UNIVERSIDADE FEDERAL DE SANTA CATARINA
CAMPUS BLUMENAU
LICENCIATURA EM MATEMÁTICA

Aline Kowalski

Elementos primos e elementos irredutíveis do anel de inteiros módulo n

Blumenau
2022

Aline Kowalski

Elementos primos e elementos irredutíveis do anel de inteiros módulo n

Trabalho de Conclusão de Curso de Graduação em Licenciatura em Matemática do Campus Blumenau da Universidade Federal de Santa Catarina para a obtenção do título de Licenciado(a) em Matemática.
Orientador: Prof. Felipe Vieira, Dr.

Blumenau
2022

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Kowalski, Aline
Elementos primos e elementos irredutíveis do anel de inteiros módulo n / Aline Kowalski ; orientador, Felipe Vieira, 2022.
85 p.

Trabalho de Conclusão de Curso (graduação) - Universidade Federal de Santa Catarina, Campus Blumenau, Graduação em Matemática, Blumenau, 2022.

Inclui referências.

1. Matemática. 2. Anéis dos inteiros módulo n. 3. Elementos Primos. 4. Elementos Irredutíveis. I. Vieira, Felipe. II. Universidade Federal de Santa Catarina. Graduação em Matemática. III. Título.

Aline Kowalski

Elementos primos e elementos irredutíveis do anel de inteiros módulo n

Este Trabalho de Conclusão de Curso foi julgado adequado para obtenção do Título de Licenciado(a) em Matemática e aprovado em sua forma final pelo Curso de Licenciatura em Matemática.

Blumenau, 30 de novembro de 2022.

Documento assinado digitalmente
Francis Felix Cordova Puma
Data: 14/12/2022 16:27:42-0300
CPF: ***.649.087-**
Verifique as assinaturas em https://v.ufsc.br

Prof. Francis Felix Cordova Puma, Dr(a).
Coordenador do Curso

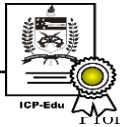
Banca Examinadora:

Documento assinado digitalmente
Felipe Vieira
Data: 14/12/2022 14:03:42-0300
CPF: ***.601.639-**
Verifique as assinaturas em https://v.ufsc.br

Prof. Felipe Vieira, Dr.
Orientador
Universidade Federal de Santa Catarina - UFSC

Documento assinado digitalmente
Rafael Aleixo de Carvalho
Data: 14/12/2022 15:36:04-0300
CPF: ***.494.178-**
Verifique as assinaturas em https://v.ufsc.br

Prof. Rafael Aleixo de Carvalho, Dr.
Avaliador
Universidade Federal de Santa Catarina - UFSC



Documento assinado digitalmente
Renan Gambale Romano
Data: 14/12/2022 14:55:47-0300
CPF: ***.828.658-**
Verifique as assinaturas em https://v.ufsc.br

Prof. Renan Gambale Romano, Dr.
Avaliador
Universidade Federal de Santa Catarina - UFSC

Este trabalho é dedicado aos meus pais, Alcir e Rosa.

AGRADECIMENTOS

Aos meus pais por todo amor, carinho, compreensão, apoio e incentivo dados. Sem isso e sem vocês, eu nada seria. Além disso, é graças ao seus esforços que hoje posso concluir esta graduação.

Ao meu orientador, este que esteve presente desde meu primeiro semestre e sempre me incentivou, auxiliou de 52! maneiras diferentes e sempre compartilhou fofocas edificantes. Meu eterno agradecimento por acreditar em meu potencial mesmo quando eu não o fazia.

Aos professores Louise, LR e Aleixo, que sempre ofereceram um abraço e uma palavra amiga quando necessária em todos estes anos de graduação.

Ao meu companheiro Lucca, por todos os momentos compartilhados durante essa jornada e por nunca deixar de acreditar em mim. Obrigada por tudo e por tanto, você ilumina meus dias.

Ao meu amigo Victor, por ser meu parceiro de estudos e por mostrar que a graduação podia ser divertida, mesmo que o motivo do riso fôssemos nós mesmos. Sem você a jornada não teria sido a mesma.

Aos meus amigos Cleison, Nicoly e Bruna vocês tornaram esta caminhada mais leve e descontraída. Obrigada por me ajudarem tanto ao longo dela.

Aos meus amigos Aline, Manoela, Maria Eduarda e Gian por me ajudarem a descontrair e estarem presentes nos dias mais difíceis.

Aos demais professores e servidores da UFSC que de alguma forma contribuíram para minha formação, meu muito obrigada.

Além disso, sem os programas Probolsas, PIBIC e monitorias minha permanência e aproveitamento do curso não se dariam da mesma forma. Meu eterno agradecimento a estes programas.

Meu mais sicero agradecimento a todos que lutam por uma educação gratuita e de qualidade.

RESUMO

Este trabalho tem como objetivo discorrer sobre os elementos primos e os elementos irredutíveis de um anel de inteiros módulo n. Para isto, inicialmente discutiremos sobre os aspectos da teoria de anéis que são necessários para o estudo de tais conteúdos. Em seguida, demonstraremos as caracterizações de cada elemento em um anel $\mathbb{Z}_n$ arbitrário. Posteriormente, será provado como calcular a quantidade dos elementos cuja caracterização foi realizada.

Palavras-chave: Anéis dos inteiros módulo n. Elementos Primos. Elementos Irredutíveis.

ABSTRACT

This work aims to discuss the prime elements and the irreducible elements of a ring of integers modulo n. For this, we will initially discuss aspects of ring theory that are necessary for the study of such contents. Then, we will demonstrate the characterizations of each element in an arbitrary $\mathbb{Z}_n$ ring. Subsequently, it will be proved how to calculate the amount of the elements whose characterization was performed.

Keywords: Ring of integers modulo n. Prime Elements. Irreducible Elements.

SUMÁRIO

1 INTRODUÇÃO

A álgebra é um dos ramos da matemática cujo objetivo é estudar operações, equações, polinômios e estruturas algébricas. Nesta área, são elaboradas regras relativamente simples e estudamos os objetos que as satisfazem, como por exemplo, o caso dos anéis.

Neste trabalho, o leitor poderá se entreter com elementos primos e elementos irredutíveis de um anel, e em particular, de um anel $\mathbb{Z}_n$. Será esmiuçado o artigo científico [1], identificando e demonstrando os resultados necessários para compreensão das demonstrações propostas pelos autores quanto à caracterização de elementos primos e de elementos irredutíveis de um anel $\mathbb{Z}_n$ qualquer. Além disso, também demonstraremos com riqueza de detalhes cada teorema proposto no artigo, que são basicamente três: a caracterização dos elementos primos de $\mathbb{Z}_n$; a determinação dos elementos irredutíveis de $\mathbb{Z}_n$; e uma forma de efetuar a contagem dos conjuntos descritos nos dois primeiros teoremas.

O segundo capítulo é dedicado exclusivamente para conceitos iniciais e conceitos necessários para a compreensão dos principais teoremas do trabalho, os quais estão localizados no terceiro capítulo. Todas as proposições necessárias para realizar as demonstrações do Capítulo 3 encontram-se no Capítulo 2, e justamente para a melhor compreensão deste capítulo que serão abordados os temas: divisibilidade, máximo divisor comum (MDC), equações diofantinas, relação, conjunto quociente, congruência módulo n, classe de congruência, anéis, suas propriedades, subanéis, ideais e anel quociente.

No Capítulo 3, serão abordados os conteúdos principais do trabalho: elementos primos e elementos irredutíveis de um anel de inteiros módulo n, e foi inteiramente baseado em [1]. No Capítulo 4 serão apresentadas as considerações finais do trabalho.

Para melhor entendimento deste trabalho, estamos considerando que o leitor tenha conhecimento prévio sobre as técnicas de demonstração por redução ao absurdo e demonstração por indução, além de conhecer e saber como operar com números inteiros, temas para os quais a autora indica a leitura das referências página 52 de [2], seção 0.1 de [3], capítulo 2 de [4], respectivamente.

2 CONCEITOS INICIAIS

Este capítulo busca abordar os conceitos necessários para o entendimento dos elementos primos e dos elementos irredutíveis dos anéis $\mathbb{Z}_n$ abordados no Capítulo 3 deste trabalho.

Assim, iniciaremos com a definição de alguns conceitos tais quais divisibilidade, máximo divisor comum e relação, além de resultados importantes referentes a estes temas. Aqui também serão abordados temas relacionados aos anéis, em particular, aos anéis $\mathbb{Z}_n$.

De forma geral, os resultados que serão demonstrados neste capítulo serão utilizados ou nos teoremas do Capítulo 3, ou a título de curiosidade para o leitor.

2.1 DIVISIBILIDADE

Definição 2.1. Dados $n, a \in \mathbb{Z}$, dizemos que n divide a ou que n é um divisor de a ou ainda que a é um múltiplo de n e escrevemos

$$n \mid a,$$

se existir $b \in \mathbb{Z}$ com $a = nb$. Caso n não divida a, escrevemos $n \nmid a$.

Exemplo 2.1.1. Veja que $5 \mid 15$, pois $15 = 5 \cdot 3$. Entretanto, $15 \nmid 5$, pois não existe um outro número inteiro que multiplicado por 15 resulte em 5.

Para demonstrarmos uma igualdade de dois números $a = b$, temos que demonstrar que $a \mid b$ e também que $b \mid a$, e vice e versa. Utilizaremos amplamente esta proposição ao longo deste trabalho.

Proposição 2.1. *Seja $a, b \in \mathbb{Z}$. Se $a \mid b$ e $b \mid a$, então $a = \pm b$.*

Demonstração. Por hipótese, $a \mid b$, ou seja, existe $x \in \mathbb{Z}$ tal que $b = ax$. E também, $b \mid a \iff a = by, y \in \mathbb{Z}$. Daí, substituindo,

$$a = (ax)y = a(xy).$$

Portanto, $xy = 1$, e isso só é possível no conjunto dos inteiros caso $x = y = 1$ ou $x = y = -1$. Assim, como $a = by$, temos que $a = b$ ou $a = -b$. ■

Tanto a Proposição 2.2 quanto a Proposição 2.3 serão utilizadas na demonstração do Teorema 3.2 na Seção 3.1.

Proposição 2.2. *Sejam $a, b \in \mathbb{Z}$. Se $a \mid b$ e $k \in \mathbb{Z}$, então $a \cdot k \mid b \cdot k$.*

Demonstração. Por hipótese, temos $a \mid b$, ou seja, $b = ax$ com $x \in \mathbb{Z}$. Veja que, ao multiplicar a igualdade por k, teremos $bk = axk$, ou seja, $bk = (ak)x$. ■

Exemplo 2.1.2. Sejam $a = 6$, $b = 18$ e $k = 7$, então veja que $6 \cdot 7 \mid 18 \cdot 7$. O que de fato ocorre, pois $18 \cdot 7 = (6 \cdot 7) \cdot 3$.

Proposição 2.3. *Sejam $p, b, c \in \mathbb{Z}$. Se $p \mid b$ e $p \mid c$, então $p \cdot p \mid b \cdot c$.*

Demonstração. Por hipótese, $p \mid b$, ou seja, $b = px$ com $x \in \mathbb{Z}$. Além disso, $p \mid c$, ou seja, $c = py$ em que $y \in \mathbb{Z}$. Daí, multiplicando a primeira igualdade pela segunda, obtemos $bc = px \cdot py = pp(xy)$, ou seja, $pp \mid bc$. ■

Exemplo 2.1.3. Sejam $p = 2$, $b = 6$ e $c = 8$. Veja que $2 \mid 6$ e que $2 \mid 8$, e ainda, que $2 \cdot 2 \mid 6 \cdot 8$, pois $6 \cdot 8 = (2 \cdot 2) \cdot 12$.

A proposição a seguir indica que se um número divide dois números inteiros a, b, então ele dividirá qualquer combinação linear destes números.

Proposição 2.4. *Em $\mathbb{Z}$, se $d \mid a$ e $d \mid b$, então $d \mid ax + by$.*

Demonstração. Como por hipótese, $d \mid a$ e $d \mid b$, temos pela definição de divisibilidade que existem $r, s \in \mathbb{Z}$ tais que $a = dr$ e $b = ds$. E ainda, multiplicando a primeira igualdade por x e a segunda por y, obtemos $ax = drx$ e $by = dsy$. Somando-as,

$$ax + by = drx + dsy = d(rx + sy).$$

Daí, obtivemos $ax+by$ como um múltiplo de d. Ou seja, $d \mid ax+by$. ■

Exemplo 2.1.4. Sejam $d = 5$, $a = 15$ e $b = 10$. Note que $a = 5 \cdot 3$ e $b = 5 \cdot 2$.
Daí, perceba que se a for multiplicado por um número x e b por y, teremos $ax = 5 \cdot 3 \cdot x$ e $by = 5 \cdot 2 \cdot y$. Somando as últimas igualdades, e colocando os fatores em evidência, obtemos

$$ax + by = 5 \cdot 3 \cdot x + 5 \cdot 2 \cdot y = 5(3 \cdot x + 2 \cdot y).$$

Veja que $5 \mid ax + by$, ou seja, $d \mid ax + by$.

Já a proposição a seguir mostra que se um inteiro q não divide outro inteiro b, e outro inteiro p o divide, então o produto entre p e q não dividirá b.

Proposição 2.5. *Sejam $a, b, n \in \mathbb{Z}$. Se $a \mid n$ e $b \nmid n$, então $ab \nmid n$.*

Demonstração. Suponha por absurdo que $ab \mid n$. Daí, temos que existe $x \in \mathbb{Z}$ tal que

$$n = xab = (xa)b,$$

ou seja n é um múltiplo de b, ou ainda, $b \mid n$. Absurdo, pois por hipótese, $b \nmid n$. ■

Exemplo 2.1.5. Veja que $2 \mid 10$ e $3 \nmid 10$. E ainda, $2 \cdot 3 = 6 \nmid 10$.

2.2 MÁXIMO DIVISOR COMUM (MDC)

Vale relembrar que todo número natural possui divisores, e que o menor divisor positivo de um número será sempre o número 1, enquanto o maior divisor de um número sempre será o próprio número.

Definição 2.2. Sejam $a, b \in \mathbb{Z}$ não simultaneamente nulos. Teremos

$$d = \text{mdc}(a, b) > 0$$

se

- $d \mid a$;
- $d \mid b$;
- Se $c \mid a$ e $c \mid b$, então $c \mid d$.

Como consequência da definição anterior, o máximo divisor comum entre dois números é o maior número natural que divide ambos, ou seja, é o maior de seus divisores.

E ainda, quando $\text{mdc}(a, b) = 1$, dizemos que a e b são coprimos, relativamente primos ou primos entre si.

A partir de agora, serão apresentadas as proposições necessárias para demonstrar o Lema 3.1, o Teorema 3.2 e o Teorema 3.4. A proposição a seguir nos aponta como lidar com o MDC entre dois números que tenham um fator em comum nas suas fatorações.

Proposição 2.6. *Sejam $a, b, n \in \mathbb{Z}^*$. Então,*

$$\text{mdc}(na, nb) = |n| \cdot \text{mdc}(a, b).$$

Demonstração. Seja $d = \text{mdc}(a, b)$. Pela definição de máximo divisor comum, temos

- $d \mid a$;
- $d \mid b$;
- se $c \mid a$ e $c \mid b$, então $c \mid d$.

Pela definição de divisibilidade, temos que $a = de$ e $b = df$, em que $d, f \in \mathbb{Z}$. Multiplicando cada igualdade por n, temos que $na = n(de) = (nd)e$ e $nb = n(df) = (nd)f$. Logo, novamente pela definição de divisibilidade,

$$nd \mid na$$

e

$$nd \mid nb.$$

Seja $k = \text{mdc}(na, nb)$. Novamente pela definição de máximo divisor comum,

- $k \mid na$;
- $k \mid nb$;
- se $h \mid na$ e $h \mid nb$, então $h \mid k$.

Contudo, sabemos que $nd \mid na$ e $nd \mid nb$, portanto pelo terceiro item anterior (basta tomar $h = nd$), $nd \mid k$[1]. Agora, veja que $n \mid nd$, assim, n deverá dividir também k, ou seja, existe $i \in \mathbb{Z}$ tal que $k = ni$. E, como $nd \mid k$, então $d \mid i$.
Entretanto, como $k = ni$ e $k = \text{mdc}(na, nb)$, então sabemos que $k \mid na$ e $k \mid nb$. Assim, considerando a primeira igualdade e as últimas duas relações, i deve dividir tanto a quanto b, ou seja, $i \mid a$ e $i \mid b$. E, como definimos $d = \text{mdc}(a, b)$, deveremos ter $i \mid d$ pelo terceiro item de sua definição (basta tomar $c = i$). Porém, se temos $i \mid d$ e $d \mid i$,

[1] Caso $nd > k$, então $\text{mdc}(na, nb) = nd$, que neste caso seria maior do que k, porém isto é um absurdo, já que $k = \text{mdc}(na, nb)$.

então $|i| = d$ pela Proposição 2.1 (lembre que d não é negativo). Mas como $k = ni$ e k é positivo temos que n e i devem ter o mesmo sinal, e visto que d também é positivo, temos que $k = ni$ implica em $k = |n| \cdot d = |n| \cdot \text{mdc}(a, b)$. Logo, $\text{mdc}(na, nb) = |n| \cdot \text{mdc}(a, b)$. ■

Exemplo 2.2.1. Sejam $n = 8$, $a = 16$ e $b = 31$. Note que

$$\begin{aligned}\text{mdc}(8 \cdot 16, 8 \cdot 31) &= \text{mdc}(2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2, 2 \cdot 2 \cdot 2 \cdot 31) \\ &= 2 \cdot 2 \cdot 2 \\ &= 8.\end{aligned}$$

E ainda, perceba que $\text{mdc}(16, 31) = 1$, e que

$$\text{mdc}(16, 31) \cdot 8 = 1 \cdot 8 = 8.$$

O corolário a seguir nos diz que se um número p divide dois inteiros a, n, então p também dividirá o MDC entre a e n.

Corolário 2.7. *Sejam $a, n, p \in \mathbb{Z}^*$. Se $\text{mdc}\,(a, n) = p$, então,*

$$\text{mdc}\left(\frac{a}{p}, \frac{n}{p}\right) = 1.$$

Para demonstrar um dos teoremas mais importantes deste trabalho, que nos resulta em quantos casos devemos quebrar a demonstração dos teoremas do Capítulo 3, demonstraremos os dois princípios a seguir.

Teorema 2.8 (Princípio da Boa Ordem)**.** *Todo subconjunto não vazio de números naturais possui um menor elemento.*

Demonstração. Conforme [4], suponha por absurdo que S seja um subconjunto não vazio do conjunto dos números naturais e que não tenha um menor elemento. Denote por S^C o conjunto complementar do conjunto S,

$$S^C = \mathbb{N} \backslash S = \{y \in \mathbb{N} : y \notin S\}.$$

Veja que se $0 \in S$, então 0 teria que ser o menor elemento de S, pois $\forall\, x \in \mathbb{N}, x \geq 0$, o que contradiz o fato de S não ter um menor elemento. Assim, $0 \notin S$, ou seja, $0 \in S^C$. Agora, suponha que $0, 1, \cdots, k \in S^C$. Daí, se $k+1 \in S$, então $k+1$ seria o menor elemento de S, o que é um absurdo também. Logo, $k+1 \in S^C$, ou seja, pelo Princípio da Indução, $S^C = \mathbb{N}$, o que implica que $S = \emptyset$, uma contradição. Assim, S deve ter um menor elemento. ■

Teorema 2.9 (Princípio do Menor Inteiro)**.** *Se A é um subconjunto não nulo de $\mathbb{Z}$ e A é limitado inferiormente então A possui um menor elemento.*

Demonstração. Conforme [4], veja que se $A \subset \mathbb{N}$, o Teorema 2.8 já nos retorna que o conjunto A possui um menor elemento, tornando esse caso um caso trivial. Dessa forma, suponha que existe um número inteiro negativo m tal que $m \leq a$, $\forall\, a \in A$. Defina o conjunto

$$B = \{a + (-m) : a \in A\}.$$

Daí, como $a \geq m$, então $B \subset \mathbb{N}$ e, pela mesma argumentação do caso trivial, possui um menor elemento. Como esse menor elemento pertence ao conjunto B, então ele deve ser escrito na forma $n + (-m)$ e dessa forma temos que n é o menor elemento de A. ■

E ainda, o teorema a seguir nos diz que todo número pode ser fatorado, ou seja, escrito em fatores, como uma multiplicação única de primos. Ou seja, por exemplo, o número $10 = 2 \cdot 5$, e só pode ser escrito dessa forma, a menos da permutação dos dois fatores, isto é, $10 = 5 \cdot 2$.

Teorema 2.10 (Teorema Fundamental da Aritmética)**.** *Todo inteiro $a > 1$ pode ser representado de maneira única (a menos da ordem) como um produto de fatores primos.*

Demonstração. Conforme [4], mostraremos a existência e a unicidade da fatoração.

1. Considere S não vazio e que contenha todos os naturais que não podem ser representados como um produto de fatores primos. Como S é formado por elementos do conjunto dos números naturais, então $S \subset \mathbb{N}$. Daí, pelo Teorema 2.8, S tem um menor elemento, o qual chamaremos de x. Veja que $x > 2$, já que o elemento 2 é primo, e x não é um primo, pois tais números admitem a fatoração em primos. Daí, existem $y, z \in \mathbb{N}$ tais que $x = y \cdot z$. Como $x > y$ e $x > z$, então ambos os elementos não pertencem ao conjunto S, e por definição admitem alguma fatoração em números primos. Portanto, x também deveria admitir fatoração prima, o que contraria hipótese de $x \in S$. Logo $S = \emptyset$.

2. Sejam duas fatorações em primos para o mesmo natural a,

$$q_1 q_2 \dots q_n = a = p_1 p_2 \dots p_k.$$

Assim, como temos

$$q_1 q_2 \dots q_n = p_1 p_2 \dots p_k,$$

temos em particular que $p_1 \mid q_1 q_2 \dots q_n$. Daí, pela definição de número primo[2], existe $1 \leq l \leq n$ tal que $p_1 \mid q_l$. Daí, como ambos os elementos são primos, temos que se um divide o outro, então $p_1 = q_l$. Assim, para todo $j < k$, existe $i < n$ tal que $p_j \mid q_i$ e pelo mesmo argumento anterior, $p_j = q_i$. Demonstraremos agora que $k = n$. Para isso, suponha por absurdo que $k < n$. Sem perda de generalidade, assuma que, $p_1 = q_1, p_2 = q_2, \dots, p_k = q_k$. Ou seja,

$$q_1 q_2 \dots q_k q_{k+1} \dots q_n = p_1 p_2 \dots p_k = q_1 q_2 \dots q_k,$$

[2] Se $p \mid a \cdot b$, então $p \mid a$ ou $p \mid b$, vide mais informações sobre os elementos primos no Capítulo 3.

que pela propriedade do cancelamento da multiplicação nos naturais resulta em

$$q_{k+1} \dots q_n = 1,$$

o que consiste num absurdo, já que cada fator "q" é um elemento primo por hipótese. De modo análogo ao assumir que $k > n$, temos outro absurdo. Ou seja, $k = n$ e os conjuntos dos p_i e dos q_j têm exatamente os mesmos elementos.

Portanto, pelo primeiro item temos que a fatoração prima existe, e pelo segundo item, temos que a fatoração é única. ■

2.3 EQUAÇÕES DIOFANTINAS

Para encontrarmos inversos multiplicativos em um anel $\mathbb{Z}_n$, será necessário o conhecimento de como trabalhar com equações diofantinas.

Definição 2.3. Uma equação diofantina é uma equação polinomial de grau um com duas ou mais variáveis que assumem apenas valores inteiros.

Antes de enunciarmos o mais importante teorema envolvendo o máximo divisor comum deste trabalho, precisamos enunciar o Algoritmo da divisão de Euclides, o qual é utilizado na demonstração do teorema em questão.

Teorema 2.11 (Algoritmo da divisão de Euclides)**.** *Sejam $a, b \in \mathbb{Z}$ com $b \neq 0$. Assim, existe um único par de números inteiros q, r com $0 \leq r < |b|$ tais que*

$$a = bq + r.$$

Demonstração. Segundo [4], separaremos esta demonstração em dois casos: $b > 0$ e $b < 0$.

1. Seja
$$B = \{a - xb : x \in \mathbb{Z}, a - xb \geq 0\}.$$
Note que
$$a - (-|a|)b = a + |a|b \geq a + |a| \geq 0,$$
ou seja, B é não vazio, pois $a - (-|a|)b \in B$. Veja também que pelo Teorema 2.9, B possui um menor elemento, o qual denotaremos por r. Assim, existe $q \in \mathbb{Z}$ tal que
$$r = a - qb \implies a = qb + r.$$
E, para mostrarmos que $r < |b| = b$, basta verificar que
$$r = b \implies a = (q+1)b \implies a - (q+1)b = 0 \implies 0 \in B,$$
o que consiste num absurdo pois r é o menor elemento de B, o que implicaria que $0 = r = b$. Agora, se $r > b$ então existe $\alpha \in \mathbb{N}$ tal que $r = b + \alpha$, onde $0 < \alpha < r$. Assim
$$b + \alpha = a - qb \implies \alpha = a - (q+1)b \in B,$$
que é outro absurdo, pois r é o menor elemento de B. Logo, $0 \leq r < |b|$. Agora, mostremos que q, r são unicamente determinados. Suponha que existem q, r, q_1, r_1 tais que $a = qb + r = q_1 b + r_1$, com $0 \leq r < |b| = b$ e $0 \leq r_1 < |b| = b$. Daí, $0 \leq |r - r_1| < b$. Por outro lado,
$$qb + r = q_1 b + r_1 \implies |q - q_1|b = |r - r_1|.$$
Se tivéssemos $r \neq r_1$, teríamos $|q - q_1| \geq 1$. Daí,
$$b \leq |q - q_1|b = |r - r_1| < b,$$
o que é um absurdo. Portanto $r = r_1$ e assim, $q = q_1$.

2. Aplicamos o caso anterior para a e $|b|$. Daí, existe um único par $q, r \in \mathbb{Z}$ tais que $a = q|b| + r$, com $0 \leq r < |b|$. Denotando $q_1 = -q$ ganhamos que $a = q_1 b + r$, com $0 \leq r < |b|$.

■

O Teorema de Bachet-Bézout nos diz que o conjunto dos números da forma $ax + by$, onde $x, y \in \mathbb{Z}$, ou seja, x, y variam sobre todos os inteiros, é exatamente o conjunto dos múltiplos de $\text{mdc}(a, b)$.

Teorema 2.12 (Teorema de Bachet-Bézout)**.** *Sejam $a, b \in \mathbb{N}$ não simultaneamente nulos. Então existem inteiros $x, y \in \mathbb{Z}$ tais que*

$$ax + by = \text{mdc}(a, b).$$

Demonstração. Seja o conjunto

$$X = \{ax + by \in \mathbb{N}^* : x, y \in \mathbb{Z}\}.$$

Conforme [4], note que X é não vazio, pois por hipótese, $a, b \in \mathbb{Z}$ são não simultaneamente nulos e tomando x e y iguais a -1, 0 ou 1 conforme a necessidade, teremos que $|a| \in X$ ou $|b| \in X$. Além disso, $X \subset \mathbb{N}$, já que $\text{mdc}(a, b) > 0$. E pelo Teorema 2.8, existe um menor elemento de X, o qual será denotado por d. Como $d \in X$, temos

$$d = at + bs, \tag{1}$$

em que $t, s \in \mathbb{Z}$.
Agora, basta mostrar que $d = \text{mdc}(a, b)$. Suponha por absurdo que $d \nmid a$. Pelo Teorema 2.11, tem-se que $a = dq + r$, com $0 \leq r < d$. Isolando o resto r e usando (1),

$$\begin{aligned} r &= a - dq \\ &= a - (at + bs)q \\ &= a - atq - bsq \\ &= a(1 - tq) + b(-sq). \end{aligned}$$

Tome $v = 1 - tq$ e $u = -sq$. Assim, r pode ser escrito na forma $r = av + bu$. Ou seja, $r \in X$. E ainda, como $0 \leq r < d$ por construção, então r é menor que d, o menor elemento do conjunto. Logo, tem-se um absurdo. Portanto, $d \mid a$, e ainda, obtem-se $d \mid b$ de forma análoga. Assim, conclui-se que $d \mid \text{mdc}(a, b)$. E, por definição, $\text{mdc}(a, b) \mid a$ e $\text{mdc}(a, b) \mid b$, e assim, pela Proposição 2.4 junto com (1), temos que $\text{mdc}(a, b) = d$. ■

De modo geral, para trabalhar com equações diofantinas, devemos:

- Escrever as divisões sucessivas, transformando o divisor e o resto em dividendo e divisor, respectivamente;
- Isolar os restos;
- Utilizar o item 2 para fazer substituições de baixo para cima.

Exemplo 2.3.1. Vamos encontrar a solução da equação diofantina

$$43x + 24y = 1.$$

Primeiro, note que $\text{mdc}(43, 24) = 1$, pois 43 é primo. Depois, faremos as divisões sucessivas:

$$43 = 24 \cdot 1 + 19$$
$$24 = 19 \cdot 1 + 5$$
$$19 = 5 \cdot 3 + 4$$
$$5 = 4 \cdot 1 + 1$$

Agora, isolando os restos temos:

$$19 = 43 - 24 \cdot 1$$
$$5 = 24 - 19 \cdot 1$$
$$4 = 19 - 5 \cdot 3$$
$$1 = 5 - 4 \cdot 1$$

Por fim, substituiremos os valores encontrados de forma encadeada:

$$\begin{aligned}
1 &= 5 - 4 \cdot 1 \\
&= (24 - 19 \cdot 1) - (19 - 5 \cdot 3) \cdot 1 \\
&= [24 - (43 - 24 \cdot 1) \cdot 1] - [(43 - 24 \cdot 1) - (24 - 19 \cdot 1) \cdot 3] \cdot 1 \\
&= [24 - (43 - 24)] - [(43 - 24) - (24 - (43 - 24)) \cdot 3] \\
&= [24 - 43 + 24] + [-(43 - 24) + (24 - (43 - 24)) \cdot 3] \\
&= 24 \cdot 2 + 43 \cdot (-1) + [-43 + 24 + 24 \cdot 3 - 43 \cdot 3 + 24 \cdot 3] \\
&= 24 \cdot 9 + 43 \cdot (-5)
\end{aligned}$$

Assim, uma solução para a equação é $y = 9$ e $x = -5$.

2.4 RELAÇÃO

Uma relação de dois elementos é apenas uma forma de os agrupar de acordo com a característica ou regra desejada.

Suponha, por exemplo, que você esteja observando sua gaveta de meias. Daí, você nota que possui dois pares de meias amarelas e dois pares de meias brancas, e as separa por cor. Perceba que as meias amarelas estão relacionadas entre si (de acordo com sua cor), e note também que as meias brancas estão relacionadas entre si (também conforme sua cor).

Exemplo 2.4.1. Pares ordenados: A(5,3), B(2,0), C(4,7). Neste caso, pares ordenados relacionam dois números reais. Note que neste caso não é produzido um terceiro elemento.

Exemplo 2.4.2. Funções: $f(x) = 5x + 7$. Neste caso, funções relacionam um elemento real com um elemento produzido através de uma regra de formação, ou seja, $f(x)$. Assim, temos a seguinte relação $(x, f(x))$, ou ainda, $(x, 5x + 7)$.

Exemplo 2.4.3. Relação de desigualdade: $5 \neq 1, 3 \neq 8$. Neste caso, temos dois números relacionados através de uma relação de desigualdade, isto é, caso dois números não sejam iguais, estes estarão relacionados.

Além disso, dada uma relação $\mathcal{R}$ em um conjunto A, as seguintes propriedades podem ou não ser satisfeitas:

- Reflexiva: $\forall\, x \in A, x\mathcal{R}x$;
- Simétrica: $\forall\, x, y \in A, x\mathcal{R}y \implies y\mathcal{R}x$;
- Transitiva: $\forall\, x, y, z \in A$, se $x\mathcal{R}y$ e $y\mathcal{R}z$, então $x\mathcal{R}z$;
- Antissimétrica: $\forall\, x, y \in A$, se $x\mathcal{R}y$ e $y\mathcal{R}x$, então $x = y$;
- Linear (ou Total): $\forall\, x, y \in A$, ou $x\mathcal{R}y$ ou $y\mathcal{R}x$.

E, caso uma relação atenda algumas destas propriedades, nomeamos esta relação como:

- Relação de Ordem: *Reflexiva*, *Transitiva* e *Antissimétrica*;
- Relação de Ordem Total: *Reflexiva, Transitiva, Antissimétrica e Linear*;
- Relação de Equivalência: *Reflexiva*, *Simétrica* e *Transitiva.*

Dada $\sim$ uma relação de equivalência em um conjunto A, e $x \in A$, vamos denotar os elementos que estão relacionados com x por $\overline{x}$:

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

Exemplo 2.4.4. Considere em $\mathbb{Z}$ a relação "têm a mesma paridade". Assim, podemos separar os elementos de $\mathbb{Z}$ em dois conjuntos, o conjunto dos números pares que podem ser representados na forma $2k$,

pois deixam resto zero na divisão por 2, e o conjunto dos números ímpares, $2k+1$, que deixam resto 1 na divisão por 2.

A proposição a seguir indica que caso os elementos estejam relacionados por uma relação de equivalência, suas classes de equivalência serão iguais, visto que se trata apenas de outra forma de apresentação. Caso as classes não sejam iguais, não terão os mesmos elementos, e por consequência, não terão interseção.

Um exemplo disso é o de gavetas de meias amarelas e brancas dado no início da seção. Perceba que se duas meias são amarelas, então estas estão relacionadas e, portanto, pertencem à mesma categoria, a qual é possuir cor amarela neste caso. Também não temos meias brancas na categoria de meias amarelas e vice e versa, ou seja, não há meias sobrando, ou meias em ambas as categorias. E ainda, se unirmos a categoria de meias amarelas e brancas, teremos então a gaveta inteira.

Proposição 2.13. *Seja $\sim$ uma relação de equivalência definida em um conjunto A e, sejam $x, y \in A$. Então,*

1. $\overline{x} = \overline{y} \iff x \sim y$;
2. $\overline{x} \neq \overline{y} \implies \overline{x} \cap \overline{y} = \varnothing$;
3. $\bigcup_{x \in A} \overline{x} = A$.

Demonstração. 1. ($\implies$) Sejam $x, y \in A$ e $\overline{x} = \overline{y}$. Por definição:

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

Como $x \in \overline{x} = \overline{y}$, temos $x \sim y$.
($\impliedby$) Sejam $x, y \in A$ e $x \sim y$. Vamos primeiro provar que $\overline{x} \subset \overline{y}$, e depois, $\overline{y} \subset \overline{x}$. Seja a um elemento arbitrário em $\overline{x}$, vamos provar que $a \in \overline{y}$. Se $a \in \overline{x}$, então $a \sim x$. Por hipótese, $x \sim y$.

Por transitividade, temos $a \sim y$. Portanto, $a \in \overline{y}$. Assim, temos $\overline{x} \subset \overline{y}$. Agora, se $x \sim y$, temos por simetria que $y \sim x$, e de forma análoga, temos $\overline{y} \subset \overline{x}$. Como vimos que $\overline{x} \subset \overline{y}$ e $\overline{y} \subset \overline{x}$, temos $\overline{x} = \overline{y}$.

2. Suponhamos $x, y \in A$ e $\overline{x} \neq \overline{y}$. Se existisse algum elemento $a \in \overline{x} \cap \overline{y}$, teríamos $a \sim x$ e $a \sim y$. Por simetria, $x \sim a$ e, por transitividade, $x \sim y$. Pelo item anterior, $\overline{x} = \overline{y}$, o que contraria a hipótese.

3. Vamos provar que $\bigcup_{x \in A} \overline{x} = A$. De fato, temos $\overline{x} \subset A, \forall\, x \in A$ e então, segue que $\bigcup_{x \in A} \overline{x} \subset A$. Reciprocamente, temos que $x \in \overline{x}, \forall\, x \in A$, portanto segue que $A \subset \bigcup_{x \in A} \overline{x}$.

■

Seja $\sim$ uma relação de equivalência em um conjunto A. Chamamos de conjunto quociente de A pela relação de equivalência $\sim$, e denotamos este conjunto por $A/_{\sim}$, de tal forma que o conjunto quociente é tido como o conjunto de todas as classes de equivalência relativas a relação $\sim$ em A. Ou seja, estamos juntando os elementos similares, isto é, relacionados, em um elemento só, as classes de equivalência.

Notação. $A/_{\sim} = \{\overline{x} : x \in A\}$.

Retomando o exemplo da gaveta de meias, teríamos

$$\text{gaveta de meias}_{/\,\text{cor}} = \{\text{amarelas}, \text{brancas}\}.$$

2.5 CONGRUÊNCIA MÓDULO n

Foi o matemático, astrônomo e físico alemão, Johann Carl Friedrich Gauss quem definiu e relatou o que entendemos por congruência módulo n entre dois números em sua obra *Disquisitiones Arithmeticae* [5].

Definição 2.4. Se $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}^*$, dizemos que a é congruente a b módulo n se $n \mid (b - a)$.

A notação foi sugerida por Gauss devido à semelhança das propriedades das relações de congruência e da igualdade [5].

Notação. $a \equiv b \pmod{n}$.

Provaremos a seguir que a congruência módulo n é uma relação de equivalência.

Proposição 2.14. *A congruência módulo n é uma relação de equivalência.*

Demonstração. Verificaremos que $\forall\, a, b, c \in \mathbb{Z}$ e $n \in \mathbb{N}^*$ temos as propriedades reflexiva, simétrica e transitiva, ou seja,

1. $a \equiv a \pmod{n}$;
2. $a \equiv b \pmod{n} \implies b \equiv a \pmod{n}$;
3. $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n} \implies a \equiv c \pmod{n}$.

Daí,

1. Perceba que $a \equiv a \pmod{n} \iff n \mid (a - a) \iff n \mid 0$. E por definição, isso sempre acontece;

2. Note que

$$\begin{aligned} a \equiv b \pmod{n} &\iff n \mid (b-a) \\ &\iff n \mid -(a-b) \\ &\iff -n \mid (a-b) \\ &\iff n \mid (a-b) \\ &\iff b \equiv a \pmod{n}; \end{aligned}$$

3. Tome a adição de $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n}$. Daí,

$$\begin{aligned} a+b \equiv b+c \pmod{n} &\iff n \mid (b+c-(a+b)) \\ &\iff n \mid (b+c-a-b) \\ &\iff n \mid (c-a) \\ &\iff a \equiv c \pmod{n}. \end{aligned}$$

■

Exemplo 2.5.1. $9 \equiv 3 \pmod{2}$, pois $2 \mid (9-3)$. Observe que tanto o resto da divisão de 9 por 2, quanto de 3 por 2 é 1.

Proposição 2.15. *Dados $a, b, c, d \in \mathbb{Z}$ e $n \in \mathbb{N}^*$, tais que $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$, temos que*

1. $a + c \equiv b + d \pmod{n}$;
2. $a - c \equiv b - d \pmod{n}$;
3. $ac \equiv bd \pmod{n}$;

Demonstração. 1. Por definição, temos de $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$, que $a - b = rn$ e $c - d = sn$. E somando estas equações, obtemos $(a+c) - (b+d) = (r+s)n \Longrightarrow a + c \equiv b + d \pmod{n}$.

2. Subtraindo $a-b=rn$ e $c-d=sn$, obtemos $(a-b)-(c-d)=(a-c)-(b-d)=(r-s)\Longrightarrow a-c\equiv b-d \pmod{n}$.

3. Multiplicando $a-b=rn$ por c, e $c-d=sn$, por b, obtemos $ac-bc=crn$ e $bc-bd=bsn$. Somando estes resultados, obtemos $ac-bc+bc-bd=(cr+bs)n\Longrightarrow ac\equiv bd \pmod{n}$.

■

2.6 CLASSES DE CONGRUÊNCIA MÓDULO n

A classe de equivalência de um elemento $a\in\mathbb{Z}$, é o subconjunto de todos os elementos de $\mathbb{Z}$ que são congruentes a a. Ou seja,

$$\overline{a}=\{x\in\mathbb{Z}: a\equiv x \pmod{n}\}$$

e então obtemos que

$$\begin{aligned} x\in\overline{a} &\iff x\equiv a \pmod{n}\\ &\iff x-a=k\cdot n, k\in\mathbb{Z}\\ &\iff x=a+k\cdot n, \end{aligned}$$

ou seja, a classe de equivalência também pode ser denotada como

$$\overline{a}=\{a+k\cdot n: k\in\mathbb{Z}\}.$$

Assim, vamos provar que $\mathbb{Z}/_{\equiv \pmod{n}}$, que denotamos por $\mathbb{Z}_n$, possui exatamente as n classes de equivalência $\{\overline{0},\overline{1},\overline{2},\ldots,\overline{n-1}\}$.

Proposição 2.16. *Se $n\in\mathbb{N}^*$, então $\mathbb{Z}_n=\{\overline{0},\overline{1},\ldots,\overline{n-1}\}$.*

Demonstração. Começamos mostrando que as classes $\overline{x}$, com x variando de 0 à $n-1$, são distintas. Tome x e y tais que $0\leq x<y\leq n-1$. Pela Proposição 2.13, $\overline{y}=\overline{x}$ equivale à $0<y-x=k\cdot n, k\in\mathbb{Z}$, o que é um absurdo. Assim, as classes $\{\overline{0},\overline{1},\ldots,\overline{n-1}\}$ são todas distintas.

E ainda, veja que se $m > n-1$ ou $m < 0$, então podemos utilizar o Algoritmo de Divisão de Euclides para verificar que o resto r da divisão de m por n satisfará $0 \leq r \leq n-1$ e $\overline{m} = \overline{r}$.
Dessa forma, $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ é um conjunto de exatamente n elementos distintos. ■

2.7 ANÉIS

Seja um conjunto não-vazio A e duas operações fechadas que estejam definidas neste conjunto, neste caso, chamaremos de adição e multiplicação (tal qual em $\mathbb{Z}$) e denotaremos por "$+$" e "$\cdot$". Assim,

$$\begin{aligned} + : A \times A &\longrightarrow A \\ (x, y) &\mapsto x + y \end{aligned}$$

e

$$\begin{aligned} \cdot : A \times A &\longrightarrow A \\ (x, y) &\mapsto x \cdot y \end{aligned}$$

Observação 1. Para termos operações fechadas, temos que aplicando ambas as operações a dois elementos quaisquer desse conjunto A, o resultado sempre terá que ser um elemento A.

Definição 2.5. Denotaremos $(A, +, \cdot)$ um anel se as seguintes propriedades são válidas para todos $a, b, c \in A$:

- Associatividade:

$$(a + b) + c = a + (b + c);$$

- Existência de elemento neutro: existe $0 \in A$ tal que

$$a + 0 = 0 + a = a;$$

- Existência de inverso: $\forall\, a \in A, \exists\, b \in A$, denotado por $b = -a$, tal que
$$a + b = b + a = 0;$$

- Comutatividade:
$$a + b = b + a.$$

- Associatividade:
$$(a \cdot b) \cdot c = a \cdot (b \cdot c);$$

- Distributividade à esquerda e à direita:
$$a \cdot (b + c) = a \cdot b + a \cdot c;$$
$$(b + c) \cdot a = b \cdot a + c \cdot a.$$

A partir de agora, dados a, b no anel A, denotaremos $a + (-b)$ por $a - b$.

Exemplo 2.7.1. Note que os naturais não formam um anel, pois ao calcular o inverso aditivo de um elemento n, vemos que o elemento $-n$ não pertence ao conjunto dos números naturais.

Nas próximas páginas vamos construir duas operações que transformarão $\mathbb{Z}_n$ em um anel. Vimos nas Seções 2.5 e 2.6 que a congruência de números é uma relação de equivalência, que $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-2}, \overline{n-1}\}$ e que cada elemento de $\mathbb{Z}_n$ representa um conjunto de elementos que estão relacionados por congruência de números, ou seja, o subconjunto $\overline{0}$ é formado pelos números inteiros que na divisão por n deixam resto zero, da mesma forma que $\overline{1}$ é constituído pelos elementos inteiros que na divisão por n deixam resto um e assim sucessivamente.

Além disso, vimos pela Proposição 2.13 que duas classes de equivalência são iguais se seus elementos estão relacionados, ou seja,

se existe congruência entre estes números. Isso nos diz que duas classes de equivalência serão iguais se seus elementos deixarem mesmo resto na divisão por n, ou pela definição de congruência, que n dividirá a subtração dos dois elementos representantes das classes de equivalência.

Exemplo 2.7.2. Veja que $\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$. E, além disso,

$$\begin{aligned}
\overline{0} &= \{\ldots, -20, -15, -10, -5, 0, 5, 10, 15, 20, \ldots\} \\
\overline{1} &= \{\ldots, -21, -16, -11, -6, 1, 6, 11, 16, 21, \ldots\} \\
\overline{2} &= \{\ldots, -22, -17, -12, -7, 2, 7, 12, 17, 22, \ldots\} \\
\overline{3} &= \{\ldots, -23, -18, -13, -8, 3, 8, 13, 18, 23, \ldots\} \\
\overline{4} &= \{\ldots, -24, -19, -14, -9, 4, 5, 14, 19, 24, \ldots\}
\end{aligned}$$

E ainda, $\overline{6} = \overline{21} \iff 5 \mid (21 - 6) = 15$.

Definição 2.6. Em $\mathbb{Z}_n$ definiremos as operações

- $\overline{a} + \overline{b} = \overline{a + b}$;
- $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$,

Veja que quando temos uma classe de equivalência em $\mathbb{Z}_n$, em suma, estamos trabalhando com congruência de números módulo n. Assim, caso $a + b$ ou $a \cdot b$ seja maior que n, basta reduzi-lo à uma classe de equivalência de $\mathbb{Z}_n$ com congruência de números.

Proposição 2.17. *As operações da Definição 2.6 estão bem definidas.*

Demonstração. Tome $\overline{a_1} = \overline{a_2}$ e $\overline{b_1} = \overline{b_2}$. Isso é equivalente a $a_1 \sim a_2$ e $b_1 \sim b_2$, respectivamente. Veja que $a_1 - a_2 = nx$ e $b_1 - b_2 = ny$, em que $x, y \in \mathbb{Z}$.

E somando ambas as igualdades, temos

$$\begin{aligned} & a_1 - a_2 + b_1 - b_2 = nx + ny \\ \iff & a_1 + b_1 - (a_2 + b_2) = n(x + y) \end{aligned}$$

Ou seja, $\overline{a_1 + b_1} = \overline{a_2 + b_2}$.
E multiplicando ambas as igualdades iniciais, temos

$$\begin{aligned} a_1 \cdot b_1 - a_2 \cdot b_2 &= a_1 \cdot b_1 - a_1 \cdot b_2 + a_1 \cdot b_2 - a_2 \cdot b_2 \\ &= a_1 \cdot (b_1 - b_2) + b_2 \cdot (a_1 - a_2) \\ &= a_1 \cdot ny + b_2 \cdot nx \\ &= n(a_1 \cdot y + b_2 \cdot x). \end{aligned}$$

Ou seja, $\overline{a_1 \cdot b_1} = \overline{a_2 \cdot b_2}$. Assim, estas operações são bem definidas. ■

Exemplo 2.7.3. Seja $\overline{a} = \overline{5}$ e $\overline{b} = \overline{3}$. Daí, em $\mathbb{Z}_6$, temos

$$\begin{aligned} \overline{5} + \overline{3} &= \overline{5 + 3} \\ &= \overline{8}. \end{aligned}$$

Note que $8 \equiv 2 \pmod 6$ e assim, $\overline{8} = \overline{2}$.
E,

$$\begin{aligned} \overline{5} \cdot \overline{3} &= \overline{5 \cdot 3} \\ &= \overline{15}. \end{aligned}$$

Note que $15 \equiv 3 \pmod 6$, logo, $\overline{15} = \overline{3}$.

Exemplo 2.7.4. $(\mathbb{Z}_n, +, \cdot)$ é um anel.

Demonstração. Sejam $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_n$. Assim,

- Associatividade:

$$\begin{aligned}(\overline{a}+\overline{b})+\overline{c} &= (\overline{a+b})+\overline{c}\\ &= \overline{(a+b)+c}\\ &= \overline{a+(b+c)}\\ &= \overline{a}+\overline{(b+c)}\\ &= \overline{a}+(\overline{b}+\overline{c});\end{aligned}$$

- Existência de elemento neutro: Seja $\overline{0} \in \mathbb{Z}_n$. Veja que

$$\begin{aligned}\overline{a}+\overline{0} &= \overline{a+0}\\ &= \overline{a}\\ &= \overline{0+a}\\ &= \overline{0}+\overline{a};\end{aligned}$$

- Existência de inverso: Seja $\overline{a} \in \mathbb{Z}_n$, note que $\exists\, \overline{b} \in \mathbb{Z}_n$, denotado por $\overline{b} = \overline{-a}$, tal que

$$\begin{aligned}\overline{a}+\overline{b} &= \overline{a}+\overline{-a}\\ &= \overline{a+(-a)}\\ &= \overline{0}\\ &= \overline{(-a)+a}\\ &= \overline{-a}+\overline{a}\\ &= \overline{b}+\overline{a};\end{aligned}$$

- Comutatividade:

$$\begin{aligned}\overline{a}+\overline{b} &= \overline{a+b}\\ &= \overline{b+a}\\ &= \overline{b}+\overline{a}.\end{aligned}$$

- Associatividade:

$$\begin{aligned}(\overline{a}\cdot\overline{b})\cdot\overline{c} &= (\overline{a\cdot b})\cdot\overline{c}\\ &= \overline{(a\cdot b)\cdot c}\\ &= \overline{a\cdot(b\cdot c)}\\ &= \overline{a}\cdot\overline{(b\cdot c)}\\ &= \overline{a}\cdot(\overline{b}\cdot\overline{c});\end{aligned}$$

- Distributividade à esquerda e à direita:

$$\begin{aligned}\overline{a}\cdot(\overline{b}+\overline{c}) &= \overline{a}\cdot\overline{b}+\overline{a}\cdot\overline{c}\\ &= \overline{a}\cdot(\overline{b+c})\\ &= \overline{a\cdot(b+c)}\\ &= \overline{a\cdot b+a\cdot c}\\ &= \overline{a\cdot b}+\overline{a\cdot c}\\ &= \overline{a}\cdot\overline{b}+\overline{a}\cdot\overline{c};\end{aligned}$$

$$\begin{aligned}(\overline{b}+\overline{c})\cdot\overline{a} &= (\overline{b+c})\cdot\overline{a}\\ &= \overline{(b+c)\cdot a}\\ &= \overline{b\cdot a+c\cdot a}\\ &= \overline{b\cdot a}+\overline{c\cdot a}\\ &= \overline{b}\cdot\overline{a}+\overline{c}\cdot\overline{a}.\end{aligned}$$

■

Outros exemplos de anéis são

- $(\mathbb{Z},+,\cdot)$. Note que todas as propriedades necessárias para termos um anel valem nos inteiros;

- $(\mathbb{Z}[\sqrt{p}],+,\cdot)$, em que $\mathbb{Z}[\sqrt{p}] = \{a+b\sqrt{p} : a,b\in\mathbb{Z}\}$. Vide a demonstração no Exemplo 1.10 de [4];

- $(\mathbf{M}_n(\mathbb{R}), +, \cdot)$, $n \in \mathbb{N}^*$, em que $\mathbf{M}_n(\mathbb{R})$ são as matrizes quadradas de ordem $n \times n$ com coeficientes reais. Vide a demonstração no Capítulo 3 (exemplos de anéis não comutativos) de [6];

- $(\mathbb{Q}, +, \cdot)$. Vide a demonstração no Exemplo 1.1 de [4].

E ainda, se o anel em questão atende com a sua segunda operação alguma das definições a seguir, este recebe nomes específicos, pois são anéis especiais.

Definição 2.7. Teremos um

- Anel com unidade quando $\exists\, 1_A \in A, 0_A \neq 1_A$ tal que

$$a \cdot 1_A = 1_A \cdot a = a, \forall\, a \in A;$$

- Anel comutativo quando $\forall\, a, b \in A$

$$a \cdot b = b \cdot a;$$

- Anel sem divisores de zero quando $a, b \in A$

$$a \cdot b = 0 \implies a = 0 \text{ ou } b = 0.$$

Exemplo 2.7.5. Encontre todos os divisores de zero de $\mathbb{Z}_{20}$.

Solução. Note que:

$$2 \cdot 10 = 20;$$
$$4 \cdot 5 = 20;$$
$$6 \cdot 10 = 60 = 20 \cdot 3;$$
$$8 \cdot 5 = 40 = 20 \cdot 2;$$
$$12 \cdot 5 = 60 = 20 \cdot 3;$$
$$14 \cdot 10 = 140 = 20 \cdot 7;$$
$$15 \cdot 4 = 60 = 20 \cdot 3;$$
$$16 \cdot 5 = 160 = 20 \cdot 8;$$
$$18 \cdot 10 = 180 = 20 \cdot 9.$$

Assim, os divisores de zero de $\mathbb{Z}_{20}$ são

$$\{\overline{2}, \overline{4}, \overline{5}, \overline{6}, \overline{8}, \overline{10}, \overline{12}, \overline{14}, \overline{15}, \overline{16}, \overline{18}\}.$$

Além disso, se o anel atende às três propriedades vista anteriormente, ele será conhecido como *domínio de integridade*.

Definição 2.8. Se $(A, +, \cdot)$ é um anel comutativo, com unidade 1_A e sem divisores de zero, dizemos que $(A, +, \cdot)$ é um domínio de integridade.

Exemplo 2.7.6. Alguns exemplos de domínios de integridade são: $(\mathbb{Q}, +, \cdot)$ confira a demonstração no Exemplo 1.6 de [4]; e $(\mathbb{Z}[p], +, \cdot)$, em que p é primo, cuja demonstração está feita no Exemplo 1.10 de [4].

Definição 2.9 (Corpo)**.** Se A for um anel com unidade 1, for comutativo e atenda a propriedade a seguir, teremos um corpo:

$$\forall\, x \in A, x \neq 0, \exists\, y \in A : x \cdot y = y \cdot x = 1.$$

Exemplo 2.7.7. Os conjuntos $(\mathbb{Q}[p], +, \cdot)$, $(\mathbb{R}, +, \cdot)$ e $(\mathbb{C}, +, \cdot)$ são corpos, vide seção 2 do Capítulo 3 de [6].

Veja que as definições que foram vistas anteriormente sobre anéis, domínios de integridade e corpos podem ser encadeadas logicamente como na Figura 1 a seguir:

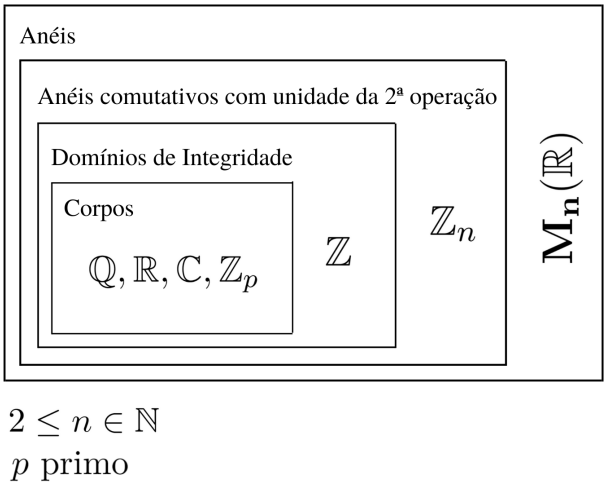


Figura 1 – Os anéis vistos em forma de diagrama.
Fonte: A autora.

No início da Seção 2.3 foi comentado que as equações diofantinas são utilizadas para encontrar inversos multiplicativos em $\mathbb{Z}_n$. Isso ocorre já que em $\mathbb{Z}$ uma equação diofantina qualquer é representada por

$$ax + by = c,$$

em que $a, b, c \in \mathbb{N}$ e $x, y \in \mathbb{Z}$. Ao substituir a por n, b pelo representante da classe de equivalência do elemento que desejamos calcular o inverso, c por 1 e trabalharmos com essa equação em $\mathbb{Z}_n$, observamos que a equação original se torna

$$\overline{n} \cdot \overline{x} + \overline{b} \cdot \overline{y} = \overline{1} \iff \overline{0} \cdot \overline{x} + \overline{b} \cdot \overline{y} = \overline{1} \iff \overline{b} \cdot \overline{y} = \overline{1}.$$

Ou seja, agora temos o elemento original $\overline{b}$ e o elemento que multiplicado por ele $\overline{y}$ resulta em $\overline{1}$.

Exemplo 2.7.8. Encontre o elemento inverso de $\overline{13}$ em $\mathbb{Z}_{20}$.

Solução. Trataremos esse problema como uma equação diofantina em $\mathbb{Z}$. Dessa forma, devemos escrevê-la como

$$20x + 13y = 1,$$

e realizar os passos da Seção 2.3: Realizando o primeiro passo,

$$\begin{aligned} 20 &= 13 \cdot 1 + 7 \\ 13 &= 7 \cdot 1 + 6 \\ 7 &= 6 \cdot 1 + 1. \end{aligned}$$

Agora, quanto ao segundo passo,

$$\begin{aligned} 7 &= 20 - 13 \cdot 1 \\ 6 &= 13 - 7 \cdot 1 \\ 1 &= 7 - 6 \cdot 1. \end{aligned}$$

E por fim, realizando o terceiro passo, temos

$$\begin{aligned} 1 &= 7 - 6 \cdot 1 \\ &= (20 - 13 \cdot 1) - (13 - 7 \cdot 1) \cdot 1 \\ &= (20 - 13) - (13 - 7) \\ &= (20 - 13) - (13 - (20 - 13 \cdot 1)) \\ &= (20 - 13) - (13 - (20 - 13)) \\ &= 20 - 13 - 13 + 20 - 13 \\ &= 20 \cdot 2 + 13 \cdot (-3) \end{aligned}$$

E veja que $\overline{13} \cdot \overline{-3} = \overline{13 \cdot (-3)} = \overline{-39} = \overline{1}$. Portanto, descobrimos que o elemento inverso de $\overline{13}$ em $\mathbb{Z}_{20}$ é $\overline{-3} = \overline{17}$.

2.7.1 Propriedades

A seguir algumas propriedades importantes dos anéis, sendo que todas as demonstrações foram norteadas por [7].

Proposição 2.18. *O elemento neutro do anel $(A, +, \cdot)$ é único.*

Demonstração. Temos que como A é um anel, então este possui um elemento neutro que denotamos por 0_A. Suponha que exista outro zero em A, digamos $0_{A'}$. Como 0_A é elemento neutro da adição, vale

$$0_A + 0_{A'} = 0_{A'}.$$

Mas, como $0_{A'}$ é, por hipótese, um elemento neutro, vale

$$0_A + 0_{A'} = 0_A.$$

Das igualdades acima concluímos que $0_A = 0_{A'}$, e portanto 0_A é o único elemento neutro do anel A. ■

Proposição 2.19. *O inverso da primeira operação do anel $(A, +, \cdot)$ é único.*

Demonstração. Seja $a \in A$. Como A é anel por hipótese, sabemos que a tem um inverso $-a \in A$. Suponha que $x \in A$ também é inverso de a. Daí,

$$\begin{aligned} x &= x + 0 \\ &= x + (a + (-a)) \\ &= x + a + (-a) \\ &= 0 + (-a) \\ &= -a. \end{aligned}$$

Logo $x = -a$ e então $-a$ é o único inverso de a. ■

Em seguida, veremos proposições que a autora entende que muitos podem achar triviais, porém que devem ser demonstradas.

Proposição 2.20. *Seja* $(A, +, \cdot)$ *um anel e tome* $a, b, c \in (A, +, \cdot)$. *Então,*

1. $a \cdot 0 = 0 \cdot a = 0$;
2. $a + b = a + c \iff b = c$;
3. $b = c \implies ab = ac$ *e* $ba = ca$;
4. $-(-a) = a$;
5. $-(ab) = (-a)b = a(-b)$;
6. $a(b - c) = ab - ac$;
7. $(a - b)c = ac - bc$;
8. $-(a + b) = -a - b$;
9. $(-a)(-b) = ab$.

Demonstração. Veja que

1. Seja $a \in A$. Além disso, seja x o simétrico de $a \cdot 0$. Veja que

$$\begin{aligned} 0 &= 0 + 0 \\ a \cdot 0 &= a \cdot (0 + 0) \\ a \cdot 0 &= a \cdot 0 + a \cdot 0 \\ a \cdot 0 + x &= a \cdot 0 + a \cdot 0 + x \\ a \cdot 0 + x &= a \cdot 0 + (a \cdot 0 + x) \\ 0 &= a \cdot 0 + 0 \\ 0 &= a \cdot 0. \end{aligned}$$

Verificamos que $a \cdot 0 = 0$. A igualdade $0 \cdot a = 0$ se prova de modo análogo;

2. ($\Longleftarrow$) Temos por hipótese a primeira operação de A sendo $+$. Sabe-se que ela associa a cada par de elementos de A um único elemento de A. E, como $b = c$, temos que os pares (a, b) e (a, c) são iguais em $A \times A$. Daí, $a + b = a + c$.

   ($\Longrightarrow$) Por hipótese $a + b = a + c$. Então, usando a direção ($\Longleftarrow$), podemos somar $-a$ em ambos os lados obtendo:

$$\begin{aligned} -a + (a + b) = -a + (a + c) &\implies (-a + a) + b = (-a + a) + c \\ &\implies 0 + b = 0 + c \\ &\implies b = c; \end{aligned}$$

3. A demonstração é análoga a ($\Longleftarrow$) da propriedade anterior, apenas trocando $+$ por $\cdot$;

4. Como $-a$ é o simétrico de a vale $a + (-a) = (-a) + a = 0$. Ou seja, a é o simétrico de $-a$. E como o símbolo $-$ indica o elemento simétrico temos $-(-a) = a$;

5. Veja que

$$\begin{aligned} (-a)b + ab &= (-a + a)b \\ &= 0 \cdot b \\ &= 0. \end{aligned}$$

   Analogamente, $ab + (-a)b = 0$, ou seja, $(-a)b$ é simétrico de ab. E, da Proposição 2.19 temos $-(ab) = (-a)b$. Analogamente, temos $-(ab) = a(-b)$;

6. Perceba que
$$\begin{aligned} a(b-c) &= a(b+(-c)) \\ &= ab + a(-c) \\ &= ab + (-ac) \\ &= ab - ac; \end{aligned}$$

7. Observe que
$$\begin{aligned} (a-b)c &= (a+(-b))c \\ &= ac + (-b)c \\ &= ac - bc; \end{aligned}$$

8. Note que
$$\begin{aligned} a+b+(-a)+(-b) &= a+(-a)+b+(-b) \\ &= 0+0 \\ &= 0. \end{aligned}$$
De modo análogo, $(-a)+(-b)+a+b=0$. Daí, o simétrico de $a+b$ é $(-a)+(-b)=-a-b$. Portanto, $-(a+b)=-a-b$;

9. Veja que
$$\begin{aligned} (-a)(-b) &= -(a(-b)) \\ &= -(-ab) \\ &= ab. \end{aligned}$$

■

Proposição 2.21. *Seja $(A,+,\cdot)$ um anel com unidade. Então, sua unidade é única.*

Demonstração. Segue de modo análogo à Proposição 2.19, trocando $+$ por $\cdot$ e 0_A por 1_A. ■

Proposição 2.22. *Seja $(A, +, \cdot)$ um anel. Se $a \in A, a \neq 0_A$ e a tem inverso em A, então seu inverso é único.*

Demonstração. Segue de modo análogo à Proposição 2.18, trocando $+$ por $\cdot$ e 0_A por 1_A. ■

Proposição 2.23. *Seja $(A, +, \cdot)$ um anel. Se $1_A = 0_A$ então $A = \{0_A\}$.*

Demonstração. Seja $a \in A$. Como o anel $(A, +, \cdot)$ tem unidade 1_A temos $a = a \cdot 1_A$. E como por hipótese, $1_A = 0_A$, usando a Proposição 2.20 temos que

$$a = a \cdot 1_A = a \cdot 0_A = 0_A.$$

Logo $A = \{0_A\}$. ■

Proposição 2.24. *O anel $(A, +, \cdot)$ não tem divisores de zero se, e somente se, $\forall\, a, b, c \in A, a \neq 0_A$, vale que* $\begin{cases} ab = ac \implies b = c, \\ ba = ca \implies b = c. \end{cases}$

Demonstração. Segundo [7]:
($\Longrightarrow$) Veja que

$$\begin{aligned} ab = ac &\implies ab - ac = 0_A \\ &\implies ab + a(-c) = 0_A \\ &\implies a(b - c) = 0_A \end{aligned}$$

Como A não tem divisores de zero e por hipótese $a \neq 0_A$, temos $b - c = 0_A$, ou seja, $b = c$. E ainda, o outro item se verifica da mesma maneira.

($\Longleftarrow$) Sejam $a, b \in A$ tais que $ab = 0$. Suponha que $a \neq 0$. Aplicando a hipótese na igualdade $ab = 0 = a \cdot 0$, temos $b = 0$. Portanto, $a = 0$ ou $b = 0$, ou seja, o anel A não tem divisores de zero. ■

Definição 2.10. Seja $(A, +, \cdot)$ um anel. Dados $a \in A$ e $n \in \mathbb{N}^*$, definimos:

- $a^1 = a$;
- $a^{n+1} = a^n \cdot a$.

Quando A tem unidade também definimos $a^0 = 1$.

Proposição 2.25. *Seja $(A, +, \cdot)$ um anel.*

1. $a^m a^n = a^{m+n}$;
2. $(a^m)^n = a^{mn}$;
3. $(ab)^n = a^n b^n$, *quando* $ab = ba$.

Demonstração. Vide a Proposição 1.3.4. de [7]. ■

3 ELEMENTOS PRIMOS E ELEMENTOS IRREDUTÍVEIS DE UM ANEL

Vimos que pelo Teorema (Fundamental da Aritmética) 2.10 que qualquer número inteiro que seja maior do que um poder ser escrito como um produto de elementos primos. Você pode estar se questionando o motivo disso ser relevante. Quem descobriu os números primos provavelmente também se questionou sobre uma possível aplicação. E ela existe, nos dias atuais, para proteção de dados sigilosos, troca de informações confidenciais e preservação da privacidade através da criptografia.

Uma delas é a criptografia RSA, nomeada em homenagem aos seus criadores Rivest-Shamir-Adleman, a qual é um sistema de criptografia que consiste basicamente em duas chaves, uma chave pública formada pelo produto de dois primos grandes, e uma chave de desencriptação privada que consiste na fatoração da chave pública. Dessa forma, qualquer pessoa poderia enviar mensagens para você utilizando a chave pública, e só você poderia desencriptá-la com sua chave privada. Qualquer outra pessoa que gostaria de ler a mensagem criptografada sem a chave de desencriptação precisaria fatorar a chave pública na força bruta, mas este processo não é eficiente.

Os números primos servem, portanto, como base de uma série de algoritmos de segurança. A criptografia pode ser encontrada no algoritmo do seu banco digital e em aplicativos de redes sociais. Outro motivo para se estudar números primos é o conhecimento pelo conhecimento, já que o assunto é simplesmente fascinante.

Relembre que em $\mathbb{Z}$ temos dois caminhos equivalentes para mostrar que p é primo:

- quando $p \neq 0$, $p \neq \pm 1$ e ainda, se $x \mid p$, então $x = \pm p$ ou $x = \pm 1$;
- $p \mid ab$, então $p \mid a$ ou $p \mid b$.

Mas, se generalizarmos esses dois caminhos para um anel geral, eles não serão equivalentes. Por isso, o primeiro será utilizado para definir elementos irredutíveis e o segundo, para elementos primos.

Por este motivo, separaremos este capítulo em três seções: elementos primos em um anel $\mathbb{Z}_n$ (3.1), elementos irredutíveis em um anel $\mathbb{Z}_n$ (3.2) e o número de elementos primos e elementos irredutíveis de um anel $\mathbb{Z}_n$ (3.3).

3.1 ELEMENTOS PRIMOS DE UM ANEL

Definição 3.1. Seja o inteiro $n \geq 1$. Um elemento $\overline{0} \neq \overline{p} \in \mathbb{Z}_n$ é primo se $\overline{p} \mid \overline{a}\overline{b}$, então $\overline{p} \mid \overline{a}$ ou $\overline{p} \mid \overline{b}$, $\forall\, \overline{a}, \overline{b} \in \mathbb{Z}_n$.

A seguir será provado que dados dois elementos de $\mathbb{Z}_n$, $\overline{a}, \overline{b}$, tais que $\overline{a} \mid \overline{b}$, teremos que o máximo divisor comum entre a e n dividirá o máximo divisor comum entre b e n. Também será demonstrada a recíproca deste Lema. Ele será amplamente utilizado para demonstrar o Teorema 3.2.

Lema 3.1. *Dado inteiro $n \geq 1$, 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. Demonstraremos que

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

1. ($\Longrightarrow$) Note que escrever $\overline{a} \mid \overline{b}$ é equivalente a escrever $\overline{b} = \overline{a} \cdot \overline{k}$, em que $\overline{k} \in \mathbb{Z}_n$. Daí, reescrevendo a igualdade em $\mathbb{Z}$, temos que $ak + ny = b$, em que $y \in \mathbb{Z}$. Note que por definição, $\mathrm{mdc}(a, n) \mid a$ e $\mathrm{mdc}(a, n) \mid n$. Assim, pela Proposição 2.4, temos que $\mathrm{mdc}(a, n) \mid b$.

($\Longleftarrow$) Por hipótese, $\text{mdc}(a,n) \mid b$, ou seja, pelo Teorema 2.12, existe $x \in \mathbb{Z} : ax+ny = b$. Em $\mathbb{Z}_n$, temos $\overline{a}\overline{x} = \overline{b}$, e por definição, temos que $\overline{a} \mid \overline{b}$.

2. ($\Longrightarrow$) Por definição, $\text{mdc}(a,n) \mid n$. Por hipótese, $\text{mdc}(a,n) \mid b$. Daí, como $\text{mdc}(a,n) \mid n$ e $\text{mdc}(a,n) \mid b$, da definição de MDC, temos que $\text{mdc}(a,n) \mid \text{mdc}(b,n)$.

   ($\Longleftarrow$) Pela definição de MDC, temos que $\text{mdc}(b,n) \mid b$. E, por transitividade, $\text{mdc}(a,n) \mid b$.

■

A partir daqui, escreveremos algumas observações que serão amplamente utilizadas na demonstração do Teorema 3.2 a seguir.

Observação 2. Suponha que um produto de primos pq divide um número a. E, ainda, suponha que a não seja primo, ou seja, a é composto, digamos $a = bc$. Daí, temos $pq \mid bc$. Além disso, veja que utilizando o Teorema 2.10 podemos fatorar bc, e ainda, podemos juntar os fatores comuns em potências de p e de q. Dessa forma, vemos que podemos reescrever os números de tal forma que $p \nmid c$ e $q \nmid b$. Daí, como p, q são primos por hipótese, estes não podem ser fatorados como produto de outros primos e obrigatoriamente, $p \mid b$ e $q \mid c$.

Exemplo 3.1.1. Tome $p = 2$, $q = 3$ e $a = 60$. Note que podemos escrever $60 = 2 \cdot 2 \cdot 3 \cdot 5$. Veja que podemos escrever $60 = 4 \cdot 15$ e daí, $b = 4$ e $c = 15$, portanto $p \mid b$ e $q \mid c$.

Observação 3. Veja que, caso tomássemos $\text{mdc}(a,n) = 1$, então pelo Teorema 2.12, existiriam $x, y \in \mathbb{Z}$ tais que $ax + ny = 1$. Daí, em $\mathbb{Z}_n$,

$$\overline{a} \cdot \overline{x} + \overline{n} \cdot \overline{y} = \overline{1}. \tag{2}$$

E em $\mathbb{Z}_n$ qualquer múltiplo k de n, ou seja $k = cn$, pode ser reduzido à classe de equivalência $\overline{0}$, pois $k \equiv 0 \pmod{n}$. Logo, de (2), temos $\overline{a} \cdot \overline{x} + \overline{0} \cdot \overline{y} = \overline{1}$. Ou seja, $\overline{a} \cdot \overline{x} = \overline{1}$, e assim $\overline{a}$ é inversível.

Observação 4. Perceba que se $n \mid a$, então $a = nk$, $k \in \mathbb{Z}$, ou seja, em $\mathbb{Z}_n$, $\overline{a} = \overline{n} \cdot \overline{k} \iff \overline{a} = \overline{0}$.

Agora, dado $n \in \mathbb{N}$ enunciaremos a caracterização do conjunto dos números primos de $\mathbb{Z}_n$.

Teorema 3.2. *Dado o inteiro $n \geq 1$, o conjunto de elementos primos de $\mathbb{Z}_n$ é descrito por*

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

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

Demonstração. Note que $\overline{a} \in \mathbb{Z}_n$ deve ser diferente de $\overline{0}$ pela definição de elemento primo. Assim, tome $\overline{a} \in \mathbb{Z}_n$ não nulo. Seja $\overline{a}$ não inversível, então temos $\mathrm{mdc}(a, n) \neq 1$ e $n \nmid a$, pois no primeiro caso, $\overline{a}$ seria inversível, conforme a Observação 3, e no segundo caso, $\overline{a} = \overline{0}$ segundo a Observação 4.
Perceba que pelo Teorema 2.10 é possível fatorar qualquer número como um produto único de primos. Assim, a demonstração deste teorema será dividida em três casos:

1. A fatoração do $\mathrm{mdc}(a, n)$ ser o produto de pelo menos dois primos distintos p, q, ou seja, $pq \mid \mathrm{mdc}(a, n)$. Será demonstrado que $\overline{a}$ não pertence ao conjunto de elementos primos de $\mathbb{Z}_n$;

2. A fatoração do $\mathrm{mdc}(a, n)$ ser o produto de dois ou mais primos iguais p, isto é, $\mathrm{mdc}(a, n) = p^k$, em que $k \geq 2 \in \mathbb{N}$ e novamente provaremos que $\overline{a}$ não é elemento primo de $\mathbb{Z}_n$;

3. A fatoração do $\text{mdc}(a, n)$ ser composta por apenas um primo p, $\text{mdc}(a, n) = p$. Provaremos que $\overline{a}$ pertence ao conjunto de elementos primos de $\mathbb{Z}_n$.

Perceba que com estes três casos já abordamos todos os casos possíveis e, em todos os casos utilizaremos que

$$\text{mdc}(a, n) \mid a \tag{3}$$

e,

$$\text{mdc}(a, n) \mid n. \tag{4}$$

1. Temos por hipótese que

$$pq \mid \text{mdc}(a, n), \tag{5}$$

em que p, q são primos distintos. E, por transitividade de (3) e (5),

$$pq \mid a. \tag{6}$$

Assim, temos o produto de dois primos distintos dividindo um número. Ou seja, a não poderá ser primo, daí tome $a = bc$. E, substituindo esta nova informação em (6), obtemos

$$pq \mid bc.$$

Conforme a Observação 2, suponha sem perda de generalidade que $p \nmid c$ e $q \nmid b$, e obtenha, $p \mid b$ e $q \mid c$, respectivamente. E ainda, como $a = bc$, então em particular, $a \mid bc$, ou seja em $\mathbb{Z}_n$, teremos $\overline{a} \mid \overline{b} \cdot \overline{c}$. Lembrando o leitor que queremos mostrar que $\overline{a}$ não é primo, e para isto, demonstraremos que $\overline{a} \nmid \overline{b}$ e $\overline{a} \nmid \overline{c}$.

Suponha por absurdo que $\overline{a} \mid \overline{b}$, então pelo Lema 3.1, $\text{mdc}(a, n) \mid \text{mdc}(b, n)$. E usando transitividade em (5), temos

$$pq \mid \text{mdc}(b, n).$$

Daí, por transitividade, $pq \mid b$ e $pq \mid n$. Lembre que $p \mid b$ e $q \nmid b$, e assim, pelo Teorema 2.5, obtemos que $pq \nmid b$, o que é um absurdo e implica que $\overline{a} \nmid \overline{b}$. Logo, $\overline{a} \nmid \overline{b}$ e de forma análoga, $\overline{a} \nmid \overline{c}$. Portanto, $\overline{a}$ não é primo, conforme desejado.

2. Por hipótese, temos

$$\text{mdc}(a, n) = p^k, \tag{7}$$

em que $k \geq 2 \in \mathbb{N}$. Seja $a = p^{k-1} \cdot a_1$,em que $0 < a_1 < a < n$. Em $\mathbb{Z}_n$, $\overline{a} = \overline{p^{k-1}} \cdot \overline{a_1}$, e em particular, $\overline{a} \mid \overline{p^{k-1}} \cdot \overline{a_1}$. Assim, da mesma forma que no caso anterior, provaremos que $\overline{a} \nmid \overline{p^{k-1}}$ e $\overline{a} \nmid \overline{a_1}$ em $\mathbb{Z}_n$, pois desejamos mostrar que $\overline{a}$ não é primo. Suponha por absurdo que $\overline{a} \mid \overline{p^{k-1}}$. Então, pelo Lema 3.1, $\text{mdc}(a, n) \mid \text{mdc}(p^{k-1}, n)$. Da hipótese (7) na equação anterior, temos

$$p^k \mid \text{mdc}(p^{k-1}, n).$$

E como por definição $\text{mdc}(p^{k-1}, n) \mid p^{k-1}$, temos por transitividade que

$$p^k \mid p^{k-1}.$$

O que consiste num absurdo, e portanto, $\overline{a} \nmid \overline{p^{k-1}}$. Agora basta mostrar que $\overline{a} \nmid \overline{a_1}$ para que $\overline{a}$ não seja primo em $\mathbb{Z}_n$. Dessa forma, suponha por absurdo que $\overline{a} \mid \overline{a_1}$. Novamente pelo Lema 3.1, $\text{mdc}(a, n) \mid \text{mdc}(a_1, n)$, ou seja, $p^k \mid \text{mdc}(a_1, n)$, e por transitividade $p^k \mid a_1$. Assim, $a_1 = p^{k-1} \cdot a_2$, onde $0 < a_2 < a_1 < a < n$ Note que estamos utilizando os mesmo artifícios realizados anteriormente. Em $\mathbb{Z}_n$, $\overline{a_1} = \overline{p^{k-1}} \cdot \overline{a_2}$, isto é,

$$\overline{a_1} \mid \overline{p^{k-1}} \cdot \overline{a_2}.$$

Daí, suponha que $\overline{a_1} \mid \overline{p^{k-1}}$. Então, pelo Lema 3.1, $\text{mdc}(a_1, n) \mid \text{mdc}(p^{k-1}, n)$. Usando a hipótese, $p^k \mid \text{mdc}(p^{k-1}, n)$. E como por definição $\text{mdc}(p^{k-1}, n) \mid p^{k-1}$, temos por transitividade que

$$p^k \mid p^{k-1}.$$

O que consiste em um absurdo, e assim, $\overline{a_1} \nmid \overline{p^{k-1}}$.

Agora, suponha que $\overline{a_1} \mid \overline{a_2}$. Novamente pelo Lema 3.1, temos $\text{mdc}(a_1, n) \mid \text{mdc}(a_2, n)$. Logo, $p^k \mid \text{mdc}(a_2, n)$, e por transitividade $p^k \mid a_2$. Ou seja, $a_2 = p^{k-1} \cdot a_3$, onde $0 < a_3 < a_2 < a_1 < a < n$.

E realizando novamente o mesmo processo, supondo $\overline{a_2} \mid \overline{p^{k-1}}$, e isso resultará em $p^k \mid p^{k-1}$, que é um absurdo. E, supondo $\overline{a_2} \mid \overline{a_3}$, obteremos $a_3 = p^{k-1} \cdot a_4$, onde $0 < a_4 < a_3 < a_2 < a_1 < a < n$.

Continuando este processo, em algum momento $a_{n-1} = p^{k-1} \cdot a_n$, em que $0 < a_n < a_{n-1} < \cdots < a_1 < a < n$ e

$$a_n < p^{k-1}. \tag{8}$$

Se aplicarmos este processo mais uma vez, concluiríamos a partir de $\overline{a_{n-1}} \mid \overline{a_n}$, que $a_n = p^{k-1} \cdot a_{n+1}$, o que contradiz (8). Daí, $\overline{a_{n-1}} \nmid \overline{a_n}$, ou seja, pela Proposição 2.2, $\overline{a_{n-1}} \cdot \overline{p^{k-1}} \nmid \overline{a_n} \cdot \overline{p^{k-1}}$, que implica em $\overline{a_{n-2}} \nmid \overline{a_{n-1}}$, e assim sucessivamente até $\overline{a} \nmid \overline{a_1}$, e portanto, $\overline{a}$ não é primo.

3. Por hipótese, existe p primo tal que

$$\text{mdc}(a, n) = p. \tag{9}$$

Substituindo (9) em (3), obtemos

$$p \mid a. \tag{10}$$

Lembrando que por construção, $n \nmid a$, e assim, $p \neq n$. E, substituindo (9) em (4), temos

$$p \mid n. \tag{11}$$

Logo, $n > p$. Por (12) e como $p \mid p$, então $\text{mdc}(p, n) = p = \text{mdc}(a, n)$. Ou seja, $\text{mdc}(p, n) \mid \text{mdc}(a, n)$ e $\text{mdc}(a, n) \mid \text{mdc}(p, n)$. Daí, pelo Lema 3.1, obtemos $\overline{p} \mid \overline{a}$ e

$$\overline{a} \mid \overline{p}, \tag{12}$$

respectivamente.

Como desejamos mostrar que $\overline{a}$ é primo em $\mathbb{Z}_n$, denotaremos este elemento como o produto de outros dois elementos no anel dos inteiros módulo n, digamos $\overline{b}, \overline{c}$, ou seja, $\overline{a} \mid \overline{b} \cdot \overline{c}$. Mas isto é equivalente a dizer que existem $r, s \in \mathbb{Z}$ tais que $bc = ar + ns$. E ainda, como temos (10) e (11), então pela Proposição 2.4, $p \mid bc$. Mas, como p é primo em $\mathbb{Z}$ por hipótese, então $p \mid b$ ou $p \mid c$.

Suponha que $p \mid b$, daí em $\mathbb{Z}_n$, temos $\overline{p} \mid \overline{b}$. E disso e usando transitividade em (12), obtemos $\overline{a} \mid \overline{b}$. Além disso, $\overline{a} \mid \overline{c}$ é obtido de modo análogo supondo que $p \mid c$. Logo, como $\overline{a} \mid \overline{b}$ ou $\overline{a} \mid \overline{c}$, temos que por definição $\overline{a}$ é primo.

■

Exemplo 3.1.2. Seja

$$\mathbb{Z}_{10} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}\}$$

Utilizando o Teorema 3.2, perceba que os elementos primos são:

$$\{\overline{2}, \overline{4}, \overline{5}, \overline{6}, \overline{8}\},$$

pois,

$$\begin{aligned}
\overline{2}&, \text{ pois } \operatorname{mdc}(2,10) = 2, 2 < 10 \text{ e } 2 \in \pi_{10};\\
\overline{4}&, \text{ pois } \operatorname{mdc}(4,10) = 2, 2 < 10 \text{ e } 2 \in \pi_{10};\\
\overline{5}&, \text{ pois } \operatorname{mdc}(5,10) = 5, 5 < 10 \text{ e } 5 \in \pi_{10};\\
\overline{6}&, \text{ pois } \operatorname{mdc}(6,10) = 2, 2 < 10 \text{ e } 2 \in \pi_{10};\\
\overline{8}&, \text{ pois } \operatorname{mdc}(8,10) = 2, 2 < 10 \text{ e } 2 \in \pi_{10}.
\end{aligned}$$

Exemplo 3.1.3. Seja

$$\mathbb{Z}_{15} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, \overline{10}, \overline{11}, \overline{12}, \overline{13}, \overline{14}\}.$$

Utilizando o Teorema 3.2, note que destes, os elementos primos são:

$$\{\overline{3}, \overline{5}, \overline{6}, \overline{9}, \overline{10}, \overline{12}\},$$

pois,

$$\begin{aligned}
\overline{3}&, \text{ pois } \operatorname{mdc}(3,15) = 3, 3 < 15 \text{ e } 3 \in \pi_{15};\\
\overline{5}&, \text{ pois } \operatorname{mdc}(5,15) = 5, 5 < 15 \text{ e } 5 \in \pi_{15};\\
\overline{6}&, \text{ pois } \operatorname{mdc}(6,15) = 3, 3 < 15 \text{ e } 3 \in \pi_{15};\\
\overline{9}&, \text{ pois } \operatorname{mdc}(9,15) = 3, 3 < 15 \text{ e } 3 \in \pi_{15};\\
\overline{10}&, \text{ pois } \operatorname{mdc}(10,15) = 5, 5 < 15 \text{ e } 5 \in \pi_{15};\\
\overline{12}&, \text{ pois } \operatorname{mdc}(12,15) = 3, 3 < 15 \text{ e } 3 \in \pi_{15}.
\end{aligned}$$

Exemplo 3.1.4. Seja

$$\mathbb{Z}_{19} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, \overline{10}, \overline{11}, \overline{12}, \overline{13}, \overline{14}, \overline{15}, \overline{16}, \overline{17}, \overline{18}\}$$

Utilizando o Teorema 3.2 perceba que destes, não temos nenhum elemento primo, pois os representantes de todos os elementos a seguir possuem como máximo divisor comum entre si e 19 o número 1, o qual não é primo e portanto $1 \notin \pi_{19}$.

3.2 ELEMENTOS IRREDUTÍVEIS DE UM ANEL

Definição 3.2. Dado o inteiro $n \geq 1$, 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 $\overline{a} = \overline{xy}$, então, $\overline{x}$ ou $\overline{y}$ será inversível.

Sabemos, por definição, que um elemento de um anel é inversível se este operado com sua segunda operação resultar na unidade da segunda operação. Mas como saber se um elemento $\overline{a}$ de $\mathbb{Z}_n$ é inversível sem ficar de forma braçal e bruta efetuando cálculos? É simples, basta utilizar a proposição a seguir.

Proposição 3.3. *Seja o inteiro $n \geq 1$ e $\overline{a} \in \mathbb{Z}_n$. Assim, $\overline{a}$ é inversível se, e somente se,* $\text{mdc}(a, n) = 1$.

Demonstração. ($\Longrightarrow$) Suponha que $\overline{a}$ seja inversível, ou seja, $\overline{a} \cdot \overline{x} = \overline{1}$, $\overline{x} \in \mathbb{Z}_n$. Em $\mathbb{Z}$, temos que $ax + ny = 1$, e pelo Teorema 2.12, $\text{mdc}(a, n) = 1$.
($\Longleftarrow$) Se $\text{mdc}(a, n) = 1$, então pelo Teorema 2.12, existem $x, y \in \mathbb{Z}$ tais que $ax + ny = 1$. Em $\mathbb{Z}_n$, temos $\overline{a} \cdot \overline{x} = \overline{1}$. ■

Exemplo 3.2.1. Seja $\overline{3} \in \mathbb{Z}_{20}$. Veja que $\text{mdc}(3, 20) = 1$. Calcularemos o elemento inverso de $\overline{3}$ em $\mathbb{Z}_{20}$.
Pelo Teorema 2.12, $\exists\, x, y \in \mathbb{Z} : 3x + 20y = 1$. Utilizando equações diofantinas, encontramos uma solução para a equação anterior.
Passo 1:

$$20 = 3 \cdot 6 + 2$$
$$3 = 2 \cdot 1 + 1$$

Passo 2:

$$2 = 20 - 3 \cdot 6$$
$$1 = 3 - 2 \cdot 1$$

Passo 3:

$$\begin{aligned} 1 &= 3 - 2 \cdot 1 \\ &= 3 - (20 - 3 \cdot 6) \cdot 1 \\ &= 3 - 20 + 3 \cdot 6 \\ &= 20 \cdot (-1) + 3 \cdot 7 \end{aligned}$$

Logo, $x = 7$ e $y = -1$. E perceba que $\overline{3} \cdot \overline{7} = \overline{3 \cdot 7} = \overline{21} = \overline{1}$, ou seja, o inverso de $\overline{3}$ em $\mathbb{Z}_{20}$ é $\overline{7}$.

A seguir, seguem dois exemplos em que utilizaremos a Proposição 3.3 para mostrar quais os elementos inversíveis de modo geral em um anel de inteiros módulo n.

Exemplo 3.2.2. Quem são os elementos inversíveis de $\mathbb{Z}_3$?

Note que $\overline{x} \in \mathbb{Z}_3$ é inversível se $\text{mdc}(x, 3) = 1$, conforme a Proposição 3.3. Assim, como $\text{mdc}(1, 3) = 1$ e $\text{mdc}(2, 3) = 1$, temos que os elementos inversíveis do conjunto são:

$$\{\overline{1}, \overline{2}\}.$$

Exemplo 3.2.3. Quem são os elementos inversíveis de $\mathbb{Z}_4$?
Veja que $\overline{x} \in \mathbb{Z}_4$ é inversível se $\text{mdc}(x, 4) = 1$, conforme a Proposição 3.3. Assim, como $\text{mdc}(1, 4) = 1$ e $\text{mdc}(3, 4) = 1$, temos que os elementos inversíveis do conjunto são:

$$\{\overline{1}, \overline{3}\}.$$

Teorema 3.4. *Dado o inteiro $n \geq 1$, o conjunto de elementos irredutíveis de $\mathbb{Z}_n$ é descrito por*

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

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

Demonstração. Seja $\overline{a} \in \mathbb{Z}_n$, com $\overline{a} \neq \overline{0}$ e $\overline{a} \neq \overline{1}$. Daí, da mesma forma que no Teorema 3.2, teremos $\text{mdc}(a, n) \neq 1$, conforme a Observação 3 e $n \nmid a$, segundo a Observação 4.
Perceba também que teremos apenas três casos possíveis para $\overline{a}$. Mostraremos que

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

Mostraremos que nos dois primeiros casos $\overline{a}$ não é irredutível, mas que o é no terceiro caso. Em todos os casos listados, utilizaremos que pela definição de mdc, temos

$$\text{mdc}(a, n) \mid a \tag{13}$$

e,

$$\text{mdc}(a, n) \mid n. \tag{14}$$

1. Por hipótese,

   $$pq \mid \text{mdc}(a, n), \tag{15}$$

   em que p, q são primos não necessariamente distintos. Note que da mesma forma que na demonstração do primeiro item do Teorema 3.2, por transitividade de (15) em (13), temos $pq \mid a$. Mas novamente, como p, q são primos por hipótese, então a não pode ser primo. Daí, tome $a = bc$, e por transitividade de (15) em (13), temos $pq \mid bc$, em que

   $$p \mid c \tag{16}$$

   e

   $$q \mid b, \tag{17}$$

pela Observação 2 localizada na Seção (3.1).

Mostraremos que $\overline{b}, \overline{c}$ não são inversíveis, ou seja, $\overline{b}, \overline{c} \nmid \overline{1}$. Suponha por absurdo que $\overline{b} \mid \overline{1}$. Isso é equivalente a dizer que existe $\overline{k} \in \mathbb{Z}_n$ tal que $\overline{k} \cdot \overline{b} = \overline{1}$. Daí,

$$kb + xn = 1 \tag{18}$$

com $k, x \in \mathbb{Z}$, mas de (15) obtemos por transitividade que $q \mid n$, e como temos (17), podemos então aplicar a Proposição 2.4 em (18) e obter que $q \mid 1$. O que consiste em um absurdo, pois q é primo em $\mathbb{Z}$ por hipótese. Assim, $\overline{b} \nmid \overline{1}$, e ainda, o caso $\overline{c} \nmid \overline{1}$ é obtido de modo análogo. Dessa forma, como $\overline{b} \nmid \overline{1}$ e $\overline{c} \nmid \overline{1}$, então $\overline{a} = \overline{b} \cdot \overline{c}$ não é irredutível.

2. Por hipótese, temos

$$\mathrm{mdc}(a, n) = p \tag{19}$$

e

$$p^2 \nmid n, \tag{20}$$

com p primo.

Assim, de (19) em (13) e (14), temos

$$p \mid a \tag{21}$$

e

$$p \mid n. \tag{22}$$

Note que $p \mid p^2$, daí, $\mathrm{mdc}(n, p^2) = p$. Perceba ainda que $p^2 \mid p^2$, mas como vale (20), então temos $\mathrm{mdc}(n, p^2) = p$.

E ainda, pelo Teorema 2.12, temos

$$p = nr + p^2 s,$$

em que $r, s \in \mathbb{Z}$.

Porém, note que de (21) temos que $a = kp$, em que $k \in \mathbb{Z}$. Agora, multiplique a equação anterior por k, e defina $x = rk$, $y = sk$, daí

$$a = nx + p^2 y.$$

Em $\mathbb{Z}_n$, temos $\overline{a} = \overline{p^2 y} = \overline{p} \cdot \overline{py}$, e em particular, $\overline{a} \mid \overline{p} \cdot \overline{py}$, ou seja, $\overline{a}$ divide um produto de números. Como este é um caso que não nos interessa, provaremos de forma similar ao item anterior que $\overline{p}, \overline{py} \nmid \overline{1}$.

Suponha por absurdo que $\overline{p} \mid \overline{1}$. Ou seja, existe $\overline{k} \in \mathbb{Z}_n$ tal que $\overline{k} \cdot \overline{p} = \overline{1}$. Pelo Teorema 2.12, temos $kp + mn = 1$, com $k, m \in \mathbb{Z}$. E, como $p \mid p$, e ainda, temos (22), podemos aplicar a Proposição 2.4, que resulta em

$$p \mid 1,$$

o que é um absurdo, já que p é um primo em $\mathbb{Z}$ por hipótese. Dessa forma, provamos que $\overline{p}$ não é inversível em $\mathbb{Z}_n$. Note que a demonstração de $\overline{py}$ não ser inversível segue de forma análoga, e portanto, temos que $\overline{a}$ não é irredutível, conforme desejado.

3. Por hipótese,

$$\text{mdc}(a, n) = p \tag{23}$$

e

$$p^2 \mid n, \tag{24}$$

com p primo.

Seja $\overline{a} = \overline{b} \cdot \overline{c}$, assim existe $k \in \mathbb{Z}$ tal que

$$a = bc + kn. \tag{25}$$

Note que de (23), temos que

$$p \mid a \tag{26}$$

e

$$p \mid n. \tag{27}$$

Daí, como temos (26) e (27), aplicando a Proposição 2.4 em (25), isso resulta em $p \mid bc$. E já que p é primo em $\mathbb{Z}$ por hipótese, sabemos que p divide pelo menos um dos fatores ou ambos os fatores. Demonstraremos a seguir que p divide apenas um destes. Suponha por absurdo que $p \mid b$ e $p \mid c$. Daí, pela Proposição 2.3, $p \cdot p \mid b \cdot c$, ou seja, $p^2 \mid bc$. E como temos (24), então aplicando a Proposição 2.4 na equação (25), teríamos que $p^2 \mid a$, o que é um absurdo, pois aí $\text{mdc}(a, n)$ seria no mínimo p^2, ou seja, $p = \text{mdc}(a, n) \geq p^2$. Dessa forma, temos que

$$p \mid b \tag{28}$$

e

$$p \nmid c, \tag{29}$$

ou que $p \nmid b$ e $p \mid c$. Suponha sem perda de generalidade que ocorra o primeiro caso.

Mostraremos que se existir outro primo q em π_n que divida n além de p, então $q \nmid c$. Assim, $q \in \pi_n - \{p\}$, ou seja, $q \mid n$. Suponha por absurdo que $q \mid c$. Daí, $\text{mdc}(c, n) \geq q$, porém, aplicando a Proposição 2.4 em (25), teríamos que $q \mid a$. Daí, como $q \mid n$, então pela definição de MDC, teríamos que $q \mid \text{mdc}(a, n)$. Mas isto configura um absurdo, pois usando (23), obtemos $q \mid p$, e ambos os números são primos distintos. Dessa forma, não existe um outro primo q que divida n e c ao mesmo tempo. Daí, como temos (29), então $\text{mdc}(c, n) \neq p$, e como acabamos de provar que se existir outro primo q além de p que divida n, $q \nmid c$, então $\text{mdc}(c, n) = 1$, e pelo Teorema 2.12, temos que existem $x, y \in \mathbb{Z}$ tais que $cx + ny = 1$. E, em $\mathbb{Z}_n$, $\overline{c} \cdot \overline{x} = \overline{1}$, ou

seja, $\overline{c}$ é inversível, e supondo que $p \mid c$ obtemos que $\overline{b}$ é inversível de modo análogo.

E ainda, para mostrarmos que $\overline{a}$ é irredutível, temos que mostrar que $\overline{a}$ não é inversível. Suponha que $\overline{a} \mid \overline{1}$, isto é, existe $\overline{m} \in \mathbb{Z}_n$ tal que $\overline{m} \cdot \overline{a} = \overline{1}$. Daí, $ma + on = 1$, $o \in \mathbb{Z}$, e como valem (26) e (27), ao aplicar o Teorema 2.4, obtemos que

$$p \mid 1.$$

O que consiste em um absurdo, pois p é primo em $\mathbb{Z}$. Assim, $\overline{a}$ não é inversível, e portanto, $\overline{a}$ é irredutível.

■

Exemplo 3.2.4. Tome $n = 20$ e $a = 15$. Note que $\text{mdc}(15, 20) = 5$. Veja também que $5^2 \nmid 20$, logo $\overline{15}$ não é irredutível em $\mathbb{Z}_{20}$.

Exemplo 3.2.5. Tome $n = 45$ e $a = 12$. Note que $\text{mdc}(12, 45) = 3$. Veja também que $3^2 \mid 45$, logo $\overline{12}$ é irredutível em $\mathbb{Z}_{45}$. Ou seja, pela definição de irredutível como $\overline{12} = \overline{3} \cdot \overline{4}$, $\overline{3}$ ou $\overline{4}$ deve ser inversível em $\mathbb{Z}_{45}$. Note que $\overline{4} \cdot \overline{34} = \overline{136} = \overline{1}$, ou seja, $\overline{4}$ é inversível em $\mathbb{Z}_{45}$.

Exemplo 3.2.6. Seja

$$\mathbb{Z}_8 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}\}.$$

Utilizando o Teorema 3.4, note que seus elementos irredutíveis são:

$$\{\overline{2}, \overline{6}\},$$

pois,

$$\overline{2}, \text{ pois } \text{mdc}(2, 8) = 2 \mid 8 \text{ e } 2^2 = 4 \mid 8;$$
$$\overline{6}, \text{ pois } \text{mdc}(2, 8) = 2 \mid 8 \text{ e } 2^2 = 4 \mid 8.$$

Exemplo 3.2.7. 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 o Teorema 3.4, 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 irredutíveis em $\mathbb{Z}_{13}$.

Exemplo 3.2.8. Seja

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

Utilizando o Teorema 3.4, perceba que são elementos irredutíveis:

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

pois,

$$\begin{aligned}\overline{3},\ &\text{pois } \operatorname{mdc}(3,45) = 3, 3 \mid 45 \text{ e } 3^2 = 9 \mid 45;\\ \overline{6},\ &\text{pois } \operatorname{mdc}(6,45) = 3, 3 \mid 45 \text{ e } 3^2 = 9 \mid 45;\\ \overline{12},\ &\text{pois } \operatorname{mdc}(12,45) = 3, 3 \mid 45 \text{ e } 3^2 = 9 \mid 45;\\ \overline{21},\ &\text{pois } \operatorname{mdc}(21,45) = 3, 3 \mid 45 \text{ e } 3^2 = 9 \mid 45;\\ \overline{24},\ &\text{pois } \operatorname{mdc}(24,45) = 3, 3 \mid 45 \text{ e } 3^2 = 9 \mid 45;\\ \overline{33},\ &\text{pois } \operatorname{mdc}(33,45) = 3, 3 \mid 45 \text{ e } 3^2 = 9 \mid 45;\\ \overline{39},\ &\text{pois } \operatorname{mdc}(39,45) = 3, 3 \mid 45 \text{ e } 3^2 = 9 \mid 45;\\ \overline{42},\ &\text{pois } \operatorname{mdc}(42,45) = 3, 3 \mid 45 \text{ e } 3^2 = 9 \mid 45.\end{aligned}$$

Veja que o MDC entre os representantes das classes a seguir e 45 não resulta em um número primo:

$$\begin{aligned}&\overline{0}, \overline{1}, \overline{2}, \overline{4}, \overline{7}, \overline{8}, \overline{9}, \overline{11}, \overline{13}, \overline{14}, \overline{15}, \overline{16}, \overline{17}, \overline{18},\\ &\overline{19}, \overline{22}, \overline{23}, \overline{26}, \overline{27}, \overline{28}, \overline{29}, \overline{30}, \overline{31}, \overline{32}, \overline{34}, \overline{36},\\ &\overline{37}, \overline{38}, \overline{40}, \overline{41}, \overline{43}, \overline{44}.\end{aligned}$$

Também o MDC entre os representantes das classes a seguir e 45 resulta em um primo, sendo que este divide 45, mas elevando este primo ao quadrado, nós obtemos um número que não divide 45:

$$\overline{5}, \overline{10}, \overline{20}, \overline{25}, \overline{35}.$$

Ou seja, não são irredutíveis em $\mathbb{Z}_{45}$:

$$\{\overline{0}, \overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}, \overline{9}, \overline{10}, \overline{11}, \overline{13}, \overline{14}, \overline{15}, \overline{16}, \overline{17}, \overline{18},$$
$$\overline{19}, \overline{20}, \overline{22}, \overline{23}, \overline{25}, \overline{26}, \overline{27}, \overline{28}, \overline{29}, \overline{30}, \overline{31}, \overline{32}, \overline{34},$$
$$\overline{35}, \overline{36}, \overline{37}, \overline{38}, \overline{40}, \overline{41}, \overline{43}, \overline{44}\}.$$

3.3 O NÚMERO DE PRIMOS E IRREDUTÍVEIS DE UM ANEL

Para começar, vamos relembrar o que é uma função conforme a Seção 3 do Capítulo 1 de [8].

Definição 3.3. Uma função $f : A \to B$ consta de três partes: um conjunto A, chamado de domínio da função (ou o conjunto onde a função é definida), um conjunto B chamado de contradomínio da função (ou o conjunto onde a função toma valores) e uma regra que permite associar, de modo determinado, a cada elemento $x \in A$, um único elemento $f(x) \in B$, chamado o valor que a função assume em x (ou no ponto x). Usa-se a notação $x \mapsto f(x)$ para indicar que f faz corresponder a x o valor $f(x)$.

Note que no teorema a seguir, estamos trabalhando com uma função que vai de um subconjunto de $\mathbb{Z}_n$ à outro subconjunto de $\mathbb{Z}_m$. Portanto, usaremos uma barra para denotar um elemento do domínio e duas barras para denotar um elemento do contradomínio.

Teorema 3.5. *Seja* $1 \leq n = pm \in \mathbb{N}$, $p \in \pi_n$ *e* $A_p = \{\overline{a} \in \mathbb{Z}_n : \text{mdc}(a, n) = p\}$. *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* $U(\mathbb{Z}_m) = \{\overline{a} \in \mathbb{Z}_m : \text{mdc}(a, m) = 1\}$ *e* $\dfrac{\overline{\overline{a}}}{p} \in U(\mathbb{Z}_m)$.

Demonstração. Sejam $\overline{a}, \overline{b} \in A_p$. Daí, pela definição do conjunto, temos

$$\begin{aligned} &\text{mdc}(a, n) = p = \text{mdc}(b, n) \\ \iff &\text{mdc}(a, pm) = p = \text{mdc}(b, pm). \end{aligned}$$

E, do Corolário 2.7, temos

$$\text{mdc}\left(\frac{a}{p}, m\right) = 1 = \text{mdc}\left(\frac{b}{p}, m\right).$$

Portanto, pela definição de $U(\mathbb{Z}_m)$, temos

$$\frac{\overline{\overline{a}}}{p}, \frac{\overline{\overline{b}}}{p} \in U(\mathbb{Z}_m).$$

A seguir, demonstraremos que a função é

1. Bem definida e injetora;
2. Sobrejetora.

Assim, provando estes três itens, teremos uma função bijetora conforme desejado.

1. Para mostrar que a função é bem definida, basta mostrar que dados $\overline{a} = \overline{b}$, então $\dfrac{\overline{\overline{a}}}{p} = \dfrac{\overline{\overline{b}}}{p}$. E, para mostrar que uma função é injetora, basta demonstrar que dados quaisquer dois elementos distintos pertencentes ao domínio, estes sempre vão possuir imagens diferentes no contradomínio. Portanto, sejam $\overline{a}, \overline{b} \in \mathbb{Z}_n$. Além disso, suponha que $f(\overline{a}) = f(\overline{b})$. Agora, basta mostrar que $\overline{a} = \overline{b}$.

$$
\begin{aligned}
f(\overline{a}) = f(\overline{b}) &\overset{a)}{\iff} \frac{\overline{\overline{a}}}{p} = \frac{\overline{\overline{b}}}{p} \\
&\overset{b)}{\iff} m \mid \frac{a}{p} - \frac{b}{p} \\
&\overset{c)}{\iff} m \cdot p \mid \left(\frac{a}{p} - \frac{b}{p}\right) \cdot p \\
&\overset{d)}{\iff} n \mid \frac{a}{p} \cdot p - \frac{b}{p} \cdot p \\
&\iff n \mid a - b \\
&\overset{e)}{\iff} \overline{a} = \overline{b}.
\end{aligned}
$$

Veja que a injetividade é provada pela ida e a função ser bem definida é provada pela volta. Veja a seguir as explicações de cada equivalência:

a) definição da função f;

b) pelo que vimos na Seção 2.7, quando duas classes de equivalência são iguais, n dividirá a subtração dos dois elementos representantes das classes de equivalência;

c) multiplicamos ambos os lados por p;

d) no lado esquerdo, usamos a hipótese de que $n = pm$, e no lado direito, a distributividade;

e) mesmo caso do item b).

Logo, f é injetora e bem definida.

2. Para mostrar que uma função é sobrejetora, basta mostrar que todos os elementos do seu contradomínio são correspondentes de um único elemento no domínio. Tome $\overline{\overline{x}} \in U(\mathbb{Z}_m)$ arbitrário. Pela definição do conjunto, $\text{mdc}(x, m) = 1$. Daí, pela Proposição 2.7, podemos multiplicar todos os fatores da igualdade anterior

por p, o que resulta em $\text{mdc}(px, pm) = p$, e como por hipótese, $n = pm$, $\text{mdc}(px, n) = p$. Veja que pela definição de A_p, $\overline{px} \in A_p$. E ainda, veja que $f(\overline{px}) = \dfrac{\overline{\overline{px}}}{p} = \overline{\overline{x}}$. Portanto, f é sobrejetora.

■

Utilizaremos a função φ de Euler para calcular a quantidade de elementos primos e de elementos irredutíveis de $\mathbb{Z}_n$. Assim, a definiremos a seguir.

Definição 3.4. Seja m um inteiro positivo e $x \in \mathbb{Z}$. Denotaremos

$$\varphi(m) = \#\{x : 1 \leq x \leq m \text{ e } \text{mdc}(x, m) = 1\}.$$

Dessa forma, conforme [5], $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(2520) = 576$ e $\varphi(p) = p - 1$, em que p é primo. Veja que de fato, os elementos coprimos à:

- 1, é apenas o elemento 1;
- 2, é apenas o elemento 1;
- 3 são os elementos 1 e 2;
- 4 são os elementos 1 e 3;
- 5 são os elementos 1, 2, 3 e 4;
- 6 são os elementos 1 e 5;
- 7 são os elementos 1, 2, 3, 4, 5 e 6;
- 9 são os elementos 1, 2, 4, 5, 7 e 8;
- 15 são os elementos 1, 2, 4, 7, 8, 11, 13 e 14.

O número de elementos primos e de elementos irredutíveis de $\mathbb{Z}_n$ é dado pelo Corolário 3.6 a seguir.

Corolário 3.6. *Dado inteiro $n \geq 1$ temos, em $\mathbb{Z}_n$, que a quantidade de:*

1. *elementos primos é dada por*

$$\sum_{\substack{p \in \pi_n \\ p<n}} \varphi\left(\frac{n}{p}\right),$$

2. *elementos irredutíveis é dada por*

$$\sum_{\substack{p \in \pi_n \\ p^2 | n}} \varphi\left(\frac{n}{p}\right),$$

em que φ é função de Euler.

Demonstração. Primeiramente, demonstraremos que o conjunto que mostramos ser o conjunto dos elementos primos (primeiro item) e o conjunto dos elementos irredutíveis (segundo item) são iguais às uniões disjuntas de A_p, tais que p satisfaz as condições de cada conjunto:

1. $\{\overline{a} \in \mathbb{Z}_n : \exists\, p \in \pi_n, p < n, \mathrm{mdc}(a, n) = p\} = \overset{\circ}{\bigcup\limits_{\substack{p \in \pi_n \\ p<n}}} A_p$;

2. $\left\{\overline{a} \in \mathbb{Z}_n : \exists\, p \in \pi_n, p^2 \mid n, \mathrm{mdc}(a, n) = p\right\} = \overset{\circ}{\bigcup\limits_{\substack{p \in \pi_n \\ p^2 | n}}} A_p$.

Veja que as demonstrações saem diretamente da definição do conjunto A_p.

1. Suponha $\overline{a} \in \{\overline{a} \in \mathbb{Z}_n : \exists\, p \in \pi_n, p < n, \text{mdc}(a,n) = p\}$. Assim, $\text{mdc}(a,n) = p$, para algum p, ou seja, $\overline{a} \in A_p$ e estará na união. E se $\overline{a}$ pertence ao segundo, então pertence a pelo menos um A_p, e se pertence a algum A_p, então pertence ao primeiro, isto é,

$$\overline{a} \in \{\overline{a} \in \mathbb{Z}_n : \exists\, p \in \pi_n, p < n, \text{mdc}(a,n) = p\} \iff \overline{a} \in \overset{\circ}{\bigcup_{\substack{p \in \pi_n \\ p<n}}} A_p;$$

2. Da mesma forma que o primeiro item, se $\overline{a}$ pertence ao primeiro, pela definição de A_p, o elemento estará em algum A_p e portanto, estará na união. Ademais, se $\overline{a}$ pertence à união, então pertence a pelo menos um A_p, e se pertence a algum A_p, então pertence ao primeiro, isto é,

$$\left\{\overline{a} \in \mathbb{Z}_n : \exists\, p \in \pi_n, p^2 \mid n, \text{mdc}(a,n) = p\right\} = \overset{\circ}{\bigcup_{\substack{p \in \pi_n \\ p^2 | n}}} A_p.$$

Agora, demonstraremos de fato o que o enunciado do Corolário propõe. Veja que mostramos no Teorema 3.5 que a função $f : A_p \to U(\mathbb{Z}_m)$ definida por $f(\overline{a}) = \overline{\dfrac{a}{p}}$ é bijetora. Como mostramos que a função é bijetora, então conforme o Capítulo 1 de [8], temos que ambos os conjuntos possuem a mesma cardinalidade, isto é, a mesma quantidade de elementos. Logo, $\#(A_p) = \#U(\mathbb{Z}_m) = \#U\left(\mathbb{Z}_{\frac{n}{p}}\right)$, em que a segunda igualdade se dá pela hipótese $n = pm$.

Porém, perceba que sabemos quem são os conjuntos A_p, e portanto, a cardinalidade da união disjunta dos conjuntos A_p é a soma das cardinalidades dos A_p.

E ainda, pela definição do conjunto, a cardinalidade de $U\left(\mathbb{Z}_{\frac{n}{p}}\right)$ é igual a $\varphi\left(\frac{n}{p}\right)$, já que tanto a função φ de Euler quanto o conjunto

$U\left(\mathbb{Z}_{\frac{n}{p}}\right)$ exigem que mdc $\left(a, \frac{n}{p}\right) = 1$, em que a pertence aos conjuntos citados anteriormente.

Dessa forma, mostramos que

$$\begin{aligned}\#\left(\overset{\circ}{\bigcup_{\substack{p\in\pi_n\\ p<n}}} A_p\right) &= \sum_{\substack{p\in\pi_n\\ p<n}} \#\left(A_p\right)\\ &= \sum_{\substack{p\in\pi_n\\ p<n}} \#\left(U\left(\mathbb{Z}_{\frac{n}{p}}\right)\right)\\ &= \sum_{\substack{p\in\pi_n\\ p<n}} \varphi\left(\frac{n}{p}\right).\end{aligned}$$

e

$$\begin{aligned}\#\left(\overset{\circ}{\bigcup_{\substack{p\in\pi_n\\ p^2|n}}} A_p\right) &= \sum_{\substack{p\in\pi_n\\ p^2|n}} \#\left(A_p\right)\\ &= \sum_{\substack{p\in\pi_n\\ p^2|n}} \#\left(U\left(\mathbb{Z}_{\frac{n}{p}}\right)\right)\\ &= \sum_{\substack{p\in\pi_n\\ p^2|n}} \varphi\left(\frac{n}{p}\right).\end{aligned}$$

■

Exemplo 3.3.1. Seja

$$\mathbb{Z}_8 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}\}.$$

Sabemos que $\pi_8 = \{2\}$ e também, pelo Corolário 3.6 que em $\mathbb{Z}_8$ o número de elementos:

1. primos é dado por

$$\sum_{\substack{p\in\pi_8\\ p<8}} \varphi\left(\frac{8}{p}\right) = \varphi\left(\frac{8}{2}\right) = \varphi\left(4\right) = 2,$$

2. irredutíveis é dado por

$$\sum_{\substack{p\in\pi_8\\ p^2|8}} \varphi\left(\frac{8}{p}\right) = \varphi\left(\frac{8}{2}\right) = \varphi(4) = 2,$$

E de fato, tanto os elementos primos quanto os elementos irredutíveis de $\mathbb{Z}_8$ são:

$$\{\overline{2}, \overline{6}\}.$$

Exemplo 3.3.2. Seja

$$\mathbb{Z}_{10} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}\}$$

Como $\pi_{10} = \{2, 5\}$, o Corolário 3.6 nos diz que em $\mathbb{Z}_{10}$ a quantidade de elementos:

1. primos é dada por

$$\sum_{\substack{p\in\pi_{10}\\ p<10}} \varphi\left(\frac{10}{p}\right) = \varphi\left(\frac{10}{2}\right) + \varphi\left(\frac{10}{5}\right) = \varphi(5) + \varphi(2) = 4 + 1 = 5,$$

2. irredutíveis é dada por

$$\sum_{\substack{p\in\pi_{10}\\ p^2|10}} \varphi\left(\frac{10}{p}\right) = 0,$$

em que φ é função de Euler. Dessa forma, como $2 \mid 10$, $5 \mid 10$ e $2^2 = 4 \nmid 10$, $5^2 = 25 \nmid 10$ e nenhum outro primo além do 2 e do 5 pertencem ao conjunto π_{10}, então temos que os elementos primos de $\mathbb{Z}_{10}$ serão as classes de equivalência cujo representante e 10 resultam em MDC igual à 2 e 5, isto é:

$$\{\overline{2}, \overline{4}, \overline{5}, \overline{6}, \overline{8}\}.$$

Infelizmente, não existem elementos irredutíveis neste anel em questão, pois nem 2 e nem 5 atendem a condição necessária de $p^2 \mid n$. Logo, não há elementos irredutíveis em $\mathbb{Z}_{10}$.

Exemplo 3.3.3. Seja

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

Sabemos que $\pi_{45} = \{3, 5\}$ e também, pelo Corolário 3.6, 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

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

Exemplo 3.3.4. Seja

$$\mathbb{Z}_{13} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, \overline{10}, \overline{11}, \overline{12}\}.$$

Pelo Corolário 3.6, em $\mathbb{Z}_{13}$ a quantidade de elementos:

1. primos é dada por

$$\sum_{\substack{p \in \pi_{13} \\ p<13}} \varphi\left(\frac{13}{p}\right) = 0,$$

2. irredutíveis é dada por

$$\sum_{\substack{p\in\pi_{13}\\ p^2|13}} \varphi\left(\frac{13}{p}\right) = 0,$$

pois não existem primos que dividam 13.

E, inspirado nesse exemplo, temos de imediato:

Teorema 3.7. *Se p é um número natural primo, então $\mathbb{Z}_p$ não possui elementos primos e nem elementos irredutíveis.*

Demonstração. Segue do fato de que $\pi_p = \emptyset$. ■

4 CONCLUSÃO

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 submeteremos uma errata com a demonstração correta.

Vale a pena ressaltar a importância que as disciplinas: Elementos de Álgebra e Aritmética e Álgebra I tiveram para a possível efetivação do tema discorrido no desenvolvimento desta monografia.

A produção deste trabalho possibilitou um contato mais aprofundado com a matemática acadêmica e vários conceitos estudados nas disciplinas citadas anteriormente da Universidade Federal de Santa Catarina - Campus Blumenau.

REFERÊNCIAS

[1] M. H. Jafari e A. R. Madadi, "Prime and irreducible elements of the ring of integers modulo n", *The Mathematical Gazette*, v. 96, n. 536, pp. 283–287, 2012.

[2] G. Polya, *A arte de resolver problemas*, 2ª ed. Interciência, 1995.

[3] F. Martinez, C. G. Moreira, N. Saldanha e E. Tengan, *Teoria dos Números: um passeio com primos e outros números familiares pelo mundo inteiro*, 2ª ed. Rio de Janeiro: IMPA, 2018. disp. em: `https://biblioteca.ibge.gov.br/visualizacao/livros/liv99700.pdf` (acesso em 16/08/2019).

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

[5] R. B. J. T. Allenby, *Rings, Fields and Groups: an introduction to abstract algebra*, 2ª ed. St Edmundsbury Press Ltd, 1991.

[6] A. Gonçalves, *Introdução à Álgebra*, 2ª ed. IMPA, 1979.

[7] O. R. Janesch e I. J. Taneja, *Álgebra I*, 2ª ed. Florianópolis: Universidade Federal de Santa Catarina, 2011. disp. em: `https://mtmgrad.paginas.ufsc.br/files/2014/04/%5C%C3%5C%81lgebra-I.pdf` (acesso em 22/09/2022).

[8] E. L. de Lima, *Curso de Análise Volume 1*, 7ª ed. IMPA, 1976.