Números Inteiros e Criptografia 2023.1

Hugo Nobrega

Lista de Exercícios 4

Entregue todas as questões marcadas com * até
10 de julho às 20:00
Em todas as questões, você sempre pode usar tudo que foi feito em sala ou que apareceu em listas de exercícios anteriores (mesmo questões que você não tenha resolvido), mas deve citar claramente o que está usando.

Questão 1 (Reescrevendo expressões)**.** Em matemática, o uso de reticências "..." em expressões é bastante comum; por exemplo, a função $f : \mathbb{N} \to \mathbb{N}$ dada por

$$f(n) = \text{ a soma dos } n \text{ primeiros números naturais}$$

é comumente escrita da forma

$$f(n) = 0 + 1 + 2 + 3 + \cdots + (n-1). \tag{$\star$}$$

Entretanto, o uso de reticências pode causar problemas de incerteza e ambiguidade, pois assume que o leitor será capaz de *deduzir* o conteúdo ocultado pelas reticências, o que pode não ser imediato. De fato, é bem questionável deduzir o valor "correto" de $f(0)$ a partir da expressão ($\star$). (O valor que funciona melhor, e que se usa por convenção, é $f(0) = 0$.)

Em geral, o uso de reticências esconde uma definição recursiva; *oficialmente* a função f acima é definida por

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

Em cada item abaixo, reescreva a expressão que define $g : \mathbb{N} \to \mathbb{N}$ de forma recursiva, sem o uso de reticências (nem de *somatórios*, *produtórios* ou afins).

a. $g(n) =$ "a soma dos quadrados dos n primeiros naturais"

b. $g(n) =$ "a soma dos n primeiros naturais ímpares"

c. $g(n) =$ "a soma dos cubos dos n primeiros naturais"

* **d.** $g(n) = \dfrac{1}{1 \cdot 2} + \dfrac{1}{2 \cdot 3} + \cdots + \dfrac{1}{(n+1)(n+2)}$

e. $g(n) =$ "o produto dos n primeiros naturais pares"

f. $g(n) =$ "o produto dos n primeiros primos". Você pode usar a expressão "o n-ésimo primo" na sua solução.

* **g.** $g(n) =$ "o produto de todos os primos até n (incluindo n, se for o caso)". Você pode usar expressões do tipo "x é primo" na definição recursiva de g. (Por exemplo, temos $g(3) = 6 = g(4)$.

h. $g(n) = \prod_{i=0}^{n} h(i)$, onde $h : \mathbb{N} \to \mathbb{N}$ é uma função qualquer dada (e "h" pode e deve aparecer na sua solução).

Questão 2. Prove por indução que

a. Para todo $n \geqslant 1$, a soma dos quadrados dos n primeiros naturais é $\frac{(n-1)n(2n-1)}{6}$.

b. Para todo $n \geqslant 1$, a soma dos cubos dos n primeiros naturais é $\frac{(n-1)^2 n^2}{4}$.

c. $n^2 < 2^n$, para todo natural $n \geqslant 5$.

d. $n^2 < n!$, para todo natural $n \geqslant 4$.

* **e.** $n^3 - n$ é divisível por 3, para todo natural n.
Dica/Lembrete: $(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$.

* **f.** $\mathrm{mdc}(F(n), F(n+1)) = 1$, para todo natural n, onde F é a função de Fibonacci.

g. $3^{n+1} - 2$ é ímpar, para todo natural n.

***Questão 3.** Encontre uma fórmula fechada (i.e., uma fórmula não-recursiva e que não use reticências, somatórios ou produtórios) para a seguinte expressão (em função de n) e depois prove (por indução) que a fórmula encontrada está correta para todo natural n:

$$\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \cdots + \frac{1}{(n+1)(n+2)}$$

Questão 4. Seja $g : \mathbb{N} \to \mathbb{N}$ uma função definida recursivamente:

$$g(n) = \begin{cases} 11, & \text{se } n = 0 \\ 3, & \text{se } n = 1 \\ g(\frac{n-1}{2} - 1) + g(n-1) + 1, & \text{se } n \geqslant 2 \text{ é ímpar} \\ 2 \cdot g(\frac{n}{2} - 1) + 3 \cdot g(n-2), & \text{se } n \geqslant 2 \text{ é par} \end{cases}$$

a. Justifique por que essa definição recursiva "funciona", i.e, está bem feita.

* **b.** Prove por indução que $g(n)$ é ímpar para todos os naturais n.

Questão 5 ("Estendendo Fibonacci")**.** Considere a seguinte "proposta" de definição recursiva de uma função $G : \mathbb{Z} \to \mathbb{Z}$, a função de *Gibonacci*:

$$G(x) = \begin{cases} 0, & \text{se } x = 0 \\ 1, & \text{se } x = 1 \\ G(x-2) + G(x-1), & \text{se } x \geqslant 2 \\ G(x+2) - G(x+1), & \text{se } x < 0 \end{cases}$$

a. Encontre os valores de $G(x)$ para todos inteiros x com $-6 \leqslant x \leqslant 6$.

b. Justifique por que a definição recursiva de G "funciona", i.e., está bem feita. Em outras palavras, dê uma "ordenação dos casos" que justifique a definição.

* **c.** Prove que para qualquer $x \in \mathbb{Z}$ temos $G(x) = G(x-2) + G(x-1)$ e $G(x) = G(x+2) - G(x+1)$.

* **d.** Prove que para qualquer $x \in \mathbb{Z}$, se $3 \mid G(x)$ então $3 \mid G(x+4)$ e $3 \mid G(x-4)$.

* **e.** Prove que para qualquer $x \in \mathbb{Z}$, se $4 \mid x$ então $3 \mid G(x)$.

f. Prove que para qualquer $x \in \mathbb{Z}$ temos:

$$G(x) = \begin{cases} G(-x), & \text{se } x \text{ é ímpar} \\ -G(-x), & \text{se } x \text{ é par} \end{cases}$$

Questão 6. São dadas 3^n moedas de um real, uma das quais foi adulterada e pesa menos do que devia. Você tem uma balança de dois pratos mas não tem pesos; a única forma de pesagem permitida consiste em pôr algumas moedas em cada prato e verificar se a balança está equilibrada. Mostre, por indução, que n pesagens deste tipo são suficientes para achar a moeda adulterada, sendo n um natural qualquer.

Questão 7. Vamos denotar o n-ésimo primo por p_n, começando a contagem em $n = 0$. Assim $p_0 = 2$, $p_1 = 3$, $p_2 = 5$, etc. O objetivo ao final desta questão é achar um limite superior para o n-ésimo primo em função de n.

a. Mostre que $p_{n+1} \leqslant (p_0 \cdot p_1 \cdot p_2 \cdots p_n) + 1$. (*Dica*: $(p_0 \cdot p_1 \cdot p_2 \cdots p_n) + 1$ é um número natural maior ou igual a 2, logo tem algum fator primo)

b. Mostre por indução que para todo $n \in \mathbb{N}$ temos $\displaystyle\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$.

(Isso apenas diz que o número que escrito em binário é $1 \cdots 1$, com $n+1$ algarismos 1, vem imediatamente antes do número que escrito em binário é $10 \cdots 0$, com $n+1$ algarismos 0.)

c. Use indução e os itens anteriores para mostrar que o n-ésimo número primo satisfaz a desigualdade $p_n \leqslant 2^{(2^n)}$.

***Questão 8** (Jogo — cobrindo tabuleiros)**.** Seja $n \in \mathbb{N}$ e considere um tabuleiro quadrado subdividido em $2^{2n} = 4^n$ quadrados. Em outras palavras, o tabuleiro inteiro é um "quadradão" com lado 2^n "quadradinhos". Considere o seguinte jogo: primeiramente um quadrado Q do tabuleiro é escolhido por seu pior inimigo. Em seguida, usando apenas peças que cobrem 3 quadradinhos em formato "L", o seu objetivo como jogador é cobrir o tabuleiro todo *exceto* pelo quadrado Q, que deve permanecer descoberto. As peças não podem se sobrepor.

(Veja um possível estágio intermediário do "jogo" para o caso $n = 4$ na Figura~1 abaixo — não há nenhuma garantia sobre esse estágio intermediário ser bom ou ruim para se obter uma solução final!)

Prove, por indução, que esse jogo pode ser vencido para qualquer $n \in \mathbb{N}$ e qualquer escolha do quadrado Q.

Dica: Para que o método de indução seja útil, você deve conseguir expressar a solução para o tabuleiro de tamanho 4^n em função de soluções para tabuleiros *mais simples* em algum sentido. Lembre-se que os números da forma 4^n com $n > 0$ sempre podem ser divididos por 4.

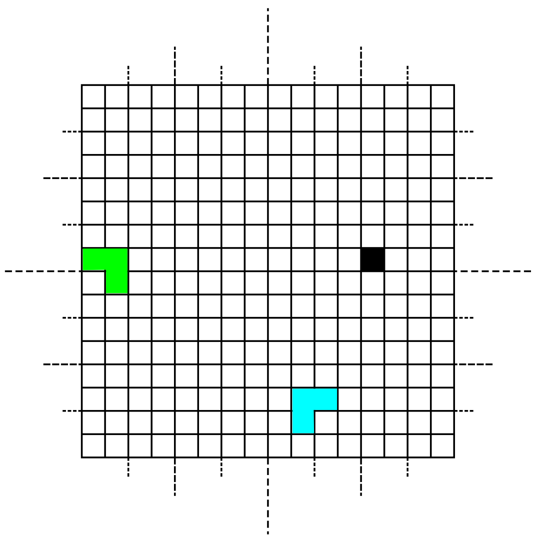

Figura 1: Um tabuleiro com $n = 4$, quadrado Q exibido em preto, e duas peças em "L" dispostas sobre o tabuleiro. As linhas tracejadas são apenas para facilitar a visualização.