Divisibilidade

Wladimir Araújo Tavares [1]

[1]Universidade Federal do Ceará - Campus de Quixadá

13 de setembro de 2016

Definição

Se a e b são inteiros com $a \neq 0$, *nós dizemos que a divide b se existe um inteiro k tal que* $b = ak$, *ou equivalentemente, se* $\frac{b}{a}$ *é inteiro. Quando a divide b, nós dizemos que a é fator ou divisor de b e b é múltiplo de a. A notação* $a|b$ *denota que a divide b. When a não divide b, denotamos por* $a \not| b$

Exemplo

Determine se $3|7$ *e se* $3|12$

$3 \not| 7$, *porque* $\frac{7}{3} \notin \mathbb{Z}$. $3|12$, *porque* $\frac{12}{3} \in \mathbb{Z}$.

Exercício

Determine se:

1. $3 | 15$

Exercício

Determine se:

1. $3|15$ sim, porque $\frac{15}{3} \in \mathbb{Z}$
2. $3|14$

Exercício

Determine se:

1. $3|15$ sim, porque $\frac{15}{3} \in \mathbb{Z}$
2. $3|14$ não, porque $\frac{14}{3} \notin \mathbb{Z}$
3. $4|15$

Exercício

Determine se:

1. $3|15$ sim, porque $\frac{15}{3} \in \mathbb{Z}$
2. $3|14$ não, porque $\frac{14}{3} \notin \mathbb{Z}$
3. $4|15$ não, porque $\frac{15}{4} \notin \mathbb{Z}$
4. $4|16$

Exercício

Determine se:

1. $3|15$ sim, porque $\frac{15}{3} \in \mathbb{Z}$
2. $3|14$ não, porque $\frac{14}{3} \notin \mathbb{Z}$
3. $4|15$ não, porque $\frac{15}{4} \notin \mathbb{Z}$
4. $4|16$ sim, porque $\frac{16}{4} \in \mathbb{Z}$
5. $5|21$

Exercício

Determine se:

1. $3|15$ sim, porque $\frac{15}{3} \in \mathbb{Z}$
2. $3|14$ não, porque $\frac{14}{3} \notin \mathbb{Z}$
3. $4|15$ não, porque $\frac{15}{4} \notin \mathbb{Z}$
4. $4|16$ sim, porque $\frac{16}{4} \in \mathbb{Z}$
5. $5|21$ não, porque $\frac{21}{5} \notin \mathbb{Z}$

Exemplo

Quantos números positivos menores que 100 são divisíveis por 8?

Exemplo

Quantos números positivos menores que 100 são divisíveis por 8?
Todos os números inteiros positivos divisíveis por 8 são da forma $8k$*, onde k é um inteiro positivo.*

Exemplo

Quantos números positivos menores que 100 são divisíveis por 8?
Todos os números inteiros positivos divisíveis por 8 são da forma $8k$*, onde k é um inteiro positivo.*
O número de inteiros positivos divisível por 8 menores que 100 é igual ao número de inteiros k com $0 < 8k < 100$ *com* $0 < k < \frac{100}{8}$

Exemplo

Quantos números positivos menores que 100 são divisíveis por 8?
Todos os números inteiros positivos divisíveis por 8 são da forma $8k$*, onde k é um inteiro positivo.*
O número de inteiros positivos divisível por 8 menores que 100 é igual ao número de inteiros k com $0 < 8k < 100$ *com* $0 < k < \frac{100}{8}$
Portanto, existem $\lfloor \frac{100}{8} \rfloor$ *inteiros positivos menores que 100 que são divisíveis por 8.*

Exemplo

Quantos números positivos menores que 100 são divisíveis por 8?
Todos os números inteiros positivos divisíveis por 8 são da forma $8k$*, onde k é um inteiro positivo.*
O número de inteiros positivos divisível por 8 menores que 100 é igual ao número de inteiros k com $0 < 8k < 100$ *com* $0 < k < \frac{100}{8}$
Portanto, existem $\lfloor \frac{100}{8} \rfloor$ *inteiros positivos menores que 100 que são divisíveis por 8.*

Exemplo

Quantos números positivos menores que n são divisíveis por d?

Exemplo

Quantos números positivos menores que n *são divisíveis por* d*?*
Todos os números inteiros positivos divisíveis por d *são da forma* dk*, onde* k *é um inteiro positivo.*

Exemplo

Quantos números positivos menores que n são divisíveis por d?
Todos os números inteiros positivos divisíveis por d são da forma dk, onde k é um inteiro positivo.
O número de inteiros positivos divisível por d menores que n é igual ao número de inteiros k com $0 < dk < n$ com $0 < k < \frac{n}{d}$

Exemplo

Quantos números positivos menores que n são divisíveis por d?
Todos os números inteiros positivos divisíveis por d são da forma dk, onde k é um inteiro positivo.
O número de inteiros positivos divisível por d menores que n é igual ao número de inteiros k com $0 < dk < n$ com $0 < k < \frac{n}{d}$
Portanto, existem $\lfloor \frac{n}{d} \rfloor$ inteiros positivos menores que n que são divisíveis por d.

Exemplo

Quantos números positivos menores que n são divisíveis por d?
Todos os números inteiros positivos divisíveis por d são da forma dk, onde k é um inteiro positivo.
O número de inteiros positivos divisível por d menores que n é igual ao número de inteiros k com $0 < dk < n$ com $0 < k < \frac{n}{d}$
Portanto, existem $\lfloor \frac{n}{d} \rfloor$ inteiros positivos menores que n que são divisíveis por d.

Teorema

Se a,b e c são inteiros, onde $a \neq 0$. Então

1. *se $a|b$ e $a|c$ então $a|(b+c)$.*
2. *se $a|b$ então $a|bc$ para todo inteiro c.*
3. *se $a|b$ e $b|c$ então $a|c$*

Demonstração.

Suponha três inteiros a,b e c tal que $a|b$ e $a|c$. Pela definição, sabemos que existe um inteiro k e k' tal que $b = ak$ e $c = ak'$. Então,

$$b + c = ak + ak' = a(k + k') \tag{1}$$

Portanto, $b + c = ar$, onde $r = k + k'$. Concluímos que $a|(b + c)$

$\square$

Corolário

Se a,b e c são inteiros, onde $a \neq 0$, tal que $a|b$ e $a|c$ então $a|mb + nc$ para todo inteiro m e n.

Demonstração.

Por (2) do Teorema anterior, temos que $a|mb$ e $a|nc$ para todo inteiro m e n.

Corolário

Se a,b e c são inteiros, onde $a \neq 0$, tal que $a|b$ e $a|c$ então $a|mb + nc$ para todo inteiro m e n.

Demonstração.

Por (2) do Teorema anterior, temos que $a|mb$ e $a|nc$ para todo inteiro m e n.
Por (1) do Teorema anterior, $a|mb + nc$ □

Algoritmo da divisão

Teorema

(Algoritmo da divisão) Seja a um inteiro e d um inteiro positivo. Então existe inteiros únicos q e r, onde $0 \leq r < d$ tal que $a = dq + r$. d é chamado de divisor, a é o dividendo, q é chamado de quociente e r é chamado de resto.

$$q = a \textbf{ div } d, r = a \textbf{ mod } d \tag{2}$$

1. $d = 0$: Erro
2. $a \in \mathbb{Z} \land d > 0$: $q = \lfloor \frac{a}{d} \rfloor \land r = a - dq$
3. $a \in \mathbb{Z} \land d < 0$: $q = -\lfloor \frac{a}{|d|} \rfloor \land r = a - dq$

Exemplo

Exemplo

Qual é o quociente e o resto quando dividimos 101 por 11?

Exemplo

Exemplo

Qual é o quociente e o resto quando dividimos 101 por 11?

$$
\begin{aligned}
q &= \left\lfloor \frac{101}{11} \right\rfloor = \lfloor 9.1 \rfloor = 9 \\
r &= 101 - 11q = 101 - 11(9) = 2
\end{aligned}
$$

Exemplo

Exemplo

Qual é o quociente e o resto quando dividimos -11 por 3?

Exemplo

Exemplo

Qual é o quociente e o resto quando dividimos -11 por 3?

$$
\begin{aligned}
q = && \lfloor \frac{-11}{3} \rfloor = && \lfloor -3.666 \rfloor = && -4 \\
r = && -11 - 3q = && 11 - 3(-4) = && 1
\end{aligned}
$$

Exemplo

Exemplo

Qual é o quociente e o resto quando dividimos 25 por -3?

Exemplo

Exemplo

Qual é o quociente e o resto quando dividimos 25 por -3?

$$\begin{aligned} q = \quad & -\lfloor \frac{25}{|-3|} \rfloor = & -\lfloor 8.33 \rfloor = & \quad 8 \\ r = \quad & 25 - (-3)q = & 25 - (-3)(-8) = & \quad 1 \end{aligned}$$

Exemplo

Qual é o quociente e o resto quando dividimos -25 por -3?

Exemplo

Exemplo

Qual é o quociente e o resto quando dividimos -25 por -3?

$$\begin{aligned} q = &\quad -\lfloor \frac{-25}{|-3|} \rfloor + 1 = &\quad -\lfloor -8.33 \rfloor = &\quad -(-9) \\ r = &\quad -25-(-3)q = &\quad -25-(-3)(9) = &\quad 2 \end{aligned}$$

Algoritmo da Divisão

```
def divide(n, d):
        if d == 0: raise ZeroDivisionError
        if d <  0:
                (q,r) = divide(n, -d)
                return (-q,r)
        if n < 0:
                (q,r) = divide (-n,d)
                if r == 0 : return (-q,0)
                else:  return (-q-1, d-r)
        #Neste ponto, temos que N >= 0 e D > 0
        q = 0,r = n
        while r >= d:
                q = q + 1
                r = r - d
        return (q,r)
```

Aritmética modular ou do relógio

Definição

Se a e b são inteiros e m é um inteiro positivo, então a é congruente a b módulo m se m divide $a - b$.

Aritmética modular ou do relógio

Definição

Se a e b são inteiros e m é um inteiro positivo, então a é congruente a b módulo m se m divide $a - b$.
Nós usamos a notação $a \equiv b (mod \; m)$ para indicar que a é congruente a b módulo m.

Aritmética modular ou do relógio

Definição

Se a e b são inteiros e m é um inteiro positivo, então a é congruente a b módulo m se m divide $a - b$.
Nós usamos a notação $a \equiv b (mod \ m)$ para indicar que a é congruente a b módulo m.
Caso contrário, indicamos por $a \not\equiv b (mod \ m)$

Definição

Se a e b são inteiros e m é um inteiro positivo, então a é congruente a b módulo m se m divide $a - b$.
Nós usamos a notação $a \equiv b \pmod{m}$ para indicar que a é congruente a b módulo m.
Caso contrário, indicamos por $a \not\equiv b \pmod{m}$

Exemplo

No relógio de parede, quando é 1h ou são 13h, os ponteiros do relógio estão no mesmo lugar. O mesmo acontece, quando são 2h ou são 14h.

Definição

Se a e b são inteiros e m é um inteiro positivo, então a é congruente a b módulo m se m divide $a - b$.
Nós usamos a notação $a \equiv b (mod \ m)$ para indicar que a é congruente a b módulo m.
Caso contrário, indicamos por $a \not\equiv b (mod \ m)$

Exemplo

No relógio de parede, quando é 1h ou são 13h, os ponteiros do relógio estão no mesmo lugar. O mesmo acontece, quando são 2h ou são 14h.
Dizemos que $13 \equiv 1 (mod \ 12)$ e $14 \equiv 2 (mod \ 12)$. Observe que $12 | 13 - 1$ e $12 | 14 - 2$.

Exercício

1. $15 \equiv x \pmod{12}$
2. $20 \equiv x \pmod{12}$
3. $22 \equiv x \pmod{12}$
4. $18 \equiv x \pmod{15}$
5. $20 \equiv x \pmod{15}$

Teorema

Seja a e b inteiros, e m um inteiro positivo. Então $a \equiv b (mod\ m)$ se somente se $a\ mod\ m = b\ mod\ m$.

Demonstração.

Suponha dois inteiros a e b e um inteiro positivo m tal que $a\ mod\ m = b\ mod\ m$. Pela definição,

$$\begin{aligned} a\ mod\ m &= b\ mod\ m \\ a - m\lfloor \frac{a}{m} \rfloor &= b - m\lfloor \frac{b}{m} \rfloor \\ a - b &= m\lfloor \frac{a}{m} \rfloor - m\lfloor \frac{b}{m} \rfloor \\ a - b &= m(\lfloor \frac{a}{m} \rfloor - \lfloor \frac{b}{m} \rfloor) \end{aligned}$$

Logo, $m|(a-b)$. Concluímos que $a \equiv b \pmod{m}$

□

Propriedades da função piso e teto:

1. $\lfloor x \rfloor = n$ se somente se $n \leq x < n + 1$.
2. $\lceil x \rceil = n$ se somente se $n - 1 < x \leq n$.
3. $x - 1 < \lfloor x \rfloor \leq x \leq \lceil x \rceil < x + 1$
4. $\lfloor -x \rfloor = -\lceil x \rceil$
5. $\lfloor x + n \rfloor = \lfloor x \rfloor + n$

Teorema

Seja a e b inteiros, e m um inteiro positivo. Então $a \equiv b (mod \ m)$ se somente se $a \ mod \ m = b \ mod \ m$.

Demonstração.

Suponha dois inteiros a e b e um inteiro positivo m tal que $a \equiv b(mod \ m)$. Pela definição,

$$m | a - b \Leftrightarrow a - b = mk \Leftrightarrow a = b + mk \tag{3}$$

Teorema

Seja a e b inteiros, e m um inteiro positivo. Então $a \equiv b(mod\ m)$ se somente se $a\ mod\ m = b\ mod\ m$.

Demonstração.

Suponha dois inteiros a e b e um inteiro positivo m tal que $a \equiv b(mod\ m)$. Pela definição,

$$m|a-b \Leftrightarrow a-b = mk \Leftrightarrow a = b+mk \tag{3}$$

Vamos mostrar que $b+mk\ mod\ m = b\ mod\ m$,

$$\begin{aligned} b+mk\ mod\ m = & \quad b+mk-m\lfloor\frac{b+mk}{m}\rfloor \\ = & \quad b+mk-m(\lfloor\frac{b}{m}\rfloor+k) \\ = & \quad b-m\lfloor\frac{b}{m}\rfloor \\ = & \quad b\ mod\ m \end{aligned}$$

Teorema

Seja m um inteiro positivo. Então $a \equiv b(mod\ m)$ se somente se existe um inteiro k tal que $a = b + km$.

Teorema

Seja m um inteiro positivo. Se $a \equiv b(mod\ m)$ e $c \equiv d(mod\ m)$, então

$$a + c \equiv b + d(mod\ m) \text{ e } ac \equiv bd(mod\ m) \tag{4}$$

Corolário

Seja m um inteiro positivo e a e b inteiros. Então

$$a + b \ mod \ m = ((a \ mod \ m) + (b \ mod \ m))modm \tag{5}$$

e

$$ab \ mod \ m = ((a \ mod \ m)(b \ mod \ m)) \ mod \ m \tag{6}$$

Demonstração.

Pela definição de mod, temos

$$a \equiv (a \ mod \ m) \ mod \ m \text{ e } b \equiv (b \ mod \ m) \ mod \ m \tag{7}$$

Pelo teorema anterior,

$$a + b \equiv (a \ mod \ m) + (b \ mod \ m)(\ mod \ m)$$
$$a + b \ mod \ m = (a \ mod \ m) + (b \ mod \ m) \ mod \ m$$

Aplicação: Aritmética modular

Exemplo

Calcule 234 *mod* 9*?*
Sabemos que

$$234 = 2 \times 10^2 + 3 \times 10^1 + 4 \times 10^0$$

Sabemos que $10^2 \equiv 1 \textbf{ mod } 9$ *e* $10 \equiv 1 \textbf{ mod } 9$

$$
\begin{aligned}
&= 2 \times 10^2 + 3 \times 10^1 + 4 \ \mathit{mod}\ 9 \\
&= 2 \times 1 + 3 \times 1 + 4 \ \mathit{mod}\ 9 \\
&= \mathit{9 \ mod \ 9} \\
&= \mathit{0}
\end{aligned}
$$

Aplicação: Aritmética Modular

Exemplo

Calcule 17^2 **mod** 19*.*
Computando diretamente,

$$17^2 = 289 \textbf{ mod } 19 = 4. \tag{8}$$

Sabemos que $17 \equiv (-2) \textbf{ mod } 19$*, então*

$$17^2 \equiv (-2)^2 \equiv 4 \textbf{ mod } 19 \tag{9}$$

Observe que a multiplicação independente da escolha do representante.

Exemplo

Encontre o último dígito de 2006^3*.*
Podemos encontrar o último dígito de 2006^3*, calculando* $2006^3 \textbf{ mod } 10$*. Sabendo que* $2006 \equiv 6 \textbf{ mod } 10$*. Então,*

$$2006^3 \equiv 6^3 \equiv 6(\textbf{ mod } 10) \tag{10}$$

Exemplo

Mostre que a equação $6a^2 - 5b = 3$ *não tem soluções inteiras?*

$$\begin{aligned} 6a^2 - 5b &\equiv 6a^2 \pmod{5} \\ &\equiv a^2 \pmod{5} \end{aligned}$$

A Tabela de $a^2 \bmod 5$*:*

$a \bmod 5$	0	1	2	3	4
$a^2 \bmod 5$	0	1	4	4	1

Logo, $a^2 \not\equiv 3 \bmod 5$

Exemplo

Mostre que a equação $18a + 6b = 1$ *não tem solução inteira.*
Suponha por absurdo que existe uma solução inteira. Sabemos que $6|18$ *e* $6|6$. *Logo,* $6|18x + 6y$, $\forall x, y \in \mathbb{Z}$. *Conseqüentemente, 6 é divisor de 1, mas não é. Portanto, não existe solução inteira para a equação.*

Exemplo

Mostre que $7 | 2^n + 6 \cdot 9^n$, *para todo* $n \in \mathbb{Z}$.

$2 \equiv 9 \textbf{ mod } 7 \Rightarrow 2^n \equiv 9^n \textbf{ mod } 7 \Rightarrow 2^n + 6 \cdot 9^n \equiv 9^n + 6 \cdot 9^n \equiv 7 \cdot 9^n \equiv 0 \textbf{ mod } 7$

Aplicação: ISBN

- Livros são identificados por um número ISBN (International Standard Book Number), um código de 10 dígitos $x_1 x_2 \ldots x_{10}$. Esses números identificam a linguagem, a editora, o número do livro e um dígito de verificação.
- O dígito verificador é um dígito ou a letra X (usada para representar 10)
- O dígito de verificador é selecionado de forma que

$$x_{10} = \sum_{i=1}^{9} i x_i (mod\ 11). \tag{11}$$

Aplicação: ISBN

Exemplo

Se os primeiros 9 dígitos são 0-07-053965. Qual é o dígito verificador para esse livro?

$$
\begin{aligned}
x_10 &= \sum_{i=1}^{9} ix_i (mod\ 11) \\
&= 1(0) + 2(0) + 3(7) + 4(0) + 5(5) + 6(3) + \\
&\quad 7(9) + 8(6) + 9(5) \pmod{11} \\
&= 0 + 0 + 10 + 0 + 3 + 7 + 8 + 4 + 1 \pmod{11} \\
&= 0
\end{aligned}
$$

Aplicação: ISBN

Exemplo

É 0-07-288008-3 é ISBN válido?

$$\begin{aligned}
x_10 &= \sum_{i=1}^{9} ix_i (mod\ 11) \\
&= 1(0) + 2(0) + 3(7) + 4(2) + 5(8) + 6(8) + \\
&\quad 7(0) + 8(0) + 9(8)\ (mod\ \ 11) \\
&= 0 + 0 + 10 + 8 + 7 + 4 + 0 + 0 + 6\ (mod\ \ 11) \\
&= 2
\end{aligned}$$

- O CPF(Cadastro de Pessoas Físicas) $x_1x_2\ldots x_{10}x_{11}$ é constituído de 11 dígitos, sendo um primeiro bloco de 9 algarismos e um segundo, com mais dois algarismo, chamados de dígitos de verificação.
- O primeiro dígito é obtido da seguinte maneira:

$$x_{10} = \sum_{i=1}^{9} ix_i (mod\ 11) \tag{12}$$

- O segundo dígito verificador é obtido da seguinte maneira:

$$x_{10} = \sum_{i=0}^{9} ix_{i+1} (mod\ 11) \tag{13}$$

Aplicação: CPF

Exemplo

Se o CPF de uma pessoa tem os seguintes 9 primeiros dígitos: 235.343.104. Quais são os dígitos verificadores deste CPF?

Aplicação: CPF

Exemplo

Se o CPF de uma pessoa tem os seguintes 9 primeiros dígitos: 235.343.104. Quais são os dígitos verificadores deste CPF?

$$\begin{aligned} x_{10} &= \sum_{i=1}^{9} ix_i (mod\ 11) \\ &= 1(2) + 2(3) + 3(5) + 4(3) + 5(4) + 6(3) + \\ &\quad 7(1) + 8(0) + 9(4)\ (mod\ \ 11) \\ &= 2 + 6 + 4 + 1 + 9 + 7 + 7 + 0 + 3\ (mod\ \ 11) \\ &= 6 \end{aligned}$$

Aplicação: CPF

Exemplo

Se o CPF de uma pessoa tem os seguintes 9 primeiros dígitos: 235.343.104. Quais são os dígitos verificadores deste CPF?

$$
\begin{aligned}
x_{10} &= \textstyle\sum_{i=1}^{9} ix_i (mod\ 11) \\
&= 1(2) + 2(3) + 3(5) + 4(3) + 5(4) + 6(3) + \\
&\quad 7(1) + 8(0) + 9(4)\ (mod\ \ 11) \\
&= 2 + 6 + 4 + 1 + 9 + 7 + 7 + 0 + 3\ (mod\ \ 11) \\
&= 6 \\
x_{11} &= \textstyle\sum_{i=0}^{9} ix_{i+1} (mod\ 11) \\
&= 0(2) + 1(3) + 2(5) + 3(3) + 4(4) + 5(3) + \\
&\quad 6(1) + 7(0) + 8(4) + 9(6)\ (mod\ \ 11) \\
&= 0 + 3 + 10 + 9 + 5 + 4 + 6 + 0 + 10 + 10\ (mod\ \ 11) \\
&= 2
\end{aligned}
$$

Geração de números pseudo-aleatórios

- Um gerador de número pseudo-aleatório é um algoritmo que gera uma sequência de números que não é verdadeiramente aleatório, mas que aproxima algumas das propriedades dos números aleatórios.
- Os geradores congruentes lineares são os algoritmos mais conhecidos e possuem a seguinte fórmula de recorrência

$$x_{n+1} = ax_n + c(mod\ m) \tag{14}$$

Geração de números pseudo-aleatórios

Exemplo

Qual é a sequência pseudo-aleatória gerada por $m = 9$, $a = 7$, $c = 4$ *e* $x_0 = 3$.

$$
\begin{aligned}
x_0 &= 3 \\
x_1 &= 7x_0 + 4 \ mod\ 9 &= 7 \\
x_2 &= 7x_1 + 4 \ mod\ 9 &= 8 \\
x_3 &= 7x_2 + 4 \ mod\ 9 &= 6 \\
x_4 &= 7x_3 + 4 \ mod\ 9 &= 1 \\
x_5 &= 7x_3 + 4 \ mod\ 9 &= 2 \\
x_6 &= 7x_3 + 4 \ mod\ 9 &= 0 \\
x_7 &= 7x_3 + 4 \ mod\ 9 &= 4 \\
x_8 &= 7x_3 + 4 \ mod\ 9 &= 5 \\
x_9 &= 7x_3 + 4 \ mod\ 9 &= 3
\end{aligned}
$$

A sequência gerada é : 3,7,8,6,1,2,0,4,5,. . .

- Quando a sequência atinge um valor já gerado, dizemos que ela forma um ciclo.
- O comprimento do ciclo gerado é chamado período do gerador.
- Quando o período é igual a m, dizemos que o gerador é de período completo.
- Quando o gerado é de período completo, qualquer semente produzirá o ciclo inteiro.
- Quando $c = 0$, chamamos de **gerador multiplicativo puro**.
- Para $m = 2^31 - 1$,$a = 16807$, período $= 2^31 - 2$.

Exercícios

1. Se $a \equiv b (\textbf{mod } m)$ então $b \equiv a (\textbf{mod } m)$.
2. Se $a \equiv b (\textbf{mod } m)$ e $b \equiv c (\textbf{mod } m)$ então $a \equiv c (\textbf{mod } m)$.
3. Se $a \equiv b (\textbf{mod } m)$ sse existe um $k \in \mathbb{Z}$ tal que $a = b + km$.
4. Se $a \equiv b (\textbf{mod } m)$ e $c \equiv d (\textbf{mod } m)$ então $a + c \equiv b + d (\textbf{mod } m)$.
5. Se $a \equiv b (\textbf{mod } m)$ e $c \equiv d (\textbf{mod } m)$ então $a - c \equiv b - d (\textbf{mod } m)$.
6. Por que se m divide $a - b$ significa que a e b tem o mesmo resto considerando a divisão por m?
7. Mostre que para todo inteiro a, $a^2 \equiv 0 (\textbf{mod } 4)$ ou $a^2 \equiv 1 (\textbf{mod } 4)$.

Exercícios

1. Mostre um contra-exemplo a seguinte proposição se $ac \equiv bc (\textbf{mod}\ m)$ então $a \equiv b (\textbf{mod}\ m)$.
2. Mostre um contra-exemplo a seguinte proposição se $a \equiv b (\textbf{mod}\ m)$ e $c \equiv d (\textbf{mod}\ m)$ então $a^c \equiv b^d (\textbf{mod}\ m)$.
3. Mostre um contra-exemplo se $ab \equiv 0 (\textbf{mod}\ m)$ então $a \equiv 0 (\textbf{mod}\ m)$ ou $b \equiv 0 (\textbf{mod}\ m)$.
4. Mostre que se $a|b$ e $b|a$, onde a e b são inteiros, então $a = b$ ou $a = -b$.
5. Mostre que se a,b e c são inteiros, onde $a \neq 0$, tal que $a|c$ e $b|d$ então $ab|cd$.
6. 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 $a - c \equiv b - d (\textbf{mod}\ m)$.