Números Inteiros e Criptografia, 2020.2

Lista de Exercícios 3[†]

Submeta as soluções das questões marcadas com *
até 30 de abril às 18:00 salvando um arquivo na sua pasta no Google Drive[‡]

Questão 1. Considere o seguinte conjunto de fórmulas

$$X = \{p, q, r, p \vee q, p \to q, \neg p, \neg q\},$$

e sobre este conjunto, considere a relação R dada por

$$\varphi \, R \, \psi \quad \text{sse} \quad \varphi \vee \psi \text{ é uma tautologia}$$

(i.e., é sempre verdadeira, para quaisquer valores de verdade das fórmulas atômicas p, q, r).

a. Represente R graficamente ou em forma de tabela.

* **b.** Prove ou refute: R é reflexiva.

* **c.** Prove ou refute: R é simétrica.

* **d.** Prove ou refute: R é antissimétrica.

* **e.** Prove ou refute: R é transitiva.

f. Prove ou refute: R é uma relação de ordem parcial.

g. Prove ou refute: R é uma relação de equivalência.

Questão 2. Prove que toda relação definida no conjunto vazio é uma relação de ordem parcial e também é uma relação de equivalência.

***Questão 3.** Prove que a seguinte afirmação não é verdadeira: "toda relação definida em um conjunto com exatamente um elemento é uma relação de ordem parcial e também é uma relação de equivalência".

Questão 4. Diremos que dois números inteiros "estão próximos" entre si sse o valor absoluto da diferença entre eles for menor ou igual a 2. Por exemplo, 3 está próximo de 5, 10 está próximo de 9, mas 8 não está próximo de 4. Chamemos de R esta relação.

[†] Publicada em 19/4; alterada em 26/4 (com nova data limite para submissão)

[‡] Link recebido por email em 1/4/2021. A pasta tem um nome similar a `<seu nome> - Cripto 2020.2 - Submissões e Feedback`; em caso de qualquer dúvida entre em contato com o professor.

a. Desenhe uma representação gráfica de R restrita apenas aos números naturais de 0 a 10 (incluindo 0 e 10).

b. Prove ou refute: R é reflexiva.

c. Prove ou refute: R é simétrica.

d. Prove ou refute: R é antissimétrica.

e. Prove ou refute: R é transitiva.

f. Prove ou refute: R é uma relação de ordem parcial.

g. Prove ou refute: R é uma relação de equivalência.

Questão 5. Desenhe o diagrama da relação de divisibilidade dos números de 0 a 19.

***Questão 6.** Seja $\leq_{\text{lex}}$ a relação de *ordem lexicográfica* entre pares de inteiros, cuja definição é: $(a, b) \leq_{\text{lex}} (c, d)$ se e somente se $(a < c)$ ou $(a = c$ e $b \leq d)$. A ordem lexicográfica também é conhecida como *ordem do dicionário*, pois é a forma como comparamos palavras para ordená-las em um dicionário.

Prove que esta é uma relação de ordem parcial no conjunto de pares de números inteiros.

Questão 7. Sejam $a, b, c \in \mathbb{N}$. Prove cada uma das afirmações abaixo:

a. $a \mid a$;

b. $a \mid 0$;

c. Se $a \mid b$ e $b \mid c$, então $a \mid c$;

* **d.** Se $a \mid b$ e $a \mid c$, então para todos $x, y \in \mathbb{Z}$ temos $a \mid (bx + cy)$;

e. Se $a \mid b$ então $a \leq b$;

f. Se $a \mid b$ e $b \mid a$, então $a = b$;

g. Se $c \neq 0$, então: $a \mid b$ sse $ac \mid bc$ (o que acontece no caso $c = 0$?);

h. Se ($a \neq 0$ ou $b \neq 0$) e ($ca \neq 0$ ou $cb \neq 0$), então $\text{mdc}(ca, cb) = c \cdot \text{mdc}(a, b)$.

i. a é divisível por 6 sse a é divisível por 2 e por 3.

j. Se $a \neq 0$ ou ($b \neq 0$ e $b + ac \neq 0$), então $\text{mdc}(a, b) = \text{mdc}(a, b + ac)$.

* **k.** Se $a \neq 0$, então $\text{mdc}(a, ca) = a$.

l. Se $\text{mdc}(a, c) = 1$ e $\text{mdc}(b, c) = 1$ então $\text{mdc}(ab, c) = 1$.

m. Não é verdade que para todos $x, y, z \in \mathbb{N}$ temos:

$$x \mid (y \cdot z) \quad \text{sse} \quad (x \mid y \text{ ou } x \mid z).$$

n. Se $a^2 - 2a + 7$ é par, então a é ímpar.