Matemática Discreta
Lista de Exercícios 03

Divisibilidade e aritmética modular

1. Mostre que se $a|b$ e $b|a$, onde a e b são inteiros com $a \neq 0$, então $a = b$ ou $a = -b$.
2. Mostre que se a,b, c e d são inteiros, onde $a \neq 0$, tal que $a|c$ e $b|d$ então $ab|cd$.
3. Mostre que se a,b e c são inteiros, onde $a \neq 0$, tal que $a|b$ então $ac|bc$.
4. Mostre que se a,b e c são inteiros, onde $a \neq 0$, tal que $ac|bc$ então $a|b$.
5. Para todo $a, b \in \mathbb{Z}$, se a e b tem a mesma paridade então $3a + 7$ e $7b - 4$ tem paridade diferentes.
6. Para todo $x \in \mathbb{Z}$, se $x^3 - 1 \equiv 0(\textbf{mod } 2)$ então $x \equiv 1(\textbf{mod } 2)$.
7. Para todo $x, y \in \mathbb{Z}$, se $x + y \equiv 0(\textbf{mod } 2)$ então $x \equiv y(\textbf{mod } 2)$.
8. Para todo $a, b \in \mathbb{Z}$, se $(a + b)^3 \equiv a^3 + b^3(\textbf{mod } 3)$.
9. Para todo $a \in \mathbb{Z}$, se $a \equiv 1(\textbf{mod } 5)$ então $a^2 \equiv 1(\textbf{mod } 5)$.
10. Para todo $n \in \mathbb{Z}$, $4|1 + (-1)^n \cdot (2n - 1)$.
11. Para todo $a, b \in \mathbb{Z}$, $a \not\equiv b(\textbf{mod } 2)$ então $a + b \equiv 1(\textbf{mod } 2)$.
12. Para todo $a, b \in \mathbb{Z}$ e $a \neq 0$. Se $a|b$ então $a^2|b^2$.
13. Para todo $a \in \mathbb{Z}$, se $5|2a$ então $5|a$. [Dica: Tente a prova direta e a contrapositiva].
14. Para todo $a, b, c\mathbb{Z}$ e $a \neq 0$. Se $a^2|b$ e $b^3|c$ então $a^6|c$.
15. Qual o quociente e o resto quando
    (a) 44 é divido por 8?
    (b) 777 é dividido por 21?
    (c) -123 é dividido por 19?
    (d) -1 é dividido por 23?
    (e) -2002 é dividido por 87?
    (f) 0 é dividido por 17?
    (g) 1234567 é dividido por 1001?
    (h) -100 é dividido por 101?
16. Seja a e b são inteiros e m um inteiro positivo. Se $a \equiv b(\textbf{mod } m)$ então $b \equiv a(\textbf{mod } m)$.
17. Seja $a, b, c \in \mathbb{Z}$ e m um inteiro positivo. Se $a \equiv b(\textbf{mod } m)$ então $ac \equiv bc(\textbf{mod } m)$.
18. Seja a e b são inteiros e m um inteiro positivo. Se $a \equiv b(\textbf{mod } m)$ e $b \equiv c(\textbf{mod } m)$ então $a \equiv c(\textbf{mod } m)$.
19. Seja a e b são inteiros e m um inteiro positivo. Se $a \equiv b(\textbf{mod } m)$ sse existe um $k \in \mathbb{Z}$ tal que $a = b + km$.
20. Seja a, b, c e d são inteiros e m um inteiro positivo. Se $a \equiv b(\textbf{mod } m)$ e $c \equiv d(\textbf{mod } m)$ então $a + c \equiv b + d(\textbf{mod } m)$.
21. Mostre que se $n \mid m$, em que n e m são números inteiros positivos maiores que 1, e se $a \equiv b \text{ (mod } m)$, em que a e b são números inteiros, então $a \equiv b(\text{mod } n)$.
22. Seja a e b são inteiros e m um inteiro positivo. Por que se m divide $a - b$ significa que a e b tem o mesmo resto considerando a divisão por m?
23. Mostre que $4 \not| 17n^2 + 1$, para todo inteiro n.
24. Mostre que $5 \not| 17n^2 + 1$, para todo inteiro n.
25. Mostre que para todo inteiro a, $a^2 \equiv 0(\textbf{mod } 4)$ ou $a^2 \equiv 1(\textbf{mod } 4)$.
26. Mostre um contra-exemplo a seguinte proposição se $ac \equiv bc(\textbf{mod } m)$ então $a \equiv b(\textbf{mod } m)$.
27. Mostre um contra-exemplo a seguinte proposição se $a \equiv b(\textbf{mod } m)$ e $c \equiv d(\textbf{mod} m)$ então $a^c \equiv b^d(\textbf{mod } m)$.
28. Mostre um contra-exemplo se $ab \equiv 0(\textbf{mod } m)$ então $a \equiv 0(\textbf{mod } m)$ ou $b \equiv 0(\textbf{mod } m)$.
29. Mostre que se $a \equiv b(\textbf{mod } m)$ e $c \equiv d(\textbf{mod } m)$, onde a,b,c,d e m são inteiros com $m \geq 2$ então $a - c \equiv b - d(\textbf{mod } m)$.

Aplicações

30. Encontre o último dígito:
    (a) 923^3
    (b) 2017^3
    (c) 2015^2
31. Sabendo que $7^2 \equiv -1 \textbf{ mod } 10$, encontre o último dígito de 7^{100}.
32. Mostre que a equação $7a^2 - 3b = 2$ não tem solução inteira.
33. Mostre que a equação $a^2 - 3b^2 = 17$ não tem solução inteira.
34. Mostre que a equação $2a^2 + 8b = 4$ não tem solução inteira.
35. Mostre que a equação $a^2 - 4b = 2$ não tem solução inteira.
36. Mostre que a equação $a^2 - 4b = 3$ não tem solução inteira.
37. Mostre que a equação $6x + 9y + 15z = 107$ não tem solução inteira.
38. Mostre que a equação $21a + 30b = 1$ não tem solução inteira.
39. Mostre que a equação $18a + 6b = 1$ não tem solução inteira.
40. Prove que $3|14^{2n} - 1$, para todo $n \in \mathbb{Z}$.
41. Prove que $3|2^{2n} - 1$, para todo $n \in \mathbb{Z}$.
42. Prove que $5|11^n - 6$, para todo $n \in \mathbb{Z}$.
43. Note que $25 \equiv 1(\textbf{ mod } 3)$ e $11 \equiv -1(\textbf{ mod } 3)$. Calcule $25^{100} + 11^{500}(\textbf{mod } 3)$.
44. Note que $3^4 \equiv 1(\textbf{mod } 80)$. Calcule $3^{5555}(\textbf{mod } 80)$
45. Qual a sequência de números pseudo-aleatórios gerada usando-se o gerador multiplicativo puro $x_{n+1} = 3x_n + 2 \textbf{ mod } 13$ com semente $x_0 = 1$?
46. Qual a sequência de números pseudo-aleatórios gerada usando-se o gerador multiplicativo puro $x_{n+1} = 4x_n + 1 \textbf{ mod } 7$ com semente $x_0 = 3$?
47. Qual a sequência de números pseudo-aleatórios gerada usando-se o gerador multiplicativo puro $x_{n+1} = 3x_n \textbf{ mod } 11$ com semente $x_0 = 2$?
48. Calcule os dígitos verificadores do CPF, se os primeiros 9 dígitos são:
    (a) 123.456.789
    (b) 111.111.111
    (c) 246.890.345
49. Todos os livros são identificados por um **número de registro denominado ISBN**, um código com 10 dígitos $x_1, x_2 \ldots x_{10}$, determinado pela editora. Esses 10 dígitos consistem de blocos que identificam a linguagem, a editora, o número determinado para o livro pela a editora e, por fim, um número com 1 dígito que é ou um dígito ou uma letra X (usada para representar 10). Este último dígito é selecionado para que $x_10 = \sum_{i=1}^{9} ix$ (**mod** 11) e é usado para detectar erros em dígitos individuais e transpor os dígitos.
    (a) Os primeiros nove dígitos de ISBN da versão européia da quinta edição deste livro são 0-07-119881. Qual é o último dígito para esse livro?
    (b) O ISBN da quinta edição de *Elementary Number Theory and Its Applications* é 0-32-123Q072, no qual Q é um dígito. Encontre o valor de Q.
    (c) O ISBN da sétima edição de *DISCRETE MATHEMATICS AND ITS APPLICATIONS* é 0-07-338309-0. Verifique se o último dígito de ISBN para este livro foi corretamente computado pela editora.