Números Inteiros e Criptografia 2022.1†

Lista de Exercícios 1

Entregar as soluções das questões assinaladas com *
até **19/5 no começo da aula**.

A entrega pode ser feita em pessoa ou digitalmente por email para
`hugonobrega@ic.ufrj.br`

Atualizada em 10/5, corrigindo o enunciado da Questão 2.

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. $a \mid b \quad \text{sse} \quad (-a) \mid b \quad \text{sse} \quad a \mid (-b) \quad \text{sse} \quad (-a) \mid (-b) \quad \text{sse} \quad |a| \mid |b|$;

* **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:

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

†Em qualquer solução de exercício, você pode usar tudo o que foi visto em sala ou os enunciados de outros exercícios de qualquer lista, desde que cite claramente o resultado que está usando e desde que você não crie dependências circulares entre os exercícios! Se você citar um exercício da lista atual que não resolveu, ganhará apenas alguma pontuação parcial.

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

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

* **p.** $\text{mdc}(a, b) = \text{mdc}(|a|, |b|)$.

Questão 2. Prove as seguintes generalizações do Teorema da Divisão Euclidiana que vimos em sala.

a.

Teorema. *Sejam $a, b \in \mathbb{Z}$ com $b \neq 0$. Então existem únicos $q, r \in \mathbb{Z}$ tais que*

$$\begin{cases} a = b \cdot q + r \\ 0 \leq r < |b| \end{cases}$$

* **b.**

Teorema. *Sejam $a, b, c \in \mathbb{Z}$ com $b \neq 0$. Então existem únicos $q, r \in \mathbb{Z}$ tais que*

$$\begin{cases} a = b \cdot q + r \\ c \leq r < c + |b| \end{cases}$$

Questão 3. Para cada par a, b de números inteiros abaixo, faça (manualmente) o teste de mesa do Algoritmo de Euclides com entradas a e b

a. 14 e 35

b. 252 e 180

c. 6643 e 2873

* **d.** 272828282 e 3242

***Questão 4.** Sejam $n > m$ inteiros positivos. Mostre que se o resto da divisão de n por m é r então o resto da divisão de $2^n - 1$ por $2^m - 1$ é $2^r - 1$.

Questão 5. O Algoritmo Euclidiano funciona tão bem que é razoavelmente difícil encontrar pares de números que o façam demorar muito.

* **a.** Encontre dois números cujo mdc é 5, 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 5, 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 5, 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 corretude formalmente.