Aritmética Modular

Matemática Discreta

Prof. Samy Sá

Universidade Federal do Ceará
Campus de Quixadá

29 de agosto de 2020

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Roteiro

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Prévia

Requisitos

- Técnicas de Demonstração de Teoremas
- Propriedades de operações aritméticas
- Divisibilidade

Esta apresentação...

- Introduz conceitos de Aritmética Modular
- Explora teoremas sobre congruências modulares e propriedades das operações em uma aritmética modular.

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Na Aula Passada...

Definição (Divisibilidade)

*Sejam a e b números inteiros com $a \neq 0$, dizemos que a **divide** b se e somente se **existe um inteiro** c **tal que** $b = ac$.*

Teorema (Propriedades de $|$)

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

1. *Se $a \mid b$ e $a \mid c$, então $a \mid (b + c)$;*
2. *Se $a \mid b$, então $a \mid b.c$ para todo c inteiro;*
3. *Se $a \mid b$ e $b \mid c$, então $a \mid c$.*

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Na Aula Passada...

Teorema (Algoritmo da Divisão)

Seja n um inteiro qualquer e d um inteiro positivo, existe ***um único par de inteiros*** *q e r com $0 \leq r < d$ tais que $n = d.q + r$.*

Definição

Sejam n, d, q, r inteiros tais que $d > 0$, $n = dq + r$ e $0 \leq r < d$, definimos as funções ***div*** *e* ***mod*** *tais que*

- n ***div*** $d = q$ ***(divisão inteira ou com resto)***
- n ***mod*** $d = r$ ***(módulo/resto da divisão)***

*** Concluímos que a definição de divisibilidade é o caso particular do Algoritmo da Divisão com $r = 0$.**

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Na Aula Passada...

Teorema (Algoritmo da Divisão)

Seja n um inteiro qualquer e d um inteiro positivo, existe ***um único par de inteiros*** *q e r com $0 \leq r < d$ tais que $n = d.q + r$.*

Definição

Sejam n, d, q, r inteiros tais que $d > 0$, $n = dq + r$ e $0 \leq r < d$, definimos as funções ***div*** *e* ***mod*** *tais que*

- n ***div*** $d = q$ ***(divisão inteira ou com resto)***
- n ***mod*** $d = r$ ***(módulo/resto da divisão)***

Teorema (*)

Sejam a, b inteiros com $a \neq 0$, então
a ***divide*** *b se e somente se b* ***mod*** *$a = 0$.*

Samy Sá (samy@ufc.br)

Roteiro

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Aritmética Modular

Concentra-se nos restos de divisões inteiras.

Exemplo (Motivação)

Considere um tipo numérico de 8 *bits representando inteiros em* $[0, 255]$

O que acontece ser somarmos $240 + 130$*?*

Em bitcode, teremos $\overbrace{\underbrace{11110000}_{8bits}}^{240} + \overbrace{\underbrace{10000010}_{8bits}}^{130} = \overbrace{\underbrace{101110010}_{9bits}}^{370}$

Como só temos 8 bits, ficaremos com $\cancel{1}$01110010*, ou seja, com* 114*.*

Interessante (1/3): *neste sistema,* $240 + 130 = 114$ *...*

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Aritmética Modular

Concentra-se nos restos de divisões inteiras.

Exemplo (Motivação)

Considere um tipo numérico de 8 *bits representando inteiros em* $[0, 255]$

O que acontece ser somarmos $240 + 130$*?*

Em bitcode, teremos $\underbrace{\overbrace{11110000}^{240}}_{8bits} + \underbrace{\overbrace{10000010}^{130}}_{8bits} = \underbrace{\overbrace{101110010}^{370}}_{9bits}$

Como só temos 8 bits, ficaremos com $\cancel{1}01110010$*, ou seja, com* 114*.*

Interessante (2/3): *neste sistema,* 370 *e* 114 *são ambos representados como "*01110010*"*

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Aritmética Modular

Concentra-se nos restos de divisões inteiras.

Exemplo (Motivação)

Considere um tipo numérico de 8 *bits representando inteiros em* $[0, 255]$

O que acontece ser somarmos $240 + 130$*?*

Em bitcode, teremos $\underbrace{\overbrace{11110000}^{240}}_{8bits} + \underbrace{\overbrace{10000010}^{130}}_{8bits} = \underbrace{\overbrace{101110010}^{370}}_{9bits}$

Como só temos 8 bits, ficaremos com $\cancel{1}$01110010*, ou seja, com* 114*.*

Interessante (3/3): *por acaso (?),* 370 ***div*** $256 = 1$
e 370 ***mod*** $256 = 114$

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Roteiro

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Congruência Modular

Definição (Congruência no Módulo m)

*Dados j, k inteiros e m inteiro positivo, dizemos que "j **é congruente a** k **no módulo** m" **se e somente se** $m \mid (j - k)$.*

Exemplos (Positivos)

1. $370 - 114 = 256$,
que é divisível por 256, *pois* 256 ***mod*** $256 = 0$
Logo, 370 ***é*** *congruente a* 114 *no módulo* 256

2. $370 - (-142) = 512$,
que é divisível por 256, *pois* 512 ***mod*** $256 = 0$
Logo, 370 ***é*** *congruente a* -142 *no módulo* 256

3. $-142 - 114 = -256$,
que é divisível por 256, *pois* -256 ***mod*** $256 = 0$
Logo, -142 ***é*** *congruente a* 114 *no módulo* 256

Samy Sá (samy@ufc.br)

Congruência Modular

Definição (Congruência no Módulo m)

Dados j, k inteiros e m inteiro positivo, dizemos que
*"j **é congruente a** k **no módulo** m" **se e somente se** $m \mid (j - k)$.*

Exemplos (Negativos)

1. $400 - 114 = 286$,
   que não é divisível por 256, *pois* 286 ***mod*** $256 = 30$,
   ou seja, 400 ***não é*** *congruente a* 114 *no módulo* 256
2. $370 - 400 = -30$,
   que não é divisível por 256, *pois* -30 ***mod*** $256 = 226$,
   ou seja, 370 ***não é*** *congruente a* 400 *no módulo* 256

Você consegue encontrar mais números congruentes a 114 no módulo 256? O que eles têm em comum?

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Congruência Modular

Definição (Congruência no Módulo m)

Dados j, k inteiros e m inteiro positivo, dizemos que
*"j **é congruente a** k **no módulo** m" **se e somente se** $m \mid (j - k)$.*

Notação

- *Escreve-se "$j \equiv k \pmod{m}$" para dizer que "j **é** congruente a k no módulo m"*
- *Escreve-se "$j \not\equiv k \pmod{m}$" para dizer o contrário, ou seja, que "j **não é** congruente a k no módulo m"*

Exemplo

1. $370 \equiv 114$ $(mod\ 256)$
2. $370 \equiv -142$ $(mod\ 256)$
3. $-142 \equiv 114$ $(mod\ 256)$
4. $400 \not\equiv 114$ $(mod\ 256)$
5. $370 \not\equiv 400$ $(mod\ 256)$

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Congruência Modular

Definição (Congruência no Módulo m)

*Dados j, k inteiros e m inteiro positivo, dizemos que "j **é congruente a** k **no módulo** m" **se e somente se** $m \mid (j - k)$.*

Notação

- *Escreve-se "$j \equiv k \pmod{m}$" para dizer que "j é congruente a k no módulo m"*
- *Escreve-se "$j \not\equiv k \pmod{m}$" para dizer o contrário, ou seja, que "j **não é** congruente a k no módulo m"*

Obs. 1: Embora "$j \equiv k \pmod{m}$" e "$j \textbf{ mod } m = k$" sejam ambos escritos com "mod", estas expressões têm significados muito diferentes!

Congruência Modular

Definição (Congruência no Módulo m (Reescrita))

Dados j, k inteiros e m inteiro positivo, dizemos que

*"$j \equiv k \pmod{m}$" **se e somente se** $m \mid (j - k)$.*

Notação

- *Escreve-se "$j \equiv k \pmod{m}$" para dizer que "j **é** congruente a k no módulo m"*
- *Escreve-se "$j \not\equiv k \pmod{m}$" para dizer o contrário, ou seja, que "j **não é** congruente a k no módulo m"*

Obs. 1: Embora "$j \equiv k \pmod{m}$" e "$j \textbf{ mod } m = k$" sejam ambos escritos com "mod", estas expressões têm significados muito diferentes!

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Congruência Modular

Definição (Congruência no Módulo m (Reescrita))

Dados j, k inteiros e m inteiro positivo, dizemos que

"$j \equiv k \pmod m$" ***se e somente se*** $m \mid (j - k)$.

Notação

- *Escreve-se "$j \equiv k \pmod m$" para dizer que "j* ***é*** *congruente a k no módulo m"*
- *Escreve-se "$j \not\equiv k \pmod m$" para dizer o contrário, ou seja, que "j* ***não é*** *congruente a k no módulo m"*

Obs. 2: Dizemos que uma expressão do tipo "$j \equiv k \pmod m$" é uma **congruência** e que m é o seu módulo.

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Roteiro

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Propriedades de Congruências Modulares

Teorema

Seja m um inteiro positivo, $n \equiv n \ (mod\ m)$ para todo n inteiro.

Prova

1. *Seja m um inteiro positivo qualquer e n um inteiro qualquer (instanciação),*
2. *Basta notar que $n - n = 0$ é múltiplo de m, pois existe um inteiro k tal que $0 = k.m$ (neste caso, teríamos $k = 0$). Ou seja, $m \mid n - n$ (definição de divisibilidade).*
3. *Logo, $n \equiv n \ (mod\ m)$ (definição de congruência modular).*

Comentário. Após a instanciação, precisaríamos concluir que $n \equiv n \ (mod\ m)$. Um caminho possível é através da **definição de congruência modular**, que nos diz que $n \equiv n \ (mod\ m)$ **se e somente se** $m \mid n - n$.

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Propriedades de Congruências Modulares

Teorema

Seja m um inteiro positivo, $n \equiv 0 \pmod{m}$ se e somente se $m \mid n$.

Prova

Seja m um inteiro positivo qualquer e n um inteiro qualquer (instanciação).

($\Rightarrow$) *Precisaremos provar que "se $n \equiv 0 \pmod{m}$, então $m \mid n$".*

1. *Por prova direta, suponha que $n \equiv 0 \pmod{m}$.*
2. *Pela definição de congruência modular, isso significa que $m \mid n - 0$.*
3. *Logo, $m \mid n$.*

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Propriedades de Congruências Modulares

Teorema

Seja m um inteiro positivo, $n \equiv 0 \pmod{m}$ se e somente se $m \mid n$.

Prova

Seja m um inteiro positivo qualquer e n um inteiro qualquer (instanciação).

($\Rightarrow$) *Precisaremos provar que "se $n \equiv 0 \pmod{m}$, então $m \mid n$". (**provado**)*

($\Leftarrow$) *Precisaremos provar que "se $m \mid n$, então $n \equiv 0 \pmod{m}$".*

1. *Por prova direta, suponha que $m \mid n$.*
2. *Pela definição de divisibilidade, existe um $k \in \mathbb{Z}$ tal que $n = km$.*
3. *Como seria conveniente concluir algo sobre $n - 0$, vamos substrair 0 de ambos os lados da equação. Obtemos que $n - 0 = km - 0$.*
4. *Ajustando a equação, temos $n - 0 = km$, o que nos diz que $m \mid n - 0$ (divisibilidade).*
5. *Logo, $n \equiv 0 \pmod{m}$.*

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Propriedades de Congruências Modulares

Teorema

Seja m um inteiro positivo, $n \equiv 0 \pmod{m}$ *se e somente se* $m \mid n$.

Corolário

Seja m um inteiro positivo, $n \equiv 0 \pmod{m}$ *se e somente se* n ***mod*** $m = 0$.

Prova

Segue pela combinação do teorema anterior com outro que fornecemos na aula anterior, garantindo que $m \mid n$ *se e somente se* n ***mod*** $m = 0$ *para todo n inteiro e m inteiro positivo.*

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Propriedades de Congruências Modulares

Teorema

Seja m um inteiro positivo,

$j \equiv k \ (mod \ m)$ *se e somente se* $k \equiv j \ (mod \ m)$.

Prova

Deixada como exercício.

DICA. Para provar ($\Rightarrow$), após instanciar as variáveis, use a definição de congruência, depois a de divisibilidade. Multiplique a equação por -1 e desfaça os passos anteriores. A prova de ($\Leftarrow$) segue exatamente os mesmos passos, podendo ser dispensada.

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Propriedades de Congruências Modulares

Teorema

Seja m um inteiro positivo,
se $j \equiv k \pmod{m}$ e $l \equiv k \pmod{m}$, então $j \equiv l \pmod{m}$.

Prova

Deixada como exercício.

DICA. É possível construir uma demonstração com estrutura muito similar à da demonstração proposta para o teorema anterior.

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Outros Teoremas

Teorema

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

Teorema (SEMANA 05 - AT1)

Sejam j e k inteiros e m um inteiro positivo, então
j **mod** $m = k$ **mod** m *se e somente se* $m \mid j - k$.

As provas destes teoremas são deixadas como exercícios.

Outros Teoremas

Teorema

Seja m um inteiro positivo, então

$a \equiv b \pmod{m}$ *se e somente se existe* $k \in \mathbb{Z}$ *tal que* $a = b + km$.

Teorema

Seja m inteiro positivo,

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

$$a + c \equiv b + d \pmod{m} \quad e \quad a \,.\, c \equiv b \,.\, d \pmod{m}.$$

Teorema

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

$$(a + b) \textbf{ mod } m = ((a \textbf{ mod } m) + (b \textbf{ mod } m)) \textbf{ mod } m \quad e$$
$$(a \,.\, b) \textbf{ mod } m = ((a \textbf{ mod } m) \,.\, (b \textbf{ mod } m)) \textbf{ mod } m.$$

As provas destes teoremas são deixadas como exercícios.

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Roteiro

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Congruências e PAs

Definição (Congruência no Módulo *m* (Reescrita))

Dados j, k inteiros e m inteiro positivo, dizemos que

$$\text{“}j \equiv k \ (mod\ m)\text{”} \textit{ se e somente se } m \mid (j - k).$$

Considere o número 4 no módulo 7.
Qual será o primeiro inteiro $n > 4$ tal que $n \equiv 4\ (mod\ 7)$?

R.: Encontraremos $11 \equiv 4\ (mod\ 7)$ **E o próximo?**
R.: Encontraremos $18 \equiv 4\ (mod\ 7)$ **E o próximo?**

Conclusão. A cada passo, somaríamos 7 unidades ao resultado anterior.

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Congruências e PAs

Teorema

Seja m um inteiro positivo e k um inteiro qualquer, os termos de $f_n = k + n.m$ são tais que $f_i \equiv f_j \pmod{m}$ para todo $i, j \in \mathbb{Z}$.

Prova

Sejam m um inteiro positivo qualquer, k, i, j inteiros quaisquer,

1. *Desejamos concluir que $f_i \equiv f_j \pmod{m}$; baseado na definição de congruência, poderemos concluir isso se garantirmos que $m \mid f_i - f_j$.*
2. *Baseado na progressão aritmética fornecida, teremos $f_i = k + i.m$ e $f_j = k + j.m$.*
3. *Logo, podemos fazer* $$\begin{aligned} f_i - f_j &= (k + i.m) - (k + j.m) \\ &= k + i.m - k - j.m \\ &= \cancel{k} + i.m - \cancel{k} - j.m \\ &= \quad i.m \quad - j.m \\ &= \quad m.(i - j). \end{aligned}$$
4. *Ou seja, $m \mid f_i - f_j$.*
5. *Portanto, $f_i \equiv f_j \pmod{m}$.*

Roteiro

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Congruências e PGs

Podemos propor um teorema muito parecido sobre termos de um PG, mas ele só funcionará para alguns valores de *m* e *k*.

Teorema

*Seja m um inteiro positivo e k um inteiro qualquer, os termos de $g_n = k.m^n$ **serão** tais que $f_i \equiv f_j \pmod{m}$ para todo $i, j \in \mathbb{Z}$ **se e somente se** __________________ .*

Exemplo

Considere a PG $g_n = 5.3^n$. Pelo texto do teorema, trabalharemos com congruências de módulo $m = 3$ e termo "inicial" $k = 5$.

- *Quando $n = 2$, teremos $g_2 = 5.3^2 = 5.9 = 45$*
- *Quando $n = 1$, teremos $g_1 = 5.3^1 = 5.3 = 15$*
- *Quando $n = 0$, teremos $g_0 = 5.3^0 = 5.1 = 5$*

Note que $45 \equiv 15 \pmod{3}$, mas $45 \not\equiv 5 \pmod{3}$.

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Congruências e PGs

Podemos propor um teorema muito parecido sobre termos de um PG, mas ele só funcionará para alguns valores de m e k.

Teorema

*Seja m um inteiro positivo e k um inteiro qualquer, os termos de $g_n = k.m^n$ **serão** tais que $f_i \equiv f_j \pmod m$ para todo $i, j \in \mathbb{Z}$ **se e somente se** ________________ .*

Exercício:

Fixe m e uma PG. Explore valores possíveis do índice n para encontrar um padrão e sugira a condição necessária para completar o enunciado do teorema. Em seguida, prove ou desprove o teorema criado com sua sugestão.

PS.: Existe ao menos uma condição que tornará o teorema correto.

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Roteiro

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Aritmética de Módulo *m*

O que é “Aritmética”?

- É o ramo da matemática que estuda a manipulação de números e as propriedades de operações sobre estes.

O que torna uma Aritmética “Modular”?

- É uma aritmética restrita aos restos de divisão pelo “**módulo**” *m*.
- Após cada operação, aplica-se a função “ **mod** *m* ” para corrigir resultados

Exemplo

*Na **Aritmética de Módulo** 256, ao somar 240 e 130, faremos*

$$\underbrace{(240+130)\ \textbf{\textit{mod}}\ 256}_{\textit{soma modular}} = 370\ \textbf{\textit{mod}}\ 256 = \underbrace{114}_{\textit{resultado}}$$

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Aritmética de Módulo *m*

O que é "Aritmética"?

- É o ramo da matemática que estuda a manipulação de números e as propriedades de operações sobre estes.

O que torna uma Aritmética "Modular"?

- É uma aritmética restrita aos restos de divisão pelo "**módulo**" *m*.
- Após cada operação, aplica-se a função " **mod** *m* " para corrigir resultados

Exemplo

*Na **Aritmética de Módulo** 256, ao multiplicar 23 e 42, faremos*

$$\underbrace{(23.42)\ \textbf{\textit{mod}}\ 256}_{\text{multiplicação/produto modular}} = 966\ \textbf{\textit{mod}}\ 256 = \underbrace{198}_{\text{resultado}}$$

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Roteiro

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Aritmética de Módulo *m*

Definição (Domínio $\mathbb{Z}_m$)

*Dado um inteiro $m > 0$, o **domínio da aritmética de módulo** m será o conjunto $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$.*

Exemplos

A Aritmética ...

- *... de Módulo* 1 *tem como domínio* $\mathbb{Z}_1 = \{0\}$
- *... de Módulo* 2 *tem como domínio* $\mathbb{Z}_2 = \{0, 1\}$
- *... de Módulo* 5 *tem como domínio* $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$
- *... de Módulo* 12 *tem como domínio* $\mathbb{Z}_{12} = \{0, 1, \ldots, 11\}$
- *... de Módulo* 24 *tem como domínio* $\mathbb{Z}_{24} = \{0, 1, \ldots, 23\}$
- *... de Módulo* 60 *tem como domínio* $\mathbb{Z}_{60} = \{0, 1, \ldots, 59\}$
- *... de Módulo* 256 *tem como domínio* $\mathbb{Z}_{256} = \{0, 1, \ldots, 255\}$

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Aritmética de Módulo *m*

Definição (Operações em $\mathbb{Z}_m$)

Dado um inteiro $m > 0$ e $x, y \in \mathbb{Z}_m$,

- $x +_m y = (x + y)$ ***mod*** m — "**soma módulo** m"
- $x \cdot_m y = (x \, . \, y)$ ***mod*** m — "**multiplicação módulo** m"

Exemplos (Soma)

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

O que ocorre em $\mathbb{Z}_{11}$ é o seguinte:

$$\{0, \overbrace{1, 2, 3, 4, 5, 6, 7}^{\text{7 unidades}}, 8, 9, 10\}$$

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Aritmética de Módulo *m*

Definição (Operações em $\mathbb{Z}_m$)

Dado um inteiro $m > 0$ e $x, y \in \mathbb{Z}_m$,

- $x +_m y = (x + y)$ ***mod*** m — *"soma módulo m"*
- $x \cdot_m y = (x \,.\, y)$ ***mod*** m — *"multiplicação módulo m"*

Exemplos (Soma)

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

O que ocorre em $\mathbb{Z}_{11}$ é o seguinte:

$$\{0, \overbrace{1, 2, 3, 4, 5, 6, 7}^{\text{7 unidades}}, \overbrace{\underbrace{8, 9, 10}_{\text{3 unidades}}\} \quad \ldots ?}^{+ \text{ 9 unidades}}$$

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Aritmética de Módulo *m*

Definição (Operações em $\mathbb{Z}_m$)

Dado um inteiro $m > 0$ e $x, y \in \mathbb{Z}_m$,

- $x +_m y = (x + y)$ ***mod*** m — ***"soma módulo*** m***"***
- $x \cdot_m y = (x \cdot y)$ ***mod*** m — ***"multiplicação módulo*** m***"***

Exemplos (Soma)

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

O que ocorre em $\mathbb{Z}_{11}$ é o seguinte:

$$\{0, \underbrace{\overbrace{1, 2, 3, 4, 5, 6, 7}^{\textbf{7 unidades}} \overset{+}{,} \overbrace{8, 9, 10\}\{0, 1, 2, 3, 4, 5}^{\textbf{9 unidades}}}_{\textbf{16 unidades}}, 6, 7, 8, 9, 10\}$$

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Aritmética de Módulo *m*

Definição (Operações em $\mathbb{Z}_m$)

Dado um inteiro $m > 0$ e $x, y \in \mathbb{Z}_m$,

- $x +_m y = (x + y)$ ***mod*** m “***soma módulo*** m”
- $x \cdot_m y = (x \, . \, y)$ ***mod*** m “***multiplicação módulo*** m”

Exemplos (Soma)

Similarmente, teremos...

- $4 +_5 3 = (4 + 3)$ ***mod*** $5 = 7$ ***mod*** $5 = 2$
- $5 +_8 3 = (5 + 3)$ ***mod*** $8 = 8$ ***mod*** $8 = 0$
- $5 +_8 3 +_8 2 = (5 + 3 + 2)$ ***mod*** $8 = 10$ ***mod*** $8 = 2$

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Aritmética de Módulo *m*

Definição (Operações em $\mathbb{Z}_m$)

Dado um inteiro $m > 0$ e $x, y \in \mathbb{Z}_m$,

- $x +_m y = (x + y)$ ***mod*** m "***soma módulo*** m"
- $x \cdot_m y = (x \,.\, y)$ ***mod*** m "***multiplicação módulo*** m"

Exemplos (Multiplicação)

- $3 ._5 4 = (3.4)$ ***mod*** $5 = 12$ ***mod*** $5 = 2$

O que ocorre em $\mathbb{Z}_5$ é o seguinte:

$$\{0, \underbrace{\overbrace{1,2,3}^{\text{3 unid.}}, \overbrace{4\}\{0,1}^{\text{3 unid.}}, \overbrace{2,3,4\}}^{\text{3 unid.}}\overbrace{\{0,1,2}^{\text{3 unid.}}}_{\text{12 unid.}}, 3, 4\}$$

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Aritmética de Módulo *m*

Definição (Domínio $\mathbb{Z}_m$)

Dado um inteiro $m > 0$, o ***domínio da aritmética de módulo*** *m será o conjunto $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$.*

Definição (Operações em $\mathbb{Z}_m$)

Dado um inteiro $m > 0$ e $x, y \in \mathbb{Z}_m$,

- $x +_m y = (x + y)$ ***mod*** m — "***soma módulo*** m"
- $x \cdot_m y = (x \,.\, y)$ ***mod*** m — "***multiplicação módulo*** m"

Definição (Aritmética de Módulo m)

Dado $m > 0$ inteiro,

a aritmética de módulo *m é a estutura $\langle \mathbb{Z}_m, +_m, \cdot_m \rangle$*

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Roteiro

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Propriedades das Operações no Módulo m

Dado um inteiro $m > 0$, as operações $+_m$ e $\cdot_m$ satisfazem às propriedades abaixo para todos $a, b, c \in \mathbb{Z}_m$.

(**Fechamento**)

1. $a +_m b \in \mathbb{Z}_m$
2. $a \cdot_m b \in \mathbb{Z}_m$

(**Associatividade**)

1. $(a +_m b) +_m c = a +_m (b +_m c)$
2. $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$

(**Comutatividade**)

1. $a +_m b = b +_m a$
2. $a \cdot_m b = b \cdot_m a$

(**Distributividade**)

1. $a \cdot_m (b +_m c) = a \cdot_m b +_m a \cdot_m c$

(**Elemento Neutro**)

1. $a +_m 0 = a$
2. $a \cdot_m 1 = a$

(**Inverso Aditivo**)

1. se $a \neq 0$, $a +_m (m - a) = 0$
2. $0 +_m 0 = 0$

Demonstrar estas propriedades é um excelente exercício.

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Propriedades das Operações no Módulo m

Demonstrar estas propriedades é um excelente exercício.

A título de exemplo, demonstraremos a comutatividade da soma.

Teorema (Comutatividade de $+_m$)

Dado um inteiro $m > 0$, se $a, b \in \mathbb{Z}_m$, então $a +_m b = b +_m a$.

Prova

1. *Sejam m um inteiro positivo qualquer a, b inteiros quaisquer, (instanciação).*
2. *Por prova direta, suponha que $a, b \in \mathbb{Z}_m$.*
3. *Pela definição da soma modular, teremos* $$\begin{aligned} a +_m b &= (a + b) \textbf{ mod } m \\ &= (b + a) \textbf{ mod } m && \text{(comut. em } \mathbb{Z}\text{)} \\ &= b +_m a && \text{(def. de } +_m\text{)} \end{aligned}$$

Estas demonstrações são parecidas com as de propriedades de somatórios. Como exercício, demonstre as demais.