4 - Congruências módulo um inteiro n

Congruências - definição

Definição

Sejam $n \in \mathbb{N}$ *e* $a, b \in \mathbb{Z}$. *Diz-se que* a *e* b *são congruentes módulo* n *se* a *e* b *têm o mesmo resto quando divididos por* n, *e escreve-se:*

$$a \equiv_n b \qquad (ou \quad a \equiv b \ (mod\, n))$$

Nota importante :

$$a \equiv_n b \quad \Longleftrightarrow \quad n | a - b$$

Proposição

A relação $\equiv_n$ *é uma relação de equivalência em* $\mathbb{Z}$, *isto é, dados* $a, b, c \in \mathbb{Z}$:

1. $a \equiv_n a$
2. $a \equiv_n b \quad \Rightarrow \quad b \equiv_n a$
3. $a \equiv_n b \ \wedge \ b \equiv_n c \quad \Rightarrow \quad a \equiv_n c$

Classes de congruência

Para calcularmos o resto da divisão de 171 por 14 podemos deslocar-nos na reta real em direcção à origem, 14 unidades de cada vez, até atingirmos um inteiro positivo inferior a 14.

Todos os valores intermédios obtidos têm o mesmo resto que 171 quando divididos por 14 e portanto são todos congruentes módulo 14.

$$0 \quad \underset{3}{\longleftarrow} \quad 3 \quad \underset{14}{\longleftarrow} \quad 17 \quad \underset{14}{\longleftarrow} \quad \cdots \quad \underset{14}{\longleftarrow} \quad 143 \quad \underset{14}{\longleftarrow} \quad 157 \quad \underset{14}{\longleftarrow} \quad 171$$

$$171 \equiv_{14} 157 \equiv_{14} 143 \equiv_{14} \cdots \equiv_{14} 17 \equiv_{14} 3$$

Classes de congruência

Definição

Dados $n \in \mathbb{N}$ e $a \in \mathbb{Z}$, chama-se classe de congruência de a módulo n ao conjunto de todos os inteiros que têm o mesmo resto que a quando divididos por n, e representa-se por: $[a]_n$.

Nota : Existem n restos possíveis na divisão por n: $0, 1, 2, 3, \cdots, n-1$ e portanto existem n classes de congruência módulo n.

A classe de congruência de 3 módulo 14 é constituida por todos os inteiros que divididos por 14 dão resto 3.

$$[3]_{14} = \{ \cdots, -25, -11, 3, 17, 31, \cdots \}$$

$$[3]_{14} = [-25]_{14} = [-11]_{14} = [17]_{14} = [31]_{14}$$

O conjunto $\mathbb{Z}_n$

Definição

Dado $n \in \mathbb{N}$ o conjunto de todas as classes de congruência módulo n representa-se por $\mathbb{Z}_n$ e diz-se o conjunto quociente de $\mathbb{Z}$ pela relação $\equiv_n$.

$$\mathbb{Z}_n = \{[0]_n, [1]_n, [2]_n, \cdots, [n-1]_n\}$$

Neste conjunto definem-se as operações $+$ e $\times$ da seguinte forma:

$$[a]_n + [b]_n = [a+b]_n \qquad [a]_n \times [b]_n = [a \times b]_n$$

Exemplo :

$$[4]_7 + [5]_7 = [9]_7 = [2]_7$$

$$[4]_7 \times [5]_7 = [20]_7 = [6]_7$$

Sistema completo de resíduos módulo n

Definição

Dado $n \in \mathbb{N}$ chama-se sistema completo de resíduos (ou restos) módulo n a qualquer conjunto de n inteiros que tenha exactamente um representante de cada classe de congruência módulo n .

Exemplo :

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13\}$$

é um sistema completo de resíduos módulo 14

$$\{14, 29, -12, 17, 32, 5, -8, -7, 22, 37, -4, -3, -2, -1\}$$

também é um sistema completo de resíduos módulo 14

Proposição

Dados $n \in \mathbb{N}$ *e* $a, b, c, d \in \mathbb{Z}$*:*

1. $a \equiv_n b \quad \wedge \quad c \equiv_n d \quad \Rightarrow \quad a + c \equiv_n b + d$
2. $a \equiv_n b \quad \wedge \quad c \equiv_n d \quad \Rightarrow \quad ac \equiv_n bd$
3. $a \equiv_n b \quad \Rightarrow \quad a + c \equiv_n b + c$
4. $a \equiv_n b \quad \Rightarrow \quad ac \equiv_n bc$
5. $a \equiv_n b \quad \Rightarrow \quad a^k \equiv_n b^k \qquad \forall\, k \in \mathbb{N}$

Congruências - Exemplo 1

Queremos calcular o resto da divisão de $a \times b$ por 17, onde:

$$a = 132467 \times 17 + 11 \qquad b = 455344 \times 17 + 6$$

Como $a \equiv_{17} 11$ e $b \equiv_{17} 6$

pela propriedade 2

$$a \times b \equiv_{17} 11 \times 6$$

Logo

$$a \times b \equiv_{17} 66 \equiv_{17} 15$$

E portanto o resto da divisão de $a \times b$ por 17 é 15

Congruências - Exemplo 2

Queremos calcular o resto da divisão por 18 de:

$$131 \times 15 + 29 \times 142$$

$131 \equiv_{18} 5 \qquad (131 - 180 = -49 \quad \text{e} \quad -49 + 36 = -13 \equiv_{18} 5)$

$15 \equiv_{18} -3$

$29 \equiv_{18} 11 \equiv_{18} -7$

$142 \equiv_{18} -2 \qquad (142 - 180 = -38 \equiv_{18} -2)$

Logo, pelas propriedades das congruências:

$$131 \times 15 + 29 \times 142 \equiv_{18} 5 \times (-3) + (-7) \times (-2) = -15 + 14 = -1 \equiv_{18} 17$$

E portanto o resto da divisão é 17

Congruências - Exemplo 3

Queremos calcular o resto da divisão de 19^{279} por 17:

$$\text{Como} \quad 19 \equiv_{17} 2 \qquad \text{então} \qquad 19^{279} \equiv_{17} 2^{279}$$

Vamos agora procurar uma potência de base 2 que seja congruente módulo 17, com 1 ou -1.

$$2^4 = 16 \equiv_{17} -1$$

Dividindo o expoente 279 por 4, obtemos:

$$279 = 69 \times 4 + 3$$

e portanto

$$2^{279} = 2^{69\times 4+3} = 2^{69\times 4} \times 2^3 = (2^4)^{69} \times 2^3 \equiv_{17} (-1)^{69} \times 2^3 = -8 \equiv_{17} 9$$

E portanto o resto da divisão é 9

Congruências - Exemplo 4

Queremos calcular o resto da divisão de $135^{43} + 42^{131}$ por 13:

Como $135 \equiv_{13} 5$ e $42 \equiv_{13} 3$ então $135^{43} + 42^{131} \equiv_{13} 5^{43} + 3^{131}$

$$5^2 = 25 \equiv_{13} -1 \quad \text{e} \quad 43 = 21 \times 2 + 1$$

$$3^3 = 27 \equiv_{13} 1 \quad \text{e} \quad 131 = 43 \times 3 + 2$$

$$5^{43} = 5^{21\times 2+1} = (5^2)^{21} \times 5 \equiv_{13} (-1)^{21} \times 5 = -5 \equiv_{13} 8$$

$$3^{131} = 3^{43\times 3+2} = (3^3)^{43} \times 3^2 \equiv_{13} (1)^{43} \times 9 = 9$$

$$135^{43} + 42^{131} \equiv_{13} 5^{43} + 3^{131} \equiv_{13} 8 + 9 = 17 \equiv_{13} 4$$

E portanto o resto da divisão é 4

Critérios de divisibilidade

Dado um inteiro $a = \overline{a_k\, a_{k-1} \cdots a_3\, a_2\, a_1\, a_0}$ com $k+1$ algarismos, isto é:

$$a = a_k \times 10^k + a_{k-1} \times 10^{k-1} + \cdots + a_3 \times 10^3 + a_2 \times 10^2 + a_1 \times 10 + a_0$$

queremos calcular o resto da divisão de a por um inteiro positivo n.

Se $n = 3$ (ou $n = 9$) como $10 \equiv_3 1$, teremos

$$a \equiv_3 a_k \times 1^k + a_{k-1} \times 1^{k-1} + \cdots + a_3 \times 1^3 + a_2 \times 1^2 + a_1 \times 1 + a_0$$

e portanto

$$a \equiv_3 a_k + a_{k-1} + \cdots + a_3 + a_2 + a_1 + a_0$$

Critérios de divisibilidade

Se $n = 4$ como $10^2 \equiv_4 0$, teremos

$$a \equiv_4 a_1 \times 10 + a_0 = \overline{a_1\, a_0}$$

Se $n = 8$ como $10^3 \equiv_8 0$, teremos

$$a \equiv_8 a_2 \times 10^2 + a_1 \times 10 + a_0 = \overline{a_2\, a_1\, a_0}$$

Exemplo : $67389645127 \equiv_8 127 \equiv_8 7$

$$67389645127 \equiv_3 6+7+3+8+9+6+4+5+1+2+7 = 58 \equiv_3 -2 \equiv_3 1$$

Critérios de divisibilidade

Se $n = 11$ como $10 \equiv_{11} -1$, teremos

$$a \equiv_{11} a_k \times (-1)^k + a_{k-1} \times (-1)^{k-1} + \cdots + a_3 \times (-1)^3 + a_2 \times 1^2 + a_1 \times (-1) + a_0$$

e portanto

$$a \equiv_{11} a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^k a_k$$

Exemplo : $645127 \equiv_{11} 7 - 2 + 1 - 5 + 4 - 6 = -1 \equiv_{11} 10$

Critérios de divisibilidade

Proposição

Seja $a = \overline{a_k\, a_{k-1} \cdots a_3\, a_2\, a_1\, a_0}$ *um inteiro com* $k+1$ *algarismos. Então*

- $a \equiv_2 a_0$
- $a \equiv_4 \overline{a_1\, a_0}$
- $a \equiv_8 \overline{a_2\, a_1\, a_0}$
- $a \equiv_5 a_0$
- $a \equiv_3 a_k + a_{k-1} + \cdots + a_3 + a_2 + a_1 + a_0$
- $a \equiv_9 a_k + a_{k-1} + \cdots + a_3 + a_2 + a_1 + a_0$
- $a \equiv_{11} a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^k a_k$