Números Inteiros e Criptografia 2023.1

Hugo Nobrega

Lista de Exercícios 2

Entregue todas as questões marcadas com * até
22 de maio às 20:00
Em todas as questões, você sempre pode usar tudo que foi feito em sala ou que apareceu em listas de exercícios anteriores (mesmo questões que você não tenha resolvido), mas deve citar claramente o que está usando.

Questão 1. Enuncie e prove os Teoremas de Terminação e Corretude para o Algoritmo Ingênuo do MDC que vimos em sala.

Questão 2. 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 3. 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 $a \mid b$ e $b \neq 0$, 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. $\mathrm{mdc}(a, ca) = |a|$;

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

*** 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:

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

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

Questão 4. 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 7, 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 7, 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 7, 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.

Questão 5. 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 $2^r - 1$. Você pode usar o seguinte fato, sem prová-lo: em uma progressão geométrica onde o termo inicial a_0, a razão x e a quantidade k de termos são números naturais, a *soma* da progressão é o seguinte número, também garantidamente natural:

$$S = \frac{a_0 \cdot (x^k - 1)}{x - 1}.$$

Dica: provar que o resto da divisão $2^n - 1$ por $2^m - 1$ 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 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 777 "dinheiro$" e a de 2023 "dinheiro$". 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$". Mostre que Fulano consegue comprar sua coxinha, assumindo que Fulano e a padaria tenham acesso a todas as moedas de que precisarem.

*** 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.