FUNDAMENTOS DE MATEMÁTICA PARA A COMPUTAÇÃO

1o. SEMESTRE DE 2018

EXERCÍCIOS

Entrega. Entregue suas soluções no Paca. Soluções entregues fora de prazo valerão menos.

Política de colaboração e uso de fontes. Todo trabalho entregue por você deve ser seu. Você é encorajado a discutir com seus colegas o material visto em sala e os enunciados dos exercícios, mas tome cuidado para não compartilhar seu trabalho além do permitido. Nos *exercícios individuais*, você não pode compartilhar suas soluções ou mesmo ideias de soluções. Nos *exercícios em grupo*, você só pode compartilhar suas ideias e soluções com membros de seu grupo. Nos exercícios em grupo, *cada membro do grupo deve escrever uma solução própria*—esta disciplina tem como um de seus objetivos estudar como escrever matemática e portanto o processo de escrita será enfatizado, mesmo nos exercícios em grupo. Ao entregar um exercício feito em grupo, não esqueça de escrever o nome de todos os membros do grupo em sua solução.

Você não deve procurar soluções de terceiros (como de amigos ou na Web). Caso você acidentalmente encontre a solução de algum exercício em algum lugar, você deve citar esta fonte em sua solução. Caso você acidentalmente acabe colaborando com colegas na descoberta de uma solução, você deve citar esta colaboração em sua solução. Seu desempenho nesta disciplina ficará prejudicado caso você viole essas regras.

Fontes dos exercícios. Vários dos exercícios vêm de nossa bibliografia. Usamos as seguintes abreviaturas (outras abreviaturas poderão ser adicionadas posteriormente). **MH:** Michael Hutchings, *Introduction to mathematical arguments*; **KH:** Kevin Houston, *How to think like a mathematician*; **DJV:** Daniel J. Velleman, *How to prove it.*

Exercícios para entrega. Os exercícios para entrega estão marcados com uma data de entrega. Nesses exercícios, há também indicação se é um exercício individual ou se pode ser feito em grupo. No caso de exercícios em grupo, o número máximo de alunos por grupo está especificado.

* * * * *

E1 Faça os exercícios de 1 a 7, p. 27, de **MH**.

E2 Faça o Exercício 1.34 de **KH**.

E3 A *diferença simétrica* $A \triangle B$ de dois conjuntos A e B é o conjunto $(A \cup B) \setminus (A \cap B)$. Prove que a operação de diferença simétrica é associativa, isto é, que $A \triangle (B \triangle C) = (A \triangle B) \triangle C$ para quaisquer conjuntos A, B e C. **{*Data de entrega*: 14/3/2018; exercício individual}**

E4 Faça o Exercício 6.11(ii) de **KH**.

E5 Faça o Exercício 6.11(iv) de **KH**.

E6 Faça os exercícios de 1 a 17 da Seção 1.2 de **DJV**.

Date: Versão de 2018/6/27, 7:06pm.

E7 Seja n um inteiro positivo. Sejam $x_1, \dots, x_n$ variáveis booleanas. Dado $S \subset [n]$, definimos as fórmulas φ_S, ψ_S e γ_S como segue:

$$\varphi_S = \bigvee_{i \in S} x_i, \qquad \psi_S = \bigvee_{i \in [n] \setminus S} \neg x_i \qquad \text{e} \qquad \gamma_S = \varphi_S \vee \psi_S. \tag{1}$$

Finalmente, seja

$$\Phi_n = \bigwedge_{S \subset [n]} \gamma_S. \tag{2}$$

Por exemplo, se $n = 2$ e $S = \{2\}$, temos $\gamma_S = \neg x_1 \vee x_2$. Ademais,

$$\Phi_2 = (x_1 \vee x_2) \wedge (x_1 \vee \neg x_2) \wedge (\neg x_1 \vee x_2) \wedge (\neg x_1 \vee \neg x_2). \tag{3}$$

(*i*) Suponha que $n = 3$ e $S = \{2, 3\}$. Diga o que é φ_S.
(*ii*) Diga o que é Φ_3.
(*iii*) Mostre que Φ_n é insatisfatível para qualquer valor de n.
[*Observação.* Você pode ficar na dúvida o que são $\varphi_\emptyset$ e $\psi_{[n]}$. Vale que $\gamma_\emptyset = \bigvee_{i \in [n]} \neg x_i$ e $\gamma_{[n]} = \bigvee_{i \in [n]} x_i$.] **{*Data de entrega*: 21/3/2018; exercício individual}**

E8 Faça o Exercício 10.11 de **KH**.

E9 Faça os itens (i) a (iv) do Exercício 11.12 de **KH**.

E10 Considere a afirmação p dada abaixo:

$$p = (\forall x,\, y \in \mathbb{R})\big(x < y \Rightarrow (\exists z \in \mathbb{R})(x < z < y)\big). \tag{4}$$

(*i*) Determine a negação $\neg p$ de p.
(*ii*) Diga em palavras (“em linguagem humana”) o significado de p e de $\neg p$.
(*iii*) A afirmação p é verdadeira? A afirmação $\neg p$ é verdadeira? Justifique.
{*Data de entrega*: 28/3/2018; exercício individual}

E11 Considere a afirmação q dada abaixo:

$$q = (\forall x,\, y \in \mathbb{N})\big(x < y \Rightarrow (\exists z \in \mathbb{N})(x < z < y)\big). \tag{5}$$

(*i*) Determine a negação $\neg q$ de q.
(*ii*) Diga em palavras (“em linguagem humana”) o significado de q e de $\neg q$.
(*iii*) A afirmação q é verdadeira? A afirmação $\neg q$ é verdadeira? Justifique.
{*Data de entrega*: 28/3/2018; exercício individual}

E12 Faça os itens (i), (ii) e (iii) do Exercício 20.14 de **KH**. [*Observação.* No item (i), basta encontrar o erro na demonstração proposta.]

E13 Faça o maior número possível dos itens (iv) a (xi) do Exercício 20.14 de **KH**.

E14 Faça os item (x) do Exercício 20.14 de **KH**. **{*Data de entrega*: 4/4/2018; exercício individual}**

E15 Prove que a hipótese de n ser ímpar no Exercício 20.14(x) de **KH** é necessária.

E16 Faça o maior número possível dos itens (i) a (ix) do Exercício 22.10 de **KH**.

E17 Fixe um inteiro $d \geq 1$. Sabemos que, para todo inteiro n, exitem inteiros q e r com $0 \leq r < d$ tais que $n = dq + r$. Ademais, sabemos que tais q e r são únicos. Para cada $0 \leq r < d$, seja

$$A_r = \{n \in \mathbb{Z} \colon n = dq + r \text{ onde } q \text{ e } r \in \mathbb{Z} \text{ e } 0 \leq r < d\}. \tag{6}$$

Seja $\mathcal{P} = \{A_0, \dots, A_{d-1}\}$. Prove que $\mathcal{P}$ é uma partição de $\mathbb{Z}$.

E18 Para todo inteiro $n \geq 1$, seja

$$\mathcal{P}_n = \big\{\{X, [n] \setminus X\} \colon X \subset [n-1]\big\}. \tag{7}$$

Assim, $\mathcal{P}_1 = \big\{\{\emptyset, \{1\}\}\big\}$ e $\mathcal{P}_2 = \big\{\{\emptyset, \{1,2\}\}, \{\{1\}, \{2\}\}\big\}$.

(i) Diga o que é $\mathcal{P}_3$ explicitamente.

(ii) Qual é a cardinalidade de $\mathcal{P}_n$?

(iii) Prove que $\mathcal{P}_n$ é uma partição de $\mathcal{P}([n])$.

E19 Seja X um conjunto e $\mathcal{F} \subset \mathcal{P}(X)$. Dizemos que $\mathcal{F}$ é *intersectante* se, para quaisquer F e $F' \in \mathcal{F}$, temos $F \cap F' \neq \emptyset$, isto é, quaisquer dois membros de $\mathcal{F}$ tem algum elemento em comum. Suponha agora que X seja finito. Seja n a cardinalidade $|X|$ de X e suponha que $\mathcal{F} \subset \mathcal{P}(X)$ seja tal que $|\mathcal{F}| > 2^{n-1}$. Prove que $\mathcal{F}$ não é intersectante. **{*Data de entrega*: 4/4/2018; exercício individual}**

E20 Seja X um conjunto com n elementos. Determine a média das cardinalidades $|A \cap B|$ onde A e B variam sobre todos os subconjuntos de X. Isto é, determine

$$\frac{1}{2^{2n}} \sum_{A \subset X} \sum_{B \subset X} |A \cap B|. \tag{8}$$

[*Sugestão.* Use funções indicadoras.] **{*Data de entrega*: 11/4/2018; exercício individual}**

E21 Uma urna contém bolas azuis e vermelhas. Seja a o número de bolas azuis e b o número de bolas vermelhas na urna. Seja $n = a+b$. Qual é o número médio de bolas azuis nos 2^n subconjuntos de bolas da urna? Isto é, determine

$$\frac{1}{2^n} \sum_{S \subset U} |S \cap A|, \tag{9}$$

onde U é conjunto das bolas na urna e A é o subconjunto das bolas azuis em U.

E22 Uma urna contém um total de $3n$ bolas, das quais n são azuis e $2n$ são vermelhas. Seja k um inteiro com $0 \leq k \leq n$. Qual é o número médio de bolas azuis nos $\binom{3n}{3k}$ subconjuntos de $3k$ bolas da urna? Esta pergunta pode também ser formulada da seguinte forma. Seja U o conjunto das $3n$ bolas na urna. Determine

$$\binom{3n}{3k}^{-1} \sum_{S} |S \cap A|, \tag{10}$$

onde a soma sobre S estende-se sobre todos os $S \subset U$ com $|S| = 3k$ e $A = \{x \in U \colon x \text{ é azul}\}$.

E23 Faça o maior número possível dos itens (i) a (xiii) do Exercício 23.8 de **KH**.

E24 Prove que a equação $x^{2018} - 2x^3 + 24 = 0$ não tem raízes racionais. **{*Data de entrega*: 11/4/2018; exercício individual}**

E25 Dado $x \in \mathbb{R}$, definimos $|x|$, o *módulo de* x, como sendo $-x$ se $x < 0$ e x se $x \geq 0$. Prove que, para todo x e $y \in \mathbb{R}$, temos

$$|x+y| \leq |x| + |y|. \tag{11}$$

E26 Prove que, para todo x e $y \in \mathbb{R}$, temos

$$\big||x| - |y|\big| \leq |x-y|. \tag{12}$$

E27 Faça o maior número possível dos itens (i) a (xvi) do Exercício 24.10 de **KH**.

E28 Seja N um inteiro positivo. O *N-ésimo número Harmônico H_N* é o número

$$\sum_{1\le k\le N} \frac{1}{k} = 1 + \frac{1}{2} + \cdots + \frac{1}{N}. \tag{13}$$

Prove que $H_{2^n} \ge 1 + n/2$ para todo inteiro $n \ge 0$. **{*Data de entrega*: 25/4/2018; exercício individual}**

E29 Neste exercício, consideramos *torneios*: o resultado de campeonatos em que todos os jogadores jogam contra todos os outros jogadores, e tais que não há empates nos jogos. Por exemplo, um torneio com $n = 4$ jogadores poderia ser tal que o jogador i venceu do jogador j se e só se o par ordenado (i, j) pertence ao conjunto

$$\{(3,1),(1,4),(4,2),(2,1),(2,3),(3,4)\}. \tag{14}$$

Note que, no torneio acima, o jogador 3 venceu do jogadores 1 e 4 e perdeu do jogador 2. Você pode achar conveniente desenhar certos diagramas para representar torneios: represente cada jogador por um ponto e se o jogador i venceu do jogador j, desenhe uma flecha de i para j. Desenhe um diagrama para representar o torneio dado acima.

Introduzimos agora uma definição: dizemos que um jogador i em um torneio é um *rei* se, para todo jogador j diferente de i, vale que i venceu de j ou i venceu de um jogador k que venceu de j. Por exemplo, no exemplo acima, o jogador 3 é um rei. Prove que todo torneio não-vazio tem um rei. [*Sugestão.* Tente fazer este exercício seriamente sem ler essa sugestão. Se não sair, leia a sugestão `:-)`. Use indução em n, o número de jogadores no torneio. Suponha que os jogadores são $1, \dots, n$. No passo de indução, aplique a hipótese de indução duas vezes: uma vez no torneio restrito aos jogadores $1, \dots, n-1$ e outra vez em um outro torneio com $n-1$ jogadores.] **{*Data de entrega*: 25/4/2018; exercício individual}**

E30 Sejam $A_1, \dots, A_n \subset X$ conjuntos. Para $x \in X$, seja $\operatorname{occ}(x)$ o número de ocorrências de x nos A_i, isto é,

$$\operatorname{occ}(x) = \sum_{1\le k\le n} I_{A_i}(x), \tag{15}$$

onde I_{A_i} é a função característica de A_i $(1 \le i \le n)$. Prove que

$$A_1 \triangle A_2 \triangle \cdots \triangle A_n = \{x \in X\colon\ \operatorname{occ}(x) \text{ é ímpar}\}. \tag{16}$$

E31 Seja $\pi(x)$ o número de números primos p com $0 < p \le x$. Prove que, para todo inteiro positivo N, temos

$$\pi(N) \ge \frac{1}{2}\log_2 N. \tag{17}$$

[*Sugestão.* Sejam $p_1, \dots, p_r$ os primos menores ou iguais a N. Assim, $r = \pi(N)$. Usando decomposição em números primos, observe que todo inteiro positivo $m \le N$ pode ser escrito na forma n^2q, onde n é um inteiro positivo e q é um produto dos p_i $(1 \le i \le r)$, com cada p_i ocorrendo no máximo uma vez em q. Quantos inteiros positivos $m \le N$ há? Quantos inteiros positivos $m \le x$ podem ser escritos na forma acima?]

E32 Faça o maior número possível dos itens (i) a (iii) do Exercício 25.7 de **KH**.

E33 Sejam $A_1, \dots, A_n \subset [n]$ $(n \in \mathbb{N})$ conjuntos com $|A_i| \ge 3$ para todo i. Prove que há i, j e k com $1 \le i < j < k \le n$ tais que $A_i \cap A_j \cap A_k \ne \emptyset$.

E34 Seja $A(n)$ $(n \geq 2)$ a afirmação

$$\text{para quaisquer } x_1, \dots, x_n \in \mathbb{R} \text{ com } x_i \geq 0 \text{ para todo } i, \text{ vale que}$$
$$\frac{1}{n}(x_1 + \cdots + x_n) \geq (x_1 \dots x_n)^{1/n}.$$

A afirmação $A(n)$ é conhecida como a desigualdade das médias aritmética e geométrica (desigualdade MAMG).

(*i*) Prove $A(2)$.

(*ii*) Seja $n \geq 2$. Prove que se $A(2)$ e $A(n)$ valem, então $A(2n)$ também vale.

(*iii*) Seja $n > 2$. Prove que se $A(n)$ vale, então $A(n-1)$ também vale. [*Sugestão.* Tome $x_n = (x_1 + \cdots + x_{n-1})/(n-1)$.]

(*iv*) Conclua que $A(n)$ vale para todo $n \geq 2$.

{*Data de entrega*: 2/5/2018; exercício individual}

E35 (*i*) Seja

$$X = \left\{ n - \frac{1}{m} : n, m \in \mathbb{N} \text{ com } n \geq 1 \text{ e } m \geq 1 \right\}. \tag{18}$$

Prove que X é bem ordenado, isto é, prove que todo $Y \subset X$ não-vazio tem um elemento mínimo: um elemento $y \in Y$ tal que, para todo $y' \in Y$, vale que $y \leq y'$.

(*ii*) Seja

$$Z = \left\{ n + \frac{1}{m} : n, m \in \mathbb{N} \text{ com } n \geq 1 \text{ e } m \geq 1 \right\}. \tag{19}$$

Prove que Z *não* é bem ordenado, isto é, prove que existe $Y \subset Z$ não-vazio *sem* elemento mínimo.

{*Data de entrega*: 2/5/2018; exercício individual}

E36 Para todo $x \in \mathbb{R}$, definimos $\lfloor x \rfloor$ como sendo o *piso* de x (ou *chão* de x): o maior inteiro que não excede x. Por exemplo, $\lfloor \pi \rfloor = 3$, $\lfloor e \rfloor = 2$, $\lfloor -\pi \rfloor = -4$ e $\lfloor -e \rfloor = -3$. Analogamente, definimos $\lceil x \rceil$ $(x \in \mathbb{R})$ como sendo o *teto* de x: o menor inteiro maior ou igual a x.

(*i*) Desenhe o gráfico da função $f\colon \mathbb{R} \to \mathbb{R}$ dada por $f(x) = \lfloor x \rfloor$ $(x \in \mathbb{R})$.

(*ii*) Prove que $\lceil x \rceil = -\lfloor -x \rfloor$ para todo $x \in \mathbb{R}$.

(*iii*) Prove ou dê contra-exemplo para as seguintes afirmações.

(*a*) Para qualquer $x \in \mathbb{R}$, não existe $k \in \mathbb{Z}$ tal que $\lfloor x \rfloor < k \leq x$.

(*b*) Se x e y são reais tais que $\lfloor x \rfloor < \lfloor y \rfloor$, então existe $k \in \mathbb{Z}$ tal que $x < k \leq y$.

(*c*) Se $n \in \mathbb{N}$, então $n = \lfloor n/2 \rfloor + \lceil n/2 \rceil$.

(*d*) Para todo x real não-negativo, temos $\lfloor \sqrt{\lfloor x \rfloor} \rfloor = \lfloor \sqrt{x} \rfloor$.

(*e*) Para todo x real não-negativo, temos $\lceil \sqrt{\lfloor x \rfloor} \rceil = \lceil \sqrt{x} \rceil$.

(*f*) Para todo $n \in \mathbb{N}$, temos $\lfloor \lfloor \lfloor n/2 \rfloor /2 \rfloor /2 \rfloor = \lfloor n/8 \rfloor$. [*Sugestão.* Considere inicialmente a afirmação $\lfloor \lfloor x \rfloor /2 \rfloor = \lfloor x/2 \rfloor$.]

E37 Este exercício é uma continuação do Exercício **E36**. Prove ou dê contra-exemplo para as seguintes afirmações.

(*i*) Se $n \in \mathbb{N}$ e $\alpha + \beta = 1$, onde α e β são reais não-negativos, então $n = \lfloor \alpha n \rfloor + \lceil \beta n \rceil$.

(*ii*) Para todo x real não-negativo e todo inteiro $k \geq 1$, temos

$$\underbrace{\left\lfloor \sqrt{\left\lfloor \sqrt{\lfloor \dots \lfloor \sqrt{\lfloor x \rfloor} \rfloor \dots \rfloor} \right\rfloor} \right\rfloor}_{k \text{ vezes}} = \left\lfloor \sqrt[2^k]{x} \right\rfloor = \left\lfloor x^{1/2^k} \right\rfloor. \tag{20}$$

(*iii*) Para todo $n \in \mathbb{N}$ e $k \geq 1$ ($k \in \mathbb{N}$), temos

$$\underbrace{\lfloor\lfloor\ldots\lfloor\lfloor n/2\rfloor/2\rfloor\ldots\rfloor/2\rfloor}_{k \text{ vezes}} = \lfloor n/2^k\rfloor. \tag{21}$$

{*Data de entrega*: 9/5/2018; este exercício pode ser feito em grupos de 2}

E38 Para todo inteiro n, sabemos como escrever n na base 2. Seja $s(n)$ a cadeia de bits que representa n na base 2; aqui, por simplicidade, supomos $n \geq 0$. Por exemplo, se $n = 22$, temos $s(n) = 10110$ e se $n = 2018$, então $s(n) = 11111100010$. Seja $\ell(n)$ o *comprimento* de $s(n)$, isto é, o número de bits em $s(n)$. Assim, $\ell(22) = 5$ e $\ell(2018) = 11$.

(*i*) Monte uma tabela com n, $s(n)$ e $\ell(n)$ para $1 \leq n \leq 15$.

(*ii*) Prove por indução que se $n \geq 1$, então $\ell(n) = \lfloor\log_2 n\rfloor + 1$.

E39 Dados inteiros positivos a e n, queremos obter a^n calculando apenas produtos. Naturalmente, é possível obter a^n calculando $a \times \cdots \times a$ ($n-1$ produtos). É possível calcular a^n com um número consideravelmente menor de produtos: de fato, (*) *é possível calcular a^n fazendo, no máximo, $2\log_2 n$ produtos*. Por exemplo, é possível calcular a^{2018} fazendo no máximo $2\log_2 2018 = 2 \times 10.9\cdots = 21.9\ldots$ produtos (o algoritmo óbvio faria 2017 produtos e a afirmação (*) diz que basta fazer 21 produtos ou menos).

(*i*) Prove a afirmação (*) acima. [*Sugestão.* Você pode achar mais conveniente demonstrar a seguinte afirmação por indução: *é possível calcular a^n fazendo no máximo $2(\ell(n)-1)$ produtos*, onde $\ell(n)$ é como definido no Exercício **E38**. *Dica*: note que, por exemplo, $a^5 = (a^2)^2 a$ e $a^{22} = \left(\left((a^2)^2\right)^2 a^2 a\right)^2$.]

(*ii*) A sugestão do item (*i*) acima dá a cota $2(\ell(n)-1)$ para o problema em questão. Prove uma cota que é em geral *melhor*, envolvendo a quantidade $\ell_1(n)$, definido como sendo o número de bits 1 na representação binária de n (por exemplo, $\ell_1(22) = 3$ e $\ell_1(2018) = 7$.) [*Observação.* A motivação aqui são exemplos como a^{1024}: esse número pode ser calculado com 10 produtos, enquanto que a cota sugerida em (*i*) é $2(\ell(n)-1) = 20 > 10$.]

{*Data de entrega*: 9/5/2018; este exercício pode ser feito em grupos de 2}

E40 Os matemáticos egípcios em 1800 A.C. expressavam frações racionais r entre 0 e 1 na forma $1/a_1 + \cdots + 1/a_k$, com os a_i naturais distintos. Por exemplo, uma forma para eles expressarem $2/5$ era $1/3 + 1/15$, e uma forma de eles expressarem $5/8$ era $1/2 + 1/8$.[1]

(*i*) Escreva um programa que recebe como entrada um racional r com $0 < r < 1$ e que tem como saída uma 'representação egípcia' de r. Para escrever seu programa, use o seguinte processo indutivo, devido a Fibonacci (1202 D.C.): suponha $r = m/n$ com m e n naturais não nulos. Seja então $q = \lceil n/m\rceil$ e use

$$\frac{m}{n} = \frac{1}{q} + \left(\text{representação de } \frac{m}{n} - \frac{1}{q}\right). \tag{22}$$

(*ii*) Use seu programa para obter uma representação egípcia de $5/121$.

(*iii*) Prove que seu programa de (*i*) funciona `:-)`. Isto é, prove que ele *termina* (não entra em um loop infinito) e que os denominadores que ele obtém para a representação

[1] Um uso da identidade $5/8 = 1/2 + 1/8$ é o seguinte: suponha que temos 5 pizzas para dividir entre 8 pessoas. Uma forma simples seria dividir cada pizza em 8 pedaços e cada um ficar com 5 pedaços. Uma forma alternativa melhor (?) é dividir 4 pizzas em metades e uma pizza em 8 partes, e cada um ficar com uma metade e um pedaço de tamanho 1/8.

egípcia são todos distintos. [*Sugestão.* Para provar que seu programa termina, prove que os 'valores de m' que ocorrem em seu programa decrescem estritamente. Para provar que os denominadores são todos distintos, prove que os 'valores de q' são estritamente crescentes.]

{*Data de entrega*: 16/5/2018; este exercício pode ser feito em grupos de 2}

E41 Em nossa análise da busca binária em listas ordenadas, ocorreram as árvores binárias B_n definidas a seguir. Para $n = 0$, a árvore B_n é uma árvore vazia (uma árvore com um único nó externo). Suponha agora que $n \geq 1$ e que B_n já esteja definida para valores menores de n. Se n é ímpar, temos que $B_n = (r, B_{\lfloor n/2 \rfloor}, B_{\lfloor n/2 \rfloor})$ (naturalmente, supomos aqui que r é um nó novo, que não ocorre nas subárvores direita e esquerda de B_n e que essas subárvores não têm nós comuns). Se n é par, temos que $B_n = (r, B_{n/2}, B_{n/2-1})$. Desenhe as árvores B_n para $0 \leq n \leq 8$.

E42 Lembre que, dada uma árvore binária T, a *profundidade* $\mathrm{prof}(x)$ de um nó x de T é sua distância à raiz de T. Assim, a raiz de T tem profundidade 0 e se x é filho de p, então $\mathrm{prof}(x) = \mathrm{prof}(p)+1$. Definimos a altura $h(T)$ de uma árvore T como sendo $\max_x \mathrm{prof}(x)$, onde o máximo é tomado sobre todos os nós x de T. Seja $h(n) = h(B_n)$, onde B_n é a árvore definida no Exercício **E41**. Determine $h(n)$ para todo $n \geq 0$. [*Observação.* Por exemplo, $h(0) = 0$, $h(1) = 1$ e $h(2) = h(3) = 2$.]

E43 Lembre que, quando fazemos uma busca binária em uma lista ordenada e essa busca é sem sucesso, chegamos a um nó externo da árvore B_n (veja o Exercício **E41**), onde n é o número de elementos em nossa lista. Fixe uma lista $x_0 \leq \cdots \leq x_{n-1}$ e suponha, por simplicidade, que todos os x_i são distintos. Suponha que fazemos buscas sem sucesso nessa lista. Cada busca sem sucesso b resulta em um certo número de perguntas do tipo "$x \leq y$?" sendo feitas. Seja $p(b)$ o número de tais perguntas feitas para realizar a busca b. Sejam $\alpha(n) = \min p(b)$ e $\beta(n) = \max p(b)$, onde o mínimo e o máximo são tomados sobre todas as buscas sem sucesso b. (Note que $\beta(n)$ é o número de tais perguntas "no pior caso", e $\alpha(n)$ é o número de perguntas "no melhor caso".)

(*i*) Determine $\alpha(n)$.

(*ii*) Determine $\beta(n)$.

(*iii*) É verdade que $\alpha(n) \leq \beta(n) \leq \alpha(n) + 1$? Justifique sua resposta.

{*Data de entrega*: 23/5/2018; exercício individual}

E44 Lembre que, quando fazemos uma busca binária em uma lista ordenada e essa busca é com sucesso, chegamos a um nó interno da árvore B_n (veja o Exercício **E41**), onde n é o número de elementos em nossa lista. Fixe uma lista $x_0 \leq \cdots \leq x_{n-1}$ e suponha, por simplicidade, que todos os x_i são distintos. Suponha que fazemos buscas com sucesso nessa lista. Cada busca com sucesso b resulta em um certo número de perguntas do tipo "$x \leq y$?" sendo feitas. Seja $p(b)$ o número de tais perguntas feitas para realizar a busca b. Note que $p(b) = \mathrm{prof}(x_i) + 1$ quando buscamos x na lista e $x = x_i$. Seja $\gamma(n) = \max p(b)$, onde o máximo é tomado sobre todas as buscas com sucesso b. (Note que $\gamma(n)$ é o número de tais perguntas "no pior caso".)

(*i*) Prove que $\gamma(n) = \lfloor \log_2 n \rfloor + 1$.

(*ii*) O *nível* ℓ de B_n é o conjunto dos nós internos y com $\mathrm{prof}(y) = \ell$. Por exemplo, no nível 0 temos somente a raiz de B_n se $n > 0$ (se $n = 0$, não há nós internos). Prove que o número de elementos no nível ℓ de B_n ($n \geq 1$) é 2^ℓ se $\ell \leq \lfloor \log_2 n \rfloor - 1$.

(*iii*) Seja $N_{1/2}$ o número de elementos x_i da lista $x_0 \le \cdots \le x_{n-1}$ tal que a busca com sucesso de x_i é tal que fazemos
$$\le \frac{1}{2}\gamma(n) \tag{23}$$
perguntas "$x < y$?". Isto é, para esses $N_{1/2}$ elementos x_i, a busca com sucesso faz metade ou menos perguntas "$x < y$?" comparado com o pior caso.

(*a*) Prove que $N_{1/2} < \sqrt{2n}$. Assim, apenas para uma fração pequena dos x_i (que tende para 0 conforme $n \to \infty$) temos que a busca de x_i "custa" $\le \gamma(n)/2$ perguntas.

(*b*) O que ocorre se trocamos 1/2 em (23) por algo como 3/4 ou 99/100? Sejam $N_{3/4}$ e $N_{99/100}$ os números de x_i correspondentes. É ainda verdade que
$$\lim_{n\to\infty} \frac{N_{3/4}}{n} = 0 \tag{24}$$
e
$$\lim_{n\to\infty} \frac{N_{99/100}}{n} = 0? \tag{25}$$
[*Observação.* A conclusão é que, para a vasta maioria das buscas com sucesso, o número de perguntas que se faz não é significativamente diferente de $\log_2 n$.]

E45 As seguintes árvores binárias M_n ($n \ge 0$) ocorrem quando estuda-se o *mergesort* (ordenação por intercalação).[2] Para $n = 0$, temos que $M_n = (z)$ (isto é, M_0 tem um único nó externo). Para $n = 1$, temos que $M_n = (r, (z), (z'))$ (assim, M_1 tem um nó interno e dois nós externos). Para $n \ge 2$, temos que $M_n = (r, M_{\lfloor n/2 \rfloor}, M_{\lceil n/2 \rceil})$.

(*i*) Desenhe M_n para $0 \le n \le 6$.

(*ii*) Quantos nós internos tem M_n? Quantos nós externos tem M_n?

(*iii*) Um nó interno é uma *folha* se ele tem dois nós externos como filhos. Quantas folhas tem M_n?

(*iv*) Seja $h(M_n)$ a altura de M_n.

(*a*) Prove que se $r \le s$, então $h(M_r) \le h(M_s)$.

(*b*) Prove que $h(M_n) = \lceil \log_2 n \rceil + 1$ para todo $n \ge 1$.

E46 Faça o maior número possível dos itens (i) a (xii) do Exercício 27.23 de **KH**.

E47 Sejam a e b números naturais, com $b > 0$. Definimos sequências de naturais $p_1, \dots, p_t$ e $q_1, \dots, q_{t-2}$ para um certo $t \ge 3$ da seguinte forma. Pomos $p_1 = a$ e $p_2 = b$. Seja agora $k \ge 3$ e suponha que já definimos $p_3, \dots, p_{k-1}$ e $q_1, \dots, q_{k-3}$. Se $p_{k-1} = 0$, então tomamos $t = k-1$ e terminamos a definição de nossas sequências $p_1, \dots, p_t$ e $q_1, \dots, q_{t-2}$. Por outro lado, se $p_{k-1} \ne 0$, definimos p_k e q_{k-2} pela divisão de p_{k-2} por p_{k-1}: isto é, tomamos p_k e q_{k-2} como sendo os únicos naturais que satisfazem
$$p_{k-2} = q_{k-2}p_{k-1} + p_k, \qquad 0 \le p_k < p_{k-1}. \tag{26}$$
O procedimento acima define indutivamente a sequência dos p_k e a sequência dos q_k.

[2] Veja `https://introcs.cs.princeton.edu/python/42sort/` e `https://introcs.cs.princeton.edu/python/42sort/merge.py.html`. Para executar `merge.py`, você precisará de `https://introcs.cs.princeton.edu/python/code/stdio.py` e `https://introcs.cs.princeton.edu/python/code/stdarray.py`.

(*i*) Prove que

$$p_1p_2 = \sum_{k=1}^{t-2} q_k p_{k+1}^2. \tag{27}$$

(*ii*) Faça um desenho que ilustra a identidade (27). [*Sugestão.* Considere um retângulo $p_1 \times p_2$.]

{*Data de entrega*: 23/5/2018; exercício individual}

E48 Um prédio tem duas escadarias, uma delas com 780 degraus e outra com 700 degraus. Sabendo que os degraus das duas escadas estão no mesmo nível exatamente quando conduzem a um mesmo andar, descubra quantos andares tem o prédio.

E49 Para todo $n \in \mathbb{N}$, definimos o *n-ésimo número de Fermat* com sendo $F_n = 2^{2^n}+1$. Assim, $F_0 = 3$, $F_1 = 5$, $F_2 = 17$ etc.

(*i*) Prove que, para todo $n \in \mathbb{N}$, temos

$$\prod_{0\le k\le n} F_k = F_{n+1} - 2. \tag{28}$$

(*ii*) Prove que se k e ℓ são dois naturais distintos, então $\mathrm{mdc}(F_k, F_\ell) = 1$.

(*iii*) É verdade que todo os F_n $(n \in \mathbb{N})$ são primos?

(*iv*) Deduza de (*ii*) acima que há infinitos números primos. [*Observação.* Essa é a prova de Goldbach para o fato de que há infinitos números primos.]

{*Data de entrega*: 30/5/2018; exercício individual}

E50 Faça o maior número possível dos itens (i) a (xi) do Exercício 28.19 de **KH**.

E51 Sejam a e b inteiros com $\mathrm{mdc}(a,b) = 1$.

(*i*) Prove que $\mathrm{mdc}(a+b, a-b) \le 2$. [*Sugestão.* Considere os números $2a$ e $2b$.]

(*ii*) Prove que $\mathrm{mdc}(a+b, a^2+b^2) \le 2$. [*Sugestão.* Considere os números $2ab$, $ab-a^2$ e $ab-b^2$.]

{*Data de entrega*: 30/5/2018; exercício individual}

E52 Sejam x e y inteiros. Professor C (de "cento e cinco") resolveu chamar de *divisores brilhantes de x e y* os divisores comuns $b \ge 0$ de x e y que têm a seguinte propriedade: *se c divide ambos x e y, então $c \mid b$.*

(*i*) Prove que para quaisquer x e $y \in \mathbb{Z}$, há no máximo um divisor brilhante para x e y.

(*ii*) Prove que, para quaisquer x e $y \in \mathbb{Z}$, há um divisor brilhante para x e y.

(*iii*) Qual é o nome usual para esses divisores brilhantes?

{*Data de entrega*: 6/6/2018; exercício individual}

E53 Sejam a e b inteiros. Provamos em sala que existem inteiros k e ℓ tais que $ka + \ell b = \mathrm{mdc}(a,b)$. A prova que vimos é indutiva: o caso $b = 0$ é claro e, se $b \ne 0$, então encontramos k' e ℓ' para o par de inteiros b e r, onde $a = bq + r$ e $0 \le r < |b|$ (q e $r \in \mathbb{Z}$), e produzimos k e ℓ a partir de k' e ℓ'. Implemente este algoritmo: escreva um programa que, dados a e b, encontra k, ℓ e $\mathrm{mdc}(a,b)$. [*Observação.* A parte principal de seu programa será uma função recursiva, que implementa o algoritmo dado nessa prova.]

E54 Sejam a e b inteiros. Queremos calcular $\mathrm{mdc}(a,b)$ e também encontrar inteiros α e β tais que $\alpha a + \beta b = \mathrm{mdc}(a,b)$. Considere o procedimento a seguir. Construímos uma sequência de matrizes

$$M^{(0)}, \dots, M^{(t)}, \tag{29}$$

para algum $t \geq 0$, da seguinte forma. Tomamos

$$M^{(0)} = \begin{pmatrix} a & 1 & 0 \\ b & 0 & 1 \end{pmatrix}. \tag{30}$$

Suponha agora que $k \geq 1$ e que $M^{(0)}, \dots, M^{(k-1)}$ já estejam definidos. Sejam m_{ij} as entradas de $M^{(k-1)}$; isto é, suponha que $M^{(k-1)} = (m_{ij})_{0 \leq i < 2,\, 0 \leq j < 3}$. Se $m_{10} = 0$, então tomamos $t = k - 1$ e terminamos a definição da sequência em (29). Caso contrário, suponha $m_{00} = m_{10}q + r$, onde q e r são inteiros e $0 \leq r < |m_{10}|$. Seja

$$N = \begin{pmatrix} 0 & 1 \\ 1 & -q \end{pmatrix}, \tag{31}$$

e faça $M^{(k)} = NM^{(k-1)}$. Isto define $M^{(k)}$ e a sequência em (29) fica definida por indução. Suponha que última matriz $M^{(t)}$ em (29) tenha a forma

$$M^{(t)} = \begin{pmatrix} m & \alpha & \beta \\ m' & \alpha' & \beta' \end{pmatrix}. \tag{32}$$

(*i*) Prove que $m = \mathrm{mdc}(a, b)$.

(*ii*) Prove que $\alpha a + \beta b = \mathrm{mdc}(a, b)$. [*Sugestão.* Suponha que $m_{ij}^{(k)}$ sejam as entradas de $M^{(k)}$ $(1 \leq k \leq t)$; isto é, $M^{(k)} = (m_{ij}^{(k)})_{0 \leq i < 2,\, 0 \leq j < 3}$. Prove que, para todo k, vale que $m_{i0}^{(k)} = m_{i1}^{(k)} a + m_{i2}^{(k)} b$ para ambos $i = 0$ e $i = 1$.]

(*iii*) Implemente este algoritmo. Você obterá assim uma versão *não-recursiva* do algoritmo de Euclides estendido `:-)`.

{*Data de entrega*: 6/6/2018; exercício individual}

E55 Dado um conjunto não-vazio de inteiros A, seja

$$\mathrm{Div}\, A = \{d \in \mathbb{N} : \text{ para todo } a \in A, \text{ vale que } d \mid a\}. \tag{33}$$

Isto é, $\mathrm{Div}\, A$ é o conjunto dos divisores não-negativos comuns dos elementos em A.

(*i*) Sejam $a_1, \dots, a_n$ inteiros $(n \geq 2)$. Prove que

$$\mathrm{Div}\{a_1, \dots, a_n\} = \mathrm{Div}\{a_1, \dots, a_{n-2}, \mathrm{mdc}(a_{n-1}, a_n)\}. \tag{34}$$

(*ii*) Seja A um conjunto não-vazio de inteiros, e suponha que A contenha um elemento não-nulo. Definimos o *máximo divisor comum* $\mathrm{mdc}\, A$ de A como sendo o elemento máximo de $\mathrm{Div}\, A$, isto é, $\mathrm{mdc}\, A = \max \mathrm{Div}\, A$. Se $A = \{0\}$, então pomos $\mathrm{mdc}\, A = 0$. Escreva um programa que, dado um conjunto $A \neq \emptyset$ de inteiros, calcula $\mathrm{mdc}\, A$.

E56 (*i*) Sejam A e B conjuntos não-vazios de inteiros, com $A \subset B$. Prove que $\mathrm{mdc}\, A \geq \mathrm{mdc}\, B$.

(*ii*) Seja $A = \{a_1, a_2, \dots\}$ um conjunto infinito de inteiros. Prove que, para algum $n \geq 1$, vale que $\mathrm{mdc}\, A = \mathrm{mdc}\{a_1, \dots, a_n\}$.

E57 Seja $A \neq \emptyset$ um conjunto de inteiros e seja $d = \mathrm{mdc}\, A$. Prove que d é uma combinação linear inteira de elementos de A. Isto é, prove que existem $a_1, \dots, a_n \in A$ e $\alpha_1, \dots, \alpha_n \in \mathbb{Z}$ tais que

$$d = \sum_{1 \leq i \leq n} \alpha_i a_i. \tag{35}$$

E58 Seja A um conjunto não-vazio de inteiros. Professor C resolveu chamar de *divisores brilhantes* de A os inteiros $b \in \operatorname{Div} A$ com a seguinte propriedade: *se* $c \in \operatorname{Div} A$, *então* $c \mid b$.

(i) Prove que, para todo $A \subset \mathbb{Z}$ com $A \neq \emptyset$, há no máximo um divisor brilhante para A.

(ii) Prove que, para todo $A \subset \mathbb{Z}$ com $A \neq \emptyset$, há um divisor brilhante para A.

(iii) Qual é o nome usual para esses divisores brilhantes?

E59 Faça o maior número possível dos itens (i) a (xiv) do Exercício 29.23 de **KH**.

E60 Faça os itens (ii), (iii) e (iv) do Exercício 31.25 de **KH**.

E61 Seja p um primo com $p \equiv 1 \pmod 4$.

(i) Sejam m e n naturais com $m + n = p - 1$. Prove que $m!n! \equiv (-1)^{n+1} \pmod p$. [*Sugestão.* Observe que $-1 \equiv p - 1 \pmod p$, $-2 \equiv p - 2 \pmod p$, etc e use o teorema de Wilson, que diz que $(p-1)! \equiv -1 \pmod p$ para todo primo p (veremos a prova desse resultado na aula de 11/6/2018).]

(ii) Prove que

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv -1 \pmod p. \tag{36}$$

(iii) Deduza que existe a inteiro com $1 \leq a \leq (p-1)/2$ tal que $a^2 \equiv -1 \pmod p$.

(iv) Considere a equação $x^2 = -1$. Deduza que essa equação tem solução nos inteiros módulo p (isto é, existe $a \in \mathbb{Z}_p$ tal que $a^2 = -1$).

(v) Tome agora $p = 11$, de forma que $p \not\equiv 1 \pmod 4$. Verifique que $x^2 = -1$ não tem solução em $\mathbb{Z}_p = \mathbb{Z}_{11}$.

{*Data de entrega*: 13/6/2018; exercício individual}

E62 Sejam a, b e n inteiros com $n > 0$. Considere a equação

$$ax \equiv b \pmod n. \tag{37}$$

(i) Prove que (37) tem solução em $\mathbb{Z}$ se e só se $\operatorname{mdc}(a, n) \mid b$.

(ii) Seja

$$S = S_{a,b,n} = \{x \in \mathbb{Z}\colon \quad ax \equiv b \pmod b\} \tag{38}$$

o conjunto solução de (37). Suponha que $x_0 \in \mathbb{Z}$ seja uma solução de (37) e seja $d = \operatorname{mdc}(a, n)$. Prove que

$$S = \{x_0 + tn/d\colon t \in \mathbb{Z}\}. \tag{39}$$

E63 Sejam p um primo e a um inteiro com $p \nmid a$. Seja $R \subset \mathbb{Z}$ um sistema completo de resíduos módulo p. Prove que

$$aR = \{ar\colon r \in R\} \tag{40}$$

é também um sistema completo de resíduos módulo p. **{*Data de entrega*: 20/6/2018; exercício individual}**

E64 Sejam p um primo e a um inteiro. Prove que

(i) $a^p + (p-1)!a \equiv 0 \pmod p$.

(ii) $a + (p-1)!a^p \equiv 0 \pmod p$.

E65 Seja $p > 3$ um primo.

(i) Prove que $p!$ e $(p-1)! - 1$ são primos entre si.

(ii) Suponha que $n \equiv (p-1)! - 1 \pmod{p!}$. Prove que os p inteiros que sucedem n são compostos. Prove que os $p - 2$ inteiros que precedem n são compostos.

E66 Seja p um primo ímpar.

(i) Prove que $1^2 3^2 \dots (p-2)^2 \equiv 2^2 4^2 \dots (p-1)^2 \pmod{p}$.

(ii) Prove que se $p \equiv 1 \pmod{4}$, então $2^2 4^2 \dots (p-1)^2 \equiv -1 \pmod{p}$.

(iii) Prove que se $p \equiv 3 \pmod{4}$, então $2^2 4^2 \dots (p-1)^2 \equiv 1 \pmod{p}$.

E67 Seja p um primo com $p \equiv 3 \pmod{4}$. Prove que

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv 1 \pmod{p}. \tag{41}$$

E68 Sejam m e n naturais positivos com $\mathrm{mdc}(m, n) = 1$. Sejam R_m e R_n sistemas completos de resíduos módulo m e n, respectivamente. Prove que

$$R = \{rn + sm \colon r \in R_m \text{ e } s \in R_n\} \tag{42}$$

é um sistema completo de resíduos módulo mn. [*Sugestão.* Suponha $nn' \equiv 1 \pmod{m}$ e $mm' \equiv 1 \pmod{n}$. Dado $a \in \mathbb{Z}$, tome $r = an'$ e $s = am'$. Conclua que há $t \in R$ tal que $t \equiv a \pmod{mn}$. Por que tal t é único? (Note que $|R| \le mn$.)].

E69 Sejam m e n naturais positivos com $\mathrm{mdc}(m, n) = 1$. Sejam R_m^* e R_n^* sistemas reduzidos completos de resíduos módulo m e n, respectivamente. Prove que

$$R^* = \{rn + sm \colon r \in R_m \text{ e } s \in R_n\} \tag{43}$$

é um sistema reduzido completo de resíduos módulo mn.

E70 Sejam m e n naturais positivos com $\mathrm{mdc}(m, n) = 1$. Deduza de **E68** e **E69** que

$$\varphi(mn) = \varphi(m)\varphi(n). \tag{44}$$

E71 Seja $n \ge 2$ um natural. Seja

$$P = P_n = \{[a] \colon \mathrm{mdc}(a, n) = 1\} \subset \mathbb{Z}_n. \tag{45}$$

(i) Prove que se $b \in [a] \in P$, então $\mathrm{mdc}(b, n) = 1$.

(ii) Sejam α e β elementos de P. Prove que $\alpha\beta \in P$.

(iii) Seja α um elemento de P. Prove que $\alpha^{-1} \in P$.

(iv) Seja

$$P' = \{\alpha \in \mathbb{Z}_n \colon \exists \beta \in \mathbb{Z}_n \text{ tal que } \alpha\beta = 1\}. \tag{46}$$

Prove que $P = P'$.

E72 Fixe $n \in \mathbb{N}$ com $n > 0$. Seja R^* um sistema reduzido completo de resíduos módulo n e seja $a \in \mathbb{Z}$ com $\mathrm{mdc}(a, n) = 1$.

(i) Prove que

$$aR^* = \{ar \colon r \in R^*\} \tag{47}$$

é também um sistema reduzido completo de resíduos módulo n.

(ii) Deduza o teorema de Euler de (i). [*Sugestão.* Verifique que $\prod_{r \in R^*} r \equiv \prod_{r \in R^*} ar \pmod{n}$.]

E73 Seja dado um inteiro $k \ge 1$. Consideramos

$$\mathbb{N}^k = \mathbb{N} \times \dots \times \mathbb{N} = \{(x_i)_{1 \le i \le k} \colon x_i \in \mathbb{N} \text{ para todo } i\}, \tag{48}$$

o conjunto das k-uplas ordenadas $(x_i)_{1 \le i \le k} = (x_1, \dots, x_k)$ de naturais. No que segue, quando conveniente, escrevemos $\mathbf{x}, \mathbf{y}, \dots$ para elementos de $\mathbb{N}^k$. Considere a relação L

de $\mathbb{N}^k$ para $\mathbb{N}^k$ (isto é, $L \subset \mathbb{N}^k \times \mathbb{N}^k$) dada por

$$L = \{((x_i)_{1\le i\le k}, (y_i)_{1\le i\le k}) \in \mathbb{N}^k \times \mathbb{N}^k \colon x_i \le y_i \text{ para todo } i\}. \tag{49}$$

Se $(\mathbf{x}, \mathbf{y}) \in L$ (isto é, $\mathbf{x}L\mathbf{y}$), escrevemos $\mathbf{x} \preceq \mathbf{y}$ (essa notação é mais intuitiva, devido à semelhança entre os símbolos $\le$ e $\preceq$). Note que, para $k = 1$, a relação $\preceq$ nada mais é que a relação de ordem $\le$ em $\mathbb{N}$. Seja P_k a seguinte propriedade:

(P_k) Se $\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \ldots$ é uma sequência (infinita) de elementos de $\mathbb{N}^k$, então existem $a < b$ tais que $\mathbf{x}_a \preceq \mathbf{x}_b$.

(*i*) Prove que P_k é válida para $k = 1$. [*Observação.* Você pode achar conveniente provar a seguinte afirmação: se $x_1, x_2, x_3, \ldots$ é uma sequência (infinita) de naturais, então existem $i_1 < i_2 < \ldots$ (com infinitos i_j) tais que $x_{i_1} \le x_{i_2} \le x_{i_3} \le \ldots$.]

(*ii*) Prove que P_k é válida para $k = 2$.

(*iii*) Prove que P_k é válida para qualquer $k \ge 1$.

{*Data de entrega*: 27/6/2018; exercício individual}

E74 Faça o maior número possível dos exercícios do Capítulo 4 (Relações) de **DJV**.

E75 Faça o maior número possível dos itens (i) a (vii) do Exercício 30.28 de **KH**.

E76 Faça o maior número possível dos exercícios do Capítulo 5 (Funções) de **DJV**.

E77 Faça o item (viii) do Exercício 30.28 de **KH**.

E78 Estude o Capítulo 7 de **DJV**. Faça os exercícios daquele capítulo.

E79 Sejam a e b naturais positivos. Prove que existe um natural m que satisfaz as seguintes duas propriedades:

(*i*) $a \mid m$ e $b \mid m$ e

(*ii*) se $a \mid c$ e $b \mid c$, então $m \mid c$.

Prove que existe no máximo um tal natural m. Tal m é, em certos contextos, denotado por $a \vee b$. Por qual nome você conhece $a \vee b$?

E80 Seja dado um inteiro $k \ge 1$. Consideramos

$$\mathbb{N}^k = \mathbb{N} \times \cdots \times \mathbb{N} = \{(x_i)_{1\le i\le k} \colon x_i \in \mathbb{N} \text{ para todo } i\}, \tag{50}$$

o conjunto das k-uplas ordenadas $(x_i)_{1\le i\le k} = (x_1, \ldots, x_k)$ de naturais. Como no exercício **E73**, consideramos a relação L de $\mathbb{N}^k$ para $\mathbb{N}^k$ (isto é, $L \subset \mathbb{N}^k \times \mathbb{N}^k$) dada por

$$L = \{((x_i)_{1\le i\le k}, (y_i)_{1\le i\le k}) \in \mathbb{N}^k \times \mathbb{N}^k \colon x_i \le y_i \text{ para todo } i\}. \tag{51}$$

Como antes, escrevemos $\mathbf{x} \preceq \mathbf{y}$ quando $(\mathbf{x}, \mathbf{y}) \in L$. Sejam $\mathbf{x}$ e $\mathbf{y}$ elementos de $\mathbb{N}^k$. Prove que existe $\mathbf{z} \in \mathbb{N}^k$ tal que

(*i*) $\mathbf{z} \preceq \mathbf{x}$ e $\mathbf{z} \preceq \mathbf{y}$ e

(*ii*) se $\mathbf{w} \in \mathbb{N}^k$ é tal que $\mathbf{w} \preceq \mathbf{x}$ e $\mathbf{w} \preceq \mathbf{y}$, então $\mathbf{w} \preceq \mathbf{z}$.

Ademais, suponha que $\mathbf{z}' \in \mathbb{N}^k$ seja tal que

(*i'*) $\mathbf{z}' \preceq \mathbf{x}$ e $\mathbf{z}' \preceq \mathbf{y}$ e

(*ii'*) se $\mathbf{w} \in \mathbb{N}^k$ é tal que $\mathbf{w} \preceq \mathbf{x}$ e $\mathbf{w} \preceq \mathbf{y}$, então $\mathbf{w} \preceq \mathbf{z}'$.

Prove que $\mathbf{z}' = \mathbf{z}$. Como você pode resolver o exercício S11 (feito em sala) usando este exercício? **{*Data de entrega*: 4/7/2018; exercício individual}**