Números Inteiros & Criptografia 2022.2[†]

Lista de Exercícios 4[‡]

Entregar as soluções das questões assinaladas com *
até **14/1 às 23:59**.

A entrega é feita digitalmente pelo Google Drive, na pasta que você recebeu 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 bem legíveis!

Questão 1. 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 (Critérios de divisibilidade)**.** *Lembrete de Fundamentos da Computação Digital.* Dado um natural $b > 1$, 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 d_i é um natural menor do que b e
- $$\begin{aligned} n &= (d_k \cdot b^k) + (d_{k-1} \cdot b^{k-1}) + \cdots + (d_2 \cdot b^2) + (d_1 \cdot b^1) + (d_0 \cdot b^0) \\ &= \sum_{i=0}^{k} d_i \cdot b^i \end{aligned}$$

Para o restante dessa questão, sejam $x, b, n \in \mathbb{N}$ tais que $b > 1$ e n tem expansão $(d_k d_{k-1} \cdots d_2 d_1 d_0)_b$ na base b. *Dica.* Lembre-se que "$y \mid z$" é equivalente a "$z \equiv 0 \mod y$".

[†] 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 2/1

*** 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 expansão decimal termina em $0, 2, 4, 6$ ou 8 e que um natural é múltiplo de 5 sse sua expansão decimal termina em 0 ou 5.

c (Generalização do item (a))**.** Seja $j \in \mathbb{N}$. Mostre que se $x \mid b^j$, então:

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

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 expansão decimal é múltiplo de 4, 25 ou 50 (respectivamente).

e. Mostre que se $b \equiv 1 \mod x$, então:

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

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

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

*** 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 expansão decimal tem 3 algarismos, sendo o do meio igual à soma dos dois das pontas.

*** j.** Use o item (h) para responder: $(4E2F62FF2)_{16}$ é múltiplo de $(11)_{16}$?

Questão 3.

*** 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 4 (Algoritmo "square-and-multiply")**.** Como vimos, há diversos *truques* para calcular potências em aritmética modular, cada um aplicável em uma situação diferente. Vamos agora desenvolver uma técnica rápida (para um computador) que funciona em geral, e é de fato implementada, por exemplo, na função `pow` do Python.

Sejam $a, e, n \in \mathbb{N}$, com $n > 0$, e suponha que você queira calcular a forma reduzida de a^e módulo n, i.e., encontrar o menor natural r tal que $a^e \equiv r \pmod{n}$. Sabendo que a expansão binária de e é $(d_k d_{k-1} d_{k-2} \cdots d_1 d_0)_2$, temos

$$\begin{aligned} a^e &\equiv a^{\left(\sum_{i=0}^{k} d_i \cdot 2^i\right)} \\ &\equiv \prod_{i=0}^{k} a^{d_i \cdot 2^i} \\ &\equiv \prod_{i=0}^{k} (a^{(2^i)})^{d_i} \pmod{n}. \end{aligned} \tag{$*$}$$

Portanto, o problema é calcular a forma reduzida do produto $(*)$ módulo n.

*** a.** Descreva um algoritmo para encontrar a forma reduzida de a^e módulo n, usando apenas as seguintes operações auxiliares (trate essas operaçõs como "caixas pretas", i.e., você <u>não precisa</u> dizer como essas operações podem ser implementadas):

1. encontrar a representação binária de um natural qualquer;
2. encontrar a forma reduzida de um natural qualquer módulo n;
3. elevar ao quadrado um natural menor do que n;
4. multiplicar dois naturais menores do que n.

Você deve argumentar por que o seu algoritmo termina e está correto.

Dica: Você vai calcular o produto $(*)$ passo-a-passo; na hora de calcular a forma reduzida de $a^{(2^{i+1})}$ módulo n, use o fato de que você calculou a forma reduzida de $a^{(2^i)}$ módulo n no passo anterior! Feito isso, o expoente d_{i+1} (que é 0 ou 1) indica se você deve multiplicar o número resultante com o seu *produto parcial acumulado* encontrado até agora ou não.

*** b.** Utilize o seu algoritmo para calcular a forma reduzida de 13^{75} módulo 9; mostre o passo-a-passo da execução.

Dica: $75 = (1001011)_2$.