Números Inteiros e Criptografia, PLE 2020, Lista de Exercícios 7
Aluno: Luiz Rodrigo Lacé Rodrigues
DRE: 118049873

Questão 1
a) $g(n) = 1^2 + 2^2 + \cdots + n^2$

$g(1) = 1$
$g(n) = g(n-1) + n^2$, para $n>1$

d) $g(n) = 1/(1 \cdot 2) + 1/(2 \cdot 3) + \cdots + 1/n(n + 1)$

$g(1) = 1/(1 \cdot 2)$
$g(n) = g(n-1) + 1/n(n+1)$, para $n>1$

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

$g(1) = 2$
$g(n) = g(n-1) * 2n$, para $n>1$

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 7 para mais detalhes). (Você pode usar p_n na definição recursiva de g.)

$g(1) = 2$
$g(n) = g(n-1) * p_n$, para $n>0$

h) g(n) = Xn i=1 f(i) = f(1) + f(2) + · · · + f(n), onde f : N → N é uma função dada. (A sua resposta pode e deve usar f na definição recursiva de g).

$g(1) = f(1)$
$g(n) = g(n-1) + f(n)$, para todo $n>1$

Questão 2. Prove por indução que:

a) $1^2 + 2^2 + \cdots + n^2 = n(n+1)(2n+1)/6$, para todo natural $n \geq 1$.

Caso base:

$1^2 = n(n+1)(2n+1)/6$

/\

\/

$1 = 1(2)(3)/6$

/\

\/

$1=1$

/\

\/

$p(1)$

Caso indutivo:

$P(k)$

/\

\/

$1^2 + 2^2 + \cdots + k^2 = k(k+1)(2k+1)/6$

/\

\/

$1^2 + 2^2 + \cdots + k^2 = (k^2 + k)\ (2k+1)$

/\

\/

$1^2 + 2^2 + \cdots + k^2 = 2k^3+3k^3+k$

/\

\/

$1^2 + 2^2 + \cdots + k^2 = (2k^3+6k^2+4k+3k^2+9k+6- 6k^2-12k-6)/6$

/\

\/

$1^2 + 2^2 + \cdots + k^2 = (2k^3+6k^2+4k+3k^2+9k+6)/6 - 6(k^2+2k+1)/6$

/\

\/

$1^2 + 2^2 + \cdots + k^2 + (k^2+2k+1) = (2k^3+6k^2+4k+3k^2+9k+6)/6$

/\

\/

$1^2 + 2^2 + \cdots + k^2 + (k+1)^2 = (2k^3+6k^2+4k+3k^2+9k+6)/6$

/\

\/

$1^2 + 2^2 + \cdots + k^2 + (k+1)^2 = (k^2+3k+2)(2k+3)/6$

/\

\/

$1^2 + 2^2 + \cdots + k^2 + (k+1)^2 = (k+1)(k+2)(2k+3)/6$

/\

\/

$1^2 + 2^2 + \cdots + k^2 + (k+1)^2 = (k+1)(k+2)(2(k+1)+1)/6$

/\

\/

$p(k+1)$

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

Caso base:

$P(1) = 1^2<2^1$,falso

$P(2) = 2^2<2^2$, falso

$P(3) = 3^2<2^3$, falso

$P(4) = 4^2<2^4$, falso

$P(5) = 5^2 < 2^5$, verdadeiro

Observamos que nossa desigualdade só é verdadeira a partir de n=5, vamos conferir agora $n^2 < 2^n$ caso $n>5$

Caso indutivo:

P(k)

/\

\/

$k^2<2^k$

/\

\/

$2k^2<2^{(k+1)}$

/\

\/

Sabendo que $2k^2>k^2$

/\

\/

$2k^2 + (1+2k) >k^2 + (1+2k)$

/\

\/

$k^2 + (k^2 +2k + 1) > k^2 + 2k + 1$

/\

\/

$k^2 + (k+1)^2 > (k+1)^2$

/\

\/

Sabendo disso, por transitividade temos que:

$(k+1)^2 < 2^{(k+1)}$

/\

\/

P(k+1)

f) $n^3 - n$ é divisível por 3, para todos naturais $n \geq 1$.

Caso base:

P(1): $3|1^3-1$

$3|0$

$0=3*0$

Caso indutivo:

P(k)

/\
\/

$3|\ k^3-k$

/\
\/

$3|(k^3-k) + 3(k^2+k)$

/\
\/

$3|(k^3+3k^2 + 3k - k)$

/\
\/

$3|(k^3+3k^2 + 3k + 1) - (k+1)$

/\
\/

$3|(k^3+2k+1)(k+1) - (k+1)$

/\
\/

$3|(k+1)^3 - (k+1)$

/\
\/

P(k+1)

g) mdc(F(n), F(n + 1)) = 1, para todo natural n ≥ 1, onde F(n) é o n-ésimo número de Fibonacci.

Temos que a sequência de Fibonacci é dada por:
0,1, 1, 2, 3, 5, 8, 13, 21…
Ou seja, podemos dizer que a definição da sequência é:
F(n+2) = F(n) + F(n+1)

Caso base:
P(1) = mdc(F(1), F(2)) = 1

Caso indutivo:
P(k)
/\
\/
mdc(F(k) + F(k+1))= 1
/\
\/
Por bezout sabemos que:
α(F(k)) + β(F(k+1)) = 1
/\
\/
Substituindo o que temos da definição da sequência de Fibonacci:
α(F(k+2) - F(k+1)) + β(F(k+1)) = 1
/\
\/
F(k+1)(β-α) + f(k+2)α= 1
Por Bezout temos:
/\
\/
mdc(F(k+1) , F(k+2)) = 1
/\
\/
P(k+1)

*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 $n \geq 1$:

$1/(1 \cdot 2) + 1/(2 \cdot 3) + \cdots + 1/n(n + 1)$

Vamos testar alguns valores:

$n(1)$: $1/(1 \cdot 2) = 1/2$

$n(2) = 1/(1 \cdot 2) + 1/(2 \cdot 3) = 1/2 + 1/6 = (6 + 2)/6*2 = 8/12 = 4/6 = 2/3$

$n(3) = 1/(1 \cdot 2) + 1/(2 \cdot 3) + 1/(3 \cdot 4) = 1/2 + 1/6 + 1/12 = 3/4$

Podemos escrever a função fechada dessa expressão como $n/n+1$

Para o caso indutivo dessa função:

$P(k)$

/\
\/

$1/(1 \cdot 2) + 1/(2 \cdot 3) + \cdots + 1/k(k + 1) = k/k+1$

/\
\/

$1/(1 \cdot 2) + 1/(2 \cdot 3) + \cdots + 1/k(k + 1) = k(k+2)/(k+1)(k+2)$

/\
\/

$1/(1 \cdot 2) + 1/(2 \cdot 3) + \cdots + 1/k(k + 1) = (k^2+2k)/(k+1)(k+2)$

/\
\/

$1/(1 \cdot 2) + 1/(2 \cdot 3) + \cdots + 1/k(k + 1) = (k^2+2k + 1) - 1/(k+1)(k+2)$

/\
\/

$1/(1 \cdot 2) + 1/(2 \cdot 3) + \cdots + 1/k(k + 1) = (k+1)^2 - 1/(k+1)(k+2)$

/\
\/

$1/(1 \cdot 2) + 1/(2 \cdot 3) + \cdots + 1/k(k + 1) = (k+1)^2/(k+1)(k+2) - 1/(k+1)(k+2)$

/\
\/

$1/(1 \cdot 2) + 1/(2 \cdot 3) + \cdots + 1/k(k + 1) = k+1/k+2 - 1/(k+1)(k+2)$

/\
\/

$1/(1 \cdot 2) + 1/(2 \cdot 3) + \cdots + 1/k(k + 1) + 1/(k+1)(k+2) = k+1/k+2$

/\
\/

$P(k+1)$

*Questão 5. Seja g uma função definida recursivamente:
$g(1) = 1$
$g(2) = 3$
$g(k) = g(k - 2) + 2 \cdot g(k - 1)$,se $k \geq 3$
Prove por indução forte que $g(n)$ é ímpar para todos os naturais $n \geq 1$.

Caso base:
$g(1) = 1$: ímpar
$g(2) = 3$: ímpar

Caso indutivo: $\forall i$, $1 \leq i \leq k$, $g(i)$ é ímpar
Nossa hipótese de indução forte é que nós assumimos que para todo "i" entre 1 e k, g(i) é ímpar

Precisamos agora provar que $g(k+1)$ é ímpar

Como $g(k) = g(k - 2) + 2 \cdot g(k - 1)$, então $g(k+1) = g(k - 1) + 2 \cdot g(k)$

Pela hipótese de indução forte $g(k-1)$ e $g(k)$ são ímpares, então escrevemos eles em forma de números ímpares:

$g(k-1) = 2x+1$
$g(k) = 2y+1$

Substituindo em $g(k+1) = g(k - 1) + 2 \cdot g(k)$ chegamos em:
$g(k+1) = (2x+1) + 2(2y+1)$
$g(k+1) = 2x+1 + 4y+ 2$
$g(k+1) = 2x + 4y + 3$, logo $g(k+1)$ é ímpar.

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

Do enunciado tiramos que nosso P(n) nos diz que de 3^n moedas, nós precisamos de n pesagens para descobrir a moeda adulterada.

Caso base:
P(1) = 3^1 moedas → 1 pesagem

Caso indutivo:
P(k) = 3^k moedas → k pesagens
Precisamos provar:
P(k+1) = 3^(k+1) moedas → k+1 pesagens

Se temos 3 "sacos" de 3^k moedas vamos precisar de uma pesagem para descobrir em qual desses grupos a moeda adulterada está contida, visto que pesando dois sacos, ou já sabemos qual deles é o adulterado pelo resultado da balança, ou se o peso se igualar, temos que o nosso grupo com a moeda adulterada é o que ainda não foi pesado.
Como sabemos que é necessário k pesagens para descobrir a moeda adulterada em 3^k moedas, se temos 3 "sacos" de 3^k moedas ou seja 3*3^k, vamos precisar das mesmas k pesagens mais uma para descobrir em qual dos sacos ela está. Logo 3^(k+1) moedas → k+1 pesagens que é o nosso P(k+1).

Questão 9

Prove por indução que qualquer número natural $n \geq 8$ pode ser escrito como uma soma de 3's e 5's

Do enunciado, podemos dizer que:

$P(n)$: $n= 3a+5b$, para $n\geq8$

Caso base:

$P(8) = 8 = 3(1) + 5(1)$

Caso indutivo:

$P(k)$

/\

\/

$k = 3d + 5e$

/\

\/

$k+1 = 3d + 5e + 1$

/\

\/

$mdc(3,5) = 1$, por bezout temos $3\alpha+5\beta = 1$

Substituindo na equação acima temos:

$k+1 = 3d + 5e + 3\alpha+5\beta$

/\

\/

$k+1 = 3(d+\alpha) + 5(e+\beta)$

/\

\/

$k+1 = 3x + 5y$, sabendo que x e y são inteiros e supondo que $x= d+\alpha$ e $y=e+\beta$

/\

\/

$P(k+1)$