Números Inteiros e Criptografia, PLE 2020

Lista de Exercícios 6

Submeta as soluções das questões marcadas com *****
até 9 de outubro às 18:00 salvando um arquivo na sua pasta no Google Drive[†]

Justifique todas as questões.

***Questão 1.** Considere as seguintes funções definidas para n natural:

- $\omega(n)$ = número de fatores primos de n *distintos*.
- $\Omega(n)$ = número de fatores primos de n *contando todas as repetições!*
- $d(n)$ = número de divisores positivos de n
- $S(n)$ = soma dos divisores positivos de n
- $h(n) = n^{123456789}$
- $j(n) = 123456789 \cdot n$

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

n	fatoração em primos	$\omega(n)$	$\Omega(n)$	divisores	$d(n)$	$S(n)$
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 $n, m \in \mathbb{N} \setminus \{0\}$:

$$\text{se } \operatorname{mdc}(n, m) = 1 \text{ então } f(n \cdot m) = f(n) + f(m).$$

- *completamente aditiva* se, para todos $n, m \in \mathbb{N} \setminus \{0\}$:

$$f(n \cdot m) = f(n) + f(m).$$

[†]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.

- *multiplicativa* se, para todos $n, m \in \mathbb{N} \setminus \{0\}$:

$$\text{se } \operatorname{mdc}(n, m) = 1 \text{ então } f(n \cdot m) = f(n) \cdot f(m).$$

- *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, h e j 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 pouco do seu trabalho notando que uma função ser *completamente aditiva* já implica que ela seja *aditiva* [qual a contrapositiva dessa implicação?], e analogamente para *completamente multiplicativa* e *multiplicativa*.)

Questão 2 (Infinitude dos primos)**.** Em sala, definimos a função *primorial* que, para um dado primo p, é definida por

$$\begin{aligned} p^{\#} &= 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdots p \\ &= \text{o produto de todos os primos menores ou iguais a } p. \end{aligned}$$

Também em sala, provamos que todos os fatores primos de $p^{\#} + 1$ são estritamente maiores do que p.

Agora vamos estender a função primorial para *todos* os naturais, fazendo:

$$\begin{cases} n^{\#} = 1, & \text{se } n < 2 \\ n^{\#} = \text{o produto de todos os primos de 2 até } n, & \text{se } n \geq 2 \end{cases}$$

*** a.** Prove que, para todos naturais n e p, se p é primo e $p \leq n$, então p não divide $n^{\#} + 1$.

*** b.** Use o item anterior para provar a *infinitude dos primos* na seguinte forma:

$$\text{para todo natural } n, \text{ existe um primo } p > n.$$

Questão 3. Considere as oito funções abaixo. Em cada uma, as entradas e

saídas são sempre número naturais.

$$\begin{cases} f_1(n,0) = n \\ f_1(n,m) = f_1(n,m-1) + 1, & \text{se } m > 0 \end{cases}$$

$$\begin{cases} f_2(n,0) = 0 \\ f_2(n,m) = f_2(n,m-1) + n, & \text{se } m > 0 \end{cases}$$

$$\begin{cases} f_3(0,m) = 0 \\ f_3(n,m) = f_3(n-1,m) + 1, & \text{se } n > 0 \end{cases}$$

$$\begin{cases} f_4(n,0) = 1 \\ f_4(n,m) = f_4(n,m-1) \cdot n, & \text{se } m > 0 \end{cases}$$

$$\begin{cases} f_5(n,m) = 0, & \text{se } m \leq 1 \\ f_5(n,m) = 1, & \text{se } m > 1 \ \& \ m \text{ divide } n \ \& \ \forall k \in \mathbb{N}(k < m \to f_5(n,k) = 0) \\ f_5(n,m) = 0, & \text{nos outros casos} \end{cases}$$

$$\begin{cases} f_6(n,m) = 0 & \text{se } m < n \\ f_6(n,m) = f_6(n,m-n) + 1, & \text{nos outros casos} \end{cases}$$

$$\begin{cases} f_7(n,m) = 0, & \text{se 7 não divide } n \text{ ou 7 não divide } m \\ f_7(n,m) = f_7(n/7, m/7) + 1, & \text{nos outros casos} \end{cases}$$

$$\begin{cases} f_8(n,0) = 1 \\ f_8(n,m) = n^{f_8(n,m-1)}, & \text{se } m > 0 \end{cases}$$

a. Determine os valores abaixo, exibindo as contas ao longo do caminho até determinar a resposta:

(i) $f_1(5,4)$

(ii) $f_2(5,4)$

(iii) $f_3(5,24)$

(iv) $f_4(4,4)$

(v) $f_5(35,5)$

(vi) $f_5(35,7)$

(vii) $f_6(4,30)$

(viii) $f_7(28,70)$

(ix) $f_8(2,4)$

*** b.** Para cada uma das sete funções g_i abaixo, definidas sem uso de recursão, encontre alguma das funções f_j acima tal que $g_i = f_j$. (Novamente, as entradas e saídas das funções g_i são sempre números naturais.) Você não precisa provar formalmente que $g_i = f_j$, mas deve dar um argumento informal e intuitivo para justificar por que $g_i = f_j$ é verdade.

$g_1(n, m) =$ o expoente de 7 na fatoração por primos de $\text{mdc}(n, m)$

$g_2(n, m) = n$

$g_3(n, m) = n * m$

$$g_4(n, m) = \begin{cases} 1, & \text{se } m \text{ é o menor número maior do que 1 que divide } n \\ 0, & \text{caso contrário} \end{cases}$$

$g_5(n, m) =$ o quociente da divisão inteira de m por n

$g_6(n, m) = n + m$

$g_7(n, m) = n^m$