Números Inteiros e Criptografia, 2021.1

Lista de Exercícios 3[†]

Submeta as soluções das questões marcadas com * salvando um arquivo na sua pasta no Google Drive[‡]

Data limite para entrega: **24 de setembro** às 18:00.

Em qualquer questão, você pode usar tudo que foi visto em aula (a não ser que a questão proíba isso) ou qualquer outro exercício das listas, desde que seja claro na sua referência do resultado que está usando, e desde que não crie dependências circulares.

Questão 1 (Reescrevendo expressões)**.** Em matemática, o uso de reticências (i.e., "$\cdots$" ou "$\ldots$") 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

$$f(n) = 1 + 2 + 3 + \cdots + (n-1). \qquad (\star)$$

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

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

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. $g(n) = 1^2 + 2^2 + \cdots + (n-1)^2$

b. $g(n) = 1 + 3 + 5 + \cdots + (2n-1)$

* **c.** $g(n) = 1^3 + 2^3 + \cdots + (n-1)^3$

[†]Publicada em 10/9.

[‡]Link recebido por email em 5/8/2021. A pasta tem um nome similar a `<seu nome> - Cripto 2021.1 - Submissões e Feedback`; em caso de qualquer dúvida entre em contato com o professor.

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

e. $g(n) = 2 \cdot 4 \cdot 6 \cdots (2n)$

f. $g(n) = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdots p_n$, onde p_n é o n-ésimo primo (veja a Questão 6 para mais detalhes). Você pode usar a expressão "p_n" na definição recursiva de g.

* **g.** $g(n) = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdots p$, onde p é o *maior* primo tal que $p \leq n$. Você pode usar expressões do tipo "x é primo" na definição recursiva de g. (Por exemplo, temos $g(3) = 6 = g(4)$. Qual deve ser a definição do caso base $g(0)$ para que a definição recursiva *funcione bem*?)

Questão 2. Prove por indução que

a. $1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$, para todo natural n.

b. $1^3 + 2^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}$, para todo natural n.

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

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

* **e.** $3^{n+1} - 2$ 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:

$$g(n) = \begin{cases} 1, & \text{se } n = 0 \\ 3, & \text{se } n = 1 \\ g(\frac{n}{2} - 1) + 2 \cdot g(n-1), & \text{se } n \geq 2 \text{ é par} \\ 4 \cdot g(\frac{n-1}{2} - 1) + 3 \cdot g(n-2), & \text{se } n \geq 2 \text{ é ímpar} \end{cases}$$

* **a.** Descreva as cinco primeiras "camadas" da "cebola" que justifica essa definição recursiva.

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

Questão 5. 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 6. 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 $p_{n+1} \leq (p_0 \cdot p_1 \cdots p_n) + 1$. (*Dica*: $(p_0 \cdot p_1 \cdots p_n) + 1$ 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 $\displaystyle\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$.

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

***Questão 7.** Prove que qualquer número natural $n \geq 8$ pode ser escrito como uma soma onde todas as parcelas são 3 ou 5 (por exemplo, $11 = 3 + 3 + 5$).