

Matemática Discreta

Lista de Exercícios 03

Divisibilidade

- O número 17 divide cada um dos números abaixo?
(a) 68 (b) 84 (c) 357 (d) 1001
- Mostre que se $a|b$ e $b|a$, em que a e b são inteiros não nulos, então $a = b$ ou $a = -b$.
- Mostre que se a , b e c são números inteiros com $c \neq 0$, tal que $ac|bc$, então $a|b$.
- Qual o quociente e o resto quando
(a) 19 é dividido por 7? (e) 0 é dividido por 19?
(b) -111 é dividido por 11? (f) 3 é dividido por 5?
(c) 789 é dividido por 23? (g) -1 é dividido por 3?
(d) 1001 é dividido por 13? (h) 4 é dividido por 1?
- Mostre que se n e k são números inteiros positivos, então $\lceil n/k \rceil = \lfloor (n-1)/k \rfloor + 1$.
- Encontre uma fórmula para o número inteiro com menor valor absoluto (mais próximo de zero) que é congruente módulo m ao número inteiro a , em que m é um número inteiro positivo.
- Avalie as quantidades abaixo.
(a) $13 \bmod 3$ (c) $155 \bmod 19$
(b) $-97 \bmod 11$ (d) $-221 \bmod 23$
- Decida se cada um dos inteiros abaixo é congruente a 5 módulo 17.
(a) 80 (b) 103 (c) -29 (d) -122
- Mostre que se $n | m$, em que n e m são números inteiros positivos maiores que 1, e se $a \equiv b \pmod{m}$, em que a e b são números inteiros, então $a \equiv b \pmod{n}$.
- Encontre contra-exemplos para cada uma das proposições abaixo sobre congruências.
(a) Se $ac \equiv bc \pmod{m}$, em que a , b , c e m são números inteiros com $m \geq 2$, então $a \equiv b \pmod{m}$.
(b) Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, em que a , b , c , d e m são números inteiros com c e d positivos e $m \geq 2$, então $a^c \equiv b^d \pmod{m}$.
- Mostre que se a , b , k e m são números inteiros, tal que $k \geq 1$, $m \geq 2$ e $a \equiv b \pmod{m}$, então $a^k \equiv b^k \pmod{m}$ sempre que k for um número inteiro positivo.
- Um estacionamento tem 31 vagas para visitantes, numeradas de 0 a 30. Os visitantes são determinados a parar nas vagas usando-se a função de hashing $h(k) = k \bmod 31$, em que k é o número formado pelos três primeiros dígitos da placa do carro do visitante.
(a) Quais vagas são determinadas pela função de hashing para os carros que têm os seguintes três primeiros dígitos da placa do carro?

317, 918, 007, 100, 111, 310

(b) Descreva um procedimento que os visitantes deverão seguir a fim de encontrar um vaga livre para estacionar, quando o espaço designado a eles está ocupado.
- Qual a sequência de números pseudo-aleatórios gerada usando-se o gerador multiplicativo puro $x_{n+1} = 3x_n \bmod 11$ com semente $x_0 = 2$?
- Codifique a mensagem "DO NOT PASS GO" substituindo as letras por números, aplicando a função de codificação dada e, então, transcrevendo os números em letras.
(a) $f(p) = (p + 3) \bmod 26$ (o código de César)
(b) $f(p) = (p + 13) \bmod 26$
(c) $f(p) = (3p + 7) \bmod 26$
- Todos os livros são identificados por um **número de registro denominado ISBN**, um código com 13 dígitos x_1, x_2, \dots, x_{10} , determinado pela editora. Esses 13 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 $\sum_{i=1}^{10} ix \equiv 0 \pmod{11}$ 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) Determine se o último dígito de ISBN para este livro foi corretamente computado pela editora.

- (a) 1 divide a . (b) a divide 0.
- Mostre que o item (iii) do Teorema 1 (pag. 202) é verdadeiro.
- Mostre que se a , b , c , e d são números inteiros, tal que $a|c$ e $b|d$, então $ab|cd$.
- Demonstre ou negue que se $a|bc$, em que a , b e c são números inteiros positivos, então $a|b$ ou $a|c$.
- Qual o quociente e o resto quando
(a) 44 é dividido por 8? (e) -2002 é dividido por 87?
(b) 777 é dividido por 21? (f) 0 é dividido por 17?
(c) -123 é dividido por 19? (g) 1234567 é dividido por 1001?
(d) -1 é dividido por 23? (h) -100 é dividido por 101?
- Considere m como um número inteiro positivo. Mostre que $a \bmod m = b \bmod m$ se $a \equiv b \pmod{m}$.
- Mostre que se a é um número inteiro e d é um número inteiro positivo maior que 1, então o quociente e o resto obtidos quando a é dividido por d são $\lfloor a/d \rfloor$ e $a - d \lfloor a/d \rfloor$, respectivamente.
- Avalie as quantidades abaixo.
(a) $-17 \bmod 2$ (c) $-101 \bmod 13$
(b) $144 \bmod 7$ (d) $199 \bmod 19$
- Liste cinco números inteiros que são congruentes a 4 módulo 12.
- Mostre que se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, em que a , b , c , d e m são números inteiros com $m \geq 2$, então $a - c \equiv b - d \pmod{m}$.
- Mostre que se a , b , c e m são números inteiros, tal que $m \geq 2$, $c > 0$ e $a \equiv b \pmod{m}$, então $ac \equiv bc \pmod{mc}$.
- Demonstre que se n é um número inteiro positivo e ímpar, então $n^2 \equiv 1 \pmod{8}$.
- Quais localizações da memória são determinadas pela função de hashing $h(k) = k \bmod 101$ para os registros de seguro de uma companhia com os números do Seguro Social abaixo?
(a) 104578690 (b) 432222187 (c) 372201919 (d) 501338753
- Qual a sequência de números pseudo-aleatórios gerada usando-se o gerador de congruência linear $x_{n+1} = (4x_n + 1) \bmod 7$ com origem $x_0 = 3$?
- Escreva um algoritmo em pseudocódigo para gerar uma sequência de números pseudo-aleatórios usando o gerador de congruência linear.
- Decodifique as mensagens abaixo codificadas usando o código de César.
(a) EOXH MHDQV (b) WHVW WRGDB (c) HDW GLP VXP

Todos os livros são identificados por um **número de registro denominado ISBN**, um código com 13 dígitos x_1, x_2, \dots, x_{10} , determinado pela editora. Esses 13 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 $\sum_{i=1}^{10} ix \equiv 0 \pmod{11}$ e é usado para detectar erros em dígitos individuais e transpor os dígitos.

- 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 .

Questões adicionais:

- Mostre que se a for um número inteiro diferente de 0, então