Matemática Discreta
Lista de Exercícios 03

Divisibilidade

1. O número 17 divide cada um dos números abaixo?

   (a) 68 (b) 84 (c) 357 (d) 1001

2. Mostre que se $a|b$ e $b|a$, em que a e b são inteiros não nulos, então $a = b$ ou $a = -b$.
3. Mostre que se a, b e c são números inteiros com $c \neq 0$, tal que $ac|bc$, então $a|b$.
4. Qual o quociente e o resto quando

   (a) 19 é dividido por 7?
   (b) -111 é dividido por 11?
   (c) 789 é dividido por 23?
   (d) 1001 é dividido por 13?
   (e) 0 é dividido por 19?
   (f) 3 é dividido por 5?
   (g) -1 é dividido por 3?
   (h) 4 é dividido por 1?

5. Mostre que se n e k são números inteiros positivos, então $\lceil n/k \rceil = \lfloor (n-1)/k \rfloor + 1$.
6. 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.
7. Avalie as quantidades abaixo.

   (a) 13 **mod** 3
   (b) -97 **mod** 11
   (c) 155 **mod** 19
   (d) -221 **mod** 23

8. Decida se cada um dos inteiros abaixo é congruente a 5 módulo 17.

   (a) 80 (b) 103 (c) -29 (d) -122

9. Mostre que se $n \mid m$, 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 $a \equiv b(\text{mod } n)$.
10. Encontre contra-exemplos para cada uma das proposições abaixo sobre congruências.

    (a) Se $ac \equiv bc(\text{mod } m)$, em que a, b, c e m são números inteiros com $m \geq 2$, então $a \equiv b(\text{mod } m)$.

    (b) Se $a \equiv b(\text{mod } m)$ e $c \equiv d(\text{mod } m)$, em que a, b, c, d e m são números inteiros com c e d positivos e $m \geq 2$, então $a^c \equiv b^d(\text{mod } m)$.

11. Mostre que se a, b, k e m são números inteiros, tal que $k \geq 1$, $m \geq 2$ e $a \equiv b(\text{mod } m)$, então $a^k \equiv b^k(\text{mod } m)$ sempre que k for um número inteiro positivo.
12. 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 $h(k) = k$ **mod** 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.

13. Qual a sequência de números pseudo-aleatórios gerada usando-se o gerador multiplicativo puro $x_{n+1} = 3x_n$ **mod** 11 com semente $x_0 = 2$?
14. 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) $f(p) = (p+3)$ **mod** 26 (o código de César)
    (b) $f(p) = (p+13)$ **mod** 26
    (c) $f(p) = (3p+7)$ **mod** 26

15. Todos os livros são identificados por um **número de registro denominado ISBN**, um código com 13 dígitos $x_1, x_2 \ldots x_{10}$, 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.

Respostas:

1. (a) Sim. (b) Não. (c) Sim. (d) Não.
2. Se $a \mid b$ e $b \mid a$, existem inteiros s e t tal que $b = as$ e $a = bt$. Logo, $a = ast$. Como $a \neq 0$, segue que $st = 1$. Assim, ou $s = t = 1$ ou $s = t = -1$. Logo, ou $a = b$ ou $a = -b$.
3. Como $ac \mid bc$, existe um inteiro s tal que $bc = acs$. Como $c \neq 0$, podemos dividir os 2 lados por c, obtendo $b = as$. Portanto $a \mid b$, pois s é inteiro.
4. (a) 2, 5 (b) -11, 10 (c) 34, 7 (d) 77, 0 (e) 0, 0 (f) 0, 3 (g) -1, 2 (h) 4, 0
5. Seja r o resto da divisão de n por k. Então, $n = k\lfloor n/k \rfloor + r$ e $0 \leq r < k$. Assim, $\lceil n/k \rceil = \lceil \lfloor n/k \rfloor + r/k \rceil = \lfloor n/k \rfloor + \lceil r/k \rceil$ e $\lfloor (n-1)/k \rfloor = \lfloor \lfloor n/k \rfloor + (r-1)/k \rfloor = \lfloor n/k \rfloor + \lfloor (r-1)/k \rfloor$. Portanto, basta provar que $\lceil r/k \rceil = \lfloor (r-1)/k \rfloor + 1$. Quando $r = 0$, temos que $\lceil r/k \rceil = 0$ e $\lfloor (r-1)/k \rfloor = -1$. Quando $0 < r < k$, temos que $\lceil r/k \rceil = 1$ e $\lfloor (r-1)/k \rfloor = 0$.
6. a **mod** m se a **mod** $m \leq \lceil m/2 \rceil$, e (a **mod** m) $- m$ se a **mod** $m > \lceil m/2 \rceil$.
7. (a) 1 (b) 2 (c) 3 (d) 9
8. (a) Não. (b) Não. (c) Sim. (d) Não.
9. Seja $m = tn$. Como $a \equiv b(\text{mod } m)$ existe um inteiro s tal que $a - b = sm$. Logo, $a - b = (st)n$, de modo que $a \equiv b(\text{mod } n)$, pois st é inteiro.
10. (a) Sejam $m = c$=2, $a = 0$ e $b = 1$. Então, 0=$ac \equiv bc$ =2(mod 2), mas $0 = a$ não equivalente a $b = 1$(mod 2).

    (b) Sejam $m = 5$, $a = b = 3$, $c = 1$ e $d = 6$. Então, $3 \equiv 3(\text{mod } 5)$ e $1 \equiv 6(\text{mod } 5)$, mas $3^1 = 3$ não equivalente a $4 \equiv 729 = 3^6(\text{mod } 5)$.

11. Como $a \equiv b(\text{mod } m)$, existe um inteiro s tal que $a = b + sm$, de modo que $a - b = sm$. Então, $a^k - b^k = (a-b)(a^{k-1} + a^{k-2}b + \ldots + ab^{k-2} + b^{k-1})$, $k \geq 2$, também é um múltiplo de m. Segue que $a^k \equiv b^k(\text{mod } m)$.
    Outra forma de resolver é aplicando k vezes o teorema que diz que se $a \equiv b(\text{mod } m)$ e $c \equiv d(\text{mod } m)$, então $ac \equiv bd(\text{mod } m)$ (basta fazer $c = a$ e $d = b$).
12. (a) 7, 19, 7, 7, 18, 0

    (b) Considere o próximo espaço disponível **mod** 31.

13. $2, 6, 7, 10, 8, 2, 6, 7, 10, 8, \ldots$
14. (a) GR QRW SDVV JR

    (b) QB ABG CNFF TB

    (c) QX UXM AHJJ ZX

15. (a) 4

    (b) O algarismo de verificaçãodo ISBN para este livro é válido porque $1 \cdot 0 + 2 \cdot 0 + 3 \cdot 7 + 4 \cdot 2 + 5 \cdot 8 + 6 \cdot 8 + 7 \cdot 0 + 8 \cdot 0 + 9 \cdot 8 + 10 \cdot 2 \equiv 0 \pmod{11}$.

Questões adicionais:

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

   (a) 1 divide a. (b) a divide 0.

2. Mostre que o item (iii) do Teorema 1 (pag. 202) é verdadeiro.
3. Mostre que se a, b, c, e d são números inteiros, tal que $a|c$ e $b|d$, então $ab|cd$.
4. Demonstre ou negue que se $a|bc$, em que a, b e c são números inteiros positivos, então $a|b$ ou $a|c$.
5. 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?

6. Considere m como um número inteiro positivo. Mostre que a **mod** $m = b$ **mod** m se $a \equiv b(mod\ m)$.
7. 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.
8. Avalie as quantidades abaixo.

   (a) -17 **mod** 2
   (b) 144 **mod** 7
   (c) -101 **mod** 13
   (d) 199 **mod** 19

9. Liste cinco números inteiros que são congruentes a 4 módulo 12.
10. Mostre que se $a \equiv b$ (mod. m) e $c \equiv d$(mod. m), em que a, b, c, d e m são número inteiros com $m \geq 2$, então $a - c \equiv$ b - d(mod.m).
11. Mostre que se a, b, c e m são números inteiros, tal que $m \geq 2$, $c > 0$ e $a \equiv b$(mod. m), então $ac \equiv bc$(mod. mc).
12. Demonstre que se n é um número inteiro positivo e ímpar, então $n^2 \equiv 1(\text{mod } 8)$.
13. Quais localizações da memória são determinadas pela função de hashing $h(k) = k$ **mod** 101 para os registros de seguro de uma companhia com os números do Seguro Social abaixo?

    (a) 104578690 (b) 432222187 (c) 372201919 (d) 501338753

14. Qual a sequência de números pseudo-aleatórios gerada usando-se o gerador de congruência linear $x_{n+1} = (4x_n + 1)$ **mod** 7 com origem $x_0 = 3$?
15. Escreva um algoritmo em pseudocódigo para gerar uma sequência de números pseudo-aleatórios usando o gerador de congruência linear.

16. 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 $x_1, x_2 \ldots x_{10}$, 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.

17. 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.