Números Inteiros e Criptografia, PLE 2020, Lista de Exercícios 6
Aluno: Luiz Rodrigo Lacé Rodrigues
DRE: 118049073

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

aditiva se, para todos n, m $\in$ N \ {0}:

se mdc(n, m) = 1 então f(n · m) = f(n) + f(m).

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

f(n · m) = f(n) + f(m).

multiplicativa se, para todos n, m $\in$ N \ {0}:

se mdc(n, m) = 1 então f(n · m) = f(n) · f(m)

completamente multiplicativa se, para todos n, m $\in$ N \ {0}:

f(n · m) = f(n) · f(m)

• ω(n) = número de fatores primos de n distintos.

Se o mdc(n,m) = 1, temos que m e n são coprimos.
Então para ω(n*m) = ω(n) + ω(m), como a função da multiplicação de n*m é igual a soma das funções desses números separadamente, podemos notar que a fatoração da multiplicação desses números será a fatoração em primos desses números separadamente e depois multiplicada.
Um exemplo é: n = 20, m=21
Fatorando esses números temos que 20 = (2^2 * 5) e 21 = (3 * 7), a multiplicação desses números é puramente (2^2 * 5 * 3 * 7), ou seja, a quantidade de fatores primos distintos segue inalterada.
Então temos que essa igualdade é verdadeira, assim essa função é aditiva.

Entretanto, quando saímos da relação entre coprimos, podemos escrever fazer que n = 2 e m = 4 vamos ter ω(8) = ω(2) + ω(4), como 8 é fatorado em 2^3, teremos um fator primo. Mas como ω(2) + ω(4) = 2, essa função não é completamente aditiva.

Novamente, supondo mdc = 1, para ω(n · m) = ω(n) · ω(m), entretanto, se fizermos n=2 e m=3, teremos ω(6) = ω(2) · ω(3).
Fatorando 6 em 2*3 temos que a função nos resulta que 2 = 1, o que não é verdade.
Assim temos que nossa função não é multiplicativa.

Dado que se uma função é completamente multiplicativa então ela implica ser multiplicativa, pela contrapositiva dessa afirmação, se uma função não é multiplicativa então ela não é completamente multiplicativa.
Provamos assim que não é multiplicativa, logo também não é completamente multiplicativa.

- $\Omega(n)$ = número de fatores primos de n contando todas as repetições!

Saindo do campo onde estamos tratando apenas coprimos, diferente de $\omega(n)$ onde estávamos limitados a apenas fatores primos distintos, podemos contabilizar os fatores repetidos.
Utilizamos n=2 e m=4, como utilizamos como contra-exemplo para $\omega(n)$, agora acharemos $\Omega(8) = \Omega(2) + \Omega(4)$. Fatorando esses números , achamos que:
$8 = 2^3$
$2 = 2$
$4 = 2^2$

Como estamos contabilizando o número de fatores com suas repetições, agora encontramos $\Omega(8) = 3$ e $\Omega(2) + \Omega(4) = 3$, que é uma igualdade verdadeira.
Resumindo, a função $\Omega(n)$ tira o bloqueio de contabilizarmos os fatores repetidos, temos agora que nossa função é completamente aditiva.
Pela definição das funções aditivas, podemos dizer que se ela é completamente aditiva, então ela implica em ser aditiva.

Voltando para o caso de mdc(nm) = 1, mas analisando $\Omega(n \cdot m) = \Omega(n) \cdot \Omega(m)$, com n=2 e m=3 teremos $\Omega(6) = \Omega(3) \cdot \Omega(2)$, vamos achar de novo que 2 = 1, o que não é verdade.
Pela contrapositiva da definição da função multiplicativa,como não é multiplicativa, também não é completamente multiplicativa.

- d(n) = número de divisores positivos de n

Para o mdc(n,m) = 1, temos então que m e n são coprimos.
Para d(n*m) = d(n) + d(m) vamos analisar o número de divisores positivos de cada partícula dessa igualdade:

Quando fazemos d(n*m) = d(n) + d(m) com n=3 e m=20 onde mdc(3,20) = 1, temos que:

d(3) = 2 divisores, sendo eles 1,3
d(20) = 6 divisores, sendo eles 1, 2, 4, 5, 10, 20
d(60) = 12 divisores, sendo eles 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60.

logo d(60) = d(20) + d(3)
12 = 8

Nossa igualdade então não é verdadeira, provando que nossa função não é aditiva. Pela definição de função aditiva, já inferimos que se uma função é completamente aditiva logo ela é aditiva, pela contrapositiva temos que se nossa função não é completamente aditiva logo não é aditiva. Provamos assim que nossa função também não é completamente aditiva.

Voltando para o campo onde mdc(n,m) = 1, onde m e n são coprimos. Analisando $d(n \cdot m) = d(n) \cdot d(m)$

Vamos supor n e m primos, que a multiplicação de m*n nos gera 4 divisores, 1, m, n e m*n, falta descobrir se $d(n) \cdot d(m)$ nos traz o mesmo resultado.
Sabendo que m e n são primos e diferentes, cada um deles possui 2 divisores diferentes, então 2 * 2 = 4.A mesma premissa se aplica para m,n coprimos em geral, pois seus divisores serão disjuntos, e sua multiplicação irá "herdar" essa quantidade de divisores. Então sim, nossa função é multiplicativa pois nossa igualdade é verdadeira.

Para todos os naturais positivos e não só os coprimos pegamos agora n=2 e m =4, onde temos $d(8) = d(2) \cdot d(4)$, entretanto vamos achar que 8 tem 4 divisores, 2 tem 2 divisores e 4 possui 3 divisores, dessa igualdade vamos chegar em 8 = 6, o que não é verdade. Logo nossa função não é completamente multiplicativa.

- S(n) = soma dos divisores positivos de n

Para para m,n onde mdc(n,m) = 1,e por isso coprimos, pegamos n=2 e m=3
assim para S(n*m) = S(n) + S(n), vamos achar que:
S(2) = 3, visto que é a soma de seus divisores (1,2)
S(3) = 4, visto que é a soma de seus divisores (1,3)
S(6) = 12, visto que é a soma de seus divisores (1,2,3,6)
Logo achamos que 12 = 7, o que não é verdade, assim provamos que nossa função não é aditiva.
Temos a afirmação que se uma função é completamente aditiva, então ela é adivita.
Pela contrapositiva dessa afirmação, se a função não é aditiva, então ela não é completamente aditiva. Logo, como vimos que nossa função não é aditiva, ela também não é completamente aditiva.

Para testarmos se nossa função é multiplicativa, voltamos apenas para os casos onde mdc(m,n)=1, logo coprimos.
Não teremos divisores comuns entre m e n.
Vamos analisar tais números na função S(n*m) = S(n) * S(n)
Os divisores de m*n vão herdar os divisores de m e n separadamente, além de agora serem divisíveis por eles mesmos
Um exemplo seria n=3, m =2
S(6) = 1+2+3+6 = 12, que fatorado nos dá 2^2 * 3
S(3) = 1,3 = 4, que fatorado nos dá 2^2
S(2) = 1,2 = 3, que fatorado dá ele mesmo
Ou seja, nossa igualdade se confirma quando confirmamos que a fatoração no número m*n é exatamente igual a multiplicação da fatoração de seus números separadamente.

Caso m,n não sejam primos temos que pegamos o exemplo de n = 2 e m = 4, assim temos que:
S(2) = 1+2 = 3
S(4) = 1+2+ 4 = 7
S(8) = 1+2+4+8 = 15

Ou seja, nossa igualdade S(8) = S(4) * S(2), nos retorna 15 = 21, o que não é verdade. Logo nossa função não é completamente multiplicativa

- h(n) = n^123456789

Para o caso de mdc(n,m) = 1, onde n,m são coprimos, vamos supor que n=2 e m=3, assim analisamos se h(n*m) = h(n)+h(m)
h(3*2) = h(3) + h(2)
Para facilitar nossa conta, vamos utilizar x = 123456789
logo temos que:
(3*2)^x = 3^x + 2^x

Manipulando essa expressão chegamos que:
3^x * 2^x = 3^x + 2^x

Dividindo todo mundo por (2^x) nós chegamos em
3^x = (3^x/2^x) + 1

O que é mentira visto que estaríamos dizendo que nosso número é menor que ele mesmo, logo nossa função não é aditiva.
E como ser completamente aditiva implica em ser aditiva, pela contrapositiva, se ela não é aditiva então não pode ser completamente aditiva. Assim temos que nossa função também não é completamente aditiva

Vamos analisar h(n*m) = h(n) * h(m). Repare que independente do número vamos encontrar que (n*m)^x = n^x * m^x, que manipulando vamos encontrar (n*m)^x = (n*m)^x. Como funciona para todos os naturais positivos, temos que nossa função é completamente multiplicativa. E como ser completamente multiplicativa implica que ela também é multiplicativa, então temos que nossa função também é multiplicativa.

- j(n) = 123456789 · n

Para mdc(n,m) = 1, ou seja n,m coprimos, vamos analisar j(m*n) = j(n) + j(m) com n=2 e m=3, temos então j(6) = j(2) + j(3) e vamos aplicar esses valores na função j(n).
Novamente para facilitar nossos cálculos vamos utilizar x = 123456789
j(6) = 6x
j(2) = 2x
j(3) = 3x
Pela igualdade temos que 6x = 2x+3x, colocando o x em evidencia temos que 6x=5x, o que não é verdade. Então nossa função não é aditiva, e como não é

aditiva, também não é completamente aditiva, como já citamos essa contrapositiva inúmeras vezes anteriormente.

Analisando agora j(m*n) = j(n) * j(m) ainda com n,m coprimos. Vamos supor de novo que n=2 e m=3, lembrando que estamos usando x = 123456789 logo j(6) = j(2) * j(3) temos que 6x = 2x * 3x, entretanto vamos chegar em 6x = 6x^2, o que não é verdade, logo nossa função não é multiplicativa. Como sabemos que se uma função é completamente multiplicativa, então pela contrapositiva dessa afirmação temos que se uma função não é multiplicativa isso implica que ela não é completamente multiplicativa. Logo nossa função também não é multiplicativa.

Questão 2)

a. Prove que, para todos naturais n e p, se p é primo e p ≤ n, então p não divide n^# + 1.

Vamos supor que p divide n^# + 1:
p|n^#+ 1^:

n^#+ 1 = p(q), sendo q um inteiro positivo

Colocando o p em evidência:

p(q - (n^#)/p) = 1

Como estamos supondo que p|n^# + 1, então temos também que p|n^# nos resultaria um número inteiro n#/p, vamos chamar esse número de K

p(q - k) = 1

Sabendo que (q - k) é um inteiro,dividimos tudo por p chegamos em:

q - k = 1/p

Como p é um número primo, ele não pode dividir 1, logo chegamos a um absurdo.
Provando então que p ≤ n, então p não divide n^# + 1.

b. Use o item anterior para provar a infinitude dos primos na seguinte forma:
para todo natural n, existe um primo p > n.

Sabemos pelo item anterior que se um número p primo é menor do que n, então ele não dividirá n^# + 1.
Entretanto,pelo Teorema fundamental da Aritmética, nós sabemos que todo número pode ser decomposto em fatores primos de forma única.
Logo no número n^# + 1, existirá um primo em sua fatoração que deve ser maior que n.

Um exemplo:
$n = 4$
$n\# = 2^2$
$n\# + 1 = 2^2 + 1 = 5$
$n = 4$ mas temos um 5 que é nosso p primo.

Questão 3)
a. Determine os valores abaixo, exibindo as contas ao longo do caminho até determinar a resposta:

(i) f1(5, 4)
$f1(n, 0) = n$;
$f1(n, m) = f1(n, m - 1) + 1$, se $m > 0$;

Pela função dada, sabemos que;

$f1(5,4) = f1(5,3) + 1$
$f1(5,3) = f1(5,2) + 1$
$f1(5,2) = f1(5,1) + 1$
$f1(5,1) = f1(5,0) + 1$
$f1(5,0) = 5$

Voltamos na conta aplicando os valores que formos encontrando;
$f1(5,1) = 5 + 1 = 6$
$f1(5,2) = 6 + 1 = 7$
$f1(5,3) = 7 + 1 = 8$
$f1(5,4) = 8 + 1 = 9$

(ii) f2(5, 4):
$f2(n, 0) = 0$
$f2(n, m) = f2(n, m - 1) + n$, se $m > 0$

$f2(5,4) = f2(5,3) + 5$
$f2(5,3) = f2(5,2) + 5$
$f2(5,2) = f2(5,1) + 5$
$f2(5,1) = f2(5,0) + 5$
$f2(5,0) = 0$

Aplicando o valor encontrado;

$f2(5,1) = 0 + 5 = 5$
$f2(5,2) = 5+ 5 = 10$
$f2(5,3) = 10 + 5 = 15$
$f2(5,4) = 15 + 5 = 20$

(iii) f3(5, 24)
$f3(0, m) = 0$
$f3(n, m) = f3(n - 1, m) + 1$, se $n > 0$

$f3(5,24) = f3(4,24) +1$
$f3(4,24) = f3(3,24) + 1$
$f3(3,24) = f3(2,24) + 1$
$f3(2,24) = f3(1,24) + 1$
$f3(1,24) = f3(0,24) + 1$
$f3(0,24) = 0$

Somando o que temos;

$f3(1,24) = 0 + 1 = 1$
$f3(2,24) = 1 + 1 = 2$
$f3(3,24) = 2 + 1 = 3$
$f3(4,24) = 3 + 1 = 4$
$f3(5,24) = 4 + 1 = 5$

(iv) $f4(4, 4)$

$f4(n, 0) = 1$
$f4(n, m) = f4(n, m - 1) \cdot n$, se $m > 0$

$f4(4,4) = f4(4,3) * 4$
$f4(4,3) = f4(4,2) * 4$
$f4(4,2) = f4(4,1) * 4$
$f4(4,1) = f4(4,0) * 4$
$f4(4,0) = 1$

Somando o que temos:
$f4(4,1) = 1 * 4 = 4$
$f4(4,2) = 4 * 4 = 16$
$f4(4,3) = 16 * 4 = 64$
$f4(4,4) = 64 * 4 = 256$

(v) $f5(35, 5)$

$f5(n, m) = 0$, se $m \leq 1$
$f5(n, m) = 1$, se $m > 1$ & m divide n & $\forall k \in N(k < m \to f5(n, k) = 0)$
$f5(n, m) = 0$, nos outros casos

$f5(35,5)$:
$n=35, m=5$
temos que $m>1$ e $m|n$
temos também que
$f5(35,4) = 0$
$f5(35,3) = 0$
$f5(35,2) = 0$
logo $f5(35,5) = 1$

(vi) $f5(35, 7)$

Temos $n=35$, $m = 7$

m>1, m|35
Entretanto temos que
f6(35,6) = 0
f5(35,5) = 1, temos um k<m mas a função nos retorna 1, logo
f5(35,7) = 0

(vii) f6(4, 30)
f6(n, m) = 0 se m < n
f6(n, m) = f6(n, m − n) + 1, nos outros casos

f6(4,30) = f6(4,26) + 1
f6(4,26) = f6(4,22) + 1
f6(4,22) = f6(4,18) + 1
f6(4,18) = f6(4,14) + 1
f6(4,14) = f6(4,10) + 1
f6(4,10) = f6(4, 6) + 1
f6(4,6) = f6(4,2) + 1
f6(4,2) = 0

Somando tudo temos que:
f(4,30) = 6

(viii) f7(28, 70)
f7(n, m) = 0, se 7 não divide n ou 7 não divide m
f7(n, m) = f7(n/7, m/7) + 1, nos outros casos

f7(28,70) = f7(4,10) + 1
f7(4,10) = 0

f7(28,70) = 1

(ix) f8(2, 4)
f8(n, 0) = 1
f8(n, m) = n^f8(n,m−1) , se m > 0

f8(2,4) = 2^f8(2,3)
f8(2,3) = 2^f8(2,2)
f8(2,1) = 2^f8(2,0)
f8(2,0) = 1

Aplicando o valor encontrado:
f8(2,1) = 2
f8(2,3) = 2^2 = 4
f8(2,4) = 2^4 = 16

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

g1(n, m) = o expoente de 7 na fatoração por primos de mdc(n, m)

Temos a nossa função f7 onde:
f7(n, m) = 0, se 7 não divide n ou 7 não divide m
f7(n, m) = f7(n/7, m/7) + 1, nos outros casos
Essa função só terá valor diferente de 0 caso 7 dívida n e m sem deixar resto.
Como 7 é um número primo, então ele fará parte da fatoração desses números, então basta analisar o expoente dele na fatoração.
Caso não sejam divisíveis por 7, então em sua fatoração por primos não terá 7, logo o expoente será 0, pois 7^0 = 1, que está presente em toda fatoração.
temos então que g1=f7

g2(n, m) = n

A função f3 nos diz que:
f3(0, m) = 0
f3(n, m) = f3(n − 1, m) + 1, se n > 0
Sendo assim essa função não depende de m, somente de n.
Repare que vamos somar 1 conforme nosso n for aumentando 1 unidade.
f3(1,m) = f3(0,m) + 1, por definição temos que f3(0,m) = 0, logo
f3(1,m) = 1
f2(2,m) = f3(1,m) + 1, ou seja
f2(2,m) = (f3(0,m) + 1) + 1
Sobra apenas a soma de 1 unidade, exatamente igual a n.
Temos então que g2 = f3

g3(n, m) = n ∗ m

Repare a função f2:
f2(n, 0) = 0
f2(n, m) = f2(n, m − 1) + n, se m > 0
Vamos partir da “base” da função começando por m=0, como está definida;
f2(n, 0) = 0
Perceba o que acontece quando vamos somando 1 unidade a m:
f2(n,1) = f2(n, 0) + n
f2(n,1) = n
f2(n,2) = f2(n,1) + n
f2(n,2) = n + n = 2n
Repare que vamos somar n a função toda vez que m aumentar 1 unidade, ou seja o valor da função será f2(n,m) = n*m
Logo temos que g3=f2

g4(n, m) = 1, se m é o menor número maior do que 1 que divide n;

0, caso contrário

Vejamos a função f5:
$f5(n, m) = 0$, se $m \leq 1$
$f5(n, m) = 1$, se $m > 1$ & m divide n & $\forall k \in N(k < m \rightarrow f5(n, k) = 0)$
$f5(n, m) = 0$, nos outros casos

Para que essa função retorne um número diferente de 0, é preciso que m seja maior que 1 e $m|n$. m também deve ser maior que qualquer número k. Vejamos o exemplo:

f5(35,5):
n=35, m=5
temos que $m>1$ e $m|n$
temos também que
$f5(35,4) = 0$, pois 4 não divide 35
$f5(35,3) = 0$, pois 3 não divide 35
$f5(35,2) = 0$, pois 2 não divide 34
$f5(35,1) = 0$, pois $m = 1$
logo $f5(35,5) = 1$, ou seja m é o menor número depois de 1 que divide n

O que é diferente do que ocorre com f5(35,7), mesmo que 7 seja maior que 1 e também seja divisor de 35, temos um k que é menor que m que retorna um número diferente de 0 que é o 5, pois $5<7$ e $f5(35,5) = 1$.

A característica dessa função é exatamente a de g4 ou seja, g4=f5

g5(n, m) = o quociente da divisão inteira de m por n
Analisando a função f6, temos que:
$f6(n, m) = 0$ se $m < n$
$f6(n, m) = f6(n, m - n) + 1$, nos outros casos

Podemos pensar que no “algoritmo” dessa função nós estamos vendo quantas vezes n cabe em m, e sempre que cabe, nos somamos 1 numa espécie de “contador”.
Vamos ver com um exemplo:
$f6(4,30) = f6(4,26) + 1$
$f6(4,26) = f6(4,22) + 1$
$f6(4,22) = f6(4,18) + 1$
$f6(4,18) = f6(4,14) + 1$
$f6(4,14) = f6(4,10) + 1$
$f6(4,10) = f6(4, 6) + 1$
$f6(4,6) = f6(4,2) + 1$
$f6(4,2) = 0$
Esse nosso “contador” é justamente o nosso quociente que é retornado pela função.
Temos então que g5=f6

g6(n, m) = n + m

Temos a função f1:

f1(n, 0) = n ;

f1(n, m) = f1(n, m − 1) + 1, se m > 0;

A função começa com

f1(n, 0) = n , o que já nos garante que ela vai ter sempre n na sua composição

Conforme vamos somando +1 para o valor de m, teremos:

f1(n, m) = f1(n, m − 1) + 1

Ou seja:

f1(n,1) = f1(n,0) + 1

f1(n,1) = n + 1

f1(n,2) = f(n,1) + 1

f1(n,2) = n + 1 + 1 = n+2

Repare que somamos exatamente o valor de m em n.

Logo, temos que f1(n,m) = n+m. Então temos que g6=f1

g7(n, m) = n^m

Temos a função f4:

f4(n, 0) = 1

f4(n, m) = f4(n, m − 1) · n, se m > 0

Como temos que f4(n, 0) = 1 , vamos analisar f4(n,1)

f4(n,1) = f(n,0) · n

f4(n,1) = 1 · n

f4(n,2) = f(n,1) · n

f4(n,2) = n · n = n^2

f4(n,3) = f4(n,2) · n

f4(n,3) = n^2 · n = n^3

Repara que conforme m cresce, nós multiplicamos o “resultado anterior” por n, ou seja vamos multiplicar n por n, m vezes, o que igual n^m.

Temos então que nossa função g7=f4