Teoria dos Números: Equações de congruência (1.7)

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

Contéudo programático

- 1.7) Equações de congruência

Equações de congruência

- Uma *equação de congruência polinomial* ou, simplesmente, uma *equação de congruência* (em uma incógnita x) é uma equação de a forma $a_n x_n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \equiv 0 (\text{mod } m)$
- Diz-se que tal equação é de *grau* n se $a_n \not\equiv 0 \pmod{m}$.
- Suponha $s \equiv t \pmod{m}$. Então s é uma solução da *equação de congruência* se e somente se t é uma solução da *equação de congruência*

Equações de congruência

- O número de soluções da equação de congruência é definido como sendo o número de soluções incongruentes ou, equivalentemente, o número de soluções no conjunto
  $0, 1, 2, \ldots, m-1$
- Essas soluções sempre podem ser encontradas por meio de testes, ou seja, substituindo cada um dos m números em a equação de congruência para ver se ela realmente satisfaz a equação.
- O conjunto completo de soluções da *equação de congruência* é um conjunto máximo de soluções incongruentes enquanto que o conjunto geral solução da *equação de congruência* é o conjunto de todas as soluções integrais da *equação de congruência*

Equações de congruência: exemplos

Considere as equações:

- (a) $x^2 + x + 1 \equiv 0 \pmod 4$
  - Não há soluções, pois 0, 1, 2 e 3 não satisfazem a equação.
- (b) $x^2 + 3 \equiv 0 \pmod 6$
  - Existe apenas uma solução entre 0, 1, ... , 5 que é 3.
  - Assim, a solução geral consiste nos inteiros $3 + 6k$ onde $k \in \mathbf{Z}$.
- (c) $x^2 - 1 \equiv 0 \pmod 8$
  - Existem quatro soluções, 1, 3, 5 e 7.
  - Isso mostra que uma equação de congruência de grau n pode ter mais de n soluções.

Equações de congruência

- Ressaltamos que não estamos interessados apenas em estudar equações de congruência para encontrar suas soluções; isso sempre pode ser encontrado testando
- Estamos interessados principalmente em desenvolver técnicas que nos ajudem a encontrar tais soluções, e uma teoria que nos diz as condições sob as quais existem soluções e o número de tais soluções.
- Tal teoria é válida para equações de congruência linear que investigamos a seguir
- Também discutiremos o chinês Teorema do resto, que é essencialmente um sistema de equações de congruência linear.

Equações de congruência

- **Observação 1**: Os coeficientes de uma equação de congruência sempre podem ser reduzidos módulo m desde que um equivalente resultaria em uma equação, isto é, uma equação com as mesmas soluções.
- Por exemplo, os seguintes são equivalentes equações já que os coeficientes são congruentes módulo $m = 6$:
  - $15x^2 + 28x + 14 \equiv 0 \pmod 6$,
  - $3x^2 + 4x + 2 \equiv 0 \pmod 6$,
  - $3x^2 - 2x + 2 \equiv 0 \pmod 6$,
  - Normalmente escolhemos coeficientes entre 0 e $m-1$ ou entre $-m/2$ e $m/2$

Equações de congruência

- **Observação 2**: Como estamos realmente procurando soluções da *equação de congruência* entre as classes de resíduos módulo m em vez de entre os inteiros, podemos ver a *equação de congruência* como uma equação sobre os inteiros módulo m, em vez de uma equação sobre $\mathbf{Z}$, os inteiros.
- Neste contexto, o número de soluções da *equação de congruência* é simplesmente o número de soluções em $\mathbf{Z}_m$.

Equação de Congruência Linear: $ax \equiv 1 \pmod{m}$

- Primeiro consideramos a equação de congruência linear especial $ax \equiv 1 \pmod{m}$,
  onde $a \not\equiv 0 \pmod{m}$.
- A história completa desta equação é dada no seguinte teorema
- **Teorema**: Se a e m são relativamente primos, então $ax \equiv 1 \pmod{m}$ tem solução única; senão tem nenhuma solução.

Equação de Congruência Linear: $ax \equiv 1 \pmod{m}$ - Exemplo

Teorema: Se a e m são relativamente primos, então $ax \equiv 1 \pmod{m}$ tem solução única; senão tem nenhuma solução.

- (a) Considere a equação de congruência $6x \equiv 1 \pmod{33}$. Como $\text{mdc}(6, 33) = 3$, esta equação não tem solução
- (b) Considere a equação de congruência $7x \equiv 1 \pmod{9}$. Como $\text{mdc}(7, 9) = 1$, a equação tem uma solução única. Testando os números $0, 1, \ldots, 8$, descobrimos que
  - $7(4) = 28 \equiv 1 (\text{mod } 9)$
  - Portanto, $x = 4$ é nossa única solução. (A solução geral é $4 + 9k$ para $k \in \mathbf{Z}$.)

Equação de Congruência Linear: $ax \equiv 1 \pmod{m}$

- Suponha que exista uma solução da equação de congruência linear, ou seja, suponha que $\text{mdc}(a, m) = 1$.
- Além disso, suponha que o módulo m é grande.
- Então o algoritmo euclidiano pode ser usado para encontrar uma solução da equação de congruência linear
- Especificamente, usamos o Algoritmo euclidiano para encontrar x_0 e y_0 tal que $ax_0 + my_0 = 1$
- Disto segue que $ax_0 \equiv 1 \pmod{m}$; ou seja, x_0 é uma solução para a equação de congruência linear.

Equação de Congruência Linear: $ax \equiv 1 \pmod{m}$ – Exemplo

- Considere a seguinte equação de congruência: $81 \equiv 1 \pmod{256}$
  - Por observação ou aplicando o algoritmo euclidiano a 81 e 256, descobrimos que $\text{mdc}(81, 256) = 1$
  - Assim a equação tem uma única solução.
  - O teste pode não ser uma maneira eficiente de encontrar essa solução, pois o módulo $m = 256$ é relativamente grande.
  - Assim, aplicamos o algoritmo euclidiano para $a = 81$ e $m = 256$.
  - Especificamente, encontramos $x_0 = -25$ e $y_0 = 7$ tal que $81x_0 + 256y_0 = 1$
  - Isso significa que $x_0 = -25$ é uma solução da equação de congruência dada.
  - Somando $m = 256$ a -25, obtemos a seguinte solução única entre 0 e 256:
    $x = 231$

Equação de Congruência Linear: $ax \equiv b \pmod{m}$

- Agora consideramos a equação de congruência linear mais geral $ax \equiv b \pmod{m}$, onde $\not\equiv 0 \pmod{m}$.
- Primeiro consideramos o caso em que a e m são coprimos.
- **Teorema**: Suponha que a e m são relativamente primos.
  - Então $ax \equiv b \pmod{m}$ tem uma solução única.
  - Além disso, se s é a solução única para $ax \equiv 1 \pmod{m}$, então a solução única para $ax \equiv b \pmod{m}$ é $x = bs$.

Equação de Congruência Linear: $ax \equiv b \pmod{m}$ – Exemplo

- Considere a equação de congruência $3x \equiv 5 (\text{mod } 8)$.
- Como 3 e 8 são primos entre si, a equação tem um único solução.
- Testando os inteiros $0, 1, \ldots, 7$, descobrimos que $3(7) = 21 \equiv 5 \pmod{8}$
- Assim $x = 7$ é a única solução da equação.

Equação de Congruência Linear: $ax \equiv b \pmod{m}$ – Exemplo

- Considere a equação de congruência linear $33x \equiv 38 \pmod{280}$
- Como mdc$(33, 280) = 1$, a equação tem solução única.
- O teste pode não ser uma maneira eficiente de encontrar isso solução, pois o módulo $m = 280$ é relativamente grande.
- Aplicamos o algoritmo euclidiano para primeiro encontrar um solução para $33x \equiv 1 (\text{mod } 280)$
- Ou seja, encontramos $x_0 = 17$ e $y_0 = -2$ como uma solução de $33x_0 + 280y_0 = 1$
- Isso significa que $s = 17$ é uma solução de $33x \equiv 1 \pmod{280}$
- Então $sb = 17(38) = 646$ é uma solução de $33x \equiv 38 \pmod{280}$
- Dividindo 646 por $m = 280$, obtemos o restante $x = 86$ que é a única solução de $33x \equiv 38 \pmod{280}$ entre 0 e 280.
- A solução geral é $86 + 280k$ com $k \in \mathbf{Z}$.

Equação de Congruência Linear: $ax \equiv b \pmod{m}$ – Exemplo

Teorema*: Considere a equação $ax \equiv b \pmod{m}$ onde $d = \text{mdc}(a, m)$.

- (i) Suponha que d não divida b. Então $ax \equiv b \pmod{m}$ não tem solução.
- (ii) Suponha que d divida b. Então $ax \equiv b \pmod{m}$ tem d soluções que são todas congruentes módulo M para a solução única de $Ax \equiv B \pmod{M}$ onde $A = a/d$, $B = b/d$, $M = m/d$.

Teorema**: Suponha que a e m são relativamente primos.

- Então $ax \equiv b \pmod{m}$ tem uma solução única.
- Além disso, se s é a solução única para $ax \equiv 1 \pmod{m}$, então a solução única para $ax \equiv b \pmod{m}$ é $x = bs$.

Ressaltamos que o Teorema** se aplica à equação $Ax \equiv B \pmod{M}$ no Teorema* já que $\text{mdc}(A, M) = 1$.

Equação de Congruência Linear: $ax \equiv b \pmod{m}$ – Exemplo

Resolva cada equação de congruência:

- (a) $4x \equiv 9 \pmod{14}$
  - Nota $\text{mdc}(4, 14) = 2$.
  - No entanto, 2 não divide 9.
  - Portanto, a equação não tem solução.

Equação de Congruência Linear: $ax \equiv b \pmod{m}$ – Exemplo

Resolva cada equação de congruência:

- (b) $8x \equiv 12 \pmod{28}$
  - Observe que $d = \text{mdc}(8, 28) = 4$ e $d = 4$ divide 12.
  - Assim a equação tem $d = 4$ soluções.
  - Dividindo cada termo na equação por $d = 4$ obtemos a equação de congruência $2x \equiv 3 \pmod{7}$ que tem uma única solução.
  - Testando os inteiros $0, 1, \ldots, 6$, descobrimos que 5 é a única solução de $2x \equiv 3 \pmod{7}$
  - Agora adicionamos $d - 1 = 3$ múltiplos de 7 à solução 5 de $2x \equiv 3$ obtendo: $5 + 7 = 12, \quad 5 + 2(7) = 19, \quad 5 + 3(7) = 26$
  - Portanto, 5, 12, 19, 26 são as soluções $d = 4$ necessárias da equação original $8x \equiv 12 \pmod{28}$.
- **Observação**: A solução da equação $2x \equiv 3 \pmod{7}$ foi obtida por inspeção.
  - No entanto, caso o módulo m é grande, sempre podemos usar o algoritmo euclidiano para encontrar sua solução única

Teorema do Resto Chinês

Um velho enigma chinês faz a seguinte pergunta.

- Existe um inteiro positivo x tal que, quando x é dividido por 3, produz um resto 2, quando x é dividido por 5 resulta em resto 4, e quando x é dividido por 7 dá um resto 6?

Em outras palavras, buscamos uma solução comum das três equações de congruência a seguir: $x \equiv 2(mod 3)$, $x \equiv 4(mod 5)$, $x \equiv 6(mod 7)$

- Observe que os módulos 3, 5 e 7 são pares relativamente primos. (Módulos é o plural de módulo.)
- Assim, aplica-se o seguinte teorema; ela nos diz que existe uma solução única módulo $M = 3 * 5 * 7 = 105$.

Teorema do Resto Chinês

- Teorema: Considere o sistema $x \equiv r_1 \pmod{m_1}$, $x \equiv r_2 \pmod{m_2}$, $\ldots$, $x \equiv r_k \pmod{m_k}$, onde os m_i são pares relativamente primos.
- Então o sistema tem um único módulo de solução $M = m_1 m_2 \ldots m_k$.
- Na verdade, pode-se fornecer uma fórmula explícita para a solução do sistema no teorema que afirmamos como uma proposição.

Teorema do Resto Chinês

- Proposição: Considere o sistema de equações de congruência. Seja $M = m_1 m_2 \ldots m_k$, e $M_1 = \frac{M}{m1}$, $M_2 = \frac{M}{m2}$, (Então cada par M_i e m_i são co-primos.)
- Sejam s_1 , s_2, ..., s_k as soluções respectivamente, das equações de congruência $M_1 x \equiv 1 \pmod{m_1}$, $M_2 x \equiv 1 \pmod{m_2}$, ..., $M_k x \equiv 1 \pmod{m_k}$
- Então segue a solução do sistema:
  $x_0 = M_1 s_1 r_1 + M_2 s_2 r_2 + \ldots + M_k s_k r_k$
- Agora resolvemos o enigma original de duas maneiras.

Teorema do Resto Chinês: Método 1

- Método 1: Primeiro aplicamos o Teorema Chinês do Resto (TRC) às duas primeiras equações, (a) $x \equiv 2 \pmod 3$ (b) $x \equiv 4 \pmod 5$
- CRT nos diz que existe uma solução única módulo $M = 3 * 5 = 15$.
- Somando múltiplos do módulo $m = 5$ ao dada solução $x = 4$ da segunda equação (b), obtemos as seguintes três soluções de (b) que são menos de 15:
  4, 9, 14
- Testando cada uma dessas soluções na equação (a), descobrimos que 14 é a única solução de ambas as equações.

Teorema do Resto Chinês: Método 1

- Agora aplicamos o mesmo processo às duas equações (c) $x \equiv 14 \pmod{15}$ e (d) $x \equiv 6 \pmod{7}$
- CRT nos diz que existe uma solução única módulo $M = 15 * 7 = 105$.
- Somando múltiplos do módulo $m = 15$ a Dada a solução $x = 14$ da primeira equação (c), obtemos as seguintes sete soluções de (b) que são menos de 105:
  14, 29, 44, 59, 74, 89, 104
- Testando cada uma dessas soluções de (c) na segunda equação (d), descobrimos que 104 é a única solução de ambas equações
- Assim, o menor inteiro positivo que satisfaz todas as três equações é $x = 104$ Esta é a solução do enigma.

Teorema do Resto Chinês: Método 2

- Método 2: Usando a notação acima, obtemos $M = 3 * 5 * 7 = 105$, $M_1 = 105/3 = 35$, $M_2 = 105/5 = 21$, $M_3 = 105/7 = 15$
- Agora buscamos soluções para as equações $35x \equiv 1 \pmod 3$, $21x \equiv 1 \pmod 5$, $15x \equiv 1 \pmod 7$
- Reduzindo 35 módulo 3, reduzindo 21 módulo 5 e reduzindo 15 módulo 7, produz o sistema $2x \equiv 1 \pmod 3$, $x \equiv 1 \pmod 5$, $x \equiv 1 \pmod 7$
- As soluções dessas três equações são, respectivamente, $s_1 = 2$, $s_2 = 1$, $s_3 = 1$

Teorema do Resto Chinês: Método 2

- Agora substituímos na fórmula $x_0 = M_1 s_1 r_1 + M_2 s_2 r_2 + \ldots + M_k s_k r_k$ para obter a seguinte solução do nosso sistema original:
  $x_0 = 35 * 2 * 2 + 21 * 1 * 4 + 15 * 1 * 6 = 314$
- Dividindo esta solução pelo módulo $M = 105$, obtemos o restante $x = 104$ que é a única solução do enigma entre 0 e 105.
- **Observação**: As soluções acima $s_1 = 2$, $s_2 = 1$, $s_3 = 1$ foram obtidas por inspeção.
- Se os módulos forem grandes, nós sempre pode usar o algoritmo euclidiano para encontrar tais soluções