Números Inteiros e Criptografia, PLE 2020

Lista de Exercícios 4

Submeta as soluções das questões marcadas com *****
até 25 de setembro às 18:00 salvando um arquivo na sua pasta no Google Drive[†]

Justifique todas as questões.

Questão 1.

*** a.** Ache um múltiplo de 330 e um múltiplo de 240 cuja soma seja 210.

*** b.** Mostre que existem infinitas soluções para o item anterior.

***Questão 2.** 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?

***Questão 3.** Sejam a natural e p primo. Fazendo uma análise (completa) de casos, determine todos os possíveis valores de $\text{mdc}(a, p^2)$ (em função de a e/ou de p).

Questão 4. Mostre que se n é composto, então o número $R(n)$, definido por

$$R(n) = \frac{10^n - 1}{9},$$

também é composto. Dica: se k é fator de n então $R(k)$ é fator de $R(n)$.

***Questão 5.** Seja $n > 0$ um número inteiro positivo composto e p seu menor fator primo. Sabe-se que $p \geq \sqrt{n}$ e que $p - 4$ divide $\text{mdc}(6n + 7, 3n + 2)$. Determine **todos** os possíveis valores de n.

***Questão 6.** Mostre que existe um inteiro múltiplo de 241^2 que termina em 241 (Dica: Observe que um número termina em 241 se ele é da forma $1000n + 241$, com n natural).

Questão 7. O Algoritmo Euclidiano funciona tão bem que é difícil encontrar pares de números que o fazem demorar muito.

*** a.** Encontre dois números cujo mdc é 1, para os quais o Algoritmo Euclidiano demora 5 passos (vamos contar cada divisão efetuada como sendo 1 passo).

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

[†]Link recebido por email em 1/9/2020 ou 17/9/2020. A pasta tem um nome similar a `Cripto - Submissões e Feedback - <seu nome>`; em caso de qualquer dúvida entre em contato com os professores.

*** 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 demora k passos.

Questão 8. ("Log de primos") Seja $\exp_p(n)$ o natural m tal que p^m divide n e p^{m+1} não divide n. Prove que $k \leq \exp_p(n) \iff p^k \mid n$.

Questão 9. Sejam a, b, c e d números naturais. Prove ou refute com um contra-exemplo.

*** a.** Se $c = \text{mdc}(a, b)$ e $x = ab$, então $c^2 \mid x$.

*** b.** ($a \mid b$ ou $a \mid c$) sse $a \mid bc$

c. Suponha que $b > 0$ e a é múltiplo de b^2. Então existem inteiros x e y tais que $\text{mdc}(x, y) = b$ e $xy = a$.

Questão 10. 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.** $\text{mmc}(a, b) \cdot \text{mdc}(a, b) = ab$.

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 "$\Rightarrow$", imagine a divisão euclidiana de m por $\text{mmc}(a, b)$. O que de impossível teria que acontecer se o resto dessa divisão não fosse 0?)