Números Inteiros e Criptografia 2022.1†

Lista de Exercícios 2

Entregar as soluções das questões assinaladas com *
até **2/6 no começo da aula**.

A entrega pode ser feita em pessoa ou digitalmente por email para
`hugonobrega@ic.ufrj.br`

Lista atualizada em 25/5, alterando o enunciado da Questão 2(b)

Questão 1. Mostre que para quaisquer inteiros a, b, c temos

$$(c \mid a \quad \text{e} \quad c \mid b) \qquad \text{sse} \qquad c \mid \text{mdc}(a, b).$$

(*Dica.* Use o Teorema de Bézout!)

Questão 2. 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 2022 "dinheiro$" e a de 2310 "dinheiro$". 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 (que tem todo o dinheiro do mundo) vai à padaria comprar uma coxinha que custa 12 "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 uma casa que custe <u>exatamente</u> 32132132132132 "dinheiro$", mesmo que Fulano e o vendedor tenham acesso a qualquer quantidade de moedas de "dinheiro$" que quiserem.

Questão 3. Determine se existem naturais $x, y, z > 0$ que satisfaçam a equação $3^x \cdot 5^4 \cdot 39^y = 195^z$.

Questão 4.

a. Seja $k \geq 2$ um natural. Mostre que todos os números $k!+2, k!+3, \ldots, k!+k$ são compostos.

b. Refute a seguinte conjectura sobre a "densidade" dos primos:

"existe um natural m tal que, dentre quaisquer m naturais consecutivos,
sempre há pelo menos um primo".

†Em qualquer solução de exercício, você pode usar tudo o que foi visto em sala ou os enunciados de outros exercícios de qualquer lista, desde que cite claramente o resultado que está usando e desde que você não crie dependências circulares entre os exercícios! Se você citar um exercício da lista atual que não resolveu, ganhará apenas alguma pontuação parcial.

***Questão 5.** Sejam b_1 e b_2 naturais primos entre si. Mostre que para qualquer $d \in \mathbb{N}$, temos: d é um divisor de $b_1 b_2$ sse $d = \mathrm{mdc}(d, b_1) \cdot \mathrm{mdc}(d, b_2)$.

***Questão 6.** Considere as seguintes funções definidas para naturais positivos:

- $\omega(n)$ = número de fatores primos de n *distintos*.
- $\Omega(n)$ = número de fatores primos de n *contando todas as repetições!*
- $d(n)$ = quantidade de divisores naturais de n.
- $S(n)$ = soma dos divisores naturais de n.
- $X(n) = n^{1234}$
- $Y(n) = 1234 \cdot n$

(A letra ω se chama "ômega minúsculo" e a letra Ω se chama "ômega maiúsculo".)

Exemplos de valores das funções ω, Ω, d, S estão dados na tabela abaixo:

n	fatoração em primos	$\omega(n)$	$\Omega(n)$	divisores naturais	$d(n)$	$S(n)$
1	—	0	0	1	1	1
2	2	1	1	1, 2	2	3
3	3	1	1	1, 3	2	4
4	2^2	1	2	1, 2, 4	3	7
8	2^3	1	3	1, 2, 4, 8	4	15
15	$3 \cdot 5$	2	2	1, 3, 5, 15	4	24
120	$2^3 \cdot 3 \cdot 5$	3	5	1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 20, 24, 30, 40, 60, 120	16	360

Dizemos que uma função $f : \mathbb{N} \to \mathbb{N}$ é:

- *aditiva* se, para todos $n, m \in \mathbb{N} \setminus \{0\}$:
$$\text{se } \mathrm{mdc}(n, m) = 1 \text{ então } f(n \cdot m) = f(n) + f(m).$$
- *completamente aditiva* se, para todos $n, m \in \mathbb{N} \setminus \{0\}$:
$$f(n \cdot m) = f(n) + f(m).$$
- *multiplicativa* se, para todos $n, m \in \mathbb{N} \setminus \{0\}$:
$$\text{se } \mathrm{mdc}(n, m) = 1 \text{ então } f(n \cdot m) = f(n) \cdot f(m).$$
- *completamente multiplicativa* se, para todos $n, m \in \mathbb{N} \setminus \{0\}$:
$$f(n \cdot m) = f(n) \cdot f(m).$$

Para cada uma das funções ω, Ω, d, S, X e Y definidas acima, e para cada uma das propriedades *aditiva*, *completamente aditiva*, *multiplicativa* e *completamente multiplicativa*, diga se a função tem a propriedade ou não, provando cada caso positivo e dando um contra-exemplo para cada caso negativo. (*Dica:* poupe um bocado do seu trabalho: argumente que uma função ser *completamente aditiva* já implica que ela seja *aditiva* [também use a contrapositiva dessa implicação!], e analogamente para *completamente multiplicativa* e *multiplicativa*. Em um dos itens, pode ser útil usar a Questão 5 acima.)