Números Inteiros e Criptografia, 2020.1

Lista de Exercícios 8

Submeta as soluções das questões marcadas com *
até 12 de fevereiro às 18:00 salvando um arquivo na sua pasta no Google Drive

Justifique todas as questões.

***Questão 1.** São oito horas da manhã. Que horas serão daqui a $243^{213!}$ horas?

Questão 2. Mostrando as suas contas, determine o resto da divisão de

* **a.** $3^{(2^{1024})}$ por 31.

b. 2^{78654} por 137.

* **c.** $1000!$ por 3^{300}.

Questão 3. 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 4.

* **a.** Prove que, para todo natural $n \geq 1$, se $p_0, p_1, \ldots, p_{n-1}$ são naturais primos distintos então para todos inteiros x, y temos:

$$x \equiv y \pmod{p_0 \cdot p_1 \cdots p_{n-1}}$$
$$\text{sse}$$
$$\text{para todo } i < n \text{ temos } x \equiv y \pmod{p_i}$$

(*Dica*: indução! Lembre-se também de que a definição da relação $\equiv \pmod{m}$ tem algo a ver com *divisibilidade* por m.)

* **b.** Mostre que a hipótese de que os primos $p_0, \ldots p_{n-1}$ são *distintos* é importante: encontre algum contraexemplo para a seguinte afirmação falsa:

"Para todo natural $n \geq 1$, se $p_0, p_1, \ldots, p_{n-1}$ são naturais primos então para todos inteiros x, y temos:

$$x \equiv y \pmod{p_0 \cdot p_1 \cdots p_{n-1}}$$
$$\text{sse}$$
$$\text{para todo } i < n \text{ temos } x \equiv y \pmod{p_i}\text{"}$$

* **c.** Uma das direções do "sse" na afirmação falsa do item **b** é válida. Diga qual das direções, e prove-a.

d. Ainda sobre a direção válida da afirmação falsa do item **b**, vamos generalizá-la ainda mais: prove que ela continua sendo válida mesmo se retirarmos a hipótese de que $p_0, p_1, \ldots, p_{n-1}$ são *primos*.

e. Mostre que, para todo natural $n \geq 0$, $n(n+1)(2n+1)$ é divisível por 6 usando o Teorema de Fermat e o Teorema do item **a**.

Questão 5. Sejam $a, b, c, p \in \mathbb{N}$, com p primo e $\text{mdc}(a, p) = 1$. Prove que se $b \equiv c \pmod{(p-1)}$, então $a^b \equiv a^c \pmod{p}$.

***Questão 6.** Sejam p um número primo e a um inteiro que não é divisível por p. Mostre que o inverso de $\overline{a}$ em $\mathbb{Z}_p$ é $\overline{a}^{p-2}$.

Questão 7. Prove que a equação $x^{41} + 81x + 41y^{15} = 197$ não possui soluções inteiras. (*Dica*: Suponha, para uma prova por contradição, que a equação tenha uma solução com x, y inteiros. Encontre um módulo p conveniente e reduza ambos os lados da equação $\pmod{p}$, encontrando uma situação impossível.)

Questão 8. Determine:

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

* **b.** x tal que $137x \equiv 544 \pmod{2887}$.

***Questão 9.** Sejam $n \in \mathbb{N}$ e $p > n$ um fator primo de $n! + 1$. Existe um inverso de $\overline{n}$ em $\mathbb{Z}_p$? Se existir, qual é?

Questão 10.

a. Prove que, se os testes de Fermat com bases b e c são inconclusivos para uma certa entrada n, então o mesmo é verdade para a base bc e entrada n.

b. Conclua que se o teste de Fermat para uma certa entrada n é conclusivo para *alguma* base, então ele necessariamente é conclusivo para alguma base prima.

c. Mostre que não sempre é verdade que, se os testes de Fermat com bases b e c são inconclusivos para uma certa entrada n, então o mesmo é verdade para a base $b + c$ e entrada n.

Questão 11. Estes são todos os primos até 317:

```
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59,
61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127,
131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193,
197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269,
271, 277, 281, 283, 293, 307, 311, 313, 317
```

* **a.** Usando esta lista, escreva uma função em Python que receba como entradas naturais `limite` e `base`, com `limite` $\leq 10^5$ e `base` ≥ 2, e retorne uma lista contendo exatamente os números entre 2 e `limite` (incluindo `limite`, se for o caso) que são pseudoprimos de Fermat para a `base` dada.

Você não precisa provar formalmente a terminação e corretude do seu programa, mas inclua uma explicação informal de por que o seu programa funciona.

* **b.** Usando sua função, responda: quantos pseudoprimos de Fermat para base 2 existem entre 2 e 10^5? E para a base 7 entre 2 e 10^5?