# Números Inteiros e Criptografia 2026-2

Hugo Nobrega

Lista de Exercícios 4

Entregue todas as questões marcadas com * até
**1º de dezembro às 18:00**

A entrega é pelo Google Drive, na pasta que você recebeu por e-mail. As listas podem ser entregues por grupos de até 4 alunos. Apenas 1 aluno do grupo deve submeter as respostas. Os nomes e DREs dos componentes do grupo devem estar indicados claramente.

Lembre-se que você **pode** usar uma questão na solução de outra, mesmo que não tenha resolvido a questão que está usando, desde que você não crie "dependências circulares".

**Questão 1.**

**Definição.** Sejam $x$ inteiro e $n$ natural positivo. Chamamos de *forma reduzida* de $x$ mod $n$ o menor natural $y$ tal que $x \equiv y \mod n$.

Calcule a forma reduzida de...

**a.** $66^{50} \mod 29$

*** b.** $2^{123456789} \mod 71$

**c.** $6^{100} \mod 31104$

*** d.** $9^{123456789} \mod 24$

**e.** $854^{1234} \mod 864$

***Questão 2.** Prove que a equação $x^{41} + 81x + 123y^{15} = 197$ 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 *módulo* $p$, chegando a uma situação impossível.)

**Questão 3.** Sejam $x$ e $n$ naturais com $x, n \geqslant 2$. Prove que:

existe natural $k$ tal $x^k \equiv 0 \mod n$
se, e somente se,
todo primo que divide $n$ também dividir $x$.

**Questão 4** (Critérios de divisibilidade)**.** *Lembrete de Fundamentos de Sistemas de Computação.* Dado um natural $b > 1$, dizemos que um natural $n$ tem *representação* $(d_k d_{k-1} \cdots d_2 d_1 d_0)_b$ *na base* $b$ se:

- cada $d_i$ é um natural menor do que $b$ e
- $n = \sum_{i=0}^{k} d_i \cdot b^i = (d_k \cdot b^k) + (d_{k-1} \cdot b^{k-1}) + \cdots + (d_2 \cdot b^2) + (d_1 \cdot b^1) + (d_0 \cdot b^0)$.

Os números $d_i$ são chamados de *algarismos* da representação de $n$ na base $b$.

Por exemplo, o número que conhecemos como 13 na base decimal tem representação $(111)_3$ na base 3 e representação $(31)_4$ na base 4.

Para o restante dessa questão, sejam $x, b, n \in \mathbb{N}$ tais que $b > 1$ e $n$ tem representação $(d_k d_{k-1} \cdots d_2 d_1 d_0)_b$ na base $b$. Sempre que mencionarmos um número sem especificar a base, estamos usando a representação decimal padrão.

*Dica.* Lembre-se que "$y \mid z$" é equivalente a "$z \equiv 0 \mod y$".

**a.** Mostre que se $x \mid b$, então:

$$x \mid n \quad \text{sse} \quad x \mid d_0.$$

**b.** Use o item (a) para concluir que um natural é par sse sua representação decimal termina em $0, 2, 4, 6$ ou 8, e que um natural é múltiplo de 5 sse sua representação decimal termina em 0 ou 5.

*** c** (Generalização do item (a))**.** Seja $j \in \mathbb{N}$. Mostre que se $x \mid b^j$, então $x \mid n$ sse $x$ divide o número formado apenas pelos $j$ últimos algarismos (à direita) da representação de $n$ na base $b$, ou seja:

$$x \mid n \quad \text{sse} \quad x \mid \left( \sum_{i=0}^{j-1} d_i \cdot b^i \right)$$

**d.** Use o item (c) para concluir que um natural é múltiplo de 4, 25 ou 50 sse o número formado pelos dois últimos algarismos de sua representação decimal é múltiplo de 4, 25 ou 50 (respectivamente).

**e.** Mostre que se $b \equiv 1 \mod x$, então $x \mid n$ sse $x$ divide a soma dos algarismos da representação de $n$ na base $b$, ou seja:

$$x \mid n \quad \text{sse} \quad x \mid \left( \sum_{i=0}^{k} d_i \right)$$

**f.** Use o item (e) para concluir que um natural é múltiplo de 3 ou 9 sse a soma dos algarismos de sua representação decimal é múltipla de 3 ou 9 (respectivamente).

*** g.** Seja $n = 3316273978515968$. Sabendo que $n = (1111112)_{386}$, responda: 7 divide $n$?

*** h.** Mostre que se $b \equiv -1 \mod x$, então:

$$x \mid n \quad \text{sse} \quad x \mid \left( \sum_{i=0}^{k} (-1)^i d_i \right)$$

**i.** Use o item (h) para mostrar que 11 divide qualquer natural cuja representação decimal tem três algarismos, sendo o do meio igual à soma dos dois das pontas.

*** j.** Use o item (h) para responder: $(4E2F62FF2)_{16}$ é múltiplo de 17? *Lembrete*: Na base 16 ("hexadecimal") usamos as letras de $A$ a $F$ para representar os "algarismos" de 10 a 15, respectivamente.

**Questão 5** (Teorema Chinês dos Restos). Sejam $\ell_1$ e $\ell_2$ naturais coprimos e $n = \ell_1 \cdot \ell_2$. Sejam também

- $\ell_1'$ o inverso de $\ell_1$ em módulo $\ell_2$
- $\ell_2'$ o inverso de $\ell_2$ em módulo $\ell_1$.

Sejam $a$ e $b$ inteiros e considere o sistema

$$\begin{cases} x \equiv a \mod \ell_1 \\ x \equiv b \mod \ell_2 \end{cases}$$

*** a** ("Existência de solução $\mod n$"). Prove que se

$$x \equiv (a \cdot \ell_2 \cdot \ell_2') + (b \cdot \ell_1 \cdot \ell_1') \pmod{n},$$

então $x$ é solução do sistema.

*** b** ("Unicidade da solução $\mod n$"). Prove que se $x$ e $y$ são soluções do sistema, então

$$x \equiv y \mod n.$$