Folhas de exercícios

Fernando Ferreira

Introdução à Teoria dos Números
2017/2018

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 raíz 1.

2. Calcule o cociente e o resto da divisão inteira de (a) 300 por 17, (b) 729 por 31, (c) 17 por 300 e (d) 18756407 por 937.

3. (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: $111\cdots111 = 111\cdots108 + 3 = 4k + 3$.

4. 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.

5. 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 $\mathrm{SIM} \cdot \mathrm{NAO}$.

6. Demonstre a asserção de existência do teorema fundamental da aritmética.

7. Mostre que no algoritmo da divisão o cociente e o resto são únicos.

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. Calcule pelo algoritmo de Euclides $\mathrm{mdc}(15, 35)$, $\mathrm{mdc}(247, 299)$, $\mathrm{mdc}(51, 897)$, $\mathrm{mdc}(136, 304)$, $\mathrm{mdc}(323, 437)$, $\mathrm{mdc}(455, 1235)$ e $\mathrm{mdc}(1547, 560)$.

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".

18. 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.)

19. 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.)

20. 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 $p^k \mid a^k$.

21. 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.)

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

23. 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 judiciosamente o facto de que $(c-1) \mid (c^k - 1)$, para $c, k \in \mathbb{N}$ e $c > 1$.)

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

24. (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.)

25. 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 $\binom{n}{k+1}$.

26. Usando o teorema do número primo mostre que $\lim_n \frac{\pi(n)}{n} = 0$.

27. Seja n um número natural.

    (a) Tome-se k inteiro tal que $0 \leq k \leq n$. Mostre que $\binom{n}{k} \leq n^{\pi(n)}$. Sugestão: use o facto de que se $p^r \mid \binom{n}{k}$ então $p^r \leq n$, para p primo.

    (b) Conclua que $\frac{2n \ln 2}{\ln(2n)} \leq 1 + \pi(2n)$. Sugestão: ensanduiche $\binom{2n}{n}$ entre dois valores apropriados e tome logaritmos.

28. Mostre que a função $x \rightsquigarrow (1 + \sqrt{2x}) \ln(2x)$ tem segunda derivada negativa em $]0, +\infty[$.

29. (a) Dado x um número real maior do que 1, mostre que a série $\sum_{n=1}^{\infty} \frac{1}{n^x}$ converge (use o teste do integral).

    (b) Dado a um número real positivo, mostre que $\zeta(1+a) \leq \frac{1+a}{a}$.

30. Mostre que $\sum_{k=2}^{\infty} \sum_{n=2}^{\infty} \frac{1}{nk^n} < \infty$. (Mostre que para $n, k \geq 3$, se tem $n^2 k^2 \leq nk^n$.)

31. Seja n um número natural. Mostre que, para todo o número complexo s com $Re(s) > 0$, se tem

$$\int_n^{n+1} \left| \frac{1}{n^s} - \frac{1}{x^s} \right| dx \leq \frac{|s|}{n^{Re(s)+1}}$$

    (Note que $\int_n^x \frac{1}{u^{s+1}} du = \frac{1}{s}\left(\frac{1}{n^s} - \frac{1}{x^s}\right)$ e majorize o valor absoluto do integrando, onde $n \leq u \leq x \leq n+1$.)

32. Dados $a, b \in \mathbb{N}$ e $n \in \mathbb{N}$. Mostre que $a \equiv b \pmod{n}$ se, e somente se, o resto da divisão de a por n é igual ao resto da divisão de b por n.

33. Será que $b \equiv c \pmod{n}$ implica sempre $a^b \equiv a^c \pmod{n}$? (Aqui, a, b, c e n são números naturais.)

34. (a) Construa as tabelas de adição e multiplicação de $\mathbb{Z}/6\mathbb{Z}$ e de $\mathbb{Z}/7\mathbb{Z}$.

    (b) Construa as tabelas de multiplicação de $(\mathbb{Z}/8\mathbb{Z})^*$, $(\mathbb{Z}/9\mathbb{Z})^*$, $(\mathbb{Z}/10\mathbb{Z})^*$ e $(\mathbb{Z}/15\mathbb{Z})^*$.

    (c) Diga quais são as ordens dos elementos de $(\mathbb{Z}/8\mathbb{Z})^*$. Faça o mesmo para $(\mathbb{Z}/9\mathbb{Z})^*$, $(\mathbb{Z}/10\mathbb{Z})^*$ e $(\mathbb{Z}/15\mathbb{Z})^*$.

35. Calcule $347 + 513 \pmod{763}$, $3274 + 1238 + 7231 + 6437 \pmod{9254}$, $153 \cdot 287 \pmod{353}$, $357 \cdot 862 \cdot 193 \pmod{943}$, $5327 \cdot 6135 \cdot 7139 \cdot 2187 \cdot 5219 \cdot 1873 \pmod{8157}$, $137^4 \pmod{327}$ e $373^6 \pmod{581}$.

36. Resolva as equações: (a) $x + 17 \equiv 23 \pmod{37}$; (b) $x + 42 \equiv 19 \pmod{51}$; (c) $x^2 \equiv 3 \pmod{11}$; (d) $x^2 \equiv 2 \pmod{13}$; (e) $x^2 \equiv 1 \pmod{8}$ e (f) $x^3 - x^2 + 2x - 2 \equiv 0 \pmod{11}$. Apresente os resultados no sistema completo de resíduos canónico e no sistema menor.

37. Seja dado n um número natural escrito em notação decimal: $n = \sum_{i=0}^{k} a_i 10^i$, onde $a_i \in \{0, 1, \ldots, 9\}$, para $0 \leq i \leq k$, e $a_k \neq 0$. Mostre que se tem $n \equiv a_0 + a_1 + \cdots + a_k \pmod{9}$.

38. Mostre que $n^5 - n$ é sempre divisível por 30. (Mostre que é sempre divisível por 2, 3 e 5.)

39. Mostre que $5^i \not\equiv -1 \pmod{8}$ para todo $i \geq 0$.

40. Sejam $n, k \in \mathbb{N}$ com $n > 1$. Dados $b, c \in \mathbb{Z}$ com $b \equiv c \pmod{n^k}$, mostre que $b^n \equiv c^n \pmod{n^{k+1}}$.

41. Sejam $a, b \in \mathbb{Z}$ e n um número natural diferente de 1. Mostre que a equação $ax \equiv b \pmod{n}$ tem solução se, e somente se, $\text{mdc}(a, n) \mid b$.

42. Mostre que se $n > 4$ é um número composto então $(n-1)! \equiv 0 \pmod{n}$.

43. Seja $n \in \mathbb{N}$. Mostre que se n e $n^2 + 2$ são primos então $n = 3$. (Veja o problema 2.18 do livro e a sua solução.)

44. Resolva os seguintes equações:

    (a) $x \equiv 3 \pmod{7}$ e $x \equiv 4 \pmod{9}$.

    (b) $x \equiv 13 \pmod{71}$ e $x \equiv 41 \pmod{97}$.

    (c) $x \equiv 4 \pmod{7}$, $x \equiv 5 \pmod{8}$ e $x \equiv 11 \pmod{15}$.

45. (a) Exiba concretamente o isomorfismo de anéis (da aula teórica) entre $\mathbb{Z}/15\mathbb{Z}$ e $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.

    (b) Exiba concretamente o isomorfismo de grupos (da aula teórica) entre $(\mathbb{Z}/15\mathbb{Z})^*$ e $(\mathbb{Z}/3\mathbb{Z})^* \times (\mathbb{Z}/5\mathbb{Z})^*$.

46. Mostre que um número é divisível por 9 se, e somente se, a soma dos seus dígitos (notação decimal) é divisível por 9. Apresente critérios semelhantes para a divisibilidade por 3, 5 e 11.

47. Encontre um número de três dígitos (notação decimal) que deixa resto 4 quando dividido por 7, 9 e 11.

48. Encontre $x \in \mathbb{Z}$ tal que $x \equiv -4 \pmod{17}$ e $x \equiv 3 \pmod{23}$.

49. Seja p um primo tal que $p \equiv 3 \pmod{4}$. Mostre que não há nenhum inteiro a tal que $p \mid (a^2 + 1)$. (Use o pequeno teorema de Fermat.)

50. Calcule $\varphi(55)$, $\varphi(128)$, $\varphi(90)$, $\varphi(89)$ e $\varphi(105)$.

51. Será que existem números naturais n e m com $\varphi(nm) \neq \varphi(n)\varphi(m)$?

52. Para que valores de n é que $\varphi(n)$ é ímpar?

53. Seja p um número primo. Mostre que $(a + b)^p \equiv a^p + b^p \pmod{p}$, para todos $a, b \in \mathbb{Z}$. Será que este facto ainda é verdade caso p não seja primo?

54. Sejam A e B dois anéis comutativos com identidade e seja $\gamma : A \to B$ um morfismo de anéis.

    (a) Mostre que se a é uma unidade de A então $\gamma(a)$ é uma unidade de B.

    (b) Admita que γ é um isomorfismo de anéis e seja $\gamma \restriction$ a restrição de γ a A^* (o grupo das unidade de A). Mostre que $\gamma \restriction : A^* \to B^*$ é um isomorfismo de grupos (B^* é o grupo das unidades de B).

55. Sejam m_1, m_2, ..., m_k números naturais diferentes de 1, co-primos dois a dois. Dados $a_1, a_2, \ldots, a_k \in \mathbb{Z}$, mostre que existe $x \in \mathbb{Z}$ tal que

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\ldots \quad \ldots \quad \ldots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

    Mostre também que x é único módulo o produto $m_1 \cdot m_2 \cdot \ldots \cdot m_k$. Sugestão: para a parte da existência argumente por indução e use o teorema chinês dos restos.

56. Sejam p e q primos ímpares distintos e $n = pq$. Mostre que o polinómio $x^2 - 1$ tem exatamente quatro raízes em $\mathbb{Z}/n\mathbb{Z}$. Encontre as quatro raízes de equação $x^2 - 1 \equiv 0 \pmod{35}$.

57. Sejam $p_1, p_2, \ldots, p_r$ primos ímpares distintos e considere-se $n = p_1 \cdot p_2 \cdot \ldots \cdot p_r$.

    (a) Seja $F \subseteq \{1, 2, \ldots, r\}$. Mostre que existe $x_F \in \mathbb{Z}$ tal que $x_F \equiv 1 \pmod{p_i}$, for $i \in F$, and $x_F \equiv -1 \pmod{p_j}$, for $j \notin F$ $(1 \leq j \leq r)$.

(b) Mostre que a equação $x^2 \equiv 1 \pmod{n}$ tem exatamente 2^r soluções.

(c) Encontre as oito soluções de $x^2 \equiv 1 \pmod{105}$.

58. Encontre um inteiro x tal que $37x \equiv 1 \pmod{101}$.

59. Sejam a e b números naturais e $d = \text{mdc}(a, b)$. Considere a equação nos inteiros $ax + by = d$.

(a) Mostre que se o par de inteiros x_0, y_0 é solução da equação acima então, para todo $z \in \mathbb{Z}$, o par $x_0 + z\frac{b}{d}$, $y_0 - z\frac{a}{d}$, também é solução da erquação.

(b) Mostre que todas as soluções da equação são da forma da alínea anterior.

60. Use o algoritmo estendido de Euclides para encontrar inteiros x e y tais que $2261x + 1275y = 17$. Usando a alínea anterior, encontre todas as soluções inteiras da equação dada.

61. Para cada um dos primos p e números a, calcule $a^{-1} \pmod{p}$ usando o algoritmo de Euclides estendido: (a) $p = 47$ e $a = 11$; (b) $p = 587$ e $a = 345$; e (c) $p = 104801$ e $a = 78467$.

62. Obtenha $x, y, z \in \mathbb{Z}$ tais que $35x + 55y + 77z = 1$.

63. Dados $a_1, a_2, \ldots a_k$ elementos de $\mathbb{N}$, defina-se $\text{mdc}(a_1, a_2, \ldots, a_k)$ como o máximo dos divisores comuns a todos os $a_1, a_2, \ldots, a_k$.

(a) Mostre que $\text{mdc}(a_1, a_2, a_3 \ldots, a_k) = \text{mdc}(\text{mdc}(a_1, a_2), a_3, \ldots, a_k)$.

(b) Mostre que existem elementos $x_1, x_2, \ldots, x_k \in \mathbb{Z}$ tais que

$$\text{mdc}(a_1, a_2, \ldots, a_k) = x_1a_1 + x_2a_2 + \cdots + x_ka_k.$$

64. Use o método da repetição do quadrado para calcular $17^{183} \pmod{256}$, $2^{477} \pmod{1000}$ e $11^{507} \pmod{1237}$.

65. Diga quais são os dois últimos dígitos de 3^{35}.

66. Mostre que $2^{11} - 1$ (= 2047) é um número composto usando o pequeno teorema de Fermat com base 3. (Faça mesmo as contas...)

67. Na aula teórica afirmámos que 561 é um número de Carmichael mas não o verificámos.

(a) Note que $561 = 3 \cdot 11 \cdot 17$. Use o pequeno teorema de Fermat para mostrar que, para todo $a \in \mathbb{Z}$,

$$a^{561} \equiv a \pmod{3}, \quad a^{561} \equiv a \pmod{11}, \quad a^{561} \equiv a \pmod{17}.$$

(b) Diga por que é que estas congruências mostram que 561 é um número de Carmichael.

(c) Use a ideia da alínea anterior para mostrar que 1729 é um número de Carmichael.

68. Encontre um inteiro a tal que $102^{70} + 1 \equiv a^{37} \pmod{113}$. (Calcule mesmo $102^{70} \bmod 113$. Se quiser use o SAGE.)

69. (a) Seja p um primo ímpar. Mostre que um polinómio $x^2 + bx + c \in \mathbb{Z}_p[x]$ tem raízes em $\mathbb{Z}_p$ se, e somente se, $b^2 - 4c$ é um quadrado módulo p.

    (b) Seja K um corpo de característica diferente de 2. Em que condições é que um polinómio $x^2 + bx + c \in K[x]$ tem raízes em K?

70. Tente o teste de Miller-Rabin para 561 com as bases 4, 5 e 7. (Sei bem que este e o próximo exercício são um bocado tolos...)

71. Tente o teste de Miller-Rabin para 1105 com as bases 2, 3 e 4.

72. Qual é a ordem de 3 módulo 11? Qual é a ordem de 2 módulo 17? (Veja à mão.)

73. Mostre que 5 é uma raíz primitiva módulo 6.

74. Seja p primo ímpar tal que $(p-1)/2$ também é primo. Mostre que os elementos de $(\mathbb{Z}/p\mathbb{Z})^*$ têm ordens 1, 2, $(p-1)/2$ ou $p-1$.

75. Seja G um grupo comutativo e a e b elementos de G com ordens n e m respetivamente. Suponha que $n \perp m$. Mostre que a ordem de ab é nm. (Veja no livro, p. 42, ou consulte os seus apontamentos de Álgebra.)

76. Um número racional positivo $q < 1$ diz-se *puramente periódico* (em base 10) se existirem $a_1, \ldots, a_r \in \{0, 1, \ldots 9\}$ tais que $q = \sum_{n \geq 0} \sum_{j=1}^{r} \frac{a_j}{10^{rn+j}}$. Ao menor r nestas circunstâncias chama-se o *período* de q.

    (a) Mostre que $\frac{1}{3}$, $\frac{1}{7}$, $\frac{1}{9}$, $\frac{1}{11}$ e $\frac{1}{13}$ são racionais puramente periódicos e diga quais são os seus períodos.

    (b) Seja d um número natural maior do que 1 e coprimo com 10. Mostre que $\frac{1}{d}$ é um número racional puramente periódico cujo período é a ordem de 10 módulo d.

77. Quantas raizes primitivas módulo 23 é que existem? E módulo 27? E módulo 50? E módulo 21?

78. Seja K um corpo finito. Mostre que o grupo $(K \setminus \{0\}, \cdot)$ é cíclico. Sugestão: adapte a demonstração de que, se p é primo, então existem raízes primitivas módulo p.

79. Seja G um grupo cíclico finito de cardinalidade n. Mostre que G tem $\varphi(n)$ geradores. (Mostre que se a gera G, então a^k gera G se, e somente se, $k \perp n$. Use a relação de Bézout.)

80. Porque é que os números quadrados são exceção na conjetura de Artin?

81. Seja dado $k \geq 3$.

    (a) Verifique que 8 não tem raízes primitivas.

    (b) Mostre que não há raízes primitivas módulo 2^k.

    (c) Calcule $\varphi(2^k)$.

    (d) Mostre que $5^{2^{k-3}} \equiv 1 + 2^{k-1} \pmod{2^k}$.

    (e) Mostre que $(\mathbb{Z}/2^k\mathbb{Z})^*$ é gerado por -1 e 5. (Use a alínea anterior e o exercício 39.)

82. Heloísa vai combinar com Abelardo uma chave secreta usando o sistema de Diffie-Hellman. Escolhem o primo 53 e $g = 2$. Heloísa toma como chave secreta $n = 29$. Qual é a chave pública de Heloísa? Entretanto, Heloísa recebe a chave pública de Abelardo, que é 12. Qual é a chave secreta que ambos combinaram?

83. Seja p um número primo e g uma raíz primitiva módulo p.

    (a) Mostre que a aplicação $\log_g : \mathbb{Z}_p^* \mapsto \mathbb{Z}_{p-1}$ que a cada $\overline{a} \in \mathbb{Z}_p^*$ faz corresponder $\overline{k} \in \mathbb{Z}_{p-1}$ tal que $g^k \equiv a \pmod{p}$ está bem definida.

    (b) Mostre que $\log_g(h_1 h_2) = \log_g(h_1) + \log_g(h_2)$, para todos $h_1, h_2 \in \mathbb{Z}_p^*$.

    (c) Mostre que $\log_g(h^n) = n \log_g h$, para todos $h \in \mathbb{Z}_p^*$ e $n \in \mathbb{Z}$.

84. Calcule $\log_2(13)$ para o primo 23. (Estamos a abusar a notação.)

85. Heloísa e Abelardo vão comunicar secretamente usando o sistema de encriptação pública ElGamal. O primo que escolhem é 467 e o elemento módulo 467 escolhido é $g = 2$. A chave secreta de Heloísa é $n = 153$.

    (a) Qual é a chave pública de Heloísa?

    (b) Abelardo pretende enviar secretamente a mensagem $M = 351$ à Heloísa e, para isso, escolhe secretamente a chave efémera $k = 197$. Que par de números é que Abelardo envia publicamente a Heloísa?

    (c) Apresente os cálculos de Heloísa para ler a mensagem que Abelardo lhe enviou.

86. Considere a seguinte variante simplificada da troca de chaves de Diffie-Hellman. Esta variante, tal como o original, baseia-se na escolha dum primo grande p e num elemento $1 < g < p$. Heloísa escolhe secretamente um número $1 < n < p$ e dá a conhecer $a := ng \pmod{p}$. Abelardo também escolhe secretamente um número $1 < m < p$ e dá a conhecer $b := mg \pmod{p}$. A chave secreta é $nmg \pmod{p}$, que tanto Heloísa como Abelardo podem calcular facilmente (porquê?). Por que é que esta troca de chaves não é segura?

87. Quais são os números naturais menores do que 20 que são soma de dois quadrados inteiros? E de três quadrados? E de quatro quadrados?

88. Através do método de fatorização de Fermat, fatorize (a) 8633, (b) 809009, (c) 92296873 e (d) 4601.

89. Tente o teste de Miller-Rabin para 172947529 com as testemunhas 17, 3 e 23 (muitas contas... use o SAGE).

90. Heloísa vai combinar com Abelardo uma chave secreta usando o sistema de Diffie-Hellman. Escolhem o primo 3793 e $g = 7$. Heloísa toma como chave secreta um número natural $n < 3783$ e diz a Abelardo que $7^n \equiv 454 \pmod{3793}$. Abelardo escolhe aleatoriamente o número 1208 e toma-o como a sua chave secreta. Qual é a chave secreta que ambos combinaram?

91. Heloísa publica a sua chave pública RSA: (2038667,103), onde $n = 2038667$ é produto de dois primos distintos e $e = 103$ é o expoente encriptador. [Para fazer este exercício e o próximo utilize uma calculadora ou um computador.]

    (a) Abelardo quer enviar a mensagem $M = 892383$ à Heloísa. Que cifra é que ele envia?

    (b) Heloísa sabe que 1301 divide 2038667. Encontre o expoente decifrador d da Heloísa.

    (c) Faça os cálculos que permitem à Heloísa obter M a partir da cifra enviada por Abelardo.

    (d) Heloísa também recebe a cifra 317730 de Abelardo. Decifre esta mensagem.

92. Neste exercício, n é o produto de dois primos distintos. Calcule estes primos (usando um método descrito na aula) sabendo que

    (a) $n = 352717$ e $\varphi(n) = 351520$.

    (b) $n = 172205490419$ e $\varphi(n) = 172204660344$.

93. O número 1433811615146881 é produto de dois primos distintos, próximos um do outro. Encontre estes dois primos.

94. Seja $n = mr$ com $m, r \in \mathbb{N} \setminus \{1\}$ e $m \perp r$. Considere-se $a \in \mathbb{Z}$ tal que $a \perp n$. Mostre que a é resíduo quadrático módulo n se, e somente se, a é resíduo quadrático módulo m e a é resíduo quadrático módulo r.

95. Seja p um primo ímpar. Mostre que, para qualquer inteiro m co-primo com p, o número de soluções da equação $x^2 \equiv m \pmod{p}$ é $1 + \left(\frac{m}{p}\right)$.

96. Calcule os seguintes símbolos de Legendre: $\left(\frac{3}{97}\right)$, $\left(\frac{3}{389}\right)$, $\left(\frac{5!}{7}\right)$, $\left(\frac{19}{31}\right)$, $\left(\frac{11}{37}\right)$, $\left(\frac{97}{101}\right)$, $\left(\frac{31}{167}\right)$ e $\left(\frac{5}{160465489}\right)$.

97. Seja p primo com $p \equiv 3 \pmod{4}$ e considere-se a, com $a \perp p$, um resíduo quadrático. Mostre que $a^{(p+1)/4}$ é uma raíz quadrada de a módulo p. (Sugestão: use o critério de Euler.)

98. Use a lei da reciprocidade quadrática de Gauss para mostrar que, para p primo com ≥ 5,

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{se } p \equiv 1, 11 \pmod{12} \\ -1 & \text{se } p \equiv 5, 7 \pmod{12} \end{cases}$$

99. Use a lei da reciprocidade quadrática para caracterizar os primos p, com $p > 5$, para os quais 5 é resíduo quadrático. (Sugestão: inspire-se no exercício anterior.)

100. Mostre que 7 é um resíduo quadrático módulo um primo ímpar p diferente de 7 se, e somente se, p é congruente com 1, 3, 9, 19, 25 ou 27 módulo 28. (Sugestão: inspire-se nos exercícios anteriores.)

101. Sejam m e n números naturais ímpares.

    (a) Mostre que $\frac{mn-1}{2}$ tem a mesma paridade que $\frac{m-1}{2} + \frac{n-1}{2}$.

    (b) Mostre que $\frac{m^2n^2-1}{8}$ tem a mesma paridade que $\frac{m^2-1}{8} + \frac{n^2-1}{8}$.

102. Calcule o símbolo de Jacobi $\left(\frac{123}{917}\right)$. Deste cálculo pode concluir que 123 é resíduo módulo 917 ou que 123 é não resíduo quadrático módulo 917?

103. Calcule os seguintes símbolos de Legendre sem fatorizar números (excetuando fatores que são potências de 2): $\left(\frac{91}{167}\right)$, $\left(\frac{1801}{8191}\right)$, $\left(\frac{3083}{3911}\right)$ e $\left(\frac{43691}{65537}\right)$.

104. Usando o critério de Euler, calcule $4^{48} \pmod{97}$. Note que 97 é primo.

105. Mostre que a equação $x^2 \equiv 5 \pmod{2^{13}-1}$ tem duas soluções nos naturais x com $x < 2^{13}$. (Note que $2^{13} - 1$ é um número primo.)

106. Seja p um número primo ímpar. Use o facto do grupo $(\mathbb{Z}/p\mathbb{Z})^*$ ser cíclico para mostrar diretamente que $\left(\frac{-3}{p}\right) = 1$ quando $p \equiv 1 \pmod{3}$. (Sugestão: há um elemento $c \in (\mathbb{Z}/p\mathbb{Z})^*$ de ordem 3 (justifique); mostre que $(2c+1)^2 = -3$.)

107. Seja p primo ímpar tal que $p \equiv 1 \pmod{5}$. Mostre diretamente que $\left(\frac{5}{p}\right) = 1$ pelo método do exercício anterior. (Sugestão: tome-se $c \in (\mathbb{Z}/p\mathbb{Z})^*$ de ordem 5 e mostre que $(c + c^4)^2 + (c + c^4) - 1 = 0$, etc.)

108. Um primo de Mersenne é um primo da forma $2^n - 1$, com n número natural.

    (a) Mostre que se $2^n - 1$ é primo então n é primo.

    (b) Seja p um primo ímpar tal que $p \equiv 3 \pmod{4}$. Suponha também que $2p + 1$ primo. Mostre que $2^p \equiv 1 \pmod{2p + 1}$. (Sugestão: calcule $\left(\frac{2}{2p+1}\right)$ de duas formas distintas.)

    (c) Mostre que $2^{251} - 1$ não é primo de Mersenne.

109. Mostre que 3 é um não resíduo quadrático módulo os primos de Mersenne maiores do que 3.

110. Seja p um primo ímpar. Mostre que o produto P de todos os resíduos quadráticos $(\mathrm{mod}\ p)$ satisfaz $P \equiv (-1)^{(p+1)/2} (\mathrm{mod}\ p)$. [Sugestão: se g é raíz primitiva módulo p, então g^2, g^4, g^6, ..., g^{p-1} são os resíduos quadráticos módulo p.]

111. (a) Seja K um corpo, $b \in K$ e $n \in \mathbb{N}$ ímpar. Mostre que

$$b^n + 1 = (b+1)(b^{n-1} - b^{n-2} + \ldots b^2 - b + 1).$$

(b) Um *primo de Fermat* é um primo da forma $2^n + 1$, com $n \in \mathbb{N}$. Mostre que se $2^n + 1$ é um primo de Fermat então n é uma potência de 2.

(c) Seja $F_n = 2^{2^n} + 1$. Fermat conjeturou que todos os números desta forma são primos. De facto, F_0, F_1, F_2, F_3 e F_4 são primos (calcule-os!). Mas F_5 não é primo (vá à Wikipédia para ver a fatorização de F_5 obtida por Euler). Não se sabe se há mais primos de Fermat.

112. Seja p um primo de Fermat.

(a) Mostre que cada não resíduo quadrático módulo p é um gerador de $(\mathbb{Z}/p\mathbb{Z})^*$.

(b) Mostre que 5 é gerador de $(\mathbb{Z}/p\mathbb{Z})^*$, exceto quando $p = 5$.

113. Seja a um inteiro positivo e p e q primos ímpares com $p \perp a$ e $q \perp a$ tais que $p + q \equiv 0 \pmod{4a}$.

(a) Mostre primeiro que se a é ímpar, então $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.

(b) Mostre que $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.

114. (a) Dado um número natural k, então $\left(\frac{-3}{6k-1}\right) = -1$.

(b) Seja n um número inteiro. Dado um número natural k, mostre que $6k - 1$ não divide $n^2 + n + 1$. (Note que $4n^2 + 4n + 4 = (2n+1)^2 + 3$.)

115. Neste exercício use um computador (por exemplo, o programa SAGE).

(a) Aplique o teste de Solovay-Strassen ao número 56052361 para várias bases. Que conclusão é que pode tirar?

(b) Aplique o teste de Solovay-Strassen ao número 2301745249 para várias bases. Que conclusão é que pode tirar?

(c) Aplique o teste de Solovay-Strassen ao número 7427466391 para várias bases. Que conclusão é que pode tirar?

116. Mostre que de quatro inteiros consecutivos, pelo menos um deles não é soma de dois quadrados. (Sugestão: considere os quadrados módulo 8.)

117. Seja dado $\alpha \in \mathbb{R}$, $n \in \mathbb{N}$ e δ um real positivo. Suponha que a desigualdade

$$\left|\alpha - \frac{a}{b}\right| < \frac{\delta}{b^n}$$

não tem soluções racionais $\frac{a}{b}$. Então, se ε é um número real positivo, a desigualdade

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{b^{n+\varepsilon}}$$

tem apenas um número finito de soluções racionais $\frac{a}{b}$.

118. Encontrar o número racional representado sob forma de fração continuada de cada item a seguir (apresente a resposta em fração reduzida): $[3,1]$, $[1,1,1]$, $[0,6,5]$, $[1,2,3,4]$ e $[3,7,15,1]$.

119. Exprima os seguintes números racionais sob a forma de fração continuada simples: $11/7$, $-37/5$, $114/235$ e $-51/23$.

120. Este exercício tem por objetivo mostrar que cada número racional pode ser representado exatamente de duas maneiras por uma fração continuada simples (finita). (No que se segue, as frações continuadas são simples.)

    (a) Para cada fração continuada simples do exercício 118, exiba outra fração continuada que represente o mesmo racional. (P. ex., $[3,1] = [4]$.)

    (b) Mostre que $[a_0, a_1, \ldots, a_{m-1}, a_m + 1] = [a_0, a_1, \ldots, a_{m-1}, a_m, 1]$.

    (c) Mostre que se $m \geq 2$ então $\lfloor [a_0, a_1, a_2 \ldots, a_m] \rfloor = a_0$.

    (d) Mostre que se $[a_0, a_1, \ldots, a_m, 1] = [b_0, b_1, \ldots, b_n, 1]$ $(\neq 1)$, então $m = n$ e $a_i = b_i$ para todo $0 \leq i \leq n$.

    (e) Conclua que cada número racional tem exatamente duas representação como fração continuada simples.

121. Seja dada uma fração continuada $[a_0, a_1, \ldots, a_n]$, com $a_0 > 0$. Mostre que, para todo $n \in \mathbb{N}$, $\frac{p_n}{p_{n-1}} = [a_n, a_{n-1}, \ldots, a_1, a_0]$ e $[a_n, a_{n-1}, \ldots, a_2, a_1] = \frac{q_n}{q_{n-1}}$.

122. Na notação da aula teórica, mostre que

$$p_n = \det \begin{bmatrix} a_0 & -1 & 0 & \ldots & 0 & 0 \\ 1 & a_1 & -1 & \ldots & 0 & 0 \\ . & . & . & \ldots & . & . \\ 0 & 0 & 0 & \ldots & a_{n-1} & -1 \\ 0 & 0 & 0 & \ldots & 1 & a_n \end{bmatrix}$$

    (Sugestão: desenvolva o determinante através da última coluna.) Mostre também que, omitindo-se a primeira linha e a primeira coluna, se obtém uma fórmula para q_n.

123. A representação do número de Napier e em fração continuada infinita simples é: $[2,1,2,1,1,4,1,1,6,1,1,\ldots]$. Encontre os primeiros seis convergentes desta fração continuada.

124. Calcule os irracionais quadráticos dados por $[\overline{1}]$, $[2,\overline{1,2,1}]$ e $[4,\overline{2,1,3,1,2,8}]$.

125. Determine as frações continuadas simples infinitas que representam os números irracionais: $\sqrt{5}$, $\sqrt{6}$, $\frac{1+\sqrt{5}}{2}$, $\sqrt{10}$, $\sqrt{13}$, $\sqrt{14}$ e $\sqrt{17}$, $\frac{1+\sqrt{13}}{2}$.

126. Suponha que π é dado por 3,1415926 ..., correto à sétima casa decimal. Calcule os quatro primeiros convergentes de π (i.e., os convergentes c_0, c_1, c_2 e c_3 de π).

127. Uma fração continuada simples finita $[a_0, a_1, \ldots, a_n]$ diz-se simétrica se $a_i = a_{n-i}$, para todo o $0 \leq i \leq n$. Por exemplo, $[2, 1, 5, 1, 2]$ é simétrica. Mostre que se o número racional $\frac{r}{s}$ tem representação simétrica (onde $r \in \mathbb{Z}$, $s \in \mathbb{N}$ e $r \perp s$), então $r \mid (s^2 + (-1)^{n+1})$. (Sugestão: note que $p_n = r$, $q_n = s$ e utilize o exercício 121.)

128. Tome-se d um número natural que não seja um quadrado dum número inteiro. A equação de Pell é a equação $x^2 - dy^2 = 1$. A solução trivial da equação nos inteiros não negativos é $x = 1$ e $y = 0$. Neste exercício vamos ver que a equação de Pell tem solução não trivial (de facto, tem uma infinidade delas) e daremos um método para a(s) calcular.

    Admita-se que $\sqrt{d} = [a_0, \overline{a_1, \ldots, a_h}]$ ($h \in \mathbb{N}$) e seja $\theta_1 = [\overline{a_1, \ldots, a_h}]$. Tome-se n *ímpar* da forma $kh - 1$, onde $k \in \mathbb{N}$.

    (a) Mostre que $p_n = q_{n+1} - a_0 q_n$ e $p_{n+1} - a_0 p_n = q_n d$. [Sugestão: note que $\sqrt{d} = (p_{n+1}\theta_1 + p_n)/(q_{n+1}\theta_1 + q_n)$.]

    (b) Mostre que $p_n^2 - q_n^2 d = 1$. [Sugestão: elimine a_0.]

    (c) Encontre duas soluções não triviais para $x^2 - 5y^2 = 1$ e $x^2 - 6y^2 = 1$.

    (d) Encontre uma solução não trivial para $x^2 - 10y^2 = 1$, $x^2 - 13y^2 = 1$, $x^2 - 14y^2 = 1$, $x^2 - 17y^2 = 1$ e $x^2 - 19y^2 = 1$.

129. Mostre que toda a fração continuada simples infinita periódica representa um número irracional quadrático.

130. Seja E a seguinte curva elíptica sobre os racionais: $y^2 = x^3 + 17$. Considere os pontos $P = (-1, 4)$ e $Q = (2, 5)$.

    (a) Verifique que estes pontos estão na curva

    (b) Calcule $P + Q$ e $P - Q$.

    (c) Calcule $2Q$.

131. Uma solução racional da equação $y^2 = x^3 - 2$ é $(3, 5)$. Encontre uma solução racional com $x \neq 3$ considerendo a linha tangente a este ponto e computando o segundo ponto de interseção.

132. Seja E a seguinte curva elíptica sobre o corpo $\mathbb{Z}/13\mathbb{Z}$: $y^2 = x^3 + 3x + 8$.

    (a) Verifique que os pontos $(1, 5)$, $(1, 8)$ e $(9, 7)$ estão na curva.

(b) Liste os nove elementos de $E(\mathbb{Z}/13\mathbb{Z})$. [Sugestão: para facilitar as contas (1) ache os quadrados de $\mathbb{Z}/13\mathbb{Z}$; (2) percorra x com os valores de $\mathbb{Z}/13\mathbb{Z}$ e veja quando os valores x^3+3x+8 são quadrados; (3) não se esqueça do $\mathcal{O}$.]

(c) Calcule $(1,8)+(9,7)$ e $(1,5)+(1,8)$.

133. Seja E a seguinte curva elíptica sobre os racionais: $y^2 = x^3 - 2x + 4$. Considere os pontos $P = (0,2)$ e $Q = (1/4, 15/8)$.

(a) Verifique que estes pontos estão na curva.

(b) Calcule $P+Q$. Interprete o resultado geometricamente.

134. Seja E a curva elíptica sobre o corpo finito $K = \mathbb{Z}/5\mathbb{Z}$ definida pela equação $y^2 = x^3 + x + 1$.

(a) Liste os nove elementos de $E(K)$.

(b) Qual a estrutura de $E(K)$ como produto de grupos cíclicos?

135. Seja E uma curva elíptica sobre $\mathbb{R}$. Mostre que o grupo $E(\mathbb{R})$ não é finitamente gerado.

136. Seja p um primo congruente com 2 módulo 3. Considere E_p a curva elíptica sobre o corpo finito $\mathbb{Z}/p\mathbb{Z}$ definida pela equação $y^2 = x^3 + 1$. O objetivo deste exercício é demonstrar que a cardinalidade de E_p é $p+1$.

(a) Mostre que a aplicação de $(\mathbb{Z}/p\mathbb{Z})^*$ para si próprio dada por $x \rightsquigarrow x^3$ é sobrejetiva. (Sugestão: use o pequeno teorema de Fermat.)

(b) Demonstre o objetivo deste exercício tendo em atenção que a aplicação de $\mathbb{Z}/p\mathbb{Z}$ para si próprio dada por $x \rightsquigarrow x^3 + 1$ é uma bijeção.

137. Suponha que a equação $y^2 = x^3 + ax + b$, com $a, b \in \mathbb{Q}$, define uma curva elíptica. Mostre que existe outra equação $y^2 = x^3 + Ax + B$, com $A, B \in \mathbb{Z}$ cujas soluções (racionais) estão em bijeção com as soluções (racionais) de $y^2 = x^3 + ax + b$.

Primeiro trabalho extra

Esta sequência de exercícios culmina com a demonstração de que $\zeta(z) \neq 0$ para $z \neq 1$ na reta vertical $Re(z) = 1$.

(a) Dado um real positivo r e $\theta \in \mathbb{R}$, mostre que $|1 - re^{i\theta}|^2 = 1 - 2r\cos\theta + r^2$.

(b) Mostre que para $0 < r < 1$ se tem $|(1-re^{i\theta})^4(1-re^{2i\theta})^2| \leq \frac{1}{(1-r)^3}$. Sugestão: ponha $u = \cos\theta$ e considere a função

$$g(u) := (1 + r^2 - 2ru)^2(1 + r^2 + 2r - 4ru^2)$$

para $u \in [-1, 1]$. Mostre que a função h dada por $u \rightsquigarrow \ln g(u)$ atinge em $-1 \leq u \leq 1$ o máximo em $u = -\frac{1}{2}$. Para ver isto, ache $h'(u)$ e calcule $h'(-\frac{1}{2})$ e $h'(1)$.

(c) Mostre que para cada número primo p se tem

$$\left|\left(1 - \frac{1}{p^x}\right)^3 \left(1 - \frac{1}{p^{x+iy}}\right)^4 \left(1 - \frac{1}{p^{x+2iy}}\right)^2\right| \leq 1,$$

sempre que $x, y \in \mathbb{R}$ com $x > 1$. Sugestão: use a alínea anterior com $\frac{1}{p^x} = r$ e $\frac{1}{p^{iy}} = e^{i\theta}$.

(d) Mostre que se tem $|\zeta(x)^3\zeta(x + iy)^4\zeta(x + 2iy)^2| \geq 1$ sempre que $x, y \in \mathbb{R}$ e $x > 1$. Sugestão: use a alínea anterior e a fórmula do produto de Euler.

(e) Mostre que se tem $|(x - 1)\zeta(x)|^3 \left|\frac{\zeta(x+iy)}{x-1}\right|^4 |\zeta(x + 2iy)|^2 \geq \frac{1}{x-1}$ sempre que $x, y \in \mathbb{R}$ e $x > 1$.

(f) Mostre que $\zeta(1 + iy) \neq 0$ para todo o número real y não nulo. Sugestão: suponha que $\zeta(1 + iy_0) = 0$, para certo $y_0 \in \mathbb{R} \setminus \{0\}$ e use a alínea anterior com $y = y_0$, fazendo $x \to 1^+$, de modo a chegar a uma contradição.

Segundo trabalho extra

Nesta sequência de exercícios mostramos que os números que ocorrem no algoritmo estendido de Euclides estão limitados adequadamente (ver a última alínea abaixo) e que, portanto, o algoritmo estendido também é eficiente.

Fixamos a e b números naturais com $a > b$ e $b \nmid a$. Ponha-se $r_0 = a$, $r_1 = b$, $s_0 = 1$, $s_1 = 0$, $t_0 = 0$ e $t_1 = 1$ e, recursivamente, $r_{i+1} = r_{i-1} - q_i r_i$, $s_{i+1} = s_{i-1} - q_i s_i$ e $t_{i+1} = t_{i-1} - q_i t_i$ até se atingir um passo k tal que $r_{k+1} = 0$ (aqui, q_i e r_{i+1} são, respetivamente, o cociente e o resto da divisão de r_{i-1} por r_i). Como sabemos, $\mathrm{mdc}(a, b) = r_k$.

1. Mostre que $s_i s_{i+1} \leq 0$ e $t_i t_{i+1} \leq 0$, para todo i com $0 \leq i \leq k$. (Proceda indutivamente.)

2. Mostre que $|s_i| \leq |s_{i+1}|$ and $|t_i| \leq |t_{i+1}|$ para $1 \leq i \leq k$.

3. Mostre que $as_i + bt_i = r_i$, para todo i com $0 \leq i \leq k+1$. (Note, em particular, que $as_k + bt_k = \mathrm{mdc}(a, b)$ e que $as_{k+1} + bt_{k+1} = 0$.)

4. Para cada i tal que $1 \leq i \leq k+1$ considere-se a matriz de 2x2,

$$A_i := \begin{bmatrix} s_{i-1} & s_i \\ t_{i-1} & t_i \end{bmatrix}$$

   Mostre que, para todo i com $1 \leq i \leq k$, se tem

$$A_{i+1} = A_i \begin{bmatrix} 0 & 1 \\ 1 & -q_i \end{bmatrix}$$

5. Mostre que, para todo i com $1 \leq i \leq k+1$, se tem $det(A_i) = (-1)^{i-1}$.

6. Mostre que $s_{k+1} \neq 0$, $t_{k+1} \neq 0$ e que $|s_{k+1}| \perp |t_{k+1}|$. Sugestão: para a co-primalidade, ponha $i = k+1$ na alínea anterior.

7. Mostre que $s_{k+1} \mid b$ e que $t_{k+1} \mid a$. Mostre também que $\left|\frac{b}{s_{k+1}}\right| = \left|\frac{a}{t_{k+1}}\right|$.

8. Seja d o valor comum da alínea anterior. Mostre que $d = \mathrm{mdc}(a, b)$. Sugestão: calcule $mdc(|s_{k+1}|, |t_{k+1}|)$.

9. Mostre que $|s_i| \leq \frac{b}{\mathrm{mdc}(a,b)}$ e $|t_i| \leq \frac{a}{\mathrm{mdc}(a,b)}$ para $0 \leq i \leq k+1$. (Use as alíneas 2, 7 e 8.)

Terceiro trabalho extra

Os quatro exercícios desta folha mostram que existem raízes primitivas módulo n ($n > 1$) se, e somente se, n é 2, 4, p^k ou $2p^k$ (com p primo ímpar e $k \in \mathbb{N}$).

1. Seja p um número primo ímpar e g uma raíz primitiva módulo p. Suponha que $g^{p-1} \equiv 1 \pmod{p^2}$. Mostre que $h := (p+1)g$ é uma raíz primitiva módulo p tal que $h^{p-1} \not\equiv 1 \pmod{p^2}$.

2. Seja p um primo ímpar e $k \in \mathbb{N}$ com $k > 1$.

   (a) Dado $a \in \mathbb{Z}$, mostre que $(1+ap)^{p^{k-2}} \equiv 1 + ap^{k-1} \pmod{p^k}$. (Sugestão: por indução em k usando o exercício 40.)

   (b) Dado $a \in \mathbb{Z}$ tal que $a \perp p$, mostre que a ordem de $1+ap$ módulo p^k é p^{k-1}.

   (c) Seja g uma raíz primitiva módulo p tal que $g^{p-1} \not\equiv 1 \pmod{p^2}$. Mostre que g é raíz primitiva módulo p^k. (Sugestão: seja r a ordem de g módulo p^k. Mostre que $(p-1)|r$ e $p^{k-1}|r$.)

3. Seja $k \in \mathbb{N}$ e p um primo ímpar. Considere-se g uma raíz primitiva módulo p^k. Mostre que ou g ou $g+p^k$ é raíz primitiva módulo $2p^k$. (Sugestão: um dos números g ou $g+p^k$ é ímpar.)

4. Mostre que se na fatorização de n aparecem dois primos ímpares distintos ou um primo ímpar e o fator 4 então todos os elementos de $(\mathbb{Z}/n\mathbb{Z})^*$ têm ordem estritamente menor do que $\varphi(n)$. Sugestão: se a fatorização de n é $\prod_{i=1}^{k} p_i^{r_i}$ então $\operatorname{mmc}(\varphi(p_1^{r_1}), \ldots, \varphi(p_k^{r_k})) < \varphi(n)$ porque pelo menos dois dos fatores $\varphi(p_i^{r_i})$ é par.

Os exercícios 1 e 2(c) acima mostram que existem raízes primitivas módulo p^k e o exercício 3 mostra que existem raízes primitivas módulo $2p^k$ (p primo ímpar e $k \in \mathbb{N}$). Verifica-se facilmente que existem raízes primitivas módulo 2 e módulo 4. O exercício 81(c) mostra que não existem raízes primitivas módulo 2^k, com $k \geq 3$. Finalmente, pelo exercício 4 acima, nos restantes casos não existem raízes primitivas.

Quarto trabalho extra

Num primeiro exercício vamos caracterizar os *triplos pitagóricos*, isto é os triplos de números naturais x, y e z tais que $x^2 + y^2 = z^2$. Fixamos um triplo pitagórico x, y e z com $x \perp y$, $x \perp z$ e $y \perp z$.

(a) Mostre que x e y não têm a mesma paridade. (Sugestão: para ver que não podem ser ambos ímpares considere a igualdade pitagórica módulo 4.)

(b) *A partir de agora, e sem perda de generalidade, supomos que x é ímpar e y é par.* Mostre que $\mathrm{mdc}(z+x, z-x) = 2$.

(c) Mostre que $z+x = 2a^2$, $z-x = 2b^2$ e $y = 2ab$ para certos naturais a e b com $a \perp b$. (Sugestão: note que $(z+x)(z-x) = y^2$.)

(d) Conclua que os triplos pitagóricos (com $x \perp y$, $x \perp z$ e $y \perp z$) têm exatamente a forma $x = a^2 - b^2$, $y = 2ab$ e $z = a^2 + b^2$, onde $a \perp b$ e a e b são de paridades opostas.

(e) Diga quais são os primeiros quatro triplos pitagóricos (i.e., com os valores mais baixos de z).

(f) E se x, y e z não forem primos dois a dois?

De seguida, vamos usar esta caracterização dos triplos pitagóricos para mostrar que a equação $x^4 + y^4 = z^2$ não tem soluções nos números naturais. Note que, em particular, se demonstra que a equação de Fermat de expoente quatro não tem soluções. Suponha, com vista a um absurdo, que $x^4 + y^4 = z^2$ com $x, y, z \in \mathbb{N}$ e z mínimo nestas condições. É claro que x, y e z são co-primos dois a dois. Pelo acima, existem $a, b \in \mathbb{N}$ tais que $x^2 = a^2 - b^2$, $y^2 = 2ab$ e $z = a^2 + b^2$ com $a \perp b$ e de paridades opostas.

(a) Mostre que b é par. (Sugestão: caso contrário obtém-se uma contradição raciocinando módulo 4.)

(b) Mostre que existem $c, d \in \mathbb{N}$ tais que $a = c^2 + d^2$, $b = 2cd$ e $x = c^2 - d^2$ com $c \perp d$.

(c) Mostre que $y'^2 = (c^2 + d^2)cd$, onde $y = 2y'$.

(d) Da alínea anterior, conclua que c, d e $c^2 + d^2$ são quadrados inteiros. (Sugestão: note que c, d e $c^2 + d^2$ são co-primos entre si.)

(e) Se $c = e^2$, $d = f^2$ e $c^2 + d^2 = g^2$, mostre que $g^2 < z$ e conclua o resultado desejado.

Quinto trabalho extra

O objetivo dos exercícios abaixo é caracterizar a forma das frações continuadas simples infinitas de $\sqrt{d}$, onde d é um número natural que não é um quadrado inteiro. O teorema de Lagrange sobre irracionais quadráticos é utilizado em 1(d) abaixo.

1. Seja θ um irracional quadrático com $\theta > 1$ e $-1 < \theta^* < 0$. (Se $\theta = a + b\sqrt{d}$, com $a, b, d \in \mathbb{Q}$, então $\theta^* = a - b\sqrt{d}$.) Para cada $n \in \mathbb{N}_0$ seja θ_n com $\theta = [a_0, a_1, \ldots, a_{n-1}, \theta_n]$ e considere-se $\gamma_n = (\theta_n)^*$.

   (a) Mostre que para todo $n \in \mathbb{N}_0$, $-1 < \gamma_n < 0$. [Sugestão: por indução, notando que $\theta_n = a_n + (1/\theta_{n+1})$ e, consequentemente, $\gamma_n = a_n + (1/\gamma_{n+1})$.]

   (b) Mostre que, para todo $n \in \mathbb{N}_0$, $a_n = \lfloor -1/\gamma_{n+1} \rfloor$.

   (c) Mostre que se $\theta_n = \theta_{n+h}$ $(n, h \in \mathbb{N})$, então $a_{n-1} = a_{n-1+h}$. Conclua que $\theta_{n-1} = \theta_{n-1+h}$.

   (d) Mostre que θ tem uma fração continuada puramente periódica.

2. Tome-se d um número natural que não seja um quadrado perfeito.

   (a) Mostre que os números reais $\sqrt{d} + \lfloor \sqrt{d} \rfloor$ e $(\sqrt{d} - \lfloor \sqrt{d} \rfloor)^{-1}$ têm frações continuadas puramente periódicas.

   (b) Mostre que $\sqrt{d}$ é da forma $[a_0, \overline{a_1, \ldots, a_h}]$ (para certo $h \in \mathbb{N}$).