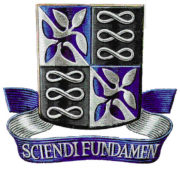
Universidade Federal da Bahia - UFBA
Instituto de Matematica e Estatística - IME
Sociedade Brasileira de Matematica - SBM
Mestrado Profissional em Matemática em Rede Nacional - PROFMAT

Dissertação de Mestrado

DAIANE SOUZA MACHADO

REPRESENTAÇÃO DECIMAIS DO NÚMEROS RACIONAIS E O TEORIA DOS GRUPOS - UMA PROPOSTA PARA O ENSINO MÉDIO

SALVADOR
2023



Universidade Federal da Bahia - UFBA
Instituto de Matematica e Estatística - IME
Sociedade Brasileira de Matematica - SBM
Mestrado Profissional em Matemática em Rede Nacional - PROFMAT

Dissertação de Mestrado

DAIANE SOUZA MACHADO

REPRESENTAÇÃO DECIMAIS DO NÚMEROS RACIONAIS E O TEORIA DOS GRUPOS - UMA PROPOSTA PARA O ENSINO MÉDIO

Dissertação de mestrado apresentada ao Departamento de Matemática da Universidade Federal da Bahia como requisito parcial para obtenção do título de Mestre em Matemática.

Orientador: Prof. Dr. Joseph Nee Anyah Yartey

SALVADOR
2023

Ficha catalográfica elaborada pela Biblioteca Universitária de Ciências e Tecnologias Prof. Omar Catunda, SIBI – UFBA.

M149 Machado, Daiane Souza

Representação decimal dos números racionais e a teoria de grupos-uma proposta para o ensino médio / Daiane Souza Machado. – Salvador, 2023.

61 f.

Orientador: Prof. Dr. Joseph Nee Anyah Yartey

Dissertação (Mestrado) – Universidade Federal da Bahia. Instituto de Matemática e Estatística,IME, 2023.

1. Matemática. 2. Números Racionais. 3. Teoria de grupos. I. Yartey, Joseph Nee Anyah. II. Universidade Federal da Bahia. III. Título.

CDU 511

"Representação decimais dos números racionais e a teoria dos grupos – Uma proposta para o ensino médio"

Daiane Souza Machado

Dissertação de Mestrado apresentada à comissão Acadêmica Institucional do PROFMAT-UFBA como requisito parcial para obtenção do título de Mestre em Matemática, aprovada em 28/11/2023.

Banca Examinadora:

Prof. Dr. Joseph Nee Anyah Yartey
Instituto de Matemática e Estatística – UFBA

Documento assinado digitalmente
gov.br
RITA DE CASSIA DE JESUS SILVA
Data: 09/12/2023 12:08:01-0300
Verifique em https://validar.iti.gov.br

Profa. Dra. Rita de Cássia de Jesus Silva
Instituto de Matemática e Estatística – UFBA

Profa. Dra. Cláudia Ribeiro Santana
Universidade Estadual de Santa Cruz – UESC

À minha família

Agradecimentos

Agradeço a Deus, que em sua infinita misericórdia me deu forças para superar as limitações que me impediam de chegar até aqui.

Agradeço aos meus filhos,Carlos Eduardo e Matheus, por me tornarem cada dia uma pessoa melhor e por serem meu combustível nessa longa caminhada.

A minha mãe,Marinalva de Santana Souza,por cada segundo de vida e dedicação exclusiva a mim,minha irmã e meus filhos.

Ao meu Esposo,Eduardo Oliveira Machado,pela paciência e por me incentivar a cada instante da minha vida.

A minha sogra,Raimunda Caldas de Oliveira,pelo incentivo, cumplicidade e amor incondicional a meus filhos.

Aos meus colegas e amigos do profmat,que estiveram sempre ao meu lado estudando e me incentivando a cada dia.

A Prof. Dr. Joseph, pela valiosa orientação e paciência inabalável.Pelo apoio e dedicação a meu trabalho.

A todos os professores do PROFMAT- UFBA,Levarei comigo o grande exemplo de Matemáticos e seres humanos que mostraram ser ao longo do curso.

"Mudaste o meu pranto em dança, a minha veste de lamento em veste de alegria, para que o meu coração cante louvores a ti e não se cale. Senhor, meu Deus, eu te darei graças para sempre .

(Bíblia Sagrada, Salmos 30:11-12)

Resumo

Neste trabalho vamos apresentar a relação entre a representação decimal de um número racional com o teoria dos grupos principalmente grupos, subgrupos, classes laterais, ordem de um grupo e teoria de Lagrange. Vamos apresentar uma proposta de ensino com a relação dos assuntos abstrato com a transformação de números racionais em decimais.

Palavras-chave: Representação Decimal, Teoria dos grupos.

Abstract

In this work we will present the relationship between the decimal representation of a rational number with group theory, mainly groups, subgroups, cosets, order of a group and Lagrange theory. We will present a teaching proposal relating these abstract subjects with the transformation of rational numbers into decimals.

Keywords: Decimal Representation, Group Theory.

Lista de ilustrações

Lista de tabelas

Sumário

Introdução

As formas de ensino da matemática são muito discutidas no ambiente acadêmico e fora dele. Na prática cotidiana da sala de aula os professores deparam-se com as dificuldades dos alunos de abstração e de visualização em diversas situações matemáticas. Habitualmente decorar fórmulas e aceitar as explicações sem questionar de onde surgiu são práticas comuns dos discentes que atrapalham o processo de ensino e aprendizagem.

Cabe ao professor buscar alternativas para minimizar os danos causados por tais atitudes. Explicar o conteúdo de maneira formal utilizando demonstrações é importante. Entretanto, a ludicidade e a busca por outras formas de ensino colaboram com a desmitificação da matemática.

Uma das atividades muito comum na escola é transformando um número racional $\frac{a}{b}$ em um inteiro, fração decimal ou dizima periódica. Por exemplo

(Tipo I): $\frac{12}{6} = 2$

(Tipo II): $\frac{4}{5} = 0{,}8, \quad \frac{7}{40} = 0{,}175$

(Tipo III): $\frac{4}{9} = 0{,}444\ldots = 0{,}\overline{4}; \quad \frac{1}{7} = 0{,}142857142857\ldots = 0{,}\overline{142857}$

(Tipo IV): $\frac{1}{6} = 0{,}1666\ldots = 0{,}1\overline{6}; \quad \frac{7}{30} = 0{,}2333\ldots = 0{,}2\overline{3}$

Transformar uma fração do Tipo (III) em uma dizima periódica parece ser uma tarefa bastante insignificante, mecânico, enfadonho no ensino de matemática na escola. No entanto tais frações contém propriedades interessantes e cativantes.

Pensando nisso, essa dissertação apresentará uma observação do posicionamento dos algarismos da parte periódica das dízimas periódicas simples verificando que estes se encontram de forma cíclica quando trocamos o numerador da fração estudada.

Examinaremos Frações do (Tipo III) com rigor matemático usando o Teoria de Números e Teoria dos Grupos. Encontraremos aí conexões com a função fi de Euler, congruência, sistema de resíduos reduzido módulo m, subgrupos de grupos, classes laterias, grupos cíclicos, ordem de um elemento em um grupo e teorema de Lagrange.

No primeiro capítulo serão exibidas algumas definições e notações que serão utilizadas no decorrer do trabalho. A representação decimal dos números será abordada no capítulo seguinte de forma genérica demonstrando assim a sua existência e unicidade. A representação dos números racionais constará no terceiro capítulo trazendo o estudo das

dízimas periódicas, simples e compostas, evidenciando o posicionamento dos algarismos da parte periódica das dízimas periódicas simples. No capítulo 4, mostraremos que,dada uma fração $\frac{1}{N}$o comprimento do seu período pode ser determinado sem fazer a divisão. Neste capítulo noções de teoria dos grupos, principalmente o grupo $\mathbb{Z}^*$,grupo multiplicativo dos inteiros mod n. Em seguida, apresentaremos uma sequência didática para facilitar a aplicação desse conteúdo em sala de aula. Diante do exposto, a proposta é mostrar que numa fração, ao fixar um denominador, para qualquer numerador natural escolhido, teremos que os algarismos da parte periódica da dízima periódica simples encontrada na representação dessa fração será uma permutação cíclica.

1 Preliminares - Teoria de Grupos e Teoria dos números

Apresentamos alguns dos conceitos e resultados sobre a teoria de Grupos e dos Números necessários neste trabalho. Leitura mais abrangentes com as demonstrações dos resultados podem ser encontrados, por exemplo, em [1], [2] e [9]

1.1 Divisibilidade em $\mathbb{Z}$

Definição 1.1. *Sejam a, b números inteiros. Dizemos que a **divide** b, denotado por $a \mid b$, se existe um número inteiro c tal que*

$$b = ac.$$

Outra maneira de colocar:

$$a \mid b \Longleftrightarrow b \text{ é um múltiplo de } a.$$

Proposição 1.1. *Sejam $a, b, c \in \mathbb{Z}$. Então,*

(a) $1 \mid c, \quad a \mid a \quad e \quad a \mid 0.$

(b) $a \mid b, \ b \neq 0$, *se, e somente se,* $|a| \leq |b|$.

(c) se $a \mid b$ *e* $b \mid c$, *então* $a \mid c$.

Proposição 1.2. *Se* $a, \ b, \ c, \ d \in \mathbb{Z}$, *com* $a \neq 0$ *e* $c \neq 0$, *então*

$$a \mid b \quad e \quad c \mid d \Longrightarrow ac \mid bd$$

Proposição 1.3. *Sejam* $a, \ b, \ c \in \mathbb{Z}$ *tais que* $a \mid b \quad e \quad a \mid c$, *então para todo* $x, y \in \ Z$,

$$a \mid (xb + yc)$$

Teorema 1.1 (Divisão Euclidiana). *Sejam* $a, \ b \in \mathbb{Z}$, *com* $b \neq 0$.

(a) Existem dois únicos inteiros q e r tais que

$$a = bq + r, \qquad 0 \leq r < |b|.$$

(b) $$q = \begin{cases} \left[\frac{a}{b}\right], & b > 0 \\ \\ -\left[\frac{a}{|b|}\right], & b < 0 \end{cases},$$

sendo $[x]$ o maior inteiro menor ou igual que x.

De fato, esta Teorema é apenas a "Divisão Longa" do ensino médio, com q sendo o "quociente" e r o "resto".

Definição 1.2. *Um inteiro n é dito **primo** se e somente se $n > 1$ e os únicos divisores positivos de n são 1 e n.*
*Um inteiro positivo n é dito **composto** se e somente se $n > 1$ e n não é primo. Logo, $n > 1$ é composto se, e somente se, existem inteiros a e b com $1 < a < b < n$ tal que $n = a \cdot b$.*

1.2 Máximo Divisor Comum

Definição 1.3 (**Máximo Divisor Comum**)**.** *Sejam $a, b \in \mathbb{Z}$, não simultaneamente nulos. O máximo divisor comum de a e b, denotado por (a, b) ou MDC(a, b), é um elemento $d \in \mathbb{Z}$ tal que*

(i) $d \mid a$ *e* $d \mid b$

(ii) $d \geq 1$

(ii) Se d' é outro elemento de $\mathbb{Z}$ satisfazendo (i) e (ii), isto é $d' \mid a$ e $d' \mid b$, então d' divide d.

Exemplo 1.1.

$$(4, 6) = 2, \qquad (17, 17) = 17, \qquad (42, 0) = 42, \qquad (12, -15) = 3.$$

O Teorema a seguir demonstra a existência do MDC(a, b) para $a, b \in \mathbb{Z}$, não simultaneamente nulos e

Teorema 1.2 (**Bézout**)**.** *Dados números inteiros a, b ambos não nulos, existe um único máximo divisor comum $d =$ MDC(a, b). Além disto, existem inteiros x, y tais que*

$$d = ax + by \quad (\textit{combinação linear de } a \textit{ e } b)$$

Exemplo 1.2.

(a) $(4, 6) = 2 \quad e \quad 2 = 6 \cdot 1 + 4 \cdot (-1)$

(b) $(12, -15) = 3 \quad e \quad 3 = -15 \cdot (-1) + 12 \cdot (-1)$

Observação 1.

(a) Temos $(12, -15) = 3$, *logo o Teorema 1.2, afirma que o conjunto de todas as combinações lineares de 12 e* -15 *- isto é o conjunto de todos os números da forma* $-15x + 12y$ *- é o conjunto de todos os múltiplos de 3:*

$$\cdots, -12, -9, -6, -3, 0, 3, 6, 9, 12, \cdots.$$

Observe que o máximo divisor comum é o menor número positivo neste conjunto.

(b) Notamos no Teorema de Bezout os inteiros x *e* y *não são únicos.*

De fato, 2 = MDC(6, 4). Mas

$$6 \cdot 1 + 4 \cdot (-1) = 2 \qquad e \qquad 6 \cdot 3 + 4 \cdot (-4) = 2.$$

(c) Em geral, também não vale a recíproca do Teorema de Bezout, pois

$$6 \cdot 2 + 4 \cdot (-2) = 4 \qquad e \qquad MDC(6, 4) \neq 4.$$

Entretanto, temos que:

$$MDC(a, b) = 1 \iff \quad existirem\ inteiros\ \ x\ \ e\ \ y\ \ \ tais\ que\ \ xa + yb = 1.$$

Esse é o único caso em que a recíproca do Teorema de Bezout é verdadeira.

Vamos ver algumas propriedades elementares do MDC(a, b).

Proposição 1.4. *Sejam* $a,\ b$ *inteiros, ambos não nulos.*

(a) $(a, b) = (b, a)$.

(b) $(a, b) = (|a|, |b|)$.

(c) $(a, b) = (a + kb, b)$ *para algum* k *inteiro.*

(d) Se $a \mid b$, *então* $(a, b) = a$.

Definição 1.4. *Dois números inteiros* a *e* b *são ditos* ***primos entre si*** *ou* ***coprimos*** *se* $(a, b) = 1$.

Exemplo 1.3. *Por exemplo, 49 e 54 são coprimos, mas 25 e 105 não são.*

Proposição 1.5. *Se* $d = (a, b)$, *então* $\left(\frac{a}{d},\ \frac{b}{d}\right) = 1$.

Lema 1.1. *Se* a *e* b *são inteiros não ambos nulos, então* $MDC(a, b) = 1$ *se, e somente se, existem números inteiros* x *e* y *tais que* $ax + by = 1$.

Lema 1.2. *[**Lema de Gauss**] Sejam $a, b, c \in \mathbb{Z}$. Se $a \mid bc$ e $MDC(a, b) = 1$, então $a \mid c$.*

Lema 1.3. *Sejam $a, b, c \in \mathbb{Z}$. Se $a \mid c$, $b \mid c$ e $MDC(a, b) = 1$, então $ab \mid c$.*

Observação 2. *Observe que no Lema 1.3, o resultado é falsa se $MDC(a, b) \neq 1$. Por exemplo:*

$$8 \mid 24 \quad e \quad 6 \mid 24, \quad mas \quad 48 = 8 \cdot 6 \nmid 24.$$

Teorema 1.3 (**Teorema Fundamental da Aritmética**)**.** *Todo número natural maior do que 1 ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como um produto de números primos.*

Por exemplo,

$$36 = 2^2 \cdot 3^2, \quad 4312 = 2^3 \cdot 7^2 \cdot 11, \quad 19 = 19^1.$$

1.3 Congruências

Ao fundamentarmos a aritmética das somas dos dígitos, faz-se interessante apresentar os principais resultados referentes à congruência módulo m, ou "a aritmética dos restos de uma divisão por $n \in \mathbb{Z}$.

Para isso,utilizaremos como base a bibliografia [1]. Como bibliografia complementar utilizamos [2].

Definição 1.5. *Sejam $a, b, n \in \mathbb{Z}$ com $n \neq 0$. Dizemos que a é congruente b módulo n e escrevemos*

$$a \equiv b \pmod{n} \quad ou \quad a \equiv_n b$$

se, e somente se, $a - b$ é um múltiplo de n, isto é, se, e somente se $a - b = kn$, para algum $k \in \mathbb{Z}$.

Observação 3. *Como $(a - b) = kn \iff (a - b) = (-k)(-n)$ nos restringiremos ao caso $n > 0$. O caso $n = 1$ é trivial pois qualquer 2 inteiros são congruentes módulo 1. Geralmente, os casos interessantes são $n > 1$.*

Exemplo 1.4.

1. $13 \equiv 18 \pmod{5}$ *pois* $(13 - 18) = 5 = 5 \cdot 1$
2. $152 \equiv_7 5$ *pois* $(152 - 5) = 147 = 7 \cdot 21$.
3. $7 \equiv_8 15$ *pois* $(7 - 15) = -8 = 8 \cdot (-1)$.
4. $-101 \equiv_3 1$ *pois* $(-101 - 1) = -102 = 3 \cdot (-34)$.

5. $16 \equiv -1 \pmod{17}$ *pois* $(16-(-1)) = 17 = 17 \cdot 1$.

Proposição 1.6. *Considere* $a, b \in \mathbb{Z}$. *São equivalentes as seguintes afirmações:*

(a) $a \equiv b \pmod{n}$;

(b) $n \,\big|\, (a-b)$;

(c) a *e* b *dão o mesmo resto, na divisão por* n.

Demonstração.

$(a) \Rightarrow (b)$: Suponha que $a \equiv b \pmod{n}$. Então

$$\begin{aligned} & a - b = nk, \quad k \in \mathbb{Z} \\ & \Rightarrow n \,\big|\, (a-b). \end{aligned}$$

$(b) \Rightarrow (c)$: Suponha que $n \,\big|\, (a-b)$

Fazendo as divisões de a e b por n, temos

$$\begin{aligned} (1) \qquad & a = q_1 n + r_1, \qquad q_1, r_1 \in \mathbb{Z}, \text{ com } 0 \leq r_1 < n \\ (2) \qquad & b = q_2 n + r_2, \qquad q_2, r_2 \in \mathbb{Z}, \text{ com } 0 \leq r_2 < n \end{aligned}$$

Suponha que $r_2 \leq r_1$. Portanto $0 \leq r_1 - r_2 \leq r_1 < n$.
Subtraindo (2) de (1) temos,

$$a - b = (q_1 - q_2)n + (r_1 - r_2) \qquad (*)$$

Desse modo, $\quad 0 \leq r_1 - r_2 < n$ é o resto da divisão de $(a-b)$ por n.
Portanto $\quad (r_1 - r_2) = 0 \Rightarrow r_1 - r_2$ pois $(a-b)$ é múltiplo de n.

$(c) \Rightarrow (a)$: Suponha que a e b deixam o mesmo resto na divisão por n, então

$$\begin{aligned} (1) \qquad & a = q_1 n + r, \qquad q_1, r \in \mathbb{Z}, \text{ com } 0 \leq r < n \\ (2) \qquad & b = q_2 n + r, \qquad q_2 \in \mathbb{Z}, \end{aligned}$$

Subtraindo (2) de (1) temos,

$$a - b = (q_1 - q_2)n$$

Portanto, a diferença $(a-b)$ é um múltiplo de n

$$\Rightarrow a \equiv b \pmod{n}.$$

□

A congruência módulo n é uma relação de equivalência. Isto é

Proposição 1.7. *Seja $n \in \mathbb{N}$. Para todos $a, b, c \in \mathbb{Z}$, tem-se:*

(a) $a \equiv a \ (mod\ n)$ (reflexiva)

(b) Se $a \equiv b \ (mod\ n)$ então $b \equiv a \ (mod\ n)$ (simétrica)

(c) Se $a \equiv b \ (mod\ n)$ e $b \equiv c \ (mod\ n)$ então $a \equiv c \ (mod\ n)$ (transitiva)

Portanto $\equiv_n$ é um relação de equivalência.

Demonstração.

(a) $a \equiv a \pmod{n}$.
De fato, $(a - a) = 0 = 0 \cdot n$.

(b) Suponha que $a \equiv b \pmod{n}$. Então $\exists\ k \in \mathbb{Z}$ tal que

$$\begin{aligned} a - b &= kn \\ \Rightarrow b - a &= (-k)n \end{aligned}$$

Como $(-k) \in \mathbb{Z}$, temos que $b \equiv a \pmod{n}$.

(c) Suponha que $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n}$.Então

$$\begin{aligned} a - b &= k_1 n, \qquad k_1 \in \mathbb{Z} \\ b - c &= k_2 n, \qquad k_2 \in \mathbb{Z} \end{aligned}$$

Somando, temos que

$$\begin{aligned} (a - b) + (b - c) &= k_1 n + k_2 n \\ \Rightarrow (a - c) &= (k_1 + k_2)n \\ \Rightarrow a &\equiv c \pmod{n} \end{aligned}$$

Como $\equiv_n$ é reflexiva, simétrica e transitiva, logo temos que é uma relação de equivalência. □

Proposição 1.8 (Propriedades básicas de congruências).

(a) Se $a \equiv b \ (mod\ n)$ e $c \equiv d \ (mod\ n)$ então $a + c \equiv b + d \ (mod\ n)$

(b) Se $a \equiv b \ (mod\ n)$ e $c \equiv d \ (mod\ n)$ então $a - c \equiv b - d \ (mod\ n)$

(c) Se $a \equiv b \ (mod\ n)$ e c é inteiro não negativo, então $ac \equiv bc \ (mod\ n)$

(d) Se $a \equiv b \ (mod\ n)$ e $c \equiv d \ (mod\ n)$ então $ac \equiv bd \ (mod\ n)$

(e) Se $a \equiv b \ (mod\ n)$ e k é um inteiro positivo, então $a^k \equiv b^k \ (mod\ n)$

(f) Se $a + c \equiv b + c \ (mod\ n)$ então $a \equiv b \ (mod\ n)$

(g) Se $da \equiv db \ (mod\ dn)$ então $a \equiv b \ (mod\ n)$.

Demonstração.

(a) Suponha que $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$. Então

$$\begin{aligned} a - b &= k_1 n, \qquad k_1 \in \mathbb{Z} \\ c - d &= k_2 n, \qquad k_2 \in \mathbb{Z} \end{aligned}$$

Somando, temos que

$$\begin{aligned} (a-b) + (c-d) &= k_1 n + k_2 n \\ \Rightarrow (a+c) - (b+d) &= (k_1 + k_2) n \\ \Rightarrow (a+c) - (b+d) &= k_3 n, \ \text{ onde } k_3 = (k_1 + k_2) \in \mathbb{Z} \\ \Rightarrow (a+c) &\equiv (b+d) \pmod{n} \end{aligned}$$

(b) Suponha que $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$. Então

$$\begin{aligned} a - b &= k_1 n, \qquad k_1 \in \mathbb{Z} \\ c - d &= k_2 n, \qquad k_2 \in \mathbb{Z} \end{aligned}$$

Subtraindo, temos que

$$\begin{aligned} (a-b) - (c-d) &= k_1 n - k_2 n \\ \Rightarrow (a-c) - (b-d) &= (k_1 - k_2) n \\ \Rightarrow (a-c) - (b-d) &= k_3 n, \ \text{ onde } k_3 = (k_1 - k_2) \in \mathbb{Z} \\ \Rightarrow (a-c) &\equiv (b-d) \pmod{n} \end{aligned}$$

(c) Suponha que $a \equiv b \pmod{n}$. Então $\exists\ k \in \mathbb{Z}$ tal que

$$a - b = kn$$

Multiplicando por c temos

$$\begin{aligned} ac - bc &= (kc) n \\ \Rightarrow ac - bc &= k_1 n \end{aligned}$$

Como $k_1 = (kc) \in \mathbb{Z}$, temos que $ac \equiv bc \pmod{n}$.

(d) Suponha que $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$. Então

$$\begin{aligned} a - b &= k_1 n, \qquad k_1 \in \mathbb{Z} \\ c - d &= k_2 n, \qquad k_2 \in \mathbb{Z} \end{aligned}$$

Queremos provar que $ac - bd = k_3 n, \quad$ sendo $\; k_3 \in \mathbb{Z}$. Observe que

$$\begin{aligned} ac - bd &= ac \underbrace{-bc + bc}_{=0} - bd \\ &= (a-b)c + (c-d)b \\ &= k_1 cn + k_2 bn \\ &= (k_1 c + bk_2)n \\ \Rightarrow ac - bd &= k_3 n \quad \text{sendo} \;\; k_3 = (k_1 c + k_2 b) \in \mathbb{Z} \\ \Rightarrow ac &\equiv bd \pmod{n} \end{aligned}$$

(e) Vamos provar usando (d)

$$k \text{ vezes} \begin{cases} a \equiv b \pmod{n} \\ a \equiv b \pmod{n} \\ \qquad \vdots \\ a \equiv b \pmod{n} \end{cases} \overset{\text{pela } (d)}{\Longrightarrow} a^k \equiv b^k \pmod{n}.$$

Podemos provar(h) também por indução. Faça com exercício.

(f) Suponha que $a + c \equiv b + c \pmod{n}$. Então $\exists \; k \in \mathbb{Z}$ tal que

$$\begin{aligned} (a+c) - (b+c) &= kn \\ \Rightarrow a - b &= kn \\ \Rightarrow a &\equiv b \pmod{n} \end{aligned}$$

(g) Suponha que $da \equiv db \pmod{dn}$. Então $\exists \; k \in \mathbb{Z}$ tal que

$$\begin{aligned} da - db &= kn \\ \Rightarrow a - b &= knd \\ \Rightarrow a &\equiv b \pmod{n} \end{aligned}$$

□

1.4 O conjunto $\mathbb{Z}_n$

Vimos na Secção 1.3, Proposição 1.7, que congruência módulo n é uma relação de equivalência. Logo podemos definir a classe de um elemento a módulo n.

Definição 1.6. *Seja n um inteiro positivo fixo. Chama-se* ***classe de congruência*** *de a módulo n $(n > 1)$ o conjunto formado por todos os inteiros que são congruentes a a módulo n. Denotamos esse conjunto por $\overline{a}$ ou $[a]_n$, isto é*

$$\overline{a} = \{x \in \mathbb{Z} : \quad x \equiv a \ (mod\ n)\} = \{x \in \mathbb{Z} : \ n \Big| (x - a) \ \} = \{a + kn : \quad k \in \mathbb{Z}\}.$$

Observação 4. *A notação $\overline{a}$ deve ser usada somente quando ficar claro, pelo contexto, o valor do inteiro n utilizado, do contrário a notação $[a]_n$ é a mais indicada.*

Exemplo 1.5. *Determine as classes de congruência módulo 3.*

Para cada $a \in \mathbb{Z}$,

$$\begin{aligned} \overline{a} &= \{x \in \mathbb{Z} \ \mid \ x \equiv a \pmod 3\} \\ &= \{x \in \mathbb{Z} \ \mid \ 3 \ \text{ divide } (x - a)\} \\ &= \{x \in \mathbb{Z} \ \mid \ x - a = 3k, \ \text{ para algum inteiro } \ k\} \end{aligned}$$

Portanto

$$\overline{a} = \{x \in \mathbb{Z} \ \mid \ x = a + 3k, \ \text{ para algum inteiro } k\}$$

Em particular

$$\begin{aligned} [0] &= \{x \in \mathbb{Z} \ \mid \ x = 0 + 3k, \ \text{ para algum inteiro } k\} \\ &= \{x \in \mathbb{Z} \ \mid \ x = 3k, \ \text{ para algum inteiro } k\} \\ &= \{\cdots, -9, -6, -3, 0, 3, 6, 9, \cdots\} \end{aligned}$$

$$\begin{aligned} [1] &= \{x \in \mathbb{Z} \ \mid \ x = 1 + 3k, \ \text{ para algum inteiro } k\} \\ &= \{\cdots, -8, -5, -2, 1, 4, 7, 10, \cdots\} \end{aligned}$$

$$\begin{aligned} [2] &= \{x \in \mathbb{Z} \ \mid \ x = 2 + 3k, \ \text{ para algum inteiro } k\} \\ &= \{\cdots, -7, -4, -1, 2, 5, 8, 11, \cdots\} \end{aligned}$$

Como $3 \equiv 0 \pmod 3$,

$$[3] = [0].$$

Mais geral,

$$[0] = [3] = [-3] = [6] = [-6] = \cdots, \text{e assim por diante.}$$

De mesmo modo

$$[1] = [4] = [-2] = [7] = [-5] = \cdots, \text{e assim por diante.}$$

$$[2] = [5] = [-4] = [8] = [-7] = \cdots, \text{e assim por diante.}$$

Observe que cada inteiros está na classe [0], [1], ou [2]. Portanto as distintas das classes de congruência módulo 3 são

$$\overline{0} = \{x \in \mathbb{Z} \mid x = 3k, \text{ para algum inteiro } k\}$$

$$\overline{1} = \{x \in \mathbb{Z} \mid x = 3k+1, \text{ para algum inteiro } k\} \quad \text{e}$$

$$\overline{2} = \{x \in \mathbb{Z} \mid x = 3k+2, \text{ para algum inteiro } k\}$$

Em geral, temos

Proposição 1.9. *Para inteiros a, b*

(i) Se $a \equiv b \pmod{n}$ então $\overline{a} = \overline{b}$.

(ii) Se $a \not\equiv b \pmod{n}$, então $\overline{a} \cap \overline{b} = \emptyset$.

Corolário 1.1. *Duas classes de congruência módulo n ou são disjuntos ou são iguais.*

Observação 5. *A classe de congruência $\overline{a}$ módulo n diz-se determinada ou definida pelo inteiro a, o qual chama-se um* ***representante*** *de $\overline{a}$. Dois inteiros são representantes de uma mesma classe de congruência módulo n $(\overline{a} = \overline{b})$ se, e somente se, são congruentes módulo n $(a \equiv b \pmod{n})$.*

Corolário 1.2. *Existem exatamente n distintas classes de congruência módulo n, dado por $\overline{0}, \overline{1}, \cdots, \overline{n-1}$.*

Demonstração. Pelo algoritmo da divisão, para qualquer inteiro a existe um único r com $0 \leq r < n$ tal que

$$a = qm + r \quad \text{com} \quad q \in \mathbb{Z}.$$

Então $a \equiv r \pmod{n}$, logo todo inteiro é congruente módulo n a exatamente um dos n inteiros $0, 1, \cdots, n-1$. Isto quer dizer que, todo inteiro pertencente exatamente uma das classes $\overline{0}, \overline{1}, \cdots, \overline{n-1}$. □

Definição 1.7. *O conjunto formado por todas as classes de congruências módulo n, é indicado por $\mathbb{Z}_n$ e chamado de* ***o conjunto dos inteiros módulo*** *n. Isto é*

$$\mathbb{Z}_n = \{\overline{r} : \ 0 \leq r \leq n-1\} = \{\overline{0}, \ \overline{1}, \ \overline{2}, \cdots, \ \overline{n-1}\}$$

Exemplo 1.6. *Como vimos no Exemplo 1.5, temos que*

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

Exemplo 1.7.

(1) $\mathbb{Z}_5 = \{\overline{0}, \ \overline{1}, \ \overline{2}, \ \overline{3}, \ \overline{4}\}$

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

1.4.1 Adição e Multiplicação em $\mathbb{Z}_n$

Definição 1.8. *Para* $\overline{a},\ \overline{b} \in \mathbb{Z}_n$, *definimos*

$$\overline{a}\ +_n\ \overline{b} := \overline{a+b},$$

e

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

Exemplo 1.1. Em $\mathbb{Z}_{10}$ temos que

$$\overline{7}\ +_{10}\ \overline{8} = ((7+8)\ (\text{ mod } 10)) = 15\ (\text{ mod } 10) = \overline{5}.$$

e

$$\overline{7}\ \cdot_{10}\ \overline{8} = ((7 \cdot 8)\ (\text{ mod } 10)) = 56\ (\text{ mod } 10) = \overline{6}.$$

Teorema 1.2. *Adição e Multiplicação em* $\mathbb{Z}_n$ *são bem-definidas. Isto é*
Se $\overline{a} = \overline{a'}$ *e* $\overline{b} = \overline{b'}$ *então*

$$\overline{a}\ +_n\ \overline{b} = \overline{a'}\ +_n\ \overline{b'}$$

e

$$\overline{a}\ \cdot_n\ \overline{b} := \overline{a'}\ \cdot_n\ \overline{b'}.$$

Portanto adição e multiplicação definidas em $\mathbb{Z}_n$ *é independentemente do representante tomado para a ou para b.*

Proposição 1.10 (Propriedade de adição e multiplicação)**.** *Sejam* $\overline{a},\ \overline{b},\ \overline{c} \in \mathbb{Z}_n$.

(1) Associatividade da soma: $(\overline{a} +_n \overline{b}) +_n \overline{c} = \overline{a} +_n (\overline{b} +_n \overline{c})$

(2) Comutatividade da soma: $\overline{a} +_n \overline{b} = \overline{b} +_n \overline{a}$

(3) Elemento neutro para a soma: $\overline{a} +_n \overline{0} = \overline{a}$

(4) Elemento simétrico para a soma: $\overline{a} +_n \overline{m-a} = \overline{0}$

(6) Associatividade da multiplicação: $(\overline{a} \cdot_n \overline{b}) \cdot_n \overline{c} = \overline{a} \cdot_n (\overline{b} \cdot_n \overline{c})$

(6) Comutatividade da multiplicação: $\overline{a} \cdot_n \overline{b} = \overline{b} \cdot \overline{a}$.

(7) Elemento neutro para a multiplicação: $\overline{a} \cdot_n \overline{1} = \overline{a}$

(8) Distributividade da multiplicação em relação á adição: $\overline{a} \cdot_n (\overline{b} +_n \overline{c}) = \overline{a} \cdot_n \overline{b} +_n \overline{a} \cdot_n \overline{c}$.

Observação 6. *Podemos representar as operações de adição e multiplicação em* $\mathbb{Z}_n$ *através de uma tabela como mostramos no exemplo a seguir:*

Exemplo 1.3. Construa a tabela de adição e multiplicação em $\mathbb{Z}_4$.

$(\mathbb{Z}_4,\ +_4)$

$+_4$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$(\mathbb{Z}_4,\ \cdot_4)$

$\cdot_4$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Na tabela de $(\mathbb{Z}_4,\ \cdot_4)$ podemos observar que:

- $\overline{2}\cdot\overline{2}=\overline{0}$ sendo $\overline{2}\neq\overline{0}$. Aqui $\overline{2}$ é o que chamamos que **divisor de zero.**
- $\overline{3}\cdot\overline{3}=\overline{1}$. Aqui $\overline{3}$ é o que chamamos que **um elemento inversível.**

Definição 1.9. *Um elemento $\overline{a}\neq\overline{0}$ é dito* ***divisor de zero*** *se existe $\overline{b}\neq 0$ tal que*

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

Definição 1.10. *Um elemento $\overline{a}\neq\overline{0}$ é dito* ***inversível*** *se existe $\overline{b}\neq 0$ tal que*

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

Neste caso dizemos que $\overline{b}$ é o ***inverso multiplicativo*** *de $\overline{a}$.*

Exemplo 1.8. *Construa a tabela de $(\mathbb{Z}_8,\cdot)$ é determine todos os divisores de zeros de $\mathbb{Z}_8$ e os elementos inversíveis com seus inversos multiplicativos.*

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{1}$	$\overline{4}$	$\overline{7}$	$\overline{2}$	$\overline{5}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{0}$	$\overline{4}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{2}$	$\overline{7}$	$\overline{4}$	$\overline{1}$	$\overline{6}$	$\overline{3}$
$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{7}$	$\overline{0}$	$\overline{7}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Portanto os divisores de zero de $\mathbb{Z}_8$ são $\overline{2}\ \overline{4},\ \overline{6}$, pois

$$\overline{2}\cdot\overline{4}=\overline{0}\quad\text{ e }\quad\overline{4}\cdot\overline{6}=\overline{0}$$

e os elementos inversíveis de $\mathbb{Z}_8$ são $\overline{1},\ \overline{3},\ \overline{5},\ \overline{7}$, pois

$$\overline{1}\cdot\overline{1}=\overline{1}\quad\text{e }\ \overline{1}\ \text{é seu proprio inverso multiplicativo.}$$

$\overline{3} \cdot \overline{3} = \overline{1}$ e $\overline{3}$ é seu proprio inverso multiplicativo.

$\overline{5} \cdot \overline{5} = \overline{1}$ e $\overline{5}$ é seu proprio inverso multiplicativo.

$\overline{7} \cdot \overline{7} = \overline{1}$ e $\overline{7}$ é seu proprio inverso multiplicativo.

Proposição 1.11. *Seja* $\overline{a} \in \mathbb{Z}_n$

(1) Dizemos que $\overline{a}$ *é um divisor de zero se, e somente se,* $MDC(a, n) > 1$.

(2) Dizemos que $\overline{a}$ *é inversível se, e somente se,* $MDC(a, n) = 1$.

Portanto temos o seguinte:

$$\mathbb{Z}_n = \{\overline{0}\} \bigcup \underbrace{\{\overline{a} \mid MDC(a,n) = d > 1\}}_{\text{divisores de zero}} \bigcup \underbrace{\{\overline{a} \mid MDC(a,n) = 1\}}_{\text{inversíveis}}$$

1.5 A Função fi, φ de Euler

Definição 1.11. *Para qualquer inteiro positivo* n*, definimos a função phi de Euler, denotado por* φ *como a quantidade de inteiros positivos menores que* n *e coprimos com* n*. Em outras palavras,*

$$\varphi(n) = \textit{número de elementos do conjunto } \{x \in \mathbb{N};\ \ 1 \leq x < n \ \ e \ \ mdc(x, n) = 1\}$$

Exemplo 1.9.

(1) Seja $n = 12$*. Os inteiros menores que 12 e são coprimos com 12 são* $\{1, 5, 7, 11\}$. *Portanto* $\varphi(12) = 4$.

(2) Seja $n = 15$*. Os inteiros menores que 15 e são coprimos com 15 são* $\{1, 2, 4, 7, 8, 11, 13, 14\}$. *Portanto* $\varphi(15) = 8$.

(3) A tabela abaixo mostra os valores da função $\varphi(n)$ *para os 20 primeiros inteiros positivos.*

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8	16	6	18	8

Tabela 1 – Os 20 primeiros valores de φ

Lema 1.4. *Se* p *é um número primo, então* $\varphi(p) = p - 1$.

Demonstração. Por definição, $\varphi(p)$ é a quantidade de inteiros positivos x menores que p e coprimos como p. Mas, como p é primo, todo inteiro $x,\ 1 \leq x \leq p - 1$ é coprimo com p. Assim $\varphi(p) = p - 1$. □

Lema 1.5. *Sejam p um número primo e $n \in \mathbb{N}$. Então*

$$\varphi(p^n) = p^{n-1}(p-1) = p^{n-1} \cdot \varphi(p).$$

Demonstração. Temos que contar a quantidade de inteiros entre 1 e p^n que são coprimos com p^n. Faremos isso de uma maneira indireta: contaremos quantos inteiros entre 1 e p^n não são coprimos com p^n.
Os inteiros que não são coprimos com p^n são exatamente os múltiplos de p. Os múltiplos de p entre 1 e p^n são:

$$p,\ 2p,\ 3p, \cdots, p^n$$

Portanto existem, p^{n-1} múltiplos de p entre 1 e p^n.
Logo

$$\begin{aligned}\varphi(p^n) &= \text{número de elementos do conjunto } \{x \in \mathbb{N};\ \ 1 \leq x \leq p^n \ \text{ e } \ \text{mdc}(x, p^n) = 1\} \\ &= \left(\begin{array}{c} \text{número de elementos do conjunto} \\ \{x \in \mathbb{N};\ \ 1 \leq x \leq p^n\} \end{array} \right) - \left(\begin{array}{c} \text{número de elementos do conjunto} \\ \{x \in \mathbb{N};\ \ 1 \leq x < p^n \ \text{ e } \ \text{mdc}(x, p^n) \neq 1\} \end{array} \right) \\ &= p^n - p^{n-1} = p^{n-1}(p-1) = p^{n-1}\varphi(p).\end{aligned}$$

□

Exemplo 1.10.

(i) $\varphi(27) = \varphi(3^3) = 3^2\varphi(3) = 9 \cdot 2 = 18$

(ii) $\varphi(625) = \varphi(5^4) = 5^3\varphi(5) = 125 \cdot 4 = 500.$

Lema 1.6. *A função de Euler é multiplicativa, isto é, quaisquer que sejam n e m números naturais satisfazendo MDC$(n, m) = 1$ (m e n são coprimos) teremos*

$$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$$

Corolário 1.3. *Sejam $p_1,\ p_2, \cdots, p_k$ números primos distintos e $n_1,\ n_2, \cdots, n_k$ números naturais. Então:*

$$\varphi\Big(p_1^{n_1} \cdot p_2^{n_2} \cdots p_n^{n_k}\Big) = \Big(p_1^{n_1} - p_1^{n_1-1}\Big)\Big(p_2^{n_2} - p_2^{n_2-1}\Big) \cdots \Big(p_k^{n_k} - p_k^{n_k-1}\Big).$$

Demonstração. Consequência direta do teorema anterior e da Lema 1.5. □

Exemplo 1.11.

$$\begin{aligned}\textit{(a)}\ \varphi(100) &= \varphi(2^2 \cdot 5^2) \\ &= \varphi(2^2) \cdot \varphi(5^2) \\ &= 2^1\varphi(2) \cdot 5^1\varphi(5) \\ &= 2 \cdot 1 \cdot 5 \cdot 4 = 40\end{aligned}$$

$$\begin{aligned}(b)\ \varphi(120) &= \varphi(2^3 \cdot 3 \cdot 5)\\ &= \varphi(2^3) \cdot \varphi(3) \cdot \varphi(5)\\ &= 2^2\varphi(2) \cdot 2 \cdot 4\\ &= 4 \cdot 1 \cdot 2 \cdot 4 = 32\end{aligned}$$

1.6 Grupos

Definição 1.12 (Grupo)**.** *Dados um conjunto não vazio G e uma operação binária $* : S \times S \to S$, dizemos que G é um grupo com respeito a operação $*$ se os seguintes axiomas são satisfeitos:*

(G1) $*$ é associativa, ou seja,

$$(a * b) * c = a * (b * c), \quad \forall a, b, c \in G$$

(G2) Existe um elemento neutro para a operação $*$, ou seja,

$$\exists e \in G \text{ tal que } \ a * e = e * a = a, \quad \forall a \in G$$

(G3) Existe elemento inverso para todo elemento de G, ou seja,

$$\forall\ a \in G,\ \exists a' \in G \ \text{ tal que } \ a * a' = a' * a = e$$

Observação 7.

- *Ao exigir que a operação $*$ seja uma operação binária em G, já estamos exigindo que ela seja **fechada** em G, isto é, dados $a, b \in G$, então $a * b \in G$.*
- *O elemento neutro é único*
- *O elemento inverso é único*
- *Por motivo de simplicidade usaremos a expressão "$(G, *)$ é um grupo" para significar que G é um grupo com respeito a operação $*$.*
- *Para fixar a notação vamos denotar o inverso de um elemento $a \in G$ por a^{-1}.*

Definição 1.13 (Grupo Abeliano)**.** *Um grupo G é chamado de grupo **abeliano** (ou grupo comutativo) se*

$$a * b = b * a \ \text{ para todo } \ a, b \in G.$$

Observe que se G é um grupo abeliano, então $(a * b)^{-1} = a^{-1} * b^{-1}$.

Definição 1.14 (Grupo Finito)**.** *Um grupo G é chamado de grupo **finito**, quando G contiver um número finito de elementos. Neste caso, definimos a **ordem** de G, denotada por $|G|$, sendo o número de elementos de G.*
*Quando G não é um grupo finito, dizemos que G é um grupo de **ordem infinita,** ou seja, isto ocorre quando o grupo G contém infinitos elementos.*

1.6.1 Exemplos

Exemplo 1.12. *O conjunto dos números inteiros $(\mathbb{Z}, +)$ munido da operação de soma é um grupo abeliano de ordem infinita, pois $\mathbb{Z}$ contém uma quantidade infinita de elementos.*

Exemplo 1.13. *O conjunto $(\mathbb{Z}_n, +_n)$ das classes módulo n, com a operação usual de soma $+_n$, é um grupo abeliano. Veja que $(\mathbb{Z}_n, +_n)$ é um grupo finito, pois $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}$ contém uma quantidade finita de elementos, a saber, $(\mathbb{Z}_n, +_n)$ é um grupo de ordem n. Denotamos isso por $|\mathbb{Z}_n| = n$.*

Exemplo 1.14. *O conjunto dos números racionais não nulos $(\mathbb{Q}^*, \cdot)$ munido da operação de multiplicação, é um grupo abeliano de ordem infinita.*

Exemplo 1.15. *Se p for um número primo então $\mathbb{Z}_p^\times = \{\overline{a} \in \mathbb{Z}_p |\ MDC(a,p) = 1\} = \{\overline{1}, \cdots, \overline{p-1}\}$. Portanto, $(\mathbb{Z}_p^\times, \cdot_p)$ é um grupo abeliano finito de ordem $|\mathbb{Z}_p^\times| = p - 1$.*

Exemplo 1.16. *Em geral, seja $\mathbb{Z}_n^\times = \{\overline{a} \in \mathbb{Z}_n |\ MDC(a,p) = 1\}$. Então, $(\mathbb{Z}_n^\times, \cdot_n)$ é um grupo abeliano finito de ordem $|\mathbb{Z}_n^\times| = \varphi(n)$.*

1.6.2 Subgrupo e Subgrupo Cíclico

Definição 1.15 (Subgrupo)**.** *Sejam $(G, *)$ um grupo e H um subconjunto não-vazio de G. Dizemos que H é um subgrupo de G se H, munido da operação $*$ do grupo G, for um grupo, ou seja, se $(H, *)$ for um grupo.*

Proposição 1.12 (Critério do Subgrupo)**.** *Seja H um subconjunto não-vazio de um grupo G. Então, H é um subgrupo de G se, e somente se,*

$$a * b^{-1} \in H \quad \text{para todo} \quad a, b \in H.$$

Definição 1.16 (Potências de um Elemento)**.** *Sejam $(G, *)$ um grupo e $a \in G$. Definimos as potências de a por*

$$\begin{aligned} a^0 &= e \\ a^n &= a^{n-1} * a \qquad \text{se} \quad n \in \mathbb{Z}, n \geq 1 \\ a^{-n} &= (a^{-1})^{-n} \qquad \text{se} \quad n \in \mathbb{Z},\ n < 0. \end{aligned}$$

Denotamos por $< a >$ o conjunto de todas as potências de a, ou seja,

$$< a >= \{a^n | n \in \mathbb{Z}\}$$

Proposição 1.13 (O subgrupo gerado por a)**.** *Sejam $(G, *)$ um grupo e $a \in G$. Então $< a >$ é um subgrupo de G, chamado de subgrupo gerado por a.*

Exemplo 1.17. *Dado o grupo $(\mathbb{Z}, +)$, então $n\mathbb{Z} = \{kn | k \in \mathbb{Z}\} =< n >$. Em particular, $2\mathbb{Z} =< 2 >$. Observe também que $\mathbb{Z} =< 1 >$.*

Definição 1.17 (Grupo Cíclico)**.** *Um grupo G é chamado grupo **cíclico** se $G =< a >$ para algum $a \in G$, ou seja, G é gerado por um elemento.*
Neste caso, dizemos que a é um gerador de G.

Observação 8. *Se G é um grupo cíclico, então o gerador de G, isto é, o elemento $a \in G$ tal que $G =< a >$, em geral, não é único. Por exemplo, $\mathbb{Z}_4 =< \overline{1} >$ e $\mathbb{Z}_4 =< \overline{3} >$.*

Definição 1.18 (Ordem de um Elemento)**.** *Seja G um grupo e seja $a \in G$. Se o subgrupo $< a >$ for finito, então dizemos que a **ordem de** a, denotada por $ord(a)$, é o número de elementos de $< a >$, ou seja, é igual à ordem de $< a >$.*
Agora, se $< a >$ for um grupo infinito, então dizemos que a ordem de a é infinita.

Observação 9.

- *Para o elemento neutro e de um grupo G, temos $< e >= \{e\}$ e portanto, $ord(e) = 1$. Para qualquer outro elemento $a \in G$ $(a \neq e)$, temos $ord(a) > 1$.*
- *Se G é um grupo cíclico com gerador a, $G =< a >$, então $ord(a) = |G|$.*

Exemplo 1.18. *Considere o grupo aditivo $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$.*

- *Pela observação anterior, temos que $ord(\overline{0}) = 1$.*
- $< \overline{1} >= \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\} = \mathbb{Z}_4$. *Portanto* $ord(\overline{1}) = 4$
- $< \overline{2} >= \{\overline{0}, \overline{2}\}$. *Portanto* $ord(\overline{2}) = 2$
- $< \overline{3} >= \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\} = \mathbb{Z}_4$. *Portanto* $ord(\overline{3}) = 4$

1.7 Classes Laterais e Teorema de Lagrange

Definição 1.19 (Classe Lateral)**.** *Sejam $(G, *)$ um grupo e $H \leq G$. Para cada $a \in G$, definamos a classe lateral de a à esquerda por*

$$a * H := \{a * h | h \in H\}$$

e a classe lateral de a à direita por

$$H * a := \{h * a | h \in H\}.$$

Observação 10.

1. *Se G é um grupo abeliano e se H é um subgrupo de G, então*

$$H * a = a * H, \ \forall a \in G$$

2. *Num grupo não-abeliano, a classe de a à direta pode ser diferente da classe de a à esquerda.*

Proposição 1.14 (Propriedades das Classes Laterais)**.** *Sejam $(G, *)$ um grupo finito, $H \leq G$ e $a, b \in G$.*

1. *$aH = bH$ se, e somente se, $b^{-1}a \in H$*

2. *$f_a : H \to aH$ definida por $f(h) = ah$ é bijetora. Em particular $|H| = |aH|$, isto é, todas as classes laterais têm $|H|$ elementos.*

3. *Seja φ :*
$$\begin{array}{ll} \{\text{classes laterais à esquerda}\} & \to \{\text{classes laterais à direta}\} \\ aH & \mapsto Ha^{-1} \end{array}$$
Então φ é bijetora.

4. *Se $aH \cap bH \neq \emptyset$, então $aH = bH$, ou, equivalentemente, se $aH \neq bH$, então $aH \cap bH = \emptyset$.*

5. *Existem elementos $a_1, a_2, \cdots, a_k \in G$, com $a_1 = e_G$, tal que $G = a_1H \cup a_2H \cup \cdots \cup a_kH$, e a união é disjunta.*

Notação: Denotaremos por $(G : H)$ o número de classes laterais à esquerda que é igual ao número de classes laterais à direita, pelo item (3) da Proposição 1.14. Também chamado de **índice** de H em G.

Teorema 1.4 (Teorema de Lagrange)**.** *Sejam G um grupo finito e H um subgrupo de G. Então, a ordem de H divide a ordem de G.*

Corolário 1.4 (Algumas Consequências do Teorema de Lagrange)**.**

1. *Sejam G um grupo finito e $a \in G$, então a ordem de a divide a ordem de G, isto é, $ord(a) \Big| |G|$.*

2. *Sejam G um grupo finito de ordem n e $a \in G$, então $a^n = e_G$.*

3. *Todo grupo de ordem primo é cíclico.*

1.8 Grupo Quociente e Subgrupo Normais

Definição 1.20 (Grupo Quociente)**.** *Sejam $(G, *)$ um grupo e H um subgrupo de G. Denotamos por*

$$G/H = \{a * H \ | a \in G\}$$

*o **conjunto das classes laterais** à esquerda com respeito a H.*

Vamos construir uma operação binária no conjunto das classes laterais G/H de modo a torná-lo um grupo. Para isto precisamos de uma propriedade adicional de H. Definimos a seguinte operação no conjunto das classes laterais G/H :

$$\psi : G/H \times G/H \to G/H$$

dada por

$$(aH, bH) \mapsto abH.$$

O problema é verificar que ψ está bem definida, ou seja, se ela não depender da escolha dos representantes de a e b das classes laterais aH e bH respectivamente.

Proposição 1.15. *Sejam G um grupo e H um subgrupo de G tal que as classes laterais à esquerda e à direta de H em G coincidem, isto é, $aH = Ha$ para todo $a \in G$.*
Então ψ é bem definida, isto é, se $aH = a_1H$ e $bH = b_1H$, com $a, a_1, b, b_1 \in G$, então

$$(aH, bH) = (a_1H, b_1H)$$

ou equivalentemente,

$$abH = a_1b_1H.$$

Os subgrupos N para os quais a operação binária em G/N está bem definida recebe uma denominação especial.

1.8.1 Subgrupo Normais

Definição 1.21 (Subgrupo Normal)**.** *Seja N um subgrupo G. Dizemos que N é um **subgrupo normal** de G (e denotamos $N \lhd G$) se $gN = Ng$ para todo $g \in G$.*

Existe outra caracterização de subgrupo normal muito usada. Para descrevê-la precisamos considerar o seguinte conjunto. Sejam H um subconjunto do grupo G e $a \in G$. Definimos o subconjunto aHa^{-1} de G por

$$aHa^{-1} = \{aha^{-1} | h \in H\}$$

Proposição 1.16. *Sejam G um grupo, H um subgrupo de G e $a \in G$.*

1. aHa^{-1} *é um subgrupo de* G

2. $aH = Ha$ *se, e somente se,* $aHa^{-1} = H$.

2 Representação Decimal de Números

2.1 Classificação dos números decimais

Definição 2.1. *Número decimal é representado por somas (finitas ou infinitas) de termos que envolvem potências de 10 ou de $\frac{1}{10}$, isto é da forma*

$$a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_1 \cdot 10^1 + a_0 \cdot 10^0 + d_1 \cdot \tfrac{1}{10} + d_2 \cdot \tfrac{1}{10^2} + b_3 \cdot \tfrac{1}{10^3} + \cdots$$

Todo número decimal é representado pela sequência dos coeficientes:

$$a_n a_{n-1} \ldots a_0{,}d_1 d_2 \ldots$$

A vírgula é utilizada (no Brasil) como um separador decimal (em alguns outros países, utiliza-se um ponto) que indica o começo da parte menor do que a unidade. Após a vírgula, cada dígito representa uma potência de $\frac{1}{10}$. Os algarismos após a vírgula são denominados "casas decimais". Os algarismos anteriores à vírgula formam a "parte inteira" do número.

Teorema 2.1. *Toda expressão decimal representa um número real e todo número real pode ser representado por uma expressão decimal.*

Toda fração ordinária tem sua representação decimal obtida por meio do algoritmo da divisão prolongada, no qual, acrescentam-se sucessivos zeros para continuar o processo de divisão. Por exemplo, a representação decimal de $\dfrac{5}{7}$ que é igual $0,\overline{714285}$ é obtido pela divisão prolongada conforme Figura 1.

Figura 1 – A divisão prolongada de $\frac{5}{7}$.

$$
\begin{array}{r|l}
5 & 7 \\
\cline{2-2}
0 & 0,714285 \\
\cline{1-1}
50 & \\
49 & \\
\cline{1-1}
10 & \\
7 & \\
\cline{1-1}
30 & \\
28 & \\
\cline{1-1}
20 & \\
14 & \\
\cline{1-1}
60 & \\
56 & \\
\cline{1-1}
40 & \\
35 & \\
\cline{1-1}
5 &
\end{array}
$$

Fonte: Produzido pelo autor

Definição 2.2. *Um número decimal é finito ou exato (tem um número finito de dígitos), quando é representado por uma soma com número finito de parcelas.*

Exemplo 2.1.

1. $0{,}25 = 0{,}2 + 0{,}05 = 2 \cdot \frac{1}{10} + 5 \cdot \frac{1}{10^2}$
2. $3{,}728 = 3 + 0{,}7 + 0{,}02 + 0{,}008 = 3 \cdot 10^0 + 7 \cdot \frac{1}{10} + 2 \cdot \frac{1}{10^2} + 8 \cdot \frac{1}{10^3}$

Definição 2.3. *Dízima periódica são números que apresenta, na sua parte fracionária, após um número finito de termos, um bloco de algarismos, não totalmente nulos, com a propriedade que, a partir dele, a sequência de dígitos é constituída exclusivamente pela repetição sucessiva deste bloco.*
E essa parte que se repete é chamada de período e o número de algarismos chamaremos de comprimento do período.

Exemplo 2.2.

1. $1{,}3592929292 \longrightarrow$ *Período:* 92; *Comprimento do período:* 2
2. $0{,}285714285714 \longrightarrow$ *Período:* 285714; *Comprimento do período:* 6
3. $0{,}00777777 \longrightarrow$ *Período:* 7; *Comprimento do período:* 1

Costumamos denotar o período com uma barra superior:

Exemplo 2.3.

1. $1{,}3592929292 = 1{,}35\overline{92}$

2. $0{,}285714285714 = 0{,}\overline{285714}$

3. $0{,}00777777 = 0{,}00\overline{7}$

Observação 11. *O decimal exato pode ser considerada uma espécie de caso particular de dízima periódica,pois* $0{,}25 = 0{,}250000... = 0{,}25\overline{0}$.

Definição 2.4. *A dízima periódica simples é uma dízima periódica que só tem a parte que se repete depois da vírgula.*

Exemplo 2.4. *Considere a dízima periódica simples 0,454545...,então seu período é 45 e o comprimento do seu período é 2.*

Definição 2.5. *A dízima periódica composta é a dízima que tem uma parte que não se repete seguida de uma parte que se repete depois da vírgula.E essa parte que não se repete chamaremos de anteperíodo e o número de algarismos desse anteperíodo é chamado de comprimento do anteperíodo.*

Exemplo 2.5. *Considere a dízima periódica composta 0,456666...,então o seu anteperíodo é 45,seu período é 6,o comprimento do seu período é 1 e o comprimento do seu anteperíodo é 2.*

Definição 2.6. *Número irracional é um numero que tem um número infinito de dígitos depois da vírgula,porém estes não se repetem de forma periódica. E esses não serão muito citados nesse trabalho.*

2.2 Notações

Na sequência letras maiúsculas denotam números inteiros. A, B, N os quais são positivos. Sempre que escrevemos a fração $\frac{M}{N}$,assumiremos $0 < M < N$ e $N \geq 2$.

Letras minúsculas com índices denotam dígitos decimais Uma sequência como $d_1d_2d_3 \cdots d_n$ denota um inteiro ou decimal representado por esses dígitos.

Exemplo 2.6. $d_1 = 1, d_2 = 2$ *e* $d_3 = 5$,*então* $d_1d_2d_3 = 125$ *e* $0{,}d_1d_2d_3 = 0,125$.

Para a fração $\dfrac{1}{N}$, vamos denotar o comprimento do seu período por $\lambda(N)$ e o comprimento do anteperíodo por $\Lambda(N)$.

Exemplo 2.7.

N	$\frac{1}{N}$	$\Lambda(N)$	$\lambda(N)$
2	$0{,}5$	1	0
3	$0{,}\overline{3}$	0	1
4	$0{,}25$	2	0
5	$0{,}5$	1	0
6	$0{,}1\overline{6}$	1	1
7	$0{,}\overline{142857}$	0	6
8	$0{,}125$	3	0
9	$0{,}\overline{1}$	0	1
10	$0{,}1$	1	0
11	$0{,}\overline{09}$	0	2
12	$0{,}08\overline{3}$	2	1
13	$0{,}\overline{076923}$	0	6
14	$0{,}0\overline{714285}$	1	6
15	$0{,}0\overline{6}$	1	1
16	$0{,}0625$	4	0
17	$0{,}\overline{0588235294117647}$	0	16
18	$0{,}0\overline{5}$	1	1
19	$0{,}\overline{052631578947368421}$	0	18
20	$0{,}05$	2	0

Tabela 2 – O valores de $\lambda(N)$ e $\Lambda(N)$ para $N = 1, 2, \cdots, 20$.

3 Representação Decimal dos Racionais

Neste capitulo vamos estudar a representação decimal dos racionais.

Na antiguidade, para facilitar o processo de contagem que era importante para o desenvolvimento da humanidade, surgiram os números, inicialmente, para representar quantidades inteiras de objetos, animais ou qualquer coisa que precisasse contar. Porém, esses números ficaram insuficientes quando ocorriam situações que necessitavam de divisões sucessivas em partes iguais surgindo assim as frações.

Teorema 3.1. *A representação decimal de qualquer fração $\frac{M}{N}$ ou ela é decimal finita ou uma dizima periódica.*

Demonstração. A fração $\frac{M}{N}$ é convertido em uma expansão decimal pela divisão longa de M por N. Na divisão por N, cada resto é menor que N, e o primeiro resto é M. O resto em qualquer ponto da divisão determina todos os dígitos do quociente a seguir. Em algum momento, o o resto será 0, caso em que a expansão termina, ou um número diferente de zero o que ocorreu antes, neste caso a expansão se repete periodicamente. No ultimo caso, o período é o número de passos entre os restos recorrentes e é menor que N, uma vez que apenas restos de 1 a $N-1$ são possíveis.

□

3.1 Representação Decimal Finita

Nesta seção vamos mostrar que partindo de um número racional (escrito em sua forma fracionária irredutível), a decomposição do denominador em fatores primos determine se a sua representação decimal será finita ou infinita.

Definição 3.1. *Uma representação decimal finita é um símbolo da forma*

$$\alpha = a_0,a_1a_2\cdots a_n \tag{3.1}$$

em que a_0 é um número inteiro ≥ 0 e $a_1, a_2\cdots, a_n$ são dígitos, isto é, números inteiros tais que $0 \leq a_n < 10$.

Lema 3.1. *A representação decimal de uma fração $\frac{M}{N}$ é um número decimal finita se e somente se a decomposição em fatores primos de N tem apenas 2 ou 5.*

Demonstração. ($\Rightarrow$) : Suponha que $\frac{M}{N}$ tem a representação

$$\frac{M}{N} = s + 0{,}t_1t_2t_3\ldots t_n$$

aqui $s \in \mathbb{Z}$ é a parte inteira e cada t_j é uma casa decimal de r, ou seja, cada t_j é um número inteiro entre 0 e 9. Vamos provar que N é da forma 2^k5^l para algum $k, l \in \mathbb{N}$. Note que se $t_j = 0$ para todo $j = 1, 2\cdots, n$ então $\frac{M}{N} = s$ é um número inteiro e podemos escrever N na forma como

$$N = 2^05^0.$$

Logo, podemos supor que pelo menos uma casa decimal é diferente de zero, ou seja, que $t_n \neq 0$. Neste caso

$$0{,}t_1t_2t_3...t_n \times 10^n = t_1t_2t_3...t_n \Rightarrow 0{,}t_1t_2t_3...t_n = \frac{t_1t_2t_3...t_n}{10^n}$$

e assim

$$\frac{M}{N} = s + 0{,}t_1t_2t_3...t_n = s + \frac{t_1t_2t_3...t_n}{10^n} = \frac{s \times 10^n + t_1t_2t_3...t_n}{10^n}.$$

Assim $N|(10^n)$. Portanto N é da forma 2^k5^l para algum $k, l \in \mathbb{N}$.

($\Leftarrow$) : Reciprocamente,seja $\frac{M}{N}$ uma fração irredutível com a $M \in \mathbb{Z},\ N = 2^p5^q$,com $p, q \in \mathbb{Z}+$.Supondo $p \geq q$ temos

$$\frac{M}{N} = \frac{M}{2^p5^q} = \frac{M}{2^p5^q}.\frac{5^{(p-q)}}{5^{(p-q)}} = \frac{M \times 5^{(p-q)}}{10^p}$$

e daqui podemos concluir que a representação decimal de $\frac{M}{N}$ possui p casas decimais. O caso de $p < q$ é análogo,o que conclui o lema.

□

Exemplo 3.1. $\frac{1}{4} = 0{,}25$ *pois* $4 = 2 \cdot 2$

Exemplo 3.2. $\frac{1}{10} = 0{,}1$ *pois* $10 = 2 \cdot 5$

Corolário 3.1. *Um número racional possui representação decimal infinita se somente se quando escrito na forma irredutível, a decomposição em fatores primos do denominador possui algum fator primo diferente de 2 e 5.*

Lema 3.2. *O comprimento do anteperíodo de* $\frac{1}{N}$ *,onde a decomposição em fatores primos de N possui apenas os fatores 2 ou 5 e* $N = 2^A5^B$ *é* $\max(A, B)$.

Demonstração. Seja $\frac{1}{N} = 0{,}t_1t_2t_3\ldots t_n$. Então o comprimento anteperiodo é n. Agora

$$\frac{1}{2^A5^B} = \frac{t_1t_2t_3\ldots t_n}{10^n}.$$

Portanto

$$2^A 5^B | (10^n).$$

Isto é possível se $n = \max(A, B)$.

□

Exemplo 3.3. $\Lambda(200) = 3$, *pois* $\frac{1}{200} = 0,005$ *e temos 3 dígitos após a vírgula. Usando o Lema 3.2, temos que*

$$\Lambda(200) = \Lambda(2^3 \cdot 5^2) = \max(2, 3) = 3.$$

Lema 3.3. *Dada qualquer fração irredutível* $\frac{M}{N}$ *o comprimento da parte decimal é independente de* M *e é portanto igual a* $\Lambda(N)$*. E a parte decimal de* $\dfrac{M}{N}$ *é* M *vezes a parte decimal de* $\frac{1}{N}$*.*

Demonstração. Sejam P igual ao comprimento do anteperíodo de $\frac{1}{N}$ e T seu anteperiodo e sejam Q igual ao comprimento do anteperíodo de $\frac{M}{N}$ e U seu anterperiodo. Então

$$T = \frac{10^P}{N} \quad \text{e} \quad U = \frac{M \cdot 10^Q}{N}.$$

P é o menor valor para o qual N divide 10^P e da mesma forma Q é o menor valor para qual $N | M \cdot 10^Q$. Como M e N são primos entre sí,eles não tem fatores em comum,então $N | 10^Q$. Q deve ser o menor valor pelo qual isso vale, pois contrario, se existe $S < Q$ e $N | 10^S$ então teríamos que $N | M \cdot 10^S$ e Q não seria o menor valor. Mas P é também o menor valor para o qual $N | 10^P$,consequentemente $P = Q$ e $U = MT$.

□

Exemplo 3.4. $\frac{4}{5} = 0,8 = 4 \cdot 0,2 = 4 \cdot \frac{1}{5}$ *e ainda* $\frac{4}{5} = \Lambda(\frac{1}{5}) = 1$*.*

Lema 3.4. *Sejam* H *e* N *números cujas decomposições em fatores primos só tem 2 ou 5, então*

$$\Lambda(HN) \leq \Lambda(H) + \Lambda(N).$$

Demonstração. Se H= $2^A \cdot 5^B$ e $N = 2^C \cdot 5^D$,então temos

$$\begin{aligned} \Lambda(HN) &= \Lambda(2^{(A+C)} \cdot 5^{(B+D)}) \\ &= \max(A + C, B + D) \\ &\leq \max(A, B) + \max(C, D) = \Lambda(H) + \Lambda(N) \end{aligned}$$

□

Exemplo 3.5. $\Lambda(200) = \Lambda(10 \cdot 20) = \Lambda(2 \cdot 5 \cdot 2^2 \cdot 5) = \Lambda(2 \cdot 5) + \Lambda(2^2 \cdot 5) = 1 + 2 = 3$. *pois* $\frac{1}{200} = 0,005$ *e ainda* $\frac{1}{10} = 0,1$ *e* $\frac{1}{20} = 0,05$*.*

Lema 3.5. *Seja N um número cuja decomposição em fatores primos só tem 2 ou 5, então*

$$\Lambda(N^k) = K \cdot \Lambda(N).$$

Demonstração. Se $N = 2^C \cdot 5^D$, então

$$\Lambda(N^K) = \Lambda(2^{KC} \cdot 5^{KD}) = \max(KC, KD) = K \cdot \max(C, D) = K \cdot \Lambda(N).$$

□

Exemplo 3.6. $\Lambda(50) = 2$, *pois* $\frac{1}{50} = 0,02$. *Logo, usando Lema 3.5, temos que* $\Lambda(50^3) = \Lambda((2\cdot 5^2)^3) = 3.\Lambda(2\cdot 5^2) = 3\cdot 2 = 6$. *E observe que* $\frac{1}{50^3} = \frac{1}{125000} = 0,000008$.

Construímos na Tabela 3, os valores de $\Lambda(2^K)$, $K = 1, 2, \cdots, 10$.

K	2^K	$\frac{1}{2^K}$	$\Lambda(2^K)$
1	2	0,5	1
2	4	0,25	2
3	8	0,125	3
4	16	0,625	4
5	32	0,03125	5
6	64	0,015625	6
7	128	0,0078125	7
8	256	0,00390625	8
9	512	0,001953125	9
10	1024	0,0009765625	10

Tabela 3 – Decimais e comprimento do anteperiodo de $\frac{1}{2^K}$ para $k = 1$ até 10.

3.2 Dízima periódica simples

Considerando a Definição 2.4, iremos mostrar que toda dízima periódica simples pode ser escrita como uma fração de denominador $10^p - 1$.

Lema 3.6. *Para qualquer dízima periódica simples* $0,\overline{d_1 d_2 \ldots d_p} = \frac{R}{10^p - 1}$, *onde* $R = d_1 d_2 \ldots d_p$ *e seu período e* p *é o comprimento do período.*

Demonstração.

$$0,\overline{d_1 d_2 \ldots d_p} = 0,d_1 d_2 \ldots d_p + 0,\underbrace{00\ldots0}_{p \text{ zeros}} d_1 d_2 \ldots d_p + 0,\underbrace{00\ldots0}_{2p \text{ zeros}} d_1 d_2 \ldots d_p + \cdots$$
$$= \frac{d_1 d_2 \ldots d_p}{10^p} + \frac{d_1 d_2 \ldots d_p}{10^{2p}} + \frac{d_1 d_2 \ldots d_p}{10^{3p}} + \cdots$$

Portanto a dízima periódica é uma série geométrica convergente. onde o primeiro termo é $0,d_1 d_2 \ldots d_p$ e sua razão é 10^{-p}. Logo a soma

$$\frac{0{,}d_1d_2\ldots d_p}{1-10^{-p}} = \frac{\frac{R}{10^p}}{1-10^{-p}} = \frac{R}{10^p-1}.$$

□

Exemplo 3.7. $0{,}\overline{125} = \dfrac{125}{10^3-1} = \dfrac{125}{999}$

.

Lema 3.7. *A expansão decimal de uma fração* $\frac{M}{N}$ *é uma dízima periódica simples se e somente se,a decomposição em fatores primos de* N *não tem os algarismos 2 ou 5, ou seja* $MDC(N,10) = 1$.

Demonstração. Seja $\frac{M}{N}$ a forma reduzida de $\frac{R}{10^p-1}$. Como M e N não tenham fatores comuns N divide $10^p - 1$.

Cada fator primo de N também divide $10^P - 1$. Mas 2 e 5 nunca pode dividir $10^P - 1$ pois o último dígito de $10^P - 1$ é sempre 9, então a decomposição de N não tem os algarismos 2 ou 5.

De forma análoga demonstramos que se N não tem na sua decomposição em fatores primos os números 2 ou 5,a expansão decimal de $\frac{M}{N}$ é uma dízima periódica simples.

□

Exemplo 3.8. $\frac{12}{27} = 0,\overline{4}$ *, pois* $27 = 3^3$ *e não tem 2 ou 5 na sua decomposição.*

Corolário 3.2. *Seja* N *tal* $MDC(N,10) = 1$, *então o comprimento do período de* $\dfrac{1}{N}$ *é o menor inteiro* $p \geq 1$ *tal que* $10^p - 1$ *é divisível por* N. *Alem disso o período é o quociente desta divisão.*

N	Expansão decimal de $\frac{1}{N}$	Menor inteiro positivo tal que N divide $10^p - 1$
3	$0,\overline{3}$	$10^1 - 1 = 3 \cdot 3$
7	$0,\overline{142857}$	$10^6 - 1 = 7 \cdot 142857$
9	$0,\overline{1}$	$10^1 - 1 = 9 \cdot 1$
11	$0,\overline{09}$	$10^2 - 1 = 11 \cdot 9$
13	$0,\overline{076923}$	$10^6 - 1 = 13 \cdot 76923$
17	$0,\overline{0588235294117647}$	$10^{16} - 1 = 17 \cdot 588235294117647$
19	$0,\overline{052631578947368421}$	$10^{18} - 1 = 19 \cdot 52631578947368421$
21	$0,\overline{047619}$	$10^6 - 1 = 21 \cdot 47619$
23	$0,\overline{0434782608695652173913}$	$10^{22} - 1 = 23 \cdot 43478260869565217391 3$
27	$0,\overline{037}$	$10^3 - 1 = 27 \cdot 37$
29	$0,\overline{0344827586206896551724137931}$	$10^{28} - 1 = 29 \cdot 34482758620689655172413793 1$

Tabela 4 – Uma ilustração do Corolário 3.2 para pequenos valores de n.

Lema 3.8. *Dada qualquer fração irredutível $\frac{M}{N}$, seu período é independente de M e é portanto igual o período $\frac{1}{N}$. De fato o período de $\frac{M}{N}$ é igual M vezes o período de $\frac{1}{N}$.*

Demonstração. Seja p o comprimento do período de $\frac{1}{N}$ e R seu período e Q seja o comprimento do período de $\frac{M}{N}$ e S seu período, então $R = \frac{10^P - 1}{N}$ e $S = \frac{M10^Q - 1}{N}$ P é o menor valor para o qual N divide $10^P - 1$ e analogamente Q é o menor valor para o qual N divide $M(10^{Q-1})$,como M e N são primos entre sí,eles não tem fatores em comum,então N divide (10^{Q-1}).Q deve ser o mínimo valor para o qual isso vale,desde que tenhamos $T < Q$ e N dividindo 10^{T-1} então teríamos que N divide $M.\ 10^{T-1})$ e Q não seria o menor valor,mas P é também o menor valor para o qual N divide 10^{P-1}.Consequentemente $P = Q$ e $S = MR$.

□

Exemplo 3.9. $\frac{4}{9} = 0,\overline{4} = 4 \cdot 0,\overline{1}$, *pois* $\frac{1}{9} = 0,\overline{1}$

Lema 3.9. *O comprimento do período $\lambda(N)$ de $\frac{M}{N}$ nunca excede $N - 1$.*

Demonstração. Todos os restos da divisão de M por N estão entre 1 e $N - 1$. Sempre que qualquer um deles ocorrer pela segunda vez uma parte periódica é estabelecida, consequentemente o período esta sempre entre 1 e $N - 1$.

Exemplo 3.10. $\lambda(19) = 18$, *pois* $\frac{1}{19} = 0,\overline{052631578947368421}$, *ou ainda* $\lambda(7) = 6$,*pois* $1/7 = 0,\overline{142857}$

Lema 3.10. *Se o período de* $\frac{M}{N}$ *é* R *e* $\lambda(N) = N - 1$ *então o período de* $\frac{J}{N}$ *é uma permutação cíclica de* R.

Demonstração. Como $0 < M$,$J < N$ e $\lambda(N) = N-1$, todo inteiro de 1 até $N-1$,incluindo M e J,deve ocorrer como um dos restos do cálculo da expansão decimal de $\frac{M}{N}$. O numerador é sempre o primeiro resto em qualquer um dos cálculos, então J ocorrerá como resto em algum momento na expansão decimal de $\frac{M}{N}$. Quando isso acontece, o dígito em $\frac{M}{N}$ naquele ponto será o primeiro dígito de $\frac{J}{N}$.

Como os dígitos subsequentes dependem somente do resto atual, os dígitos de $\frac{J}{N}$ repetirá os dígitos de $\frac{M}{N}$ mas iniciando em um diferente ponto, ou seja, os dígitos de $\frac{J}{N}$ serão uma permutação cíclica doa dígitos de $\frac{M}{N}$.

□

Exemplo 3.11. *Vamos considerar* $N = 7$. *Então*

$$\begin{array}{ccccccccccccc} 0,\overline{142857} & \to & 0,\overline{428571} & \to & 0,\overline{285714} & \to & 0,\overline{857142} & \to & 0,\overline{571428} & \to & 0,\overline{714285} & \to & 0,\overline{142857} \\ \frac{1}{7} & \to & \frac{3}{7} & \to & \frac{2}{7} & \to & \frac{6}{7} & \to & \frac{4}{7} & \to & \frac{5}{7} & \to & \frac{1}{7} \end{array}$$

As Tabelas 5 até Tabela 8 abaixo ilustra o exemplo da representação decimal de $\frac{M}{21}$ para $M = 1$ até $M = 21$ onde $\varphi(21) = 12$ e $\lambda(12) = 6$.

M	$\frac{M}{21}$
1	$0,\overline{047619}$
2	$0,\overline{095238}$
3	$0,\overline{142857}$
4	$0,\overline{190476}$
5	$0,\overline{238095}$
6	$0,\overline{285174}$
7	$0,\overline{3}$
8	$0,\overline{380952}$
9	$0,\overline{428571}$
10	$0,\overline{476190}$
11	$0,\overline{523809}$
12	$0,\overline{571428}$
13	$0,\overline{619048}$
14	$0,\overline{6}$
15	$0,\overline{714285}$
16	$0,\overline{761904}$
17	$0,\overline{809523}$
18	$0,\overline{857142}$
19	$0,\overline{904761}$
20	$0,\overline{952380}$
21	$0,\overline{9}$

Tabela 5 – Decimal representações de $\frac{M}{21},\ M = 1, \cdots 21$..

M	$\frac{M}{21}$
1	$0{,}\overline{047619}$
10	$0{,}\overline{476190}$
16	$0{,}\overline{761904}$
13	$0{,}\overline{619048}$
4	$0{,}\overline{190476}$
19	$0{,}\overline{904761}$

M	$\frac{M}{21}$
2	$0{,}\overline{095238}$
20	$0{,}\overline{952380}$
11	$0{,}\overline{523809}$
5	$0{,}\overline{238095}$
8	$0{,}\overline{380952}$
17	$0{,}\overline{809523}$

Tabela 6 – Os dois ciclos nas quais $\frac{M}{21}$ se reduza.

M	$\frac{M}{21}$
3	$0{,}\overline{142857}$
9	$0{,}\overline{428571}$
6	$0{,}\overline{285174}$
18	$0{,}\overline{857142}$
12	$0{,}\overline{571428}$
15	$0{,}\overline{714285}$

Tabela 7 – O ciclo na qual $\frac{M}{21}$ reduza a $\frac{M}{7}$.

M	$\frac{M}{21}$
7	$0{,}\overline{3}$
14	$0{,}\overline{6}$
21	$0{,}\overline{9}$

Tabela 8 – O ciclo na qual $\frac{M}{21}$ reduza a $\frac{M}{3}$.

Lema 3.11. *Se $\lambda(N) = N - 1$, então N é primo.*

Demonstração. Se N fosse composto, então $\frac{M}{N}$ seria redutível para $\frac{J}{K}$, para algum $K < N$. Como $\lambda(N)$ nunca pode exceder $N - 1$, temos $\lambda(K)$ não poderia exceder $K - 1$ que é menor que $N - 1$. Mas pelo lema anterior $\lambda(K) = \lambda(N) = N - 1$. Contradição, e consequentemente N é primo.

□

Exemplo 3.12. $\lambda(7) = 6, pois 1/7 = 0, \overline{142857}$

Observação 12. *A reciproca do Lema 3.11 é falsa.*
Por exemplo $\lambda(3) = 1 \neq 2$ *pois* $1/3 = 0, \overline{3}$ *e* $\lambda(11) = 2 \neq 10$,*pois* $1/11 = 0, \overline{09}$

Se $\lambda(N) < N - 1$ então podem existir múltiplos ciclos de comprimento $\lambda(N)$. Isso pode ser expresso mais precisamente a seguir.

Lema 3.12. *$\lambda(N)$ divide $\varphi(N)$,onde $\varphi(N)$ é a função fi de Euler.*

Demonstração. A função fi de Euler $\varphi(N)$ é o número de inteiros primos com N, menores que N. Isto é portanto o número de inteiros $M < N$ tal que $\frac{M}{N}$ é irredutível. O número de ciclos do comprimento $\lambda(N)$ é $\frac{\phi(N)}{\lambda(N)}$. □

N	3	11	13	17	19	21	23	31	33	37	39	41	51
$\lambda(N)$	1	2	6	16	18	12	22	15	2	3	6	5	16
$\varphi(N)$	2	10	12	16	18	12	22	30	20	33	24	40	32

Tabela 9 – Alguns valores que mostram que $\lambda(N)$ divide $\varphi(N)$

Lema 3.13. *λ não é multiplicativo por números inteiros que não tenham 2 ou 5 na sua decomposição em fatores primos. Isto é para H e N inteiros que não possuem 2 ou 5 na sua decomposição em fatores primos,$\lambda(HN)$ não é necessariamente igual $\lambda(H) \cdot \lambda(N)$ e $\lambda(N^(K))$ não é necessariamente igual a $K \cdot \lambda(N)$.*

Demonstração. Usaremos exemplos para mostrar o nosso lema.

Tomemos $H = 7$ e $N = 11$,$\frac{1}{H} = \frac{1}{7}$ e $\frac{1}{N} = \frac{1}{11}$.

$\lambda(H) = 6$ e $\lambda(N) = 2$, logo $\lambda(H).\lambda(N) = 12$ e $\lambda(HN) = \lambda(77) = 6$.

E concluímos neste caso que $\lambda(HN) \neq \lambda(H) \cdot \lambda(N)$

E ainda para $N = 7$ e $K = 2$ termos que $\lambda(7^2) \neq 2.\ \lambda(7)$,pois $\lambda(7^2) = 42$ e $\lambda(7) = 6$.

O que mostra o nosso lema.

□

3.2.1 Propriedade dos noves

Definição 3.2. *Dizemos que um número M tem a "propriedade dos noves" se $M = 999\ldots99$ (N dígitos iguais a 9). Podemos mostrar que*

$$\underbrace{999\ldots99}_{N \textbf{ dígitos iguais a 9}} = 10^N - 1.$$

Analogamente dizemos que um número M tem a "propriedade das unidades" se

$$M = \underbrace{111\ldots11}_{N \textbf{ dígitos iguais a 1}} = \frac{10^N - 1}{9}.$$

Mais geral dizemos que um número M tem a"propriedade dos digitos d" se

$$M = \underbrace{ddd\ldots dd}_{N \textbf{ dígitos iguais a d}} = d \cdot \underbrace{(111\ldots11)}_{N \textbf{ dígitos iguais a 1}} = \frac{d}{9}\left(10^N - 1\right).$$

□

Lema 3.14. *Cada primo P, exceto 2, 3 e 5, divide um número com a propriedade das unidades. Isto é P divide* $\underbrace{111\ldots11}_{N \textbf{ dígitos iguais a 1}} = \frac{10^N-1}{9}$ *para algum $N < P$.*

Demonstração. Seja N o comprimento do período de $\frac{1}{P}$ e R seu período. Então

$$\frac{1}{P} = \frac{R}{10^N - 1}, \text{ para algum } N < P.$$

Logo

$$P \cdot R = 10^N - 1 = \underbrace{999\ldots99}_{N \textbf{ dígitos iguais a 9}} = 9 \cdot \underbrace{111\ldots11}_{N \textbf{ dígitos iguais a 1}}$$

Como $P \neq 3$ então P divide $\underbrace{111\ldots11}_{N \textbf{ dígitos iguais a 1}}$. □

Observação 13. *Para $P = 3$, $N = P$, pois 3 divide 111.*

Exemplo 3.13.

1. *7 divide* 111111 *ou seja,* $111111 = 15873 \cdot 7$.

2. *13 divide* 111111111111 *ou seja,* $111111111111 = 8547008547 \cdot 13$

Lema 3.15 (**Teorema de Midy**). *Na expansão decimal de $\frac{M}{N}$, se N é primo diferente de 2 ou 5 e $\lambda(N)$ é par, então a soma das duas metades do período é um número com a propriedade das noves.*
Isto é se $\lambda(N) = 2L$ e o período é $a_1a_2\ldots a_Lb_1\ldots b_L$.
Sejam $A = a_1\ldots a_L$ e $B = b_1\ldots b_L$, então

$$A + B = 10^L - 1 = \underbrace{999\ldots99}_{L \textbf{ dígitos iguais a 9}}.$$

Um número N que satisfazer as condições do Lema é dito "tem a propriedade de nove".

Demonstração. Seja $L = \frac{1}{2} \cdot \lambda(N)$, o comprimento de cada metade, e seja R o período. A expansão decimal é uma dizima periódica pois a decomposição em fatores primos de N não tenha os dígitos 2 ou 5. $\frac{M}{N}$ é uma fração irredutível para todo M pois N é primo. Temos que

$$\frac{M}{N} = \frac{R}{10^{2L} - 1} \text{ e } N|(10^{2L} - 1) = (10^L + 1).(10^L - 1).$$

Como N é primo, então $N|(10^L + 1)$ ou $N|(10^L - 1)$. Mas se $N|(10^L - 1)$,então $\lambda(N)$ seria L, entanto assumimos que $\lambda(N) = 2L$. Logo $N|(10^L + 1)$.

Considere $A = \frac{M}{N}(10^L + 1) - 1$. Então A é um inteiro com $0 < A < (10^L - 1)$ pois $N|(10^L + 1)$ e $M < N$. Então A tem então no máximo L algarismos.

Denotamos $A = a_1a_2\cdots a_L$ e consideremos $B = 10^L - 1 - A$, no qual é inteiro com $0 < B < (10^{L-1})$ e denotamos $B = b_1b_2\cdots b_L$.

Vamos computar

$$\begin{aligned} a_1a_2\cdots a_Lb_1b_2\cdots b_L &= A10^L + B \\ &= \left[\frac{M}{N}(10^2L+1) - 1\right]10^L + 10^L - 1 - \left[\frac{M}{N}10^L - 1\right] \\ &= \frac{M}{N}(10^L+1)10^L - \frac{M}{N}(10^L-1) = \frac{M}{N}(10^L+1)(10^L-1) \\ &= \frac{M}{N}(10^{2L}-1) = R \end{aligned}$$

A e B são as duas metades da parte periódica e $A + B = 10^L - 1 = \underbrace{999\ldots99}_{L \text{ dígitos iguais a } 9}$. □

Exemplo 3.14.

1. *$N = 13$ tem a propriedade de nove, pois $\lambda(13) = 6$ par e $\frac{1}{13} = 0{,}\overline{076923}$ e $076+923 = 999$*
2. *$N = 17$ tem a propriedade de nove, pois $\lambda(17) = 16$ par e $\frac{1}{17} = 0{,}\overline{0588235294117647}$ e $05882352 + 94117647 = 99999999$.*

Corolário 3.3. *Se N divide $10^p + 1$, sendo p primo, então N tem a propriedade dos noves.*

Exemplo 3.15.

$10^3 + 1 = 1001 = 7 \cdot 11 \cdot 13$. Portanto além dos numeros 7, 11 e 13 são números com a propriedade dos noves, temos também que $77, 91, 143$ e 1001 são números de tem a propriedade dos noves.

$$\frac{1}{77} = 0{,}\overline{012987} \quad e \quad 012 + 987 = 999.$$
$$\frac{1}{91} = 0{,}\overline{010899} \quad e \quad 010 + 989 = 999.$$
$$\frac{1}{143} = 0{,}\overline{006993} \quad e \quad 006 + 993 = 999.$$
$$\frac{1}{1001} = 0{,}\overline{000999} \quad e \quad 000 + 999 = 999.$$

3.2.2 Dizima periódica simples e a Estrutura Grupo

Lema 3.16. *Na expansão decimal da fração $\frac{1}{N}$, com $MDC(N, 10) = 1$, temos que os restos na divisão de 1 por N forma um subgrupo cíclico H, gerado por 10, do grupo multiplicativo $(\mathbb{Z}_N^\times, \odot_N)$ de ordem $\lambda(N)$. Isto é*

$$H = \{10,\ 10^2, \cdots, 10^{\lambda(N)} \equiv 1\} \ (\bmod N)$$

Além disto, temos $\frac{\varphi(N)}{\lambda(N)}$ classes laterais a $\odot_N H$ em $(\mathbb{Z}_N^\times, \odot_N)$.

Exemplo 3.16. *Vamos considerar a fração* $\frac{1}{39}$.

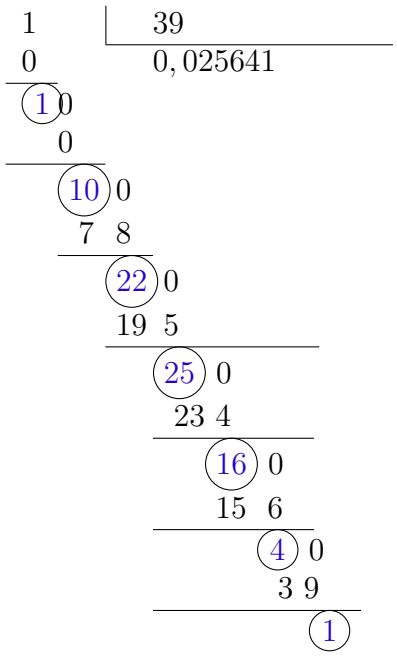
- $\frac{1}{39} = 0{,}\overline{025641}$. *Logo* $\lambda(39) = 6$
- $\varphi(39) = \varphi(3 \cdot 13) = \varphi(3) \cdot \varphi(13) = 2 \cdot 12 = 24$.
- *O grupo* $(\mathbb{Z}_{39}^{\times}, \odot_{39})$ *é um grupo com 24 elementos. Isto é*

$$\mathbb{Z}_{39}^{\times} = \{\overline{1}, \overline{2},\ \overline{4}, \overline{5}, \overline{7}, \overline{8}, \overline{10}, \overline{11}, \overline{14}, \overline{16}, \overline{17}, \overline{19}, \overline{20}, \overline{22}, \overline{23}, \overline{25}, \overline{28}, \overline{29}, \overline{31}, \overline{32}, \overline{34}, \overline{35}, \overline{37}, \overline{38}\}$$

- *Fazendo a divisão longa de 1 por 27, conforme a Figura 2 abaixo os restos da divisão forma o subgrupo cíclico de ordem* $\lambda(39) = 6$.

$$H = \{\overline{1},\ \overline{10},\ \overline{22},\ \overline{25},\ \overline{16},\ \overline{4}\} = \{10^6,\ 10^1,\ 10^2,\ 10^3,\ 10^4,\ 10^5\}\ (\text{ mod } 39).$$

Figura 2 – A divisão prolongada de $\frac{1}{39}$ com os restos circulados.



Fonte: Produzido pelo autor

Na divisão prolongada, o resto sempre determina inequivocamente (de acordo com o algoritmo de divisão) tanto o dígito da expansão decimal quanto o próximo resto. Poderíamos ilustrar esse processo na Tabela 10

Olhando para a Tabela 10, fica claro que se tomarmos, alternadamente, como dividendo os números 10, 22, 25, 16 e 4 diferentes de 1 em nosso subgrupo, a expansão

Resto do subgrupo	1	10	22	25	16	4
O digito do período	0	2	5	6	4	1

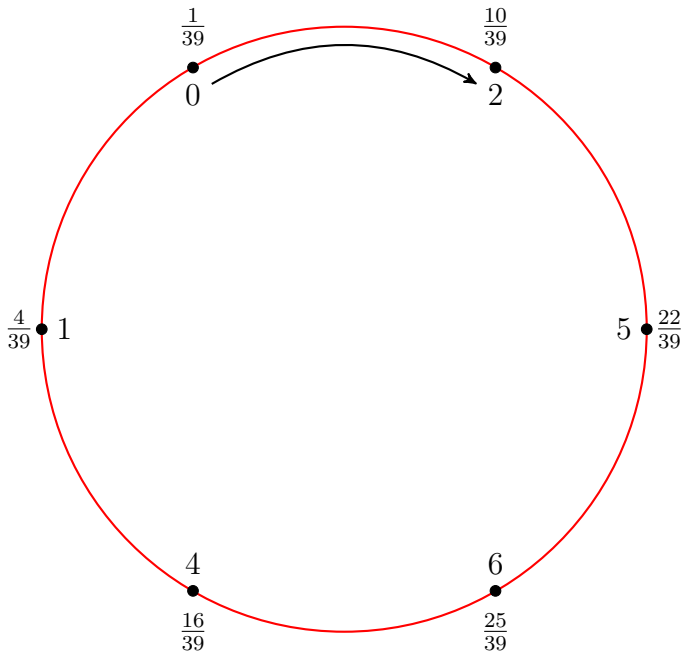
Tabela 10 – Restos do subgrupo na divisão $\frac{1}{39}$ e os dígitos que eles produzem

decimal deve sempre se repetir ciclicamente a expansão $\frac{1}{39} = 0{,}\overline{025641}$. *Isto é*

$$\begin{array}{ccccccccccccc} 0{,}\overline{025641} & \to & 0{,}\overline{256410} & \to & 0{,}\overline{564102} & \to & 0{,}\overline{641025} & \to & 0{,}\overline{410256} & \to & 0{,}\overline{102564} & \to & 0{,}\overline{025641} \\ \frac{1}{39} & \to & \frac{10}{39} & \to & \frac{22}{39} & \to & \frac{25}{39} & \to & \frac{16}{39} & \to & \frac{4}{39} & \to & \frac{1}{39} \end{array}$$

Isso também pode ser ilustrado por um círculo, veja a Figura 3 .

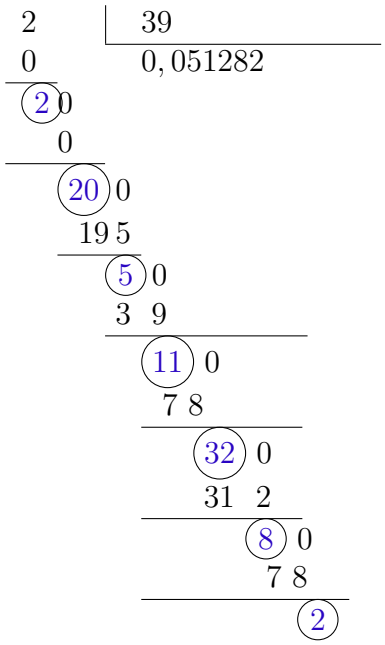
Figura 3 – A divisão prolongada de $\frac{1}{39}$.



Fonte: Produzido pelo autor

- *Temos* $\frac{\varphi(39)}{\lambda(39)} = \frac{24}{6} = 4$ *classes laterias de* H *em* $(\mathbb{Z}_{39}^{\times}, \odot_{39})$.
- *Agora vamos fazer a divisão longa* $\frac{2}{39}$ *onde o dividendo 2 não pertence ao subgrupo* H.

Figura 4 – A divisão prolongada de $\frac{2}{39}$ com os restos circulados.



Fonte: Produzido pelo autor

Agora os restos são 2, 20, 5, 11, 32 e 8, e também pertencem ao conjunto $\mathbb{Z}_{39}^{\times}$. *Eles forma a classe lateral esquerdo (ou direito) de* H *em* $\mathbb{Z}_{39}^{\times}$ *contendo* 2. *Isto é*

$$\begin{aligned} 2 \odot_{39} H &= \{2 \odot_{39} h \mid h \in H\} \\ &= \{2 \odot_{39} 1, \quad 2 \odot_{39} 10, \quad 2 \odot_{39} 22, \quad 2 \odot_{39} 25, \quad 2 \odot_{39} 16, \quad 2 \odot_{39} 4\} \\ &= \{2,\ 20,\ 5,\ 11,\ 32,\ 8\} \end{aligned}$$

A divisão $\dfrac{2}{39}$ *nos dá o decimal* $0{,}\overline{051282}$ *(ver Tabela 11).*

Resto do subgrupo	2	20	5	11	32	8
O digito do período	0	5	1	2	8	2

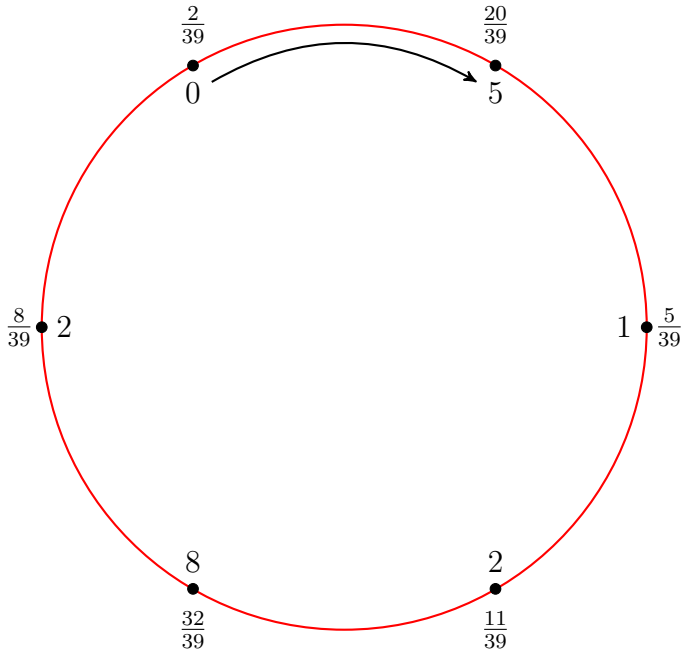
Tabela 11 – Restos do subgrupo na divisão $\frac{2}{39}$ e os dígitos que eles produzem

O comprimento do período é novamente 6. Olhando para a Tabela 11, fica claro que se tomarmos, alternadamente, como dividendo os números 20, 5, 11, 32 e 8 diferentes de 2 em nosso subgrupo, a expansão decimal deve sempre se repetir ciclicamente a expansão $\dfrac{2}{39} = 0{,}\overline{051282}$. *Isto é*

$$\begin{array}{ccccccccccccc} 0{,}\overline{051282} & \to & 0{,}\overline{512820} & \to & 0{,}\overline{128205} & \to & 0{,}\overline{282051} & \to & 0{,}\overline{820512} & \to & 0{,}\overline{205128} & \to & 0{,}\overline{051282} \\ \frac{2}{39} & \to & \frac{20}{39} & \to & \frac{5}{39} & \to & \frac{11}{39} & \to & \frac{32}{39} & \to & \frac{8}{39} & \to & \frac{2}{39} \end{array}$$

Isso também pode ser ilustrado por um círculo, veja a Figura 5 .

Figura 5 – A divisão prolongada de $\frac{2}{39}$.



Fonte: Produzido pelo autor

- *Da formas análogas, temos as outras 2 classes laterais:*

$$\begin{aligned} 7 \odot_{39} H &= \{7 \odot_{39} h \mid h \in H\} \\ &= \{7 \odot_{39} 1, \quad 7 \odot_{39} 10, \quad 7 \odot_{39} 22, \quad 7 \odot_{39} 25, \quad 7 \odot_{39} 16, \quad 7 \odot_{39} 4\} \\ &= \{7,\ 31,\ 37,\ 19,\ 34,\ 28\} \end{aligned}$$

que corresponde a divisão $\dfrac{7}{39} = 0{,}\overline{179487}$. *E logo a representação cíclica*

$$\begin{array}{ccccccccccccc} 0{,}\overline{179487} & \to & 0{,}\overline{794871} & \to & 0{,}\overline{948717} & \to & 0{,}\overline{487179} & \to & 0{,}\overline{871794} & \to & 0{,}\overline{717948} & \to & 0{,}\overline{179487} \\ \frac{7}{39} & \to & \frac{31}{39} & \to & \frac{37}{39} & \to & \frac{19}{39} & \to & \frac{34}{39} & \to & \frac{28}{39} & \to & \frac{7}{39} \end{array}$$

- *A última classe lateral é*

$$\begin{aligned} 14 \odot_{39} H &= \{14 \odot_{39} h \mid h \in H\} \\ &= \{14 \odot_{39} 1, \quad 14 \odot_{39} 10, \quad 14 \odot_{39} 22, \quad 14 \odot_{39} 25, \quad 14 \odot_{39} 16, \quad 14 \odot_{39} 4\} \\ &= \{14,\ 23,\ 35,\ 38,\ 29,\ 17\} \end{aligned}$$

que corresponde a divisão $\dfrac{14}{39} = 0{,}\overline{358974}$. *E logo a representação cíclica*

$$\begin{array}{ccccccccccccc} 0{,}\overline{358974} & \to & 0{,}\overline{589743} & \to & 0{,}\overline{897435} & \to & 0{,}\overline{974358} & \to & 0{,}\overline{743589} & \to & 0{,}\overline{435897} & \to & 0{,}\overline{358974} \\ \frac{14}{39} & \to & \frac{23}{39} & \to & \frac{35}{39} & \to & \frac{38}{39} & \to & \frac{29}{39} & \to & \frac{17}{39} & \to & \frac{14}{39} \end{array}$$

- *Temos o Grupo Quociente*

$$\mathbb{Z}_{39}^{\times}/H = \{H,\ 2 \odot_{39} H,\ 7 \odot_{39} H,\ 14 \odot_{39} H\}.$$

Vamos formar a Tabela de Cayley:

	H	$2 \odot_{39} H$	$7 \odot_{39} H$	$14 \odot_{39} H$
H	H	$2 \odot_{39} H$	$7 \odot_{39} H$	$14 \odot_{39} H$
$2 \odot_{39} H$	$2 \odot_{39} H$	H	$14 \odot_{39} H$	$7 \odot_{39} H$
$7 \odot_{39} H$	$7 \odot_{39} H$	$14 \odot_{39} H$	H	$2 \odot_{39} H$
$14 \odot_{39} H$	$14 \odot_{39} H$	$7 \odot_{39} H$	$2 \odot_{39} H$	H

Tabela 12 – O grupo quociente $\mathbb{Z}_{39}^{\times}/H$

4 Proposta de Atividades para o Ensino Médio

Segue algumas ilustrações de como fazer a aplicação em sala de aula para que o aluno perceba que ao fixar o denominador e mudar os numeradores encontraremos uma permutação cíclica existente na divisão sem que saiba as definições da mesma e ainda encontrar o período das dízimas sem fazer as contas,apenas observando o que ocorre nos ciclos dados.

Observando as dízimas periódicas

Conteúdo
Números decimais e dízimas periódicas.

Objetivos

- Proporcionar ao aluno uma aula mais prazerosa sobre os números decimais.
- Recorrer aos ciclos para observar o que acontece com a parte periódica.
- Incentivar a pesquisa e observação dos alunos,aguçando o interesse pela disciplina.

Anos Ensino fundamental e médio.

Tempo estimado Três aulas.

Duração: 3 aulas de 50 minutos

Desenvolvimento

1ª etapa

Entrega do material da apostila aos alunos para apreciação.

Sondagem: Pedir para que eles observem os círculos dados e encontre uma associação com as frações dadas.

Organização da turma:

A organização pode ser feita em grupos de no máximo 5 estudantes.

2ª etapa

Proponha cálculos das divisões das frações dadas e persista na observação dos círculos.

Adaptação: Se, nessa atividade, o educador notar que a turma está com dificuldades de perceber a regularidade e generalizar o procedimento adotado, pode levar um dos círculos ao quadro e começar as associações.

3ª etapa

Pedir para os grupos completarem as lacunas sem o uso de cálculos e apenas observando os círculos dados. E criar os outros ciclos sugeridos da tabela citada no material.

Encadeamento das etapas: a progressão do desafio continua aqui. Com a atividade proposta, a classe pode avançar mais um pouco e estender o conhecimento para outras frações.

Avaliação

Proponha outras frações que possam ser resolvidas com o que sabem agora sobre essa repetição dos números. E assim o professor consegue perceber a assimilação do conteúdo para avaliar individualmente cada aluno dos grupos.

Atividade :

- Fixa $b \in \mathbb{N}$ tal que $\text{MDC}(b, 10) = 1$.
  Ilustramos com por exemplo seja $b = 7$ ou $b = 21$.

- Peça os alunos para determine a quantidades de a's tal a fração $\frac{a}{b}$ é irredutível. Esta quantidade é $\varphi(b)$. (O professor não precisa falar nada sobre a função fi de Euler para os alunos.)

  Com $b = 7$, os valores de a são 1, 2, 3, 4, 5, 6. Portanto $\varphi(7) = 6$.

  Com $b = 21$, os valores de a são 1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20. Portanto $\varphi(21) = 12$.

- Agora peça para escreve a fração $\frac{a}{b}$ na forma decimal (sem usar a calculadora), começando com $\frac{1}{b}$. E determine o período $\lambda(b)$.

- Deduzir que $\lambda(b)$ divide $\varphi(b)$.

- Se o período $\lambda(b) = \varphi(b)$, (que é o caso quando $b = 7$) na expansão decimal, o aluno deve verificar que outras escolhas do numerador a também fornece uma repetição cíclica do resultado de $\frac{1}{b}$.

  Por exemplo $\frac{1}{7} = 0{,}\overline{142857}$ e $\frac{2}{7} = 0{,}\overline{285714}$, $\frac{3}{7} = 0{,}\overline{428571}, \cdots$
  Agora complete as lacunas abaixo observando o ciclo dado acima.

$$\tfrac{1}{7} = \boxed{}$$

$$\tfrac{3}{7} = \boxed{}$$

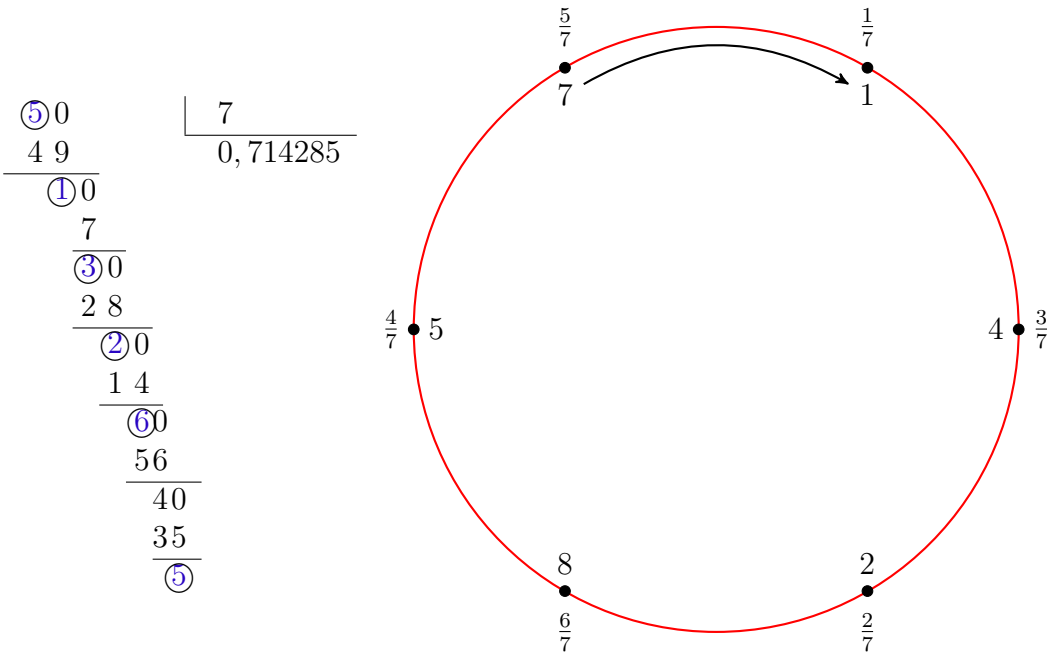
$$\tfrac{2}{7} = \boxed{}$$

$$\tfrac{6}{7} = \boxed{}$$

$$\tfrac{4}{7} = \boxed{}$$

- Faça uma tabela ou um gráfico para ilustrar. Fizemos o gráfico de $\frac{1}{7}$ abaixo.

Figura 6 – O relógio decimal para o denominador 7.



Fonte: Produzido pelo autor

- Se o período $\lambda(b) < \varphi(b)$, então $\dfrac{\varphi(b)}{\lambda(b)}$ daria o número de classes laterais em grupo multiplicativo $\mathbb{Z}_b^\times$.
  Por exemplo quando $b = 21$, temos $\dfrac{\varphi(21)}{\lambda(21)} = \dfrac{12}{6} = 2$ classes laterias.
  Escolhe um representante a' de cada classe lateral e faça as divisões $\dfrac{a'}{b}$. Elabore tabelas, gráficos ou outras ilustrações para obter uma apresentação compacta para todas as divisões $\dfrac{a}{b}$.

- Explique por que o comprimento do período da divisão $\dfrac{a}{b}$ não depende do numerador a.

- Mostre que b sendo primo não garante o comprimento máximo $b-1$ do período na divisão $\dfrac{a}{b}$.

- Encontre todos os primos $p < 50$ que geram o comprimento máximo $p-1$ do período pelo divisões $\dfrac{1}{p}$.

- É possível obter a comprimento máximo do período pela divisão $\dfrac{a}{b}$ se b for um número composto? Examine e explique.

Conclusão

A concretização dessa dissertação alcançou,como um dos objetivos almejados,o desenvolvimento de uma sequência didática que contribuísse na significação e compreensão dos conteúdos expostos nessa dissertação. Iniciar com o estudo das representações decimais nos possibilitou um melhor embasamento teórico para demonstrar o que propõe o trabalho: observar o posicionamento dos algarismos da parte periódica de uma dízima periódica simples.

No decorrer do processo de pesquisa surgiu a necessidade de criação de um material de apoio para aplicação em sala de aula visando a melhora do processo de ensino-aprendizagem dos alunos do Ensino Fundamental e Médio. A partir daí foi criada uma sequencia didática para ser disponibilizada para os professores que se interessarem em aplicar.

Espera-se que com a utilização desse material os alunos tenham uma melhor exemplificação e compreensão do posicionamento dos algarismos da parte periódica de uma dízima periódica simples visto que as demonstrações formais apresentadas no decorrer desse trabalho são muito complexas para o entendimento desses alunos.

É papel do professor buscar alternativas para melhorar o entendimento e aguçar o interesse dos seus alunos.

Referências

1 José Plinio de Oliveira Santos, **Introdução à Teoria dos Números** Coleção Matemática Universitária, 1998.

2 César Polcino Milies & Sônia Pitta Coelho, **Números - Uma Introdução à Matemática** EDUSP, 2001.

3 Duncan Samson & Peter Breetzke. **The Beauty of Cyclic Numbers** Disponível em https://mail.google.com/mail/u/0/#sent/FMfcgxwLsmdtqCppwndppFgqxVnjpQCL?projector=1&me Acessado em 03/03/2021.

4 Lawrence Brenton **Remainder Wheels and Group Theory** Disponivel em:https://mail.google.com/mail/u/0/#sent/FMfcgxwLsmdtqCpppCMdTKdwvkXrBHQg?projector= Acessado em 03/03/2021

5 A REPRESENTAÇÃO DECIMAL DOS REAIS http://mat.ufrgs.br/ vclotilde/disciplinas/html/decimais-web/decimais_texto_Representacao_decimal_reais_tarefa1.htm

6 A REPRESENTAÇÃO DECIMAL DOS REAIS http://mat.ufrgs.br/ vclotilde/disciplinas/html/decimais-web/decimais_texto_Representacao_decimal_reais_tarefa1.htm

7 CERRI, Cristina. **D**esvendando os Números Reais (pdf). Mini-curso, Bienal de Matemática, 2006. Disponível em: www.mat.ufg.br/bienal/2006/mini/cristina.cerri.pdf

8 PENTEADO, Cristina **.**Dissertação de Mestrado em educação Matemática. PUC-SP, 2004. Disponível em: http://www.sapientia.pucsp.br//tde_busca/arquivo.php?codArquivo=4687

9 MOREIRA, C. G. T. A. **Frações Contínuas, Representações de Números e Aproximações Diofantinas.** Disponível em: https://www.sbm.org.br/docs/coloquios/SE-1.06.pdf.

10 MOREIRA, C. G. T. A. **Teoria dos Números (Frações Contínuas) - Nível 3.** Disponível em: https://www.youtube.com/watch?v=0utc8PgixFo & t=1486s.

11 W E. Weisstein **Repeating Decimal, from MathWorld** Disponivel em http://mathworld.wolfram.com/RepeatingDecimal.html

12 OLDS, C. D.; **Continued Fractions.** California: Random House and The L. W. Singer Company, 1963.