Congruências em $\mathbb{Z}$ e Aritmética Modular

Prof. Eanes Torres Pereira

FMCC2

Roteiro

Congruências

- **Definição** Sejam a, b, n inteiros com $n > 0$. Então a é congruente com b módulo n [escreve-se $a \equiv b(mod\ n)$], desde que n divida $a - b$.
- **Exemplo**. $17 \equiv 5(mod\ 6)$ por que 6 divide $17 - 5 = 12$. De modo similar, $4 \equiv 25(mod\ 7)$ por que 7 divide $4 - 25 = -21$ e $6 \equiv -4(mod\ 5)$ por que 5 divide $6 - (-4) = 10$.

Congruências

- **Teorema 1**. Seja n um inteiro positivo. Para todo a, b, $c \in \mathbb{Z}$, então:

1. $a \equiv a (mod\ n)$;
2. se $a \equiv b (mod\ n)$, então $b \equiv a (mod\ n)$;
3. se $a \equiv b (mod\ n)$ e $b \equiv c (mod\ n)$, então $a \equiv c (mod\ n)$.

- **Teorema 2**. Seja m um inteiro positivo. Os inteiros a e b são congruentes módulo m se e somente se existe um inteiro k tal que $a = b + km$.

Congruências

- **Exercício**. Prove que $a \equiv b(mod\ n)$ se, e somente se, a e b deixam o mesmo resto quando divididos por n.

Congruências

- **Exercício**. Prove que $a \equiv b (mod\ n)$ se, e somente se, a e b deixam o mesmo resto quando divididos por n.

  Sugestão de solução:

  $p : a \equiv b(mod\ n)$

  $q : a = xn + r \wedge b = yn + r$

  $p \iff q = (p \longrightarrow q) \wedge (q \longrightarrow p)$

  prove a primeira implicação por absurdo supondo que os restos são diferentes.

  prove a segunda implicação por prova direta substituindo os valores de a e b em $a - b$.

Congruências Lineares

- **Definição**. Uma congruência da forma $ax \equiv b(mod\ m)$, em que m é um inteiro positivo, a e b são inteiros e x é uma variável, é chamada de **congruência linear**.
- **Definição**. Um inteiro $\overline{a}$ tal que $\overline{a}a \equiv 1(mod\ m)$ é chamado de **inverso** de a módulo m.
- **Teorema 3**. Se a e m são inteiros primos relativos e $m > 1$, então existe um inverso de a módulo m. Além disso, esse inverso é único módulo m.
- **Exemplo**. Calcule um inverso de 3 módulo 7, calculando primeiro os coeficientes de Bézout de 3 e de 7.

  Solução. Como mdc(3,7) = 1 e aplicando o algoritmo de Euclides, obtemos: 7 = 2.3+1. Dessa equação, vemos que -2.3 + 1.7 = 1. Os coeficientes de Bézout são -2 e 1. Então, -2 é um inverso de 3 módulo 7.

Congruências Lineares

Exemplo. Calcule um inverso de 101 módulo 4620.

Solução. Primeiro, aplicamos o algoritmo de Euclides:

4620 = 45.101 + 75 (a)

101 = 1.75 + 26 (b)

75 = 2.26 + 23 (c)

26 = 1.23 + 3 (d)

23 = 7.3 + 2 (e)

3 = 1.2 + 1 (f)

2 = 2.1 (g)

Portanto, mdc(4620,101) = 1.

- de (f): 1 = 3 - 1.2
- de (e): 1 = 3 - 1.(23 - 7.3) = 3 - 1.23 + 7.3
- 1 = 8.3 - 1.23
- de (d): 1 = 8.(26 - 1.23) - 1.23 = 8.26 - 9.23
- de (c): 1 = 8.26 - 9.(75 - 2.26) = 26.26 - 9.75
- de (b): 1 = 26.(101 - 1.75) -9.75 = 26.101 - 35.75
- de (a): 1 = 26.101 - 35.(4620 - 45.101) =

  -35.4620 + 1601.101

Congruências Lineares

- **Exemplo**. Calcule um inverso de 101 módulo 4620.
- **Continuação**.

  Como $1 =$ -35.4620 + 1601.101, os coeficientes de Bézout são -35 e 1601.

  Então, 1601 é um inverso de 101 módulo 4620, pois 1601.101 mod 4620 = 1. Ou seja, $1601 \times 101 = 161701$ e o resto da divisão de 161701 por 4620 é 1.

Congruências Lineares

- **Exemplo**. Quais são as soluções da congruência linear: $3x \equiv 4(mod\ 7)$?

  Solução.

  Como mdc(3,7) = 1, podemos escrever: 1 = -2.3 + 1.7 pela substituição retroativa no algoritmo de Euclides.

  -2.3 = -6; -6 mod 7 = 1; logo -2 é um inverso módulo 7 de 3.

  Multiplicando a congruência linear por -2:
  $-2.3x \equiv -2.4(mod\ 7)$.

  Pela definição de inverso: $-6 \equiv 1(mod\ 7)$.

  Como $-8\ mod\ 7 = 1$ e $-6\ mod\ 7 = 1$, $-8 \equiv 6(mod\ 7)$.

  Pela propriedade transitiva:
  $-8 \equiv\ 6(mod\ 7) \wedge x \equiv -8(mod\ 7) \rightarrow x \equiv 6(mod\ 7)$.
- Concluímos que as soluções da congruência são os inteiros x tal que $x \equiv 6(mod\ 7)$, a saber: 6, 13, 20, ... e -1, -8, -15, ...

Roteiro

1. Congruências

2. O Teorema Chinês do Resto

3. Classes de Congruências

4. Aritmética Modular

5. Aritmética Computacional com Números Grandes

O Teorema Chinês do Resto - TCR

- **Teorema 4**. Sejam m_1, m_2, ..., m_n inteiros positivos primos relativos maiores do que 1 e a_1, a_2, ..., a_n inteiros arbitrários. Então, o sistema:

  $x \equiv a_1 (mod\ m_1)$

  $x \equiv a_2 (mod\ m_2)$

  $\vdots$

  $x \equiv a_n (mod\ m_n)$

- tem uma solução única módulo $m = m_1 m_2 \dots\ m_n$.
- Ou seja, existe uma solução x com $0 \leq x < m$ e todas as soluções são congruentes módulo m a essa solução.

O Teorema Chinês do Resto - TCR

- **Exemplo (O problema de Sun-Tsu)**. Há algumas coisas cuja quantidade não se conhece. Essa quantidade, quando dividida por 3 o resto é 2; quando dividida por 5, o resto é 3; e quando dividida por 7, o resto é 2. Qual é a quantidade?

  Solução.

  Esse enigma pode ser traduzido para a seguinte questão: quais são as soluções dos sistemas de congruência:

  $x \equiv 2(mod\ 3)$,

  $x \equiv 3(mod\ 5)$,

  $x \equiv 2(mod\ 7)$?

O Teorema Chinês do Resto - TCR

- **Continuação**. Para resolver o problema de Sun-Tsu, façamos $m = 3 \times 5 \times 7 = 105$, $M_1 = m/3 = 35$, $M_2 = m/5 = 21$ e $M_3 = m/7 = 15$.
  2 é um inverso de M_1 módulo 3.
  1 é um inverso de M_2 módulo 5.
  1 é um inverso de M_3 módulo 7.
- As soluções para o sistema são os x tais que:
  $x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 (mod\ 105)$.
  $x \equiv 2.35.2 + 3.21.1 + 2.15.1$
  $x \equiv 233 (mod\ 105)$
  $x \equiv 23 (mod\ 105)$.
- Assim, 23 é o menor inteiro positivo que é uma solução simultânea. Concluímos que 23 é o menor inteiro positivo que deixa resto 2 quando dividido por 3, deixa resto 3 quando dividido por 5 e deixa resto 2 quando dividido por 7.

O Teorema Chinês do Resto - TCR

- **Exemplo**. Use o método de substituição retroativa para encontrar todos os inteiros x tais que $x \equiv 1 (mod\ 5)$, $x \equiv 2 (mod\ 6)$ e $x \equiv 3 (mod\ 7)$.

  Solução. Pelo Teorema 2, na primeira congruência: $x = 5t + 1$, $t \in \mathbb{Z}$.

  Substituindo a expressão para x na segunda congruência: $5t + 1 \equiv 2 (mod\ 6)$ e $t \equiv 5 (mod\ 6)$.

  Aplicando o Teorema 2 novamente, vemos que $t = 6u + 5$, com u inteiro.

  Substituindo essa expressão para t na equação $x = 5t + 1$, temos: $x = 5(6u + 5) + 1 = 30u + 26$.

  Inserindo essa expressão para x na terceira equação: $30u + 26 \equiv 3 (mod\ 7)$, $x = 30(7v + 6) + 26 = 210v + 206$.

  Reescrevendo $x = 210v + 206$ como congruência: $x \equiv 206 (mod\ 210)$

Roteiro

Classes de Congruências

- **Teorema 5**. Se $a \equiv b(mod\ n)$ e $c \equiv d(mod\ n)$, então:

1. $a + c \equiv b + d(mod\ n)$;
2. $ac \equiv bd(mod\ n)$.

- **Definição**. Sejam a e n inteiros com $n > 0$. A classe de congruência de a módulo n (denotada como [a]) é o conjunto de todos os inteiros que são congruentes a a módulo n, isto é,

$$[a] = \{b | b \in \mathbb{Z} \ e \ b \equiv a(mod\ n)\}.$$

- Na congruência módulo 5, temos:
$[9] = \{9 + 5 \mid k \in \mathbb{Z}\} = \{9, 9 \pm 5, 9 \pm 10, 9 \pm 15, \dots\}$
$= \dots, -11, -6, -1, 4, 9, 14, 19, 24, \dots$

Classes de Congruências

- **Teorema 6** $a \equiv c (mod\ n)$ se, e somente se, $[a] = [c]$.
- **Corolário 7**. Duas classes de congruência módulo n são ou disjuntas ou idênticas.
- **Corolário 8**. Há exatamente n classes de congruência distintas módulo n, a saber: $[0]$, $[1]$, $[2]$, $\ldots$, $[n-1]$.
- **Definição**. O conjunto de todas as classes de congruências módulo n é denotado Z_n.
- **Exemplo**. O conjunto Z_3 consiste de três elementos $[0]$, $[1]$ e $[2]$.

Classes de Congruências

- Os elementos de $\mathbb{Z}_n$ são classes, não inteiros únicos.
- A afirmação $[5] \in \mathbb{Z}$ é verdadeira, mas a afirmação $5 \in \mathbb{Z}_n$ é falsa.
- **Exemplo 1**. Cada elemento de $\mathbb{Z}_n$ pode ser denotado de diferentes modos. Sabemos que: $2 \equiv 5(mod\ 3)$, $2 \equiv -1(mod\ 3)$, $2 \equiv 14(mod\ 3)$. Portanto, $[2] = [5] = [-1] = [14]$ em $\mathbb{Z}_3$.
- **Exemplo 2**. Em congruência módulo 5, temos:
  $[9] = \{9 + 5k \mid k \in \mathbb{Z}\} = \{9, 9 \pm 5, 9 \pm 10, 9 \pm 15, \ldots\}$
  $= \{\ldots, -11, -6, -1, 4, 9, 14, 19, 24, \ldots\}$

Roteiro

Aritmética Modular

- **Teorema 9**. Se $[a] = [b]$ e $[c] = [d]$ em Z_{n}, então: $[a + b] = [b + d]$ e $[ac] = [bd]$.
- **Definição**. A adição e a multiplicação em Z_n são definidas por: $[a] \oplus [c] = [a + c]$ e $[a] \odot [b] = [ac]$.
- **Exemplo**. As tabelas de adição e multiplicação para Z_5 são:

$\oplus$	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]

$\odot$	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]

Aritmética Modular

- **Exercício**. Prove o Teorema 9, usando o Teorema 5 e o Teorema 6.

Propriedades da Aritmética Modular

- **Teorema 10**. Para quaisquer classes $[a]$, $[b]$ e $[c] \in \mathbb{Z}_n$, valem as seguintes propriedades:

1. Se $[a] \in \mathbb{Z}_n$ e $[b] \in \mathbb{Z}_n$, então $[a] \oplus [b] \in \mathbb{Z}_n$.
2. $[a] \oplus ([b] \oplus [c]) = ([a] \oplus [b]) \oplus [c]$.
3. $[a] \oplus [b] = [b] \oplus [a]$.
4. $[a] \oplus [0] = [a] = [0] \oplus [a]$.
5. Para cada $[a] \in \mathbb{Z}_n$, a operação $[a] \oplus X = [0]$ tem uma solução em $\mathbb{Z}_n$.
6. Se $[a] \in \mathbb{Z}_n$ e $[b] \in \mathbb{Z}_n$, então $[a] \odot [b] \in \mathbb{Z}_n$.
7. $[a] \odot ([b] \odot [c]) = ([a] \odot [b]) \odot [c]$.
8. $[a] \odot ([b] \oplus [c]) = [a] \odot [b] \oplus [a] \odot [c]$ e $([a] \oplus [b]) \odot [c] = [a] \odot [c] \oplus [b] \odot [c]$.
9. $[a] \odot [b] = [b] \odot [a]$.
10. $[a] \odot [1] = [a] = [1] \odot [a]$.

Aritmética Modular - Nova Notação

- Sempre que o contexto deixar claro que estamos lidando com $\mathbb{Z}_n$, abreviaremos a notação de classe, $[a]$, e escreveremos a.
- **Exemplo**. As tabelas de adição e multiplicação para $\mathbb{Z}_3$ são:

$\oplus$	0	1	2
0	0	1	2
1	1	2	3
2	2	3	4

$\odot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Aritmética Modular - Exercícios

1. Escreva as tabelas de adição e multiplicação para: a) $\mathbb{Z}_2$; b)$\mathbb{Z}_4$; c) $\mathbb{Z}_7$; d) $\mathbb{Z}_{12}$

Roteiro

Aritmética Computacional com Números Inteiros Grandes

- Suponha que $m_1, m_2, \ldots, m_n$ são par-a-par primos relativos módulo e seja m seu produto. Pelo Teorema Chinês do Resto podemos mostrar que um inteiro a com $0 \leq a < m$ pode ser representado unicamente como uma n-tupla consistindo de seus restos da divisão por m_i, $i = 1, 2, \ldots, n$. Isto é, podemos representar unicamente a por:

$$(a\ mod\ m_1, a\ mod\ m_2, \ldots, a\ mod\ m_n)$$

Aritmética Computacional com Números Grandes

- **Exemplo**. Quais são os pares usados para representar os inteiros não-negativos menores que 12 quando eles são representados por pares ordenados em que o primeiro componente é o resto do inteiro após divisão por 3 e o segundo componente é o resto do inteiro após divisão por 4?
- **Resposta**. $0 = (0, 0)$; $1 = (1,1)$; $2 = (2, 2)$; $3 = (0, 2)$; $4 = (1, 0)$; $5 = (2, 1)$; $6 = (0, 2)$; $7 = (1, 3)$; $8 = (2, 0)$; $9 = (0, 1)$; $10 = (1 , 2)$; $11 = (1, 2)$; $12 = (2, 3)$.

Aritmética Computacional com Números Grandes

- **Exemplo**. Pelo TCR, todo inteiro não-negativo menor que $99 \times 98 \times 97 \times 95 = 89403930$ pode ser representado unicamente por seus restos quando divididos por esses quatro números.
- Podemos representar 123684 como $(33, 8, 9, 89)$ por que $123684\ mod\ 99 = 33$; $123684\ mod\ 98 = 8$; $123684\ mod\ 97 = 9$; $123684\ mod\ 95 = 89$. De modo similar, representamos $413456 = (32, 92, 42, 16)$.
- Para calcular a soma de 123684 e 413456, trabalhamos com as quatro tuplas ao invés dos dois inteiros diretamente.
- Obtemos: $(33, 8, 9, 89) + (32, 92, 42, 16) = (65, 2, 51, 10)$
- Para calular a soma, é necessário resolver o sistema de congruências: $x \equiv 65(mod\ 99)$, $x \equiv 2(mod\ 98)$, $x \equiv 51(mod\ 97)$, $x \equiv 10(mod\ 95)$.
- Pode-se mostrar que 537140 é a única solução não-negativa para esse sistema menor que 89403930.

Referência

- Abstract Algebra an Introduction. Thomas W. Hungerford.
- Matemática Discreta e suas Aplicações. Kenneth Rosen.