Números Inteiros & Criptografia 2022.2[†]

Lista de Exercícios 2[‡]

Entregar as soluções das questões assinaladas com *
até **3/11 às 21:00**.

A entrega é feita digitalmente pelo Google Drive, na pasta que você recebeu (ou receberá) por email.

Você pode escrever suas soluções manualmente e escanear as folhas de resposta, ou escrever as respostas usando algum editor de texto. Atenção! Você deve garantir que as soluções estejam <u>bem legíveis</u>!

***Questão 1.** Determine se existem naturais $x, y, z > 0$ que satisfaçam a equação $3^x \cdot 5^y \cdot 55^2 = 495^z$.

***Questão 2.** Sejam $n > m$ inteiros positivos. Mostre que se o resto da divisão de n por m é r então o resto da divisão de $2^n - 1$ por $2^m - 1$ é $2^r - 1$. Você pode usar o seguinte fato: em uma progressão geométrica onde o termo inicial a_0, a razão x e a quantidade k de termos são números naturais, a *soma* da progressão é o seguinte número, <u>também natural</u>:

$$S = \frac{a_0 \cdot (x^k - 1)}{x - 1}.$$

Dica: provar que o resto da divisão $2^n - 1$ por $2^m - 1$ é $2^r - 1$ significa provar que existe um *quociente* <u>natural</u> que, junto com o resto proposto, satisfaz certas propriedades em relação ao dividendo e ao divisor.

Questão 3. Em um futuro distante, o presidente do Brasil é um excêntrico que decide mudar o sistema monetário. Por questões de numerologia, no novo sistema há apenas dois valores de moedas: a moeda de 2022 "dinheiro$" e a de 3102 "dinheiro$". Apenas o pagamento em dinheiro "vivo" (com possível troco) é permitido (ou seja, não há cartão, "pix" nem nada similar).

*** a.** Neste futuro distante, Fulano (que tem todo o dinheiro do mundo) vai à padaria comprar uma coxinha que custa 18 "dinheiro$". Mostre que Fulano consegue comprar sua coxinha, assumindo que Fulano e a padaria tenham acesso a todas as moedas de que precisarem.

[†] Em qualquer solução de exercício, você pode usar tudo o que foi visto em sala ou os enunciados de outros exercícios de qualquer lista, desde que cite claramente o resultado que está usando e desde que você não crie dependências circulares entre os exercícios! Se você citar um exercício da lista atual que não resolveu, ganhará apenas alguma pontuação parcial.

[‡] Publicada em 17/10; atualizada em 18/10 (nova data e horário para entrega)

*** b.** Mostre que é impossível Fulano comprar uma casa que custe <u>exatamente</u> 77777777 "dinheiro$", mesmo que Fulano e o vendedor tenham acesso a qualquer quantidade de moedas de "dinheiro$" que quiserem.

Questão 4.

a. Seja $k \geq 2$ um natural. Mostre que todos os números $k!+2, k!+3, \ldots, k!+k$ são compostos.

b. Refute a seguinte conjectura sobre a "densidade" dos números primos:

"existe um natural m tal que, dentre quaisquer m naturais consecutivos, sempre há pelo menos um primo".

Questão 5. Seja $n \in \mathbb{N}$ com $n > 0$. Prove que os primos que dividem $n!$ são exatamente os primos menores ou iguais a n.

Questão 6. Sejam $a, b \geq 2$ números naturais. Ao longo desta questão, suponha que as fatorações em primos de a e b são

$$a = \prod_{i=0}^{k-1} p_i^{e_i} \qquad e \qquad b = \prod_{j=0}^{\ell-1} q_j^{f_j}.$$

*** a.** Em termos dessas fatorações, como podemos determinar se a é um divisor de b ou não? Em outras palavras, complete e prove a seguinte frase:

"$a \mid b$ sse $\ldots$"

onde em "$\ldots$" você deve apenas falar sobre as fatorações em primos de a e b.

*** b.** Suponha que $a \mid b$ e que $\frac{b}{a} \geq 2$. Qual é a fatoração em primos de $\frac{b}{a}$?

*** c.** Qual é a fatoração em primos de $\mathrm{mdc}(a, b)$?

*** d.** Qual é a fatoração em primos de a^2?

*** e.** Dizemos que um número real x é *racional* se existem inteiros y, z, com $z \neq 0$, tais que $y = x \cdot z$, ou em outras palavras, $x = \frac{y}{z}$. Prove o seguinte teorema.

Teorema. *Para todo <u>natural</u> n, temos:*
$\sqrt{n}$ é um número racional sse $\sqrt{n}$ é um número natural.

Dica para uma das direções: Se $\sqrt{n} > 0$ é racional, então $\sqrt{n} = \frac{y}{z}$ para algum par de naturais não nulos y, z. Logo $n = \frac{y^2}{z^2}$. Pelo item (d), o que se sabe sobre as fatorações em primos de y^2 e z^2? Pelo item (b), o que isso implica sobre a fatoração em primos de n?

*** f.** Prove que $\sqrt{2}$ não é um número racional. Você pode usar os seguintes fatos: $\sqrt{2}$ é um número real e, para quaisquer reais $x, y > 0$, se $x > y$ então $x^2 > y^2$.