Números Inteiros e Criptografia, 2021.1

Lista de Exercícios 4[†]

Submeta as soluções das questões marcadas com * salvando um arquivo na sua pasta no Google Drive[‡]

Data limite para entrega: **4 de outubro** às 18:00.

Em qualquer questão, você pode usar tudo que foi visto em aula (a não ser que a questão proíba isso) ou qualquer outro exercício das listas, desde que seja claro na sua referência do resultado que está usando, e desde que não crie dependências circulares.

***Questão 1.** Prove que a equação $x^{41} + 81x + 41y^{15} = 197$ não possui soluções com $x, y \in \mathbb{Z}$. (*Dica*: Suponha, para uma prova por contradição, que a equação tenha uma solução com x, y inteiros. Encontre um módulo p primo conveniente e reduza ambos os lados da equação (mod p), encontrando uma situação impossível.)

Questão 2.

*** a.** Sejam $n, k \in \mathbb{N}$ e $x, y \in \mathbb{Z}$. Prove que se

$$x \equiv y \pmod{n \cdot k}$$

então

$$x \equiv y \pmod{n} \qquad \text{e} \qquad x \equiv y \pmod{k}$$

(*Dica*: Lembre-se de que a definição de $x \equiv y \pmod{z}$ fala sobre *divisibilidade*.)

*** b.** Mostre que a recíproca do item **a** não é sempre verdadeira.

*** c.** Sejam $n, k \in \mathbb{N}$ **coprimos** e $x, y \in \mathbb{Z}$. Prove que neste caso vale a recíproca do item **a**, isto é, prove que se

$$x \equiv y \pmod{n} \qquad \text{e} \qquad x \equiv y \pmod{k}$$

então

$$x \equiv y \pmod{n \cdot k}$$

Questão 3 (Critérios de divisibilidade)**.** *Lembrete.* Dada um natural $b > 0$, dizemos que um natural n tem *expansão* $(d_k d_{k-1} \cdots d_2 d_1 d_0)_b$ na base b se cada

[†]Publicada em 24/9.

[‡]Link recebido por email em 5/8/2021. A pasta tem um nome similar a `<seu nome> - Cripto 2021.1 - Submissões e Feedback`; em caso de qualquer dúvida entre em contato com o professor.

d_i é um natural menor do que b e

$$\begin{aligned} n &= (d_k \cdot b^k) + (d_{k-1} \cdot b^{k-1}) + \cdots + (d_2 \cdot b^2) + (d_1 \cdot b^1) + (d_0 \cdot b^0) \\ &= \sum_{i=0}^{k} d_i \cdot b^i \end{aligned}$$

*** a.** Sejam $a, b, n \in \mathbb{N}$ tais que $a > 0$, $b \equiv 1 \pmod{a}$ e n tem expansão $(d_k d_{k-1} \cdots d_2 d_1 d_0)_b$ na base b.

Mostre que n é divisível por a se, e somente se, $\left(\sum_{i=0}^{k} d_i\right)$ é divisível por a.

*** b.** Use o item **a** para mostrar que $(123412341)_8$ é divisível por 7.

*** c.** Prove que um natural é divisível por 5 se, e somente se, ao ser escrito em base 10, seu último algarismo (i.e., o seu algarismo da casa das unidades) é divisível por 5 (ou seja, é 0 ou 5).