Números Inteiros e Criptografia, PLE 2020, Lista de Exercícios 5
Aluno: Luiz Rodrigo Lacé Rodrigues
DRE: 118049873

Questão 1.
Determine se existem inteiros positivos x, y e z que satisfaçam a equação $2^x \cdot 3^4 \cdot 26^y = 39^z$.

Temos $2^x \cdot 3^4 \cdot 26^y = 39^z$

Por algebrismo, abrimos 26 e 39 com seus fatores:
$2^x \cdot 3^4 \cdot (2 \cdot 13)^y = (3 \cdot 13)^z$

Que é igual a:
$2^x \cdot 3^4 \cdot 2^y \cdot 13^y = 3^z \cdot 13^z$

Juntando as bases:
$2^{(x+y)} \cdot 3^4 \cdot 13^y = 3^z \cdot 13^z$

Devido ao fato da fatoração em primos ser única, comparamos os expoentes dos dois lados dessa igualdade:

$3^4 = 3^z$; $z = 4$

$13^y = 13^z$; $y = z = 4$

O que nos sobra $2^{(x+y)}$, como o lado direito da igualdade não é zero, essa parte da expressão deve ser igual a 1, assim:

$2^{(x+y)} = 2^0 \rightarrow x + y = 0$; sabemos que $y = 4$, teríamos então $x = -4$, entretanto estamos buscando apenas inteiros positivos. Outra possibilidade para essa igualdade ser verdadeira seria $x = y = 0$.

Então não é possível que x, y e z sejam inteiros positivos para que essa igualdade seja verdadeira.

Questão 2.
a. Seja $k > 1$ um inteiro. Mostre que os números $k! + 2, k! + 3, \ldots, k! + k$ são todos compostos.

Supomos $k \geq i \geq 1$ então podemos dizer que $i \mid k!$
$k! = iq$
Por exemplo:
$5! = 5 \times (24)$
$5.4.3.2.1 = 5 . (4.3.2.1)$

Como também $i \mid i$, logo ele divide a soma de k! com i
$i \mid k!+i \rightarrow k!+i = iq'$

Podemos agora dizer que k!+i > i > 1

Logo os números k! + 2, k!+3,…,k!+k serão sempre compostos

b. Refute a seguinte afirmação: existe um inteiro positivo m tal que, dentre quaisquer m inteiros positivos consecutivos, sempre há pelo menos um primo.

Temos agora um inteiro positivo m, aplicado à nossa sequência anterior, somando com 1 para não termos o caso de m=1:

(m+1)! + 2,...,(m+1)! + (m+1)

Assim temos m inteiros consecutivos que são todos compostos.

Questão 3.
Prove ou refute com um contra-exemplo cada umas das afirmações abaixo.

* a. A soma de um número irracional com um número racional é sempre irracional.

Vamos supor a soma de um racional com um irracional nos dê um racional

racional + irracional = racional

Onde
x/y = racional;
k = irracional;
m/n = racional

Fazemos a soma:
x/y + k = m/n

Isolando nosso k:

k = m/n - x/y

Por algebrismo chegamos em:

k = (my-xn)/yn

Temos agora que (my) é uma multiplicação de dois números inteiros, assim como (xn) e (yn). Como temos uma subtração de dois números inteiros (my-xn) que resulta em um inteiro, que também está sendo dividida por um número inteiro (yn). Logo toda a partícula (my-xn)/yn é um número racional. Entretanto estamos igualando a k, que supomos ser um número irracional, isso é uma contradição. Logo não há como a soma de um racional com um irracional resultar em um racional.

* b. A soma de dois números irracionais é sempre irracional.

A soma de dois números irracionais pode nos gerar, tanto racionais quanto irracionais.

($\frac{1}{2}$ + $\sqrt{2}$) é um número irracional
($\frac{1}{2}$ - $\sqrt{2}$) também é um número irracional
Ambos possuem $\sqrt{2}$ que é um número irracional
Quando fazemos a sua soma temos que ($\frac{1}{2}$ + $\sqrt{2}$) + ($\frac{1}{2}$ - $\sqrt{2}$) = 1
Logo nem sempre a soma de dois irracionais é um irracional

Questão 4.
* a. Sejam b1 e b2 inteiros positivos primos entre si. Mostre que d é um divisor de b1b2 sse d = d1d2 onde d1 = mdc(d, b1) e d2 = mdc(d, b2).

Do enunciado temos que mdc(d,b1) = d1, assim d1|d e d1|b1, como d1 divide d, temos d = d1(q).
Como d1 divide b1 que é um número primo, e d2 divide b2 que também é um número primo, então temos que d1 e d2 também são primos,logo mdc(d1, d2) = 1

Temos também que mdc(d,b2) = d2, então d2|d e d2|b2.
Assim d2 divide d = d1(q), então pelo lema da propriedade fundamental dos primos d2 divide q; d2 ≤ q.

Considerando agora que q divide um numero primo, então ele é um primo, provavelmente ele mesmo, então mdc(q, b1) = 1, e q divide d = b1b2
Portanto, novamente pelo lema,temos que q divide b2. Assim q é um divisor comum entre b2 e d, donde q ≤ d2. Logo d2 = q.

* b. Dado um natural n > 0, seja S(n) a soma de todos os divisores naturais de n. Por exemplo, S(2) = 1 + 2 = 3, S(3) = 1 + 3 = 4 e S(6) = 1 + 2 + 3 + 6 = 12. Use o item anterior para mostrar que se b1 e b2 são inteiros positivos primos entre si então S(b1b2) = S(b1)S(b2).

b1: a(0) = 1, a(1), a(2), . . . , a(m)
b2: c(0) = 1, c(1), c(2), . . . , c(n)

Mas S(b1)S(b2) = (1 + a(1) + a(2) + · · · + a(m))(1 + c(1) + c(2) + · · · + c(n)).
Logo S(b1)S(b2) é a soma dos números da forma a(i)c(j) onde 0 ≤ i ≤ m e 0 ≤ j ≤ n que, como vimos acima, são exatamente os divisores de b1b2.

Portanto S(b1)S(b2) = S(b1b2).

Questão 5.
Nesta questão vamos determinar relações entre as fatorações em primos de inteiros positivos a e b com as fatorações em primos de mdc(a, b) e mmc(a, b).

* b. Dadas as fatorações em primos de dois números inteiros positivos a e b, descreva um algoritmo para determinar mdc(a, b) e mmc(a, b).

mdc(a,b):
Passo 1: Supomos a>b ou b>a
Passo 2: Dividimos a,b, separadamente por n, começando por n = 2, se não der resultados inteiros, faça n+1 até n = b, caso b>a ou n=a caso a>b.
Passo 3: Verifique que n nunca vai dividir a e b ao mesmo tempo. Logo o mdc = 1

mmc(a,b):
Passo 1: como a e b são primos, tentamos dividi-los por outros números primos, verificamos que a vai dividir a e b dividir b
Passo 2: multiplicamos o números encontrados

```
a , b |   a
1 , b |   b
1 , 1 |-----------------
          ab
```

Assim mmc(a,b) = ab

* c. Use o algoritmo do item b para provar que se mdc(a, n) = mdc(b, n) = 1 então mdc(ab, n) = 1.

Questão 8.
Bem-vindo ao M-mundo, onde os únicos números que existem são inteiros positivos que deixam resto 1 quando são divididos por 4. Em outras palavras, os M-números são {1, 5, 9, 13, 17, . . .}

* a. “No M-mundo nós não podemos somar dois números”: mostre que a soma de dois M-números nunca é um M-número

Como os M-números sempre restam 1 quando divididos por 4, podemos escrever que M= 4k+1, sendo k um inteiro positivo, M seria um múltiplo de 4 se não fosse o fator “+1”.

Como M é a nossa definição de M-número, podemos fazer M1+M2, que nos resulta (4k1 + 1) + (4k2+1) = 4k1+4k2+2, por mais que tenhamos 2 múltiplos de 4, quando dividirmos o número inteiro, vamos achar resto 2 agora, diferente do M-número que precisamos achar resto 1.

Sendo assim, pela própria definição de M-número, quando dois M-números são somados, eles não resultam em um M-número.

.

* b. “No M-mundo nós podemos multiplicar dois números”: mostre que o produto de dois M-números é sempre um M-número.

Com a definição do exercício anterior podemos fazer:
M1(M2) = (4k1+1)(4k2+1) = 16k1k2 + 4k1 + 4k2 + 1

Temos agora 3 múltiplos de 4 compondo nosso resultado, mas agora, diferente da soma, a multiplicação de dois M-números sempre terá resto 1 quando dividido por 4.

Dados M-números m e n, dizemos que m é um M-divisor de n se existe um M-número k tal que n = mk. Também dizemos que um M-número n é um M-primo se n =/= 1 e os únicos M-divisores de n são 1 e o próprio n.

* c. Ache os seis primeiros M-primos.

Continuando a sequência de M-números, nós temos:
{1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61...}
Testando os valores da sequência, chegamos que os 6 primeiros M-primos são
{5, 9,13,17, 21,29}
Pois esses números não são múltiplos de nenhum outro no M-mundo, sendo assim, somente divisíveis por 1 e por eles mesmos no M-mundo

* d. Prove ou refute a propriedade fundamental dos M-primos: Sejam a, b, p M-números, com p M-primo. Se p é M-divisor de ab, então p é M-divisor de a ou p é M-divisor de b.

Temos que p|ab → p|a ou p|b, sendo p um M-primo

ab = p(q) → a= pq’ ou b= pq’’

isolando p, temos que ab/q

Substituindo nas expressões

a = ab(q’)/q → 1 = b(q’)/q → q = b(q’)

b = ab(q’’)/q → 1 = a(q’’)/q → q = a(q’’)

Sendo assim ab é sempre um múltiplo de a ou múltiplo de b, o que garante que p vá dividir a partícula restante deste produto

* g. Ache um M-número n que tem duas fatorações diferentes em M-primos.

No mundo real, temos que 9 pode ser fatorado em 3*3, e o 21 por 3*7, e como são múltiplos de 3, podemos procurar uma igualdade do tipo fazer que 9x=21y, dessa expressão tiramos y=21 e x = 49

Temos agora 9(49) = 21(21)
441 = 441

Nosso M-número então é 441, visto que pode ser fatorado como 9*49 ou 21*21, sendo todos esses m-primos.

Questão 9.
Dado um inteiro positivo n, seja d(n) o número de divisores positivos de n. Dizemos que um inteiro positivo n é altamente composto se d(m) < d(n) é verdade para todo inteiro positivo m < n. Por exemplo, como d(1) = 1, d(2) = 2 = d(3) e d(4) = 3, temos que 1, 2 e 4 são altamente compostos mas 3 não é.

* a. Implemente em Python uma função que, tendo como entrada um inteiro positivo n, imprime na tela todos os números altamente compostos menores ou iguais a n. (Nota: submeta sua solução adicionando o arquivo-fonte .py à sua pasta no Drive.)

* b. Usando o seu programa do item anterior, determine quantos números inteiros positivos altamente compostos existem até (incluindo, se for o caso) 5000.

O número 5000 possui 2218 números alimentos compostos até ele.