_{\text{prog. geométrica}} \right) \right)$

Problemas

08/05/2023

Potência fatorial de expoente $r \in \mathbb{N}$ de u_k

$u_k^{\underline{0}} = 1$

$u_k^{\underline{r}} = u_k \times u_{k-1} \times u_{k-2} \times \dots \times u_{k-(r-1)}$

↳ $u_k = k$

$k^{\underline{r}} = k(k-1)(k-2)\dots(k-(r-1))$

$$\sum_{k=p}^{n} k^{\underline{r}} = \left[\frac{k^{\underline{r+1}}}{r+1} \right]_p^{n+1}$$

FICHA 4

regra de Ruffini = método de Horner

4.1

g) $\sum_{k=0}^{n}(3k^4 - 7k^2 + 4k) = \sum_{k=0}^{n}(3k^{\underline{4}} + 18k^{\underline{3}} + 14k^{\underline{2}}) = 3\sum_{k=0}^{n} k^{\underline{4}} + 18\sum_{k=0}^{n} k^{\underline{3}} + 14\sum_{k=0}^{n} k^{\underline{2}}$ (A) (B) (C)

	3	0	−7	4
1		3	3	−4
	3	3	−4	0
2		6	18	
	3	9	14	
3		9		
	3	18		

i) $3k^4 - 7k^2 + 4k = k(3k^3 - 7k + 4) = 3k^{\underline{4}} + 18k^{\underline{3}} + 14k^{\underline{2}}$

$k(k-1)(k-2)(k-3) + k(k-1)(k-2) + k(k-1) + k$

(A) $3\sum_{k=0}^{n} k^{\underline{4}} = 3\left[\frac{k^{\underline{5}}}{5}\right]_0^{n+1} = \frac{3(n+1)n(n-1)(n-2)(n-3)}{5}$

(B) $18\sum_{k=0}^{n} k^{\underline{3}} = 18\left[\frac{k^{\underline{4}}}{4}\right]_0^{n+1} = \frac{18(n+1)n(n-1)(n-2)}{4}$

(C) $14\sum_{k=0}^{n} k^{\underline{2}} = 14\left[\frac{k^{\underline{3}}}{3}\right]_0^{n+1} = \frac{14(n+1)n(n-1)}{3}$

a) $\sum_{k=1}^{n}(5k^3 - 3k^2) = \sum_{k=1}^{n}(5k^{\underline{3}} + 12k^{\underline{2}} + 2k^{\underline{1}}) = 5\sum_{k=1}^{n} k^{\underline{3}} + 12\sum_{k=1}^{n} k^{\underline{2}} + 2\sum_{k=1}^{n} k^{\underline{1}}$ (A) (B) (C)

	5	−3	0
1		5	2
	5	2	12
2		10	
	5	12	

i) $5k^3 - 3k^2 = k(5k^2 - 3k) = 5k^{\underline{3}} + 12k^{\underline{2}} + 2k^{\underline{1}}$

(A) $5\sum_{k=1}^{n} k^{\underline{3}} = 5\left[\frac{k^{\underline{4}}}{4}\right]_1^{n+1} = \frac{5(n+1)n(n-1)(n-2)}{4} - \frac{1\times0\times(-1)(-2)}{4} = 0$

(B) $12\sum_{k=1}^{n} k^{\underline{2}} = 12\left[\frac{k^{\underline{3}}}{3}\right]_1^{n+1} = \frac{12(n+1)n(n-1)}{3} - \frac{1\times0\times(-1)}{3} = 0$

(C) $2\sum_{k=1}^{n} k^{\underline{1}} = 2\left[\frac{k^{\underline{2}}}{2}\right]_1^{n+1} = \frac{2(n+1)n}{2} - \frac{1\times0}{2} = 0$

b) $\sum_{k=0}^{n}(k^3 - 3k^2 + 2k) = \sum_{k=0}^{n} k^{\underline{3}} + \sum_{k=0}^{n} k^{\underline{2}} - \sum_{k=0}^{n} k^{\underline{1}} = \left[\frac{k^{\underline{4}}}{4}\right]_0^{n+1} + \left[\frac{k^{\underline{3}}}{3}\right]_0^{n+1} - \left[\frac{k^{\underline{2}}}{2}\right]_0^{n+1}$ (A) (B) (C)

	1	−3	2
1		1	−1
	1	−2	1
2		2	
	1	1	

i) $k^3 - 3k^2 + 2k = k(k^2 - 3k + 2) = k^{\underline{3}} + k^{\underline{2}} - k^{\underline{1}}$

(A) $\frac{(n+1)n(n-1)(n-2)}{4}$ (B) $\frac{(n+1)n(n-1)}{3}$ (C) $-\frac{(n+1)n}{2}$

arc

c) $\sum_{j=1}^{n}(j^3+2j)=\sum_{j=1}^{n}(j^3+3j^2+3j^1)=\sum_{j=1}^{n}j^3+3\sum_{j=1}^{n}j^2+3\sum_{j=1}^{n}j^1=$

$$\begin{array}{c|ccc} 1 & 0 & 2 \\ & 1 & 1 \\ \hline 1 & 1 & 3 \\ & 2 & 2 \\ \hline & 1 & 3 \end{array}$$

i) $j^3+2j-j(j^2+2)=j^3+3j^2+3j^1$

$=\left[\frac{j^4}{4}\right]_1^{n+1}+3\left[\frac{j^3}{3}\right]_1^{n+1}-3\left[\frac{j^2}{2}\right]_1^{n+1}$ (A) (B) (C)

(A) $\frac{(n+1)n(n-1)(n-2)}{4}$ (B) $\frac{3(n+1)n(n-1)}{3}$ $C=-\frac{3(n+1)n}{2}$

Recorra

$n,p,r\in\mathbb{N}$, $n\geq p$

$$\sum_{k=p}^{n}(ak+b)^k=\left[\frac{(ak+b)^{r+1}}{a(r+1)}\right]_p^{n+1}$$

k) $\sum_{k=1}^{n-1}\underbrace{(3k+2)}_{u_k}\underbrace{(3k-1)}_{u_{k-1}}\underbrace{(3k-4)}_{u_{k-2}}=\sum_{k=1}^{n-1}(3k+2)^3=\left[\frac{(3k+2)^4}{3\times4}\right]_1^n=\left[\frac{(3k+2)(3k-1)(3k-4)(3k-7)}{12}\right]_1^n=$

$=\frac{(3n+2)(3n-1)(3n-4)(3n-7)}{12}-\frac{5\times2\times(-1)(-4)}{12}$

e) $\sum_{k=0}^{n}(2k^3-3k^2+5k-4)=\sum_{k=0}^{n}(2k^3-3k^2+5k)+\underbrace{\sum_{k=0}^{n}(-4)}_{-4(n+1)}=$

$$\begin{array}{c|ccc} 2 & -3 & 5 \\ & 2 & -1 \\ \hline 2 & -1 & 4 \\ & 2 & 4 \\ \hline & 2 & 3 \end{array}$$

i) $2k^3-3k^2+5k=k(2k^2-3k+5)=2k^3+3k^2+4k^1$

$=2\sum_{k=0}^{n}k^3+3\sum_{k=0}^{n}k^2+4\sum_{k=0}^{n}k^1+4(n+1)=2\left[\frac{k^4}{4}\right]_0^{n+1}+3\left[\frac{k^3}{3}\right]_0^{n+1}+4\left[\frac{k^2}{2}\right]_0^{n+1}-4(n+1)$

(A) (B) (C)

$A=\frac{2(n+1)n(n-1)(n-2)}{4}$

$B=\frac{3(n+1)n(n-1)}{3}$ $C=4\frac{(n+1)n}{2}=2(n+1)n$

Potência factorial de expoente $r\in\mathbb{Z}\setminus\mathbb{N}$ e base u_k

$r\in\mathbb{N}_1$ $\quad u_k^{\underline{-r}}=\frac{1}{u_{k+1}\times u_{k+2}\times\ldots\times u_{k+r}}$

$u_k=k+5$

$(k+5)^{\underline{-2}}=\frac{1}{(k+6)(k+7)}$ (u_{k+1}, u_{k+2})

$u_k=2k$

$(2k)^{\underline{-4}}=\frac{1}{(2k+2)(2k+4)(2k+6)(2k+8)}$ (u_{k+1}, u_{k+2}, u_{k+3}, u_{k+4})

$\Rightarrow u_k=k$ $\quad k^{\underline{-r}}=\frac{1}{(k+1)(k+2)\ldots(k+r)}$

Teorema

$$\sum_{k=p}^{n} k^{\underline{r}} = \left[\frac{k^{\underline{r+1}}}{r+1}\right]_p^{n+1} \qquad \sum_{k=p}^{n} (ak+b)^{\underline{r}} = \left[\frac{(ak+b)^{\underline{r+1}}}{a(r+1)}\right]_p^{n+1}$$

$r \in \mathbb{N}$

FICHA 1

(5.2)

a) $$\sum_{k=0}^{n} \frac{2}{(k+1)(k+2)} = 2\sum_{k=0}^{n} \frac{1}{(k+1)(k+2)} = 2\sum_{k=0}^{n} k^{\underline{-2}} = 2\left[\frac{k^{\underline{-1}}}{-1}\right]_0^{n+1} = 2\left[-\frac{1}{k+1}\right]_0^{n+1} =$$

$$2\left(-\frac{1}{n+1} - \left(-\frac{1}{1}\right)\right)$$

b) $$\sum_{k=0}^{n-1} \frac{3k-2}{(k+1)(k+2)(k+3)} = 3\sum_{k=0}^{n-1} \frac{(k+3)-3}{(k+1)(k+2)(k+3)} = 2\sum_{k=0}^{n} \frac{1}{(k+1)(k+2)(k+3)} = 3\left(\sum_{k=0}^{n-1} \frac{1}{(k+1)(k+2)} - 3\sum_{k=0}^{n-1} \frac{1}{(k+1)(k+2)(k+3)}\right) -$$

$k^{\underline{-3}}$

$$-2\sum_{k=0}^{n-1} k^{\underline{-3}} = 3\underbrace{\sum_{k=0}^{n-1} k^{\underline{-2}}}_{\text{A: vec ex anteriores}} - 11\underbrace{\sum_{k=0}^{n-1} k^{\underline{-3}}}_{B}$$

onde $$B = \left[\frac{k^{\underline{-2}}}{-2}\right]_0^{n} = \left[-\frac{1}{2}\times\frac{1}{(k+1)(k+2)}\right]_0^{n} = -\frac{1}{2}\times\frac{1}{(n+1)(n+2)} - \left(-\frac{1}{2}\times\frac{1}{2}\right)$$

j) $$\sum_{k=0}^{n} \frac{1}{(5k+4)(5k-1)} = \sum_{k=0}^{n} (5k-6)^{\underline{-2}} = \left[\frac{(5k-6)^{\underline{-1}}}{5(-1)}\right]_0^{n+1} = \left[-\frac{1}{5}\times\frac{1}{5k-1}\right]_0^{n+1} =$$

u_{k+1} u_k

$$= -\frac{1}{5}\times\frac{1}{5n+4} - \left(-\frac{1}{5}\times\frac{1}{-1}\right)$$

c)

i) $$\sum_{k=1}^{n} \frac{3}{4k^2-1} = 3\sum_{k=1}^{n} \frac{1}{(2k)^2-1^2} = 3\sum_{k=1}^{n} \frac{1}{(2k-1)(2k+1)} = 3\sum_{k=1}^{n} (2k-2)^{\underline{-2}} = 3\left[\frac{(2k-2)^{\underline{-1}}}{2(-1)}\right]_1^{n+1} =$$

u_{k+1} u_{k+2} $u_k = 2k-2$

$$= 3\left[\frac{1}{2}\times\frac{1}{2k-1}\right]_1^{n+1} = 3\left(\frac{1}{2}\times\frac{1}{2n+1} - \left(-\frac{1}{2}\times\frac{1}{1}\right)\right)$$

HAP na 2ª hora da aula no AR
a 1ª hora é no auditório normal

11/05/2023

Funções Geradoras

Cap 6

- resolução de recorrências (relevante na análise de eficiência de algoritmos recursivos)
- problemas combinatórios

Definição

A função geradora da sucessão u_k é a série de potências

$$G_u(z) = \sum_{k=0}^{+\infty} u_k z^k$$

⇒ informalmente $u_0 + u_1 z + u_2 z^2 + u_3 z^3 + \ldots$ ("polinómio" infinito)

ex:

$u_k = 2k+1 \rightsquigarrow G_u(z) = \sum_{k=0}^{+\infty} (2k+1) z^k$

$u_k = k \rightsquigarrow G_u(z) = \sum_{k=0}^{+\infty} z^k$

$u_k = \begin{cases} 1 & \text{se múltiplo de 3} \\ 0 & \text{caso contrário} \end{cases} \rightsquigarrow 1 + 0z^1 + 0z^2 + z^3 + z^4 + z^5 = \sum_{k=0}^{1} z^{3k}$

$u_0 = 1 \quad u_1 = 0 \quad u_2 = 0 \quad u_3 = 1 \quad u_4 = 0 \quad u_5 = 0 \quad u_6 = 1$

u_k 0, 3, -5, 0, 7, 0, 0, 0, 0, 0, 0

$G_u(z) = \sum_{k=0}^{4} u_k z^k = 3z - 5z^2 + 7z^4$ — Qualquer polinómio é uma função geradora

4 → função geradora da sucessão 4, 0, 0, 0, 0, 0, 0

Em certas situações é possível representar uma função geradora através de uma expressão algébrica.

Forma fechada da função geradora

Soma de funções geradoras

u_k

$G_u(z) = \sum_{k=0}^{+\infty} u_k z^k \quad (= u_0 + u_1 z + u_2 z^2 + u_3 z^3 + \dots)$

v_k

$G_v(z) = \sum_{k=0}^{+\infty} v_k z^k \quad (= v_0 + v_1 z + v_2 z^2 + v_3 z^3 + \dots)$

$G_u(z) + G_v(z) = \sum_{k=0}^{+\infty} (u_k + v_k) z^k = (u_0 + v_0) + (u_1 + v_1) z + (u_2 + v_2) z^2 + \dots$

w_k

Comutativa — tem elemento neutro: função geradora da sucessão 0, 0, 0, 0, 0, 0, ... → 0

Associativa (tal como a soma de polinómios)

Multiplicação de funções geradoras

$G_u(z) \times G_v(z) = u_0 v_0 + (u_0 v_1 + u_1 v_0) z + (u_0 v_2 + u_1 v_1 + u_2 v_0) z^2 + (u_0 v_3 + u_1 v_2 + u_2 v_1 + u_3 v_0) z^3 + \dots = \sum_{k=0}^{+\infty} \left(\sum_{j=0}^{k} u_j v_{k-j} \right) z^k$

Comutativa
Associativa
Distributiva em relação à soma

Tem elemento neutro $1 \to FG$ da sucessão $1, \underbrace{0}_{v_1}, \underbrace{0}_{v_2}, 0, 0, \ldots$

ex:

$U_K = 1$ $\quad$ $V_K = 1, -1, 0, 0, 0, 0, 0, \ldots$

$G_U(z) = \sum_{K=0}^{+\infty} z^K$ $\quad$ $G_V(z) = 1 - z = \sum_{K=0}^{+\infty} V_k z^K$

$= 1 + 1 z^1 + 1 z^2 + 1 z^3 + \ldots$

$G_U(z) \times G_V(z) = U_0 V_0 + (U_0 V_1 + U_1 V_0) z^1 + (U_0 V_2 + U_1 V_1 + U_2 V_0) z^2 + \ldots$

$\Downarrow$

$G_U(z) \quad G_V(z)$

$$\sum_{K=0}^{+\infty} z^K \times (1 - z) = 1$$

$$1 + \underbrace{(-1+1)}_{0} z^1 + \underbrace{(0-1+1)}_{0} z^2 + \underbrace{(0+0-1+1)}_{0} z^3 + \ldots = 1$$

Definição

Se $G_U(z) \times G_V(z) = 1$ diz-se $G_U(z)$ é inversa de $G_V(z)$ ($G_V(z)$ é inversa de $G_U(z)$)

$$\hookrightarrow G_U(z) = \frac{1}{G_V(z)} \qquad G_V(z) = \frac{1}{G_U(z)}$$

$\Downarrow$

$$\sum_{K=0}^{+\infty} z^K = \frac{1}{1-z}$$ forma fechada

$$\sum_{K=0}^{+\infty} a^K z^K = \sum_{K=0}^{+\infty} (az)^K \underset{az=y}{=} \sum_{K=0}^{+\infty} y^K = \frac{1}{1-y} \underset{az=y}{=} \frac{1}{1-az}$$ forma fechada

$$\sum_{K=0}^{+\infty} z^{pK} = \sum_{K=0}^{+\infty} (z^p)^K \underset{z^p=y}{=} \sum_{K=0}^{+\infty} y^K = \frac{1}{1-y} \underset{z^p=y}{=} \frac{1}{1-z^p}$$ forma fechada

Teorema

$G_V(z)$ tem inversa se e só se $v_0 \neq 0$

$U_K = K + 1$

$$G_U(z) = \sum_{K=0}^{+\infty} (K+1) z^K \quad (=) \quad G_U(z) - z G_U(z) = \sum_{K=0}^{+\infty} (K+1) z^K - z \sum_{K=0}^{+\infty} (K+1) z^{K+1} \quad (=)$$

$-z G_U(z)$

$$(=) (1-z) G_U(z) = 1 + z + z^2 + z^3 + z^4 + z^5 + \ldots = \sum_{K=0}^{+\infty} z^K = \frac{1}{1-z} \quad (=)$$

$$(=) G_U(z) = \frac{1}{(1-z)^2}$$ forma fechada

$$G(z)=\sum_{k=0}^{+\infty} k z^k = \sum_{k=0}^{+\infty}(k+1-1)z^k = \sum_{k=0}^{+\infty}(k+1)z^k - \sum_{k=0}^{+\infty} z^k =$$

$$= \frac{1}{(1-z)^2} - \frac{1}{1-z} = \frac{1-(1-z)}{(1-z)^2} = \boxed{\frac{z}{(1-z)^2}}$$ forma fechada

Ex. para HAD

Lista 1 - toda
Lista 2 - só secção 1

Probabilidades

12/05/2023

ATENÇÃO

No livro:
Cap. 5
→ números de Stirling (ignorar)
→ método de Horner = Regra de Ruffini

$$\sum_{k=p}^{n} k^{\underline{r}} = \left[\frac{k^{\underline{r+1}}}{r+1}\right]_p^{n+1}$$

$$k^{\underline{r}} = \frac{1}{(k+1)(k+2)\dots(k+r)}$$

$$u_k = \frac{1}{u_{k+1}\times u_{k+2}\times \dots \times u_{k+r}}$$

Ficha 1

(5.2)

e) $$\sum_{k=1}^{n} \frac{1}{(k+1)(k+4)} = \sum_{k=1}^{n} \frac{(k+2)(k+3)}{(k+1)(k+2)(k+3)(k+4)} = \sum_{k=1}^{n} \frac{(k+3)(k+2)}{(k+1)(k+2)(k+3)(k+4)}$$

$$\sum_{k=p}^{n} (ak+b)^{\underline{r}} = \left[\frac{(ak+b)^{\underline{r+1}}}{a(r+1)}\right]_p^{n+1}$$

$$= \sum_{k=1}^{n} \frac{(k+3)(k+4)-2(k+2)}{(k+1)(k+2)(k+3)(k+4)} = \sum_{k=1}^{n} \frac{1}{(k+1)(k+2)} - 2\sum_{k=1}^{n} \frac{k+3}{(k+1)(k+2)(k+3)(k+4)} =$$

$$= \sum_{k=1}^{n} \frac{1}{(k+1)(k+2)} - 2\left(\sum_{k=1}^{n} \frac{1}{(k+1)(k+2)(k+3)} - \sum_{k=1}^{n} \frac{1}{(k+1)(k+2)(k+3)(k+4)}\right) = \underbrace{\sum_{k=1}^{n} k^{\underline{-2}}}_{(A)} - 2\left(\underbrace{\sum_{k=1}^{n} k^{\underline{-3}}}_{(B)} - \underbrace{\sum_{k=1}^{n} k^{\underline{-4}}}_{(C)}\right) =$$

onde (A) $$= \left[\frac{k^{\underline{-1}}}{-1}\right]_1^{n+1} = \left[-\frac{1}{k+1}\right]_1^{n+1} = -\frac{1}{n+2} + \frac{1}{2}$$

(B) $$= \left[\frac{k^{\underline{-2}}}{-2}\right]_1^{n+1} = \left[-\frac{1}{2(k+1)(k+2)}\right]_1^{n+1} = -\frac{1}{2(n+2)(n+3)} + \frac{1}{2\times 2\times 3}$$

(C) $$= \left[\frac{k^{\underline{-3}}}{-3}\right]_1^{n+1} = \left[-\frac{1}{3(k+1)(k+2)(k+3)}\right]_1^{n+1} = -\frac{1}{3(n+2)(n+3)(n+4)} + \frac{1}{3\times 2\times 3\times 4}$$

f) $$\sum_{k=1}^{n-1} \frac{1}{k(k+1)(k+2)} = \sum_{k=1}^{n-1} (k-1)^{\underline{-2}} = \left[\frac{(k-1)^{\underline{-1}}}{-1}\right]_1^{n} = \left[-\frac{1}{2k(k+1)}\right]_1^{n} = -\frac{1}{2n(n+1)} + \frac{1}{2\times 2}$$

k) $$\sum_{k=0}^{n-1} \frac{k}{(4k+1)(4k+5)(4k+9)} = \frac{1}{4}\sum_{k=0}^{n-1} \frac{(4k+9)-9}{(4k+1)(4k+5)(4k+9)} = \frac{1}{4}\left(\sum_{k=0}^{n-1} \frac{1}{(4k+1)(4k+5)} - 9\sum_{k=0}^{n-1} \frac{1}{(4k+1)(4k+5)(4k+9)}\right) =$$

$$= \frac{1}{4}\left(\sum_{k=0}^{n-1} (4k-3)^{\underline{-2}} - 9\sum_{k=0}^{n-1} (4k-3)^{\underline{-3}}\right) = \frac{1}{4}\left(\left[\frac{(4k-3)^{\underline{-1}}}{-4}\right]_0^{n} - 9\left[\frac{(4k-3)^{\underline{-2}}}{-8}\right]_0^{n}\right) =$$

$$= \frac{1}{4}\left(\underbrace{\left[-\frac{1}{4(4k+1)}\right]_0^{n}}_{(A)} - 9\underbrace{\left[-\frac{1}{8(4k+1)(4k+5)}\right]_0^{n}}_{(B)}\right)$$

onde (A) $$= -\frac{1}{4(4n+1)} + \frac{1}{4}$$

(B) $$= -\frac{1}{8(4n+1)(4n+5)} + \frac{1}{8\times 5}$$

indução completa não sai

Lista 2 h) f) i)

1.1

h) $\sum_{j=1}^{n} \frac{1}{\sqrt{j}} \leq 2\sqrt{n} - 1$, para cada $n \in \mathbb{N}_1$

base: $\boxed{n=1}$ → indicar base

$$\underbrace{\sum_{j=1}^{1} \frac{1}{\sqrt{j}}}_{=\frac{1}{\sqrt{1}}=1} \overset{?}{\leq} \underbrace{2\sqrt{1} - 1}_{=2\times 1-1=1} \qquad 1 \leq 1$$

→ substituir explicitamente

H.I.: $\sum_{j=1}^{n} \frac{1}{\sqrt{j}} \leq 2\sqrt{n} - 1$ → especificar hipótese de indução

pode ser mais fácil

Passo de indução: Demonstrar que $\underbrace{\sum_{j=1}^{n+1} \frac{1}{\sqrt{j}} \leq 2\sqrt{n+1} - 1}_{\text{Tese}}$ ou $\underbrace{\sum_{j=1}^{n+1} \frac{1}{\sqrt{j}} - 2\sqrt{n+1} + 1 \leq 0}$

→ especificar a tese

Demonstração:

$$\sum_{j=1}^{n+1} \frac{1}{\sqrt{j}} - 2\sqrt{n+1} + 1 = \underbrace{\sum_{j=1}^{n} \frac{1}{\sqrt{j}}}_{} + \frac{1}{\sqrt{n+1}} - 2\sqrt{n+1} + 1 \underset{HI}{\leq} 2\sqrt{n} \cancel{-1} + \frac{1}{\sqrt{n+1}} - 2\sqrt{n+1} \cancel{+1}$$

até aqui se tudo estiver bem feito como a seta que tenho 2/3 da cotação

$$= \frac{1}{\sqrt{n+1}} + 2\frac{(\sqrt{n} - \sqrt{n+1})(\sqrt{n} + \sqrt{n+1})}{\sqrt{n} + \sqrt{n+1}} = \frac{1}{\sqrt{n+1}} + 2\left(\frac{n-(n+1)}{\sqrt{n} + \sqrt{n+1}}\right) = \frac{1}{\sqrt{n+1}} - 2\frac{1}{\sqrt{n} + \sqrt{n+1}} =$$

último terço da cotação são as contas finais

$$= \frac{\sqrt{n} + \sqrt{n+1} - 2\sqrt{n+1}}{\sqrt{n+1}(\sqrt{n} + \sqrt{n+1})} \begin{matrix} <0 \\ >0 \end{matrix} \leq 0$$

f) $\sum_{k=1}^{n} \frac{1}{k} \geq \frac{2n}{n+1} \quad \forall n \in \mathbb{N}_1$

base $\boxed{n=1}$ $\quad \underbrace{\sum_{k=1}^{1} \frac{1}{k}}_{=\frac{1}{1}=1} \geq \underbrace{\frac{2\times 1}{1+1}}_{=\frac{2}{2}=1} \qquad 1 \geq 1$

H.I.: $\sum_{k=1}^{n} \frac{1}{k} \geq \frac{2n}{n+1}$ $\qquad$ Tese: $\sum_{k=1}^{n+1} \frac{1}{k} \geq \frac{2(n+1)}{n+2}$ ou $\sum_{k=1}^{n+1} \frac{1}{k} - \frac{2(n+1)}{n+2} \geq 0$

Demonstração

$$\sum_{k=1}^{n+1} \frac{1}{k} - \frac{2(n+1)}{n+2} = \sum_{k=1}^{n} \frac{1}{k} + \frac{1}{n+1} - \frac{2(n+1)}{n+2} \underset{HI}{\geq} \frac{2n}{n+1} + \frac{1}{n+1} - \frac{2(n+1)}{n+2} =$$

$$= \frac{2n+1}{n+1} - \frac{2(n+1)}{n+2} = \frac{(2n+1)(n+2) - 2(n+1)^2}{(n+1)(n+2)} = \frac{2n^2 + 4n + n + 2 - (2n^2 + 4n + 2)}{(n+1)(n+2)} =$$

$$= \frac{n}{(n+1)(n+2)} \begin{matrix} >0 \\ >0 \end{matrix} > 0$$

arc

$a, b \in \mathbb{Z}$ 15/05/2023

a é múltiplo de b → $a = \dot{b}$ $b \neq 0$ b é divisor de a

se $a = k \times b$ para algum $k \in \mathbb{Z}$ $b | a$

$15 = \dot{3}$ $15 = 5 \times 3$ $3 | 15$

$15 = (\dot{-3})$ $15 = 5 \times (-3)$ $-3 | 15$

$0 = \dot{3}$ $0 = 0 \times 3$ $3 | 0$

$0 \in \mathbb{Z}$

Divisores de 15: 1, 3, 5, 15
-1, -3, -5, -15

Divisores de -15: os mesmos

Algumas propriedades dos divisores

- se $b | a$ então $-b | a$
- $b | 0$ $(b \neq 0)$
- $1 | a$
- $a | a$ $(a \neq 0)$
- se $b | a$ então $b | (-a)$

Definição

mdc(m,n)

$m, n \in \mathbb{Z}$ não simultaneamente nulos

O máximo divisor comum de m,n é o maior número inteiro que é simultaneamente divisor de m e de n

$mdc(0, 35) = 35$ $mdc(0, -35) = 35$

~~mdc(0,0)~~ = $mdc(35, 35) = 35$

Propriedades

- $mdc(m,n) = mdc(n,m)$
- $mdc(m,n) \geq 1$
- $mdc(m,n) = mdc(m,-n) = mdc(-m,n) = mdc(-m,-n)$
- $mdc(0,m) = |m|$
- $a, b \in \mathbb{N}$ ⇒ $mdc(a,b) = mdc(b, mod(a,b))$

mod(a,b) → resto da divisão inteira de a por b

$a, b \in \mathbb{N}$

$a \lfloor b$

$q \in \mathbb{N}$

$a = b \times q + r$

mod(a,b) ← $\boxed{r}$

$a \% b$

$0 \leq r < b$

(resto)

Algoritmo de Euclides

input: $m, n \in \mathbb{N}$, não simultaneamente nulos

output: mdc(m,n)

quocientes		1	2	3
	120	84	36	12
restos	36	12	0	

$\longrightarrow$ mdc(120,84)

$120 \,|\, 84$
$36 \quad 1$

$84 \,|\, 36$
$12 \quad 2$

$36 \,|\, 12$
$00 \quad 3$

3 divisões

divisor da 1ª divisão c/ resto 0
$\downarrow$
mdc(120, 84)

mdc(187,154)

	1	4	1	2
187	154	33	22	11
33	22	11	0	

$\longrightarrow$ mdc(187,154)

$\longrightarrow 22 \,|\, 11$
$0 \quad 2$

$45 = mdc(0,45) = 0 \times \underset{\in \mathbb{Z}}{0} + 45 \times \underset{\in \mathbb{Z}}{1}$

$0 \qquad 1$

Definição:
Coeficiente de Bézout para $a,b \in \mathbb{Z}$ não simultaneamente nulos são $x,y \in \mathbb{Z}$ tais que $ax+by = mdc(a,b)$

Teorema
Existem sempre coeficientes de Bézout para $a,b \in \mathbb{Z}$ não simultaneamente nulos.

Aplica-se o algoritmo de Saunderson (algoritmo de Euclides estendido) $\rightarrow$ input: $m,n \in \mathbb{N}$
output: coeficientes de Bézout para m,n

Algoritmo de Saunderson aplicado a 120,84

a_i	q_i	x_i	y_i
120		1	0
84	1	0	1
36	2	1	-1
12	3	-2	3
0			

mdc(120,84)

$\rightarrow 1 - 0 \times 1 = 1$
$0 - 1 \times 1 = -1$

$a_0 \,|\, a_1$
$\vdots \quad q_1$
a_2

$a_{j-2} \,|\, a_{j-1}$
$\vdots \quad q_{j-1}$
a_j

$a_j = x_j \times m + y_j \times n$

$x_j = x_{j-2} - x_{j-1} \times q_{j-1}$

$y_j = y_{j-2} - y_{j-1} \times q_{j-1}$

coef Bézout para 120

coef de Bézout para 84

$0 - 1 \times 2 = -2$
$1 - (-1) \times 2 = 3$

$\boxed{12 = 120 \times (-2) + 84 \times (3)}$

Algoritmo de Saunderson aplicado a 187 e 154

a_i	q_i	x_i	y_i
187		1	0
154	1	0	1
33	4	1	-1
22	1	-4	5
11	2	5	-6
0			

mdc(187,154)

$\rightarrow 0 - 1 \times 4 = -4$
$1 - (-1) \times 4 = 5$

$1 - (-4) \times 1 = 5$
$-1 - 5 \times 1 = -6$

coef Bézout para 154

coef Bézout para 187

$\boxed{11 = 187 \times 5 + 154(-6)}$

Problemas ✨

15/05/2023

LISTA 2

(2.2) Sucessão de Fibonacci é definida por recursão como se segue

$f_0 = 0,\ f_1 = 1,\ f_{k+1} = f_k + f_{k-1} \quad k \in \mathbb{N}_1$

Use indução matemática completa para estabelecer os resultados seguintes

b) $f_k \geq \left(\frac{3}{2}\right)^{k-2}$ para todo o $k \in \mathbb{N}_1$

Base: $k=1$ $\quad \underbrace{f_1}_{=1} \geq \underbrace{\left(\frac{3}{2}\right)^{1-2}}_{=\frac{2}{3}} \quad 1 \geq \frac{2}{3}$ ✓

HI: $f_k \geq \left(\frac{3}{2}\right)^{k-2}$

Tese: $f_{k+1} \geq \left(\frac{3}{2}\right)^{k+1-2}$ ou $\boxed{f_{k+1} - \left(\frac{3}{2}\right)^{k-1} \geq 0}$

Demonstração:

$$f_{k+1} - \left(\frac{3}{2}\right)^{k-1} \underset{\text{definição de sucessão de Fibonacci}}{=} f_k + f_{k-1} - \left(\frac{3}{2}\right)^{k-1} \underset{\text{H.I}}{\geq} \left(\frac{3}{2}\right)^{k-2} + f_{k-1} - \left(\frac{3}{2}\right)^{k-1}$$

Problema

HI: $f_j \geq \left(\frac{3}{2}\right)^{j-2}$ para $j \in \{1, 2, \ldots, k\}$

Demi: $f_{k+1} - \left(\frac{3}{2}\right)^{k-1} = \underbrace{f_k}_{\geq} + \underbrace{f_{k-1}}_{\geq} - \left(\frac{3}{2}\right)^{k-2} \geq \left(\frac{3}{2}\right)^{k-2} + \left(\frac{3}{2}\right)^{(k-1)-2} - \left(\frac{3}{2}\right)^{k-1} =$

$$= \left(\frac{3}{2}\right)^{k-3}\left(\left(\frac{3}{2}\right) + 1 - \left(\frac{3}{2}\right)^2\right) = \underbrace{\left(\frac{3}{2}\right)^{k-3}}_{>0}\left(\frac{3}{2} + 1 - \frac{9}{4}\right) = \left(\frac{3}{2}\right)^{k-3}\left(\frac{1}{4}\right) \geq 0$$

$\frac{10}{4}$

Tese: $f_{k+1} \geq \left(\frac{3}{2}\right)^{k-1}$ ou $f_{k+1} - \left(\frac{3}{2}\right)^{k-1} \geq 0$

Base: ~~$\left(\frac{3}{2}\right)^{-2}$~~

$k=1$ $\quad f_1 \overset{?}{\geq} \underbrace{\left(\frac{3}{2}\right)^{1-2}}_{=\frac{2}{3}} \quad 1 \geq \frac{2}{3}$ ✓

$k=2$ $\quad \underbrace{f_2}_{=1} \geq \underbrace{\left(\frac{3}{2}\right)^0}_{=1}$ ✓

$\frac{f_1}{f_2}$ ✓

$f_3 \in$

Temos de ter a certeza que o primeiro valor a ser provado por hereditariedade já tem os valores que necessita provados na base

indução matemática completa

indução matemática simples

c) $f_{k+10} = f_k \times f_{11} + f_{k-1} \times f_{10}$

Base: $\boxed{k=1}$ $f_{11} = \underbrace{f_1 \times f_{11} + f_0 \times f_{10}}_{= 1 \times f_{11} + 0 \times f_{10}} = f_{11}$ ✓

$\boxed{k=2}$ $f_{12} = \underbrace{f_2 \times f_{11} + f_1 \times f_{10}}_{= 1 \times f_{11} + 1 \times f_{10}} = f_{12}$ ✓

HI: $f_{j+10} = f_j \times f_{11} + f_{j-1} \times f_{10}$ para $j \in \{1, \dots, k\}$

Tese: $\underbrace{f_{k+1+10}}_{k+11} = f_{k+1} \times f_{11} + f_k \times f_{10}$

Dem:

$f_{k+11} = f_{k+10} + f_{k+9} = \underbrace{f_{k+10}}_{f_{12}} + \underbrace{f_{(k-1)+10}}_{f_{11}} \underset{HI}{=} f_k \times f_{11} + f_{k-1} \times f_{10} + f_{k-1} \times f_{11} + f_{k-2} \times f_{10} =$

pela definição da sucessão de Fibonacci

$j=k$
$j=k-1$

$k+1=3$
$k=2$
$k-1=1$

$= (f_k + f_{k-1}) f_{11} + (f_{k-1} + f_{k-2}) f_{10} = \boxed{f_{k+1} \times f_{11} + f_k \times f_{10}}$

2.1 todo o $n \in \mathbb{N}_2$ se pode escrever como produto de potências de nºs primos.

Base: $\boxed{n=2}$ 2 pode escrever-se como produto de potências de primos
$2 = 2^1$, 2 primo ✓

HI: j pode escrever-se como produto de potências de primos, $j \in \{2, 3, \dots, n\}$

Tese: $n+1$ pode escrever-se como produto de potências de primos

Dem:

$n+1$

$n+1$ é primo
$n+1 = (n+1)^1$

$n+1$ não é primo
$n+1 = k_1 \times k_2$ $\quad 1 < k_1, k_2 < n+1$
por HI, k_1 e k_2 podem escrever-se como produto de potências de primos
rearranjando as potências
$n+1$ é produto de potências de primos

$n=2$ ✓
3 ✓

2.5

a) $f_0 + f_1^2 + \dots + f_n^2 = f_n f_{n+1}$ para todo $n \in \mathbb{N}$

$\sum_{k=0}^{n} f_k^2 = f_n \times f_{n+1}$ $n \in \mathbb{N}$

Base: $\boxed{n=0}$ $\underbrace{\sum_{k=0}^{0} f_k^2}_{= f_0^2 = 0^2 = 0} \overset{?}{=} \underbrace{f_0 \times f_1}_{= 0 \times f_1 = 0}$ ✓

HI: $\sum_{k=0}^{n} f_k^2 = f_n \times f_{n+1}$ $\quad$ Tese: $\sum_{k=0}^{n+1} f_k^2 = f_{n+1} \times f_{n+2}$

Dem $\sum_{k=0}^{n+1} f_k^2 = \sum_{k=0}^{n} f_k^2 + f_{n+1}^2 \underset{HT}{=} f_n \times f_{n+1} + f_{n+1}^2 = f_{n+1}(\overbrace{f_n + f_{n+1}}^{f_{n+2}}) =$

$= f_{n+1} \times f_{n+1}$

d) Sucessão Fibonacci

LISTA 3

encontrar expressão não recursiva para s_k

2.1) Resolva as seguintes recorrências usando funções geradoras

b) $s_0 = 2$ e $s_k = 4s_{k-1} + 1$ $k \in \mathbb{N}_1$

(i) Calcular forma fechada para a função geradora de f

$$\sum_{k=1}^{+\infty} s_k z^k = \sum_{k=1}^{+\infty} (4s_{k-1} + 1) z^k \quad k \in \mathbb{N}_1$$

$$\sum_{k=0}^{+\infty} s_k z^k - s_0 z^0 = 4\sum_{k=1}^{+\infty} s_{k-1} z^k + \sum_{k=1}^{+\infty} z^k$$

$$G_s(z) - 2 = 4z \sum_{k=1}^{+\infty} s_{k-1} z^{k-1} + z \sum_{k=1}^{+\infty} z^{k-1}$$

$s_0 z^0 + s_1 z^1 + \dots$

$z^0 + z^1 + z^2 + \dots$

$$G_s(z) - 2 = 4z \sum_{k=0}^{+\infty} s_k z^k + z \sum_{k=0}^{+\infty} z^k$$

$$G_s(z) - 2 = 4z G_s(z) + z \frac{1}{1-z} \Rightarrow \boxed{G_s(z) = \frac{2}{1-4z} + z \frac{1}{(1-z)(1-4z)}}$$

(ii) Obter expressão não recursiva por s_k a partir

$$G_s(z) = 2 \times \frac{1}{1-4z} + \frac{z}{(1-z)(1-4z)}$$

$A(1-4z) + B(1-z) = z$

$z = 1 \mid A(1-4) = 1 \Rightarrow A = -\frac{1}{3}$

$z = \frac{1}{4} \mid B(1-\frac{1}{4}) = \frac{1}{4} \Rightarrow B = \frac{1}{4} \Rightarrow B = \frac{1}{3}$

$$\frac{z}{(1-z)(1-4z)} = \frac{A}{1-z} + \frac{B}{1-4z}$$

$$G_s(z) = 2 \times \frac{1}{1-4z} - \frac{1}{3}\frac{1}{1-z} + \frac{1}{3} \times \frac{1}{1-4z} = \frac{7}{3} \times \frac{1}{1-4z} - \frac{1}{3} \times \frac{1}{1-z} =$$

$$\sum_{k=0}^{+\infty} 4^k z^k \qquad \sum_{k=0}^{+\infty} z^k$$

$$= \boxed{\sum_{k=0}^{+\infty} \underbrace{\left(\frac{7}{3} \times 4^k - \frac{1}{3}\right)}_{s_k} z^k}$$

$$\boxed{s_k = \frac{7}{3} \times 4^k - \frac{1}{3}}$$

expressão não recursiva de s_k

f) $s_0 = 0$ e $s_k = 2s_{k-1} + 3k$ $k \in \mathbb{N}_1$

$$\sum_{k=1}^{+\infty} s_k z^k = \sum_{k=1}^{+\infty} (2s_{k-1} + 3k) z^k \quad k \in \mathbb{N}_1$$

$$\sum_{k=0}^{+\infty} s_k z^k - \underbrace{s_0 z^0}_{=0} = 2\sum_{k=1}^{+\infty} s_{k-1} z^k + 3\sum_{k=1}^{+\infty} k z^k = \sum_{k=0}^{+\infty} k z^k$$

$$G_s(z) = 2z \sum_{k=1}^{+\infty} s_{k-1} z^{k-1} + 3\frac{z}{(1-z)^2} \qquad G_s(z) = 2z G_s(z) + \frac{3z}{(1-z)^2}$$

$$= \sum_{k=0}^{+\infty} s_k z^k$$

$\Rightarrow \boxed{G_s(z) = \frac{3z}{(1-2z)(1-z)^2}}$

T.P.C (ii) $\frac{3z}{(1-2z)(1-z)^2} = \frac{A}{1-2z} + \frac{B}{1-z} + \frac{C}{(1-z)^2}$

$A=-3$
$B=6$
$C=-3$

confirmar o WolframAlpha resultado final

18/05/2023

Tópicos em teoria de números

Teorema

1. Se $mdc(m,n)=d$ então $mdc\left(\frac{m}{d},\frac{n}{d}\right)=1$
2. Se $mdc(m,n)=1$ e $m \times t = \dot{n}$ então $t=\dot{n}$
3. Se $mdc(m,n_1)=1$ e $mdc(m,n_2)=1$ então $mdc(m,n_1,n_2)=1$

$ax+by=mdc(a,b)$

coeficientes de Bézout $x,y \in \mathbb{Z}$

$mdc(a,b)=1$
$\Rightarrow$
a,b são primos entre si ou coprimos

Equações Diofantinas

LISTA 4

equações em que os coeficientes são inteiros e os variáveis que procuramos também são inteiros

(4.4)
a) $28x+8y=100$
$\in \mathbb{N}$

$x=1 \wedge y=9$ $\quad 28+72$
$x=3 \wedge y=2$ $\quad 84+16$

ex: $\underbrace{\underbrace{4x}_{par}+\underbrace{6y}_{par}}_{par}=\underbrace{53}_{ímpar}$

não tem solução

vários soluções ← pedem não ter solução

Vamos estudar: as equações diofantinas lineares com duas variáveis
$ax+by=c$
- $a,b,c \in \mathbb{Z}$
- os valores que se pretendem obter para x e $y \in \mathbb{Z}$

(4.1)
f) $187x+154y=44$

$187 \times 5 + 154(-6) = 11$
$\downarrow \times 4$
$187 \times \underbrace{20}_{x} + 154\underbrace{(-24)}_{y} = 44$

187		1	0
154	1	0	1
33	4	1	-1
22	1	-4	5
11	2	5	-6
0			

$mdc(187,154)=11$

$x=20$
$y=-24$
solução da equação

arc

TEOREMA

1) A equação diofantina $ax+by=c$ tem solução se e só se c é múltiplo do $mdc(a,b)$

2) Se tem solução, uma solução pode ser calculada através dos coeficientes de Bézout para a e b

TEOREMA

Se $x_0, y_0 \in \mathbb{Z}$ são solução de $ax+by=c$ então $x, y \in \mathbb{Z}$ são soluções da equação se e só se $x = x_0 + \frac{b}{mdc(a,b)}k$, $y = y_0 - \frac{a}{mdc(a,b)}k$

$k \in \mathbb{Z}$

$\underbrace{187}_{a}x + \underbrace{154}_{b}y = 44$

· 44 é múltiplo de $11 = mdc(187, 154)$ a equação tem solução

· usando o alg. de Saunderson concluímos que $x_0 = 20$ e $y_0 = -24$ são soluções da equação

O conjunto de soluções é

$$\rightarrow \begin{cases} x = 20 + \frac{154}{11}k = 20 + 14k \\ y = -24 - \frac{187}{11}k = -24 - 17k \end{cases} \quad k \in \mathbb{Z}$$

$k=0 \rightarrow \begin{cases} x = 20 \\ y = -24 \end{cases}$ $k=1 \rightarrow \begin{cases} x = 34 \\ y = -24 - 17 = -41 \end{cases}$ $k=-1 \rightarrow \begin{cases} x = 20 - 14 = 6 \\ y = -24 + 17 = -7 \end{cases}$

19/05/2023

Problemas ✦

LISTA 3

2.i)

1) $S_0 = 3$, $S_1 = 4$, $S_k = S_{k-1} + 6S_{k-2}$, $k \in \mathbb{N}_2$

$$\sum_{k=2}^{+\infty} S_k z^k = \sum_{k=2}^{+\infty} (S_{k-1} + 6S_{k-2}) z^k$$

$$\sum_{k=0}^{+\infty} S_k z^k - S_0 - S_1 z = \sum_{k=1}^{+\infty} S_{k-1} z^k + 6\sum_{k=2}^{+\infty} S_{k-2} z^k$$

$$G_S(z) - 3 - 4z = z\left(\sum_{k=1}^{+\infty} S_{k-1} z^{k-1}\right) + 6z^2\left(\sum_{k=2}^{+\infty} S_{k-2} z^{k-2}\right) \rightarrow \sum_{k=0}^{+\infty} S_k z^k = G_S(z)$$

$S_0 z^0 + S_1 z^1 + S_2 z^2 + \dots$

$S_0 z^0 + S_1 z^1 + S_2 z^2 + \dots = \sum_{k=0}^{+\infty} S_k z^k$

$$G_S(z) = 3 + 4z + z\left(\sum_{k=0}^{+\infty} S_k z^k - S_0\right) + 6z^2 G_S(z)$$

$$G_S(z) = 3 + 4z + z(G_S(z) - 3z) + 6z^2 G_S(z)$$

$$G_S(z) - zG_S(z) + 6z^2 G_S(z) = 3 + 4z - 3z \Leftrightarrow (1 - z - 6z^2) G_S(z) = 3 + z \Leftrightarrow \boxed{G_S(z) = \frac{3+z}{1-z-6z^2}}$$

by Staples

i) $\frac{3+z}{1-z-6z^2} = \frac{3+z}{-6(z+\frac{1}{2})(z-\frac{1}{3})} = \frac{3+z}{-6\times\frac{1}{2}(1+2z)(-\frac{1}{3})(1-3z)}$ $\quad z = \frac{1 \pm \sqrt{1+24}}{-12}$ $\quad -\frac{1}{2}$ $\quad \frac{1}{3}$

$= \frac{3+z}{(1+2z)(1-3z)} = \frac{A}{1+2z} + \frac{B}{1-3z} =$ $\quad A(1-3z) + B(1+2z) = 3+z$

$z = \frac{1}{3} \Rightarrow B(\frac{5}{3}) = \frac{10}{3} \Rightarrow B = 2$ $\quad z = -\frac{1}{2} \Rightarrow A(\frac{5}{2}) = \frac{5}{2} \Rightarrow A = 1$

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

$= \sum_{k=0}^{+\infty} \underbrace{((-2)^k + 2\times 3^k)}_{S_k} z^k$ $\quad \Rightarrow$ (expressão não recursiva para S_k)

ii) $S_0 = 2,\ S_1 = 1 \quad S_k = 3S_{k-1} - 2S_{k-2} + 2 \quad k \in \mathbb{N}_2$

i) $\sum_{k=2}^{+\infty} S_k z^k = \sum_{k=2}^{+\infty} (3S_{k-1} - 2S_{k-2} + 2) z^k$

$\sum_{k=0}^{+\infty} S_k z^k - S_0 - S_1 z = 3\sum_{k=2}^{+\infty} S_{k-1} z^k - 2\sum_{k=2}^{+\infty} S_{k-2} z^k + 2\sum_{k=2}^{+\infty} z^k \qquad \sum_{k=0}^{+\infty} z^k = \frac{1}{1-z}$

$G_S(z) - 2 - z = 3z\sum_{k=2}^{+\infty} S_{k-1} z^{k-1} - 2z^2 \sum_{k=2}^{+\infty} S_{k-2} z^{k-2} + 2z^2 \sum_{k=2}^{+\infty} z^{k-2}$

$G_S(z) = 2 + z + 3z(G_S(z) - S_0) - 2z^2 G_S(z) + 2z^2 \frac{1}{1-z} =$

$G_S(z) - 3zG_S(z) + 2z^2 G_S(z) = 2 + z - 6z + 2z^2 \frac{1}{1-z}$

$G_S(z)(1 - 3z + 2z^2) = 2 - 5z + \frac{2z^2}{1-z}$

$G_S(z) = \frac{2-5z}{(1-3z+2z^2)} + \frac{2z^2}{(1-z)(1-3z+2z^2)}$

i) $\frac{2-5z}{(1-3z+2z^2)} \rightarrow \frac{2z^2}{(1-z)(1-3z+2z^2)} = \frac{2-5z}{2(z-\frac{1}{2})(z-1)} + \frac{2z^2}{2(1-z)(z-\frac{1}{2})(z-1)} =$ $\quad z = \frac{3 \pm 1}{4}$ $\quad \frac{1}{2}$ $\quad 1$

quando nenhum é óbvio é preferível juntar uma e depois fazer

$= \frac{2-5z}{-2\times\frac{1}{2}(1-2z)(1+z)} + \frac{2z^2}{-2(1-z)^2(-\frac{1}{2})(1-2z)} = \frac{2-5z}{(1-z)(1-2z)} + \frac{2z^2}{(1-z)^2(1-2z)}$

$= \frac{A}{1+z} + \frac{B}{1-2z} + \frac{C}{1-z} + \frac{D}{(1-z)^2} + \frac{E}{1-2z} = 3\frac{1}{1-z} - \frac{1}{1-2z} - 2\times\frac{1}{(1-z)^2} + 2\frac{1}{1-2z}$ $\quad (*)$

$A(1-2z) + B(1+z) = 2 - 5z \qquad C(1+z)(1-2z) + D(1-2z) + E(1+z)^2 = 2z^2$

$z = \frac{1}{2} \Rightarrow B(\frac{3}{2}) = -\frac{3}{2} \Rightarrow B = -1$ $\quad z = 1 \Rightarrow D(-1) = 2 \Rightarrow D = -2$

$z = -1 \Rightarrow A(-1) = -3 \Rightarrow A = 3$ $\quad z = -\frac{1}{2} \Rightarrow E(\frac{1}{4}) = \frac{1}{2} \Rightarrow E = 2$

$z = 0 \Rightarrow C + D + E = 0 \Rightarrow C = 0$

$(*) = 3\sum_{k=0}^{+\infty} z^k - \sum_{k=0}^{+\infty} 2^k z^k + 2\sum_{k=0}^{+\infty} (k+1) z^k + 2\sum_{k=0}^{+\infty} 2^k z^k =$

$= \sum_{k=0}^{+\infty} (3z^k - 2^k z^k + 2kz^k + 2z^k + 2\times 2^k z^k) =$

$= \sum_{k=0}^{+\infty} \underbrace{(2^k + 2k + 1)}_{S_k \text{ expressão não recursiva}} z^k$

(2.6) $C_{k+1} - C_k = -\beta V_k + m$ $\quad V_k = \alpha C_{k-1}$ $\quad \alpha = 1$ $\quad \beta = \frac{3}{16}$ $\quad C_0 = C_1 = 0$ $\quad m = 2$

T.P.C

$C_{k+1} = C_k - \frac{3}{16} C_{k-1} + 2$

$C_k - C_{k-1} = -\frac{3}{16} C_{k-2} + 2 \Leftrightarrow C_k = C_{k-1} - \frac{3}{16} C_k$

concentração de CO_2 no sangue no instante k

No teste vai sair um problema de equações diofantinas

LISTA 4

(1.1)

5) mdc(84, 54)

ñ escrever no teste (usar máquina

	1	1	1	4
84	54	30	24	6
30	24	6	0	

→ mdc(84, 54)

84	54	54	30	30	24	24	6
30	1	24	1	6	1	0	4

a)

	1	1	2	7
74	44	30	14	2
30	14	2	0	

→ mdc(74, 44)

(1.2)

e) mdc(−92, 36) = mdc(92, 36)

	2	1	1	4
92	36	20	16	4
20	16	4	0	

→ mdc(−92, 36)

−7	3	−7	3
+6	2	+9	−3
−1		2	

(2.5)

92		1	0
36	2	0	1
20	1	1	−2
16	1	−1	3
4	4	2	−5
0			

→ coef Bézout para 36

coef Bézout para 92

$92 \times \_\_ + 36 \times \_\_ = 4$

mdc(92, 36)

R: 2 e −5

$92 \times 2 + 36(-5) = 4$

T.P.C

(2.12)

1020		1	0
924	1	0	1
96	9	1	−1
60	1	−9	10
36	1	10	−11
24	1	−9	21
12	2	29	−32
0			

mdc(1020, 924) = 12

$1020(29) - 924(-32) = 12$

$1020(29) - 924(32) = 12$

R: 29 e 32

22/05/2023

Congruência módulo

1 Definição

$a, b \in \mathbb{Z}$, $n \in \mathbb{N}$

$a \equiv_n b$ se $a-b$ é múltiplo de n

↓

a congruente com b módulo n

$a - b = n \times k$ $\quad a = b + nk$

$23 \equiv_3 11 \rightarrow 23 - 11 = 12 = \dot{3}$ $\quad a - a = 0 = \dot{n}$

$24 \not\equiv_3 8 \rightarrow 24 - 8 = 16$

Propriedades

$a, b \in \mathbb{Z}$, $n \in \mathbb{N}$

1. $a \equiv_n a$
2. $a \equiv_n b$ então $b \equiv_n a$
3. se $a \equiv_n b$ e $b \equiv_n c$ então $a \equiv_n c$
4. $a \equiv_n \text{mod}(a, n)$
5. se $a \equiv_n a'$ e $b \equiv_n b'$

$\begin{array}{c|c} a & n \\ \vdots & q \end{array}$ $\quad \text{mod}(a,n)$

$a = n \times q + \text{mod}(a,n)$

i) $a + b \equiv_n a' + b'$ $\quad (a+b) - (a'+b') = (a-a') + (b-b') =$

ii) $a \times b \equiv_n a' \times b'$

iii) $a^p \equiv_n (a')^p$ $\quad p \in \mathbb{N}$

caso particular de $a \equiv_n a'$

$a - b \equiv_n a - b'$ $\quad a \times b \equiv_n a \times b'$

$m \in \mathbb{N}$ $\quad m \equiv_3$ soma dos seus dígitos

$m = d_0 + d_1 \times 10 + d_2 \times 10^2 + \ldots + d_k \times 10^k$

d_i's dígitos $\in \{0, \ldots, 9\}$

$10 \equiv_3 1 \overset{\text{S i)}}{\Rightarrow} 10^1 \equiv_3 1 \Rightarrow 10^j \equiv_3 1 \overset{\text{S ii)}}{\Rightarrow} d_j 10^j \equiv_3 d_j$

$d_0 \equiv_3 d_0$ $\quad d_1 10 \equiv_3 d_1$ $\quad d_2 10^2 \equiv_3 d_2$ $\quad \ldots$ $\quad d_k 10^k \equiv_3 d_k$

$\Downarrow$ S i)

$\underbrace{d_0 + d_1 10 + d_2 10^2 + \ldots d_k 10^k}_{m} \equiv_3 \underbrace{d_0 + d_1 + d_2 + \ldots + d_k}_{\text{soma}}$

$m - \text{soma} = 3k$

divisão nem sempre mantém a congruência

Teorema

$a \times c \equiv_n b \times c$ sse $a \equiv_{\frac{n}{mdc(c,n)}} b$

Teorema

se $mdc(p,q) = 1$ $\quad a \equiv_{pq} b$ sse $a \equiv_p b$ e $a \equiv_q b$

Teorema

se $a \equiv_n b$ e $b \in \{0, \dots, n-1\}$
então $b = mod(a,n)$

Pequeno Teorema de Fermat

p primo $\quad n \in \mathbb{Z}$

$n^p \equiv_p n$

$\alpha \underbrace{x}_{\in \mathbb{Z}} \equiv_n \beta \qquad \alpha, \beta \in \mathbb{Z}, n \in \mathbb{N} \qquad \alpha x - n k = \beta$

??

$2x \equiv_3 1 \qquad 2x - 1 = \dot{7} \qquad 8x \equiv_6 4$

-3

4

2

resolver a eq diofantina

$2x \equiv_8 3 \longrightarrow \underbrace{\underbrace{2x}_{par} - \underbrace{3}_{ímpar}}_{ímpar} = \underbrace{\dot{8}}_{par}$

existência de solução
$\rightarrow \beta$ múltiplo de $mdc(\alpha, -n)$

$187x \equiv_{154} 44 \iff 187x - 154t = 44$

x_0 é solução de $\alpha x \equiv_n \beta$
$\alpha x \equiv_n \beta$ sse $x \equiv_{\frac{n}{mdc(\alpha,n)}} x_0$

Cálculo de solução
calcular solução para x da eq. diofantina

ex:
eleições parlamento europeu 5 em 5 anos últimas: 2019
autarquias locais 4 em 4 anos " 2021

$x = 2019 + 5k \iff x - 2019 = \underbrace{5k}_{5} \qquad x = 2021 + 4k$

$\begin{cases} x \equiv_5 2019 \\ x \equiv_4 2021 \end{cases} \longrightarrow 2029$

LISTA 5

3.1

a) $\begin{cases} x \equiv_3 2 \\ x \equiv_4 3 \\ x \equiv_5 2 \end{cases}$

importante escrever

Pode aplicar-se o TCR porque $mdc(3,4)=1$, $mdc(3,5)=1$, $mdc(4,5)=1$

$x = x_0 + \underbrace{M}_{3\times4\times5 = 60} t$

? 107

K_i	m_i	n_i	$n_i \tilde{n}_i \equiv_{m_i} 1$		$\tilde{n}_i$	$K_i n_i \tilde{n}_i$
2	3	20	$20\tilde{n}_1 \equiv_3 1$	$2\tilde{n}_1 \equiv_3 1$	2	80
3	4	15	$15\tilde{n}_2 \equiv_4 1$	$3\tilde{n}_2 \equiv_4 1$	-1	-45
2	5	12	$12\tilde{n}_3 \equiv_5 1$	$2\tilde{n}_3 \equiv_5 1$	3	+ 72
						$x_0 = 107$

$n_1 = \frac{\cancel{3}\times4\times5}{\cancel{3}}$

$20 \equiv_3 2$

$15 \equiv_4 3 \rightarrow mod(18,4)$

$12 \equiv_5 2 \rightarrow mod(12,5)$

$x = 107 + 60t \quad t \in \mathbb{Z}$

Problemas

22/05/2023

LISTA 4

4.1

a) $4x + 8y = 22$

$mdc(4,8) = 4 \qquad 22 \neq \dot{4}$ não tem solução

d) $20x + 12y = 2$

$mdc(20,12) = 4 \qquad 2$ ñ é múltiplo de 4 logo ñ tem solução

e) $52x + 36y = 20$

52		1	0
36	2	0	1
20	1	1	-2
16	1	-1	3
4	4	2	-5
0			

$mdc(52,36) = 4$

$20 = 4$

logo tem solução

$\times 5 \begin{cases} 52\times2 + 36\times(-5) = 4 \\ 52\times10 + 36\times(-25) = 20 \end{cases}$

$x = 10$

$y = -25$

são uma solução de eq. diofantina

4.2 $mdc(a,b) = 1 \qquad ax_0 + by_0 = 1$

$\downarrow \times c$

$ax + by = c$

4.3

e) $52x + 36y = 20$

x_0, y_0 solução

· ver se há solução

· encontrar uma solução $\rightarrow x_0 = 10 \quad y_0 = -25$

Cj todas as soluções

$x = x_0 + \frac{b}{mdc(a,b)} k \qquad y = y_0 - \frac{a}{mdc(a,b)} k$

$x = 10 + \frac{36}{4} k = 10 + 9k \qquad y = -25 - \frac{52}{4} k = -25 - 23k \quad , k \in \mathbb{Z}$ fim

$k=0 \rightarrow x = 10, \; y = -25 \qquad k=1 \rightarrow x = 19, \; y = -48 \qquad k=-1 \rightarrow x = 1, \; y = -2$

$x = 10 + 9k = 1 + 9 + 9k = 1 + 9(k+1)$

$\downarrow t = k+1 \Rightarrow t - 1 = k$

$y = -25 - 23(t-1)$

$= -25 - 23t + 23 = -2 - 23t$

$\begin{cases} x = 1 + 9t \\ y = -2 - 23t \end{cases}$

arc

g) $-75x + 108y = 30$ $\quad 108y - 75x = 30$

ATENÇÃO
Algoritmo de Saunderson só se aplica a números em $\mathbb{N}$

108		1	0
75	1	0	1
33	2	1	-1
9	3	-2	3
6	1	7	-10
3	2	-9	13
0		1	1

$mdc(-75, 108) = 3$ $\quad$ 30 é 3 logo tem solução

$\times 10$ $\quad 108(-9) - 75(13) = 3$

$108(-90) - 75(-130) = 30$

$y_0 = -90 \quad x_0 = -130$

$x = -130 + \frac{108}{3}k = -130 + 36k$ $\quad y = -90 + \frac{75}{3}k = -90 + 25k \quad , k \in \mathbb{Z}$

4.5

a) $28x + 8y = 100$ $\quad mdc(28, 8) = 4$ $\quad$ 100 é 4 logo tem solução

$\times 25$ $\quad 28 \times 1 + 8(-3) = 4$

$28 \times 25 + 8(-75) = 100$

28		1	0
8	3	0	1
4	2	1	-3
0			

$x_0 = 25 \quad y_0 = -75$

$x = 25 + \frac{8}{4}k = 25 + 2k$ $\quad y = -75 - \frac{28}{4}k = -75 - 7k \quad , k \in \mathbb{Z}$

$\begin{cases} x \geq 0 \\ y \geq 0 \end{cases} \Leftrightarrow \begin{cases} 25 + 2k \geq 0 \\ -75 - 7k \geq 0 \end{cases} \Leftrightarrow \begin{cases} k \geq -\frac{25}{2} \\ k \leq -\frac{75}{7} \end{cases}$ $\quad k \in \left[-\frac{25}{2}, -\frac{75}{7}\right]$

$k = -11 \quad x = 25 + 2(-11) = 3$
$\quad y = -75 - 7(-11) = 2$

$k = -12 \quad x = 25 + 2(-12) = 1$
$\quad y = -75 - 7(-12) = 9$

Compra 3 calças e 2 t-shirts/tops
ou
compra 1 calças e 9 t-shirts/tops

$-12{,}5 \quad , -10{,}7$

$k = \{-12, -11\}$

e) m euros e n cêntimos $\rightarrow \boxed{100m + n}$ valor do cheque
deu n euros e m cêntimos $\rightarrow 100n + m$
$+ 111$ cêntimos
$+ 100n + m + 111$ $\quad 200n + 2m + 222$

$200n + 2m + 222 = 100m + n \Leftrightarrow 98m - 199n = 222$ $\quad m \geq 0$, $n \geq 0$, $n < 100$

199		1	0
98	2	0	1
3	32	1	-2
2	1	-32	65
1	2	33	-67
0			

$mdc(98, -199) = 1 \quad 222$ é 1

$199(33) + 98(-67) = 1$

$\times 222$ $\quad 98(-67) - 199(-33) = 1$

$98(-14874) - 199(-7326) = 222$

$m_0 = -14874$
$n_0 = -7326$

$m = -14874 + \frac{-199}{1}k \quad n = -7326 - \frac{98}{1}k \quad , k \in \mathbb{Z}$

$\begin{cases} -1487k - 199k \geq 0 \\ -3326 - 98k \geq 0 \\ -3326 - 98k < 100 \end{cases} \Leftrightarrow \begin{cases} k \leq \frac{1487}{-199} \\ k \leq \frac{3326}{-98} \\ -3426 - 98k < 0 \end{cases} \Leftrightarrow \begin{cases} k \leq -74,74 \\ k \leq -74,95 \\ k > \frac{3426}{-98} > -75,27 \end{cases}$

$k = -75$ $\quad m = -1487k - 199(-75) = 51$ €
$n = -3326 - 98(-75) = 24$

O cheque valia 51 euros e 24 cêntimos 51,24€

Criptografia

25/09/2023

Sistema criptográfico

- Espaço das mensagens (o que se pode encriptar)
- Espaço das chaves (o que se usa para encriptar e desencriptar)
- Regras ou funções → de encriptação
  → de desencriptação

Sistemas criptográficos
- de chave simétrica
- de chave pública (RSA, ...)

Sistemas de chave simétrica

- chave igual
  ou
- muito fácil obter chave de desencriptação através da chave de encriptação

Sistemas de chave pública

- emissor envia mensagem encriptada por chave pública e o recetor desencripta com a chave privada
- recetor gera as duas chaves e envia a chave pública para o emissor
- os agentes podem combinar a chave pública por um canal inseguro

Sistema RSA (Rivest, Shamir, Adelman)

Chave pública

módulo (n, a) → expoente
- pq (p, q primos distintos)
- $a \in \mathbb{N}_{<(p-1)(q-1)}$
- $mdc(a, (p-1)(q-1)) = 1$

$\mathbb{N}_{<k} = \{0, \ldots, k-1\}$

(1)

Chave privada

(n, b) → $b \in \mathbb{N}_{<(p-1)(q-1)}$
→ $ab \equiv_{(p-1)(q-1)} 1$

②

① encriptação: m

$e(m) = \text{mod}(m^a, n)$

m'

Espaço das mensagens

$\{0, 1, 2, \ldots, n-1\}$

② desencriptação:

$d(m') = \text{mdc}((m')^b, n)$

m

α → β

- escolhe primos p, q, e calcula $n = p \times q$
- escolhe $a \in \mathbb{N}_{<(p-1)(q-1)}$ (e) que $\text{mdc}(a, (p-1)(q-1)) = 1$

(n, a)

$e(m) = \text{mod}(m^a, n)$ ←

Calcula $b \in \mathbb{N}_{<(p-1)(q-1)}$ tal que $ab \equiv_{(p-1)(q-1)} 1$

(n, b)

$e(m)$ →

$d(e(m)) = \text{mdc}(e(m)^b, n) = m$

desencripta $e(m)$

ex.

$p = 5 \quad q = 11 \quad n = 55 \quad (55, 3)$ (n, a)

$(p-1)(q-1) = 4 \times 10 = 40$ $\quad 3 \in \mathbb{N}_{<40} \quad \text{mdc}(3, 40) = 1$

$m = 5 \quad e(5) = \text{mod}(5^3, 55) = 15$

$3b \equiv_{40} 1$ $\quad (55, 27)$ (n, b) $\quad 3 \times 27 = 81 \equiv_{40} 1$

$b = 27$

$d(15) = \text{mod}(15^{27}, 55) = 5$

$\text{mod}(15^{27}, 55)$

$15^{27} \equiv_{55} \square$

$16 < 54$

i) $27 = 16 + 8 + 2 + 1$ $\quad 15^{27} \equiv 15^{16} \times 15^8 \times 15^2 \times 15$

ii) $15^2 \equiv_{55} 5$ $\quad 15^2 \equiv_{55} \text{mod}(15^2, 55) = 5$

$15^4 \equiv_{55} 25$ $\quad 25^2 \equiv_{55} \text{mod}(25^2, 55) = 20$

$15^8 \equiv_{55} 25^2 \equiv_{55} 20$ $\quad 20^2 \equiv_{55} \text{mod}(20^2, 55) = 15$

$15^{16} \equiv_{55} 20^2 \equiv_{55} 15$

$15^{27} = 15^{16} \times 15^{8} \times 15^{2} \times 15 \equiv_{55} \underbrace{15 \times 20}_{\equiv 55} \times 5 \times 15 \equiv_{55} \underbrace{25 \times 5}_{\equiv 55} \times 15 \equiv_{55} 15 \times 15 \equiv$

$\hookrightarrow mod(15 \times 20, 55)$ $\quad \hookrightarrow mod(25 \times 5, 55)$ $\quad \equiv_{55} \boxed{5}$

Problemas

26/05/2023

LISTA 5

3.1

e) $\begin{cases} x \equiv_5 3 \\ x \equiv_7 2 \\ x \equiv_8 5 \end{cases}$ Posso aplicar o TCR porque $mdc(5,7)=1$, $mdc(5,8)=1$ e $mdc(7,8)=1$

temos de escrever isto

$56 \equiv_5 1$

$\downarrow$

$56\tilde{n}_1 \equiv_5 \tilde{n}_1$

$56\tilde{n}_1 \equiv_5 1$

$\Leftrightarrow$

$\tilde{n}_1 \equiv_5 1$

K_i	m_i	n_i	$n_i\tilde{n}_i \equiv_{m_i} 1$		$\tilde{n}_i$	$K_i n_i \tilde{n}_i$
3	5	56	$56\tilde{n}_1 \equiv_5 1$	$\tilde{n}_1 \equiv_5 1$	1	168
2	7	40	$40\tilde{n}_2 \equiv_7 1$	$5\tilde{n}_2 \equiv_7 1$	3	240
5	8	35	$35\tilde{n}_3 \equiv_8 1$	$3\tilde{n}_3 \equiv_8 1$	3	525
						$+\ 933 = x_0$

solução particular

$56 \equiv_5 \underbrace{mod(56,5)}_{1}$

$1 \equiv_5 56\tilde{n}_1 \equiv_5 \tilde{n}_1$

$mod(40,7)=5$ $\quad 40 \equiv_7 mod(40,7)$

$mod(35,8)=3$ $\quad 35 \equiv_8 mod(35,8)$

$5 \times 3 = 15$

$15-1=14 \quad 14=7$

$3 \times 3 = 9$

$9-1=8 \quad 8=8$

conjunto das soluções $\rightarrow x = 933 + 280t \quad t \in \mathbb{Z}$

$M = 5 \times 7 \times 8 = 280$

f) $\begin{cases} x \equiv_4 3 \\ x \equiv_7 3 \\ x \equiv_{11} 2 \end{cases}$ Posso aplicar o TCR porque $mdc(4,7)=1$, $mdc(4,11)=1$ e $mdc(7,11)=1$

$mod(77,4)=1$

$mod(44,7)=2$

$mod(28,11)=6$

K_i	m_i	n_i	$n_i\tilde{n}_i \equiv_{m_i} 1$		$\tilde{n}_i$	$K_i n_i \tilde{n}_i$
3	4	77	$77\tilde{n}_1 \equiv_4 1$	$\tilde{n}_1 \equiv_4 1$	1	231
3	7	44	$44\tilde{n}_2 \equiv_7 1$	$2\tilde{n}_2 \equiv_7 1$	4	528
2	11	28	$28\tilde{n}_3 \equiv_{11} 1$	$6\tilde{n}_3 \equiv_{11} 1$	2	112
						$+\ 871 = x_0$

$M = 4 \times 7 \times 11 = 308$

$x = 871 + 308t \quad t \in \mathbb{Z}$

K) $\begin{cases} 8x \equiv_{11} 5 \\ 10x \equiv_{14} 2 \\ 5x \equiv_{20} 15 \end{cases} \Leftrightarrow \begin{cases} x \equiv_{11} 2 \\ 5x \equiv_{14} 1 \\ x \equiv_{20} 3 \end{cases} \Leftrightarrow \begin{cases} x \equiv_{11} 2 \\ 5x \equiv_7 1 \\ x \equiv_4 3 \end{cases} \Leftrightarrow \begin{cases} x \equiv_{11} 2 \\ x \equiv_7 3 \\ x \equiv_4 3 \end{cases}$

$\rightarrow x_0 = 2$ $\quad \rightarrow x_0 = 3$

Posso usar o TCR porque $mdc(11,7)=1$, $mdc(11,4)=1$ e $mdc(7,4)=1$

$\frac{7}{mdc(5,7)} = 7$

K_i	m_i	n_i	$n_i\tilde{n}_i \equiv_{m_i} 1$		$\tilde{n}_i$	$K_i n_i \tilde{n}_i$
2	11	28	$28\tilde{n}_1 \equiv_{11} 1$	$6\tilde{n}_1 \equiv_{11} 1$	2	112
3	7	44	$44\tilde{n}_2 \equiv_7 1$	$2\tilde{n}_2 \equiv_7 1$	4	528
3	4	77	$77\tilde{n}_3 \equiv_4 1$	$\tilde{n}_3 \equiv_4 1$	1	231
						$+\ 871 = x_0$

$M = 4 \times 7 \times 11 = 308$

$x = 871 + 308t, \ t \in \mathbb{Z}$

$x_0 = 5$

1) $\begin{cases} 3x \equiv_{21} 0 \\ 2x \equiv_{14} 4 \\ 6x \equiv_{15} 18 \end{cases} \Leftrightarrow \begin{cases} x \equiv_{\frac{21}{mdc(3,21)}} 5 \\ x \equiv_{\frac{14}{mdc(2,14)}} 2 \\ x \equiv_{\frac{15}{mdc(6,15)}} 3 \end{cases} \Leftrightarrow \begin{cases} x \equiv_8 5 \\ x \equiv_7 2 \\ x \equiv_5 3 \end{cases}$ Posso usar o TCR porque $mdc(8,7)=1$, $mdc(7,5)=1$ e $mdc(8,5)=1$

ver resolução em 3.1 e)

3.2

a) $\begin{cases} x \equiv_{10} 2 \\ x \equiv_{18} 4 \\ x \equiv_{\frac{x}{4}} 12 \end{cases}$ não se pode aplicar TCR porque $mdc(10,18)=2 \neq 1$

mas pode aplicar-se a generalização porque $\begin{cases} k_1 - k_2 = 2-4 = -2 \\ -2 \text{ é múltiplo de } mdc(10,18)=2 \end{cases}$

$k_1 - k_3 = 2 - 12 = -10$

-10 é múltiplo de $mdc(10,20)=10$ e $\begin{cases} k_2 - k_3 = 4 - 12 = -8 \\ -8 \text{ é múltiplo de } mdc(18,20)=2 \end{cases}$

$10 = 2 \times 5$

$18 = 2 \times 3^2$

$20 = 2^2 \times 5$

$mmc(10,18,20) = 2^2 \times 3^2 \times 5 = 180 = mmc(4,9,5)$ (2: único primo comum)

$4 = 2^2 \quad 5 = 5 \quad 9 = 3^2$

C's: 4, 9, 5

- $mmc(10,18,20) = mmc(4,9,5)$
- $mdc(4,5)=1$, $mdc(4,5)=1$ e $mdc(5,5)=1$
- 4 divisor de 20, 9 divisor de 18, 5 divisor de 10

k_i	m_i	c_i	n_i	$n_i \tilde{n}_i \equiv c_i\ 1$		$\tilde{n}_i$	$k n_i \tilde{n}_i$
2	10	5	36	$36\tilde{n}_1 \equiv_5 1$	$\tilde{n}_1 \equiv_5 1$	1	72
4	18	9	20	$20\tilde{n}_2 \equiv_9 1$	$2\tilde{n}_2 \equiv_9 1$	5	400
12	20	4	45	$45\tilde{n}_3 \equiv_4 1$	$1\tilde{n}_3 \equiv_4 1$	1	540
							$+1012 = x_0$

$M = 5 \times 9 \times 4 = 180$

$x = 1012 + 180t, t \in \mathbb{Z}$

c) $\begin{cases} x \equiv_5 2 \\ x \equiv_8 2 \\ x \equiv_{\frac{12}{3}} 10 \end{cases}$ não se pode aplicar TCR porque $mdc(8,12) = 4 \neq 1$

mas pode aplicar-se a generalização porque

$k_1 - k_2 = 2 - 2 = 0$ é múltiplo de $mdc(5,8)=1$ e $k_1 - k_3 = 2 - 10 = -8$, -8 é múltiplo de $mdc(5,12)=1$

$k_2 - k_3 = 2 - 10 = -8$

-8 é múltiplo de $mdc(8,12)=4$

$5 = 5 \quad 8 = 2^3 \quad 12 = 2^2 \times 3 \quad mmc(5,8,12) = 2^3 \times 3 \times 5 = 120 = mmc(8,3,5)$

C's: 8, 3, 5

- $mmc(5,8,12) = mmc(8,3,5)$
- $mdc(8,3)=1$, $mdc(8,5)=1$ e $mdc(3,5)=1$
- $8 \mid 8$, $3 \mid 12$, $5 \mid 5$

$mdc(4,5)=1$

$mdc(15,8)=1$

$mdc(4,3)=1$

k_i	m_i	c_i	n_i	$n_i \tilde{n}_i \equiv c_i\ 1$		$\tilde{n}_i$	$k n_i \tilde{n}_i$
2	8	5	24	$24\tilde{n}_1 \equiv_5 1$	$4\tilde{n}_1 \equiv_5 1$	4	192
2	8	8	15	$15\tilde{n}_2 \equiv_8 1$	$7\tilde{n}_2 \equiv_8 1$	7	210
10	12	3	40	$40\tilde{n}_3 \equiv_3 1$	$\tilde{n}_3 \equiv_3 1$	1	400
							$+802 = x_0$

$M = 120$

$x = 802 + 120t, t \in \mathbb{Z}$

Teoria de Grafos

29/05/2023

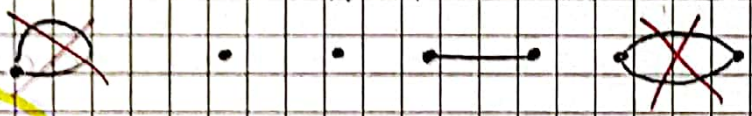
Capítulo 7

Estruturas matemáticas usadas para estudar relações entre pares de entidades.

Os grafos são constituídos por:
- número finito de vértices (ou nós)
- número finito de arestas

Grafo

- cada aresta une dois nós
- entre dois nós há no máximo uma aresta



começa num ponto e termina noutro



início fim

não é possível começar e acabar no mesmo tempo

Variantes

→ se existirem arestas que unem um nó a si próprio: Pseudografo
→ se existirem várias arestas a unir dois nós: Multigrafo
→ se existir informação associada às arestas: Rede
→ se existir orientação (há origem, nó destino) nas arestas (arcos ou setas): Grafo orientado / Digrafo
→ Pseudomultigrafo, Pseudo-rede, Rede orientada

Definição

O grau de um vértice é o número de arestas nele incidente

Teorema: Primeiro Teorema da Teoria dos Grafos

G grafo ou multigrafo

1. A soma dos graus dos nós de G é o dobro do número de arestas (e portanto é par)

$v_1, v_2, v_3, \ldots, v_n$ vértices

$grau(v_1) + grau(v_2) + grau(v_3) + \ldots + grau(v_n) = 2 \times$ nº arestas, nº par

cada aresta é contabilizada 2 vezes



2. Se G tem q vértice de grau ímpar, então q é par

soma dos graus dos vértices de grau ímpar + soma dos graus dos vértices de grau par = nº par

tem de ser par



q parcelas → q tem de ser par

Definição:
Um subgrafo de um (multi)grafo G é um multigrafo constituído apenas por vértices e arestas de G.

Definição
Um caminho num grafo (multigrafo, pseudografo) é uma sequência alternada de vértices $v_1, \dots, v_n$ e arestas $a_1, \dots, a_{n-1}$ $\gamma = \langle v_1, a_1, v_2, a_2, v_3, a_3, \dots, v_n \rangle$ com a_i incidente em v_i em v_{i+1}. No caso de um grafo podem omitir-se as arestas e escrever $\gamma = \langle v_1, v_2, \dots, v_n \rangle$

Diz-se que um caminho

- é **fechado** quando $v_1 = v_n$ e é **aberto** quando $v_1 \neq v_n$
- é um **atalho** se não repete arestas.
- é uma **trajetória** se não repete vértices (exceto se fechado)
- é um **ciclo** se é trajetória fechada com 3 ou mais arestas

Definição
Um (multi)grafo é **conexo** se para quaisquer vértices v_1, v_2 distintos existe um caminho que começa em v_1 e termine em v_2.

atalho fechado com todas as arestas e todos os vértices

↓

atalho euleriano fechado

caminho que não repete arestas; todas as arestas e todos os vértices; 1º e último vértices iguais

TEOREMA DE EULER-HIERHOLZER

G (mult.) grafo

G é euleriano se e só se é conexo e todos os vértices têm grau par

Definição
Uma **ponte** num (multi)grafo G é uma aresta que

- se removida transforma G num grafo desconexo, caso G seja conexo
- se removida aumenta o número de componentes conexas em G, caso G seja desconexo

Algoritmo de Fleury

input: grafo euleriano G
output: atalho euleriano fechado

ver ex. nos slides

Definição
Um (multi)grafo é atravessável se tem um atalho euleriano aberto

Teorema de Euler-Hierholzer (parte 2)

G (multigrafo) — G é atravessável se e só se é conexo e tem exatamente dois vértices de grau ímpar

Problemas

29/05/2023

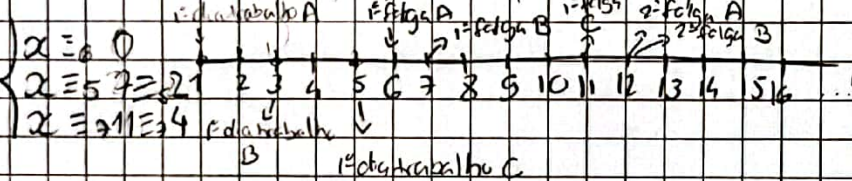
LISTA 5

(3.3)

a) $\begin{cases} x \equiv_4 3 \\ x \equiv_7 3 \\ x \equiv_{11} 2 \end{cases} \xrightarrow[\text{ex. 3.1 f)}]{\text{aula anterior}} x = 871 + 308k, \ k \in \mathbb{Z}$

$t = -2 \rightarrow x = 255$ $\quad \begin{array}{r|l} 871 & 308 \\ \hline \boxed{235} & 2 \end{array}$ $\quad mod(871, 308) = 255$

R: 255 é o mais pequeno inteiro positivo que verifica as condições



(3.6) $\begin{cases} x \equiv_6 0 \\ x \equiv_5 7 \equiv_5 -2 \\ x \equiv_7 11 \equiv_7 4 \end{cases}$

1º dia trabalho A; 1º folga A; 1º folga B; 1º folga C; 2º folga A; 2º folga B; 1º dia trabalho B; 1º dia trabalho C; 2º folga C; 3º folga A

abril a outubro: 214 dias

A: $x = 6k$ ~~$x \equiv_6 0$~~ $x - 0 = 6 \rightarrow 1 = 6k$

B: $x = 5k + 7$

C: $x = 7k + 11$

Pode aplicar-se TCR porque $mdc(6,5) = 1$, $mdc(6,7) = 1$ e $mdc(5,7) = 1$

k_i	m_i	n_i	$n_i \tilde{n}_i \equiv_{m_i} 1$		$\tilde{n}_i$	$k_i n_i \tilde{n}_i$
0	6	35	$35\tilde{n}_1 \equiv_6 1$	$5\tilde{n}_1 \equiv_6 1$	-1	0
2	5	42	$42\tilde{n}_2 \equiv_5 1$	$2\tilde{n}_2 \equiv_5 1$	3	252
4	7	30	$30\tilde{n}_3 \equiv_7 1$	$2\tilde{n}_3 \equiv_7 1$	4	480
						$+732 = x_0$

$M = 210$

Como M é mais pequeno que o intervalo vai sempre haver um dia

$x = 732 + 210t, \ t \in \mathbb{Z}$

$t = 1: x = 522$ $\quad t = 2: x = 312$ $\quad t = 3: x = 102$

R: Vão folgar o 3 dia 11 de julho

$\alpha x \equiv_n \beta \Leftrightarrow x \equiv_{\frac{n}{mdc(\alpha, n)}} x_0$

$\begin{cases} 14x \equiv_{12} 24 \\ 3x \equiv_7 2 \end{cases} \Leftrightarrow \begin{cases} x \equiv_{\frac{12}{mdc(14,12)}} 6 \\ x \equiv_7 6 \end{cases}$

$3 = x_0$ $\quad \Leftrightarrow x \equiv_{\frac{7}{mdc(3,7)}} 3$

$x \equiv_7 3$

LISTA 6

(2) $p = 13$ $\quad q = 11$

a) $(143, 23)$

n módulo da chave; a expoente da chave pública

Chave pública
- $143 = 13 \times 11$
- $23 \in \mathbb{N}_{<120}$
- $mdc(23, 120) = 1$

↳ 23 é primo e $120 \neq 23$

$(p-1)(q-1) = 12 \times 10 = 120$

120		1	0
23	5	0	1
5	4		-5
3	1		21
2	1		-26
1	2		47
0			

Chave privada

$(143, b)$
- $b \in \mathbb{N}_{<120}$
- $23b \equiv_{120} 1$

$23b - 120y = 1$

$23 \times 47 - 120y = 1$

$b = 47 - \frac{120}{1}k \quad k \in \mathbb{Z}$

R: $b = 47$

arc

b) 1º bloco 20

$e(20) = mod(20^{23}, 143) = 80$

$20^{23} \equiv_{143} r$

$\{9, \ldots, 143\}$

i) $23 = 16 + 4 + 2 + 1$

$20^2 = 400 \equiv_{143} \overbrace{mod(400, 143)}^{114}$

no teste: $20^2 \equiv_{143} 114$

$20^4 \equiv_{143} (114)^2 \equiv_{143} \underbrace{mod(114^2, 143)}_{126}$

$20^4 \equiv_{143} 126$

$20^8 \equiv_{143} (126)^2 \equiv_{143} \underbrace{mod(126^2, 143)}_{3}$

$20^8 \equiv_{143} 3$

$20^{16} \equiv_{143} 3^2$

$20^{16} \equiv_{143} 9$

$$\begin{array}{r} 23 \\ -16 \\ \hline 7 \\ -4 \\ \hline 3 \\ -2 \\ \hline 1 \\ -1 \\ \hline 0 \end{array}$$

$20^{23} = 20^{16} \times 20^4 \times 20^2 \times 20 \equiv_{143} \underbrace{9 \times 126}_{mod(9 \times 126, 143)} \times 114 \times 20 \equiv_{143} \underbrace{133 \times 114}_{mod(133 \times 114, 143)} \times 20 \equiv_{143} 4 \times 20 \equiv$

$\equiv_{143} 80$

c) Chave privada $(143, 47)$

$e(80) = mod(80^{47}, 143) = 20$

01/06/2023

Algoritmo de Kruskal

Definição

Uma árvore é um grafo

- que não tem ciclos (trajetória fechada com 3 ou mais arestas)
- é conexo

Teorema

Se $s \neq u$ são vértices de uma árvore T então existe uma e uma só trajetória $\langle s, \ldots, u \rangle$ em T.

Definição

Uma árvore de cobertura de um (multi)grafo G é um subgrafo de G que inclui todos os vértices de G e é uma árvore.

Definição

Uma rede é um grafo a cujas arestas estão associados valores numéricos (custos ou pesos).

Definição

O custo de um caminho numa rede é a soma dos custos das suas arestas. De igual modo se define o custo de um subgrafo da rede.

Definição
Uma árvore de cobertura de custo mínimo de uma rede é uma árvore de cobertura da rede cujo custo é menor ou igual que o custo de qualquer outra árvore de cobertura da rede.

Algoritmo de Kruskal

Input: Rede R
Output: Árvore de cobertura de custo mínimo de R A

S
conjunto de todas as arestas de R
a
eliminar de S a aresta de custo mínimo que ainda lá se encontre

A
todos os nós de R
vértices
+
a
se a não introduzir ciclo na árvore A

Problemas ✧✧ Reconhecimento e representação de linguagens 02/06/2023

Conceitos relevantes
- Alfabeto, palavra e linguagem
- Autómato finito
- Autómato de pilha
- Gramática
- Expressão regular

Definição
Um alfabeto é um conjunto finito e não vazio. Os seus elementos são os símbolos do alfabeto.

Definição
Σ alfabeto
- uma palavra sobre Σ é uma sequência finita de símbolos em Σ
- considera-se também a palavra vazia que se denota por ε
- o comprimento de uma palavra w, denotado por $|w|$, é o número total de símbolos que ocorrem na palavra.
- o conjunto de todas as palavras sobre Σ denota-se Σ^* (incluindo ε)

$\Sigma_1 = \{0, 1\}$ $\quad \Sigma_1^* = \{\varepsilon, \ldots\}$
0 1 100 01 01001 ...
$|\varepsilon| = 0$ $\quad 101001 = 5$

$\Sigma_2 = \{a, b, \ldots, z, 0, \ldots, 9, @, .\}$

@@@.a.b $\notin L$ $\quad$ mpg@gmail.com $\in L$

Definição
Uma linguagem sobre o alfabeto Σ é um conjunto de palavras sobre Σ, isto é, uma linguagem é um subconjunto de Σ^*.

Autómatos finitos determinísticos

Um autómato pode ser especificado

- diagramaticamente (grafo orientado
- algebricamente (conjuntos, funções

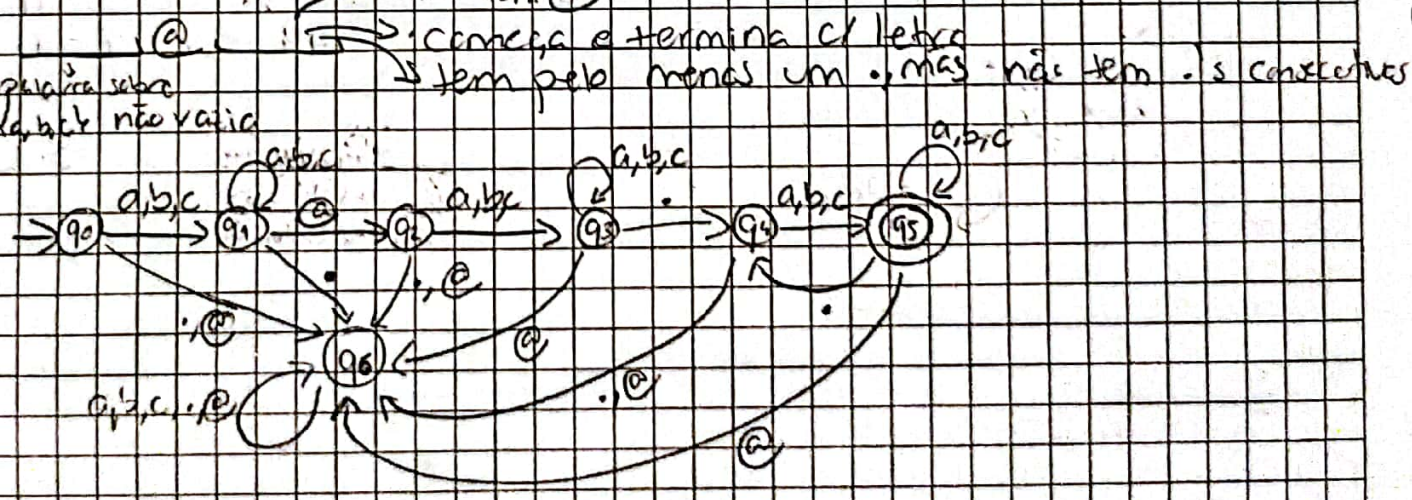
Estas especificações são facilmente convertidas em programas/funções em qualquer linguagem de programação.

Um autómato finito determinístico é constituído por:

- estados
  - em número finito
  - um e um só estado inicial
  - estados finais
  - estados que não são o inicial nem os finais
- transições entre estados
  - a cada transição tem de estar associado um símbolo de um certo alfabeto
  - a partir de cada estado existe uma e uma só transição associada a cada símbolo desse alfabeto

LISTA 8

2.1)



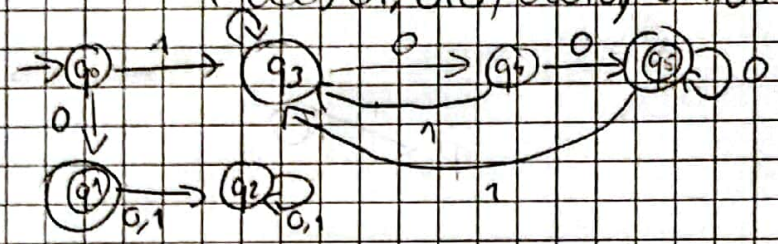
ab@a.c.a
q0 q1 q1 q2 q3 q4 q5 q6
↑ estado final
palavra aceite

ab@.
q0 q1 q2 q6
↑ estado não final
palavra não aceite

2.6

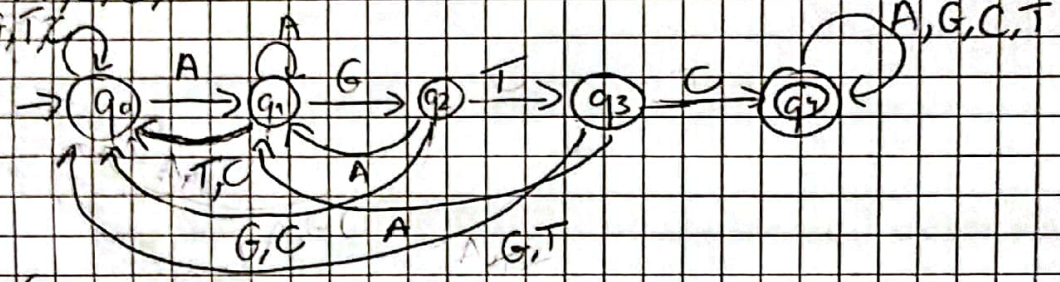
b) $n \equiv_4 0$ $\{0, 100, 1000, 1100, 101000, \ldots\}$ aceites

$1, 000, 01, 010, 00010, 001100$ não aceites

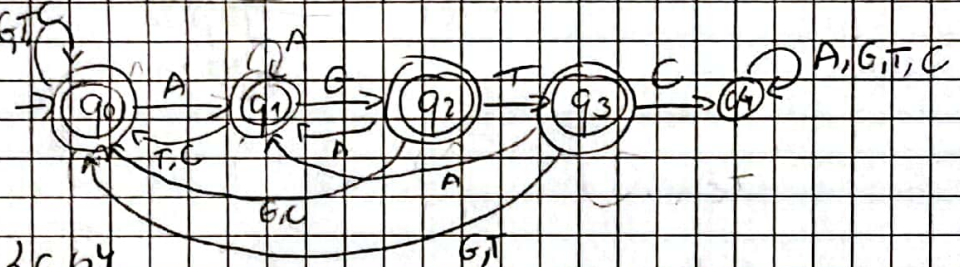


2.2 $\{A, C, G, T\}$

a) G, T, C



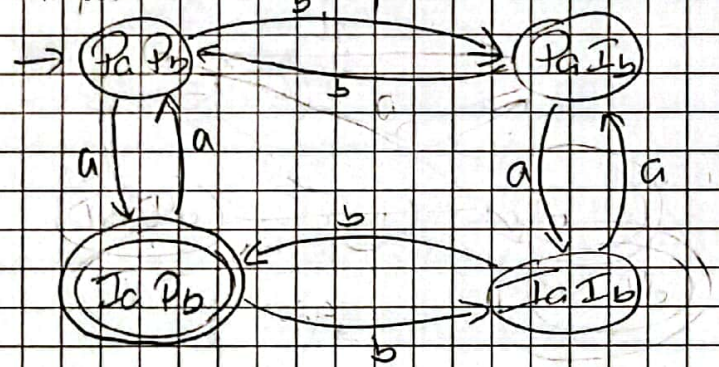
c)



est inicial é final
Σ é aceite
por este autómato

2.4 $\{a, b\}$

a) nº ímpar a's nº par b's



a ✓
aba ✗
bba ✓

Rep. algébrica

$Q = \{PaPb, IaIb, PaIb, IaPb\}$
$\Sigma = \{a, b\}$ $q_0 = PaPb$
$\delta : Q \times \Sigma \to Q$ $F = \{IaPb\}$

δ	a	b
PaPb	IaPb	PaIb
IaIb	PaIb	IaPb
PaIb	IaIb	PaPb
IaPb	PaPb	IaIb

$\delta(PaPb, a) = IaPb$
$\delta(PaPb, b) = PaIb$
⋮

Definição

Um autómato finito determinístico é um quíntuplo $A = (Q, \Sigma, \delta, q_0, F)$ em que

Q é um conjunto finito e não vazio (o conjunto dos estados)
Σ é um conjunto finito e não vazio (o alfabeto)
$\delta : Q \times \Sigma \to Q$ é uma função (a função de transição)
$q_0 \in Q$ (o estado inicial)
$F \subseteq Q$ (o conjunto dos estados de aceitação ou estados finais)

Definição 05/06/2023

Uma rede s-t capacitada (ou rede capacitada) é uma rede

- orientada e conexa
- a cujas setas estão associados números naturais, a capacidade da seta
- sem setas em direção opostas entre dois vértices,

e com

- um vértice especial s (source) que não é destino de nenhuma seta
- um vértice especial t (target) que não é origem de nenhuma seta

Os restantes vértices designam-se por vértices intermédios



ver slides para as outras definições

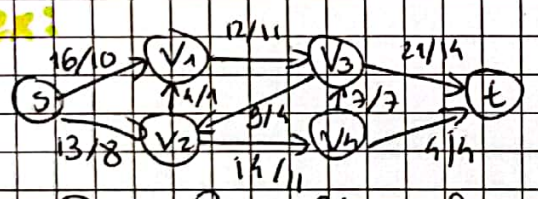
Método/Algoritmo de Ford-Fulkerson

1. Começa-se com fluxo nulo (f_0) - atribui 0 a cada uma das setas

2. Seguindo certos critérios constroem-se sucessivamente fluxos $f_1, f_2, f_3, \ldots$ tal que $val(f_0) < val(f_1) < val(f_2) < \ldots < val(f)$

condição de paragem? f não tem quasi-trajetórias de incremento

ex:



Rede R e fluxo f

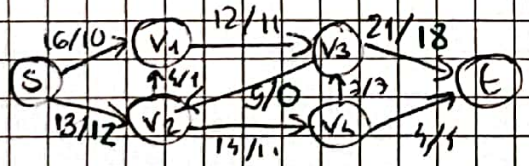
Quasi-trajetória Q_1



Grafo G induzido por R

$Q_1 = \langle s, \overbrace{v_2, v_3}^{-,4}, t \rangle$

$\underbrace{}_{+,5}$ $\underbrace{}_{+,7}$



Novo fluxo f'

$val(f') = val(f) + \Delta f(Q_1)$

$\Delta f(Q_1) = \min(\{5, 4, 7\}) = 4$

capacidade residual de Q_1 relativa a f

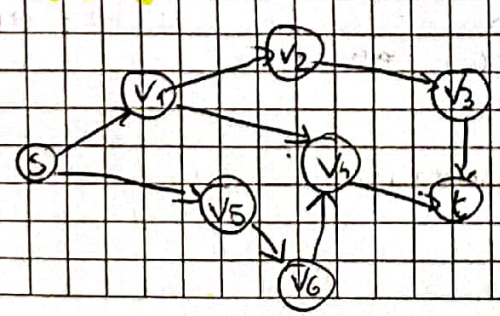
Teorema do fluxo máximo

f é um fluxo máximo

LISTA 3

4.2

b)



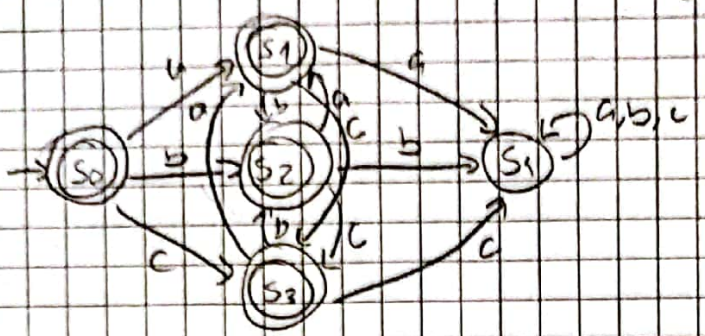
Problemas

05/06/2023

LISTA 3

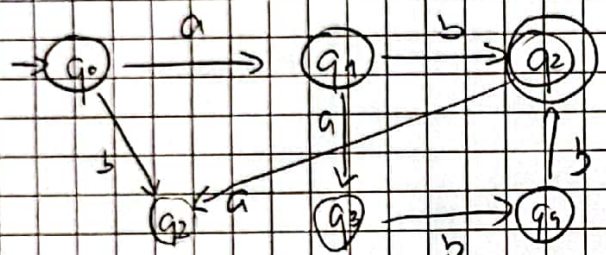
2.3

f) $\{a,b,c\}$ sem símbolos consecutivos iguais, inclui Σ



Ex.: Mostre que é regular a linguagem L das palavras que se escrevem com as letras do alfabeto $\{a,b\}$ e são do tipo $a^n b^n$ com $n \in \mathbb{N}_1$

ab
aabb
aaabbb



Esta linguagem não é regular

$\boxed{afd} \to a^n b^n$

tem nº finito de estados

$$\overbrace{a.a.a.\ldots.a.\ldots.a}^{n\ a's}.\overbrace{b.b.\ldots b}^{n\ b's}$$

q_0 q' q' q_4 final

$a^{n'} b^n$ $n' > n$ $\qquad$ $a^{n'} b^n$ $n' < n$

contradição

Lei da Bombagem para autómatas regulares

$$w = \alpha\beta\gamma$$

1. β tem pelo menos um símbolo
2. $|\alpha\beta| \leq k$ ($\alpha\beta$ tem no máximo k símbolos)
3. $\alpha\beta^n\gamma \in L$, $n \in \mathbb{N}$ $\qquad$ $\alpha\gamma \in L$, $\alpha\beta\beta\gamma \in L$, $\alpha\beta\beta\beta\gamma \in L$

3.1 Suponha-se por absurdo que L é regular. Então verifica o lema da bombagem. Seja $k \in \mathbb{N}_1$, o inteiro garantido pelo lema. Considere-se a palavra

$$a^k b^k \in L$$

i) Como $|a^k b^k| = 2k \geq k$, então $a^k b^k = \alpha\beta\gamma$ onde α, β e γ verificam as propriedades 1, 2 e 3 do lema.

ii) Por 2, $\alpha\beta$ só tem a's. Logo β só tem a's

iii) Seja $\beta = a^m$. Por 1, $m \geq 1$

iv) Por 3, por exemplo, $\alpha\gamma \in L$ $\qquad$ $\alpha\beta\beta\gamma \in L$ $\quad$ $a^{k+m} b^k$ contradição

Mas $\alpha\gamma = a^{k-m} b^k$ o que é uma contradição porque $k-m \neq k$ $(m \geq 1)$

Logo, L não é regular

arc

3.2 Igual às palavras

3.4

palavra $a^{2k}b^k \in L$

i) Como $|a^{2k}b^k| = 3k \geq k$

ii) $xy = a^{2k-m}b^k$ o que é uma contradição. porque $2k-m$ não é o dobro de k

3.5 abb abbbb aabbbb

$a^k b^{k+1} \in L$

i) Como $|a^k b^{k+1}| = 2k+1 \geq k$

ii) $y = a^r$ Para $r \geq 1$, $k \geq 1$

iii) $\alpha\beta\gamma$

Mas $\alpha\beta^2\gamma = a^{k+r}b^{k+1}$ ∴ porque $k+1$ não é maior que $k+r$

3.7 ab aab aaaabb

$a^k b^{k'} \in L$

i) $|a^k b^k| = 2k \geq k$

ii) $\alpha\gamma$

Mas $\alpha\gamma = a^{k-r}b^k$ ∴ porque k não é menor ou igual que $k-r$

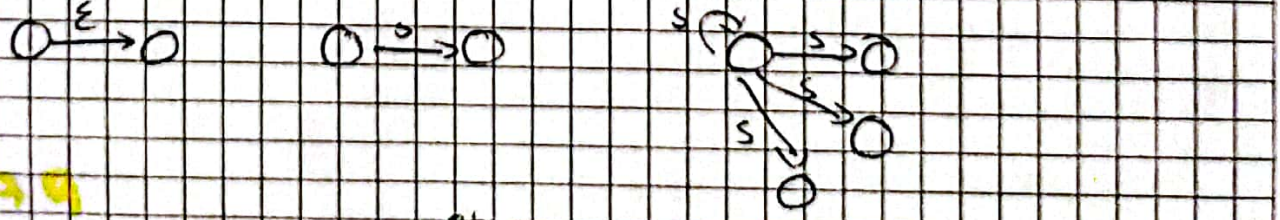
$k \not\leq k-r$

Logo, L não é regular

Autómatos finitos não determinísticos

- transições entre estados

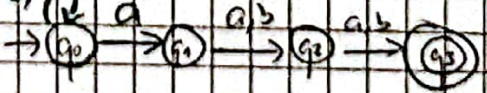
- a cada transição está associado um símbolo de certo alfabeto ou nenhum (estas designam-se transições-ε)
- a partir de um estado pode existir mais de uma transição associada a um símbolo desse alfabeto



LISTA 9

9.3

a) abb
aaa
abb
aab



bababa

$q_1 - q_0 - q_1 - q_2 - (q_3)$ → fim

$q_0 - q_1 - q_2$

q_1

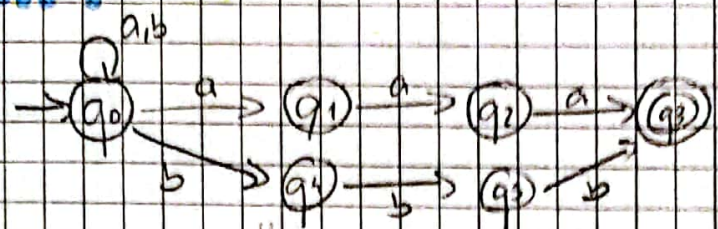
Problemas

LISTA 1

03/06/2023

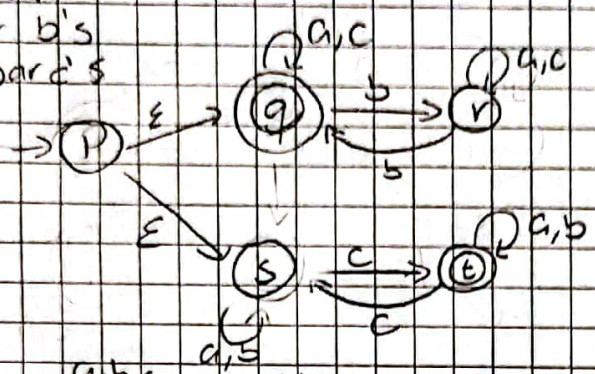
2.2

a)



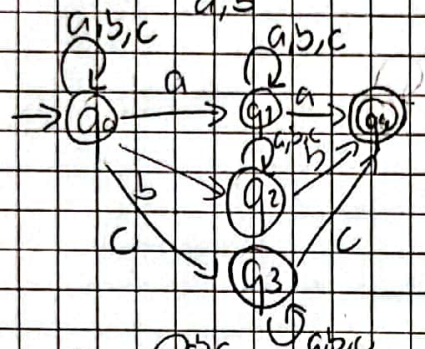
2.3 {a,b,c}

c) nº par b's
nº ímpar c's

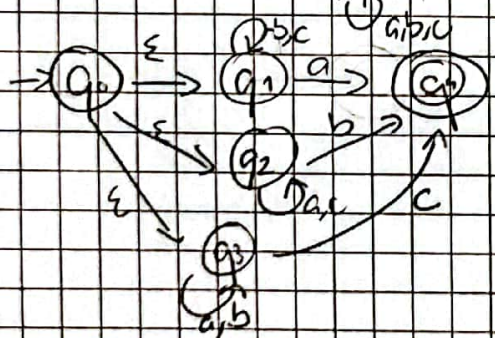


p-q-q-q-r
s-s-t-t final
palavra aceite

b)



a)



N af não determinístico

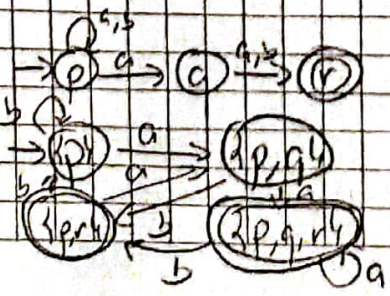
↓ Passo 1

N' af não determinístico sem transições -ε

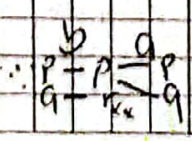
↓ Passo 2

A af determinístico (equivalente a N)

3.7



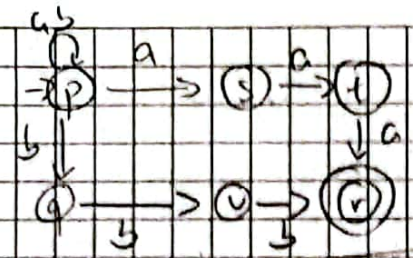
af ñ deter. ñ há transições -ε só se aplica passo 2



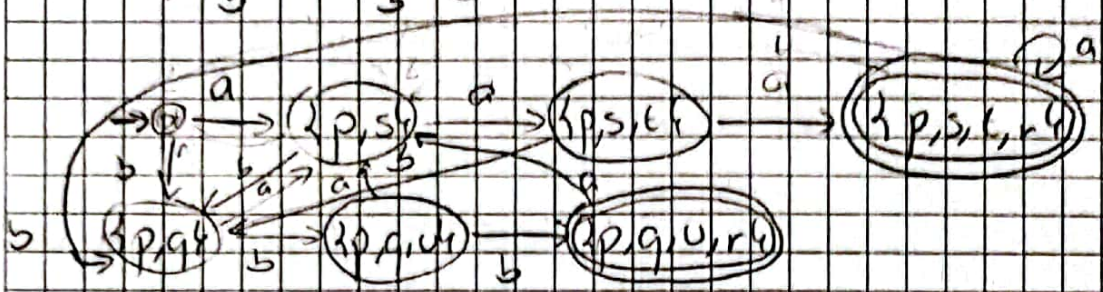


os finais são os que têm r

3.6



	a	b	ε
p	{p,s}	{p,q}	{}
q	{}	{u}	{}
r	{}	{}	{}
s	{t}	{}	{}
t	{r}	{}	{}
u	{}	{r}	{}

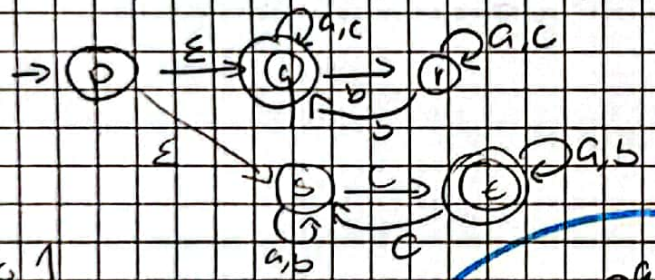


	a	b
{p}	{p,s}	{p,q}
{p,s}	{p,s,t}	{p,q}
{p,q}	{p,s}	{p,q,u}
{p,s,t}	{p,s,t,r}	{p,q}
{p,q,u}	{p,s}	{p,q,u,r}
{p,s,t,r}	{p,s,t,r}	{p,q}
{p,q,u,r}	{p,s}	{p,q,u,r}

estado inicial: {p}

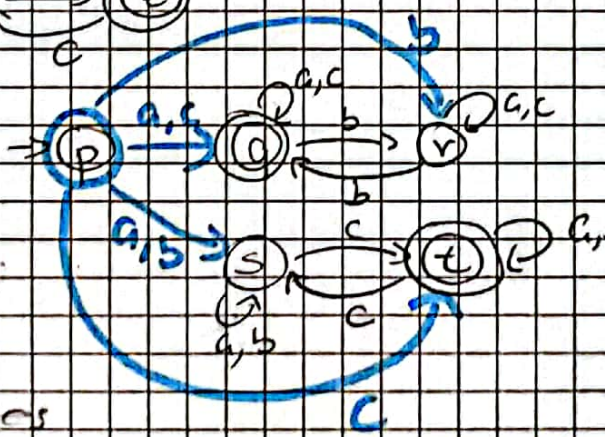
conjunto dos estados finais: {p,s,t,r} e {p,q,u,r}

3.10



Passo 1

os mesmos estados
mesmo estado inicial
mesmas transições
mesmos estados finais



Primeiro teorema da teoria dos grafos

LISTA 7

12/06/2023

1.1 Não é possível porque o grafo tem um total de 3 vértices de grau ímpar (2 de grau 3 e 1 de grau 5) o que contradiz o resultado que estabelece que se um grafo tem um total de n vértices de grau ímpar então n é par

Alternativa

Soma dos graus dos vértices = 2x3+2x4+2+5 = 21 ≠ dobro do nº de arestas porque 21 é ímpar logo não é possível

(1.4) A situação pode ser modelada por um grafo G com
- 15 vértices (os 15 deputados)
- Existe aresta d_i — d_j se e só se d_i e d_j já estiveram numa mesma comissão anterior
- 5 ($= \frac{15}{3}$) vértices têm grau 3
- 10 vértices têm grau 0

Como G teria um total de 5 vértices de grau ímpar, alguém se enganou, pois em qualquer grafo o nº total de vértices de grau ímpar é par

(1.5) G grafo com n vértices
G é completo, logo cada vértice tem grau n-1
Pelo primeiro teorema da teoria dos grafos

$n(n-1) = 2 \times$ nº arestas $\Rightarrow$ nº arestas $= \frac{n(n-1)}{2}$

↓
soma dos graus dos vértices

Problema ✦

12/06/2023

(3) p = 19 q = 67 (1273, 25) → chave pública

a) (1273, 25)
Smodule sexpoente
- $19 \times 67 = 1273$
- $25 \in \mathbb{N}_{<1188}$
- $mdc(1188, 25) = 1$ justificação ver adiante

$18 \times 66 = 1188$

chave privada: (1273, b)
módulo

- $b \in \mathbb{N}_{<1188}$
- $25b \equiv_{1188} 1$
- $25b - 1188y_0 = 1$

1188		1	0
25	47	0	1
13	1	1	-47
12	1	1	48
1	12	1	-95
0			

$mdc(1188, 25) = 1$

$25(-95) - 1188y_0 = 1$

$b = -95 - \frac{1188}{1}k \quad k \in \mathbb{Z}$

↓ k = -1

$b = -95 + 1188 = 1093$

chave privada: (1273, 1093)

b) chave pública (1273, 25)

$e(54) = mod(54^{25}, 1273)$

$54^{25} \equiv_{1273} r \in \{0, \ldots, 1272\}$ $\exists!\, r = mod(\ldots)$

$mod(54^{25}, 1273)$

Teste

$25 = 16 + 8 + 1$

$54^2 \equiv_{1273} 685^2 \equiv_{1273} 1165$

$54^4 \equiv_{1273} 370^2 \equiv_{1273} 685$

$54^{16} \equiv_{1273} 1165^2 \equiv_{1273} 207$

$54^{25} = 54^{16} \times 54^8 \times 54 \equiv_{1273} 207 \times 1165 \times 54 \equiv_{1273} 558 \times 54 \equiv_{1273} 853$

só vai subir 1 ao 5 ao 16 ao 5 ao 1 ao 0

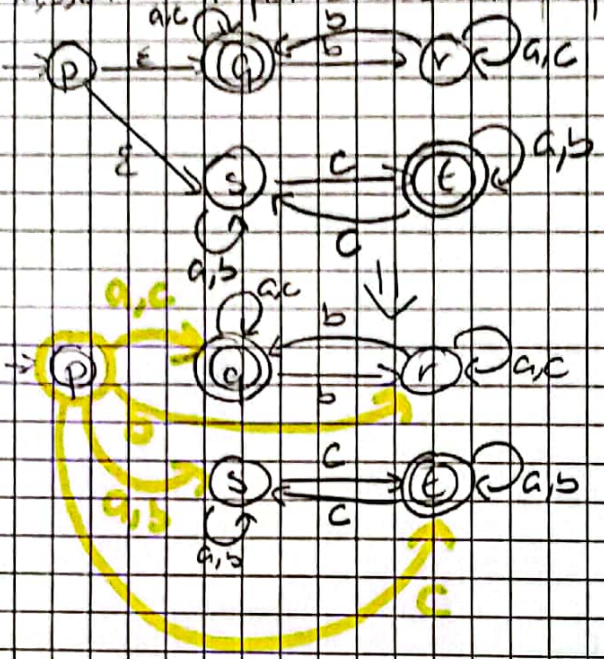
$mod(54^2, 1273) = 370$
$mod(370^2, 1273) = 685$
$mod(685^2, 1273) = 1165$
$mod(1165^2, 1273) = 207$
$mod(207 \times 1165, 1273) = 558$
$mod(558 \times 54, 1273) = 853$

exemplação
$c(54) = 853$

arc

LISTA A

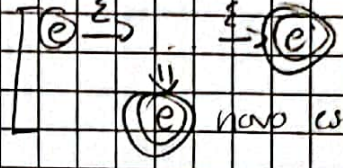
3.10) {a,b,c}* nº par b's ou nº ímpar de c's



fecho-ε(p) = {p, q, s}
fecho-ε(q) = {q}
fecho-ε(s) = {s}
fecho-ε(r) = {r}
fecho-ε(t) = {t}

Passo 1 - tirar transições-ε

Novo estados finais



δ'	a	b	c
p	{q,s}	{r,s}	{q,t}
q	{q}	{r}	{t}
r	{r}	{q}	{r}
s	{s}	{s}	{t}
t	{}	{t}	{}

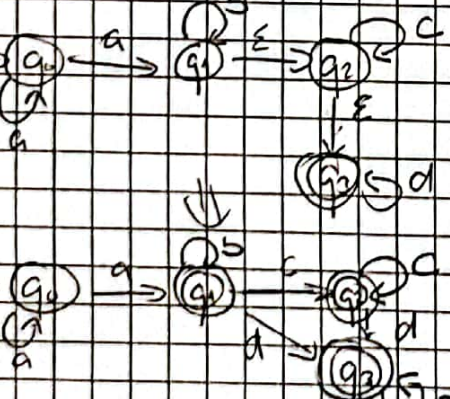
Passo 2 ⇒

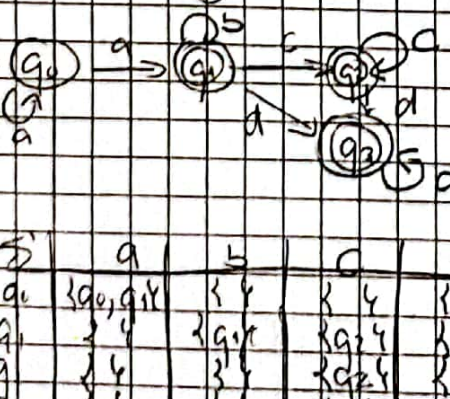
	a	b	c
→p	{q,s}	{r,s}	{q,t}
{q,s}	{q,s}	{r,s}	{q,t}
{r,s}	{r,s}	{q,s}	{t,t}
{q,t}	{q,t}	{r,t}	{q,s}
{r,t}	{r,t}	{q,t}	{r,s}

estado inicial

conjunto dos estados finais: {p}, {q,s}, {q,t}, {r,t}

3.11)





fecho-ε(q0) = {q0}
fecho-ε(q1) = {q1, q2, q3}
fecho-ε(q2) = {q2, q3}
fecho-ε(q3) = {q3}

Passo 1

δ'	a	b	c	d
q0	{q0, q1}	{}	{}	{}
q1	{}	{q1}	{q2}	{q3}
q2	{}	{}	{q2}	{q3}
q3	{}	{}	{}	{q3}

Passo 2 ⇒

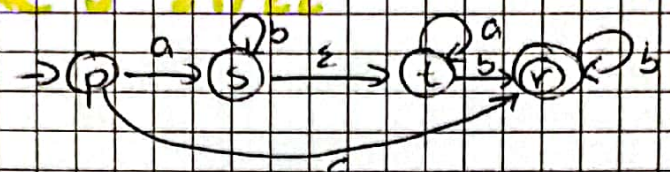
	a	b	c	d
→{q0}	{q0, q1}	{}	{}	{}
{q0, q1}	{q0, q1}	{q1}	{q2}	{q3}
{q1}	{}	{q1}	{q2}	{q3}
{q2}	{}	{}	{q2}	{q3}
{q3}	{}	{}	{}	{q3}

estado inicial: {q0}

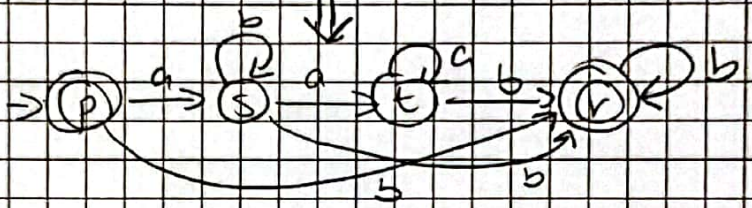
conjunto dos estados finais: {q0, q1}, {q1}, {q2}, {q3}

by Stardes

Teste 3 21/22



Passo 1



δ	a	b
p	{s}	{r}
s	{t}	{s, r}
t	{t}	{r}
r	∅	∅

Passo 2 ⇒

	a	b
{p}		

estado inicial: {p}
Cj estados finais: {p},

Instituto Superior Técnico - Departamento de Matemática
Licenciatura em Engenharia de Telecomunicações e Informática

Matemática Discreta
Teste 1-MAP 45 (Versão A)

Duração: 45m

Cotação : 20 valores

Grupo 1 (5.5+5.5 valores)

Calcule uma forma fechada para cada um dos somatórios seguintes:

1. $\sum_{k=1}^{n}(4k^3 - 12k^2 + 5k)$

2. $\sum_{k=0}^{n-1} \frac{1}{(5k+1)(5k+11)}$

Grupo 2 (3 valores)

Calcule a derivada finita da sucessão de termo geral $u_k = \frac{k!}{2^k}$ e use-a para obter uma forma fechada do somatório

$$\sum_{k=0}^{n} \frac{k!(k-1)}{2^k}$$

Grupo 3 (6 valores)

Use indução matemática para demonstrar que para todo o $n \in \mathbb{N}_1$ se tem que

$$\sum_{k=1}^{n} \frac{1}{k^2} \leq 2 - \frac{1}{n}$$

$(K!)' = (K+1)! - K! = (K+1)K! - K! = K!(K+1-1) = KK!$

$U_K = 5K-4 \qquad U_{K+1} = 5(K+1)-4 = 5K+1 \qquad U_{K+2} = 5(K+2)-4 = 5K+6$

$U_{K+3} = 5(K+3)-4 = 5K+11$

Grupo 1

① $\sum_{K=1}^{n} (4K^3 - 12K^2 + 5K) = 4\sum_{K=1}^{n} K^3 - 3\sum_{K=1}^{n} K^2 = (n+1)n(n-1)(n-2) - \frac{3}{2}n(n+1)$

② $\sum_{K=0}^{n-1} \frac{1}{(5K+1)(5K+11)} = \sum_{K=0}^{n-1} \frac{(5K+6+5)-5}{(5K+1)(5K+6)(5K+11)} = \sum_{K=0}^{n-1} \frac{1}{(5K+1)(5K+6)} - 5\sum_{K=0}^{n-1} \frac{1}{(5K+1)(5K+6)(5K+11)}$

$U_K \quad U_{K+1} \quad U_{K+2}$

$U_{K+2} = 5K+6$

$= \sum_{K=0}^{n-1} (5K-4)^{-2} - 5\sum_{K=0}^{n-1} (5K-4)^{-3} = \ldots = -\frac{1}{5(5n+1)} + \frac{1}{5} - 5\left(-\frac{1}{10(5n+1)(5n+10)}\right)$

Grupo 2

$(U_K)' = \frac{K!(K-1)}{2^{K+1}} \qquad 2\sum_{K=0}^{n} \frac{K!(K-1)}{2^{K+1}} = 2\sum_{K=0}^{n} \left(\frac{K!}{2^K}\right)' = 2\left(\frac{(n+1)!}{2^{n+1}} - \frac{(0+1)!}{2^0}\right) =$

$= 2\left(\frac{(n+1)!}{2^{n+1}} - 1\right)$

Instituto Superior Técnico - Departamento de Matemática
Licenciatura em Engenharia de Telecomunicações e Informática

Matemática Discreta
Teste 2-MAP 45 (versão B)

Duração: 45m

Cotação : 20 valores

Grupo 1 (6 valores)

Usando funções geradoras, resolva a recorrência $s_0 = 2,\ s_1 = 0$ e $s_k = -4s_{k-1} + 12s_{k-2}$ $(k \in \mathbb{N}_2)$.

Grupo 2 (7 valores)

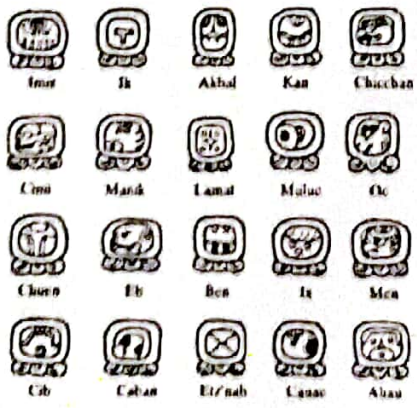
Recorrendo ao que aprendeu sobre equações diofantinas e sua resolução resolva o seguinte problema. Um certa companhia de aviação vende bilhetes para um determinado destino a preços que variam com a antecedência com que a viagem é marcada e paga. Os vôos mais caros, que, havendo ainda disponibilidade, podem ser comprados até à véspera da viagem, custam 370€. Bilhetes pagos até um mês antes da viagem custam 260€. Os mais baratos, pagos até dois meses antes da viagem têm um custo de 110€. A companhia recebeu um total de 26600€ relativo a um determinado vôo para este destino. Quantos passageiros compraram bilhete, e quantos bilhetes foram vendidos de cada tipo, sabendo que o número de bilhetes mais baratos vendidos é o dobro do número dos de preço intermédio, e que foram vendidos menos de 50 dos mais caros?

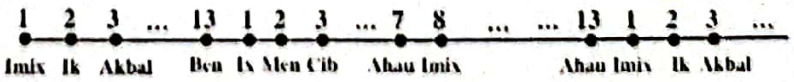
Grupo 3 (5+2 valores)

1. Calcule o conjunto de todas as soluções do sistema de congruências

$$\begin{cases} 2x & \equiv_6 & 4 \\ x & \equiv_{10} & 3 \\ x & \equiv_{11} & 1 \end{cases}$$

2. Indique, <u>sem resolver</u>, um sistema de congruências que lhe permita solucionar o seguinte problema. Os dias do calendário dos Maias são designados através de número de 1 a 13 e de um de 20 nomes, na ordem da figura abaixo. A contagem dos dias é assim: 1 Imix, 2 Ik, 3 Akbal,..., 13 Ben, 1 Ix,..., 7 Ahau, 8 Imix,..., até 13 Ahau, dia após o qual recomeça a contagem em 1 Imix. Um certo acontecimento importante para este povo ocorreu no dia 1 Imix do seu calendário, dia que no calendário ocidental foi um sábado (de um certo ano não relevante para a resolução do problema). Determine quantos dias após esse acontecimento o dia 5 Ix no calendário dos Maias é um domingo no nosso calendário.





$\frac{3}{2} + 9z + \frac{1}{2} - z = 2 + 8z$ ✓

Grupo 1

$S_k = \frac{3}{2} 2^k + \frac{1}{2}(-6)^k$

Grupo 2

140 passageiros
80 de 110€
40 de 260€
20 de 370€

Grupo 3

① $\begin{cases} x \equiv_3 2 \\ x \equiv_{10} 3 \\ x \equiv_{11} 1 \end{cases}$

$2x \equiv_6 4 \iff x \equiv_{\frac{6}{mdc(6,2)=2}} 2$

$\ldots \tilde{n}_i$	$k_i n_i \tilde{n}_i$
2	440
$\ldots -3$	-297
-4	-120
	$23 = x_0$

$M = 330$

$x = 23 + 330t, t \in \mathbb{Z}$

②

Sábado → domingo ⇒ 1 dia

$13 \times 20 = 260$ dias periodicidade Maias

7 dias periodicidade ocidental

$\begin{cases} x \equiv_{260} 0 \\ x \equiv_7 1 \end{cases}$

Instituto Superior Técnico - Departamento de Matemática
Licenciatura em Engenharia de Telecomunicações e Informática

Matemática Discreta
Teste 3-MAP 45 - versão A

Duração: 45m — Cotação : 20 valores

Grupo 1 (4 valores)

Considere o sistema criptográfico de chave pública RSA com primos $p = 17$ e $q = 47$.

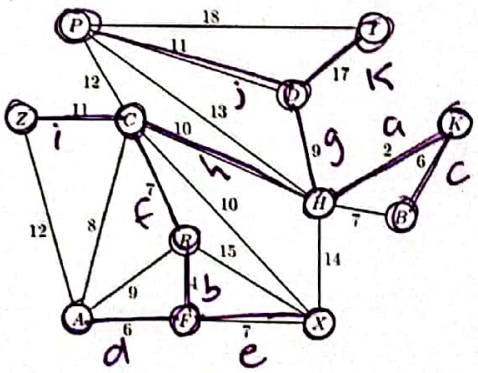
1. Explique porque é $(799, 21)$ uma chave pública possível neste sistema, e calcule a chave privada correspondente.

2. Pretende-se usar a chave pública indicada para encriptar a *password temporária* 72558480, que para tal é dividida previamente em blocos de dois dígitos. Encripte de **forma eficiente** o bloco 80.

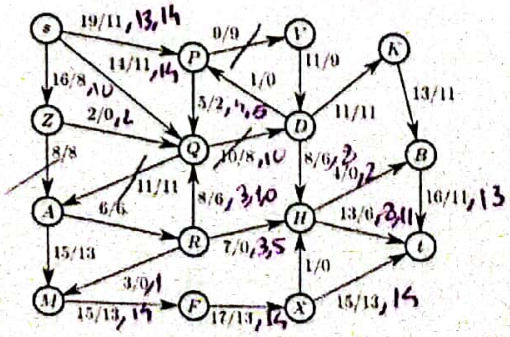
3. Explique como a partir da encriptação recebida se recupera o bloco encriptado na alínea anterior (<u>não</u> é necessário efetuar cálculos).

Grupo 2 (2.5+4+2.5 valores)

1. Aplique o algoritmo de Kruskal à rede seguinte para obter uma árvore de cobertura de custo mínimo para esta rede. *Apresente a resolução na folha com a cópia do grafo que lhe foi distribuída. Deve indicar claramente sobre a figura a ordem pela qual as arestas foram sendo selecionadas.*



2. Considere a rede s-t capacitada seguinte e suponha que, após várias iterações do algoritmo Ford-Fulkerson, se obteve o fluxo nela representado (a capacidade de cada seta é o valor à esquerda, e o fluxo é o valor à direita)



$Q_1 = \langle s, P, Q, D, H, t \rangle$
$\Delta Q_1 = 2$
$Q_2 = \langle s, Q, R, H, t \rangle$
$\Delta Q_2 = 3$
$Q_3 = \langle s, Z, Q, R, H, B, t \rangle$
$\Delta Q_3 = 2$
$Q_4 = \langle s, P, Q, R, M, X, t \rangle$
$\Delta Q_4 = 1$

(vire sff)

(i) Continue a aplicar o algoritmo para obter um fluxo máximo, e no fim indique o valor do fluxo obtido (não se esqueça de ir indicando as quasi-trajetórias de incremento usadas, numeradas pela ordem que foram consideradas e respetivas capacidades residuais). (ii) Indique depois um corte mínimo e a respetiva capacidade, e enuncie o teorema que garante que é um corte mínimo. *Apresente a resolução na folha com a cópia da rede que lhe foi distribuída.*

3. **Na resposta a esta questão deve recorrer a teoremas sobre grafos que estudou, e deve enunciar claramente todos os que usar.** Um grafo conexo $\mathcal{G}$ tem 20 vértices e 78 arestas. Cada vértice de $\mathcal{G}$ ou tem grau 10, ou tem grau 8 ou tem grau 7. Há 5 vértices de grau 10. Quantos vértices de $\mathcal{G}$ têm grau 8? Quantos vértices têm grau 7? Se for conexo, este grafo é atravessável?

Grupo 3

(4+3 valores)

1. Especifique um autómato finito determinístico que aceite todas as palavras sobre o alfabeto $\{a, b, c\}$ que começam em c e nas quais a sequência *aba* ocorre uma e uma só vez, e apenas essas. Por exemplo *caabacab* deve ser aceite, mas *cbab* e *cababa* não devem ser aceites.

2. O que significa dizer que uma linguagem L é regular? Enuncie o lema da bombagem para linguagens regulares e, de seguida, use-o para justificar que a linguagem L das palavras sobre o alfabeto $\{x, y\}$ que são palíndromos não é regular. Diz-se que uma palavra é um palíndromo se é igual quer se leia da direita para a esquerda, quer da esquerda para a direita. Por exemplo, $xyyxyyx$ e $yyxxxyy$ são palíndromos, mas $xxyy$ e $yyxy$ não são.

Versão A

Grupo 1

$mod(80^2, 799) = 8$

$mod(8^2, 799) = 64$

$mod(64^2, 799) = 101$

$mod(101^2, 799) = 613$

$mod(613 \times 64, 799) = 81$

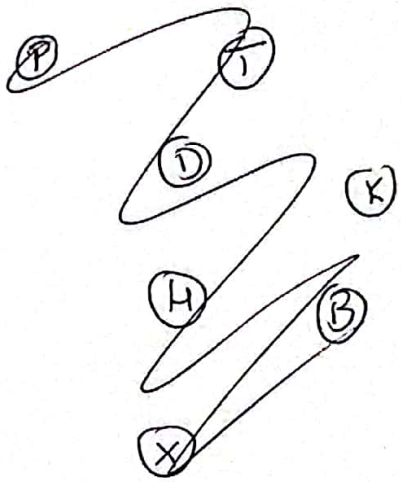
$mod(81 \times 80, 799) = 88$

① c.pris $(799, 701)$

② $e(80) = mod(80^{21}, 799) = 88$

③ $d(88) = mod(88^{701}, 799)$

Grupo 2



① custo 90

② fluxo: $38 = 13 + 11 + 14$

ii) corte: $\overrightarrow{ZA}, \overrightarrow{QA}, \overrightarrow{QD}, \overrightarrow{PV}$

capacidade: $8 + 11 + 10 + 9 = 38$

③ $20 - 15 = 15$ vértices

$\overset{5\times10}{50} + 8x + 7y = \overset{2\times78}{156}$ y é par

$8x + 7y = 106$

$mdc(8, 7) = 1$

$8 \times 106 + 7(-106) = 106$

$x = 106 + 7k$ $\quad y = -106 - 8k$

$k = -15$: $x = 1$, $y = 14$ $\Rightarrow$ 15 vértices

1 de grau 8

14 de grau 7

Não é atravessável

Grupo 3

①

