

Números Inteiros e Criptografia, 2021.2

Lista de Exercícios 2[†]

Submeta as soluções das questões marcadas com * salvando um arquivo na sua pasta no Google Drive[‡]

Data limite para entrega: **21/1 às 18:00**

Em qualquer questão, você pode usar tudo que foi visto em aula (a não ser que a questão proíba isso) ou qualquer outro exercício das listas, desde que seja claro na sua referência do resultado que está usando, e desde que não crie dependências circulares.

Questão 1. Sejam $a, b, c \in \mathbb{Z}$. Prove cada uma das afirmações abaixo:

- a. $a \mid a$;
- b. $|a|$ é o maior divisor de a ;
- c. Se $a \mid b$ e $b \mid c$, então $a \mid c$;
- d. $a \mid b$ sse $(-a) \mid b$ sse $a \mid (-b)$ sse $(-a) \mid (-b)$;
- * e. Se $a \mid b$ e $a \mid c$, então para todos $x, y \in \mathbb{Z}$ temos $a \mid (bx + cy)$;
- f. Se $a \mid b$ então $|a| \leq |b|$;
- g. Se $a \mid b$ e $b \mid a$, então $|a| = |b|$;
- h. Se $c \neq 0$, então: $a \mid b$ sse $ac \mid bc$ (o que acontece no caso $c = 0$?);
- i. $\text{mdc}(ca, cb) = c \cdot \text{mdc}(a, b)$.
- j. a é divisível por 6 sse a é divisível por 2 e por 3.
- * k. $\text{mdc}(a, b) = \text{mdc}(b, a + bc)$.
- l. $\text{mdc}(a, ca) = |a|$;
- m. Se $\text{mdc}(a, c) = 1$ e $\text{mdc}(b, c) = 1$ então $\text{mdc}(ab, c) = 1$.
- * n. Não é verdade que para todos $x, y, z \in \mathbb{Z}$ temos:
$$x \mid (y \cdot z) \quad \text{sse} \quad (x \mid y \text{ ou } x \mid z);$$
- * o. $\text{mdc}(a, b) = \text{mdc}(|a|, |b|)$.

[†]Publicada em 8/12. Atualizada em 15/12, corrigindo *typo* no exemplo da Questão 3.

[‡]Link recebido por email em 8/12/2021. A pasta tem um nome similar a <seu nome> - Cripto 2021.2 - Submissões e Feedback; em caso de qualquer dúvida entre em contato com o professor.

***Questão 2.** Mostre que para quaisquer inteiros a, b, c temos

$$(c \mid a \text{ e } c \mid b) \quad \text{sse} \quad c \mid \text{mdc}(a, b).$$

(*Dica.* Use o Teorema de Bézout!)

Questão 3. Para cada par a, b de números inteiros abaixo, calcule o seu máximo divisor comum:

- a. 14 e 35
- b. 252 e 180
- c. 6643 e 2873
- d. 272828282 e 3242

Questão 4. O Algoritmo Euclidiano funciona tão bem que é difícil encontrar pares de números que o façam demorar muito.

* **a.** Encontre dois números cujo mdc é 4, para os quais o Algoritmo Euclidiano efetua exatamente 4 divisões. (*Dica.* Experimente pensar nas divisões que algoritmo executa, mas em ordem contrária, começando pela última.)

b. Encontre dois números cujo mdc é 4, para os quais o Algoritmo Euclidiano efetua exatamente 5 divisões. (*Dica.* Tente estender a ideia que você usou na letra **a**).

* **c.** Descreva um método para resolver o seguinte problema: dado um natural $k > 0$, encontrar dois números cujo mdc é 4, para os quais o Algoritmo Euclidiano efetua exatamente k divisões. Você deve fornecer alguma explicação de por que seu método funciona, mas não precisa provar terminação e correteza formalmente.

Questão 5. Sejam a e b inteiros com $a \neq 0$ e $b \neq 0$. O *mínimo múltiplo comum* de a e b é o menor número natural que é maior que 0 e múltiplo de ambos a e b . Vamos denotar esse número por $\text{mmc}(a, b)$. Prove as seguintes afirmações.

* **a.** $\text{mmc}(a, b) \cdot \text{mdc}(a, b) = ab$.

(*Dica:* mostre separadamente que $\text{mmc}(a, b) \cdot \text{mdc}(a, b) \geq a \cdot b$ e $\text{mmc}(a, b) \cdot \text{mdc}(a, b) \leq a \cdot b$. Lembre-se: $\text{mdc}(a, b)$ é definido como o *máximo* ..., o que nos dá uma estratégia para concluirmos que $\text{mdc}(a, b)$ é maior ou igual a um dado inteiro; analogamente, $\text{mmc}(a, b)$ é definido como o *mínimo* ..., o que nos dá uma estratégia para concluirmos que $\text{mmc}(a, b)$ é menor ou igual a um dado inteiro. Em uma dessas provas, utilize o item **c** abaixo — você pode usá-lo mesmo se não conseguir prová-lo).

* **b.** $\text{mmc}(a, b) = ab$ sse $\text{mdc}(a, b) = 1$.

* **c.** Para qualquer inteiro m , temos $(a \mid m \text{ e } b \mid m)$ sse $\text{mmc}(a, b) \mid m$. (*Dica:* para a direção “ \Rightarrow ”, imagine a divisão inteira de m por $\text{mmc}(a, b)$. O que de impossível teria que acontecer se o resto dessa divisão não fosse 0?)

Questão 6. Em um futuro distante, o presidente do Brasil é um excêntrico que decide mudar o sistema monetário. Por questões de numerologia, no novo sistema há apenas dois valores de moedas: a moeda de 303 “dinheiro\$” e a de 2310 “dinheiro\$”.

a. Neste futuro distante, Fulano vai à padaria comprar uma coxinha, que custa 12 “dinheiros”. Quantas moedas de cada tipo ele entrega para o caixa da padaria, e quantas de cada tipo recebe de troco, para pagar o valor exato da coxinha? (Há infinitas respostas corretas para esta questão.)

b. Mostre que é impossível Fulano comprar uma casa que custe 1231231231231 “dinheiro\$”, pagando em dinheiro vivo e recebendo troco também em dinheiro vivo, sem que o vendedor saia perdendo (porque Fulano pagou menos que o valor real da casa), nem que o Fulano saia perdendo (pois pagou mais do que o valor real da casa).