Números Inteiros e Criptografia 2026-2

Hugo Nobrega

Lista de Exercícios 2

Entregue todas as questões marcadas com * até
9 de outubro às 18:00 (nova data)

A entrega é pelo Google Drive, na pasta que você recebeu por e-mail. As listas podem ser entregues por grupos de até 4 alunos. Apenas 1 aluno do grupo deve submeter as respostas. Os nomes e DREs dos componentes do grupo devem estar indicados claramente.

Questão 1. 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

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

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

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

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 (assim, "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. $\text{mdc}(F(n), F(n+1)) = 1$, para todo natural n, onde F é a função de Fibonacci.

***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. 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:

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

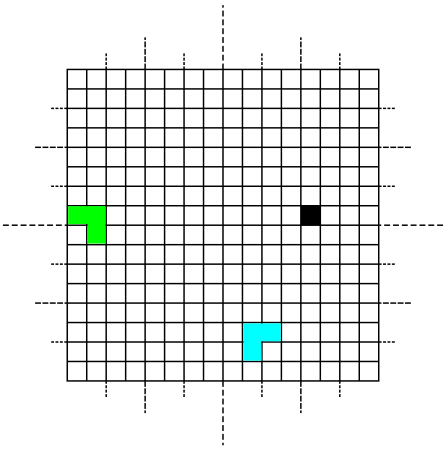
Questão 6. São dadas 3^n moedas de um real, uma das quais foi adulterada e pesa menos do que devia. Você tem uma balança de dois pratos mas não tem pesos; a única forma de pesagem permitida consiste em pôr algumas moedas em cada prato e verificar se a balança está equilibrada. Mostre, por indução, que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

***Questão 7.** 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, e cada peça deve cobrir 3 quadradinhos do tabuleiro.

(Veja um possível estágio intermediário do "jogo" para o caso $n = 4$ na figura 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.



Questão 8. No jogo de xadrez, o cavalo se move em "L", i.e., andando 2 casas na horizontal/vertical e 1 casa na vertical/horizontal (respectivamente).

a. Prove que, para qualquer $n \geqslant 4$, um cavalo começando na casa do canto inferior esquerdo de um tabuleiro $n \times n$ consegue chegar a qualquer outra casa do tabuleiro em uma quantidade finita de movimentos.

b. Prove que o mesmo vale mesmo sem assumirmos que o cavalo começa no canto inferior esquerdo do tabuleiro, i.e., prove que para todo $n \geqslant 4$ o cavalo consegue chegar de qualquer casa a qualquer casa de um tabuleiro $n \times n$ em uma quantidade finita de movimentos.

Questão 9.

Definição 1. 1. Dizemos que um polígono é *convexo* se nenhum segmento de reta ligando lados distintos do polígono encontra algum outro lado (i.e., se todo segmento de reta entre lados distintos do polígono fica completamente no interior do polígono).

2. Uma *diagonal* de um polígono convexo é um segmento de reta que liga dois vértices não-consecutivos do polígono (i.e., é um segmento de reta que liga dois vértices do polígono, desde que esse segmento não seja um dos lados do polígono).

3. Uma *triangulação* de um polígono convexo é um conjunto de triângulos com as propriedades:

   (a) Os vértices dos triângulos são vértices do polígono original;

   (b) As arestas dos triângulos não se cruzam, i.e., só podem se encontrar em vértices dos triângulos ou coincidirem exatamente;

   (c) Os triângulos cobrem exatamente o polígono todo (sem sobra nem falta).

   Em outras palavras, uma triangulação de um polígono é obtida pela adição ao polígono de diagonais que não se cruzem, de forma que na nova figura todas as regiões formadas sejam triângulos.

Você pode assumir como verdadeiro o seguinte:

Teorema 2. *Qualquer diagonal de um polígono convexo o "separa" em dois polígonos convexos menores.*

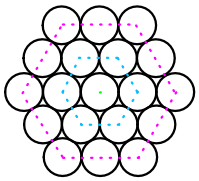
a. Prove por indução que todo polígono convexo com $n \geqslant 3$ vértices possui exatamente $\dfrac{n(n-3)}{2}$ diagonais.

b. Prove por indução que toda triangulação de polígono convexo com $n \geqslant 3$ vértices possui exatamente $n-2$ triângulos.

*** c.** Prove por indução que, para todo polígono convexo P com $n \geqslant 4$ vértices e toda diagonal d de P, há uma triangulação de P na qual d é aresta de algum dos triângulos.

Questão 10.

Definição 3. Vamos dizer que um número natural n é *compacto* se podemos organizar n moedas de mesmo tamanho formando um "padrão hexagonal", como na figura abaixo.[a]



[a] Vamos forçar um pouco a barra e dizer que uma única moeda também forma um hexágono.

Assim, 1, 7 e 19 são compactos (pela figura acima), mas 9 não é. O nome "compacto" vem do fato desta ser a forma mais eficiente de se cobrir o plano com círculos de mesmo tamanho, fato provado por Lagrange no século XVIII. Esse é um caso particular do problema de *empacotamento de esferas*.

a. Dê uma definição recursiva para a sequência dos números compactos $1, 7, 19, \ldots$

b. 129 é um número compacto?

***Questão 11.** Em um torneio de *Winning Eleven* com $n \geqslant 2$ jogadores, cada jogador jogou exatamente 1 vez contra cada outro jogador, e nenhum jogo terminou em empate. Prove que existe um jogador A tal que, para todo outro jogador B:

- B perdeu seu jogo contra A, ou
- B perdeu o jogo contra alguém que por sua vez perdeu seu jogo contra A.