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. Um número positivo diz-se *perfeito* se é igual à soma dos seus divisores positivos (diferentes dele próprio). Mostre que 6 e 28 são perfeitos.
4. Determine as factorizações primas de 100, 641, 999, 1024 e 7007.
5. Determine a factorização prima de 10!.
6. Os números 101, 107 e 113 são primos ?
7. 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 ?
8. 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, $p \mid ab \ \Rightarrow\ (p \mid a) \vee (p \mid b)$.
9. Calcule $\text{mdc}(24, 36)$ e $\text{mdc}(22, 17)$.
10. Os inteiros 17 e 21 são primos entre si ?
11. Calcule $\text{mdc}(2^2 \cdot 3^3 \cdot 5^2, 2^5 \cdot 3^3 \cdot 5^2)$ e $\text{mdc}(2^2 \cdot 7, 5^3 \cdot 13)$.
12. Determine $\text{mdc}(414, 662)$ usando o algoritmo de Euclides.
13. Quais inteiros positivos menores que 12 são primos com 12 ?
14. Mostre que n é primo se e só se $\phi(n) = n - 1$.
15. Quantos zeros existem no final de 100! ?
16. Calcule $17 \bmod 5$, $-133 \bmod 9$ e $2001 \bmod 101$.
17. Liste cinco inteiros congruentes com 4 módulo 12.

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

19. Resolva em $\mathbb{Z}_7$ as equações $3 +_7 5 = x$, $3 \times_7 3 = x$, $3 +_7 x = 0$ e $3 \times_7 x = 1$.

20. Que sequência de números pseudo-aleatórios é gerada por $x_{n+1} = (4x_n + 1) \bmod 7$ com raiz $x_0 = 3$?

21. (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) Desencripte 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.]

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

23. 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 $0, 1, 2, \ldots, 22$ (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

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

25. (a) Mostre que 937 é um inverso de 13 módulo 2436.

    (b) Encripte as mensagens "STOP" e "ATAQUE" usando o sistema RSA com $p = 43$, $q = 59$ e $a = 13$. Se recebermos a mensagem 0981 1175 encriptada com esse sistema, como a desencriptamos? E a mensagem 2222 2116 1723? (Nota: aqui será preciso alguma ajuda computacional se quiser fazer isto em pouco tempo.)

26. Mostre que, no sistema criptográfico RSA, sendo $n = pq$ um produto de dois primos p e q e $m = (p-1)(q-1)$, será fácil, a um intruso, descobrir os valores dos dois primos p e q se conhecer os valores de n e m.