Números Inteiros e Criptografia, PLE 2020

Lista de Exercícios 8

Submeta as soluções das questões marcadas com *
até 26 de outubro às 18:00 salvando um arquivo na sua pasta no Google Drive†

Justifique todas as questões.

Questão 1. Dados $a \in \mathbb{Z}$ e $n \in \mathbb{N}$ com $n > 0$, chamamos de *forma reduzida de* $a \pmod{n}$ o único $b \in \{0, 1, 2, \ldots, n-1\}$ que satisfaz $b \equiv a \pmod{n}$.

Calcule a forma reduzida de cada item abaixo:

a. $(-99999!)^{99999!} \pmod{1}$

b. $2351 \pmod{2}$

* **c.** $-(1234567890^{99999!}) \pmod{2}$

d. $50121 \pmod{13}$

e. $321671 \pmod{14}$

f. $5^{20} \pmod{7}$

g. $7^{1001} \pmod{11}$

* **h.** $2^{130} \pmod{263}$ (Use o fato que $2^{131} \equiv 1 \pmod{263}$)

i. $26^{221} \pmod{19}$

Questão 2. Prove que, para todos $a, b, n \in \mathbb{N}$ com $n > 0$, temos:

b é a forma reduzida de $a \pmod{n}$
sse
b é o resto da divisão de a por n.

Questão 3. Determine o resto da divisão de

a. $3^{(2^{1024})}$ por 31 (Use o fato que $3^{30} \equiv 1 \pmod{31}$).

b. $3^{19!}$ por 307 (Use o fato que $3^{34} \equiv 1 \pmod{307}$).

* **c.** $39^{50!}$ por 2251 (Use o fato que $39^{1125} \equiv 1 \pmod{2251}$).

d. 2^{78654} por 137 (Use o fato que $2^{68} \equiv 1 \pmod{136}$).

†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.

e. 34^{642} por 12.

f. $3^{(1034^2)}$ por 1033 (Use o fato que $3^{516} \equiv 1 \pmod{1033}$).

*** g.** $2^{987657} + 5^{15}$ por 65. (*Dica*: lembre-se que $2^6 \equiv 64 \equiv -1 \pmod{65}$.)

h. $3^{(5^{2014})}$ por 29 (Use o fato que $3^{28} \equiv 1 \pmod{29}$).

i. $2^{250!} + 5^{450!}$ por 129. (*Dica*: $2^7 \equiv 128 \equiv -1 \pmod{129}$ e $5^3 \equiv 125 \equiv -4 \equiv -(2^2) \pmod{129}$, portanto para qualquer inteiro $k > 0$ temos $5^{3k} \equiv [-(2^2)]^k \equiv (-1)^k \cdot 2^{2k} \pmod{129}$.)

j. $1000!$ por 3^{300}.

***Questão 4.** Prove **por indução** que, para todo inteiro $n \geq 1$, temos $n^3 \equiv n \pmod{6}$.

Questão 5. Usando arimética modular, determine um inteiro x tal que

$$12435x + 798y = 3$$

para algum y inteiro.

***Questão 6.** São oito horas da manhã. Que horas serão daqui a $243^{213!}$ horas?

Questão 7. Determine x tal que $\overline{7085}x + \overline{50000!} = \overline{23}$ em $\mathbb{Z}_{8856}$.

Questão 8. Sabe-se que $\overline{3}^{(2^7)} = \overline{256}$ em $\mathbb{Z}_{257}$.

a. Encontre algum inteiro $k > 0$ tal que $3^k \equiv 1 \pmod{257}$.

b. Calcule o resto da divisão de 3^{2307} por 257.

***Questão 9.** Seja $p > 1200$ um fator primo de $1200! + 1$. $\overline{1200}$ tem inverso em $\mathbb{Z}_p$? Se existir, qual é o seu inverso em $\mathbb{Z}_p$?

Questão 10. Determine:

a. o inverso de $\overline{71}$ em $\mathbb{Z}_{8635}$, se existir.

b. o resto da divisão de $2^{(2^{21})}$ por 71 (Use o fato que $2^{35} \equiv 1 \pmod{71}$).

Questão 11. Determine:

*** a.** o inverso de 137 módulo 2887;

*** b.** x tal que $137x \equiv 544 \pmod{2887}$, usando o item anterior.

Questão 12. Prove, por indução em n, que se $n \geq 2$ então $2^{(3^{n-2})} \equiv 3^{n-1} - 1 \pmod{3^n}$.

Questão 13.

*** a.** Prove que para todo inteiro $b > 0$, se b não é divisível por 7 então $b^6 \equiv 1 \pmod{7}$. (*Dica*: prove separadamente para cada $b \in \{1, 2, 3, 4, 5, 6\}$ e mostre que isso implica o resultado desejado. *Outra dica:* Na verdade, como o expoente 6 é par, mostre que basta provar separadamente para cada $b \in \{1, 2, 3\}$, mostrar que isso implica o resultado desejado para cada $b \in \{4, 5, 6\}$, e daí seguir a primeira dica.)

*** b.** Calcule o resto da divisão de

$$1^{1!} + 2^{2!} + 3^{3!} + 4^{4!} + 5^{5!} + 6^{6!} + 7^{7!} + 8^{8!} + 9^{9!} + 10^{10!}.$$

por 7. (*Dica*: use o item anterior.)

Questão 14. Considere um natural n com seis dígitos a, b, c, d, e, f (i.e., sejam $a, b, c, d, e, f \in \mathbb{N}$ com $0 \leq a, b, c, d, e, f \leq 9$, $a \neq 0$ e $n = a \cdot 10^5 + b \cdot 10^4 + c \cdot 10^3 + d \cdot 10^2 + e \cdot 10^1 + f \cdot 10^0$.)

Mostre que n é divisível por 33, se $(a \cdot 10 + b) + (c \cdot 10 + d) + (e \cdot 10 + f)$ é divisível por 33. Por exemplo, $n = 653202$ é divisível por 33, pois $65 + 32 + 2$ é divisível por 33.

Questão 15. Considere as relações R_1 e R_2 abaixo, definidas no conjunto $\mathbb{Z}$ dos números inteiros. Determine se são reflexivas, simétricas e/ou transitivas. Alguma das duas relações é de equivalência?

*** a.** $a\ R_1\ b$ quando $\mathrm{mdc}(a, b) = 1$.

*** b.** Fixe $n > 0$ inteiro. Então $a\ R_2\ b$ quando $\mathrm{mdc}(a, n) = \mathrm{mdc}(b, n)$.

Questão 16. Quais os elementos de $\mathbb{Z}_4$ que têm inversos? E de $\mathbb{Z}_{11}$? E de $\mathbb{Z}_{15}$? Calcule os inversos desses elementos em cada caso.

Questão 17. Usando o conceito de inverso multiplicativo, determine uma solução para x em cada uma das seguintes equações, se existir, ou prove que não existe solução:

a. $4x \equiv 3 \pmod 4$.

b. $3x + 2 \equiv 0 \pmod 4$.

c. $2x - 1 \equiv 7 \pmod{15}$

Questão 18. Ache um elemento a de $\mathbb{Z}_{34}$ de modo que todo elemento invertível de $\mathbb{Z}_{34}$ seja uma potência de a.

Questão 19. O objetivo desta questão (i.e., o que vamos concluir após os itens **a**, **b** e **c** abaixo) é mostrar que nenhum número da forma $4n+3$ pode ser escrito como a soma dos quadrados de dois inteiros.

*** a.** Mostre que o quadrado de qualquer inteiro só pode ser congruente a 0 ou 1 módulo 4.

*** b.** Use o item anterior para mostrar que se x e y são inteiros então $x^2 + y^2$ só pode ser congruente a 0, 1 ou 2 módulo 4.

*** c.** Use o item anterior para mostrar que um inteiro da forma $4n+3$ não pode ser escrito como soma de dois quadrados de inteiros. Este resultado é um caso particular de um teorema comunicado por Fermat em uma carta a Roberval datada de 1640. Fermat também sabia que qualquer primo da forma $4n + 1$ pode ser escrito como soma de dois quadrados de inteiros.