Números Inteiros e Criptografia 2026-2

Hugo Nobrega

Lista de Exercícios 1

Entregue todas as questões marcadas com * até
23 de setembro às 18:00

A entrega é pelo Google Drive, na pasta que você receberá no e-mail que usou para preencher o formulário no início do período. As listas podem ser entregues por grupos de até 4 alunos. Apenas 1 aluno do grupo deve submeter as respostas. Os nomes e DREs dos componentes do grupo devem estar indicados claramente.

Questão 1. Prove a seguinte generalização do Teorema da Divisão Euclidiana: *Dica*: tente adaptar as provas que fizemos em aula.

Teorema 1. *Sejam a, b, ℓ inteiros com $b \neq 0$. Existem únicos inteiros q, r tais que*

$$\begin{cases} a = bq + r \\ e \\ \ell \leqslant r < \ell + |b| \end{cases}$$

Questão 2. Prove ou refute cada afirmação abaixo.

a. Para todo natural x existe um único natural y tal que $x = y + y$.

b. Para todo natural x existe um único natural y tal que $y = x + x$.

c. Para todo real x existe um único real y tal que $x = y \cdot y$.

d. Para todo real x existe um único real y tal que $y = x \cdot x$.

e. Para todo real $x \geqslant 0$ existe um único real y tal que $x = y \cdot y$.

f. Para todo real $x \geqslant 0$ existe um único real $y \geqslant 0$ tal que $x = y \cdot y$.

*** g.** Para todo natural x existe no máximo um natural y tal que $x = y \cdot y$.

h. Para todo natural x existe pelo menos um natural y tal que $x = y \cdot y$.

Questão 3. Enuncie e prove os Teoremas de Terminação e Corretude para o Algoritmo Ingênuo do MDC que vimos em sala.

Questão 4. Escreva os testes de mesa do Algoritmo de Euclides para as seguintes entradas.

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

b. $a = 34$, $b = 21$

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

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

Questão 5. 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 $|a| \leqslant |b|$;

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

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

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

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

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

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

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

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

n. Para todos $x, y, z \in \mathbb{Z}$ temos:

$$(x \mid y \quad \text{e} \quad x \mid z) \qquad \text{sse} \qquad x \mid \text{mdc}(y, z)$$

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

Questão 6. O Algoritmo de Euclides 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 13, para os quais o Algoritmo de Euclides 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 13, para os quais o Algoritmo de Euclides 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 13, para os quais o Algoritmo de Euclides efetua exatamente k divisões. Você deve fornecer alguma explicação de por que seu método funciona, mas não precisa provar terminação e corretude formalmente.

Questão 7. Sejam $a > b$ inteiros positivos. Mostre que se o resto da divisão de a por b é r então o resto da divisão de $2^a - 1$ por $2^b - 1$ é $2^r - 1$. Você pode usar o seguinte fato, sem prová-lo: em uma progressão geométrica onde o termo inicial t_0, a razão x e a quantidade ℓ de termos são números naturais, a *soma* da progressão é o seguinte número, também garantidamente natural:

$$S = \frac{t_0 \cdot (x^\ell - 1)}{x - 1}.$$

Dica: provar que o resto da divisão $2^a - 1$ por $2^b - 1$ é $2^r - 1$ significa provar que existe um *quociente* natural que, junto com o resto proposto, satisfaz certas propriedades em relação ao dividendo e ao divisor.

Questão 8. Em um futuro distante, o presidente do Brasil é um excêntrico que decide mudar o sistema monetário. A nova moeda se chama "dinheiro$", e por questões de numerologia, no novo sistema há apenas dois valores para as moedas: a de 777 dinheiro$ e a de 2093 dinheiro$. Apenas o pagamento em dinheiro "vivo" (com possível troco) é permitido (ou seja, não há cartão, "pix" nem nada similar).

a. Neste futuro distante, Fulano vai à padaria comprar uma coxinha que custa 35 dinheiro$. Descreva uma transação possível para que o Fulano consiga comprar sua coxinha, i.e., encontre números **naturais** x, y, z, w tais que se Fulano pagar com x moedas de 777 dinheiro$ e y moedas de 2093 dinheiro$, e receber de troco z moedas de 777 dinheiro$ e w moedas de 2093 dinheiro$, o saldo final da transação é que Fulano pagou 35 dinheiro$.

*** b.** Mostre que é impossível Fulano comprar um produto que custe exatamente 123456 dinheiro$, mesmo que Fulano e o vendedor tenham acesso a qualquer quantidade de moedas de dinheiro$ que quiserem.