Teoria dos Números: Relações de Congruência (1.6)

Prof. Rafael Alves Bonfim de Queiroz
rafael.queiroz@ufop.edu.br

Conteúdo programático

- 1.6) Relação de congruência

Relação de congruência

- Seja m um inteiro positivo. Dizemos que a é congruente a b módulo m, escrito
  $a \equiv b$ (módulo m) ou simplesmente $a \equiv b \pmod{m}$
  se m divide a diferença $a - b$.
- O inteiro m é chamado de módulo. A negação de $a \equiv b \pmod{m}$ é escrita $a \not\equiv b \pmod{m}$.
- Por exemplo
  1. $87 \equiv 23 \pmod{4}$ já que 4 divide 87 - 23 $=$ 64.
  2. $67 \equiv 1 \pmod{6}$ já que 6 divide 67 - 1 $=$ 66.
  3. $72 \equiv -5 \pmod{7}$ já que 7 divide 72 - (-5) $=$ 77.
  4. $27 \not\equiv 8 \pmod{9}$ já que 9 não divide 27 - 8 $=$ 19.

Relação de congruência

Teorema: Seja m um inteiro positivo. Então:

- (i) Para qualquer inteiro a, temos $a \equiv a \pmod{m}$.
- (ii) Se $a \equiv b \pmod{m}$, então $b \equiv a \pmod{m}$.
- (iii) Se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então $a \equiv c \pmod{m}$.

Observação: Suponha que m seja positivo e a seja qualquer número inteiro. Pelo Algoritmo da Divisão, existem inteiros q e r com $0 = r \leq m$ tal que $a = mq + r$. Por isso $mq = a - r$
ou
$m|(a - r)$ ou $a \equiv r \pmod{m}$ De acordo:

1. Qualquer inteiro$a$ é congruente módulo m a um único inteiro no conjunto $\{0, 1, 2, \cdots, m - 1\}$ A unicidade vem do fato de que m não pode dividir a diferença de dois desses inteiros.
2. Quaisquer dois inteiros a e b são congruentes módulo m se e somente se eles tiverem o mesmo resto quando divididos por m.

Classes de Resíduos

- Como o módulo de congruência m é uma relação de equivalência, ela particiona o conjunto Z de inteiros em classes de equivalência disjuntas chamadas de **classes de resíduos módulo** m.
- Pelas observações acima, uma classe de resíduo consiste em todos aqueles inteiros com o mesmo resto quando divididos por m.
- Portanto, existem m tais classes de resíduos e cada classe resíduo contém exatamente um dos inteiros no conjunto de restos possíveis, isto é, $\{0, 1, 2, \cdots, m-1\}$
- De um modo geral, um conjunto de m inteiros $\{a_1, a_2, \cdots, a_m\}$ é dito ser um **sistema de resíduos completo** módulo m se cada a_i vem de um classe distinta de resíduos.
- Nesse caso, cada a_i é chamado de **representante** de sua classe de equivalência.

Classes de Resíduos

- Assim, os inteiros de 0 a m - 1 formam um sistema de resíduos completo.
- De fato, quaisquer m inteiros consecutivos formam um sistema completo de resíduos módulo m
- A notação $[x]_m$, ou simplesmente $[x]$ é usada para denotar a classe de resíduo (módulo m) contendo um inteiro x, que ou seja, aqueles inteiros que são congruentes a x.
- Em outras palavras, $[x] = \{a \in \mathrm{Z} | a \equiv x (modm)\}$
- Assim, as classes de resíduos podem ser denotadas por [0], [1], [2], $\cdots$, $[m-1]$ ou usando qualquer outra escolha de números inteiros em um sistema de resíduos completo.

Classes de Resíduos: Exemplo

As classes de resíduos módulo $m = 6$ seguem:

- $[0] = \{..., -18, -12, -6, 0, 6, 12, 18, ...\}$,
- $[1] = \{..., -17, -11, -5, 1, 7, 13, 19, ...\}$,
- $[2] = \{..., -16, -10, -4, 2, 8, 14, 20, ...\}$,
- $[3] = \{..., -15, -9, -3, 3, 9, 15, 21, ...\}$
- $[4] = \{..., -14, -8, -2, 4, 10, 16, 22, ...\}$
- $[5] = \{..., -13, -7, -1, 5, 11, 17, 23, ...\}$
- Observe que $\{-2, -1, 0, 1, 2, 3\}$ também é um sistema de resíduo completo módulo $m = 6$, e esses representantes têm valores absolutos mínimos.´

Aritmética de congruência

A congruência A relação comporta-se muito como a relação de igualdade. Nomeadamente:

- Teorema: Suponha $a \equiv c \pmod{m}$ e $b \equiv d \pmod{m}$. Então:
  - (i) $a + b \equiv c + d (\mathrm{mod}\ m)$;
  - (ii) $ab \equiv cd (\mathrm{mod}\ m)$
- Observação: Suponha que $p(x)$ seja um polinômio com coeficientes inteiros. Se $s \equiv t (\mathrm{mod}\ m)$, então usando o teorema acima repetidamente podemos mostrar que $p(s) \equiv p(t) (\mathrm{mod}\ m)$.

Aritmética de Congruência: Exemplo

Observe que $2 \equiv 8(mod 6)$ e $5 \equiv 41(\text{mod } 6)$. Então:

- (a) $2 + 5 \equiv 8 + 41$ (mod 6) ou $7 \equiv 49$ (mod 6)
- (b) $2 \cdot 5 \equiv 8 \cdot 41$ (mod 6) ou $10 \equiv 328$ (mod 6)
- (c) Suponha $p(x) = 3x^2 - 7x + 5$. Então $p(2) = 12$ - $14 + 5 = 3$ e $p(8) = 192$ - $56 + 5 = 141$
  Daí $3 \equiv 141$ (mod 6).

Aritmética das classes de resíduos

- A adição e a multiplicação são definidas para nossas classes de resíduos módulo m da seguinte forma: $[a] + [b] = [a + b]$ e $[a][b] = [ab]$
- Por exemplo, considere as classes de resíduos módulo $m = 6$; aquilo é, $[0], [1], [2], [3], [4], [5]$
- Então $[2] + [3] = [5]$, $[4] + [5] = [9] = [3]$, $[2][2] = [4]$, $[2][5] = [10] = [4]$
- O conteúdo do Teorema anterior nos diz que as definições acima estão bem definidas, ou seja, a soma e o produto de as classes de resíduos não dependem da escolha do representante da classe de resíduos

Aritmética das classes de resíduos

- Existe apenas um número finito m de classes de resíduos módulo m.
- Assim, pode-se facilmente escrever explicitamente suas tabelas de adição e multiplicação quando m é pequeno.
- A figura abaixo mostra as tabelas de adição e multiplicação para as classes de resíduos módulo $m = 6$.

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

×	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

- Por conveniência de notação, omitimos os colchetes e simplesmente denotamos as classes de resíduos pelos números 0, 1, 2, 3, 4, 5.

Inteiros Módulo m, Z_m

- Os inteiros módulo m, denotados por Z_m , referem-se ao conjunto $Z_m = \{0, 1, 2, 3, \cdots, m-1\}$ onde a adição e a multiplicação são definidas pelo módulo aritmético m ou, em outras palavras, o correspondente operações para as classes de resíduos.
- Por exemplo, a figura abaixo também pode ser vista como tabelas adição e multiplicação por Z_6

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

×	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Não há diferença essencial entre Z_m e a aritmética do resíduo classes módulo m, e por isso serão usadas de forma intercambiável.

Leis de Cancelamento para Congruências

- Lembre-se de que os inteiros satisfazem o seguinte:

  Lei do cancelamento: Se $ab = ac$ e $a \neq 0$, então $b = c$.

- A diferença crítica entre a aritmética ordinária e a aritmética módulo m é que o cancelamento acima a lei não é verdadeira para congruências. Por exemplo, $3 \cdot 1 \equiv 3 \cdot 5 \pmod{6}$ mas $1 \not\equiv 5 \pmod{6}$
- Ou seja, não podemos cancelar o 3 mesmo sendo $3 \not\equiv 0 \pmod{6}$. No entanto, temos o seguinte **Modificado Lei de cancelamento** para nossas relações de congruência.
- Teorema (**Lei de Cancelamento Modificada**): Suponha $ab \equiv ac \pmod{m}$ e $\text{mdc}(a, m) = 1$. Então $b \equiv c \pmod{m}$
- Teorema: Suponha que $ab \equiv ac \pmod{m}$ e $d = \text{mdc}(a, m)$. Então $b \equiv c \pmod{m/d}$.

Leis de Cancelamento para Congruências: Exemplo

Considere a seguinte congruência: $6 \equiv 36 \pmod{10}$

- Como mdc(3, 10) $= 1$ mas mdc(6, 10) $\not\equiv 1$, podemos dividir ambos os lados da congruência por 3, mas não por 6.
- Ou seja, $2 \equiv 12 \pmod{10}$ mas $1 \not\equiv 6 \pmod{10}$
- Porém, pelo Teorema anterior, podemos dividir ambos os lados da congruência por 6 se também dividirmos o módulo por 2 que é igual a mdc(6, 10).
- Ou seja, $1 \equiv 6 \pmod{5}$

Leis de Cancelamento para Congruências: Exemplo

- Suponha que p seja primo.
- Então os inteiros de 1 a $p-1$ são relativamente primos de p.
- Assim, o habitual a lei do cancelamento é válida quando o módulo é um primo p.

Se $ab \equiv ac \pmod{p}$ e $a \not\equiv 0 \pmod{p}$, então $b \equiv c \pmod{p}$

- Assim, Z_p , os inteiros módulo a primo p, desempenham um papel muito especial na teoria dos números.

Sistemas de Resíduos Reduzidos, Função Euler Phi

- A lei de cancelamento modificada é indicativa do papel especial desempenhado por aqueles inteiros que são relativamente primos (coprime) ao módulo m.
- Notamos que a é primo de m se e somente se todo elemento na classe de resíduo $[a]$ é primo de m.
- Assim, podemos falar de uma classe de resíduo coprimida a m.
- O número de classes de resíduos relativamente primos para m ou, equivalentemente, o número de inteiros entre 1 e m (inclusive) que são relativamente primos a m é denotado por $\phi(m)$
- A função $\phi(m)$ é chamada de **função phi de Euler**.
- A lista de números entre 1 e m que são primos entre si m ou, mais geralmente, qualquer lista de $\phi(m)$ inteiros incongruentes que são primos de m, é chamado de **resíduo reduzido módulo do sistema** m.

Sistemas de Resíduos Reduzidos, Função Euler Phi: Exemplo

1. Considere o módulo $m = 15$. Existem oito inteiros entre 1 e 15 que são primos de 15: 1, 2, 4, 7, 8, 11, 13, 14.
   Assim, $\phi(15) = 8$ e os oito inteiros acima formam um sistema de resíduo reduzido módulo 15.
2. Considere qualquer primo p. Todos os números $1, 2, \cdots, p-1$ são coprimos a p; portanto $\phi(p) = p - 1$.

função phi de Euler – multiplicativa

- Uma função f com domínio de inteiros positivos N é dita multiplicativa se, sempre que a e b são relativamente melhor, $f(ab) = f(a)f(b)$
- Teorema: A função phi de Euler é multiplicativa. Ou seja, se a e b são relativamente primos, então $\phi(ab) = \phi(a)\phi(b)$