










## Teoria de Números Computacional

---


folha 1

---

1.  Recorde o Pequeno Teorema de Fermat (PTF):  $n$  primo implica  $a^{n-1} \equiv 1 \pmod n$ , se  $(a, n) = 1$ .  
Seja  $n = 2^{512} + 1$ .
  - (a) Considere  $a = 2$ . Verifique se a tese é satisfeita (ou seja, se  $2^{n-1} \equiv 1 \pmod n$ ).
  - (b) Procure outros exemplos de bases que verifiquem a tese do teorema.
  - (c) Mostre, usando o PTF, que o número não é primo.
2.  A conjectura dos primos gémeos afirma que existe uma infinidade de pares de números primos  $p$  e  $p+2$ . Escreva uma função que encontre os primos gémeos inferiores a um certo argumento.
3.  Teste a Conjectura (forte) de Goldbach: todo o natural par maior que 3 pode-se escrever como a soma de dois números primos.
4.  Implemente uma função que tenha como argumento um natural  $n > 2$  e como retorno a lista dos números primos não superiores a  $n$ , fazendo uso do crivo de Eratóstenes.
5.  Implemente uma função que teste a primalidade de um número à custa da divisão por tentativas.
6.  Implemente a função *factorial modular* sem recorrer à recursividade. Use-a para implementar o teste de primalidade de Wilson.
7.  Um primo  $p$  diz-se um *primo de Sophie Germain* se  $2p+1$  também for primo. Implemente uma função que encontre todos primos de Sophie Germain menores que um certo argumento dado.  
Conjectura-se que existam uma infinidade de primos de Sophie Germain.
8.  Um primo  $p$  diz-se *primo de Wieferich* se  $2^{p-1} \equiv 1 \pmod{p^2}$ . Encontre o menor primo de Wieferich. Escreva uma função que encontre todos primos de Wieferich menores que um certo argumento dado.  
Uma conjectura afirma que  $2^{p-1} \equiv 1 \pmod{p^2}$  admite uma infinidade de soluções  $p$ , para todo o  $a$ .
9.  Um primo  $p$  diz-se *primo de Wolstenholme* se  $\binom{2p-1}{p-1} \equiv 1 \pmod{p^4}$ , onde o termo à esquerda é o coeficiente binomial. Implemente uma função que encontre todos primos de Wolstenholme menores que um certo argumento dado.  
Uma conjectura afirma que são em número infinito... apesar de se conhecerem apenas dois: 16843 e 2124679.

10.  Experimente

```
mens='ABCDEFGHIJKLMNOPQRSTUVWXYZ'; L=list(map(ord, mens))
[L[k-1]-65 for k in [1..len(L)]]
[str(chr(L[k-1])) for k in [1..len(L)]].
```

11.  Crie funções de cifração e decifração das seguintes cifras clássicas:

- (a) A cifra *shift* tem como funções de cifração e decifração, respectivamente,

$$e_k(x) = x + k \pmod{n}; \quad d_k(y) = y - k \pmod{n}$$

onde  $n$  indica a cardinalidade do alfabeto usado. Para  $k = 3$  obtemos a cifra de César.

- (b) A cifra *afim* tem como funções de cifração e decifração, respectivamente,

$$e(x) = ax + k \pmod{n}; \quad d_k(y) = a^{-1}(y - k) \pmod{n}$$

onde  $n$  indica a cardinalidade do alfabeto usado e  $a$  é tal que  $(a, n) = 1$ .


- (c) A *cifra de Vigenère* é uma cifra polialfabética com funções de cifração e decifração

$$e_K(x_1, x_2, \dots, x_m) = (x_1 + k_1, x_2 + k_2, \dots, x_m + k_m)$$


$$d_K(x_1, x_2, \dots, x_m) = (x_1 - k_1, x_2 - k_2, \dots, x_m - k_m)$$

onde  $K = (k_1, k_2, \dots, k_m) \in \mathbb{Z}_n^m$ . Este vector  $K$  pode corresponder a uma palavra. Por exemplo, se  $A \sim 0, B \sim 1, C \sim 2, \dots$ , então se a chave="BLAISE" obtemos  $K = (1, 11, 0, 8, 18, 4)$ ,  $m = 6$ .

- (d) A cifra de Hill é uma cifra polialfabética. Antes de mais, a mensagem, de tamanho  $m$ , é dividida em blocos iguais, cada um de tamanho  $k$ . Se necessário acrescentam-se símbolos por forma a que  $k|m$ . A chave privada é uma matriz  $M$  do tipo  $k \times k$  sobre  $\mathbb{Z}_n$ , onde  $n$  denota a cardinalidade do alfabeto, por forma a que  $M$  seja invertível sobre  $\mathbb{Z}_n$ . Tal é equivalente a ter-se  $(\det(M), n) = 1$ . A função de cifração é  $x_\ell M$  e a de decifração é  $y_\ell M^{-1}$ , onde  $x_\ell, y_\ell$  denotam blocos de tamanho  $1 \times k$  dos vectores-linha  $x$  e  $y$ .

12.  Verifique que  $(a, n) = 1$  e determine  $a^{-1}$ , para

- (a)  $a = 77; n = 100$ .
- (b)  $a = 121; n = 224$ .
- (c)  $a = 2354; n = 3269$ .
- (d)  $a = 3001; n = 3006$ .

13.  Use o algoritmo estendido de Euclides para encontrar  $s, r \in \mathbb{Z}$  para os quais  $(a, b) = as + br$ , onde  $a$  e  $b$  são, respectivamente,


- (a) 43,33

- (b) 45, 75
- (c) 102, 222
- (d) 666, 1414
- (e) 6635, 38232
- (f) 1002, 8723
- (g) 2198, 9212
- (h) 20785, 44350
- (i) 34709, 100313
- (j) 71221, 128102
- (k) 9876543210, 123456789
- (l) 218709872121, 2182710222
- (m) 11100000001, 1000000001
- (n) 1111111111, 1000000001
- (o) 987219167212121, 98732871300832
- (p) 45666020043321, 73433510078091009

14. Pretende-se dar um exemplo de um domínio de integridade que não é domínio de factorização única.

Considere  $R = \mathbb{Z} + i\sqrt{5}\mathbb{Z} = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$ . Diz-se que  $p \in R$  é primo se  $p = ab \Rightarrow (a = \pm 1 \vee b = \pm 1)$ .

- (a) Mostre que  $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ .
- (b) Considere a função *norma* em  $R$  definida por  $N : R \rightarrow \mathbb{N}_0$  com  $N(a + b\sqrt{-5}) = a^2 + 5b^2$ .
  - i. Mostre que  $N$  é multiplicativa, ou seja, que  $N(\alpha\beta) = N(\alpha)N(\beta)$ , para quaisquer  $\alpha, \beta \in R$ .
  - ii. Mostre que  $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$  são primos em  $R$ .
- (c) Conclua que  $R$  não é um domínio de factorização única.


15.  Pretende-se determinar  $\frac{\pi(x)}{\frac{x}{\log x}}$ , para alguns valores de  $x$ .  
Use a função `numerical_approx`.

16.  A sucessão de Fibonacci está definida recursivamente por

$$f_1 = 1, f_2 = 1, f_n = f_{n-1} + f_{n-2}, \text{ para } n \geq 3.$$

Construa uma função que calcule os primeiros  $n$  termos da sucessão de Fibonacci.

17. Considere a sucessão de Fibonacci  $(f_n)$ .

- (a) Prove que  $\sum_{k=1}^n f_k = f_{n+2} - 1$ . [Repare que  $f_k = f_{k+2} - f_{k+1}$ , com  $k \in \mathbb{N}$ .]
- (b) Use o segundo princípio de indução para mostrar que  $f_n > \alpha^{n-2}$ , onde  $\alpha = \frac{1+\sqrt{5}}{2}$  é o *número de ouro* ou *número áureo*. [Repare que  $\alpha$  é solução de  $x^2 - x - 1 = 0$ .]
- (c) Mostre que se  $a_n = \frac{1}{\sqrt{5}}(\alpha^n - \beta^n)$ , onde  $\alpha = \frac{1+\sqrt{5}}{2}, \beta = \frac{1-\sqrt{5}}{2}$ , então  $a_n = a_{n-1} + a_{n-2}$  e  $a_1 = a_2 = 1$ . Conclua que  $f_n = a_n$ .
- (d) Mostre que o quociente da divisão inteira de termos consecutivos da sucessão de Fibonacci é 1 (excepto  $f_2$  e  $f_3$ ).
- (e) Sejam  $f_{n+1}, f_{n+2}$  termos consecutivos da sucessão de Fibonacci, com  $n > 1$ . Mostre que o algoritmo de Euclides tem exactamente  $n$  passos para mostrar que  $(f_{n+1}, f_{n+2}) = 1$ .
18.  A sucessão de Lucas está definida recursivamente por  $L_1 = 1, L_2 = 3, L_n = L_{n-1} + L_{n-2}$ , para  $n \geq 3$ . Construa uma função que calcule os primeiros  $n$  termos da sucessão de Lucas.