Divisibilidade e Aritmética Modular
Matemática Discreta

Prof. MSc. Samy Sá

Universidade Federal do Ceará
Campus de Quixadá

12 de março de 2014

Outline

Introdução

Divisão

O Algoritmo de Divisão

Aritmética Modular

Aritmética de Módulo m

Avisos

Outline

Introdução

Divisão

O Algoritmo de Divisão

Aritmética Modular

Aritmética de Módulo m

Avisos

Introdução

- A divisão de inteiros produz um resultado e um resto.
- A aritmética modular permite trabalharmos com restos de divisão.
- Aplicações incluem a geração de números pseudo-aleatórios, alocação de memória para arquivos, e criptografia.

Outline

Introdução

Divisão

O Algoritmo de Divisão

Aritmética Modular

Aritmética de Módulo m

Avisos

Divisão

Definição

Se a e b são inteiros, com $a \neq 0$, dizemos que a divide b se existe um inteiro c tal que $b = ac$ ou, equivalentemente, se $\frac{b}{a}$ é um inteiro.

Divisão

Definição

Se a e b são inteiros, com $a \neq 0$, dizemos que a divide b se existe um inteiro c tal que $b = ac$ ou, equivalentemente, se $\frac{b}{a}$ é um inteiro.

Definição

Quando a divide b, dizemos que a é um fator ou divisor de b e que b é um múltiplo de a. A notação $a|b$ denota que a divide b. Escrevemos $a \nmid b$ para sinalizar que a não divide b.

Divisão

PERGUNTA:

Sejam n e d números inteiros, $n \neq 0$. Quantos inteiros positivos que não excedem n são divisíveis por d?

Divisão

PERGUNTA:

Sejam n e d números inteiros, $n \neq 0$. Quantos inteiros positivos que não excedem n são divisíveis por d?

O número de inteiros positivos que não execedem n é a quantidade de inteiros k tal que $0 < dk \leq n$.

Divisão

PERGUNTA:

Sejam n e d números inteiros, $n \neq 0$. Quantos inteiros positivos que não excedem n são divisíveis por d?

O número de inteiros positivos que não execedem n é a quantidade de inteiros k tal que $0 < dk \leq n$. Podemos dividir a desigualdade por d e obter $0 < k \leq n/d$.

Divisão

PERGUNTA:

Sejam n e d números inteiros, $n \neq 0$. Quantos inteiros positivos que não excedem n são divisíveis por d?

O número de inteiros positivos que não execedem n é a quantidade de inteiros k tal que $0 < dk \leq n$. Podemos dividir a desigualdade por d e obter $0 < k \leq n/d$. Portanto, temos $\lfloor n/d \rfloor$ inteiros positivos divisíveis por d e que não excedem n.

Divisão

Teorema

Sejam a, b e c inteiros, onde $a \neq 0$. Então:

(i) *Se $a|b$ e $a|c$, então $a|(b+c)$;*

(ii) *Se $a|b$, então $a|bc$ para todo inteiro c;*

(iii) *Se $a|b$ e $b|c$, então $a|c$.*

Divisão

Teorema

Sejam a, b e c inteiros, onde $a \neq 0$. Então:

(i) *Se $a|b$ e $a|c$, então $a|(b+c)$;*

(ii) *Se $a|b$, então $a|bc$ para todo inteiro c;*

(iii) *Se $a|b$ e $b|c$, então $a|c$.*

Prova

Daremos uma prova direta de (i). Suponha que $a|b$ e $a|c$. Então existem inteiros s e t tais que $b = as$ e $c = at$. Portanto, $b + c = as + at = a(s + t)$. Como $s + t$ é um inteiro, a divide $b + c$.

Divisão

Teorema

Sejam a, b e c inteiros, onde $a \neq 0$. Então:

(i) *Se $a|b$ e $a|c$, então $a|(b+c)$;*

(ii) *Se $a|b$, então $a|bc$ para todo inteiro c;*

(iii) *Se $a|b$ e $b|c$, então $a|c$.*

Prova

Daremos uma prova direta de (i). Suponha que $a|b$ e $a|c$. Então existem inteiros s e t tais que $b = as$ e $c = at$. Portanto, $b + c = as + at = a(s + t)$. Como $s + t$ é um inteiro, a divide $b + c$.

Exercício:

Demonstre os items (ii) e (iii) do teorema.

Divisão

Corolário

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

Divisão

Corolário

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

Prova

Pela parte (ii) do teorema anterior, vemos que $a|mb$ e que $a|nc$.
Pela parte (i), concluímos que $a|mb + nc$.

Outline

Introdução

Divisão

O Algoritmo de Divisão

Aritmética Modular

Aritmética de Módulo m

Avisos

O Algoritmo de Divisão

Quando um inteiro é divido por outro inteiro, há um quociente e um resto.

Teorema

Seja a um inteiro qualquer e d um inteiro positivo, então existem inteiros únicos q e r, com $0 \leq r \leq d$, e tais que $a = dq + r$.

O Algoritmo de Divisão

Definição

Em uma igualdade $a = dq + r$ como no algoritmo de divisão,

- *d é chamado divisor;*
- *a é chamado dividendo;*
- *q é chamado quociente;*
- *r é chamado resto.*

O Algoritmo de Divisão

Definição

Em uma igualdade $a = dq + r$ como no algoritmo de divisão,

- *d é chamado divisor;*
- *a é chamado dividendo;*
- *q é chamado quociente;*
- *r é chamado resto.*

*Usamos a seguinte notação pra expressar o quociente e o resto: $q = a$ **div** d, $r = a$ **mod** d.*

O Algoritmo de Divisão

Definição

Em uma igualdade $a = dq + r$ como no algoritmo de divisão,

- *d é chamado divisor;*
- *a é chamado dividendo;*
- *q é chamado quociente;*
- *r é chamado resto.*

*Usamos a seguinte notação pra expressar o quociente e o resto: $q = a$ **div** d, $r = a$ **mod** d.*

Constatação:

*Para um d qualquer fixo, a **div** d e a **mod** d são funções no conjunto dos inteiros.*

O Algoritmo de Divisão

PERGUNTA:

Qual o quociente e resto da divisão de 101 por 11?

O Algoritmo de Divisão

PERGUNTA:

Qual o quociente e resto da divisão de 101 por 11?

Temos que 101 = 11.9 + 2. Portanto...

- o quociente da divisão de 101 por 11 é $9 = 101$ **div** 11;
- e o resto da divisão é $2 = 101$ **mod** 11.

Outline

Introdução

Divisão

O Algoritmo de Divisão

Aritmética Modular

Aritmética de Módulo *m*

Avisos

Aritmética Modular

Concentra-se nos restos de divisões inteiras.

- Considere a representação de inteiros não negativos em 8 bits.
- Podemos representar inteiros 0 a 255, ou seja, 256 números.

Aritmética Modular

Concentra-se nos restos de divisões inteiras.

- Considere a representação de inteiros não negativos em 8 bits.
- Podemos representar inteiros 0 a 255, ou seja, 256 números.
- Se somarmos 240 + 130, o que teremos?

Aritmética Modular

Concentra-se nos restos de divisões inteiras.

- Considere a representação de inteiros não negativos em 8 bits.
- Podemos representar inteiros 0 a 255, ou seja, 256 números.
- Se somarmos 240 + 130, o que teremos?
- O resultado é 370, o que passa de 256 por 114.

Aritmética Modular

Concentra-se nos restos de divisões inteiras.

- Considere a representação de inteiros não negativos em 8 bits.
- Podemos representar inteiros 0 a 255, ou seja, 256 números.
- Se somarmos 240 + 130, o que teremos?
- O resultado é 370, o que passa de 256 por 114.
- Logo, a representação de 370 é a mesma de 114.

Aritmética Modular

Concentra-se nos restos de divisões inteiras.

Definição

Se j e k são inteiros e m é um inteiro positivo, então j é congruente a k no módulo m se m divide $j - k$.

Aritmética Modular

Concentra-se nos restos de divisões inteiras.

Definição

Se j e k são inteiros e m é um inteiro positivo, então j é congruente a k no módulo m se m divide $j - k$.

Definição

Usamos a notação $j \equiv k \pmod{m}$ para indicar que j é congruente a k no módulo m.

Aritmética Modular

Concentra-se nos restos de divisões inteiras.

Definição

Se j e k são inteiros e m é um inteiro positivo, então j é congruente a k no módulo m se m divide $j - k$.

Definição

Usamos a notação $j \equiv k \pmod{m}$ para indicar que j é congruente a k no módulo m. Dizemos que $j \equiv k \pmod{m}$ é uma congruência e que m é o seu módulo.

Aritmética Modular

Concentra-se nos restos de divisões inteiras.

Definição

Se j e k são inteiros e m é um inteiro positivo, então j é congruente a k no módulo m se m divide $j - k$.

Definição

Usamos a notação $j \equiv k \pmod{m}$ para indicar que j é congruente a k no módulo m. Dizemos que $j \equiv k \pmod{m}$ é uma congruência e que m é o seu módulo. Se j e k não são congruentes pelo módulo m, escrevemos $j \not\equiv k \pmod{m}$.

Aritmética Modular

Concentra-se nos restos de divisões inteiras.

Definição

Se j e k são inteiros e m é um inteiro positivo, então j é congruente a k no módulo m se m divide $j - k$.

Definição

Usamos a notação $j \equiv k \pmod{m}$ para indicar que j é congruente a k no módulo m. Dizemos que $j \equiv k \pmod{m}$ é uma congruência e que m é o seu módulo. Se j e k não são congruentes pelo módulo m, escrevemos $j \not\equiv k \pmod{m}$.

IMPORTANTE!!!

*Embora $j \equiv k \pmod{m}$ e j **mod** $m = k$ sejam escritos com "mod", os dois representam conceitos diferentes!*

Aritmética Modular

Exemplo

Determine se 17 é congruente a 5 no módulo 6.

- Porque 6 divide 17-5, observamos que $17 \equiv 5$ (*mod* 6).

Aritmética Modular

Exemplo

Determine se 17 é congruente a 5 no módulo 6.

- Porque 6 divide 17-5, observamos que $17 \equiv 5$ (*mod* 6).

Exemplo

Determine se 24 é congruente a 14 no módulo 6.

- Uma vez que 6 divide 24-14, temos que $24 \not\equiv 14$ (*mod* 6).

Aritmética Modular

Teorema

*Sejam a e b inteiros e seja m um inteiro positivo, então $a \equiv b \pmod{m}$ se e somente se a **mod** $m = b$ **mod** m.*

Prova

Deixada como exercício.

Aritmética Modular

Teorema

Seja m um inteiro positivo. Os inteiros a e b são congruentes no módulo m se e somente se existe um inteiro k tal que $a = b + km$.

Prova

Deixada como exercício.

Aritmética Modular

O seguinte teorema sugere que adição e multiplicação preservam as congruências.

Teorema

Seja m inteiro positivo, se $a \equiv b \pmod{m}$ *e* $c \equiv d \pmod{m}$, *então*

$$a + c \equiv b + d \pmod{m} \text{ e } ac \equiv bd \pmod{m}.$$

Prova

Deixada como exercício.

Aritmética Modular

O seguinte teorema sugere que adição e multiplicação preservam as congruências.

Corolário

Seja m um inteiro positivo e a, b inteiros, então

$$(a + b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$$

Aritmética Modular

O seguinte teorema sugere que adição e multiplicação preservam as congruências.

Corolário

Seja m um inteiro positivo e a, b inteiros, então

$$(a+b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$$
$$e$$
$$(ab) \bmod m = ((a \bmod m)(b \bmod m)) \bmod m.$$

Prova

Deixada como exercício.

Outline

Introdução

Divisão

O Algoritmo de Divisão

Aritmética Modular

Aritmética de Módulo m

Avisos

Aritmética de Módulo m

Envolve definirmos operações aritméticas no conjunto $\mathbb{Z}_m$, o conjunto dos inteiros não negativos menores que m, ou seja,

$$\mathbb{Z}_m = \{0, 1, 2, ..., m-1\}.$$

Aritmética de Módulo m

Envolve definirmos operações aritméticas no conjunto $\mathbb{Z}_m$, o conjunto dos inteiros não negativos menores que m, ou seja,

$$\mathbb{Z}_m = \{0, 1, 2, ..., m-1\}.$$

Definição

*Denotamos a soma no módulo m por $+_m$. Definimos essa operação como $a +_m b = (a + b)$ **mod** m.*

Aritmética de Módulo m

Envolve definirmos operações aritméticas no conjunto $\mathbb{Z}_m$, o conjunto dos inteiros não negativos menores que m, ou seja,

$$\mathbb{Z}_m = \{0, 1, 2, ..., m-1\}.$$

Definição

*Denotamos a soma no módulo m por $+_m$. Definimos essa operação como $a +_m b = (a + b)$ **mod** m.*

Exemplo

$7 +_{11} 9 = (7 + 9)$ ***mod*** $11 = 16$ ***mod*** $11 = 5$.

Aritmética de Módulo m

Envolve definirmos operações aritméticas no conjunto $\mathbb{Z}_m$, o conjunto dos inteiros não negativos menores que m, ou seja,

$$\mathbb{Z}_m = \{0, 1, 2, ..., m-1\}.$$

Definição

*Denotamos a multiplicação no módulo m por $\cdot_m$. Definimos essa operação como $a \cdot_m b = (a \cdot b)$ **mod** m.*

Aritmética de Módulo m

Envolve definirmos operações aritméticas no conjunto $\mathbb{Z}_m$, o conjunto dos inteiros não negativos menores que m, ou seja,

$$\mathbb{Z}_m = \{0, 1, 2, ..., m-1\}.$$

Definição

*Denotamos a multiplicação no módulo m por $\cdot_m$. Definimos essa operação como $a \cdot_m b = (a \cdot b)$ **mod** m.*

Exemplo

$7 \cdot_{11} 9 = (7 \cdot 9)$ **mod** $11 = 63$ **mod** $11 = 8$.

Propriedades das Operações no Módulo m

As operações $+_m$ e $\cdot_m$ satisfazem muitas propriedades comuns à adição e multiplicação comum de inteiros.

- **Fechamento**: se a e b pertencem a $\mathbb{Z}_m$, então

$$a +_m b \text{ e } a \cdot_m b \text{ pertencem a } \mathbb{Z}_m;$$

Propriedades das Operações no Módulo m

As operações $+_m$ e $\cdot_m$ satisfazem muitas propriedades comuns à adição e multiplicação comum de inteiros.

- **Fechamento**: se a e b pertencem a $\mathbb{Z}_m$, então

$$a +_m b \text{ e } a \cdot_m b \text{ pertencem a } \mathbb{Z}_m;$$

- **Associatividade**: se a, b, c pertencem a $\mathbb{Z}_m$, então

$$(a +_m b) +_m c = a +_m (b +_m c)$$

Propriedades das Operações no Módulo m

As operações $+_m$ e $\cdot_m$ satisfazem muitas propriedades comuns à adição e multiplicação comum de inteiros.

- **Fechamento**: se a e b pertencem a $\mathbb{Z}_m$, então

$$a +_m b \text{ e } a \cdot_m b \text{ pertencem a } \mathbb{Z}_m;$$

- **Associatividade**: se a, b, c pertencem a $\mathbb{Z}_m$, então

$$(a +_m b) +_m c = a +_m (b +_m c) \text{ e}$$
$$(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c);$$

Propriedades das Operações no Módulo m

As operações $+_m$ e $\cdot_m$ satisfazem muitas propriedades comuns à adição e multiplicação comum de inteiros.

- **Fechamento**: se a e b pertencem a $\mathbb{Z}_m$, então

$$a +_m b \text{ e } a \cdot_m b \text{ pertencem a } \mathbb{Z}_m;$$

- **Associatividade**: se a, b, c pertencem a $\mathbb{Z}_m$, então

$$(a +_m b) +_m c = a +_m (b +_m c) \text{ e}$$
$$(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c);$$

- **Comutatividade**: se a, b pertencem a $\mathbb{Z}_m$, então

$$a +_m b = b +_m a$$

Propriedades das Operações no Módulo m

As operações $+_m$ e $\cdot_m$ satisfazem muitas propriedades comuns à adição e multiplicação comum de inteiros.

- **Fechamento**: se a e b pertencem a $\mathbb{Z}_m$, então

$$a +_m b \text{ e } a \cdot_m b \text{ pertencem a } \mathbb{Z}_m;$$

- **Associatividade**: se a, b, c pertencem a $\mathbb{Z}_m$, então

$$(a +_m b) +_m c = a +_m (b +_m c) \text{ e}$$
$$(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c);$$

- **Comutatividade**: se a, b pertencem a $\mathbb{Z}_m$, então

$$a +_m b = b +_m a \text{ e}$$
$$a \cdot_m b = b \cdot_m a;$$

Propriedades das Operações no Módulo m

As operações $+_m$ e $\cdot_m$ satisfazem muitas propriedades comuns à adição e multiplicação comum de inteiros.

- **Identidade**: 0 e 1 são elementos de identidade da soma e multiplicação, respectivamente. Isto é, se a pertence a $\mathbb{Z}_m$,

$$a +_m 0 = a$$

Propriedades das Operações no Módulo m

As operações $+_m$ e $\cdot_m$ satisfazem muitas propriedades comuns à adição e multiplicação comum de inteiros.

- **Identidade**: 0 e 1 são elementos de identidade da soma e multiplicação, respectivamente. Isto é, se a pertence a $\mathbb{Z}_m$,

$$a +_m 0 = a \text{ e}$$
$$a \cdot_m 1 = a;$$

Propriedades das Operações no Módulo m

As operações $+_m$ e $\cdot_m$ satisfazem muitas propriedades comuns à adição e multiplicação comum de inteiros.

- **Identidade**: 0 e 1 são elementos de identidade da soma e multiplicação, respectivamente. Isto é, se a pertence a $\mathbb{Z}_m$,

$$a +_m 0 = a \text{ e}$$
$$a \cdot_m 1 = a;$$

- **Inverso Aditivo**: se $a \neq 0$ pertence a $\mathbb{Z}_m$, então $m - a$ é o aditivo inverso de a no módulo m. O 0 é o aditivo inverso de si mesmo. Isso significa que

$$a +_m (m - a) = 0$$

Propriedades das Operações no Módulo m

As operações $+_m$ e $\cdot_m$ satisfazem muitas propriedades comuns à adição e multiplicação comum de inteiros.

- **Identidade**: 0 e 1 são elementos de identidade da soma e multiplicação, respectivamente. Isto é, se a pertence a $\mathbb{Z}_m$,

$$a +_m 0 = a \text{ e}$$
$$a \cdot_m 1 = a;$$

- **Inverso Aditivo**: se $a \neq 0$ pertence a $\mathbb{Z}_m$, então $m - a$ é o aditivo inverso de a no módulo m. O 0 é o aditivo inverso de si mesmo. Isso significa que

$$a +_m (m - a) = 0 \text{ e}$$
$$0 +_m 0 = 0;$$

Propriedades das Operações no Módulo m

As operações $+_m$ e $\cdot_m$ satisfazem muitas propriedades comuns à adição e multiplicação comum de inteiros.

- **Identidade**: 0 e 1 são elementos de identidade da soma e multiplicação, respectivamente. Isto é, se a pertence a $\mathbb{Z}_m$,

$$a +_m 0 = a \text{ e}$$
$$a \cdot_m 1 = a;$$

- **Inverso Aditivo**: se $a \neq 0$ pertence a $\mathbb{Z}_m$, então $m - a$ é o aditivo inverso de a no módulo m. O 0 é o aditivo inverso de si mesmo. Isso significa que

$$a +_m (m - a) = 0 \text{ e}$$
$$0 +_m 0 = 0;$$

- **Distributividade**: se a, b, c pertencem a $\mathbb{Z}_m$, então

$$a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c);$$

Outline

Introdução

Divisão

O Algoritmo de Divisão

Aritmética Modular

Aritmética de Módulo m

Avisos

Avisos

- Leitura Complementar + Exercícios na quinta.
- Lembre: Teste 03 no dia 17/03.