Anéis de Inteiros Módulo n

Prof. Dr. Vinícius Wasques

Universidade Estadual Paulista “Júlio de Mesquita Filho” - Campus Rio Claro

22 de junho de 2020

Anéis de inteiros módulo n

Construiremos o anel de inteiros módulo n através do quociente de $\mathbb{Z}$ pela relação $\equiv \pmod{n}$, ao qual denotamos por:

$$\mathbb{Z}_n = \mathbb{Z}/\sim$$

em que $\sim$ é a relação congruência módulo n.

Lembrando que os elementos de $\mathbb{Z}_n$ são classes de equivalência denotados por:

$$\bar{x} = \{y \in \mathbb{Z} | x \sim y\}$$

Exemplo:

O anel $\mathbb{Z}_2$ é definido pela congruência módulo 2 e possui dois elementos:

$$\bar{0} = \{\dots, -4, -2, 0, 2, 4, \dots\}$$

e

$$\bar{1} = \{\dots, -3, -1, 1, 3, \dots\}$$

Sendo $\bar{0}$ e $\bar{1}$ conhecidos como conjunto dos números pares e ímpares, respectivamente.

A definição de $\bar{x}$ como um subconjunto de $\mathbb{Z}$ não será o foco desse curso.

Será utilizado apenas como uma maneira de formalizar o fato de que estamos "identificando" todos os inteiros que deixam o mesmo resto na divisão por n.

Assim, o importante é termos claro que

$$\begin{aligned} \bar{a} \equiv \bar{b} \quad &\Leftrightarrow \quad a \equiv \ b \,(mod \ n) \\ &\Leftrightarrow \quad \text{a e b deixam o mesmo resto na divisão por n} \end{aligned}$$

Se$n > 0$, a divisão euclidiana diz que todo inteiro a é côngruo a um único inteiro b com $0 \leq a0 < n$.

Escrevemos então:

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

Para esse quociente, definimos as operações:

(Soma) $\bar{a} + \bar{b} = \overline{a+b}$

(Diferença) $\bar{a} - \bar{b} = \overline{a-b}$

(Multiplicação) $\bar{a} \cdot \bar{b} = \overline{a \cdot b}$

Exemplo:

Considere $\mathbb{Z}_6$, assim:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

e

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Inverso multiplicativo

A próxima proposição revela quando existe o “inverso multiplicativo” de a módulo n.

Proposição. Sejam $a, n \in \mathbb{Z}$, $n > 0$. Então existe $b \in \mathbb{Z}$ com

$$ab \equiv \ 1 \ (mod \ \ n) \text{ se, e somente se, } mdc(a, n) = 1$$

Demonstração

Temos que $ab \equiv\ 1\ (mod\ n)$ admite solução na variável b se, e somente se, existem $b, k \in \mathbb{Z}$ tais que

$$ab - 1 = nk \Leftrightarrow ab - nk = 1.$$

Pelo Corolário obtido através do teorema de Bachet-Bézout, isto acontece se, e somente se, $mdc(a, n) = 1$.

Dizemos portanto que a é invertível módulo n quando $mdc(a, n) = 1$ e chamamos b com $ab \equiv 1 \ (mod\ n)$ de inverso multiplicativo de a módulo n.

Denotaremos o conjunto formado por todos os elementos invertíveis de $\mathbb{Z}_n$, por

$$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid mdc(a, n) = 1\}.$$

Exemplo:

Considere $\mathbb{Z}_{15}^{*}$. A tabela de multiplicação entre seus elementos é dada por:

$\cdot$	$\overline{1}$	$\overline{2}$	$\overline{4}$	$\overline{7}$	$\overline{8}$	$\overline{11}$	$\overline{13}$	$\overline{14}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{4}$	$\overline{7}$	$\overline{8}$	$\overline{11}$	$\overline{13}$	$\overline{14}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{8}$	$\overline{14}$	$\overline{1}$	$\overline{7}$	$\overline{11}$	$\overline{13}$
$\overline{4}$	$\overline{4}$	$\overline{8}$	$\overline{1}$	$\overline{13}$	$\overline{2}$	$\overline{14}$	$\overline{7}$	$\overline{11}$
$\overline{7}$	$\overline{7}$	$\overline{14}$	$\overline{13}$	$\overline{4}$	$\overline{11}$	$\overline{2}$	$\overline{1}$	$\overline{8}$
$\overline{8}$	$\overline{8}$	$\overline{1}$	$\overline{2}$	$\overline{11}$	$\overline{4}$	$\overline{13}$	$\overline{14}$	$\overline{7}$
$\overline{11}$	$\overline{11}$	$\overline{7}$	$\overline{14}$	$\overline{2}$	$\overline{13}$	$\overline{1}$	$\overline{8}$	$\overline{4}$
$\overline{13}$	$\overline{13}$	$\overline{11}$	$\overline{7}$	$\overline{1}$	$\overline{14}$	$\overline{8}$	$\overline{4}$	$\overline{2}$
$\overline{14}$	$\overline{14}$	$\overline{13}$	$\overline{11}$	$\overline{8}$	$\overline{7}$	$\overline{4}$	$\overline{2}$	$\overline{1}$

Anel dos Inteiros Módulo n

O conjunto

$$(\mathbb{Z}_n, +, \cdot)$$

possui uma estrutura de anel.

Anel dos Inteiros Módulo n

O conjunto

$$(\mathbb{Z}_n, +, \cdot)$$

possui uma estrutura de anel.

Mostre esse fato.

Referências

MARTINEZ, F.E.B; MOREIRA, C.G.T; SALDANHA, N.,T.; TENGAN, E. Teoria dos Números. Um passeio com Primos e outros Números Familiares pelo Mundo Inteiro. IMPA, 2013.

GRAHAM, R. L., KNUTH, D. E., PATASHNIK, O Matemática Concreta. LTC, São Paulo, 1995

NIVEN, I. E.; ZUCKERMAN, N.S. An Introduction to the Theory of Numbers, NY, John Wiley & Sons, 1991.

Contato

Prof. Dr. Vinícius Wasques

email: viniciuswasques@gmail.com

Departamento de Matemática

site: `https://viniciuswasques.github.io/home/`