Números Inteiros e Criptografia, PLE 2020

Lista de Exercícios 5

Submeta as soluções das questões marcadas com *
até 2 de outubro às 18:00 salvando um arquivo na sua pasta no Google Drive†

Justifique todas as questões.

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

Questão 2.

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

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.

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

c. O número $\sqrt{2} + \sqrt{3}$ é racional

d. O produto de dois números racionais é sempre irracional.

e. O produto de dois números irracionais é sempre irracional.

Questão 4.

*** a.** Sejam b_1 e b_2 inteiros positivos primos entre si. Mostre que d é um divisor de $b_1 b_2$ sse $d = d_1 d_2$ onde $d_1 = \mathrm{mdc}(d, b_1)$ e $d_2 = \mathrm{mdc}(d, b_2)$.

*** 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 b_1 e b_2 são inteiros positivos primos entre si então $S(b_1 b_2) = S(b_1) S(b_2)$.

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

†Link recebido por email em 1/9/2020 ou 17/9/2020. A pasta tem um nome similar a `Cripto - Submissões e Feedback - <seu nome>`; em caso de qualquer dúvida entre em contato com os professores.

a. Determine $\mathrm{mdc}(2^{35}\cdot 5^{47}\cdot 101^3, 2^{23}\cdot 5^{50}\cdot 43^2)$ e $\mathrm{mmc}(2^{35}\cdot 5^{47}\cdot 101^3, 2^{23}\cdot 5^{50}\cdot 43^2)$.

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

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

d. Ainda usando o algoritmo do item b, prove que $a \cdot b = \mathrm{mdc}(a, b) \cdot \mathrm{mmc}(a, b)$.

Questão 6. Seja n um inteiro positivo. Determine todos os fatores primos de $n!$.

Questão 7. Em aula, usamos o teorema da fatoração única e o fato que para todos a, b inteiros positivos temos $2a \neq 2b + 1$ para provar que $\sqrt{p}$ é irracional (para todos m, n inteiros temos $m^2 \neq n^2 p$). De qual fato precisamos para provar que $\sqrt[3]{5 \cdot 7}$ é irracional usando a mesma estratégia de prova?

Questão 8. Bem-vindo ao $\mathbb{M}$-mundo, onde os únicos números que existem são inteiros positivos que deixam resto 1 quando são divididos por 4. Em outras palavras, os $\mathbb{M}$-*números* são

$$\{1, 5, 9, 13, 17, \ldots\}$$

*** a.** "No $\mathbb{M}$-mundo nós não podemos somar dois números": mostre que a soma de dois $\mathbb{M}$-números nunca é um $\mathbb{M}$-número.

*** b.** "No $\mathbb{M}$-mundo nós podemos multiplicar dois números": mostre que o produto de dois $\mathbb{M}$-números é sempre um $\mathbb{M}$-número.

Dados $\mathbb{M}$-números m e n, dizemos que m é um $\mathbb{M}$-*divisor* de n se existe um $\mathbb{M}$-número k tal que $n = mk$. Também dizemos que um $\mathbb{M}$-número n é um $\mathbb{M}$-*primo* se $n \neq 1$ e os únicos $\mathbb{M}$-divisores de n são 1 e o próprio n.

*** c.** Ache os seis primeiros $\mathbb{M}$-primos.

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

e. Prove ou refute: para qualquer $\mathbb{M}$-número $n > 1$, o menor $\mathbb{M}$-número $m > 1$ que divide n é um $\mathbb{M}$-primo.

f. Descreva um algoritmo que, dado como entrada um $\mathbb{M}$-número $n > 1$, retorna uma fatoração completa de n em fatores $\mathbb{M}$-primos.

*** g.** Ache um $\mathbb{M}$-número n que tem duas fatorações *diferentes* em $\mathbb{M}$-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.