

Matemática Discreta

————— Exercícios - Teoria de Números ————— página 1 —————

1. Sejam  $a, b \in \mathbb{Z}$  tais que  $a < 0$  e  $b > 0$ . Sejam  $q, r, q_1, r_1 \in \mathbb{Z}$  tais que  $-a = bq_1 + r_1$  e  $0 \leq r_1 < b$ ,  $a = bq + r$  e  $0 \leq r < b$ . Mostre que:
  - (a) se  $r_1 = 0$  então  $q = -q_1$  e  $r = 0$ .
  - (b) se  $r_1 \neq 0$  então  $q = -(q_1 + 1)$  e  $r = b - r_1$ .
2. Determine o quociente e o resto na divisão de :
  - (a) 310156 por 197;
  - (b) 32 por 45;
  - (c) 0 por 28;
  - (d) -19 por 6;
  - (e) -234 por -9.
3. Mostre que se  $a$  e  $b$  são inteiros e  $b > 0$ , então existem, e são únicos,  $q$  e  $r$  inteiros tais que  $a = qb + r$  e  $0 \leq r < b$ .
4. Utilizando o Algoritmo da Divisão, mostre que
  - (a) o quadrado de um inteiro é da forma  $3k$  ou  $3k + 1$ , para certo inteiro não negativo  $k$ ;
  - (b)  $3a^2 - 1$  não é um quadrado perfeito, para todo o inteiro  $a$ .
5. Na divisão de 392 por 45, determine:
  - (a) o maior inteiro que se pode somar ao dividendo sem alterar o quociente;
  - (b) o maior inteiro que se pode subtrair ao dividendo sem alterar o quociente.
6. Verifique que, para todo o inteiro  $n \geq 1$ ,  $\frac{n(n+1)(2n+1)}{6}$  é um inteiro.
7. Dê exemplos de inteiros  $a, b$  e  $c$  tais que  $a \mid bc$  mas  $a \nmid b$  e  $a \nmid c$ .
8. Mostre que, se  $a \mid b$ , então  $(-a) \mid b$ ,  $a \mid (-b)$  e  $(-a) \mid (-b)$ .
9. Mostre que, se  $a \mid (2x - 3y)$  e  $a \mid (4x - 5y)$ , então  $a \mid y$ .
10. Justifique que, dados dois inteiros quaisquer  $a$  e  $b$ , os inteiros  $a$  e  $a + 2b$  têm a mesma paridade.
11. Mostre que, para todo o inteiro  $a$ , um dos inteiros  $a$  e  $a + 2$  ou  $a + 4$  é divisível por 3.
12. Recorrendo ao Princípio de Indução, verifique que são verdadeiras as seguintes afirmações, para  $n \geq 1$ :
  - (a)  $8 \mid (5^{2n} + 7)$ ; [Sugestão: Observe que  $5^{2(n+1)} + 7$  pode ser escrito como  $5^2(5^{2n-2} + 7) + (7 - 5^2 \times 7)$ .]
  - (b)  $15 \mid (2^{4n} - 1)$ .
13. Verifique que, se  $a$  e  $b$  são ambos inteiros ímpares, então  $16 \mid (a^4 + b^4 - 2)$ .
14. Prove que o produto de quatro inteiros consecutivos é divisível por 24.
15. Mostre que  $\text{m.d.c.}(a, b) = 1 = \text{m.d.c.}(a, c)$  se e só se  $\text{m.d.c.}(a, bc) = 1$ .
16. Mostre que, dado um inteiro  $a \neq 0$ , se tem  $\text{m.d.c.}(a, 0) = |a| = \text{m.d.c.}(a, a)$  e  $\text{m.d.c.}(a, 1) = 1$ .

Matemática Discreta

Exercícios - Teoria de Números página 2

17. Verifique que, dados um inteiro positivo  $n$  e um inteiro  $a$ ,  $\text{m.d.c.}(a, a+n)$  divide  $n$ . Conclua que dois inteiros consecutivos são primos entre si.
18. Sejam  $a$  e  $b$  inteiros não simultaneamente nulos. Mostre que
  - (a) existem inteiros  $x$  e  $y$  tais que  $c = ax + by$  se e só se  $\text{m.d.c.}(a, b) \mid c$ .
  - (b) se existem inteiros  $x$  e  $y$  tais que  $ax + by = \text{m.d.c.}(a, b)$ , então  $\text{m.d.c.}(x, y) = 1$ .
19. Mostre que, se  $a = qb + r$ , então  $\text{m.d.c.}(a, b) = \text{m.d.c.}(b, r)$ .
20. Utilizando o Algoritmo de Euclides, determine o máximo divisor comum de cada par de inteiros  $a$  e  $b$  e escreva-o como combinação linear de  $a$  e  $b$ :
  - (a)  $a = 1001, b = 357$ ;
  - (b)  $a = 1001, b = 33$ ;
  - (c)  $a = 56, b = 126$ ;
  - (d)  $a = -90, b = 1386$ ;
  - (e)  $a = -2860, b = -2310$ .
21. Exprima o  $\text{m.d.c.}(2, 3)$  como combinação linear de 2 e 3, de dois modos distintos.
22. Determine, usando o Algoritmo de Euclides, inteiros  $x$  e  $y$  que satisfaçam:
  - (a)  $\text{m.d.c.}(56, 72) = 56x + 72y$ ;
  - (b)  $\text{m.d.c.}(24, 138) = 24x + 138y$ .
23. Sabendo que  $\text{m.d.c.}(a, b) = 1$ , conclua que:
  - (a)  $\text{m.d.c.}(a+b, a-b) = 1$  ou  $\text{m.d.c.}(a+b, a-b) = 2$ ;
  - (b)  $\text{m.d.c.}(a+b, ab) = 1$ .
24. Determine o menor inteiro positivo  $k$  da forma  $k = 22x + 55y$ , onde  $x$  e  $y$  são inteiros.
25. Sejam  $a, b \in \mathbb{Z}$ ,  $a \neq 0$  e  $b \neq 0$ . Mostre que:
  - (a) se  $a \mid b$ , então  $|a| = \text{m.d.c.}(a, b)$  e  $|b| = \text{m.m.c.}(a, b)$ ;
  - (b) se  $d = \text{m.d.c.}(a, b)$ , então  $|k|d = \text{m.d.c.}(ka, kb)$ , para qualquer  $k \in \mathbb{Z}$  e  $k \neq 0$ .
26. Sejam  $a$  e  $b$  inteiros não negativos. Verifique que as seguintes afirmações são verdadeiras:
  - (a) se  $a \neq 0$  ou  $b \neq 0$ , então  $\text{m.d.c.}(a, b) = \text{m.m.c.}(a, b)$  se e só se  $a = b$ .
  - (b) se  $k > 0$ , então  $\text{m.m.c.}(ka, kb) = k \times \text{m.m.c.}(a, b)$ ;
  - (c) se  $m$  é um múltiplo comum de  $a$  e  $b$ , então  $\text{m.m.c.}(a, b) \mid m$ . [Sugestão: Use o Algoritmo da Divisão para escrever  $m$  na forma  $qt + r$ , onde  $t = \text{m.m.c.}(a, b)$  e  $0 \leq r < t$ . Mostre que  $r$  é um múltiplo de  $a$  e  $b$ .]
27. Mostre que
  - (a) se  $p$  é primo e  $p \mid a_1 a_2 \dots a_n$ , então  $p \mid a_k$ , para algum  $k$  tal que  $1 \leq k \leq n$ ;
  - (b) se  $p, q_1, q_2, \dots, q_n$  são todos primos e  $p \mid q_1 q_2 \dots q_n$ , então  $p = q_k$ , para algum  $k$  tal que  $1 \leq k \leq n$ .

## Matemática Discreta

Exercícios - Teoria de Números ————— página 3 —————

28. Prove que

- (a) todo o primo da forma  $3n + 1$  é da forma  $6m + 1$  ( $m, n \in \mathbb{N}$ );
- (b) o único primo da forma  $n^3 - 1$  é o 7 ( $n \in \mathbb{N}$ ); [Sugestão: Escreva  $n^3 - 1$  como  $(n - 1)(n^2 + n + 1)$ .]
- (c) todo o inteiro da forma  $n^4 + 4$ , em que  $n > 1$ , é composto.

29. Fatorize os inteiros 105, 684, 1375 e 139 como produto de números primos.

30. Sejam  $m = p_1^{s_1} p_2^{s_2} \dots p_k^{s_k}$  e  $n = p_1^{t_1} p_2^{t_2} \dots p_k^{t_k}$ , em que  $p_1, p_2, \dots, p_k$  são primos distintos,  $s_i \geq 0$  para  $1 \leq i \leq k$  e  $t_i \geq 0$  para  $1 \leq i \leq k$ . Para cada  $i$ , sejam  $u_i = \min\{s_i, t_i\}$  e  $v_i = \max\{s_i, t_i\}$ . Prove que:

- (a)  $\text{m.d.c.}(m, n) = p_1^{u_1} p_2^{u_2} \dots p_k^{u_k}$ ;
- (b)  $\text{m.m.c.}(m, n) = p_1^{v_1} p_2^{v_2} \dots p_k^{v_k}$ .

31. Usando a fatorização de 507 e 1287 em fatores primos, determine  $\text{m.d.c.}(507, 1287)$  e  $\text{m.m.c.}(507, 1287)$ .32. Verifique que 701 é um número primo, testando todos os primos  $p \leq \sqrt{701}$  como possíveis divisores.33. Prove que  $\sqrt{p}$  é irracional para todo o primo  $p$ ;34. Mostre que se  $a \in \mathbb{N}$  e  $\sqrt[n]{a}$  é racional, então  $\sqrt[n]{a}$  é um inteiro.35. (a) Mostre que é condição necessária para que um inteiro  $p \neq 2$  seja primo que satisfaça  $p = 4n \pm 1$ ,  $n \in \mathbb{N}$ .

(b) Esta condição é também suficiente? Justifique.

36. Mostre que há uma infinidade de primos da forma  $6n + 5$ .

37. Quais das seguintes equações diofantinas têm solução?

- (a)  $6x + 51y = 22$ ;
- (b)  $33x + 14y = 115$ ;
- (c)  $14x + 35y = 93$ .

38. Determine as soluções inteiras das seguintes equações diofantinas:

- (a)  $56x + 72y = 40$ ;
- (b)  $24x + 138y = 18$ ;
- (c)  $221x + 35y = 11$ .

39. Determine as soluções inteiras positivas das seguintes equações diofantinas:

- (a)  $18x + 5y = 48$ ;
- (b)  $54x + 21y = 906$ ;
- (c)  $5x - 11y = 29$ .

40. Exprima 100 como soma de dois inteiros positivos de modo que o primeiro seja divisível por 7 e o segundo seja divisível por 11.

## Matemática Discreta

————— Exercícios - Teoria de Números ————— página 4 —————

41. Determine as soluções inteiras não negativas da equação  $39x + 26y = 104$ .
42. Justifique que a equação  $30x + 17y = 300$  tem soluções inteiras positivas.
43. De quantas maneiras se pode exprimir o número 4 como diferença de dois inteiros positivos, dos quais o primeiro é divisível por 8 e o segundo é múltiplo de 15? Indique três delas.
44. Determine dois inteiros, um positivo e outro negativo, cuja soma é 42 e tais que um deles é múltiplo de 126 e o outro é divisível por 56.
45. Diga, justificando, se é possível exprimir o número 104 como soma de dois inteiros positivos, tais que um deles é múltiplo de 64 e o outro é divisível por 11.
46. (a) Para que valores de  $x$  e de  $y$  se tem  $11x + 7y = 200$ ?  
(b) Para que valores encontrados em (a) se tem  $3x + y$  múltiplo de 3?
47. Determine, caso existam, o menor inteiro não negativo  $x$  e o menor inteiro não negativo  $y$  tais que  $55x - 121y = 329$ .
48. Determine, caso existam, as soluções  $(x, y)$  da equação  $297x + 349y = 3$ , tais que  $x, y \in \mathbb{Z}$ ,  $x \in ]-\infty, 557]$  e  $y \in ]-\infty, 417[$ .
49. Determine as soluções inteiras não negativas da equação  $39x + 26y = 104$ .
50. Um teatro amador cobra 1,80 euros de entrada a cada adulto e 75 cêntimos a cada criança. Num espetáculo, as receitas totais somaram 90 euros. Sabendo que estiveram presentes mais adultos do que crianças, diga quantas pessoas estiveram a assistir a esse espetáculo.
51. Um turista espanhol e um guia subiram a correr os degraus da pirâmide Keops perseguidos por um leão! O turista conseguia subir cinco degraus de uma só vez, o guia seis degraus e o leão sete degraus. A dada altura, o turista estava a um degrau do topo da pirâmide, o guia a nove degraus e o leão a dezanove degraus. Quantos degraus pode ter a pirâmide?
52. Tenho um certo número de pérolas. Se fizer 76 pulseiras com o mesmo número de pérolas, faltam-me 50 pérolas para fazer a 77<sup>a</sup> pulseira. Mas se fizer 78 pulseiras com o mesmo número de pérolas, uso a totalidade das pérolas que possuo. Qual o número mínimo de pérolas que tenho?
53. Quando morreu, a idade de um homem era  $\frac{1}{29}$  do ano do seu nascimento. Que idade tinha o homem em 1940?
54. Prove que
  - (a) se  $a \equiv b \pmod{n}$  e  $m \mid n$ , então  $a \equiv b \pmod{m}$ ;
  - (b) se  $a \equiv b \pmod{n}$  e  $c > 0$ , então  $ca \equiv cb \pmod{n}$ .
55. Dê um exemplo que mostre que  $a^2 \equiv b^2 \pmod{n}$  não implica que  $a \equiv b \pmod{n}$ .
56. Verifique que, se  $a \equiv b \pmod{n}$ , então  $\text{m.d.c.}(a, n) = \text{m.d.c.}(b, n)$ .
57. Para que valores de  $n$  se tem  $25 \equiv 4 \pmod{n}$  ?

Matemática Discreta

———— Exercícios - Teoria de Números ————— página 5 —————

58. Justifique, se é verdadeira ou falsa cada uma das afirmações seguintes:

- (a)  $91 \equiv 0 \pmod{7}$ ;
- (b)  $-2 \equiv 2 \pmod{8}$ ;
- (c)  $17 \not\equiv 13 \pmod{2}$ .

59. Verifique se:

- (a) o conjunto  $\{-12, -4, 11, 13, 22, 32, 91\}$  é um sistema completo de resíduos módulo 7;
- (b) o conjunto  $\{-2, -1, 0, 1, 2\}$  é um sistema completo de resíduos módulo 5.

60. Determine quais dos seguintes conjuntos são sistemas completos de resíduos módulo 4:

- (a)  $\{-2, -1, 0, 1\}$ ;
- (b)  $\{0, 4, 8, 12\}$ ;
- (c)  $\{-13, 4, 17, 13\}$ ;
- (d)  $\{-5, 0, 6, 22\}$ .

61. Determine um sistema completo de resíduos módulo 7 constituído apenas por números primos.

62. Justifique se, em  $\mathbb{Z}_6$ , é verdadeira ou falsa cada uma das seguintes afirmações:

- (a)  $[89]_6 + [13]_6 = [0]_6$  e  $[25]_6 \cap [16]_6 = [5]_6$ ;
- (b)  $[89]_6 + [13]_6 = [3]_6$  e  $[25]_6 \cap [16]_6 = \emptyset$ ;
- (c)  $[89]_6 + [13]_6 = [0]_6$  e  $[25]_6 \cap [16]_6 = \emptyset$ ;

63. Indique quatro inteiros, dois positivos e dois negativos, na classe  $[3]$ :

- (a) como elemento de  $\mathbb{Z}_5$ ;
- (b) como elemento de  $\mathbb{Z}_6$ .

64. Indique, justificando, caso existam, caso existam:

- (a) um inteiro primo  $x$  tal que  $x \in [-22]_{15} \cap [8]_{15}$ ;
- (b) dois elementos  $x, y$  em  $[20]_{15} \times ([39]_{15} + [-80]_{15})$  tais que  $-40 < x < 0$  e  $y > 80$ ;
- (c) um número primo  $x$  tal que  $x \equiv 6 \pmod{12}$ ;
- (d) dois elementos distintos em  $[-182]_9 \cap [20]_9$ ;
- (e) o maior número par  $n$  tal que  $-89 \equiv 5 \pmod{n}$ ;
- (f) o maior inteiro  $x$  par, não positivo, tal que  $x \equiv 50 \pmod{109}$ .

65. Indique os restos das divisões de  $2^{50}$  e  $41^{63}$  por 7.

66. Calcule o resto da divisão de  $4^{215}$  por 9.

67. Usando as propriedades das congruências, mostre que, para  $n \geq 1$ , se tem:

- (a) 7 divide  $5^{2n} + 3 \times 2^{5n-2}$ ;
- (b) 13 divide  $3^{n+2} + 4^{2n+1}$ .

## Matemática Discreta

————— Exercícios - Teoria de Números ————— página 6 —————

68. Na divisão por 5, um inteiro  $p$  admite resto 3. Qual é o resto da divisão de  $p^2 + 2p - 1$  por 5?
69. Prove que:
- (a) se  $a$  é um inteiro ímpar, então  $a^2 \equiv 1 \pmod{8}$ ;
  - (b) para todo o inteiro  $a$ ,  $a^3 \equiv 0, 1$  ou  $6 \pmod{7}$ ;
  - (c) para todo o inteiro  $a$ ,  $a^4 \equiv 0$  ou  $1 \pmod{5}$ ;
  - (d) para todo o inteiro  $a$  que não é divisível por 2 e por 3, tem-se  $a^2 \equiv 1 \pmod{24}$ .
70. Determine o resto da divisão de  $2357 \times 1036 + 499$  por 11.
71. Mostre que  $11^{10} \equiv 1 \pmod{100}$ .
72. Mostre que, para qualquer inteiro  $n$ ,  $n^3 - n = 3k$ , para certo inteiro  $k$ .
73. Prove que
- (a) dado um inteiro  $a$ , o dígito das unidades de  $a^2$  é 0, 1, 4, 5, 6 ou 9.
  - (b) qualquer um dos inteiros 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 pode ser o dígito das unidades de  $a^3$ , para algum inteiro  $a$ ;
  - (c) dado um inteiro  $a$ , o dígito das unidades de  $a^4$  é 0, 1, 5 ou 6.
74. Indique os dois últimos dígitos de  $9^{9^9}$ .
75. Trabalhando módulo 9 ou 11, indique os dígitos que faltam nos cálculos apresentados:
- (a)  $\overline{51840} + \overline{273581} = \overline{1418243x040}$ ;
  - (b)  $\overline{2x99561} = [3(523 + x)]^2$ ;
  - (c)  $\overline{246x} = \overline{x} \times 493$ ;
  - (d)  $512 \times \overline{1x53125} = 1000000000$ .
76. Deduza, no sistema decimal, o critério de divisibilidade por 6 e por 8.
77. Determine os algarismos  $x, y$  de modo que o inteiro  $\overline{3x5y}$  seja simultaneamente divisível por 4 e por 9.
78. Determine os dígitos  $x$  e  $y$  tais que o número  $34xx58y$  é simultaneamente divisível por 9 e por 11.
79. Determine os algarismos  $a$  e  $b$  tais que o número  $279a15b0$  é simultaneamente divisível por 4 e por 9.
80. Determine os algarismos  $a$  e  $b$  tais que o número  $\overline{56a21b}$  é simultaneamente divisível por 2 e por 11.
81. Resolva as seguintes congruências lineares:
- (a)  $25x \equiv 15 \pmod{29}$ ;
  - (b)  $5x \equiv 2 \pmod{26}$ ;
  - (c)  $140x \equiv 133 \pmod{301}$ ;

## Matemática Discreta

---

Exercícios - Teoria de Números

---

página 7

---

82. Diga, justificando, quais das congruências seguintes são solúveis e, para essas, indique a menor solução não negativa:
- (a)  $10x \equiv 14 \pmod{15}$ ;
  - (b)  $10x \equiv 14 \pmod{16}$ ;
  - (c)  $12x \equiv 7 \pmod{35}$ ;
  - (d)  $60x \equiv -30 \pmod{165}$ ;
83. Usando congruências, resolva a seguinte equação diofantina:  $4x + 51y = 9$ . [Sugestão:  $4x \equiv 9 \pmod{51} \Leftrightarrow x = 15 + 51t$  e  $51y \equiv 9 \pmod{4} \Leftrightarrow y = 3 + 4s$ . Encontre a relação entre  $s$  e  $t$ .]
84. Relativamente à congruência linear  $3x \equiv 2 \pmod{70}$ , determine, caso exista:
- (a) a maior solução negativa inferior a  $-96$ ;
  - (b) uma solução que seja um número primo.
85. Diga, justificando, se a congruência linear  $14x \equiv 18 \pmod{60}$  tem soluções pares.
86. Relativamente à congruência  $13x \equiv 17 \pmod{42}$ , determine, caso existam,
- (a) as soluções negativas superiores a  $-100$ ;
  - (b) uma solução par.
87. Relativamente à congruência linear  $16x \equiv 9 \pmod{11}$ , determine, justificando:
- (a) duas soluções que sejam números primos;
  - (b) duas soluções que sejam números pares;
  - (c) o conjunto das soluções do intervalo  $]-\infty, 337]$ .
88. Considere a congruência linear  $18x \equiv 9 \pmod{21}$ .
- (a) Verifique que a congruência linear dada admite solução.
  - (b) Quantas soluções tem a congruência linear  $18x \equiv 9 \pmod{21}$  no intervalo inteiro  $]-1, 80]$ ? Calcule-as.
89. Resolva os seguintes sistemas de congruências lineares:
- $$(a) \begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \end{cases} ; \quad (b) \begin{cases} 2x \equiv 1 \pmod{5} \\ 3x \equiv 9 \pmod{6} \\ 4x \equiv 1 \pmod{7} \\ 5x \equiv 9 \pmod{11} \end{cases} ; \quad (c) \begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{6} \\ x \equiv 4 \pmod{7} \end{cases} ;$$
- $$(d) \begin{cases} x \equiv 3 \pmod{11} \\ x \equiv 6 \pmod{8} \end{cases} ; \quad (e) \begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{5} \\ x \equiv 5 \pmod{7} \end{cases} .$$
90. Resolva os seguintes sistemas de congruências lineares:
- $$(a) \begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 4 \pmod{5} \\ x \equiv 1 \pmod{2} \end{cases} ; \quad (b) \begin{cases} 3x \equiv 2 \pmod{5} \\ 2x \equiv 4 \pmod{6} \\ x \equiv 1 \pmod{2} \end{cases} .$$

## Matemática Discreta

---

Exercícios - Teoria de Números

---

página 8

---

91. Utilizando o Teorema Chinês dos Restos, resolva a congruência  $17x \equiv 5 \pmod{42}$ .
92. Determine o menor inteiro  $a$  tal que  $2 \mid a$ ,  $3 \mid a + 1$ ,  $4 \mid a + 2$ ,  $5 \mid a + 3$  e  $6 \mid a + 4$ .
93. Quando se retiram 2, 3, 4, 5, 6 ovos de cada vez de um determinado cesto, ficam, respetivamente, 1, 2, 3, 4, 5 ovos no cesto. Ao retirar 7 ovos de uma só vez, não sobra qualquer ovo no cesto. Qual o menor número de ovos que o cesto pode conter?
94. Um bando de 17 piratas roubou um saco de moedas. Ao tentarem dividir igualmente por todos eles a fortuna roubada, deram conta que sobravam 3 moedas. Lutaram, para ver quem ficava com as três moedas e, nessa luta, morreu um pirata. Distribuíram, de novo, as moedas por todos e, desta vez, sobraram 10 moedas. Tendo havido nova luta, mais um pirata morreu. Desta vez, a fortuna pôde ser distribuída, na íntegra, por todos! Qual é o número mínimo de moedas que o saco roubado poderia ter contido?
95. Recorrendo ao Teorema Chinês dos Restos, determine as soluções inteiras de congruência linear  $19x \equiv 4 \pmod{84}$  que pertençam ao intervalo  $] - 200, 284]$ .
96. Um inteiro positivo  $a$  dividido por 5 dá resto 3 e dividido por 9 dá resto 4.
- (a) Determine o resto da divisão de  $a$  por 45.
  - (b) Calcule os inteiros positivos ímpares, compreendidos entre 100 e 300, que têm, na divisão por 45, o mesmo resto que  $a$ .
97. Determine os inteiros positivos  $x$  inferiores a 336 e tais que  $x \equiv 2 \pmod{8}$ ,  $x \equiv 1 \pmod{7}$  e  $x \equiv 2 \pmod{6}$ .
98. Aplicando o Teorema Chinês dos Restos, indique três inteiros  $n$ , dos quais um é negativo e dois são positivos, para os quais se tem, simultaneamente,  $3 \mid n$ ,  $5 \mid (n + 2)$  e o resto da divisão de  $n - 3$  por 9 é 6.
99. Recorrendo ao Teorema Chinês dos Restos, resolva a congruência linear  $14x \equiv 18 \pmod{60}$ .
100. Recorrendo ao Pequeno Teorema de Fermat, mostre que:
- (a)  $a^{21} \equiv a \pmod{15}$ , para todo o inteiro  $a$ ;
  - (b)  $a^{13} \equiv a \pmod{273}$ , para todo o inteiro  $a$ ;
  - (c)  $a^{12} \equiv 1 \pmod{35}$ , para todo o inteiro  $a$  tal que  $\text{m.d.c.}(a, 35) = 1$ .
101. Mostre que 60 divide  $a^4 + 59$  se  $\text{m.d.c.}(a, 30) = 1$ .
102. Se  $a \in \mathbb{Z}$  é tal que  $7 \nmid a$ , prove que  $a^3 + 1$  ou  $a^3 - 1$  é divisível por 7.
103. Seja  $p$  um número primo. Mostre que  $2 \times (p - 3)! \equiv -1 \pmod{p}$ .
104. Determine
- (a) o resto da divisão de  $15!$  por 17;
  - (b) o resto da divisão de  $2 \times 26!$  por 29.
105. Verifique que  $4 \times 29! + 5!$  é divisível por 31.
106. Considere a função de Euler  $\phi$ . Calcule  $\phi(420)$ ,  $\phi(1001)$ ,  $\phi(5040)$ .



Matemática Discreta

———— Exercícios - Teoria de Números ————— página 9 —————

107. Verifique que  $\phi(n+2) = \phi(n) + 2$ , para  $n = 12, 14, 20$ .
108. Verifique o Teorema de Euler para  $n = 10$  e  $a = 3$ .
109. Seja  $a \in \mathbb{Z}$  tal que  $\text{m.d.c.}(a, 15) = 1$ . Mostre que  $a^{17} \equiv a \pmod{15}$ :
- (a) recorrendo ao Pequeno Teorema de Fermat;
  - (b) recorrendo ao Teorema de Euler.
110. Quais os dois últimos dois dígitos na representação decimal de  $3^{256}$ ?
111. Mostre que se  $n$  é um número inteiro ímpar que não é múltiplo de 5 então  $n$  divide um inteiro cujos dígitos são todos iguais a 1.
112. Por que é que se tem  $\phi(2n) = \phi(n)$  para qualquer inteiro positivo ímpar  $n$ ?