MATEMÁTICA DISCRETA

Lic. Ciências da Computação

Exercícios de Teoria de Números - Divisibilidade

---

1. Sejam $a, b, c, d \in \mathbb{Z}$. Mostre que:
   (a) $1 \mid a, \quad a \mid a \quad$ e $\quad a \mid 0$;
   (b) $a \mid 1$ sse $a = \pm 1$;
   (c) $0 \mid a$ sse $a = 0$;
   (d) se $c \neq 0$, então $a \mid b$ sse $ac \mid bc$;
   (e) $a \mid b$ e $a \mid b + c$ implica que $a \mid c$;
   (f) se $ab \neq 0$ e $a \mid b$ e $b \mid a$, então $|a| = |b|$.
2. Sejam $a, x, y \in \mathbb{Z}$. Mostre que, se $a \mid (2x + 3y)$ e $a \mid (4x + 5y)$, então $a \mid y$.
3. Usando indução natural, mostre que $4 \mid 5^n - 1$ para qualquer $n \in \mathbb{N}$.
4. Calcule o quociente e o resto da divisão de a por b em cada caso:
   (a) $a = 29$ e $b = 4$;
   (b) $a = -29$ e $b = 4$;
   (c) $a = -29$ e $b = -4$;
   (d) $a = 29$ e $b = -4$;
   (e) $a = -1350$ e $b = 45$;
   (f) $a = -1351$ e $b = 45$;
   (g) $a = -1351$ e $b = -45$;
   (h) $a = 0$ e $b = -37$.
5. Sejam $a, b \in \mathbb{Z}$ e $b \neq 0$. Prove as afirmações seguintes.
   (a) m.d.c.$(a, b) =$ m.d.c.$(|a|, |b|) =$ m.d.c.(b, a).
   (b) se $b \mid a$, então m.d.c.$(a, b) = |b|$.
   (c) m.d.c.$(0, b) = |b|$.
6. Em cada caso, utilizando o algoritmo de Euclides, calcule o máximo divisor comum de a e b e escreva-o como combinação linear de a e b.
   (a) $a = 144$ e $b = 34$;
   (b) $a = 34$ e $b = 144$;
   (c) $a = 39$ e $b = 51$;
   (d) $a = -39$ e $b = -51$;
   (e) $a = -63$ e $b = -37$;
   (f) $a = -63$ e $b = 37$.

7. Resolva as seguintes equações no conjunto dos números inteiros:

   (a) $144x + 34y = 20$,
   (b) $39x + 51y = 7$,
   (c) $63x - 37y = 3$,
   (d) $63x + 37y = 3$,
   (e) $119x - 29y = 8$.

8. Sejam a e b inteiros não ambos nulos. Mostre que o conjunto

$$S = \{ax + by \mid x, y \in \mathbb{Z}\}$$

   é o conjunto de todos os múltiplos de m.d.c.(a, b).

9. Prove que o resto da divisão do quadrado de qualquer número inteiro por 4, ou é 0 ou é 1.

10. Seja $a \in \mathbb{Z}$. Mostre que $\frac{a(a^2+2)}{3} \in \mathbb{Z}$.

11. Utilizando o Algoritmo da Divisão, prove que:

   (a) um quadrado perfeito não é da forma $3k + 2$;
   (b) um inteiro da forma $3k^2 - 1$ não é um quadrado perfeito.

12. Sejam a e b inteiros não ambos nulos. Mostre que:

   (a) a e b são primos entre si sse, existem inteiros x e y, tais que $1 = ax + by$;
   (b) se $d =$ m.d.c.(a, b), então $\frac{a}{d}$ e $\frac{b}{d}$ são primos entre si;
   (c) se m.d.c.$(a, b) = 1$ e $c \in \mathbb{Z}$ é tal que $a \mid c$ e $b \mid c$, então $ab \mid c$.

13. Prove que dois inteiros consecutivos são primos entre si.

14. Verifique que $6 \mid a(a + 1)(2a + 1)$, qualquer que seja $a \in \mathbb{Z}$.

15. Verifique que, para qualquer $n \in \mathbb{N}$, $6 \mid n^3 - n$.

16. Sejam $a, b \in \mathbb{Z} \setminus \{0\}$. Mostre que:

   (a) m.m.c.$(a, b) =$ m.m.c.$(|a|, |b|) =$ m.m.c.(b, a).
   (b) m.m.c.$(a, a) = |a|$.
   (c) se $b \mid a$, então m.m.c.$(a, b) = |a|$.
   (d) m.d.c.$(a, b) \mid$ m.m.c.(a, b).
   (e) m.m.c.$(ka, kb) = |k|$m.m.c.(a, b) para qualquer $k \in \mathbb{Z} \setminus \{0\}$.

17. Em cada caso, calcule o mínimo múltipo comum de a e b e escreva-o como combinação linear de a e b.

   (a) $a = 144$ e $b = 34$;
   (b) $a = 34$ e $b = 144$;
   (c) $a = 39$ e $b = 51$;
   (d) $a = -39$ e $b = -51$;
   (e) $a = -63$ e $b = -37$.

18. Seja $p \in \mathbb{P}$ e $p > 3$. Mostre que o resto da divisão de p por 6 é igual a 1 ou a 5.

19. Prove que, se $p \in \mathbb{P}$ e $p > 3$, então $p^2 + 2$ é um número composto. (Sugestão: use o resultado do exercício 18.)

20. Mostre, que se $p, p + 2 \in \mathbb{P}$ e $p > 3$, então $6 \mid (p + 1)$.

21. Fatorize como produto de primos os números: 36300, 5661, 529, 677.

22. Sejam $a = 86625$ e $b = 38220$.

    (a) Fatorize a e b em primos.

    (b) Escreva a fatorização em primos de m.d.c.(a, b).

    (c) Escreva a fatorização em primos de m.m.c.(a, b).

23. Sejam $a = 4918793$ e $b = 35302597$. Calcule m.d.c.(a, b), sabendo que $a \times 9514662 - b \times 1325700 = 66$.

24. Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Mostre que m.d.c.$(a^n, b^n) =$ m.d.c.$(a, b)^n$.

25. Determine os números primos p tais que $17p + 1$ é um quadrado perfeito.

26. Mostre que o único primo p da forma $p = n^3 - 1$, com $n \in \mathbb{N}$, é $p = 7$. (Sugestão: note que 1 é raiz do polinómio $n^3 - 1$ de incógnita n.)

27. Determine um fator primo do número $2^{30} + 1$.

28. Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Mostre que se $n = a^4 - b^4$, então n não é um número primo.

29. Sejam $a, b, c \in \mathbb{Z}$ e $p \in \mathbb{P}$. Diga quais das seguintes afirmações são verdadeiras:

    (a) Se m.d.c.$(a, b) =$ m.d.c.(b, c), então m.d.c.$(a, b) =$ m.d.c.(a, c).

    (b) Se m.d.c.$(a, b) =$ m.d.c.(b, c), então m.m.c.$(a, b) =$ m.m.c.(b, c).

    (c) Se m.d.c.$(a, b) =$ m.d.c.(b, c), então m.d.c.$(a^2, b^2) =$ m.d.c.(b^2, c^2).

    (d) Se $p \mid a$ e $p \mid (ab + b^2)$, então $p \mid b$.

    (e) Se $b \mid (a^2 + 1)$, então $b \mid (a^4 + 1)$.

    (f) Se $b \mid (a^2 - 1)$, então $b \mid (a^4 + 1)$.

30. Prove que o conjunto dos números primos da forma $6n + 5$ é infinito.

31. Determine o conjunto de todos os inteiros positivos x tais que $x < 100$ e $x \equiv 9 \pmod{11}$.

32. Calcule os valores de m para os quais $25 \equiv 4 \pmod{m}$.

33. Determine dois positivos e dois negativos, na classe $[5]_m$ em que:

    (a) $m = 11$;
    (b) $m = 18$.

34. Determine um número $x \in \mathbb{N}$ tal que: $x \equiv 0 \pmod{11}$ e $x \equiv 0 \pmod{14}$.

35. Sejam $a, b, c \in \mathbb{Z}$ e $m, n \in \mathbb{N}$. Prove que, se $a \equiv b \pmod{m}$, então

    (a) $a + c \equiv b + c \pmod{m}$;
    (b) $ac \equiv bc \pmod{m}$;
    (c) $a^n \equiv b^n \pmod{m}$.

36. Sejam $a,\ b,\ c \in \mathbb{Z}$ e $m, n \in \mathbb{N}$. Prove que:

    (a) se $a \equiv b \pmod{m}$ e $n \mid m$, então $a \equiv b \pmod{n}$;
    (b) $a^2 \equiv b^2 \pmod{m}$ não implica $a \equiv b \pmod{m}$;
    (c) se $a \equiv b \pmod{m}$, então, m.d.c.(a, m) = m.d.c.(b, m).

37. Verifique se S é um sistema completo de resíduos módulo 7.

    (a) $S = \{-6, -5, -4, -3, -2, -1, 0\}$;
    (b) $S = \{-4, -3, -2, -1, 0, 8, 23\}$;
    (c) $S = \{-12, -4, 11, 13, 22, 32, 91\}$;
    (d) $S = \{-19, -4, 11, -1, 22, 54, 21\}$.

38. Caso exista, determine S um sistema completo de resíduos módulo m em que

    (a) $m = 12$;
    (b) $m = 7$ e os elementos de S são números primos;
    (c) $m = 11$ e os elementos de S são menores do que 4;
    (d) $m = 11$ e os elementos de S são múltiplos de 3;
    (e) $m = 12$ e os elementos de S são múltiplos de 3.

39. (a) Que dia da semana será o dia 23 de abril de 2021?
    (b) Que dia da semana foi o dia 23 de abril de 2000?

40. (a) Verifique se 22051946 é um quadrado perfeito.
    (b) Mostre que o último algarismo de um quadrado perfeito não pode pertencer a $\{2, 3, 7, 8\}$.

41. Calcule o menor $a \in \mathbb{N}_0$ tal que, em $\mathbb{Z}_{23}$, $[a]_{23}$ é o simétrico de:

    (a) $[5]_{23}$;
    (b) $[-29]_{23}$;
    (c) $[26]_{23}$;
    (d) $[46]_{23}$.

42. Diga se são verdadeiras ou falsas as seguintes igualdades em $\mathbb{Z}_{23}$:

    (a) $[17]_{23} + [15]_{23} = [9]_{23}$;
    (b) $[17]_{23} \cup [15]_{23} = [9]_{23}$;
    (c) $[5]_{23} \cap [15]_{23} = [0]_{23}$;
    (d) $[30]_{23} \cap [53]_{23} = [7]_{23}$;
    (e) $[5]_{23} \cap [15]_{23} = \emptyset$;
    (f) $[-29]_{23} \cdot [15]_{23} = [9]_{23}$;
    (g) $[26]_{23} \setminus [15]_{23} = [3]_{23}$.

43. Diga se são verdadeiras ou falsas as seguintes igualdades em $\mathbb{Z}_{15}$:

    (a) $[17]_{15} + [15]_{15} = [17]_{15}$;
    (b) $[17]_{15} \setminus [15]_{15} = [2]_{15}$;
    (c) $[5]_{15} \cdot [15]_{15} = [0]_{15}$;
    (d) $[5]_{15} \cap [15]_{15} = \emptyset$;
    (e) $[-29]_{15} \cdot [27]_{15} = [27]_{15}$;
    (f) $[3]_{15} \cdot [25]_{15} = [0]_{15}$;
    (g) $[19]_{15} \cdot [32]_{15} \cdot [17]_{15} = [1]_{15}$.

44. Mostre que:

    (a) $41 \mid 2^{20} - 1$;
    (b) o resto da divisão de 41^{65} por 7 é igual a 6;
    (c) $4^{215} \equiv 7 \pmod 9$.

45. Calcule:

    (a) o resto da divisão de 2^{50} por 7;
    (b) $\left(\sum_{n=1}^{100} n!\right) \pmod{12}$.

46. Seja $n \in \mathbb{N}$. Mostre que

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

47. Mostre que, para qualquer $n \in \mathbb{Z}$, $n^3 - n = 3k$, para certo $k \in \mathbb{Z}$.

48. Sejam $a \in \mathbb{Z}$ e $b \in \mathbb{N}$. Prove que, se m.d.c.$(a, b) \neq 1$, então não existe $c \in \mathbb{Z}$ que verifique $ac \equiv 1 \pmod b$.

49. Caso exista, calcule:

    (a) o inverso de 3 módulo 7;
    (b) o inverso de 3 módulo 11;
    (c) o inverso de 6 módulo 25;
    (d) o inverso de 15 módulo 231;
    (e) o inverso de 4 módulo 45.

50. Determine os valores de $x \in \mathbb{Z}$ tais que:

    (a) $3x \equiv 1 \pmod 7$;
    (b) $3x \equiv 2 \pmod 7$;
    (c) $6x \equiv 8 \pmod{11}$;
    (d) $15x \equiv 1 \pmod{231}$;
    (e) $15x \equiv 6 \pmod{231}$.

51. Sejam $x, y \in \mathbb{Z}$. Determine o conjunto dos inteiros x tais que:

    (a) $3x + 7y = 1$;
    (b) $3x + 7y = 2$;
    (c) $6x + 25y = 1$;
    (d) $15x + 231y = 1$;
    (e) $15x + 231y = 6$.

52. Mostre que a equação $x^2 + y^2 = 4z + 3$, nas incógnitas x, y e z, não tem soluções inteiras.

53. Mostre que a soma dos algarismos de um quadrado perfeito não pode ser igual a 375.

54. Com base nos critérios de divisibilidade estudados, mostre que o número 155832732 é divisível por 396.

55. Sejam a e d dígitos (ou algarismos). Determine os valores de a e d de modo que:

    (a) o número inteiro $n = \overline{3a5d}$ (i.e. $n = 3 \times 10^3 + a \times 10^2 + 5 \times 10 + d$) é múltiplo de 4 e de 9;
    (b) o número inteiro $n = \overline{34aa58d}$ é múltiplo de 11 e de 9.

    .

56. Resolva as seguintes equações diofantinas nas incógnitas x e y.

    (a) $31x + 25y = 3$;

    (b) $42x + 66y = 12$;

    (c) $54x + 21y = 906$.

57. Caso existam, determine as soluções positivas das seguintes equações diofantinas.

    (a) $6x + 25y = 353$;

    (b) $18x + 7y = 43$;

    (c) $6x - 11y = 17$;

    (d) $39x + 24y = 104$.

58. Se possível, escreva 100 como a soma de dois números positivos tais que:

    (a) um é múltiplo de 7 e o outro é múltiplo de 11;

    (b) um é múltiplo de 5 e o outro é múltiplo de 8:

59. De quantas maneiras se pode escrever o número 6 como diferença de dois inteiros positivos, sendo que o primeiro é múltiplo de 13 e o segundo é múltiplo de 11?

60. Considere a a equação diofantina $11x + 7y = 200$ nas incógnitas x e y.

    (a) Resolva a equação.

    (b) Quantas soluções positivas tem a equação.

    (c) Para que soluções da equação se verifica $3x + 5y$ é múltiplo de 3.

61. Um turista espanhol e um guia tiveram de fugir e subiram a correr os degraus de uma pirâmide por serem perseguidos por um leão! O turista subia cinco degraus de cada 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 tem a pirâmide?

62. Dispondo de dois relógios sonoros, um que sinaliza intervalos de 5 minutos e o outro que sinaliza intervalos de 11 minutos, como podemos marcar o tempo de cozedura de um ovo que se pretende seja exatamente de 4 minutos?

63. Para que inteiros x e y não nulos se verifica que $\frac{x+y}{xy} \in \mathbb{Z}$?

64. Considere a congruência linear $16x \equiv 9 (\mathrm{mod}\, 11)$. Determine:

    (a) duas soluções que sejam números primos;

    (b) duas soluções que sejam números pares;

    (c) o conjunto das soluções menores do que 100.

65. Resolva os seguintes sistemas de congruências:

    (a) $\begin{cases} 2x \equiv 1 (\mathrm{mod}\, 5) \\ 3x \equiv 9 (\mathrm{mod}\, 6) \\ 2x \equiv 4 (\mathrm{mod}\, 7) \end{cases}$;

(b) $\begin{cases} 2x \equiv 1 \pmod 9 \\ 5x \equiv 9 \pmod 7 \\ 4x \equiv 8 \pmod{11} \end{cases}$.

66. Resolva as seguintes congruências:

(a) $16x \equiv 9 (\mathrm{mod}\, 300)$;

(b) $462x \equiv 840 (\mathrm{mod}\, 300)$;

67. Determine o menor número natural $a > 2$ tal que $2 \mid a$, $3 \mid a+1$, $4 \mid a+2$, $5 \mid a+3$ e $6 \mid a+4$.

68. Resolva os seguintes sistemas de congruências:

(a) $\begin{cases} 3x \equiv 1 \pmod 4 \\ 5x \equiv 1 \pmod 6 \\ 2x \equiv 7 \pmod{15} \\ 2x \equiv 4 \pmod 9 \end{cases}$;

(b) $\begin{cases} 7x \equiv 11 \pmod{12} \\ 7x \equiv 20 \pmod{30} \\ 2x \equiv 19 \pmod{45} \end{cases}$;

(c) $\begin{cases} 7x \equiv 11 \pmod{12} \\ 7x \equiv 29 \pmod{30} \\ 2x \equiv 19 \pmod{45} \end{cases}$.

69. Calcule o resto da divisão de 3^{372} por 37.
70. Mostre que $7 \nmid n^2 + 1$ qualquer que seja $n \in \mathbb{Z}$.
71. Calcule

    (a) $31^{100} \bmod 19$, (b) $2^{10000} \bmod 29$.
72. Mostre que $11^{84} - 5^{84}$ é divisível por 7.
73. Mostre que $a^{13} \equiv a \pmod{273}$, para todo o inteiro a.
74. Mostre que $a^{12} \equiv 1 \pmod{35}$, para todo o inteiro a o tal que m.d.c.$(a, 35) = 1$.
75. Mostre que, para qualquer $n \in \mathbb{N}$, $n^{13} - n \equiv 0 \pmod{2730}$.
76. Seja $a \in \mathbb{Z}$ tal que m.d.c.$(a, 7) = 1$. Mostre que $7 \mid a^3 + 1$ ou $7 \mid a^3 - 1$.
77. Mostre que $a^{n-1} \equiv 1 \pmod{n}$ para qualquer inteiro a tal que m.d.c.$(a, n) = 1$ se

    (i) $n = 561$, (ii) $n = 1105$, (iii) $n = 1729$.

p-1 —> PTF

78. Seja p é um primo e a um inteiro tais que $a \not\equiv 1 \pmod{p}$. Prove que $1+a+\cdots+a^{p-1} \equiv 1 \pmod{p}$.
79. Determine os valores de n para os quais

    (a) $\phi(n) = 2$,
    (b) $\phi(n) = 6$,
    (c) $\phi(2n) = \phi(n)$,
    (d) $\phi(2n) = \phi(3n)$,
    (e) $\phi(n) = n - 2$.
80. Calcular os últimos dois dígitos de 1993^{1993}.
81. Calcule o inverso de 2 e de 3 módulo 35.
82. Calcule o resto da divisão de 2^{720} por 225.
83. Mostre que $n^{12} \equiv 1 \pmod{72}$ para qualquer inteiro n tal que m.d.c.$(n, 72) = 1$.
84. Verifique que se p é primo, então

$$1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} \equiv -1 \pmod{p}.$$

85. Calcule o resto da divisão de

    (i) 87! por 89; (ii) 18! por 437; (iii) $\frac{13!}{7!}$ por 7.
86. Mostre que se p é um primo ímpar, então $2(p-3)! \equiv -1 \pmod{p}$.