Critérios de divisibilidade

Se $a_0, a_1, \dots, a_n \in \{0,1,2,3,\dots,8,9\}$ e $a_n \neq 0$, o número

$$a = a_n \times 10^n + a_{n-1} \times 10^{n-1} + \dots + a_2 \times 10^2 + a_1 \times 10 + a_0$$

é um inteiro positivo com $n+1$ algarismos (representação de a na base 10)

Representamos este número $\overline{a_n a_{n-1} \dots a_2 a_1 a_0}$. Não havendo ambiguidade, não se coloca a barra.

Por exemplo, $\overline{459} = 4 \times 10^2 + 5 \times 10 + 9$.

$\overline{5p8} = 5 \times 10^2 + p \times 10 + 8$

Teorema Seja $m \in \mathbb{N}$. Se $R_1, R_2, \dots, R_{n-1}, R_n$ são os restos da divisão de $10, 10^2, \dots, 10^{n-1}, 10^n$, respect., por m, então

$$\overline{a_n a_{n-1} \dots a_2 a_1 a_0} \equiv a_n R_n + a_{n-1} R_{n-1} + \dots + a_2 R_2 + a_1 R_1 + a_0 \pmod{m}$$

Demonst: Temos $10^k \equiv r_k \pmod{m}$

Logo $a_k 10^k \equiv a_k r_k \pmod{m}$, Somando ao longo de

$k \in \{0, 1, \dots, n\}$ vem $a_n 10^n + \dots + a_1 10 + a_0 \equiv a_n r_n + \dots + a_1 r_1 + a_0 \pmod{m}$.

□

Exemplo Determinar o resto da divisão de 1492 por 3

Como $10 \equiv 1 \pmod{3}$

$10^2 = 1 \pmod{3}$

$10^3 \equiv 1 \pmod{3}$

Logo $1 \times 10^3 + 4 \times 10^2 + 9 \times 10 + 2 \equiv 1 + 4 + 9 + 2 \pmod{3}$

ou seja, $1492 \equiv 16 \pmod{3}$ mas $16 \equiv 1 \pmod{3}$

Logo $1492 \equiv 1 \pmod{3}$.

Critérios de divisibilidade para: 2, 5, 3, 9, 4 e 11

- $n = 2$

$$\left.\begin{array}{l} 10 \equiv 0 \pmod 2 \\ 10^k \equiv 0 \pmod 2 \end{array}\right\} \Rightarrow \overline{a_n a_{n-1} \cdots a_2 a_1 a_0} \equiv a_0 \pmod 2$$

Critério da divisibilidade por 2: O resto da divisão de um inteiro positivo a por 2 é o resto que se obtém dividindo o algarismo das unidades por 2.

- $n = 5$

Como $\left.\begin{array}{l} 10 \equiv 0 \pmod 5 \\ 10^k \equiv 0 \pmod 5 \end{array}\right\} \Rightarrow \overline{a_n a_{n-1} \cdots a_2 a_1 a_0} \equiv a_0 \pmod 5$

Critério da divisibilidade por 5: O resto da divisão de um inteiro positivo a por 5 é o resto que se obtém dividindo o algarismo das unidades por 5.

- $n = 3$

$$\left.\begin{array}{l} 10 \equiv 1 \pmod 3 \\ 10^k \equiv 1 \pmod 3 \end{array}\right\} \Rightarrow \overline{a_n a_{n-1} \cdots a_2 a_1 a_0} \equiv a_n + a_{n-1} + \cdots + a_2 + a_1 + a_0 \pmod 3$$

Critério da divisibilidade por 3: O resto da divisão de um inteiro positivo a por 3 é o resto que se obtém dividindo por 3 a soma de todos os algarismo de a.

- $n = 9$

$$\left.\begin{array}{l} 10 \equiv 1 \pmod 9 \\ 10^k \equiv 1 \pmod 9 \end{array}\right\} \Rightarrow \overline{a_n a_{n-1} \cdots a_2 a_1 a_0} \equiv a_n + a_{n-1} + \cdots + a_2 + a_1 + a_0 \pmod 9$$

Critério da divisibilidade por 9: O resto da divisão de um inteiro positivo a por 9 é o resto que se obtém dividindo por 9 a soma de todos os algarismo de a.

- $n = 4$

$$\left.\begin{array}{l} 10 \equiv 2 \pmod 4 \\ 10^2 \equiv 4 \pmod 4 \\ 10^2 \equiv 0 \pmod 4 \\ 10^k \equiv 0 \pmod 4,\ k \geq 2 \end{array}\right\} \Rightarrow \overline{a_n a_{n-1} \cdots a_2 a_1 a_0} \equiv a_1 \times 2 + a_0 \pmod 4$$

Critério da divisibilidade por 4: O resto da divisão de um inteiro positivo a por 4 é o resto da divisão por 4 da soma do algarismo das unidades com o dobro do algarismo das dezenas de a.

- $n = 11$

$$\left.\begin{array}{l} 10 \equiv -1 \pmod{11} \\ 10^k \equiv (-1)^k \pmod{11} \end{array}\right\} \Rightarrow \overline{a_n a_{n-1} \cdots a_2 a_1 a_0} \equiv$$

$$\equiv a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^n a_n \pmod{11}$$

$$\Rightarrow \overline{a_n a_{n-1} \dots a_2 a_1 a_0} = (a_0 + a_2 + a_4 + \dots) - (a_1 + a_3 + \dots) \pmod{11}$$

Critério da divisibilidade por 11: O resto da divisão de um inteiro positivo a por 11 é o resto da divisão por 11 da diferença da soma dos algarismos de ordem par com a soma dos algarismo de ordem ímpar.

Congruências lineares

Definição: Chama-se congruência linear a toda a expressão da forma $ax \equiv b \pmod{n}$ em que $a, b \in \mathbb{Z}$, $a \neq 0$ e x é uma incógnita. Chama-se solução da congruência linear a qualquer inteiro x_0 que verifique $ax_0 \equiv b \pmod{n}$ $n \in \mathbb{N}$

Exemplo A congruência linear $4x \equiv 5 \pmod 6$ não tem soluções

Se existisse solução x_0 então $6 \mid 4x_0 - 5$ mas $4x_0 - 5$ é um número ímpar logo $6 \nmid 4x_0 - 5$ e $4x \equiv 5 \pmod 6$ não tem solução.

Exemplo A Congruência $3x \equiv 9 \pmod{12}$ admite por exemplo $x_0 = 3$, $x_0 = -1$, $x_1 = -9$, $x_2 = 7$. Note-se que $3 \equiv -9 \pmod{12}$ mas $3 \not\equiv -1 \pmod{12}$. Algumas soluções são congruentes entre si e outras não.

Notamos que:

$$ax \equiv b \pmod n \iff n \mid ax - b$$

$$\iff ax - b = ny \quad (\text{para algum } y \in \mathbb{Z})$$

$$\Leftrightarrow \quad ax - ny = b$$

Assim resolver a congruência linear $ax \equiv b \pmod{n}$ é o mesmo que resolver a equação diofantina $ax - ny = b$.

Teorema: Sejam $a, b \in \mathbb{Z}$, $a \neq 0$, $n \in \mathbb{N}$. A congruência linear tem solução sse $m.d.c(a, n) \mid b$.

Teorema: Sejam $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$, $a \neq 0$ e $d = m.d.c(a, n)$. Se x_0 é solução da congruência $ax \equiv b \pmod{n}$ então

$$x_0, \quad x_0 + \frac{n}{d}, \quad x_0 + \frac{2n}{d}, \quad \ldots, \quad x_0 + \frac{(d-1)}{d} n$$

é a lista completa das soluções de $ax \equiv b \pmod{n}$ que não são congruentes (módulo n) entre si.

Corolário Se $m.d.c(a,n) = 1$ então a congruência linear

$ax \equiv b \pmod{n}$ tem uma e uma só solução módulo n.

Exemplo: Consideramos a congruência linear $4x \equiv 5 \pmod{6}$

Não tem solução pois $m.d.c(4,6) = 2$ e $2 \nmid 5$.

Exemplo: Consideremos a congruência linear $18x \equiv 30 \pmod{42}$.

Temos $m.d.c(18,42) = 2 \times 3 = 6$ e $6 \mid 30$.

18	2	42	2
9	3	21	3
3	3	7	7
1		1	

Então a congruência tem soluções, na verdade tem 6 soluções módulo 42

Uma solução possível é $x_0 = 4$. Logo as 6 soluções

módulo 42 são: $x_0 + \frac{t}{6}\,42 \quad t \in \{0,1,2,\dots,5\}$

$x_0 + t \times 7 \quad t \in \{0,1,2,\dots,5\}$

Temos $4, 4+7 = 11, 4+2\times 7 = 18, 4+3\times 7 = 25, 4+4\times 7 = 32$

e $4+5\times 7 = 39$ são as 6 soluções módulo 42.

Nota: Não é necessário "adivinhar" a solução.
Podemos sempre usar o algoritmo de Euclides

Teorema: Seja $ax \equiv b \pmod n$ uma congruência linear que admite soluções. Então existem $c \in \mathbb{Z}$ e $m \in \mathbb{N}$ tais que x_0 é solução de $ax \equiv b \pmod n$ sse x_0 é solução de $x \equiv c \pmod m$.

Demonst: Sejam x_0 uma solução de $ax \equiv b \pmod{n}$ e $d = m.d.c(a,n)$. Então $d \mid b$ e, por um teorema anterior,

$$\frac{a}{d} x_0 \equiv \frac{b}{d} \left(\mod \frac{n}{d} \right) \qquad (*)$$

(teorema da lei do corte).

Sabemos também que, como $m.d.c\left(\frac{a}{d}, \frac{n}{d}\right) = 1$ então existe x_0^* tal que

$$\frac{a}{d} x_0^* \equiv 1 \left(\mod \frac{n}{d} \right)$$

Multiplicando a congruência $(*)$ por x_0^* temos $\left(\frac{a}{d} x_0^*\right) x_0 \equiv x_0^* \frac{b}{d} \left(\mod \frac{n}{d} \right)$, obtemos

$$x_0 \equiv \frac{b}{d} x^* \pmod{n/d}$$

ou seja, x_0 é solução de $x \equiv c \pmod{m}$ onde

$m = \frac{n}{d}$ e $c = \frac{b}{d} x^*$

Reciprocamente se x_0 é solução de $x \equiv \frac{b}{d} x^* \pmod{\frac{n}{d}}$

então os cálculos anteriores mostram que x_0 é solução

de $ax \equiv b \pmod{n/d}$

Sistemas de congruências lineares

Definição Chama-se sistema de congruências lineares a

um sistema do tipo (S): $\begin{cases} a_1 x \equiv b_1 \pmod{n_1} \\ a_2 x \equiv b_2 \pmod{n_2} \\ \vdots \\ a_k x \equiv b_k \pmod{n_k} \end{cases}$

Uma solução de (S) é qualquer inteiro $x_0 \in \mathbb{Z}$ que verifique todas as congruências que constam de (S).

Exemplo: O sistema de congruências lineares $\begin{cases} x \equiv 1 \pmod 4 \\ x \equiv 3 \pmod 6 \end{cases}$

admite como soluções $x_0 = 3$ e $x_1 = 9$.

Exemplo: O sistema de congruências lineares $\begin{cases} x \equiv 1 \pmod 4 \\ x \equiv 4 \pmod 6 \end{cases}$

não admite soluções inteiras.

Suponhamos, por redução ao absurdo, que x_0 é solução. Então $4 \mid x_0 - 1$ e $6 \mid x_0 - 4$. Logo existem q_1 e $q_2 \in \mathbb{Z}$ tais que $x_0 = 4q_1 + 1$ e $x_0 = 6q_2 + 4$

então $4q_1 + 1 = 6q_2 + 4$ ou seja

$4q_1 - 6q_2 = 3$

ie, (q_1, q_2) é solução da equação diofantina

$4x - 6y = 3$. Ora m.d.c $(4,6) = 2$ mas $2 \nmid 3$

logo a equação $4x - 6y = 3$ não tem solução. □

Teorema (Teorema Chinês dos Restos)

Seja $k \in \mathbb{N} \setminus \{1\}$, $a_1, a_2, \dots, a_k \in \mathbb{Z}$ e $n_1, n_2, \dots, n_k \in \mathbb{N}$

tais que

$$\forall i,j \in \{1, \dots, k\} \quad (i \neq j) \Rightarrow \text{m.d.c}(n_i, n_j) = 1$$

Então o sistema de congruências lineares

$$(S)\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \vdots \\ x \equiv a_k \pmod{n_k} \end{cases}$$

tem uma e uma só solução módulo $n_1 n_2 \cdots n_k$.

Demonst: Ver sebenta