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) $a \mid bc \ \wedge\ \mathrm{mdc}(a,b) = 1 \ \Rightarrow a \mid c$.
   (c) Se p é primo, $p \mid ab \ \Rightarrow\ (p \mid a) \vee (p \mid b)$.
9. Calcule $\mathrm{mdc}(24,36)$ e $\mathrm{mdc}(22,17)$.
10. Os inteiros 17 e 21 são primos entre si ?
11. Calcule $\mathrm{mdc}(2^2 \cdot 3^3 \cdot 5^2, 2^5 \cdot 3^3 \cdot 5^2)$ e $\mathrm{mdc}(2^2 \cdot 7, 5^3 \cdot 13)$.
12. Determine $\mathrm{mdc}(414, 662)$ usando o algoritmo de Euclides.
13. Quais inteiros positivos menores que 12 são primos com 12 ?
14. Determine $\phi(4)$ e $\phi(10)$.
15. Mostre que n é primo se e só se $\phi(n) = n - 1$.
16. Quantos zeros existem no final de 100! ?
17. Calcule 17 mod 5, -133 mod 9 e 2001 mod 101.
18. Liste cinco inteiros congruentes com 4 módulo 12.
19. Mostre que $a \equiv_m b \ \wedge\ c \equiv_m d \ \Rightarrow\ a + c \equiv_m b + d$.
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. Resolva as congruências $3x \equiv_7 4$ e $2x \equiv_{17} 7$.

23. Mostre que 937 é um inverso de 13 módulo 2436.

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

25. Encripte as mensagens "STOP" e "ATAQUE" usando o sistema RSA com $p = 43$, $q = 59$ e $a = 13$. Se recebermos a mensagem 0981 0461 encriptada com esse sistema, como a desencriptamos ? E a mensagem 0667 1947 0671 ? (Nota: aqui será preciso alguma ajuda computacional se quiser fazer isto em pouco tempo.)

Raciocínio matemático, indução e recursão

1. Sejam p a proposição "$n \equiv_3 1$" e q a proposição "$n^2 \equiv_3 1$". A implicação $p \to q$, que é "se $n \equiv_3 1$, então $n^2 \equiv_3 1$" é verdadeira. Se q é verdadeira, ou seja, $n^2 \equiv_3 1$, decorre daí que p é verdadeira, isto é, que $n \equiv_3 1$?

2. Mostre que a proposição $P(0)$ é verdadeira, para as seguintes proposições $P(n)$:

    (a) $P(n)$: Se $n > 1$ então $n^2 > n$.
    (b) $P(n)$: Se a e b são inteiros positivos com $a \geq b$, então $a^n \geq b^n$.

3. Será correcto assumir que se $\neg p$ é verdadeira então $\neg q$ é verdadeira, usando o facto de que $p \to q$ é verdadeira ?

4. Apresente uma prova por contradição do teorema "Se $3n + 2$ é ímpar, então n é ímpar."

5. Prove que o quadrado de um número par é par usando

    (a) uma prova directa.
    (b) uma prova por contradição.

6. Seja n um inteiro. Prove a equivalência das seguintes três proposições:

    p_1: $n \bmod 3 = 1$ ou $n \bmod 3 = 2$.
    p_2: n não é divisível por 3.
    p_3: $n^2 \equiv_3 1$.

7. Para que inteiros não negativos n é válida a desigualdade $2n + 3 \leq 2^n$? Justifique a sua resposta usando indução matemática.

8. Prove, por indução matemática, que, para qualquer inteiro positivo n:

    (a) A soma dos primeiros n inteiros positivos ímpares é igual a n^2.
    (b) A soma dos primeiros n inteiros positivos é igual a $(n^2 + n)/2$.
    (c) $n < 2^n$.
    (d) $n^3 - n$ é divisível por 3.
    (e) $1 + 2 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$.