
UNIVERSIDADE ESTADUAL DA PARAÍBA
CAMPUS I - CAMPINA GRANDE
CENTRO DE CIÊNCIAS E TECNOLOGIA
DEPARTAMENTO DE MATEMÁTICA
CURSO DE LICENCIATURA PLENA EM MATEMÁTICA

DEIVERSON REINAN BARBOSA ALVES

# UMA ANÁLISE ACERCA DO NÚMERO DE HOMOMORFISMOS DE ANÉIS ENTRE $\mathbb{Z}_m$ e $\mathbb{Z}_n$

CAMPINA GRANDE - PB
2020

DEIVERSON REINAN BARBOSA ALVES

# UMA ANÁLISE ACERCA DO NÚMERO DE HOMOMORFISMOS DE ANÉIS ENTRE $\mathbb{Z}_m$ e $\mathbb{Z}_n$

Trabalho de conclusão do Curso Licenciatura em Matemática da Universidade Estadual da Paraíba, em cumprimento às exigências para obtenção do Título de Licenciado em Matemática.

**Área de concentração:** Álgebra

**Orientadora:** Profa. Dra. Emanuela Régia de Sousa Coelho

**CAMPINA GRANDE**

**2020**

A474a Alves, Deiverson Reinan Barbosa.

Uma análise acerca do número de homomorfismos de anéis entre Zm e Zn [manuscrito] / Deiverson Reinan Barbosa Alves. - 2020.

35 p.

Digitado.

Trabalho de Conclusão de Curso (Graduação em Matemática) - Universidade Estadual da Paraíba, Centro de Ciências e Tecnologia , 2020.

"Orientação : Profa. Dra. Emanuela Régia de Sousa Coelho , Departamento de Matemática - CCT."

1. Congruências. 2. Homomorfismos de anéis. 3. Álgebra. 4. Teoria de números. I. Título

21. ed. CDD 512.72

Elaborada por Giulianne M. Pereira - CRB - 15/714 BC/UEPB

DEIVERSON REINAN BARBOSA ALVES

**UMA ANÁLISE ACERCA DO NÚMERO DE HOMOMORFISMOS DE ANÉIS ENTRE $\mathbb{Z}_m$ e $\mathbb{Z}_n$**

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Licenciatura Plena em Matemática da Universidade Estadual da Paraíba, em cumprimento às exigências para obtenção do Título de Licenciado em Matemática.

**Área de concentração:** Álgebra

Aprovado em: 10 / 12 / 2020

BANCA EXAMINADORA:

Profa. Dra. Emanuela Régia de Sousa Coelho (Orientadora)
Universidade Estadual da Paraíba (UEPB)

Prof. Dr. Israel Burití Galvão
Universidade Estadual da Paraíba (UEPB)

Profa. Dra. Maria Isabelle Silva Dias Yanes
Universidade Estadual da Paraíba (UEPB)

À Deus, por ser o centro da minha vida e minha força diária, à toda minha família por me ensinar os valores da vida e ter me apoiado em todas as minhas decisões, aos meus professores por serem exemplos de profissionalismo, em especial a minha orientadora, Professora Emanuela, DEDICO.

# Agradecimentos

Agradeço primeiramente a Deus pelo dom da vida, por me manter sempre firme e forte na minha caminhada acadêmica, dando-me forças para nunca desistir e sempre seguir em frente com a cabeça erguida em busca da realização dos meus sonhos.

Aos meus pais Josiel e Maria da Assunção, assim como os meus irmãos (Flávio, Álef e Tayslâne), meus cunhados e familiares de forma geral por me darem todo o apoio necessário que eu precisava, seja financeiro, emocional e/ou afetivo, me ensinando sempre os valores da vida, a lutar pelos meus ideais, e acima de tudo, nunca me deixar levar pelas minhas fraquezas.

Um agradecimento a todos que regem a Universidade Estadual da Paraíba, aos meus professores que passaram pela minha vida Estudantil, e por compartilhar todo o conhecimento necessário para a minha formação, em especial aos professores Isabelle e Israel por aceitarem participar da banca e fazer parte desse momento tão especial e tão esperado, a defesa do meu TCC.

Agradeço de forma carinhosa e muito especial a minha orientadora do trabalho, a professora Emanuela que não mediu esforços para me auxiliar nesse período de orientação, e que tanto contribuiu com a minha carreira estudantil, como também profissional, pois muitos dos alunos, assim como eu, se espelham em profissionais como ela.

Por fim, mas não menos importante, agradeço aos meus amigos que fizeram parte desse sonho juntamente comigo no decorrer desses 4 anos, que sempre estiveram ao meu lado para me ajudar quando eu precisava, sempre me apoiando em minhas decisões e dúvidas acadêmicas, em especial Igor, Ana Cristina, Mayrton, Claudiana, Lucas G., Anuciada, Vanessa, Geovana, Weslley, Wellington, Emerson, e tantos outros que sabem a quem me refiro, mas para não tornar essa lista tão cansativa, citei apenas alguns dos vários nomes.

À todos, minha eterna GRATIDÃO!

"A Man is like a fraction whose numerator is what he is and whose denominator is what he thinks of himself. The larger the denominator, the smaller the fraction."

Leo Tolstoy

# Resumo

O presente trabalho tem como objetivo realizar um estudo sobre homomorfismos entre os anéis $\mathbb{Z}_m$ e $\mathbb{Z}_n$, especificamente, apresentamos um resultado que quantifica os homomorfismos existentes entre eles. Para o desenvolvimento do trabalho, propomos uma abordagem didática do Artigo intitulado *The number of homomorphisms from* $\mathbb{Z}_n$ *to* $\mathbb{Z}_m$ de Diaz-Vargas e Santos e para isso, utilizamos alguns conceitos e resultados de Teoria dos Números e de Álgebra Abstrata, tais como: Divisibilidade, Congruências módulo m, Grupos, Anéis, Homomorfismos de Anéis, entre outros.

**Palavras-chave:** Congruências, Homomorfismos de Anéis, Inteiros módulo m.

# Abstract

The present work has as its purpose to realize a study about homomorphisms between the $\mathbb{Z}_m$ and $\mathbb{Z}_n$ rings, besides, specifically we showed a result that quantifies the existing homomorphisms between them. For the work development, we propose a didactic approach of the entitled article *The number of homomorphisms from $\mathbb{Z}_n$ to $\mathbb{Z}_m$ by Diaz-Vargas and* Santos, and thereunto, we will use some concepts and results from the Number Theory and Abstract Algebra, such as: divisibility, congruences modulo m, groups, rings, ring homomorphisms, and others.

**Keywords:** Congruences, Ring homomorphisms, Integer modulo m.

# Sumário

# 1. Introdução

O presente trabalho consiste em apresentar um resultado que determina o número de homomorfismos existentes entre os anéis $\mathbb{Z}_m$ e $\mathbb{Z}_n$ e, para isto, fez-se necessário abordar alguns conceitos e resultados preliminares da Teoria dos Números, da Teoria de Grupos, e por fim, da Teoria de Anéis. Esse resultado é apresentado tanto em Gallian e Buskirk (1984), quanto em Diaz-Vargas e Santos (2015). A priori, tomamos como base esses dois artigos, fizemos uma análise de ambos e, posteriormente, desenvolvemos o trabalho. Embora tratem da mesma temática, os autores trazem abordagens diferentes para o desenvolvimento da prova do referido resultado: Enquanto Gallian e Buskirk trazem argumentos essencialmente da Teoria de Anéis, Diaz-Vargas e Santos apresentam argumentos majoritariamente da Teoria dos Números, especialmente, das relações de congruência. Nesse sentido, escolhemos apresentar as ideias de Diaz-Vargas e Santos, uma vez que os resultados de Teoria dos Números nos são mais familiares, enquanto alunos do Curso de Licenciatura, do que os resultados da Teoria de Anéis.

Ressaltamos que, tanto Gallian e Bussirk, quanto Diaz-Vargas e Santos apresentam também um resultado que quantifica os homorfismos de grupos entre $\mathbb{Z}_n$ e $\mathbb{Z}_m$, com a abordagem semelhante ao que eles fazem para o caso dos Homomorfismos de Anéis. Esse resultado foi estudado por Santos (2018) e apresentado de forma didática, a partir da abordagem dada por Gallian e Bussirk.

Entendemos que a relevância do tema proposto se deve ao fato de que a Teoria de Anéis é pouco vista nos cursos de Licenciatura em Matemática, em muitos casos, nem sequer é estudada. Nessa perspectiva, pretendemos auxiliar os futuros discentes da área a compreender melhor essa subárea da Álgebra Abstrata, como também disponibilizar um recurso para futuros docentes da área levarem até os seus alunos, como forma de material extra a ser utilizado em salas de aula de turmas de graduação.

A Matemática é uma ciência que sobrevive de argumentos. Não é suficiente apenas supor que um resultado, uma afirmação, seja verdadeira, é necessário provar a veracidade desta afirmação por meios de raciocínios lógicos. Sua estrutura se fundamenta a partir de axiomas que são constituídos de afirmativas consideradas verdades absolutas; teoremas e proposições que são demonstrados através de raciocínio lógico ou dedutivo, e outros tipos de raciocínio, corolários que são resultados os quais seguem imediatamente dos teoremas,

lemas usados para demonstrar um teorema, e assim vai se construindo a base de um conhecimento sólido e robusto.

Hoje, a Matemática é dividida em dezenas de áreas. Essas subdivisões têm a finalidade de facilitar o seu estudo, por exemplo: Aritmética, Álgebra, Geometria, Cálculo Diferencial e Integral, entre outras. Diante disso, o presente trabalho tem como foco o ramo da Álgebra, mais precisamente, o estudo da Teoria de Anéis, de modo específico, relacionado a Homomorfismos de Anéis através de aplicações de resultados da Teoria dos Números.

Segundo Baumgart (1992), Al-Khowarizmi (780-850), que foi um matemático árabe, escreveu um livro intitulado Hissab al Jabr wa-l-Muqabala que deu origem ao nome Álgebra. Ela surgiu para atender à necessidade das pessoas de calcularem quando apenas o cálculo aritmético não era mais suficiente. Porém, levou-se bastante tempo para que a linguagem criada para a Álgebra fosse compreendida por aquelas pessoas, tendo em vista que envolvia uma linguagem bastante simbólica.

Uma ferramenta muito importante da Álgebra, que também é muito importante para o nosso trabalho, quando estudamos problemas de divisibilidade, envolve o trato de congruências módulo $m$ que, segundo Milies e Coelho (2006), foram originadas a partir de estudos de restos de divisões por primos feitas por Leonhard Euler (1707-1783). Embora outros matemáticos também tenham se envolvido com a problemática, a Teoria das Congruências só foi formalizada por Gauss, nas suas Disquisitiones.[1] Gauss introduziu a notação $\equiv$ para a congruência, graças a familiaridade de suas propriedades com a relação de igualdade , simbolizada por $=$.

Já com respeito à Álgebra Moderna, segundo Milies (2004), o primeiro a introduzir o conceito de Grupo Abstrato foi Arthur Cayley(1821-1895), a partir da generalização de casos particulares que vinham sendo estudados, mas foi Evariste Galois (1811 - 1832), que utilizou o termo grupo com o sentido que conhecemos hoje, no seu trabalho de 1830. Por fim, Millies ainda afirma que foi Richard Dedekind (1831-1916) o primeiro a apresentar uma definição rigorosa de Anel que, à época, ele chamava de ordem. O termo anel,como conhecido hoje, foi introduzido em 1897 por David Hilbert (1862 - 1943), mas num contexto específico. A definição geral, foi dada em 1914 por Abraham A. Fraenkel (1891 - 1965). O que nos mostra que, considerando a história da Matemática, essa teoria é consideravelmente nova.

Como dito, a proposta desse trabalho consiste em quantificar o número de Homomorfismo de Anéis existentes entre $\mathbb{Z}_m$ e $\mathbb{Z}_n$ utilizando resultados de Teoria dos Números. Para alcançar nosso objetivo, é necessário apresentar alguns conceitos e resultados previamente estudados para bem entendermos todo o procedimento executado na prova do nosso resultado principal. Por isso, este texto está organizado da seguinte forma:

[1] O texto completo de Gauss está disponível em <https://gdz.sub.uni-goettingen.de/id/PPN235993352?tify={%22view%22:%22info%22}>

No Segundo Capítulo, apresentaremos as definições e resultados da Teoria dos Números que serão úteis e importantes para o nosso estudo, desde divisibilidade até os Inteiros $\mathbb{Z}_m$. Ainda, serão expostos as principais definições e resultados da Álgebra Abstrata que serão utilizadas, estas envolvem desde conceitos de Grupos até Anéis, especificamente Homomorfismo de Anéis.

No Terceiro Capítulo, demonstraremos por sua vez o resultado mais importante do nosso trabalho, que se trata do número de homomorfismo de anéis, a partir de uma abordagem didática da referência Diaz-Vargas e Santos (2015) .

# 2. Resultados Preliminares

Neste Capítulo, apresentamos algumas definições e resultados que serão necessários para nos auxiliar no próximo capítulo, o qual é o principal deste texto, com o objetivo de deixar esta monografia o mais autossuficiente possível.

A princípio, trabalhamos alguns conceitos básicos de Teoria dos Números, pois, o resultado principal do nosso trabalho trata-se do número de homomorfismo entre os anéis $\mathbb{Z}_m$ e $\mathbb{Z}_n$ e, portanto, faz-se necessário estudarmos o conjunto $\mathbb{Z}_m$. Além disso, sua demonstração utiliza prioritariamente resultados referentes a divisibilidade e a relação de congruência módulo $m$.

Para a construção dessa primeira seção, seguimos as ideias de Hefez (2014), Milies e Coelho (2006), Santos (2017) e Vieira (2015). Sempre que possível, iremos exibir as provas dos resultados apresentados e, aquelas que não forem possíveis - por utilizarem muitos conceitos que fogem ao nosso objetivo - podem ser facilmente encontradas em qualquer das referências indicadas.

## 2.1 Tópicos em Teoria dos Números

Começamos apresentando alguns resultados básicos de divisibilidade.

### 2.1.1 Divisibilidade e Máximo Divisor Comum

**Definição 2.1** (Divisibilidade)**.** *Sejam $a, b \in \mathbb{Z}$, dizemos que $a$ divide $b$, e denotamos por $a \mid b$, se existir um inteiro $c$, tal que*

$$b = a \cdot c.$$

*Assim sendo, podemos dizer ainda que $b$ é divisível por $a$, que $a$ é divisor de $b$, ou ainda, que $b$ é múltiplo de $a$. Ainda, escrevemos $c = b/a$ ou $c = \frac{b}{a}$ .*

**Proposição 2.1.** *Sejam $a, b \in \mathbb{Z}$. Se $b|a$ e $a \neq 0$, então $|b| \leq |a|$.*

**Prova:** Suponha que $b|a$ logo, por definição, existe $c \in \mathbb{Z}$, tal que

$$a = bc.$$

Assim,

$$|a| = |bc| = |b||c|.$$

Como $a \neq 0$, segue que $b \neq 0$ e $c \neq 0$, logo, $|c| \geq 1$, daí,

$$|a| = |b||c| \geq |b| \cdot 1 = |b| \Rightarrow |b| \leq |a|.$$

□

**Proposição 2.2** (Algoritmo da Divisão)**.** *Sejam a,b inteiros, com $b > 0$. Então, existem únicos inteiros q e r, tais que:*

$$a = bq + r, \text{ com } 0 \leq r < b.$$

**Observação 2.1.** *Os inteiros r e q da Proposição 2.2 são chamados de* ***quociente*** *e* ***resto*** *da Divisão Euclidiana de a por b, respectivamente.*

**Definição 2.2.** *Sejam a,b $\in \mathbb{Z}$, com $a \neq 0$ ou $b \neq 0$. Dizemos que $d \in \mathbb{N}$ é máximo divisor comum* (mdc) *entre a e b quando as seguintes condições são satisfeitas:*

*(i) $d|a$ e $d|b$;*

*(ii) Se $c|a$ e $c|b$, então $c|d$.*

*Em outras palavras, o máximo divisor comum entre a e b é um número natural que os divide e é divisível por todo divisor comum de a e b. Nessas condições, utilizamos a notação*

$$d = \text{mdc(a, b)}.$$

*Quando $mdc(a, b) = 1$, dizemos que a e b são primos entre si.*

**Teorema 2.1** (Teorema de Bézout)**.** *Sejam $a, b \in \mathbb{Z}$, não ambos nulos, e $d = \text{mdc(a, b)}$. Então, existem inteiros r e s tais que $d = ra + sb$.*

**Observação 2.2.** A recíproca do Teorema de Bézout, em geral, não é válida, ou seja, se $d$ satisfaz $d = ra + sb$, para algum $r, s \in \mathbb{Z}$, não implica em $d = \text{mdc(a, b)}$. De fato, observe que $4 = 2 \cdot 4 + (-2) \cdot 2$, mas $4 \neq 2 = \text{mdc}(2, 4)$.

Agora, se $d = 1$, ou seja, se $\text{mdc(a, b)} = 1$, então vale a recíproca.

Com efeito, suponha que existem $r, s \in \mathbb{Z}$, com $1 = ra + sb$. Se $d = \text{mdc(a, b)}$, então $d|a$ (portanto, $d|ra$) e $d|b$ (portanto, $d|sb$), logo, $d|(ra+sb) = 1$. Da Proposição 2.1, segue que $d \leq 1$. Como $d \in \mathbb{N}$, segue que $d = 1$.

**Proposição 2.3.** *Sejam $a, b \in \mathbb{Z}$ não ambos nulos, $d = \text{mdc(a, b)}$ e c um inteiro não nulo, então,* $\text{mdc(ac, bc)} = d|c|$.

**Prova:** De fato, como $d = \text{mdc(a, b)}$, segue pela Definição 2.2 que $d|a$ e $d|b$, logo $(d|c|)|(ac)$ e $(d|c|)|(bc)$. Ainda, do Teorema de Bézout, existem $r, s \in \mathbb{Z}$, tais que $d = ra + sb$, logo

$$d|c| = r(a|c|) + s(b|c|)$$

Agora, se $d'$ é um inteiro tal que $d'|ac$ e $d'|bc$, da relação acima, vem imediatamente que $d'|(d|c|)$ e, portanto, pela Definição 2.2, temos o desejado.

□

**Teorema 2.2** (Teorema de Euclides)**.** *Sejam $a, b, c \in \mathbb{Z}$, tais que $a|(bc)$. Se $mdc(a, b) = 1$, então $a|c$.*

**Prova:** A prova é imediata, pois se $mdc(a, b) = 1$, então da proposição anterior, temos $mdc(ac, bc) = |c|$. Agora, como $a|(ac)$ e, por hipótese, $a|(bc)$, então, pela definição de $mdc$, segue que $a||c|$, ou seja, $a|c$.

□

**Corolário 2.1.** *Sejam $a, b \in \mathbb{Z}$, com $mdc(a, b) = 1$. Se $c \in \mathbb{Z}$ é tal que, $a|c$ e $b|c$, então $(ab)|c$.*

**Prova:** Como $a|c$ e $b|c$, existem $k, r \in \mathbb{Z}$, tais que $c = ak$ e $c = br$, logo $ak = br$, isto é, $a|(br)$. Do Teorema de Euclides, $a|r$, portanto, $r = as$, $s \in \mathbb{Z}$, e assim

$$c = abs$$

e $(ab)|c$ .

□

**Proposição 2.4.** *Seja $a \in \mathbb{Z}$, então $mdc(a, a - 1) = 1$.*

**Prova:** Suponha que $d = \text{mdc(a, a} - 1)$, então $d \geq 1$, $d|a$ e $d|(a - 1)$, daí $a = d \cdot k$ e $a - 1 = d \cdot r$, com $k, r \in \mathbb{Z}$. Donde das duas igualdades, temos

$$1 = a - (a - 1) = d \cdot k - d \cdot r = d \cdot (k - r)$$

e portanto, $d|1$, o que garante, pela Proposição 2.1, que $d \leq 1$. Logo, $mdc(a, a - 1) = 1$.

□

**Definição 2.3.** *Um número $p \in \mathbb{Z} - \{0, \pm 1\}$ é dito **primo** quando seus únicos divisores positivos são 1 e $|p|$. Caso contrário, dizemos que $p$ é **composto**.*

**Teorema 2.3** (Teorema Fundamental da Aritmética - TFA)**.** *Seja $a \in \mathbb{Z}$, $a \neq 0, 1, -1$. Então, existem primos $p_1 < p_2 < \cdots < p_r$ e inteiros positivos $n_1, n_2, \cdots, n_r$ tais que*

$$a = \pm p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}.$$

*Ademais, a decomposição é única.*

**Observação 2.3.** (i) A fatoração do número $a \in \mathbb{Z}$ dada pelo Teorema Fundamental da Aritmética é, por vezes, chamada de Fatoração Canônica de $a$.

(ii) Se $a, b \in \mathbb{Z}$ e $a = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$, então podemos escrever $b = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r} q$ com $mdc(p_i, q) = 1$. De fato, considere $a = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$, produto onde os fatores são números primos. Observe que para a fatoração de $b$, se $p_1$ não divide $b$, então $m_1 = 0$, pois teríamos $p_1^0 = 1$ e claro que $1|b$, logo ele está na fatoração de $b$. Se $p_1|b$, então $m_1$ será o maior natural tal que $p_1^{m_1}|b$ e $p_1^{m_1+1}$ não divide $b$. Os demais fatores até $p_r^{n_r}$ são analisados de forma análoga. Agora, observe que se essa já for a fatoração de $b$, então claramente $q = 1$, porém, se tiver faltando mais primos na fatoração de $b$ além de $p_1^{m_1}, p_2^{m_2}, \cdots, p_r^{m_r}$ então $q$ vai ser o produto desses outros primos que vão estar faltando na fatoração de $b$. Daí, como todos esses outros primos não são nenhum dos $p_i$'s então $mdc(p_i, q) = 1$.

### 2.1.2 Congruência módulo $m$

Os principais argumentos utilizados para a prova do Teorema principal do presente trabalho envolvem propriedades relacionadas a Congruência módulo $m$, tais resultados são apresentados nesta seção.

**Definição 2.4** (Congruência)**.** *Sejam $a, b, m \in \mathbb{Z}$ e $m > 1$. Dizemos que $a$ é congruente a $b$ módulo $m$, em símbolos*

$$a \equiv b (\text{mod } m),$$

*quando $m$ divide $a - b$, em símbolos, $m \mid (a - b)$. Em outras palavras, existe um inteiro $k$ tal que,*

$$a - b = km, \text{ ou ainda, } a = b + km.$$

**Exemplo 2.1.** $7 \equiv 2(mod 5)$*, pois, por definição,*

$$7 \equiv 2(mod 5) \Leftrightarrow 5 \mid (7 - 2) \Leftrightarrow 7 - 2 = 5k$$

*e, como $7 - 2 = 5 = 5.1$, então, $7 \equiv 2(mod 5)$.*

**Proposição 2.5.** *Seja $m \in \mathbb{Z}$, $m > 1$. Dois inteiros $a$ e $b$ são congruentes módulo $m$ se, e somente se, $a$ e $b$ possuem o mesmo resto quando divididos por $m$.*

**Prova:** Sejam $a, b \in \mathbb{Z}$. Pelo Algoritmo da Divisão (Proposição 2.2), temos

$$a = mq_1 + r_1 \text{ e } b = mq_2 + r_2$$

com $r_1, r_2, q_1, q_2, \in \mathbb{Z}$ e $0 \leq r_1, r_2 < m$.
Assim

$$a - b = m(q_1 - q_2) + (r_1 - r_2),$$

logo $m|(a-b)$ se, e somente se, $m|(r_1-r_2)$, donde $(r_1-r_2) \geq m$. Mas,
como $0 \leq |r_1-r_2| < m$, temos $m|(r_1-r_2)$ se, e somente se, $r_1-r_2=0$ e, portanto,

$$a \equiv b(\text{mod } m) \Leftrightarrow r_1 - r_2 = 0$$

o que prova o desejado.

□

**Proposição 2.6.** *Sejam $m>1$ um inteiro fixo e $a,b,c,d \in \mathbb{Z}$. São válidos:*

**i)** *Se $a \equiv b(\text{mod } m)$ e $c \equiv d(\text{mod } m)$, então $(a+c) \equiv (b+d)(\text{mod } m)$;*

**ii)** *Se $a \equiv b(\text{mod } m)$, então $(a+c) \equiv (b+c)(\text{mod } m)$;*

**iii)** *Se $a \equiv b(\text{mod } m)$ e $c \equiv d(\text{mod } m)$, então $ac \equiv bd(\text{mod } m)$;*

**iv)** *Se $a \equiv b(\text{mod } m)$, então $a^n \equiv b^n(\text{mod } m)$, para todo $n \in \mathbb{N}$;*

**v)** *Se $(a+c) \equiv (b+c)(\text{mod } m)$, então $a \equiv b(\text{mod } m)$.*

**Prova:** A fim de evitar repetições, provaremos (i) e (iii), os demais itens são análogos e podem ser encontrados em quaisquer das referências indicadas.

**i)** Se $a \equiv b(\text{mod } m)$ e $c \equiv d(\text{mod } m)$, então existem $k_1, k_2 \in \mathbb{Z}$,

$$a-b = k_1 m \text{ e } c-d = k_2 m$$

logo,

$$(a+c)-(b+d) = (a-b)+(c-d) = k_1m+k_2m = (k_1+k_2)m \Rightarrow m|[(a+c)-(b+d)]$$

e, portanto, $(a+c) \equiv (b+d)(\text{mod } m)$.

**iii)** Se $a \equiv b(\text{mod } m)$ e $c \equiv d(\text{mod } m)$, então existem $k_1, k_2 \in \mathbb{Z}$, com

$$a-b = k_1 m \text{ e } c-d = k_2 m,$$

logo

$$ac = (k_1m+b)(k_2m+d) = bd + (k_1k_2m + k_1d + k_2b)m = bd + km$$

ou seja, $ac-bd = km$ e $m|(ac-bd)$, portanto,

$$ac \equiv bd(\text{mod } m),$$

com $k = k_1k_2m + k_1d + k_2b \in \mathbb{Z}$, portanto vale o item iii).

□

Para finalizar esta seção, considere a congruência

$$ax \equiv b(\text{mod } m), \tag{2.1}$$

com $a, b, m \in \mathbb{Z}, a \neq 0, m > 1$ e $x \in \mathbb{Z}$ a se determinar. A congruência acima é chamada de congruência linear e um número $x_0 \in \mathbb{Z}$ que satisfaz (2.1) é dito solução da equação.

**Teorema 2.4** (Teorema Chinês do Resto)**.** *Sejam $n_1, n_2, \cdots, n_k$ inteiros, dois a dois, relativamente primos entre si, e sejam $c_1, c_2, \cdots, c_k \in \mathbb{Z}$. O sistema de congruências lineares*

$$\begin{cases} X \equiv c_1 \pmod{n_1} \\ X \equiv c_2 \pmod{n_2} \\ \quad \vdots \\ X \equiv c_k \pmod{n_k} \end{cases} \tag{2.2}$$

*admite solução, que é única módulo $n = n_1 n_2 \cdots n_k$.*

**Prova:** Inicialmente, considere $n = n_1 n_2 \cdots n_k$ e defina $N_i = \frac{n}{n_i} = n_1 n_2 \cdots n_{i-1} n_{i+1} \cdots n_k$ para cada $i = 1, \cdots, k$. Sabemos que, como $N_i$ é o produto de todos os inteiros $n_1, n_2, \cdots, n_k$ exceto o próprio $n_i$, então eles são relativamente primos entre si, ou seja, $mdc(N_i, n_i) = 1$. Sendo assim, pelo Teorema de Bézout (2.1), existem $r_i, s_i \in \mathbb{Z}$, tais que

$$r_i N_i + s_i n_i = 1, 1 \leq i \leq k \tag{2.3}$$

Vamos mostrar que o número $x_0 = c_1 r_1 N_1 + c_2 r_2 N_2 + \cdots + c_k r_k N_k$ é solução de 2.2.

De fato, se $i \neq j$, então , $n_i | N_j$ ou seja, $N_j \equiv 0(\text{mod } n_i)$, em outras palavras, $N_j$ é múltiplo de $n_i$. Deste modo, $c_j r_j N_j \equiv 0(\text{mod } n_i)$ e, portanto,

$$x_0 = c_1 r_1 N_1 + c_2 r_2 N_2 + \cdots + c_k r_k N_k \equiv c_i r_i N_i (\text{mod } n_i),$$

ou seja,

$$x_0 \equiv c_i r_i N_i (\text{mod } n_i).$$

Por outro lado, multiplicando (2.3) por $c_i$, temos $c_i = c_i r_i N_i + c_i s_i n_i$, ou seja,

$$c_i r_i N_i \equiv c_i (\text{mod } n_i).$$

Daí, por transitividade[1], $x_0 \equiv c_i (\text{mod } n_i)$, donde $i = 1, \cdots, k$, portanto isso mostra que $x_0$ é uma solução de 2.3, restando mostrar agora que ele é único módulo $n$.

[1]Mostramos, na Proposição 2.7 na próxima seção, que a relação $\equiv (\text{mod } n)$ é uma relação de equivalência sobre $\mathbb{Z}$ e, portanto, transitiva.

Considerando agora $y_0$ uma outra solução de 2.3, sendo assim, $y_0 \equiv c_i (\text{mod } n_i)$, para $i = 1, \cdots, k$. Consequentemente, $x_0 \equiv y_0 (\text{mod } n_i)$, isto é, $n_i | (x_0 - y_0)$ para cada $1 \leq i \leq k$, e como $n_1, n_2, \cdots, n_k$ são primos entre si, logo segue do Corolário 2.1 que $n = n_1 n_2 \cdots n_k | (x_0 - y_0)$, ou seja, $x_0 \equiv y_0 (\text{mod } n)$, como queríamos, provando assim a unicidade da solução módulo $n$.

□

### 2.1.3 Inteiros Módulo $m$, $\mathbb{Z}_m$

A seguir, recordamos alguns conceitos e resultados acerca de Relações sobre um conjunto não vazio $A$ que são esseciais para a definição do nosso objeto de estudo principal, o conjunto $\mathbb{Z}_m$.

**Definição 2.5** (Relação de equivalência)**.** *Dizemos que a relação $\sim$ sobre um conjunto $A$ é de equivalência, quando a mesma satisfaz as seguintes condições, para quaisquer $a, b, c \in A$:*

**i)** *Reflexividade, ou seja, $a \sim a$;*

**ii)** *Simetria, ou seja, se $a \sim b$, então $b \sim a$;*

**iii)** *Transitividade, isto é, se $a \sim b$ e $b \sim c$, então $a \sim c$.*

*Nessas condições, para cada $a \in A$, o conjunto de todos os elementos $x \in A$ tais que $x \sim a$ chama-se* ***classe de equivalência de*** *$a$ e indica-se por $\overline{a}$. Ou seja,*

$$\overline{a} = \{x \in A : x \sim a\}.$$

*Um elemento $b \in \overline{a}$ é dito um* ***representante*** *da classe $\overline{a}$.*

*O conjunto de todas as classes de equivalência segundo a relação $\sim$ é chamado conjunto quociente de $A$ por $\sim$ e indica-se por $A/\sim$. Assim,*

$$A/\sim = \{\overline{a} : a \in A\}.$$

**Observação 2.4.** *Segue da definição de relação de equivalência sobre um conjunto $A$ que:*

*(i) Sendo $\sim$ uma relação de equivalência sobre $A$, então $a \sim a$ para todo $a \in A$. Logo, $a \in \overline{a}$, o que implica em $\overline{a} \neq \varnothing$.*

*(ii)* $A = \cup_{a \in A} \overline{a}$

*(iii)* $\overline{a} = \overline{b}$ *ou* $\overline{a} \cap \overline{b} = \varnothing$*, para todo* $a, b \in A$.

**Proposição 2.7.** *A congruência módulo $m$ ($\equiv (\text{mod } m)$) é uma relação de equivalência sobre $\mathbb{Z}$.*

**Prova:** Para provarmos que a congruência módulo $m$ é uma relação de equivalência, temos que mostrar que ela é reflexiva, simétrica e transitiva.

*Reflexiva:* Para qualquer $a \in \mathbb{Z}$, temos

$$m|0 \Rightarrow m|(a-a) \Rightarrow a \equiv a(\text{mod } m),$$

isto é, $a \equiv a(\text{mod } m)$. Portanto $\equiv (\text{mod } m)$ é reflexiva.

*Simétrica*: Para todo $a, b \in \mathbb{Z}$, se $a \equiv b(modn)$, então $a - b = c \cdot m$, para algum $c \in \mathbb{Z}$, e, assim,

$$b - a = -(a-b) = (-c) \cdot m \Rightarrow m|(b-a).$$

Logo, $b \equiv a(\text{mod } m)$, o que implica que a relação é simétrica.

*Transitiva*: Sejam $a, b, c \in \mathbb{Z}$, tais que $a \equiv b(\text{mod } m)$ e $b \equiv c(\text{mod } m)$, então $a-b = e \cdot m$ e $b - c = f \cdot m$, para alguns $e, f \in \mathbb{Z}$. Logo,

$$a - c = a - b + b - c = e \cdot m + f \cdot m = (e+f) \cdot m.$$

Portanto, $a \equiv c(\text{mod } m)$, o que implica que a relação é transitiva.

Logo, tal relação é de equivalência.

□

**Definição 2.6** (Conjunto dos números inteiros módulo $m$)**.** *Seja $m \in \mathbb{Z}$, com $m > 1$. Para cada $a \in \mathbb{Z}$, denotamos a classe de equivalência de $a$ módulo $m$ por*

$$\overline{a} := \{b \in \mathbb{Z}; b \equiv a(\text{mod } m)\}.$$

*Chamamos de $\mathbb{Z}_m$ o conjunto quociente de $\mathbb{Z}$ pela relação de congruência módulo $m$. Portanto,*

$$\mathbb{Z}_m = \{\overline{a}; a \in \mathbb{Z}\}.$$

Agora, sejam $m \in \mathbb{Z}, m > 1$ e $\overline{a} \in \mathbb{Z}_m$. Como $a \in \mathbb{Z}$, aplicando o Algoritmo da Divisão (Proposição 2.2), temos a existência de $q, r \in \mathbb{Z}$ tais que

$$a = q \cdot m + r \text{ com } 0 \leq r < m.$$

Logo, $a - r = q \cdot m$, o que implica em $a \equiv r(\text{mod } m)$ e portanto, $\overline{a} = \overline{r}$, $0 \leq r < m$. Sendo assim, podemos concluir que

$$\mathbb{Z}_m = \{\overline{0}, \overline{1}, ..., \overline{m-1}\}.$$

Como $\overline{a} = \overline{r}$, em que $r$ é o resto da divisão de $a$ por $m$, $\mathbb{Z}_m$ é também chamado de classe de restos.

**Exemplo 2.2.** *Seja $m = 3$, do comentário acima, temos*

$$\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\},$$

*em que*
$\overline{0} = \{a \in \mathbb{Z}; a \equiv 0(mod3)\} = \{a = 3 \cdot k, k \in \mathbb{Z}\} = \{..., -3, 0, 3, 6, ...\}$;
$\overline{1} = \{a \in \mathbb{Z}; a \equiv 1(mod3)\} = \{a = 3 \cdot k + 1, k \in \mathbb{Z}\} = \{..., -2, 1, 4, 7, ...\}$;
$\overline{2} = \{a \in \mathbb{Z}; a \equiv 2(mod3)\} = \{a = 3 \cdot k + 2, k \in \mathbb{Z}\} = \{..., -1, 2, 5, 8, ...\}$.

**Proposição 2.8.** *Seja $m > 1$ um número inteiro. Então,*

$$\begin{array}{rccc} + : & \mathbb{Z}_m \times \mathbb{Z}_m & \longrightarrow & \mathbb{Z}_m \\ & (\overline{a}, \overline{b}) & \longmapsto & \overline{a} + \overline{b} = \overline{a + b} \end{array} \quad e \quad \begin{array}{rccc} \cdot & : \mathbb{Z}_m \times \mathbb{Z}_m & \to & \mathbb{Z}_m \\ & (\overline{a}, \overline{b}) & \mapsto & \overline{a} \cdot \overline{b} = \overline{a \cdot b} \end{array}$$

*definem duas operações sobre $\mathbb{Z}_m$, a primeira chamada de adição(ou soma) e a segunda de produto(ou multipliação).*

**Prova:** Sejam $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ tais que

$$\overline{a_1} = \overline{a_2} \text{ e } \overline{b_1} = \overline{b_2}.$$

Devemos mostrar que

$$\overline{a_1} + \overline{b_1} = \overline{a_2} + \overline{b_2} \text{ e } \overline{a_1} \cdot \overline{b_1} = \overline{a_2} \cdot \overline{b_2},$$

ou seja, os resultados que obtermos através dessas operações, independem de quais representantes das classes $\overline{a_1}$ e $\overline{b_1}$ forem escolhidos.

Por hipótese, temos $\overline{a_1} = \overline{a_2}$ e $\overline{b_1} = \overline{b_2}$ logo, por definição, $a_1 \equiv a_2 (\text{mod } m)$ e $b_1 \equiv b_2 (\text{mod } m)$ e, da Proposição 2.6 (item (i)), temos

$$(a_1 + b_1) \equiv (a_2 + b_2) (\text{mod } m)$$

portanto,

$$\overline{a_1 + b_1} = \overline{a_2 + b_2}$$

e, por esse motivo, temos

$$\overline{a_1} + \overline{b_1} = \overline{a_1 + b_1} = \overline{a_2 + b_2} = \overline{a_2} + \overline{b_2}.$$

Por conseguinte, façamos a mesma análise para a multiplicação. Do item (iii) da Proposição 2.6, temos

$$a_1 \cdot b_1 \equiv a_2 \cdot b_2 (\text{mod } m),$$

ou seja,

$$\overline{a_1 \cdot b_1} = \overline{a_2 \cdot b_2}.$$

Portanto,

$$\overline{a_1} \cdot \overline{b_1} = \overline{a_1 \cdot b_1} = \overline{a_2 \cdot b_2} = \overline{a_2} \cdot \overline{b_2},$$

como queríamos demonstrar.

□

**Teorema 2.5.** *As operações "+"e "·", adição e multiplicação respectivamente, sobre $\mathbb{Z}_m$ têm as seguintes propriedades:*

*(i)* $\overline{a} + (\overline{b} + \overline{c}) = (\overline{a} + \overline{b}) + \overline{c}$, *para quaisquer* $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_m$ *(+ é associativa);*

*(ii)* $\overline{a} + \overline{b} = \overline{a} + \overline{b}$, *para quaisquer* $\overline{a}, \overline{b} \in \mathbb{Z}_m$*(+ é comutativa);*

*(iii)* $\overline{a} + \overline{0} = \overline{a}$, *para quaisquer* $\overline{a} \in \mathbb{Z}_m$ *(existência de neutro da adição);*

*(iv)* $\overline{a} + \overline{m - a} = \overline{0}$*(existência do inverso sob +)*

*(v)* $\overline{a} \cdot (\overline{b} \cdot \overline{c}) = (\overline{a} \cdot \overline{b}) \cdot \overline{c}$, *para quaisquer* $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_m$ *(· é associativa);*

*(vi)* $\overline{a} \cdot \overline{b} = \overline{a} \cdot \overline{b}$, *para quaisquer* $\overline{a}, \overline{b} \in \mathbb{Z}_m$*(· é comutativa);*

*(vii)* $\overline{a} \cdot \overline{1}$, *para qualquer* $\overline{a} \in \mathbb{Z}_m$ *(· tem elemento neutro);*

**Prova:** A fim de não causar exaustão, faremos a prova para os itens $(i)$, $(iii)$ e $(vi)$. As demais são análogas e podem ser encontradas nas referências recomendadas.

$(i)$ Sejam $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_m$, e levando em consideração o fato da adição em $\mathbb{Z}$ ser associativa, temos

$$\overline{a} + (\overline{b} + \overline{c}) = \overline{a} + (\overline{b + c}) = \overline{a + (b + c)} = \overline{(a + b) + c} = (\overline{a + b}) + \overline{c} = (\overline{a} + \overline{b}) + \overline{c},$$

ou seja, a adição é associativa.

$(iii)$ Seja $\overline{a} \in \mathbb{Z}_m$. Queremos mostrar que existe $\overline{e} \in \mathbb{Z}_m$ de tal modo que $\overline{a} + \overline{e} = \overline{a}$. Para isso, usaremos as operações que estão definidas em $\mathbb{Z}_m$, sendo assim,

$$\overline{a} + \overline{e} = \overline{a} \Leftrightarrow \overline{a + e} = \overline{a}.$$

Entretanto, a sentença acima só é verdadeira se $e$ for múltiplo de $m$, pois

$$\overline{a + e} = \overline{a} \Leftrightarrow a + e \equiv a (\text{mod } m) \Leftrightarrow a + e - a = mk$$

daí,

$$e = km, k \in \mathbb{Z}.$$

Donde podemos concluir que a classe de $e$ é igual a classe do zero, ou seja,

$$\overline{e} = \overline{0}$$

Portanto, $\overline{0}$ é o neutro da adição em $\mathbb{Z}_m$.

$(vi)$ Considere $\overline{a}, \overline{b} \in \mathbb{Z}_m$, então como o produto em $\mathbb{Z}$ é comutativo, segue

$$\overline{a} \cdot \overline{b} = \overline{a \cdot b} = \overline{b \cdot a} = \overline{b} \cdot \overline{a}.$$

□

**Definição 2.7.** *Um elemento $\overline{a} \in \mathbb{Z}_m$ é dito invertível se existe $\overline{b} \in \mathbb{Z}_m$, tal que*

$$\overline{a} \cdot \overline{b} = \overline{1}$$

*Neste caso, dizemos que $\overline{b}$ é o inverso multiplicativo de $\overline{a}$ e denotaremos por $\overline{b} = (\overline{a})^{-1}$*

**Proposição 2.9** (Existência do inverso sob $\cdot$)**.** *Dado $\overline{a} \in \mathbb{Z}_m$, existe $\overline{b} \in \mathbb{Z}_m$ com $\overline{a} \cdot \overline{b} = \overline{1}$, se, e só se, $mdc(a, m) = 1$ .*

**Prova:** Seja $\overline{a} \in \mathbb{Z}_m$, suponha que existe $\overline{a} \in \mathbb{Z}_m$ tal que $\overline{a} \cdot \overline{b} = \overline{a \cdot b} = \overline{1}$. Assim,

$$ab \equiv 1 (\text{mod } m).$$

Daí, existe $k \in \mathbb{Z}$, tal que

$$ab - 1 = km,$$

ou ainda,

$$1 = ab + (-k)m,$$

donde concluímos, pela Observação 2.2, que $mdc(a, m) = 1$.

Reciprocamente, suponha $mdc(a, b) = 1$. Pelo Teorema 2.1 existem $r, s \in \mathbb{Z}$, tais que $d = ra + sm$, porém, como $d = mdc(a, m) = 1$, então, $1 = ra + sm$, logo

$$\overline{1} = \overline{ra + sm} = \overline{ra} + \overline{sm} = \overline{ra} + \overline{0} = \overline{r} \cdot \overline{a},$$

ou seja, $\overline{a} \cdot \overline{r} = \overline{1}$, de modo que $\overline{a}$ tenha inverso multiplicativo, neste caso $(\overline{a})^{-1} = \overline{r}$.

□

## 2.2 Tópicos em Álgebra Abstrata

O resultado principal do nosso trabalho trata de quantificar os homomorfismos de Anéis entre $\mathbb{Z}_m$ e $\mathbb{Z}_n$. Um Anel é uma Estrutura Algébrica formada por um conjunto não vazio, munido de duas operações que satisfazem determinadas condições e um homomorfismo de anéis é uma função entre duas dessas estruturas que "preserva as operações". Nesta seção mostramos que $\mathbb{Z}_m$ é um anel com as operações de soma e produto.

Antes disso, apresentamos alguns conceitos e resultados relativos a Grupos, que são Estruturas Algébricas mais simples formadas por um conjunto não vazio e uma operação definida nesse conjunto satisfazendo algumas condições.

Para esta seção, utilizamos como referências Domingues (2003), Garcia e Lequain (2018) e Vieira (2013) e as recomendamos para um estudo mais aprofundado dos assuntos abordados.

### 2.2.1 Teoria de Grupos

**Definição 2.8** (Operação Binária)**.** *Seja $A$ um conjunto não vazio. Uma aplicação $* : A \times A \to A$ chama-se operação binária sobre $A$.*

**Exemplo 2.3.** A aplicação $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ dada por $+(a, b) = a + b$ é uma operação binária chamada de adição sobre $\mathbb{N}$. Da mesma forma, a aplicação $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ chamada de multiplicação também é uma operação sobre $\mathbb{N}$. E mais, vale ressaltar que estas operações podem ser estendidas aos conjuntos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$.

**Exemplo 2.4.** A soma e produto são operações binárias em $\mathbb{Z}_m$, pela Proposição 2.8.

**Definição 2.9** (Grupos)**.** *Seja $G$ um conjunto não vazio, munido com uma operação binária $\star$. Dizemos que o par $(G, \star)$ é um grupo se o mesmo satisfazer as seguintes condições:*

**i)** A operação $\star$ é associativa, ou seja,

$$a \star (b \star c) = (a \star b) \star c, \text{ para quaisquer } a, b, c \in G;$$

**ii)** Existe um elemento neutro para $\star$, isto é, existe $e \in G$, tal que

$$a \star e = e \star a = a, \text{ para qualquer } a \in G;$$

**iii)** Todo elemento em $G$ possui inverso em relação a $\star$, ou seja, dado $a \in G$, existe $a' \in G$, tal que

$$a \star a' = e = a' \star a.$$

$a'$, nessas condições, é dito inverso de $a$ e denotado por $a^{-1}$.

**Exemplo 2.5.** O conjunto $\mathbb{Z}_m$ munido da operação de multiplicação não é um grupo, pois embora $\overline{1}$ seja neutro, $\overline{0}$ não possui inverso, já que não existe $\overline{a} \in \mathbb{Z}_m$ tal que

$$\overline{0} \cdot \overline{a} = \overline{1}.$$

Mas, pelo Teorema 2.5, $\mathbb{Z}_m$ com a soma é um grupo.

**Observação 2.5.** Se o grupo $(G, *)$ satisfaz também a comutatividade, ou seja,

$$a \star b = b \star a, \forall a, b \in G$$

então, é chamado de Grupo Abeliano ou Grupo Comutativo.

**Definição 2.10** (Homomorfismo de Grupos)**.** *Sejam $(G_1, \star)$ e $(G_2, *)$ grupos e $f : G_1 \to G_2$ uma aplicação. Dizemos que $f$ é homomorfismo do grupo $G_1$ em $G_2$ quando,*

$$f(a \star b) = f(a) * f(b), \text{ para todo } a, b \in G_1.$$

**Proposição 2.10.** *Sejam $(G_1, \star)$ e $(G_2, *)$ grupos e $f : G_1 \to G_2$ um homomorfismo de grupos, então, $f(e_1) = e_2$, em que $e_1$ é elemento neutro de $G_1$ e $e_2$ é neutro em $G_2$.*

**Prova:** A prova da proposição é imediata, pois como $e_1 = e_1 \star e_1$, então

$$f(e_1) = f(e_1 \star e_1) = f(e_1) * f(e_1)$$

Considerando, $f(e_1)^{-1} \in G_2$, temos

$$e_2 = f(e_1)^{-1} * f(e_1) = f(e_1)^{-1} * f(e_1) * f(e_1) = e_2 * f(e_1) = f(e_1).$$

□

**Observação 2.6.** Considere os grupos $(\mathbb{Z}_n, +)$ e $(\mathbb{Z}_m, +)$ e seja $f : \mathbb{Z}_n \to \mathbb{Z}_m$ um homomorfismo de grupos, assim, para $\overline{a}, \overline{b} \in \mathbb{Z}_n$,

$$f(\overline{a} + \overline{b}) = f(\overline{a}) + f(\overline{b}).$$

A fim de não causar confusão, vamos denotar os elementos de $\mathbb{Z}_n$ por $\overline{a}$ e os elementos de $\mathbb{Z}_m$ por $\overline{\overline{b}}$. Agora, para cada $\overline{x} \in \mathbb{Z}_n$, temos

$$f(\overline{x}) = f(\underbrace{\overline{1} + \overline{1} + \cdots + \overline{1}}_{x \text{ vezes}}) = \underbrace{f(\overline{1}) + f(\overline{1}) + \cdots + f(\overline{1})}_{x \text{ vezes}} = xf(\overline{1}),$$

então, escrevendo $\overline{\overline{a}} = f(\overline{1})$, temos $f(\overline{x}) = \overline{\overline{a}}x$. Logo, o homomorfismo é determinado pelo valor de $f$ em $\overline{1}$.

Consequentemente, para identificar os homomorfismos de grupos de $\mathbb{Z}_n$ em $\mathbb{Z}_m$, precisamos encontrar os valores de $\overline{\overline{a}} \in \mathbb{Z}_m$ tal que a função $f(\bar{x}) = \overline{\overline{a}}x, \bar{x} \in \mathbb{Z}_n$ é um homomorfismo de grupos.

Note que, se $f(\bar{x}) = \overline{\overline{a}}x, \bar{x} \in \mathbb{Z}_n$ é um homomorfismo de grupos, então $f(\bar{0}) = \overline{\overline{0}}$, pela Proposição 2.10, como $\overline{0} = \overline{n}$, e $f(\overline{n}) = n\overline{\overline{a}} = \overline{\overline{na}}$, segue que

$$\overline{\overline{na}} = \overline{\overline{0}},$$

ou ainda,

$$na \equiv 0 (\text{mod } m).$$

**Exemplo 2.6.** *Sejam $n = 4$ e $m = 6$, então $g : \mathbb{Z}_4 \to \mathbb{Z}_6$ tal que $g(\bar{x}) = \overline{\overline{ax}}$, para $\overline{x} \in \mathbb{Z}_4$ é homomorfismo de grupos, se e somente se,*

$$\overline{\overline{a}} \in \mathbb{Z}_6 \text{ e } 4a \equiv 0(\text{mod } 6).$$

*Temos*

$$4 \cdot 0 \equiv 0(\text{mod } 6), 4 \cdot 1 \equiv 4(\text{mod } 6), 4 \cdot 2 \equiv 2(\text{mod } 6), 4 \cdot 3 \equiv 0(mod6)$$

$$4 \cdot 4 \equiv 4(mod6) \text{ e } 4 \cdot 5 \equiv 2(mod6),$$

*logo $g(\bar{x}) = \overline{\overline{ax}}$, para $\overline{x} \in \mathbb{Z}_4$ é homomorfismo de grupos, se e somente se, $\overline{\overline{a}} = \overline{\overline{0}}$ ou $\overline{\overline{a}} = \overline{\overline{3}}$.*

**Exemplo 2.7.** *Sejam $m = 2$ e $n = 4$, então $g : \mathbb{Z}_2 \to \mathbb{Z}_4$ tal que $g(\bar{x}) = \overline{\overline{ax}}$, para $\overline{x} \in \mathbb{Z}_2$ é homomorfismo, se e somente se,*

$$\overline{\overline{a}} \in \mathbb{Z}_4 \text{ e } 2a \equiv 0(mod4).$$

*Temos*

$$2 \cdot 0 \equiv 0(mod4), 2 \cdot 1 \equiv 2(mod4), 2 \cdot 2 \equiv 0(mod4), 2 \cdot 3 \equiv 2(mod4)$$

*logo $g(\bar{x}) = \overline{\overline{ax}}$, para $\overline{x} \in \mathbb{Z}_4$ é homomorfismo, se e somente se, $\overline{\overline{a}} = \overline{\overline{0}}$ ou $\overline{\overline{a}} = \overline{\overline{2}}$.*

### 2.2.2 Teoria de Anéis

Serão apresentados nesta seção, as principais definições e resultados acerca da Teoria dos Anéis que nos serão úteis, na tentativa de fazer com que o entendimento do resultado principal se torne o mais simples e claro possível.

**Definição 2.11** (Anéis)**.** *Seja um conjunto não vazio $A$ munido de duas operações de adição "+"e multiplicação ".". Chamamos esse conjunto $A$ de* ***anel*** *quando as seguintes propriedades são satisfeitas:*

**(i)** *$(A, +)$ é um grupo abeliano;*

**(ii)** *A multiplicação é associativa, ou seja,*

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z, \forall x, y, z \in A.$$

**(iii)** *A multiplicação é distributiva sobre a adição, isto é,*

$$x \cdot (y + z) = x \cdot y + x \cdot z \text{ e } (x + y) \cdot z = x \cdot z + y \cdot z, \ \forall x, y, z \in A$$

**Exemplo 2.8.** *$\mathbb{Z}_m$ com a soma e produto usuais é anel. Pelo exposto no Teorema 2.5, para que as condições da definição anterior sejam satisfeitas, resta mostrar o item (iii). Seja $\overline{x}, \overline{y}, \overline{z} \in \mathbb{Z}_m$, então*

$$\overline{x} \cdot (\overline{y} + \overline{z}) = \overline{x} \cdot (\overline{y + z}) = \overline{x \cdot (y + z)} = \overline{x \cdot y + x \cdot z} = \overline{x \cdot y} + \overline{x \cdot z} = \overline{x} \cdot \overline{y} + \overline{x} \cdot \overline{z}$$

*e*

$$(\overline{x} + \overline{y}) \cdot \overline{z} = (\overline{x + y}) \cdot \overline{z} = \overline{(x + y) \cdot z)} = \overline{x \cdot z + y \cdot z} = \overline{x \cdot z} + \overline{y \cdot z} = \overline{x} \cdot \overline{z} + \overline{y} \cdot \overline{z}$$

*Portanto, o item (iii) da definição é satisfeito, sendo assim, $\mathbb{Z}_m$ com a soma e produto é anel.*

**Definição 2.12.** *Sejam $A_1$ e $A_2$ anéis. Uma aplicação $f : A_1 \to A_2$ chama-se* ***homomorfismo de Anéis*** *entre $A_1$ e $A_2$ quando as seguintes condições são satisfeitas:*

**a)** *$f(a + b) = f(a) + f(b)$, para quaisquer $a, b \in A_1$.*

**b)** *$f(a \cdot b) = f(a) \cdot f(b)$, para quaisquer $a, b \in A_1$.*

Na condição (a) da definição anterior, a adição do lado esquerdo $(a+b)$ refere-se naturalmente à adição do anel $A_1$, enquanto a adição do lado direito $(f(a)+f(b))$ corresponde à adição do anel $A_2$. O mesmo comentário vale para a multiplicação em (b).

**Observação 2.7.** Segue do fato de $(A_1, +)$ ser grupo e do item (a) da Definição anterior que todo homomorfismo de anéis é também um homomorfismo de grupos. Em particular, da Observação 2.6 todo homomorfismo de $\mathbb{Z}_m$ em $\mathbb{Z}_n$ é da forma $f(\overline{x}) = \overline{\overline{a}}x$.

**Exemplo 2.9.** Da observação anterior e do Exemplo 2.6, as únicas possibilidades para a aplicação $g : \mathbb{Z}_4 \to \mathbb{Z}_6$ dada por $g(\bar{x}) = \overline{\overline{ax}}$, para $\overline{x} \in \mathbb{Z}_4$ ser um homomorfismo de grupos, acontecem quando $\overline{\overline{a}} = \overline{\overline{0}}$ ou $\overline{\overline{a}} = \overline{\overline{3}}$.

Se $\overline{\overline{a}} = \overline{\overline{0}}$, então

$$g(\bar{x}) = \overline{\overline{0}}, \quad \text{para todo } \overline{x} \in \mathbb{Z}_4$$

e, nesse caso, $g$ é claramente homomorfismo de anéis, chamado de **Homomorfismo Trivial**.

Se $\overline{\overline{a}} = \overline{\overline{3}}$, então

$$g(\bar{x}) = \overline{\overline{3x}}, \quad \text{para todo } \overline{x} \in \mathbb{Z}_4$$

e, aqui $g$ também é um homomorfismo de anéis. De fato, temos

$$g(\overline{0}) = \overline{0}, g(\overline{1}) = \overline{3}, g(\overline{2}) = \overline{0} \text{ e } g(\overline{3}) = \overline{3},$$

daí, para $\overline{x}, \overline{y} \in \mathbb{Z}_4$:

Se $\overline{x} = \overline{0}$, então $g(\overline{0} \cdot \overline{y}) = g(\overline{0}) = \overline{\overline{0}} = g(\overline{0})g(\overline{y})$

Se $\overline{x} = \overline{1}$, então $g(\overline{1} \cdot \overline{y}) = g(\overline{y}) = \overline{\overline{3}} \cdot \overline{y} = \overline{\overline{9}} \cdot \overline{y} = \overline{\overline{3}} \cdot \overline{\overline{3}} \cdot \overline{y} = g(\overline{1})g(\overline{y})$

Se $\overline{x} = \overline{2}$, então

$$\overline{2} \cdot \overline{y} = \begin{cases} \overline{0}, \text{ se } \overline{y} = \overline{2} \text{ ou } \overline{y} = \overline{0} \\ \overline{2}, \text{ se } \overline{y} = \overline{1} \text{ ou } \overline{y} = \overline{3} \end{cases}$$

Portanto, $g(\overline{2} \cdot \overline{y}) = \overline{\overline{0}} = \overline{\overline{0}}g(\overline{y}) = g(\overline{2})g(\overline{y})$. Como a operação de produto é comutativa em $\mathbb{Z}_n$ e $\mathbb{Z}_m$, então $g$ é homomorfismo de anéis.

Agora, fazendo a mesma análise para o Exemplo 2.7, vamos ter dois homomorfismos de grupos, assim como no exemplo anterior, porém apenas um deles é homomorfismo de anéis. Com efeito, dada a função $g : \mathbb{Z}_2 \to \mathbb{Z}_4$ definida por $g(\bar{x}) = \overline{\overline{ax}}$, para $\overline{x} \in \mathbb{Z}_2$ ser um homomorfismo de grupos, acontecem quando $\overline{\overline{a}} = \overline{\overline{0}}$ ou $\overline{\overline{a}} = \overline{\overline{2}}$.

Se $\overline{\overline{a}} = \overline{\overline{0}}$, então

$$g(\bar{x}) = \overline{\overline{0}}, \quad \text{para todo } \overline{x} \in \mathbb{Z}_2$$

e, nesse caso, $g$ é claramente homomorfismo de anéis, o chamado **Homomorfismo Trivial**.

Se $\overline{\overline{a}} = \overline{\overline{2}}$, então

$$g(\bar{x}) = \overline{\overline{2x}}, \quad \text{para todo } \overline{x} \in \mathbb{Z}_2$$

e, aqui $g$ nesse caso não é um homomorfismo de anéis, pois

$$g(\overline{0}) = \overline{\overline{0}} \text{ e } g(\overline{1}) = \overline{\overline{2}},$$

Agora, fazendo $g(\overline{1} \cdot \overline{1}) = g(\overline{1}) = \overline{\overline{2}}$. Por outro lado, $g(\overline{1})g(\overline{1}) = \overline{\overline{2}} \cdot \overline{\overline{2}} = \overline{\overline{0}}$. Como $g(\overline{1} \cdot \overline{1}) = \overline{\overline{2}} \neq \overline{\overline{0}} = g(\overline{1})g(\overline{1})$, então para $\overline{\overline{a}} = \overline{\overline{0}}$, a função dada não define um homomorfismo de anel.

O Teorema que apresentaremos no próximo capítulo indica quando $g : \mathbb{Z}_m \longrightarrow \mathbb{Z}_n$ dada por $g(\overline{x}) = \overline{\overline{ax}}$ é homomorfismo de anéis e quantifica os $\overline{\overline{a}} \in \mathbb{Z}_m$ que fazem de $g$ um homomorfismo de anéis, isto é, diz exatamente quantos homomorfismos de anéis existem entre os anéis $\mathbb{Z}_m$ e $\mathbb{Z}_n$

# 3. O número de homomorfismos de anéis de $\mathbb{Z}_m$ em $\mathbb{Z}_n$

Neste Capítulo, nosso objetivo é determinar o número de homomorfismos de anéis existentes entre $\mathbb{Z}_m$ e $\mathbb{Z}_n$, utilizando os resultados que enunciamos no capítulo anterior. As ideias aqui apresentadas foram retiradas de Diaz-Vargas e Santos (2015) que, por sua vez, se baseou em Gallian e Buskirk (1984).

Gallian e Buskirk provaram que existem exatamente $2^{\omega(n)-\omega(k)}$ homomorfismos de anéis entre $\mathbb{Z}_m$ e $\mathbb{Z}_n$, em que $k = n/mdc(m,n)$ e $\omega(a)$ é a quantidade de números primos existentes na fatoração de um número inteiro $a$. A prova feita por eles utiliza muitos resultados da Teoria de Anéis, tais como decomposição em soma direta, propriedades de elementos idempotentes, entre outros. Já a prova apresentada por Diaz-Vargas e Santos, utiliza apenas a definição de homomorfismos e majoritariamente resultados de Teoria dos Números, tornando-a mais acessível e, por este motivo, essa é a prova que vamos apresentar aqui.

Chamamos a atenção que, no enunciado proposto por Diaz-Vargas e Santos, a quantidade procurada é $2^l$ em que $l = \#\{i; \alpha_i \leq \beta_i\}$ e os $\alpha_i's$, $\beta_i's$ são expoentes na decomposição em primos de $m, n$. Em verdade, e como esperado, $2^{\omega(n)-\omega(k)}$ e $2^l$ são iguais.

De fato, sejam $m, n \in \mathbb{N}$ e considere $m = p_1^{\beta_1} \cdots p_r^{\beta_r}$ a sua fatoração canônica e $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r} q$ que pode ser escrito assim, devido a Observação 2.3.
Daí,

$$mdc(m,n) = p_1^{\gamma_1} \cdots p_r^{\gamma_r}, \text{ com } \gamma_i = min\{\alpha_i, \beta_i\}$$

logo,

$$k = \frac{n}{mdc(n,m)} = \frac{p_1^{\alpha_1} \cdots p_r^{\alpha_r} q}{p_1^{\gamma_1} \cdots p_r^{\gamma_r}} \tag{3.1}$$

Se $\alpha_j = \gamma_j$, então o primo $p_j$ não estará na fatoração de $k$, como se vê facilmente por 3.1, isto é, se $\alpha_j \leq \beta_j$, o primo $p_j$ não estará na fatoração de $k$. Assim,

$$\omega(k) = \omega(n) - \#\{i; \alpha_i = \gamma_i\} = \omega(n) - \#\{i; \alpha_i \leq \beta_i\} = \omega(n) - l$$

Portanto,

$$l = \omega(n) - \omega(k).$$

Para atingir nosso objetivo, precisamos ainda de alguns resultados auxiliares que serão apresentados a seguir:

**Lema 3.1.** *A aplicação $g_a : \mathbb{Z}_n \to \mathbb{Z}_m$ dada por $g(\overline{x}) = \overline{\overline{ax}}$, para $\overline{x} \in \mathbb{Z}_n$, com $\overline{\overline{a}} \in \mathbb{Z}_m$ fixado, é um homomorfismo de anéis se, e somente se,*

$$na \equiv 0(modm) \quad e \quad a \equiv a^2(modm). \tag{3.2}$$

**Prova:** Suponha que $g_a(\overline{x}) = \overline{\overline{ax}}$, para $\overline{x} \in \mathbb{Z}_n$, é um homomorfismo de anéis então, da Observação 2.7, $g_a$ é um homomorfismo de grupos e da Observação 2.6, $na \equiv 0(modm)$. Ainda da Observação 2.6, $\overline{\overline{a}} = g_a(\overline{1})$ e da segunda condição na Definição de Homomorfismo de Anéis, temos

$$\overline{\overline{a}} = g_a(\bar{1}) = g_a(\bar{1}^2) = g_a(\bar{1})^2 = \overline{\overline{a}}^2 \quad \text{em } \mathbb{Z}_m,$$

ou seja,

$$a \equiv a^2(modm).$$

Reciprocamente, se $a \in \mathbb{Z}$ satisfaz (3.2, devemos provar que $g_a$ é homomorfismo de anéis, ou seja, estamos supondo que $na \equiv 0(modm)$ e $a \equiv a^2(modm)$. Da Observação 2.6, já sabemos que dados $\bar{x}, \bar{y} \in \mathbb{Z}_n$, temos $g_a(\bar{x}+\bar{y}) = g_a(\bar{x})+g_a(\bar{y})$ desde que $na \equiv 0(modm)$. Na divisão de $xy$ por $n$ pelo Algoritmo da divisão, existem $k, r \in \mathbb{Z}$ tais que $xy = nk + r$ com $0 \leq r < n$, logo $xy \equiv r(modn)$ e, portanto,

$$g_a(\overline{xy}) = g_a(\overline{nk} + \overline{r}) = g_a(\overline{0} + \overline{r}) = g_a(\overline{r}) = \overline{\overline{ar}} = \overline{\overline{a(xy - nk)}}.$$

Como $xy - nk \equiv xy(modm)$ e $a \equiv a^2(modm)$, por (3.2), da Proposição 2.6, temos

$$axy - ank \equiv a^2xy(modm)$$

logo,

$$g_a(\overline{xy}) = \overline{\overline{a(xy - nk)}} = \overline{\overline{a^2xy}} = (\overline{\overline{ax}})(\overline{\overline{ay}}) = g_a(\overline{x})g_a(\overline{y}) \ \text{ em } \mathbb{Z}_m.$$

Portanto, $g_a$ é um homomorfismo de anéis.

□

A fim de encontrar o número de homomorfismo de anéis de $\mathbb{Z}_m$ em $\mathbb{Z}_n$, devemos determinar o número de soluções do sistema de congruências no Lema 3.1. É nessa direção que apresentamos os resultados seguintes.

**Lema 3.2.** *Seja $f$ um polinômio de coeficientes inteiros. Se $x_0, a_1, m_1 \in \mathbb{Z}$ são tais que, $x_0 \equiv a_1(modm_1)$ e $f(x_0) \equiv 0(modm_1)$, então $f(a_1) \equiv 0(modm_1)$.*

**Prova:**: Da hipótese $x_0 \equiv a_1(mod m_1)$, existe $q \in \mathbb{Z}$ tal que $x_0 = m_1 q + a_1$.

Escrevendo $f(x) = \alpha_k x^k + \alpha_{k-1}x^{k-1} + ... + \alpha_1 x + \alpha_0$, com $\alpha_i \in \mathbb{Z}, 0 \leq i \leq k$ e aplicando em $x = x_0 = qm_1 + a_1$, temos

$$f(x_0) = f(qm_1 + a_1)^k = \alpha_k(qm_1 + a_1)^k + \alpha_{k-1}(qm_1 + a_1)^{k-1} + ... + \alpha_1(qm_1 + a_1) + \alpha_0.$$

Usando a fórmula do Binômio de Newton para $(qm_1 + a_1)^n$, segue que

$$\begin{aligned}
(qm_1 + a_1)^k &= c_k^0 a_1^0 m_1^k q^k + c_k^1 a_1^1 (m_1 q)^{k-1} + c_k^2 a_1^2 (m_1 q)^{k-2} + ... + c_k^k a_1^k (m_1 q)^0 \\
&= m_1^k q^k + c_k a_1^1 m_1^{k-1} q^{k-1} + c_k^2 a_1^2 m_1^{k-2} q^{k-2} + ... + a_1^k \\
&= m_1(m^{k-1} q^k + c_k^1 a_1 m_1^{k-2} q^{k-1} + c_k^2 a_1^2 m^{k-3} q^{k-2} + ... + c_k^{k-1} a_1^{k-1} q) + a_1^k \\
&= m_1 t + a_1^k,
\end{aligned}$$

em que $t = m^{k-1}q^k + c_k^1 a_1 m_1^{k-2} q^{k-1} + c_k^2 a_1^2 m^{k-3} q^{k-2} + ... + c_k^{k-1} a_1^{k-1} q \in \mathbb{Z}$ e $c_k^j = \binom{k}{j}$ são os números binomiais, para $0 = 1, \cdots, k$. Dessa igualdade, concluímos que

$$(m_1 q + a_1)^k \equiv a_1^k (mod m_1).$$

Analogamente, podemos concluir que,

$$\begin{aligned}
(m_1 q + a_1)^{k-1} &\equiv a_1^{k-1} (\text{mod } m_1) \\
(m_1 q + a_1)^{k-2} &\equiv a_1^{k-2} (\text{mod } m_1) \\
&\vdots \\
(m_1 q + a_1) &\equiv a_1 (\text{mod } m_1).
\end{aligned}$$

Do Item (iii) da Proposição 2.6 e da reflexividade da relação de congruência, temos

$$\begin{aligned}
\alpha_k(m_1 q + a_1)^k &\equiv \alpha_k a_1^k (mod m_1) \\
\alpha_{k-1}(m_1 q + a_1)^{k-1} &\equiv \alpha_{k-1} a_1^{k-1} (\text{mod } m_1) \\
\alpha_{k-2}(m_1 q + a_1)^{k-2} &\equiv \alpha_{k-2} a_1^{k-2} (\text{mod } m_1) \\
&\vdots \\
\alpha_1(m_1 q + a_1) &\equiv \alpha_1 a_1 (\text{mod } m_1) \\
\alpha_0 &\equiv \alpha_0 (\text{mod } m_1).
\end{aligned}$$

Agora, do Item (i) da Proposição 2.6, segue que

$$\begin{aligned}
\alpha_k(m_1 q + a_1)^k \quad &+\alpha_{k-1}(m_1 q + a_1)^{k-1} + \alpha_{k-2}(m_1 q + a_1)^{k-2} + ... + \alpha_1(m_1 q + a_1) + \alpha_0 \\
&\equiv \alpha_k a_1^k + \alpha_{k-1} a_1^{k-1} + \alpha_{k-2} a_1^{k-2} + ... + \alpha_1 a_1 + \alpha_0 (\text{mod } m_1)
\end{aligned},$$

e podemos concluir que $f(x_0) = f(m_1 q + a_1) \equiv f(a_1)(mod m_1)$.

Portanto, como $f(x_0) \equiv f(a_1)(\text{mod } m_1)$ e $f(x_0) \equiv 0(\text{mod } m_1)$, por hipótese, então

$$f(a_1) \equiv 0(\text{mod } m_1).$$

□

**Teorema 3.1.** *Sejam $f_1, f_2, ..., f_k$ polinômios com coeficientes inteiros e, para $m > 1$, inteiro, denote $N(m)$ como sendo o número de soluções do sistema de congruências*

$$\begin{aligned} f_1(x) &\equiv 0 \quad (modm), \\ f_2(x) &\equiv 0 \quad (modm), \\ &\vdots \\ f_k(x) &\equiv 0 \quad (modm). \end{aligned} \tag{3.3}$$

*Se $m = m_1 m_2$, com $mdc(m_1 m_2) = 1$, então $N(m) = N(m_1)N(m_2)$. Se $m = \prod_{i=1}^{r} p_i^{\alpha_i}$ é a fatoração de $m$ em fatores primos, então, $N(m) = \prod_{i=1}^{r} N(p_i^{\alpha_i})$.*

**Prova:** Para a prova do Teorema, a ideia principal é mostrar que para cada $x \in \mathbb{Z}$ satisfazendo o sistema (3.3), existe um par $(a_1, a_2) \in \mathbb{Z}\times\mathbb{Z}$ de tal modo que $x \equiv a_i(modm_i)$ e $a_i$ satisfaz, para $i = 1, 2$,

$$\begin{aligned} f_1(a_i) &\equiv 0 \quad (modm_i), \\ f_2(a_i) &\equiv 0 \quad (modm_i), \\ &\vdots \\ f_k(a_i) &\equiv 0 \quad (modm_i), \end{aligned} \tag{3.4}$$

e vale a recíproca, isto é, se $a_i \in \mathbb{Z}$, $i = 1, 2$ satisfaz (3.4), então existe $x \in \mathbb{Z}$, tal que $x \equiv a_i(modm_i)$, para $i = 1, 2$ e $x$ satisfaz (3.3).

Seja $x \in \mathbb{Z}$, tal que vale 3.3

com $m = m_1 m_2$, assim,

$$f_1(x) = q_1 m = (q_1 m_2)m_1$$

para algum $q_1 \in \mathbb{Z}$, ou seja, $f_1(x) \equiv 0(modm_1)$ e, de forma análoga, para $f_2(x), ..., f_k(x)$.

Por conseguinte, seja $\overline{a_1} \in \mathbb{Z}_{m_1}$ tal que $x \equiv a_1(modm_1)$. Note que $\overline{a_1}$ é único nessas condições, já que a relação de Congruência é de Equivalência em $\mathbb{Z}$. Pelo Lema anterior, $f_1(a_1) \equiv 0(modm_1)$, $f_2(a_1) \equiv 0(modm_1), ..., f_k(a_1) \equiv 0(modm_1)$. Do mesmo modo, temos a existência de $\overline{a_2} \in \mathbb{Z}_{m_2}$ tal que $x \equiv a_2(modm_2)$ e $f_1(a_2) \equiv 0(modm_2), ..., f_k(a_k) \equiv 0(modm_2)$. Portanto, se $x$ é solução do sistema de congruências módulo $m$, temos um par $(a_1, a_2)$, no qual $a_i$ é uma solução do sistema de congruências módulo $m_i$, para $i = 1, 2$, o que prova a primeira parte do teorema.

Para a segunda parte, sejam $a_1$ e $a_2$ satisfazendo (3.4), para $i = 1, 2$, respectivamente. Pelo Teorema Chinês do Resto (Teorema 2.4), já que $mdc(m_1, m_2) = 1$, existe $x \in \mathbb{Z}$ tal

que

$$x \equiv a_1(modm_1) \text{ e } x \equiv a_2(modm_2)$$

e $x$ é único módulo $m$. Do Lema anterior, concluímos que $x$ satisfaz simultaneamente (3.4) para $i = 1$ e $i = 2$. Assim,

$$m_1|f_j(x) \text{ e } m_2|f_j(x),$$

para $j = 1, \cdots, k$. Como $mdc(m_1, m_2) = 1$, do Corolário 2.1, segue que

$$m = m_1m_2|f_j(x)$$

para $j = 1, \cdots, k$ e $x$ satisfaz (3.3), como queríamos.

Da relação apresentada acima, temos

$$N(m) = N(m_1)N(m_2)$$

e o Teorema é válido. Ademais, se $m = \prod_{i=1}^{r} p_i^{\alpha_i}$ é a fatoração de $m$ em fatores primos dada pelo Teorema Fundamental da Aritmética (Teorema 2.3), então, $mdc(p_i, p_j) = 1$, para $i \neq j$ e, da primeira parte, $N(m) = \prod_{i=1}^{r} N(p_i^{\alpha_i})$.

□

Neste momento, com base no último teorema visto, como também todos os conceitos preliminares apresentados até então, enunciamos o resultado principal do nosso trabalho, que é justamente uma análise feita para encontrar o número de homomorfismo existentes entre os anéis $\mathbb{Z}_n$ e $\mathbb{Z}_m$.

**Teorema 3.2.** *Sejam $m, n \in \mathbb{Z}, m, n > 1$. Se $m = p_1^{\alpha_1}p_2^{\alpha_2}...p_r^{\alpha_r}$ é a fatoração canônica de $m$ e $n = p_1^{\beta_1}p_2^{\beta_2}...p_r^{\beta_r}q$ com $mdc(q, m) = 1$, então número de homomorfismos de anéis $g : \mathbb{Z}_m \to \mathbb{Z}_n$ de $\mathbb{Z}_n$ é $2^k$, em que $k = \#\{i; \alpha_i \leq \beta_i\}$.*

**Prova:** Seja $g : \mathbb{Z}_m \to \mathbb{Z}_n$ um homomorfismo de anéis. Da Observação 2.7,$g$ é também um homomorfismo de grupos, logo, da Observação 2.6, $g = g_a$, para algum $\overline{\overline{a}} \in \mathbb{Z}_n$, em que

$$\begin{array}{rccc} g_a: & \mathbb{Z}_m & \longrightarrow & \mathbb{Z}_n \\ & \overline{x} & \mapsto & g_a(\overline{x}) = \overline{\overline{ax}}. \end{array}$$

Do Lema 3.1, $a$ satisfaz

$$na \equiv 0(modm) \quad \text{e} \quad a \equiv a^2(modm).$$

Assim, para provar o Teorema basta saber quantas soluções existem para o sistema acima.

Considerando $f_1(x) = nx$ e $f_2(x) = x - x^2$, para $x \in \mathbb{Z}$, então estamos nas condições

do Teorema 3.1, logo, se $N(m)$ é a quantidade de soluções do sistema

$$f_1(x) \equiv 0(modm) \quad \text{e} \quad f_2(x) \equiv 0(modm), \tag{3.5}$$

então

$$N(m) = \prod_{i=1}^{r} N(p_i^{\alpha_i}),$$

ou seja, precisamos descobrir o valor de $N(p_i^{\alpha_i})$, para $i = 1, \cdots, r$.

Sejam $p$ um número primo, $a > 0$ e $\alpha > 0$ inteiros satisfazendo

$$a(a-1) = a^2 - a \equiv 0(modp^{\alpha}).$$

Nesse caso, $a \equiv 0(modp^{\alpha})$ ou $a \equiv 1(modp^{\alpha})$.

De fato, desde que $mdc(a, a-1) = 1$, pela Proposição 2.4 apenas um dos termos, $a$ ou $a-1$, pode ser divisível por $p$, então $mdc(p^{\alpha}, a) = 1$ ou $mdc(p^{\alpha}, a-1) = 1$. Se $mdc(p^{\alpha}, a) = 1$, como $p^{\alpha}|a(a-1)$, do Teorema de Euclides (Teorema 2.2), $p^{\alpha}|(a-1)$, daí $a \equiv 1(modp^{\alpha})$. Analogamente, se $mdc(p^{\alpha}, a-1) = 1$, então $p^{\alpha}|a$ e daí, $a \equiv 0(modp^{\alpha})$.

Mas, 1 é solução de $f_1(x) \equiv 0(modp^{\alpha})$ se, e somente se, $p^{\alpha}|n$, enquanto 0 é sempre uma solução. Portanto, o sistema de congruências

$$f_1(x) \equiv 0(modp^{\alpha}), f_2(x) \equiv 0(modp^{\alpha})$$

tem duas soluções se $p^{\alpha}|n$. Caso contrário, o sistema de congruências tem uma única solução (módulo $p^{\alpha}$).

Assim, se $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ é a fatoração canônica de $m$ e $n = p_1^{\beta_1} p_2^{\beta_2} ... p_r^{\beta_r} q$ com $mdc(q, m) = 1$, o número de soluções $N(p_i^{\alpha_i})$ para

$$f_1(x) \equiv 0(modp_i^{\alpha_i}) \quad \text{e} \quad f_2(x) \equiv 0(modp_i^{\alpha_i}),$$

com $i = 1, \cdots, r$, é dado por

$$N(p_i^{\alpha_i}) = \begin{cases} 2, \text{ se } p_i^{\alpha_i}|n \\ 1, \text{ se } p_i^{\alpha_i} \nmid n \end{cases}$$

Então, o número de soluções é

$$N(m) = \prod_{i=1}^{r} N(p_i^{\alpha_i}) = \prod_{p_i^{\alpha_i}|n} 2 = \prod_{\alpha_i \leq \beta_i} 2 = 2^k,$$

em que $k = \#\{i; \alpha_i \leq \beta_i\}$, é o número de elementos no conjunto $\{i; \alpha_i \leq \beta_i\}$.

□

# 4. Considerações Finais

Este trabalho objetivou apresentar um resultado que determina o número de homomorfismo existentes entre os anéis $\mathbb{Z}_m$ e $\mathbb{Z}_n$. Ele originou-se a partir do nosso contato com as disciplinas de Teoria dos Números e Estruturas Algébricas, durante o curso de Licenciatura em Matemática oferecido pela Universidade Estadual da Paraíba - Campus I.

Desde então, dada a complexidade da Álgebra Abstrata, bem como sua relevância em se tratando dos estudos matemáticos na academia, surgiu a necessidade de aprofundar-se ainda mais nesse ramo. Outro motivo que justifica e norteia a escolha do tema é o fato de, no curso supracitado, não estudarmos a parte de anéis em estruturas algébricas, o que também originou dificuldades no desenvolvimento do trabalho, haja vista a precariedade no contato com tais teorias, o que não impossibilitou sua concretude.

Com base nos artigos em estudo, percebemos que não existe uma única forma de provar o resultado que fornece a quantidade de homomorfismos existentes entre os anéis $\mathbb{Z}_m$ e $\mathbb{Z}_n$, tampouco de enunciar tal resultado. Entretanto, é necessário chegar ao mesmo número, o que de fato acontece, como vimos no Capítulo final do nosso texto. Verificou-se, ainda, que é possível determinar o número de homomorfismos existentes entre $\mathbb{Z}_m$ e $\mathbb{Z}_n$, através de apenas alguns conceitos simples da Teoria dos Números, da Teoria dos grupos, como também alguns conceitos da Teoria dos Anéis.

Nesse sentido, espera-se colaborar com a produção de conhecimento científico,ao passo que fornecemos aqui uma abordagem didática para apresentação de um resultado que, em geral, não encontra-se em livros didáticos de Álgebra Abstrata. Além disso, contribuímos no sentido de subsidiar uma formação mais segura e sólida ao Professor ao atuar em sala de aula diante desses objetos de conhecimento, bem como sua relevância para sua formação algébrica.

# Referências Bibliográficas


BAUMGART, J. K. Álgebra. In: *Tópicos de história da matemática para uso em sala de aula*. São Paulo: Atual, 1992.

DIAZ-VARGAS, J.; SANTOS, G. V. de los. The number of homomorphisms from $\mathbb{Z}_n$ to $\mathbb{Z}_m$. *Abstraction & Application*, n. 13, p. 1–3, 2015.

DOMINGUES, H. H. *Álgebra Moderna*. 4. ed. São Paulo: Atual Editora, 2003.

GALLIAN, J. A.; BUSKIRK, J. V. The number of homomorphisms from $\mathbb{Z}_n$ to $\mathbb{Z}_m$. *The American Mathematical Monthly*, v. 91, n. 3, p. 196–197, Mar 1984.

GARCIA, A. I.; LEQUAIN, Y. *Elementos de Álgebra*. Rio de Janeiro: IMPA, 2018. 363 p.

HEFEZ, A. Aritmética. In: *PROFMAT*. Rio de Janeiro: SBM, 2014. 338 p.

MILIES, C. P. Breve História da Álgebra Abstrata. In: *II Bienal da SBM*. Salvador: [s.n.], 2004. Disponível em <www.bienasbm.ufba.br/M18.pdf>. Acesso em 02 de Dezembro de 2020.

MILIES, C. P.; COELHO, S. P. *Números. Uma Introdução à Matemática*. São Paulo: Edusp, 2006. 248 p.

SANTOS, J. G. L. *Analisando os homomorfimos de $\mathbb{Z}_m$ em $\mathbb{Z}_n$*. Monografia (Trabalho de Conclusão de Curso) — Universidade Estadual da Paraíba, Curso de Licenciatua Plena em Matemática, Campina Grande, 2018.

SANTOS, J. P. O. *Introdução à Teoria dos Números*. Rio de Janeiro: IMPA, 2017. 196 p.

VIEIRA, V. L. *Álgebra Abstrata para Licenciatura*. Campina Grande: EDUEPB, 2013. 613 p.

VIEIRA, V. L. *Um curso Básico em Teoria dos Números*. Campina Grande: EDUEPB, 2015. 560 p.