Aula 15. Sistemas de congruências

Seja dado o sistema das congruências:

$$\begin{cases} a_1 \cdot x \equiv b_1 \pmod{m_1} \\ a_2 \cdot x \equiv b_2 \pmod{m_2} \\ \vdots \\ a_k \cdot x \equiv b_k \pmod{m_k}, \end{cases} \tag{15.1}$$

onde $a_1, \ldots, a_k$, $b_1, \ldots, b_k$ são inteiros dados, $m_1, \ldots, m_k - 1$ inteiros dados positivos e x é inteiro incognito.

Notamos que para existir a solução do sistema é necessario (mas não é suficiente) que $\mathrm{mdc}(a_i, m_i) \mid b_i$ para todo $i = 1, \ldots, k$.

Seja $d_i = \mathrm{mdc}(a_i, m_i)$ e supouha gue $d_i \mid b_i$. Assim a congruência linear $a_i x \equiv b_i \pmod{m_i}$ tem mesmas soluções como a congruência

$$x \equiv c_i \pmod{n_i},$$

onde $n_i = \frac{m_i}{d_i}$, $c_i = \tau_i \cdot \frac{b_i}{d_i}$ (com r_i tal que $a_i r_i + m_i s_i = d_1$ pelo Teorema de Bezout). Logo o sistema inicial é equivalente ao sistema

$$\begin{cases} x \equiv c_1 \pmod{n_1} \\ x \equiv c_2 \pmod{n_2} \\ \vdots \\ x \equiv c_k \pmod{n_k}, \end{cases} \tag{15.2}$$

Theorem 15.1: Chinese do Resto

Sejam $n_1, \ldots, n_k$ tais que $\mathrm{mdc}(n_i, n_j) = 1$, se $i \neq j$ e sejam $c_1, \ldots, c_k$ os inteiros dados. Assim o sistema acima admite a solução $t \in \mathbb{Z}$. Alem disso, se $q \in \mathbb{Z}$ é qualquer outro solução do sistema, assim

$$q \equiv t \pmod{n_1 \cdot n_2 \cdot \ldots n_k}.$$

Prova

Consideramos os seguintes numeros,

$$N = n_1 \cdot n_2 \cdot \ldots h_k,$$
$$N_i = \frac{N}{n_i}, \quad i = 1, \ldots, k.$$

Como $\mathrm{mdc}(n_i, n_j) = 1$ para $i \neq j$, assim

$$\mathrm{mdc}\,(N_i, n_i) = 1,$$

e pelo Teorema de Bezout existem r_i, s_i tais que:

$$N_i \cdot r_i + n_i \cdot s_i = 1.$$

Considere o seguinte numero

$$t = N_i r_1 \cdot c_1 + N_2 \cdot r_2 c_2 + \ldots + N_k r_k \cdot c_t.$$

Mostremos que t é solução do sistema. Como $N_i r_i + n_i s_i = 1$, assim $N_i r_i \equiv 1 \pmod{n_i}$, logo

$$N_i r_i c_i \equiv c_i \pmod{n_i}, \quad i = 1, \ldots, k.$$

Além disso, se $i \neq j$ então $n_i \mid N_j$ e $N_j \equiv 0 (\bmod n_i)$. logo

$$N_j r_j c_j \equiv 0 (\bmod n_i), \quad i \neq j$$

Assim

$$\underbrace{N_1 r_1 C_1 + N_2 r_2 C_2 + \ldots + N_i r_i c_i + \ldots + N_k r_k c_k}_{=t} = 0 + 0 \ldots + c_i + 0 + \ldots + 0 \pmod{n_i}.$$

Ou seja $t \equiv c_i (\bmod n_i)$ para todo $i = 1, \ldots, k$, e t é solução do sistema.
Se q é inteiro tal que $q \equiv c_i (\bmod n_i)$, assim $q \equiv t (\bmod n_i)$ para toolo i, logo $n_i \mid q - t$. Mas n_i são dois a dois primos entre se, assim $n_1 \cdot \ldots \cdot n_k \mid q - t$, ou seja

$$q \equiv t \pmod{n_1 \cdot n_2 \cdot \ldots \cdot n_k}.$$

Finalmente, se $q \equiv t \pmod{n_1 \cdot \ldots \cdot n_k}$ assim $n_1 \cdot \ldots n_k \mid q - t$, logo $n_i \mid q - t$ e

$$q \equiv c_i \pmod{n_i}.$$

Portanto todos outros soluções do sistema tem forma $q \equiv t \pmod{n_1 \cdot \ldots \cdot n_k}$.

15.1 Exemplos

Exemplo 15.1

Considere o seguinte sistema

$$\begin{aligned} 6x &\equiv 2 \pmod 4 \\ 2x &\equiv 1 \pmod 3 \\ 4x &\equiv 2 \pmod 7). \end{aligned}$$

Primeiramente vamos reduzir esse sistema para forma (15.2). No caso temos $a_1 = 6, a_2 = 2, a_3 = 4$, $b_1 = 2, b_2 = 1, b_3 = 2$ e $m_1 = 4$, $m_2 = 3$, $m_3 = 7$. Agora

$$\begin{aligned} d_1 &= \mathrm{mdc}(a_1, m_1) = \mathrm{mdc}(6,4) = 2, & 2 &= 6 \cdot 1 + 4 \cdot (-1), & r_1 &= 1, \\ d_2 &= \mathrm{mdc}(a_2, m_2) = \mathrm{mdc}(2,3) = 1, & 1 &= 2 \cdot 2 + 3 \cdot (-1), & r_2 &= 2 \\ d_3 &= \mathrm{mdc}(a_3, m_3) = \mathrm{mdc}(4,7) = 1, & 1 &= 4 \cdot 2 + 7 \cdot (-1), & r_3 &= 2. \end{aligned}$$

Portanto temos

$$\begin{aligned} x &\equiv r_1 \frac{b_1}{d_1} = 1 (\mathrm{mod}\, \frac{4}{2}) \\ x &\equiv r_2 \frac{b_2}{d_2} = 2 (\mathrm{mod}\, \frac{3}{1}) \\ x &\equiv r_3 \frac{b_3}{d_3} = 4 (\mathrm{mod}\, \frac{7}{1}). \end{aligned}$$

Assim esse sistema é

$$x \equiv 1 (\mathrm{mod} 2), \quad x \equiv 2 (\mathrm{mod} 3), \quad x \equiv 4 (\mathrm{mod} 7).$$

e $c_1 = 1$, $c_2 = 2$, $c_3 = 4$, $n_1 = 2$, $n_2 = 3$, $n_3 = 7$.
Usando o formula da prova do Teorema Chinês do Resto, recebemos

$$N = n_1 \cdot n_2 \cdot n_3 = 42,$$

e

$$N_1 = N/n_1 = 42/2 = 21, \quad N_2 = N/n_2 = 42/3 = 14, \quad N_3 = N/n_3 = 42/7 = 6.$$

Agora

$$\begin{aligned} \mathrm{mdc}(N_1, n_1) &= \mathrm{mdc}(21,2) = 1, & 1 &= 21 \cdot 1 - 2 \cdot 10, & r_1 &= 1, \\ \mathrm{mdc}(N_2, n_2) &= \mathrm{mdc}(14,3) = 1, & 1 &= 14 \cdot 2 - 3 \cdot 9, & r_2 &= 2 \\ \mathrm{mdc}(N_3, n_3) &= \mathrm{mdc}(6,7) = 1, & 1 &= 6 \cdot (-1) + 7 \cdot 1, & r_3 &= (-1). \end{aligned}$$

Assim a solução t é

$$\begin{aligned} N_1 \cdot r_1 \cdot c_1 + N_2 \cdot r_2 \cdot c_2 + N_3 \cdot r_3 \cdot c_3 =& 21 \cdot 1 \cdot 1 + 14 \cdot 2 \cdot 2 + 6 \cdot (-1) \cdot 4 = \\ =& 21 + 56 + (-24) = 53. \end{aligned}$$

È fácil conferir que

$$53 \equiv 1 (\mathrm{mod} 2), \quad 53 \equiv 2 (\mathrm{mod} 3), \quad 53 \equiv 4 (\mathrm{mod} 7)$$

Todos outros soluções (através o Teorema Chinese de Resto) tem forma

$$53 + 2 \cdot 3 \cdot 7 \cdot k = 53 + 42k, \quad k \in \mathbb{Z}.$$

È interessante saber o que acoutece se n_i's não foram relativamente primos? No caso acontece que o sistema (15.2) pode ter ou não ter as soluções. Vamos ver alguns exemplos.

Exemplo 15.2

Considere o sistema

$$x \equiv -1(\operatorname{mod} 4)$$
$$x \equiv 2(\operatorname{mod} 6)$$

Como $x \equiv -1(\operatorname{mod} 4)$ assim $x = 4t - 1$ com t um inteiro. Agora $x \equiv 2(\operatorname{mod} 6)$ implique que

$$4t - 1 \equiv 2(\operatorname{mod} 6)$$

ou seja $4t \equiv 3 \pmod 6$. Mas ultima congruência não tem as soluções, pois $\operatorname{mdc}(4,6) = 2 \nmid 3$. assim o sistema original não tem as soluções.

Exemplo 15.3

Considere o sistema

$$x \equiv -1(\operatorname{mod} 4)$$
$$x \equiv 2(\operatorname{mod} 6)$$

um pouco modificado. De novo $x = 4k - 1$ com k um inteiro. Agora equação $x \equiv 3(\operatorname{mod} 6)$ implique que $4k - 1 \equiv 3(\operatorname{mod} 6)$ ou seja $4k \equiv 4 \pmod 6$. Claro que $k = 1$ é solução da ultima congruencia e todas outras soluções tem forma $k = 1 + 3l$, com l um inteiro. Logo

$$x = 4k - 1 = 4(1 + 3l) - 1) = 12l - 3$$

são todas soluções do sistema dado.

15.2 *Algoritmo de Gauss*

Notamos que o Teorema Chinês de Resto fornece um algoritmo para procurar as soluções do sistema (15.2). Este algoritmo é chamado Algoritmo de Gauss. De baixo vamos descrever o algoritmo em detalhes.

Seja dado o sistema

$$x \equiv c_1 \,(\operatorname{mod} n_1)$$
$$\vdots$$
$$x \equiv c_k \,(\operatorname{mod} n_k)$$

com $\operatorname{mdc}(n_i, n_j) = 1$ se $i \neq j$. Seja

$$N = n_1 \cdot \cdots \cdot n_k,$$

assim a geral solução desse sistema é dado por

$$x \equiv N_1 \cdot c_1 \cdot d_1 + N_2 \cdot c_2 \cdot d_2 + \ldots + N_k \cdot c_k \cdot d_k (\operatorname{mod} N)$$

Johann Carl Friedrich Gauß (1777–1855)

onde $N_i = \frac{N}{n_i}$ e d_i tais que

$$N_i \cdot d_i \equiv 1 \pmod{n_i}.$$

Observem que a parte "pesado" do algoritmo é encontrar aqueles inteiros d_i's. Como vamos ver de baixo podemos simplificar o cargo considerando o noção de inverso modular.

Definição: Inverso modular

Sejam a, n dois inteiros com $n > 0$. O *inverso modular* de a modulo n é qualquer inteiro x tal que

$$a \cdot x \equiv 1 (\operatorname{mod} n).$$

Observação 15.1

Observem que o inverso modular do a modulo n existe se e somente se a congruência

$$a \cdot x \equiv 1 (\operatorname{mod} n),$$

tem solução, ou seja se e somente se

$$\operatorname{mdc}(a, n) \mid 1,$$

o que equivalente que $\operatorname{mdc}(a, n) = 1$.

Observem que em algoritmo de Gauss aqueles inteiros d_i's são inversos modulares de N_i's modulo n_i's. Assim a seguinte pergunta aparece naturalmente: como procurar inverso modular de um inteiro dado?

De baixo apresentamos dois metodos: um atraves o algoritmo de Euclides e outro é "teste-erros".

1°. **Metodo** (usando algoritmo de Euclides).

Se $\operatorname{mdc}(a, n) = 1$, assim

$$a \cdot r + n \cdot s = 1,$$

para alguns inteiros r, s, logo

$$a \cdot r \equiv 1 \pmod{n}$$

e portanto o inverso modular de a é r.

2°. **Metodo** ("Preguiçoso")

È testar todos r possiveis entre $1, \ldots, n-1$ ou testar $r = a^i$ quando $i = 1, 2, \ldots, n-1$.

Exemplo 15.4

Suponha que $a = 3$ e $n = 20$. Aplicando algoritmo de Euclides, temos que

$$20 = 3 \cdot 6 + 2$$
$$3 = 2 \cdot 1 + 1.$$

Invertendo, temos

$$1 = 3 - 2 \cdot 1 = 3 - (20 - 3 \cdot 6) = 3 \cdot 7 - 20.$$

Assim inverso modular de 3 modulo 20 é 7.
O mesmo resultado podemos receber aplicando o segundo método, testando $r = 1, 2, ...19$, temos

$$\begin{aligned} r &= 1, \quad 3 \cdot 1 = 3 \\ r &= 2, \quad 3 \cdot 2 = 6 \\ r &= 3, \quad 3 \cdot 3 = 9 \\ r &= 4, \quad 3 \cdot 4 = 12 \\ r &= 5, \quad 3 \cdot 5 = 15 \\ r &= 6, \quad 3 \cdot 6 = 18 \\ r &= 7, \quad 3 \cdot 7 = 21 \end{aligned}$$

21 tem resto 1 quando divide por 20, assim 7 é inverso modular do 3.
Equivalente, podemos testar as potencias de a^i:

$$\begin{aligned} r &= a^1, \quad 3 \cdot 3 = 9 \\ r &= a^2, \quad 3 \cdot 9 = 27 \\ r &= a^3, \quad 3 \cdot 3^3 = 81 \end{aligned}$$

Agora 81 tem resto 1 quando divide por 20, assim $r = a^3 = 27$ é inverso modular de 3. Notamos que $27 \equiv 7 (\bmod 20)$ assim isso é compatível com as respostas acima.

Exemplo 15.5

Seja

$$\begin{aligned} x &\equiv 1(\bmod 3) \\ x &\equiv 2(\bmod 4) \\ x &\equiv 3(\bmod 5) \end{aligned}$$

Aplicando Algoritmo de Gauss, temos:

$$N = n_1 \cdot n_2 \cdot n_3 = 3 \cdot 4 \cdot 5 = 60.$$

$$\begin{aligned} N_1 &= \frac{N}{n_1} = \frac{60}{3} = 20, \quad d_1 = 2, \text{ pois } 2 \cdot 20 \equiv 1(\bmod 3) \\ N_2 &= \frac{N}{u_2} = \frac{60}{4} = 15, \quad d_2 = 3, \text{ pois } 3 \cdot 15 = 1(\bmod 4) \\ N_3 &= \frac{N}{n_3} = \frac{60}{5} = 12, \quad d_3 = 3, \text{ pois } 3 \cdot 12 \equiv 1(\bmod 5) \end{aligned}$$

$$\begin{aligned} \Rightarrow x &= N_1 \cdot c_1 \cdot d_1 + N_2 \cdot c_2 \cdot d_2 + N_3 \cdot c_3 \cdot d_3 \\ &= 20 \cdot 1 \cdot 2 + 15 \cdot 2 \cdot 3 + 12 \cdot 3 \cdot 3 = 238 \end{aligned}$$

Ou, equivalente,

$$x \equiv 58 \quad (\bmod 60).$$

Exercício 15.1: (Trabalho p/ casa)

a) $\begin{cases} x & \equiv 1 \quad (\bmod 4) \\ x & \equiv 3 \quad (\bmod 7) \end{cases}$

b) $\begin{cases} x & \equiv 2 \quad (\bmod 3) \\ x & \equiv 0 \quad (\bmod 5) \\ x & \equiv 0 \quad (\bmod 8) \end{cases}$

c) $\begin{cases} x \equiv 1 \quad (\bmod 2) \\ x \equiv 2 \quad (\bmod 3) \\ x \equiv 3 \quad (\bmod 5) \\ x \equiv 4 \quad (\bmod 7) \end{cases}$

Respostas: a) $x \equiv 17(\bmod 42)$

b) $x \equiv 80(\bmod 120)$

c) $x \equiv 53(\bmod 210)$