I ENCONTRO DE PÓS-GRADUANDOS EM MATEMÁTICA NA UFSC

UNIVERSIDADE FEDERAL DE SANTA CATARINA

ELEMENTOS PRIMOS E ELEMENTOS IRREDUTÍVEIS DO ANEL $\mathbb{Z}_n$

ALINE KOWALSKI[1], PROF. FELIPE VIEIRA[2]

Universidade Federal de Santa Catarina - campus Blumenau, SC, Brasil

alinee.kowalski@gmail.com[1], f.vieira@ufsc.br[2]

Introdução

Este trabalho é a síntese do trabalho de conclusão de curso da autora, o qual se trata da demonstração completa do artigo [1]. Demonstraremos a caracterização dos conjuntos de elementos primos e de elementos irredutíveis do anel $\mathbb{Z}_n$, com n arbitrário. Além disso, demonstraremos uma forma de realizar a contagem dos elementos destes conjuntos.

Fundamentação Teórica

Seguindo uma abordagem qualitativa para a compreensão da teoria envolvida, usou-se o procedimento metodológico bibliográfico, em que as principais referencias utilizadas foram [1], [2] e [3]. A primeira referência foi a base do trabalho, a segunda foi utilizada para o entendimento de anéis e a terceira foi utilizada para o entendimento e demonstração de propriedades de divisibilidade e máximo divisor comum (mdc).

Desenvolvimento

Definição 1. *Um elemento $\overline{0} \neq \overline{p} \in \mathbb{Z}_n$ é primo se $\overline{p} \mid \overline{a}\cdot\overline{b}$, então $\overline{p} \mid \overline{a}$ ou $\overline{p} \mid \overline{b}$, $\forall\, \overline{a}, \overline{b} \in \mathbb{Z}_n$.*

Lema 1. *Sejam $\overline{a}, \overline{b} \in \mathbb{Z}_n$. Então, $\overline{a} \mid \overline{b}$ se, e somente se, $\mathrm{mdc}(a,n) \mid \mathrm{mdc}(b,n)$.*

Demonstração. A ideia é demonstrar que

$$\overline{a} \mid \overline{b} \text{ em } \mathbb{Z}_n \overset{1}{\iff} \mathrm{mdc}(a,n) \mid b \overset{2}{\iff} \mathrm{mdc}(a,n) \mid \mathrm{mdc}(b,n).$$

□

Teorema 2. *Dado $n \in \mathbb{Z}$, o conjunto de elementos primos de $\mathbb{Z}_n$ é descrito por*

$$\left\{\overline{a} \in \mathbb{Z}_n : \exists\, p \in \pi_n, p < n, \mathrm{mdc}(a,n) = p\right\},$$

em que π_n é o conjunto de números primos que dividem n.

Demonstração. A ideia é separar esta demonstração em três casos:

1. Existem p, q primos distintos tais que $pq \mid \mathrm{mdc}(a,n)$;
2. Existem p primo e $k \geq 2 \in \mathbb{N}$ tais que $\mathrm{mdc}(a,n) = p^k$;
3. Existe p primo tal que $\mathrm{mdc}(a,n) = p$.

□

Definição 2. *Um elemento $\overline{0} \neq \overline{a} \in \mathbb{Z}_n$ é irredutível, se $\overline{a}$ não for inversível, e sempre que existirem $\overline{x}, \overline{y} \in \mathbb{Z}_n$ tais que $\overline{a} = \overline{x} \cdot \overline{y}$, então, $\overline{x}$ ou $\overline{y}$ será inversível.*

Proposição 3. *Seja $\overline{a} \in \mathbb{Z}_n$. Assim, $\overline{a}$ é inversível se, e somente se, $\mathrm{mdc}(a,n) = 1$.*

Teorema 4. *Dado $n \in \mathbb{Z}$, o conjunto de elementos irredutíveis de $\mathbb{Z}_n$ é descrito por*

$$\left\{\overline{a} \in \mathbb{Z}_n : \exists\, p \in \pi_n, p^2 \mid n, \mathrm{mdc}(a,n) = p\right\}$$

em que π_n é o conjunto de números primos que dividem n.

Demonstração. A ideia é separar esta demonstração em três casos:

1. Existem p, q primos não necessariamente distintos tais que $pq \mid \mathrm{mdc}(a,n)$;
2. Existe p primo tal que $p = \mathrm{mdc}(a,n)$ e $p^2 \nmid n$;
3. Existe p primo tal que $p = \mathrm{mdc}(a,n)$ e $p^2 \mid n$.

□

Teorema 5. *Seja $n = pm \in \mathbb{N}$, $p \in \pi_n$ e $A_p = \{\overline{a} \in \mathbb{Z}_n : \mathrm{mdc}(a,n) = p\}$. Então, a função $f : A_p \to U(\mathbb{Z}_m)$ é definida por $\overline{a} \mapsto f(\overline{a}) = \dfrac{\overline{\overline{a}}}{p}$ é bijetora. Em que $U(\mathbb{Z}_m) = \{\overline{a} \in \mathbb{Z}_m : \mathrm{mdc}(a,m) = 1\}$ e $\dfrac{\overline{\overline{a}}}{p} \in U(\mathbb{Z}_m)$.*

Corolário 6. *Em $\mathbb{Z}_n$, a quantidade de elementos primos é dado por $\displaystyle\sum_{\substack{p \in \pi_n \\ p<n}} \varphi\left(\frac{n}{p}\right)$ e a quantidade de elementos irredutíveis é dado por $\displaystyle\sum_{\substack{p \in \pi_n \\ p^2 \mid n}} \varphi\left(\frac{n}{p}\right)$, em que φ é função de Euler.*

Resultados

Seja $\mathbb{Z}_{45} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, \overline{10}, \overline{11}, \overline{12}, \overline{13}, \overline{14}, \overline{15}, \overline{16}, \overline{17}, \overline{18}, \overline{19}, \overline{20}, \overline{21}, \overline{22}, \overline{23}, \overline{24}, \overline{25}, \overline{26}, \overline{27}, \overline{28}, \overline{29}, \overline{30}, \overline{31}, \overline{32}, \overline{33}, \overline{34}, \overline{35}, \overline{36}, \overline{37}, \overline{38}, \overline{39}, \overline{40}, \overline{41}, \overline{42}, \overline{43}, \overline{44}\}$. Note que $\pi_{45} = \{3, 5\}$.

Exemplo 1. *Utilizando o Teorema 2, perceba que os elementos primos de $\mathbb{Z}_{45}$ são:*

$$\{\overline{3}, \overline{5}, \overline{6}, \overline{10}, \overline{12}, \overline{20}, \overline{21}, \overline{24}, \overline{25}, \overline{33}, \overline{35}, \overline{39}, \overline{40}, \overline{42}\},$$

pois o mdc entre os representantes das classes de equivalência de $\mathbb{Z}_{45}$ e 45 resultam nos elementos de π_{45}.

Exemplo 2. *Utilizando o Teorema 4, note que os elementos irredutíveis de $\mathbb{Z}_{45}$ são:*

$$\{\overline{3}, \overline{6}, \overline{12}, \overline{21}, \overline{24}, \overline{33}, \overline{39}, \overline{42}\},$$

pois o mdc entre os representantes das classes de equivalência de $\mathbb{Z}_{45}$ e 45 resultam nos elementos de π_{45} que elevados ao quadrado ainda dividem 45.

Exemplo 3. *Pelo Corolário 6, que em $\mathbb{Z}_{45}$ o número de elementos:*

1. primos é dado por

$$\sum_{\substack{p \in \pi_{45} \\ p<45}} \varphi\left(\frac{45}{p}\right) = \varphi\left(\frac{45}{3}\right) + \varphi\left(\frac{45}{5}\right) = \varphi(15) + \varphi(9) = 8 + 6 = 14,$$

2. irredutíveis é dado por

$$\sum_{\substack{p \in \pi_{45} \\ p^2 \mid 45}} \varphi\left(\frac{45}{p}\right) = \varphi\left(\frac{45}{3}\right) = \varphi(15) = 8.$$

Perceba que no segundo caso, como $5^2 = 25$ e $25 \nmid 45$, então são irredutíveis apenas elementos de $\mathbb{Z}_{45}$ cujo mdc entre os representantes das classes de equivalência de $\mathbb{Z}_{45}$ e 45 resultam em 3, pois $3^2 = 9 \mid 45$.

Exemplo 4. *Seja $\mathbb{Z}_{13} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, \overline{10}, \overline{11}, \overline{12}\}$. Utilizando os Teoremas 2 e 4, note que não temos nenhum elemento irredutível, pois o MDC entre os representantes dos elementos de $\mathbb{Z}_{13}$ e 13 não resulta em um número primo, ou seja, não há primos e nem irredutíveis em $\mathbb{Z}_{13}$.*

Teorema 7. *Se p é primo em $\mathbb{N}$, então $\mathbb{Z}_p$ não possui elementos primos e nem elementos irredutíveis.*

Conclusões

Neste trabalho foi possível revisar conceitos da teoria de anéis e principalmente da teoria de números que fizeram parte da minha formação acadêmica. O objetivo deste trabalho era compreender por completo o artigo científico que o originou, com o intuito de entender quais são os elementos primos e os elementos irredutíveis de um anel de inteiros módulo n, além de demonstrar o teorema que aponta como descobrir a cardinalidade destes dois conjuntos. Além disso, foi identificado um erro na demonstração de um dos teoremas do artigo, que não o invalida, e portanto submeteremos uma errata com a demonstração correta.

Referências

[1] M. H. Jafari, A. R. Madadi. Prime and irreducible elements of the ring of integers modulo n, Cambridge: *The Mathematical Gazette*, volume 1, n. 536, p. 283-287, 2012.

[2] A. Gonçalves. *Introdução à Álgebra*, 2ª ed, Rio de Janeiro: IMPA, 1979.

[3] F. Vieira, R. A. de Carvalho. *Elementos de Aritmética e Álgebra*, 1ª ed. Rio de Janeiro: SBM, 2020.