Números Inteiros & Criptografia 2022.2[†]

Lista de Exercícios 1[‡]

Entregar as soluções das questões assinaladas com *
até **18 de outubro às 21:00**.

A entrega é feita digitalmente pelo Google Drive, na pasta que você recebeu (ou receberá) por email.

Você pode escrever suas soluções manualmente e escanear as folhas de resposta, ou escrever as respostas usando algum editor de texto. Atenção! Você deve garantir que as soluções estejam bem legíveis!

Questão 1. Enuncie e prove os Teoremas de Terminação e Corretude para o Algoritmo Ingênuo do MDC que vimos em sala. Como fizemos em sala, você **pode** assumir que as entradas são números naturais diferentes de 0.

Questão 2. Escreva os testes de mesa do Algoritmo de Euclides para as seguintes entradas.

a. $a = 60$, $b = 75$

*** b.** $a = 21$, $b = 13$

c. $a = 123456789$, $b = 123456788$

*** d.** $a \in \mathbb{N}$ qualquer, $b = a + 1$

***Questão 3.** Em sala, provamos o seguinte teorema:

Teorema (Teorema da Divisão Euclideana para naturais)**.** *Para todos naturais a, b com $b \neq 0$, existem únicos naturais q, r satisfazendo ambas as propriedades*

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

Fizemos a prova em duas partes: "existem" com um algoritmo (que chamamos de Algoritmo Ingênuo da Divisão), e "únicos" com uma prova direta.

Vamos agora estender esse teorema. Prove o seguinte resultado:

[†]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.

[‡]Publicada em 3/10, atualizada em 18/10 (novo horário para entrega)

Teorema (Teorema da Divisão Euclideana para inteiros)**.** *Para todos* ***inteiros*** *a, b com $b \neq 0$,* <u>*existem*</u> <u>*únicos*</u> ***inteiros*** *q, r satisfazendo ambas as propriedades*

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

Dica: tente adaptar a prova anterior. No algoritmo ingênuo da divisão que vimos em sala, o "teste" para decidir se precisávamos continuar ou não era ver se o chute de Resto era maior ou igual a b ou não; como deve ficar o novo teste? E, caso precisemos continuar, como deve ser feita a atualização das variáveis? Lembre-se de que, se você escrever um algoritmo, deve provar sua terminação e corretude.

Questão 4. Sejam $a, b, c \in \mathbb{Z}$. Prove cada uma das afirmações abaixo:

a. Se $a \neq 0$, então $|a|$ é o maior divisor de a;

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

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

d. Se $a \mid b$ então $|a| \leq |b|$;

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

f. Se $c \neq 0$, então: ($a \mid b$ sse $ac \mid bc$);

g. $\text{mdc}(ca, cb) = c \cdot \text{mdc}(a, b)$.

* **h.** $\text{mdc}(a, b) = \text{mdc}(b, a + bc)$.

i. $\text{mdc}(a, ca) = |a|$;

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

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

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

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

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

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

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

a. Encontre dois números cujo mdc é 3, 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 3, 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 3, 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.