A afirmação seguinte de Karl Gauss está na origem do conceito fundamental desta secção:
"se um inteiro positivo m mede a diferença entre dois números a e b, então a e b dizem-se congruentes em relação a n. Caso contrário, a e b dizem-se incongruentes."

Definição

Sejam $a, b \in \mathbb{Z}$ e $m \in \mathbb{N}$. Diz-se que a é congruente com b módulo m se $m \mid a - b$.

Se a é congruente com b módulo m escreve-se

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

Caso contrário, diz-se que a e b são incongruentes módulo m e escreve-se $a \not\equiv b \pmod{m}$.

Nota:

Usando o algoritmo da divisão, podemos escrever:

$$\left.\begin{array}{l} a = m\,q_a + r_a \\ b = m\,q_b + r_b \end{array}\right\} \quad \rightarrow \quad a - b = m(q_a - q_b) + (r_a - r_b),$$

em que o valor absoluto de $r_a - r_b$ é inferior a m.

Então, $m \mid a - b$ sse $m \mid r_a - r_b$ e, consequentemente,

$$a \equiv b (\mathrm{mod}\, m) \Leftrightarrow r_a = r_b.$$

Notação:

- $a \bmod m$ representa um número natural que é o resto da divisão de a por m (em cima representado por r_a).
- $a \equiv b (\mathrm{mod}\, m)$ é uma proposição, que pode ser verdadeira ou falsa, e que é equivalente a $a \bmod m = b \bmod m$.

Exercício

Que dia da semana será daqui por 1000 dias?

Proposição

Seja $m \in \mathbb{N}$. A relação de congruente módulo m é uma relação de equivalência.

Exercícios

1. Determine os valores de x tais que:
   1. $x \equiv 0 \pmod{2}$ (isto é, calcule $[0]_2$ a classe de equivalência de 0);
   2. $x \equiv 1 \pmod{2}$ (isto é, calcule $[1]_2$ a classe de equivalência de 1).
2. Determine os valores de x tais que:
   1. $x \equiv 0 \pmod{3}$ (isto é, calcule $[0]_3$ a classe de equivalência de 0);
   2. $x \equiv 1 \pmod{3}$ (isto é, calcule $[1]_3$ a classe de equivalência de 1);
   3. $x \equiv 2 \pmod{3}$ (isto é, calcule $[2]_3$ a classe de equivalência de 2).
3. Quais os valores de x tais que $x \equiv 1 \pmod{1}$?

Faria sentido falar de 'congruente módulo 0'? E de 'congruente módulo -3'?

Proposição ($\equiv \pmod{m}$ é 'bem comportada')

Sejam $a, b, c, d \in \mathbb{Z}$ e $m \in \mathbb{N}$. Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então

- $a + c \equiv b + d \pmod{m}$;
- $ac \equiv bd \pmod{m}$.

PROVA

Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $m \mid (a-b)$ e $m \mid (c-d)$. Consequentemente, $m \mid (a-b)x + (c-d)y$ para quaisquer $x, y \in \mathbb{Z}$.

- Se $x = y = 1$, resulta que $m \mid (a-b) + (c-d)$, ou seja, que $m \mid (a+c) - (b+d)$, o que é equivalente a ter $a + c \equiv b + d \pmod{m}$;
- Se $x = c$ e $y = b$, resulta que $m \mid (a-b)c + (c-d)b$, ou seja, que $m \mid (ac - bd)$, o que é equivalente a ter $ac \equiv bd \pmod{m}$.

Corolário

Sejam $a, b, c \in \mathbb{Z}$ e $m, n \in \mathbb{N}$. Se $a \equiv b \pmod{m}$, então

- $a + c \equiv b + c \pmod{m}$;
- $ac \equiv bc \pmod{m}$;
- $a^n \equiv b^n \pmod{m}$.

Definição

Sistema completo de resíduos módulo m é um conjunto S de inteiros tal que cada inteiro é congruente com exatamente um elemento de S, ou seja, é um conjunto S de inteiros que contém exatamente um elemento de cada classe de equivalência da relação $\equiv \pmod{m}$.

EXEMPLOS 2

- $S = \{0, 1, \ldots, m-1\}$ (sistema standard de restos).
- $S = \{-\frac{m}{2} + 1, \ldots, -1, 0, 1, \ldots, \frac{m}{2}\}$ se m é par.
- $S = \{-\frac{m-1}{2}, \ldots, -1, 0, 1, \ldots, \frac{m-1}{2}\}$ se m é ímpar.

O conjunto quociente $\mathbb{Z}/_{\equiv \pmod{m}}$, que usualmente se representa simplesmente por $\mathbb{Z}_m$, é constituído pelas classes de equivalência da relação $\equiv \pmod{m}$, isto é,

$$\mathbb{Z}_m = \mathbb{Z}/_{\equiv \pmod{m}} = \{[0]_m, \dots, [m-1]_m\}$$

As propriedades da relação $\equiv \pmod{m}$ permitem afirmar que a relação é 'bem comportada' relativamente à operações de adição e multiplicação de inteiros e definir duas operações em $\mathbb{Z}_m$:

1. $[a]_m +_m [b]_m = [a+b]_m$;
2. $[a]_m \cdot_m [b]_m = [ab]_m$.

para quaisquer $a, b \in \mathbb{Z}$. (Os símbolos $+_m$ e $\cdot_m$ representam-se, normalmente, apenas por $+$ e $\cdot$)

EXEMPLO 3

- $[3]_7 + [2]_7 = [5]_7$
- $[5]_7 + [6]_7 = [11]_7$
- $[5]_7 + [6]_7 = [4]_7$
- $[5]_7 + [2]_7 = [0]_7$
- $[3]_7 \cdot [2]_7 = [6]_7$
- $[5]_{11} \cdot [5]_{11} = [3]_{11}$
- $[10]_{20} \cdot [6]_{20} = [0]_{20}$
- $[15]_{20} \cdot [8]_{20} = [0]_{20}$

$(\mathbb{Z}_m, +_m, \cdot_m)$ é um anel comutativo com identidade.

Lei do anulamento do produto

Proposição

Se $a,\ b \in \mathbb{Z}$, $m \in \mathbb{N}$ e $\mathrm{m.d.c.}(a, m) = 1$ $^{(*)}$, então

$$ab \equiv 0 \pmod{m} \quad \text{se e só se} \quad b \equiv 0 \pmod{m}\ .$$

PROVA

$$ab \equiv 0 \pmod{m} \ \Leftrightarrow\ m \mid ab \ \Leftrightarrow_{(*)}\ m \mid b \ \Leftrightarrow\ b \equiv 0 \pmod{m}.$$

A proposição acima é equivalente a afirmar que, se $\mathrm{m.d.c.}(a, m) = 1$,

$$[a]_m \cdot [b]_m = [0]_m \Leftrightarrow [b]_m = [0]_m$$

Lei do corte

EXEMPLO 1 $2 \equiv 12 \pmod{10}$ mas $1 \not\equiv 6 \pmod{10}$. No entanto, $1 \equiv 6 \pmod{5}$.

Proposição

Se $a,\ b \in \mathbb{Z}$ e $c,\ m \in \mathbb{N}$, então

$$ac \equiv bc \pmod{mc} \quad \text{se e só se} \quad a \equiv b \pmod{m}.$$

PROVA

$$\begin{aligned} ac \equiv bc \pmod{mc} \quad &\Leftrightarrow mc \mid (ac - bc) \Leftrightarrow \exists_{k\in\mathbb{Z}} mck = (a-b)c \\ &\Leftrightarrow \exists_{k\in\mathbb{Z}} mk = (a-b) \Leftrightarrow m \mid (a-b) \Leftrightarrow \quad a \equiv b \pmod{m}. \end{aligned}$$

Proposição

Se $a,\ b,\ c \in \mathbb{Z}$, $m \in \mathbb{N}$ e $\text{m.d.c.}(m, c) = 1$ $^{(*)}$, então

$$ac \equiv bc \pmod{m} \quad \text{se e só se} \quad a \equiv b \pmod{m}.$$

PROVA

$$ac \equiv bc \pmod{m} \Leftrightarrow m \mid ac - bc \Leftrightarrow m \mid (a-b)c \Leftrightarrow_{(*)} m \mid (a-b) \Leftrightarrow a \equiv b \pmod{m}.$$

Lei do corte

As proposições anteriores podem escrever-se, respetivamente, nas formas seguintes:

Se $a, b \in \mathbb{Z}$ e $c, m \in \mathbb{N}$, então

$$[ac]_{mc} = [bc]_{mc} \iff [a]_m = [b]_m$$

Se $a, b, c \in \mathbb{Z}$, $m \in \mathbb{N}$ e $\mathrm{m.d.c.}(m, c) = 1$, então

$$[ac]_m = [bc]_m \iff [a]_m = [b]_m,$$

ou equivalentemente,

$$[a]_m \cdot [c]_m = [b]_m \cdot [c]_m \iff [a]_m = [b]_m.$$

Definição

Sejam a, a' e m inteiros. Diz-se que a' é um inverso de a módulo m se

$$a \cdot a' \equiv 1 \pmod{m}$$

Equivalentemente, pode-se dizer que a' é um inverso de a módulo m se

$$[a]_m \cdot [a']_m = [1]_m$$

Proposição

Um inteiro a é invertível módulo m se e só se $\mathrm{m.d.c.}(a, m) = 1$.

PROVA

$$\begin{aligned}
a \text{ é invertível módulo } m \; &\Leftrightarrow \exists_{a' \in \mathbb{Z}}\; a \cdot a' \equiv 1 \pmod{m} \\
&\Leftrightarrow \exists_{a' \in \mathbb{Z}}\; m \mid aa' - 1 \\
&\Leftrightarrow \exists_{a', y \in \mathbb{Z}}\; my = aa' - 1 \\
&\Leftrightarrow \exists_{a', y \in \mathbb{Z}}\; aa' - my = 1 \\
&\Leftrightarrow \mathrm{m.d.c.}(a, m) = 1
\end{aligned}$$

$$10 \equiv \begin{cases} 0 & \pmod 2 \\ 0 & \pmod 5 \\ 1 & \pmod 3 \\ 1 & \pmod 9 \\ -1 & \pmod{11} \end{cases}$$

pelo que para $i \geq 1$, $\quad 10^i \equiv \begin{cases} 0 & \pmod 2 & \\ 0 & \pmod 4 & \text{se } i \geq 2 \\ 0 & \pmod 8 & \text{se } i \geq 3 \\ 0 & \pmod 5 & \\ 1 & \pmod 3 & \\ 1 & \pmod 9 & \\ 1 & \pmod{11} & \text{se } i \text{ é par} \\ -1 & \pmod{11} & \text{se } i \text{ é ímpar} \end{cases}$

n é divisível por m se e só se $n \equiv 0 \pmod{m}$.

Critérios de divisibilidade por 2,3,4,5,8,9,11

$$n = a_k \times 10^k + \cdots + a_1 \times 10 + a_0$$

$$n \equiv \begin{cases} a_0 & \pmod{2} \\ 2a_1 + a_0 & \pmod{4} \\ 4a_2 + 2a_1 + a_0 & \pmod{8} \\ a_0 & \pmod{5} \\ a_k + \cdots + a_0 & \pmod{3} \\ a_k + \cdots + a_0 & \pmod{9} \\ (-1)^k a_k + \cdots + a_2 - a_1 + a_0 & \pmod{11} \end{cases}$$