Aula 12. Congruências II

12.1 Congruências lineares

Vamos lembrar que na Aula passada a gente definiu as congruências e vimos como aplicar eles nas manipulações para encontrar os restos da divisão de certos inteiros.

Definição

Seja n um inteiro positivo. Dois inteiros a, b chamam-se *congruentes modulo n* se n divide $(a - b)$. Neste caso escrevemos

$$a \equiv b \pmod{n}.$$

Hoje vamos tentar resolver as *congruências lineares*

$$ax \equiv b \pmod{n},$$

onde a, b, n são inteiros dados e n é inteiro incógnito. Dizemos que um inteiro t é solução da congruência linear se

$$at \equiv b \pmod{n}.$$

Se não existir tais t, assim dizemos que a congruência linear não tem as soluções. Notamos que tais congruências podem ter ou não ter as soluções. Por exemplo

$$2x \equiv 1 \pmod{4},$$

não tem as soluções, pois o lado esquerdo da congruência é sempre par independendo do x e lado direito é um inteiro impar. Logo a diferençá $2x - 1$ nunca é um múltiplo de 4. Por outro lado a congruência

$$2x \equiv 0 \pmod{3},$$

tem vários soluções, por exemplo é fácil ver que

$$x = 0, 3, 6, 9, \dots,$$

são soluções dessa congruência.

Assim nossos objetivos para hoje é entender quando a congruência linear dada tem as soluções e descrever todas soluções

12.2 Existência das soluções

Para receber o criterio da existencia das soluções de

$$ax \equiv b \pmod{n},$$

notamos o seguinte

$$\begin{aligned} a \cdot x \equiv b (\text{mod } n) & \\ \text{tem solução} &\Leftrightarrow \text{ Existe } t \text{ tal que} \\ & \quad a \cdot t \equiv b (\text{mod } n) \\ &\Leftrightarrow n \mid a \cdot t - b \\ &\Leftrightarrow n \cdot k = a \cdot t - b \\ &\Leftrightarrow b = a \cdot t + n \cdot (-k) \\ &\Leftrightarrow \text{ Equação }, \quad b = a \cdot x + n \cdot y \text{ tem solução} \\ &\Leftrightarrow \text{mdc}(a, n) \mid b \end{aligned}$$

Assim isso prova do critério bem simples da existência das soluções:

Teorema 12.1

A congruência $ax \equiv b \pmod{n}$ tem solução se e somente se $d = \text{mdc}(a, n)$ divide b.

Exemplo 12.1

A gente viu antes que a congruencia

$$2x \equiv 1 \pmod{4},$$

não tem as soluções. È fácil ver isso através o critério acima também. No caso temos que $a = 2$, $b = 1$, $n = 4$. Assim

$$d = \text{mdc}(a, n) = \text{mdc}(2, 4) = 2 \nmid 1 = b.$$

Logo, não há soluções.

Exemplo 12.2

A congruência

$$4x \equiv 10 \pmod{6},$$

tem as soluções, pois

$$d = \text{mdc}(a, n) = \text{mdc}(4, 6) = 2 \mid 10 = b.$$

È fácil ver isso manualmente, pois neste caso, por exemplo

$$4 \cdot 1 \equiv 10 \pmod{6}.$$

Exemplo 12.3

Se temos a congruência

$$31x \equiv 47 \pmod{53}.$$

Assim,

$$d = \mathrm{mdc}(a,n) = \mathrm{mdc}(31,53) = 1 \mid 47 = b.$$

Logo a congruências tem as soluções. Mas não é muito claro como encontrar pelo menos uma solução. Isso é o que vamos fazer na próxima seção.

12.3 *Todas soluções*

Teorema 12.2

Suponha que dada a congruência $ax \equiv b \pmod{n}$ com $d = \mathrm{mdc}(a,n) \mid b$. Assim essa congruência tem exatamente d soluções não-congruente dois a dois dados por seguintes formulas:

$$\begin{aligned} x_0 &= r \cdot b/d, \\ x_1 &= r \cdot b/d + n/d, \\ x_2 &= r \cdot b/d + 2n/d, \\ &\vdots \\ x_{d-1} &= r \cdot b/d + (d-1)n/d, \end{aligned}$$

onde

$$d = ar + ns,$$

usando o Teorema de Bezout (veja Aula 6).

Prova

Vamos dividir a prova em três etapas. 1) Primeiramente mostremos que todo x_i é solução da congruência acima. Como $d = \mathrm{mdc}(a,n)$ divide a, n, b, assim existem a_1, n_1, b_1, tais que

$$a = a_1 \cdot d, \quad n = n_1 \cdot d, \quad b = b_1 \cdot d,$$

ou seja

$$a/d = a_1, \quad n/d = n_1, \quad b/d = b_1.$$

Nestes termos temos que $1 = a_1 r + n_1 s$. Assim, para todo i temos

$$\begin{aligned} ax_i - b &= a \cdot (r \cdot b_1 + i \cdot n_1) - b \\ &= a_1 \cdot d \cdot (r \cdot b + in_1) - b_1 \cdot d \\ &= d \cdot (a_1 \cdot r \cdot b_1 + a_1 \cdot i \cdot n_1 - b_1) \\ &= d \cdot (b_1 (a_1 r - 1) + ia_i n_1) \\ &= d \cdot (b_1(-n, s) + ia_1 n_1) \\ &= d \cdot n_1 (-b_1 s + iq_1) \Rightarrow n \mid (ax_i - b) \end{aligned}$$

Prova

2) Agora vamos mostrar que x_i's não congruentes dois a dois. Suponha que $x_i \equiv x_j \pmod{n}$ para alguns i e j, ou seja

$$r \cdot b_1 + i \cdot n_1 \equiv r \cdot b_1 + j \cdot n_1 \pmod{n}.$$

Assim temos que

$$i \cdot n_1 \equiv j \cdot n_1 \pmod{n}.$$

Logo $n = n_1 d$ divide $n_1(i-j)$, ou seja $d \mid (i-j)$. Como i, j variam entre 0 e $d-1$, assim

$$0 \leq i \leq d-1$$
$$-d+1 \leq -j \leq 0$$

Somando estes desigualdades temos

$$-(d-1) \leq i-j \leq d-1$$

Logo, o fato que $d \mid (i-j)$ implique que $i = j$.
3) Finalmente, vamos mostrar que se g é uma outra solução da congruência, assim g é congruente para algum x_d. De fato, neste caso temos que

$$n \cdot t = a \cdot g - b,$$

para algum t, ou seja par (g, t) é solução da equação diofântina

$$a \cdot X + n \cdot Y = b.$$

Da Aula 8, todas soluções tem forma

$$\left(rb_1 + kn_1, sb_1 - ka_1\right),$$

para algum $k \in \mathbb{Z}$. Assim $g = rb_1 + kn_1$ para algum k. Usando algoritmo da divisão de k por d, temos

$$k = qd + r', \qquad 0 \leq r' < d.$$

Assim

$$g = r \cdot b_1 + \left(q \cdot d + r'\right) n_1 = \underbrace{rb_1 + r'n_1} + qdn_1 = x_{r'} + n \cdot q.$$

Ou seja

$$g \equiv x_{r'} \pmod{n}.$$

Corolário 12.1

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

$$ax \equiv b \pmod{n}$$

tem uma única solução modulo n.

12.4 *Exemplos*

Exemplo 12.4

Suponha que dada congruência

$$2x \equiv 3 (\text{mod } 5)$$

Temos $a = 2$, $b = 3$, $n = 5$. Neste caso $d = \text{mdc}(2, 5) = 1$ assim a equação tem uma única solução. Podemos apresentar d como $d = 1 = 2 \cdot 3 + 5 \cdot (-1) = a \cdot r + n \cdot s$. Agora usando o formula do Teorema, temos

$$x = r \cdot b/d = 3 \cdot \frac{3}{1} = 9.$$

Agora notamos que $9 \equiv 4 \ (\text{mod} 5)$. Assim a solução da congruência é $x \equiv 4$ (ou seja $x = 5t + 4$, para algum t inteiro).

Exemplo 12.5

Suponha que dada congruência

$$9x \equiv 21 (\text{mod } 30)$$

Temos $a = 9$, $b = 21$, $n = 30$. Neste caso $d = \text{mdc}(9, 30) = 3$ assim a equação tem $d = 3$ soluções. Podemos apresentar $d = 3$ como $d = 3 = 9 \cdot (-3) + 30 \cdot 1 = a \cdot r + n \cdot s$. Agora usando o formula do Teorema, temos

$$\begin{aligned}
x_0 &= r \cdot b/d = -3 \cdot \frac{21}{3} = -21, \\
x_1 &= r \cdot b/d + n/d = -3 \cdot \frac{21}{3} + 30/3 = -21 + 10 = -11, \\
x_2 &= r \cdot b/d + 2n/d = -3 \cdot \frac{21}{3} + 2 \cdot 30/3 = -21 + 20 = -1.
\end{aligned}$$

Agora notamos que $-21 \equiv 9 \ (\text{mod } 30)$, $-11 \equiv 19 \ (\text{mod } 30)$ e $-1 \equiv 29 \ (\text{mod } 30)$. Assim as soluções da congruência são

$$x_0 \equiv 9, \quad x_1 \equiv 19, \quad x_2 \equiv 29.$$

Exemplo 12.6

Suponha que dada congruência

$$6x \equiv 14 (\bmod\ 4)$$

Temos $a = 6$, $b = 14$, $n = 4$. Neste caso $d = \text{mdc}(6, 4) = 2$ assim a equação tem $d = 2$ soluções. Podemos apresentar $d = 2$ como $d = 2 = 6 \cdot 1 + 4 \cdot (-1) = a \cdot r + n \cdot s$. Agora usando o formula do Teorema, temos

$$x_0 = r \cdot b/d = 1 \cdot \frac{14}{2} = 7,$$
$$x_1 = r \cdot b/d + n/d = 1 \cdot \frac{14}{2} + 4/2 = 7 + 2 = 9.$$

Agora notamos que $9 \equiv 1 \pmod 4$, e $7 \equiv 3 \pmod 4$. Assim as soluções da congruência são

$$x_0 \equiv 1, \quad x_1 \equiv 3.$$

Exemplo 12.7

Suponha que dada congruência

$$34x \equiv 8 (\bmod\ 10)$$

Temos $a = 34$, $b = 8$, $n = 10$. Neste caso $d = \text{mdc}(34, 10) = 2 \mid 8$ assim a equação tem $d = 2$ soluções. Podemos encontra o r invertendo algoritmo de Euclides. Pelo algoritmo de Euclides temos

$$34 = 3 \cdot 10 + 4$$
$$10 = 2 \cdot 4 + 2$$
$$4 = 2 \cdot 2 + 0.$$

Invertendo o processo, temos

$$2 = 10 - 2 \cdot 4 = 10 - 2 \cdot (34 - 3 \cdot 10) = 34 \cdot (-2) + 10 \cdot 7,$$

ou seja $r = (-2)$. Aplicando os formulas temos

$$x_0 = r \cdot b/d = (-2) \cdot \frac{8}{2} = -8,$$
$$x_1 = r \cdot b/d + n/d = (-2) \cdot \frac{8}{2} + 10/2 = -8 + 5 = -3.$$

Agora notamos que $-8 \equiv 2 \pmod{10}$, e $-3 \equiv 7 \pmod{10}$. Assim as soluções da congruência são

$$x_0 \equiv 2, \quad x_1 \equiv 7.$$

Exercício 12.1

Descrever todos b tais que

$$34x \equiv b (\text{mod } 17)$$

tem as soluções.

Solução 12.1

Pelo Teorema 12.1 a congruência tem as soluções se e somente se $\text{mdc}(34, 17)$ divide b. Como $\text{mdc}(34, 17) = 17$, assim 17 deve dividir b, ou seja

$$b = 17t, \quad t \in \mathbb{Z}.$$

Exercício 12.2

Resolve

$$(n-1)x \equiv b \pmod{n}.$$

Solução 12.2

Para todo inteiro n temos

$$(n-1) \equiv -1 \pmod{n}.$$

Multiplicando essa congruencia por x temos

$$(n-1)x \equiv -x \pmod{n}.$$

Assim, temos que

$$-x \equiv b \pmod{n},$$

ou seja

$$x = nt - b, \quad t \in \mathbb{Z}.$$

Exercício 12.3: (Trabalho p/ casa)

Encontre as soluções das seguintes congruências

(a) $2x \equiv 5 (\bmod 7)$.

(b) $6x \equiv 5 (\bmod 8)$.

(c) $19x \equiv 30 (\bmod 40)$.

(d) $234x \equiv 60 (\bmod 762)$.

(e) $128x \equiv 833 (\bmod 1001)$.

Resposta:

(a) $x \equiv 6$.

(b) Não tem soluções.

(c) $x \equiv 10$.

(d) $x \equiv 124, 251, 378, 505, 632, 759$.

(e) $x \equiv 72$.