Números Inteiros e Criptografia, PLE 2020

Lista de Exercícios 9

Submeta as soluções das questões marcadas com *****
até 3 de novembro às 18:00 salvando um arquivo na sua pasta no Google Drive[†]

Justifique todas as questões.

Questão 1. Use o Pequeno Teorema de Fermat para determinar:

*** a.** o resto de $10^{10^{100}}$ dividido por 7.

b. o resto de 37^{100} dividido por 17.

c. se 6497 é ou não é primo, dado que $500^{3248} \equiv 2849 \mod 6497$.

Questão 2.

a. Sejam $a \neq 0$ um inteiro e p um número primo. Determine duas soluções inteiras para x (não congruentes módulo p) tal que $x^2 \equiv a^2 \mod p$.

b. Determine todos os inteiros x e y tais que $x^{86} \equiv 6 \mod 29$.

***Questão 3.** Prove que se um n ímpar é um pseudoprimo de Fermat para alguma base, então ele é pseudoprimo de Fermat para um número par de bases.

Questão 4. Prove que para quaisquer naturais n, m, o número $3^{6n} - 2^{6m}$ nunca é primo. (Dica: use o Teorema de Fermat).

Questão 5. Em cada item abaixo, use o Teste de Fermat com a base b indicada e conclua que o número n dado é composto. Você deve fazer as contas *à mão*; só pode contar com ajuda de computador ou calculadora para efetuar adições, multiplicações, subtrações e divisões.

*** a.** $n = 1687, b = 4$

*** b.** $n = 2107, b = 7$

c. $n = 1057, b = 8$

Questão 6. 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
```

[†]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.

*** 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.

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

Questão 7.

*** a.** Sabendo que os únicos números de Carmichael até 10.000 são `561, 1105, 1729, 2465, 2821, 6601 e 8911`, escreva um algoritmo que responda corretamente se um número natural n dado como entrada, com $1 < n \leq 10.000$, é um número primo ou composto. Seu algoritmo **deve** ser baseado no Teste de Fermat e não precisa ser muito eficiente, mas não deve testar se o número é primo apenas pela definição, nem implementar um crivo, nem testar exaustivamente usando a lista de primos dada na Questão 6, etc.

*** b.** Implemente seu algoritmo em Python.

Questão 8.

*** a.** Prove que, para todo natural $n \geq 1$, se $p_1, p_2, \ldots, p_n$ são naturais primos distintos então para todos inteiros x, y temos:

$$x \equiv y \pmod{p_1 \cdot p_2 \cdots p_n}$$
$$\text{sse}$$
$$\text{para todo } i \leq n \text{ temos } x \equiv y \pmod{p_i}$$

(*Dica*: indução.)

*** b.** Mostre que a hipótese de que os primos $p_1, \ldots p_n$ são *distintos* é importante: encontre algum contraexemplo para o falso teorema:

"Para todo natural $n \geq 1$, se $p_1, p_2, \ldots, p_n$ são naturais primos então para todos inteiros x, y temos:

$$x \equiv y \pmod{p_1 \cdot p_2 \cdots p_n}$$
$$\text{sse}$$
$$\text{para todo } i \leq n \text{ temos } x \equiv y \pmod{p_i}$$"

c. Uma das direções do "sse" no falso teorema do item **b** é válida. Diga qual das direções, e prove-a.

d. Ainda sobre a direção válida do falso teorema do item **b**, vamos generalizá-la ainda mais: prove que ela continua sendo válida mesmo se retirarmos a hipótese de que $p_1, \ldots, p_n$ 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 9. Mostre, usando o Teorema de Fermat, que $2^{70} + 3^{70}$ é divisível por 13.

Questão 10. Seja a um número inteiro positivo escrito em base 10. Mostre que os algarismos das unidades de a^5 e a são os mesmos.

Questão 11. Use o Teorema de Fermat para provar que para todo inteiro n, o número $n^3 + (n+1)^3 + (n+2)^3$ é divisível por 9. (*Dica*: expanda as potências, depois junte os termos semelhantes e veja no que isso dá módulo 9.)

Questão 12. Seja p um número primo diferente de 2 e 5. Mostre que p divide um dos números do conjunto: $\{1, 11, 111, 1111, 11111, \ldots\}$. Sugestão: pelo Pequeno Teorema de Fermat, temos que se $p > 5$ então 10^{p-1} deixa resto 1 quando dividido por p. O caso $p = 3$ tem que ser tratado separadamente.

Questão 13. Mostre que a equação $x^{13} + 12x + 13y^6 = 1$ não admite soluções inteiras. Sugestão: Reduza módulo 13 e use Fermat.

Questão 14. Calcule o resto da divisão de:

a. 39501 por 2251;

b. 19394 por 191.

Questão 15. O objetivo desta questão é dar uma demonstração do teorema de Fermat, devida a L. Euler, e que não usa indução. Seja p um primo e $\overline{a}$ um elemento de $U_p = \mathbb{Z}_p \setminus \{\overline{0}\}$ (U_p é o conjunto com todas as classes de $\mathbb{Z}_p$ que tem inverso multiplicativo). Considere o subconjunto $S = \{\overline{a}, \overline{2a}, \overline{3a}, \ldots, \overline{(p-1)a}\}$ de U_p.

*** a.** Mostre que os elementos de S são todos distintos e conclua que $S = U(p)$.

*** b.** Mostre que o produto de todos os elementos de S é igual a $\overline{(p-1)!} = \overline{1} \cdot \overline{2} \cdots \overline{p-1}$.

*** c.** Mas, diretamente pela definição de S, o produto dos elementos de S pode ser escrito de outra forma. Encontre essa forma e prove o teorema de Fermat. (*Dica*: em algum momento você deve precisar argumentar que $\overline{(p-1)!}$ é invertível em $\mathbb{Z}_p$.)

***Questão 16.** Seja 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 $\overline{a}^{p-2}$.