Números Inteiros e Criptografia, PLE 2020

Lista de Exercícios 3

Submeta as soluções das questões marcadas com *
até 18 de setembro às 18:00 salvando um arquivo na sua pasta no Google Drive (link recebido por email em 1º de setembro)†

Justifique todas as questões.

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

a. 14 e 35

b. 252 e 180

Questão 2. Sendo n um número natural maior que 1, verifique as seguintes igualdades:

a. $\operatorname{mdc}(n, 2n+1) = 1$

b. $\operatorname{mdc}(2n+1, 3n+1) = 1$

c. $\operatorname{mdc}(n!+1, (n+1)!+1) = 1$

***Questão 3.** 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 4. Sejam $n > m$ inteiros positivos. O objetivo desta questão é calcular $\operatorname{mdc}(2^{2^n} + 1, 2^{2^m} + 1)$.

*** a.** Usando que $2^{2^{m+1}} - 1 = (2^{2^m} + 1)(2^{2^m} - 1)$, mostre que $2^{2^n} - 1$ é múltiplo de $2^{2^m} + 1$ quando $n > m$. Qual é o quociente desta divisão?

b. Usando o item anterior, mostre que o resto da divisão de $2^{2^n} + 1$ por $2^{2^m} + 1$ é 2.

c. Usando o item anterior, determine o $\operatorname{mdc}(2^{2^n} + 1, 2^{2^m} + 1)$.

Questão 5. Sejam $m \neq n$ dois números naturais. Usando a questão anterior, determine $\operatorname{mdc}(a^{2^m} + 1, a^{2^n} + 1)$, se a é ímpar.

***Questão 6.** Encontre todos os inteiros positivos n tais que $2n^2 + 1 \mid n^3 + 9n - 17$.

†A pasta tem um nome similar a `Cripto - Submissões e Feedback - <seu nome aqui>`; em caso de qualquer dúvida entre em contato com os professores.

Questão 8. Verdadeiro ou falso? Apresente uma prova se a afirmação for verdadeira ou um contra-exemplo se ela for falsa.

* **a.** O produto de dois números que deixam resto 7 quando divididos por 8 também deixa resto 7 quando dividido por 8.

b. A soma de um número irracional com uma fração, onde o numerador e denominador são números inteiros, é sempre irracional.

Questão 9. Determine $\mathrm{mdc}(a, c)$ sabendo-se que a, b e c são inteiros maiores que 2, que c divide $a + b$ e que $\mathrm{mdc}(a, b) = 1$.

Questão 10. Determine o $\mathrm{mdc}(53n + 22, 12n + 5)$ para qualquer n inteiro positivo.

Questão 11. Verdadeiro ou falso? Apresente uma prova se a afirmação for verdadeira ou um contra-exemplo se ela for falsa.

* **a.** Sejam a, x e y inteiros. Se a divide $2x - 3y$ e a divide $4x - 5y$, então a divide y.

* **b.** Sejam a, b e c inteiros. Se b divide o produto ac, então b divide c.

* **c.** Seja a um número inteiro. Se $a^2 - 2a + 7$ é par, então a é ímpar.

Questão 12. Determine $\mathrm{mdc}(12n^2 + 23n + 3, 4n + 7)$ para $n > 2^{100!}$.

Questão 13. Sejam $a, b, c \in \mathbb{N}$. Prove ou refute:

a. Se $a \neq 0$, então $a \mid a$;

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 $a \mid b$ e $b \mid a$, então $a = b$;

* **f.** Se $a \mid b$ então $a \leq b$;

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

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

Questão 14. c é divisível por 6 sse c é divisível por 2 e por 3.

Questão 15. Se $\mathrm{mdc}(a, c) = 1$ e $\mathrm{mdc}(b, c) = 1$ então $\mathrm{mdc}(ab, c) = 1$.

Questão 16. Prove que para $a, b, c \in \mathbb{N}$, o mdc satisfaz as seguintes propriedades:

a. $\mathrm{mdc}(a, b) = \mathrm{mdc}(a, b + ac)$.

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

Questão 17. Para quaisquer a e b, prove que se existem n, m tais que $an - bm = 1$ então $\mathrm{mdc}(a, b) = 1$.

Questão 18. Para quaisquer a e b, prove que se existem $x, y \in \mathbb{N}$ que satisfazem $ax + by = \mathrm{mdc}(a, b)$, então $\mathrm{mdc}(x, y) = 1$.