Números Inteiros e Criptografia, 2020.1

Lista de Exercícios 4

Submeta as soluções das questões marcadas com *****
até 15 de janeiro às 18:00 salvando um arquivo na sua pasta no Google Drive[†]

Atualizada em 11 de janeiro, 22:00

Justifique todas as questões.

Questão 1. Para cada par a, b de números naturais abaixo, calcule o seu máximo divisor comum.

a. 14 e 35

*** b.** 252 e 180

*** c.** 6643 e 2873

d. 272828282 e 3242

Questão 2. O mínimo múltiplo comum de a e b é o menor inteiro positivo que é múltiplo de a e que é múltiplo de b. Vamos denotar esse número por $\text{mmc}(a, b)$. Prove as seguintes afirmações.

*** a.** Se $a \neq 0$ ou $b \neq 0$, então $\text{mmc}(a, b) \cdot \text{mdc}(a, b) = ab$.

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 natural m, temos ($a \mid m$ e $b \mid m$) sse $\text{mmc}(a, b) \mid m$. (Dica: para a direção "⇒", 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 3. O Algoritmo Euclidiano funciona tão bem que é difícil encontrar pares de números que o fazem demorar muito.

[†]Link recebido por email em 4/12/2020. A pasta tem um nome similar a `<seu nome> - Cripto 2020.1 - Submissões e Feedback`; em caso de qualquer dúvida entre em contato com o professor.

*** a.** Encontre dois números cujo mdc é 1, para os quais o Algoritmo Euclidiano efetua exatamente 5 divisões.

*** b.** Encontre dois números cujo mdc é 1, para os quais o Algoritmo Euclidiano efetua exatamente 6 divisões (dica: estenda a ideia que você usou na letra **a**).

*** c.** Descreva um método para resolver o seguinte problema: dado um natural k, encontrar dois números cujo mdc é 1, para os quais o Algoritmo Euclidiano efetua exatamente k divisões.

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 $2^r - 1$. (*Dica*: a soma de uma progressão geométrica finita onde todos os termos são números naturais é um número natural!)

Questão 5. Sejam $a, b, c \in \mathbb{N}$. Prove cada uma das afirmações abaixo:

a. $a \mid a$;

b. $a \mid 0$;

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

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

e. Se $a \mid b$ então $a \leq b$;

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

*** g.** Se $c \neq 0$, então: $a \mid b$ sse $ac \mid bc$ (o que acontece no caso $c = 0$?);

h. Se ($a \neq 0$ ou $b \neq 0$) e ($ca \neq 0$ ou $cb \neq 0$), então $\text{mdc}(ca, cb) = c \cdot \text{mdc}(a, b)$.

i. a é divisível por 6 sse a é divisível por 2 e por 3.

j. Se $a \neq 0$ ou ($b \neq 0$ e $b + ac \neq 0$), então $\text{mdc}(a, b) = \text{mdc}(a, b + ac)$.

*** k.** Se $a \neq 0$, então $\text{mdc}(a, ca) = a$.

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

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

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

*** n.** Se $a^2 - 2a + 7$ é par, então a é ímpar.

o. $\text{mdc}(n, 2n + 1) = 1$

p. $\text{mdc}(2n + 1, 3n + 1) = 1$

*** q.** $\text{mdc}(n! + 1, (n + 1)! + 1) = 1$

Questão 6. Em Brasilândia, o jogo de basquete é jogado com regras diferentes. Existem apenas dois tipos de pontuações para as cestas: 5 e 11 pontos. É possível uma pontuação entre dois times de 86×39?