UFRJ - Universidade Federal do Rio de Janeiro

Rio de Janeiro, 06 de Abril de 2017

5ª PASSADA:

$a \equiv b \pmod{n}$

(a congruente a b módulo n).

$\Updownarrow$

$a - b = n \cdot t \quad (t \in \mathbb{Z})$

$\Updownarrow$

$a - b$ é multiplo de n

Dado um conjunto X e uma relação $\sim$ neste conjunto, $\sim$ é uma relação de equivalência se e somente se satisfaz às seguintes propriedades:

(1) REFLEXIVIDADE: para todo $a \in X$, $a \sim a$

(2) SIMETRIA: para todo $a, b \in X$, se $a \sim b$, então $b \sim a$

(3) TRANSITIVIDADE: para todo $a, b, c \in X$, se $a \sim b$ e $b \sim c$, então $a \sim c$.

Para um n fixado, a relação de congruência módulo n é uma relação de equivalência

---

Seja X um conjunto e $\sim$ uma relação de equivalência. Se $a \in X$, definimos o conjunto $\bar{a}$ da seguinte forma:

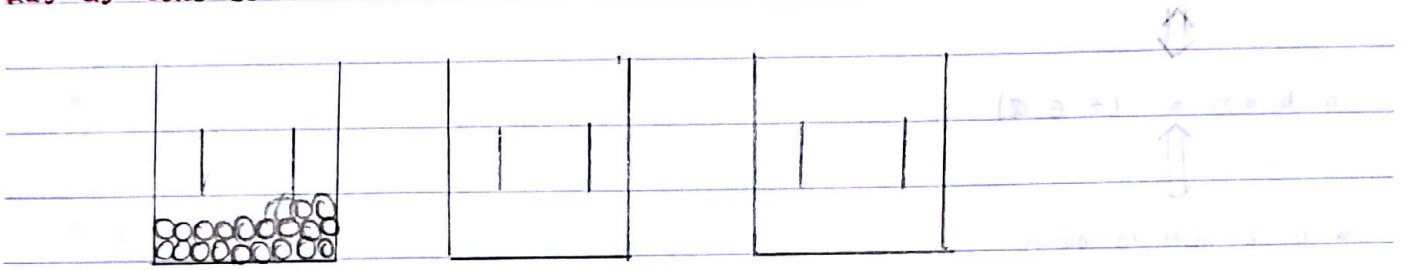
$$\bar{a} = \{b \in X : b \sim a\}$$

$\bar{a}$ = todos os elementos de X que são equivalentes a "a" pela relação de equivalência $\sim$. O conjunto $\bar{a}$ é conhecido como "classe de equivalência" de a pela relação $\sim$.

EXEMPLO: X = conjunto de bolas

$\sim$ = bolas da mesma cor

CLASSES DE EQUIVALÊNCIA: = urnas com a marcação de cor onde serão agrupadas todas as bolas de uma mesma cor.



A ideia de classes de equivalência é que um elemento qualquer da classe pode ser usado para representar toda a classe.

RESULTADO: Se $a \in X$ e $b \in \bar{a}$, então $\bar{b} = \bar{a}$.

$$\bar{a} = \{c \in X : c \sim a\}$$

Se $b \in \bar{a}$, então $b \sim a$. Quero mostrar que $\bar{a} = \bar{b}$. Vou mostrar que se $z \in \bar{a}$, então $z \in \bar{b}$ e se $z \in \bar{b}$, então $z \in \bar{a}$.

Se $z \in \bar{a}$, $z \sim a$.

$z \sim a$

$b \sim a \Rightarrow a \sim b$ } $z \sim b \Rightarrow z \in \bar{b}$

SIMETRIA → TRANSITIVIDADE

Se $z \in \bar{b}$, $z \sim b$

$$\left.\begin{array}{l} z - b \\ b \sim a \end{array}\right\} z \sim a \Rightarrow z \in \bar{a}$$

↳ TRANSITIVIDADE

Se $a \sim b$, então $\bar{a} = \bar{b}$.

RESULTADO:

$$X = \bigcup_{a \in X} \bar{a}$$

X é igual à união de todos as classes de equivalência dos seus elementos.

DEFINIÇÃO: O conjunto de todas as classes de equivalência dos elementos de x é chamado de conjunto quociente de x pela relação $\sim$ e denotado por $X/\sim$.

Vamos considerar o conjunto dos inteiros $\mathbb{Z}$ e um módulo n. Seja $a \in \mathbb{Z}$, a classe de equivalência $\bar{a}$ pela relação de congruência módulo n é:

$$\bar{a} = \{b \in \mathbb{Z} : b \equiv a \pmod{n}\}$$

$$\bar{a} = \{b \in \mathbb{Z} : b \equiv a \pmod{n}\}$$

$$\Updownarrow$$

$$\bar{a} = \{b \in \mathbb{Z} : b - a \text{ é multiplo de } n\}$$

$$\Updownarrow$$

$$\bar{a} = \{b \in \mathbb{Z} : b - a = n \cdot t\}$$

$$\Updownarrow$$

$$\bar{a} = \{b \in \mathbb{Z} : b = a + n \cdot t\}$$

EXEMPLO: $n=5$

$\bar{2} = \{\dots, -8, -3, 2, 7, 12, \dots\}$

↳ OS INTEIROS QUE CAEM SOBRE A CASA "2" DO "RELÓGIO" DE 5 CASAS.

O conjunto quociente de $\mathbb{Z}$ pela relação de congruência módulo n, para um n fixado, é conhecido como conjunto dos inteiros módulo n e denotado por $\mathbb{Z}_n$

↳ CONJUNTO DAS CASAS DO "RELÓGIO" DE N CASAS.

- Quais são os elementos de $\mathbb{Z}_n$?

Sejam $a, b \in \mathbb{Z}$.

$b \in \bar{a}$

$\Updownarrow$

$b = a + n \cdot t$, para algum $t \in \mathbb{Z}$

Ao pegar um b qualquer em $\mathbb{Z}$, quero determinar a qual classe de equivalência ele pertence.

Dividindo b por n, obtenho:

$b = n \cdot q + r$, $0 \leq r < n$

↳ resto

↳ quociente

$\rightarrow b \in \bar{r}$

CONCLUSÃO: Qualquer inteiro b pertence a uma classe de equivalência $\bar{r}$ onde $0 \leq r < n$.

$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$

↳ n elementos

- ARITMÉTICA MODULAR:

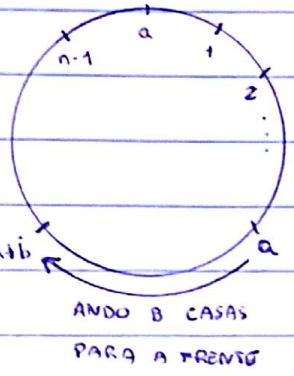
↳ OPERAÇÕES ARITMÉTICAS (SOMA, DIFERENÇA, PRODUTO, DIVISÃO, POTENCIAÇÃO) REALIZADAS COM ELEMENTOS DE $\mathbb{Z}_n$ AO INVÉS DE $\mathbb{Z}$

- SOMA MODULAR:

Fixo o módulo n.

$a, b \in \mathbb{Z}_n$

$\bar{a} + \bar{b} = ?$



ANDO B CASAS PARA A FRENTE

Preciso verificar que se $\bar{a} = \bar{a'}$ e $\bar{b} = \bar{b'}$, então:

$\bar{a} + \bar{b} = \bar{a'} + \bar{b'}$.

Se $\bar{a} = \bar{a'}$, então $a' = a + n \cdot t$

Se $\bar{b} = \bar{b'}$, então $b' = b + n \cdot t'$ SOMAR

$(a' + b') = (a+b) + n(t+t')$

POSSO CONCLUIR QUE:

$(a' + b') = (a+b) \pmod n$

ESTÃO NA MESMA CLASSE DE EQUIVALÊNCIA — CAEM NA MESMA POSIÇÃO DO "RELÓGIO".

- MÉTODO PARA SOMA MODULAR: $\bar{a} + \bar{b} = \overline{a+b}$

EXEMPLOS: 1) $n = 7$

$\bar{2} + \overline{29} = \overline{2+29} = \overline{31} = \bar{3}$

$31 = 7 \cdot 4 + 3$

↳ RESTO

↳ QUOCIENTE

$\bar{2} + \overline{29} = \bar{2} + \bar{1} = \overline{2+1} = \bar{3}$

$29 = 7 \cdot 4 + 1$

↳ RESTO

2) $n = 12$

$\bar{9} + \bar{10} = \overline{9+10} = \overline{19} = \bar{7}$

$19 = 12 \cdot 1 + 7$

↳ RESTO

↳ QUOCIENTE

$\bar{9} + \overline{46} = \overline{55} = \bar{7}$

$55 = 12 \cdot 4 + 7$

↳ RESTO

↳ QUOCIENTE

DEFINIÇÃO: O valor entre 0 e n ($0 \leq r < n$) que pode ser usado para representar uma classe de equivalência é conhecido como forma reduzida módulo n.

EXEMPLOS:

1) A forma reduzida de 31 módulo 7 é 3.

2) A forma reduzida de 19 módulo 12 é 7.

/ /

3) A forma reduzida de 55 módulo 12 é 7.

CONCLUSÃO: A forma reduzida de a módulo n é igual ao resto da divisão de a por n