# Folhas de exercícios I

Fernando Ferreira

*Introdução à Teoria dos Números*
2018/2019

1. Dado $a \in \mathbb{Z}$ e $n \in \mathbb{N}$, mostre que $(a-1) \mid (a^n - 1)$. (Sugestão: note que o polinómio $X^n - 1$ tem raiz 1.)

2. Um *primo de Mersenne* é um número primo da forma $2^n - 1$, para $n$ número natural. Mostre que, neste caso, $n$ é primo.

3. Sejam $a, n \in \mathbb{N}$. Suponha que $a^n - 1$ é primo e que $n \neq 1$. Mostre que $a = 2$.

4. Calcule o cociente e o resto da divisão inteira (a) de 300 por 17, (b) de 729 por 31, (c) de 17 por 300, (d) de 56431 por 791, (e) de 18756407 por 937 e (f) de 4970618935 por 95043.

5. (a) Mostre que se $n \in \mathbb{N}$ é um quadrado, então $n$ não é da forma $4k + 3$ (com $k$ inteiro não negativo). (Sugestão: calcule o resto da divisão por 4 dos números $(4m)^2$, $(4m+1)^2$, $(4m+2)^2$ e $(4m+3)^2$.)

   (b) Mostre que nenhum número natural da sequência

   $$11, 111, 1111, 11111, 111111, \ldots$$

   é um quadrado (os números da sequência estão escritos em notação decimal). (Sugestão: $111\cdots111 = 111\cdots108 + 3 = 4k + 3$.)

6. Calcule diretamente nas bases em questão $(212)_3 \cdot (122)_3$, $(101101)_2 \cdot (11001)_2$, $(10011001)_2 : (1011)_2$ e $(40122)_7 : (126)_7$. Converta cada uma destes números para a base 10, efectue a operação em base 10 e, depois, converta o resultado para a base em questão.

7. Considere o alfabeto de 26 letras (inclue-se o K, W e Y) como sendo os símbolos da notação posicional de base 26 (em que a ordem alfabética corresponde à ordem crescente dos símbolos). Calcule o produto $\mathrm{SIM} \cdot \mathrm{NAO}$.

8. Seja $b$ um natural maior do que 1. Dado $n \in \mathbb{N}$ denota-se por $lh_b(n)$ o comprimento de representação de $n$ em base $b$. Mostre que $lh_b(n) = \lfloor \log_b n \rfloor + 1$ (onde $\lfloor x \rfloor$ denota a parte inteira de $x$, i.e., o maior inteiro que não excede $x$).

9. Mostre a seguinte igualdade logarítmica: $\log_b n = \log_b c \cdot \log_c n$, para todos os reais positivos $n$, $b$ e $c$ com $b \neq 1$ e $c \neq 1$.

10. Seja $b$ um natural diferente de 1 (uma base). Dado $n \in \mathbb{N}$, mostre que existem inteiros $a_0, a_1, \ldots, a_k$ com $0 \leq a_i < b$ (para $0 \leq i \leq k$) e $a_k \neq 0$ tais que $n = \sum_{i=0}^{k} a_i b^i$. Argumente que estes números são únicos.

11. Sejam $a$ e $b$ números naturais com $a \geq b$. Suponha que $a = bq + r$ e $b = rs + t$, onde $q$, $r$, $s$ e $t$ são inteiros não negativos com $0 < r < b$ e $0 \leq t < r$. Mostre que $t < \frac{b}{2}$.

12. Seja $a_0, a_1, \ldots, a_n$ uma sucessão de números naturais tal que $a_{i+1} \leq \frac{1}{2} a_i$, para todo $0 \leq i < n$. Mostre que $2^n \leq a_0$.

13. Use o algoritmo de Euclides para calcular $\mathrm{mdc}(15, 35)$, $\mathrm{mdc}(247, 299)$, $\mathrm{mdc}(51, 897)$, $\mathrm{mdc}(136, 304)$, $\mathrm{mdc}(323, 437)$, $\mathrm{mdc}(455, 1235)$, $\mathrm{mdc}(1547, 560)$, $\mathrm{mdc}(1187319, 438987)$ e $\mathrm{mdc}(4152983, 298936)$.

14. Seja $n$ um número natural diferente de 1. Mostre que $n$ é primo se, e somente se, não é divisível por nenhum primo $p$ com $p \leq \sqrt{n}$.

15. Enumere todos os primos até 200 usando o crivo de Eratóstenes.

16. Mostre que $n!$ divide sempre o produto de $n$ números naturais consecutivos. (Sugestão: considere um coeficiente binomial adequado.)

17. Dado um elemento $a + b\sqrt{-5}$ de $\mathbb{Z}[\sqrt{-5}]$ $(a, b \in \mathbb{Z})$, define-se a sua *norma* como sendo $N(a + b\sqrt{-5}) := a^2 + 5b^2$.

    (a) Mostre que a norma dum produto é o produto das normas.

    (b) Descubra os "divisores" de 2, 3, $1 + \sqrt{-5}$ e $1 - \sqrt{-5}$.

    (c) Mostre que 6 pode ser "fatorizado em primos de duas maneiras diferentes". (Tecnicamente, deveríamos ter utilizado a terminologia "fatorizado em irredutíveis de duas maneiras diferentes". Em $\mathbb{Z}[\sqrt{-5}]$ há uma distinção entre a noção de primo e a noção de irredutível.)

18. Ao contrário do exemplo do exercício anterior, os números da forma $a + bi$, com $a, b \in \mathbb{Z}$, os chamados *números inteiros de Gauss*, formam um domínio de fatorização única. Use este facto e a alínea seguinte para mostrar a alínea (b) abaixo.

    (a) Diga quais são as quatro unidades dos inteiros de Gauss.

    (b) Sejam dados inteiros $a, b, c, d$. Mostre que se $a^2 + b^2 = c^2 + d^2$ e $a + bi$ e $c + di$ são ambos "primos do anel de Gauss", então ($a = \pm c$ e $b = \pm d$) ou ($a = \pm d$ e $b = \pm c$).

19. Sejam $a, b, c \in \mathbb{N}$ tais que $a^2 = b^2 c$. Mostre que $c$ é um quadrado. (Use o teorema fundamental da aritmética.)

20. Sejam $a, b, c \in \mathbb{N}$ tais que $a \mid c$, $b \mid c$ e $a \perp b$. Mostre que $ab \mid c$. (Use o teorema fundamental da aritmética.)

21. Usando o teorema fundamental da aritmética mostre o seguinte:

    (a) Sejam $a, b \in \mathbb{N}$ com $a \perp b$ e $ab$ um número quadrado. Mostre que $a$ e $b$ são quadrados.

    (b) Dados $a, b, n \in \mathbb{N}$, mostre que se $a^n \mid b^n$ então $a \mid b$.

    (c) Sejam $a, b, c \in \mathbb{N}$. Mostre que se $a \mid bc$ e $a \perp b$, então $a \mid c$. Conclua o seguinte: dados $a, b, n \in \mathbb{N}$ com $a \perp b$, se $a \mid b^n$ então $a = 1$.

    (c) Seja $p$ um número primo e $a, k \in \mathbb{N}$. Mostre que se $p \mid a^k$ então $p^k \mid a^k$.

22. Sejam $a, b \in \mathbb{N}$. O *mínimo múltiplo comum* de $a$ e $b$ é o número natural $\min\{m \in \mathbb{N} : a \mid m \text{ e } b \mid m\}$. Este número denota-se por $\operatorname{mmc}(a, b)$. Mostre que $ab = \operatorname{mdc}(a, b) \operatorname{mmc}(a, b)$ (use o teorema fundamental da aritmética).

23. Dado $n \in \mathbb{N}$, mostre que a fração $\frac{12n+1}{30n+2}$ está em forma reduzida. (Veja exercício 2.24 do livro e a sua solução.)

24. Sejam $n, m \in \mathbb{N}$ ímpares. Mostre que $\operatorname{mdc}(n + m, n - m) = 2 \operatorname{mdc}(n, m)$.

25. Seja $n \in \mathbb{N}$ com $n \neq 1$.

    (a) Dados $a, b \in \mathbb{N}$ e $r$ o resto da divisão de $a$ por $b$. Mostre que $n^r - 1$ é o resto da divisão de $n^a - 1$ por $n^b - 1$. (Use o exercício 1.)

    (b) Mostre que $\operatorname{mdc}(n^a - 1, n^b - 1) = n^{\operatorname{mdc}(a,b)} - 1$. (Pense no algoritmo de Euclides para calcular o máximo divisor comum.)

26. (a) Mostre que há um número infinito de primos da forma $4n - 1$. (b) Mostre que há um número infinito de primos da forma $6n - 1$. (Veja no livro.)

27. Seja $n$, $k$ e $r$ inteiros. Mostre que se $0 \leq k < r \leq \frac{n}{2}$, então $\binom{n}{k} < \binom{n}{r}$. (Sugestão: calcule o cociente entre $\binom{n}{k}$ e $\binom{n}{k+1}$.)