



## Teoria de Números Computacional

---

folha 2

---


1.  Use a factorização de Fermat para encontrar uma factorização de
  - (a) 143
  - (b) 979
  - (c) 3139
  - (d) 3713
  - (e) 2279
  - (f) 8051
  - (g) 11413
  - (h) 11021
  - (i) 46009
  - (j) 3200399
  - (k) 24681023
  - (l) 4210289
  - (m) 4574741741
  - (n) 184670524079
  - (o) 649989426469
2.  Implemente uma função que obtenha uma factorização de um natural usando o método de Fermat.
3. Mostre que se  $n \equiv 2 \pmod{4}$  então  $n$  não se pode escrever como diferença de quadrados.
4. Verifique a igualdade de Aurifeuille:
$$2^{4n+2} + 1 = (2^{2n+1} - 2^{n+1} + 1) (2^{2n+1} + 2^{n+1} + 1).$$
Use-a para obter uma factorização não trivial de  $2^{58} + 1$ .
5. Mostre que
  - (a) se  $a$  é um inteiro par então  $a^2 \equiv 0 \pmod{4}$ ;
  - (b) se  $a$  é um inteiro ímpar então  $a^2 \equiv 1 \pmod{4}$ .
6. Mostre que se  $a$  é um inteiro ímpar então  $a^2 \equiv 1 \pmod{8}$ .
7. O que pode concluir sobre  $a$  e  $b$  se  $a^2 \equiv b^2 \pmod{p}$ , onde  $a, b \in \mathbb{Z}$  e  $p$  é primo?

8.  Encontre as soluções de:


- (a)  $123456789x \equiv 9876543210 \pmod{10000000001}$
- (b)  $333333333x \equiv 87543211376 \pmod{967454302211}$
- (c)  $734342499999x \equiv 1 \pmod{1533331}$
- (d)  $499999x \equiv 1 \pmod{1533331}$
- (e)  $1000001x \equiv 1 \pmod{1533331}$

9. Mostre que  $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ , enquanto anéis, para  $(m, n) = 1$ .

Sugestão: mostre que o homomorfismo  $\psi([a]_{mn}) = ([a]_m, [a]_n)$  é injectivo, ou seja, que  $\psi([a]_{mn}) = ([0]_m, [0]_n)$  implica que  $[a]_{mn} = [0]_{mn}$ .

10.  Numa máquina que opera com números inferiores a 100, calcule

- (a)  $323 + 1261$
- (b)  $123655 + 410231$
- (c)  $124 \times 201$

11.  Numa máquina que opera com números inferiores a 1000, calcule


- (a)  $3243 + 71261$
- (b)  $4009143 + 2107002$
- (c)  $1003 \times 4101$

12. Sejam  $a, b \in \mathbb{N}$  com  $a > b$ . Mostre que

- (a) se  $r$  é o resto da divisão de  $a$  por  $b$  então  $2^r - 1$  é o resto da divisão de  $2^a - 1$  por  $2^b - 1$ . Como sugestão, observe que

$$2^{bq+r} - 1 = (2^b - 1) (2^{b(q-1)+r} + \dots + 2^{b+r} + 2^r) + (2^r - 1).$$

- (b)  $(2^a - 1, 2^b - 1) = 2^{(a,b)} - 1$ .
- (c)  $(2^a - 1, 2^b - 1) = 1$  se e só se  $(a, b) = 1$ .

13.  Suponha que tem à sua disposição uma máquina que permite efectuar operações aritméticas que não excedam  $2^{35}$ , e que pretende calcular o produto de 1237940039285380274899124225 por 2475880078570760549798248453. Mostre como tal se pode efectuar.

Sugestão: defina  $m_1=2^{35}-1$ ;  $m_2=2^{34}-1$ ;  $m_3=2^{33}-1$ ;  $m_4=2^{31}-1$ ;  $m_5=2^{29}-1$ ;  $m_6=2^{23}-1$ ; e  $M=m_1*m_2*m_3*m_4*m_5*m_6$ , e considere o Teorema Chinês dos Restos.

14. Use  $\rho$ -Pollard, com  $x_0 = 2$  e  $f(x) = x^2 + 1$  para encontrar a factorização de

- (a) 133
- (b) 1189

- (c) 1927
- (d) 8131
- (e) 36287
- (f) 48227

15. Use  $\rho$ -Pollard para factorizar 1387, fazendo uso de

- (a)  $x_0 = 2; f(x) = x^2 + 1$
- (b)  $x_0 = 3; f(x) = x^2 + 1$
- (c)  $x_0 = 2; f(x) = x^2 - 1$
- (d)  $x_0 = 2; f(x) = x^3 + x + 1$