

## Os inteiros

1. Quais são os divisores de 12?
2. Sejam  $n$  e  $d$  inteiros positivos. Quantos inteiros positivos  $\leq n$  são divisíveis por  $d$ ?
3. Determine a factorização prima de  $10!$ .
4. Determine as factorizações primas de 100, 641, 999, 1024 e 7007.
5. Os números 101, 107 e 113 são primos?
6. Qual é o quociente e o resto da divisão inteira de:
  - (a) -11 por 3?
  - (b) 101 por 11?
  - (c) 101 por -11?
  - (d) -101 por 11?
  - (e) -101 por -11?
7. Calcule  $\text{mdc}(2^2 \cdot 3^3 \cdot 5^2, 2^5 \cdot 3^3 \cdot 5^2)$  e  $\text{mdc}(2^2 \cdot 7, 5^3 \cdot 13)$ .
8. Quais inteiros positivos menores que 12 são primos com 12?
9. Determine  $\text{mdc}(414, 662)$  usando o algoritmo de Euclides.
10. Quantos zeros existem no final de  $100!$ ?
11. Calcule  $17 \bmod 5$ ,  $-133 \bmod 9$  e  $2001 \bmod 101$ .
12. Resolva em  $\mathbb{Z}_7$  as equações  $3 +_7 5 = x$ ,  $3 \times_7 3 = x$ ,  $3 +_7 x = 0$  e  $3 \times_7 x = 1$ .
13. (a) Encripte a mensagem “MATEMATICA” traduzindo as letras em números, aplicando a seguinte função de encriptação e depois traduzindo os números de volta em letras:
  - (i)  $f(p) = (p + 3) \bmod 23$  (cifra de César)
  - (ii)  $f(p) = (2p + 5) \bmod 23$ .

(b) Desencrpte as seguintes mensagens:

(i) SURMEMGR IZPDU (que foi encriptada usando a *cifra de César*).

(ii) ZIV LFRRFP (que foi encriptada usando a função de (a)(ii)).

[Nota: neste exercício use o alfabeto português com 23 letras.]

14. Encripte a mensagem “DESCOBRIMOS O CODIGO” traduzindo as letras em números, aplicando a seguinte função de encriptação e depois traduzindo os números de volta em letras:

(a)  $f(p) = (p + 3) \bmod 23$  (cifra de César)

(b)  $f(p) = (3p + 7) \bmod 23$ .

15. Descodifique a mensagem “HLX BEL”, que foi encriptada com a função

$$f(p) = (6p + 1) \bmod 23,$$

identificando as 23 letras do alfabeto pelos inteiros  $0, 1, 2, \dots, 22$  (como mostra a figura).

A	B	C	D	E	F	G	H	I	J	L	M	N	O	P	Q	R	S	T	U	V	X	Z
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22

16. Resolva as congruências  $3x \equiv_7 4$  e  $2x \equiv_{17} 7$ .

17. Mostre que  $a \equiv_m b \wedge c \equiv_m d \Rightarrow a + c \equiv_m b + d$ .

18. Mostre que

(a)  $a \mid b, a \mid c \Rightarrow a \mid (b + c)$ .

(b)  $a \mid bc \wedge \text{mdc}(a, b) = 1 \Rightarrow a \mid c$ .

(c) Se  $p$  é primo,  $p \mid ab \Rightarrow (p \mid a) \vee (p \mid b)$ .