

**UNIVERSIDADE FEDERAL DO AMAZONAS**

**DIEGO CARVALHO SOARES**

**FRAÇÕES DECIMAIS**

**MANAUS – AM**

**2020**

### Ficha Catalográfica

Ficha catalográfica elaborada automaticamente de acordo com os dados fornecidos pelo(a) autor(a).

S676f Soares, Diego Carvalho  
Frações decimais / Diego Carvalho Soares . 2020  
24 f.: 31 cm.

Orientador: Jorge Fernandes de Lima Neto  
TCC de Graduação (Matemática) - Universidade Federal do Amazonas.

1. Parte inteira. 2. Mantissa. 3. Número racional. 4. Período. I. Lima Neto, Jorge Fernandes de. II. Universidade Federal do Amazonas III. Título

DIEGO CARVALHO SOARES

FRAÇÕES DECIMAIS

Trabalho de conclusão de curso II  
apresentado à coordenação do curso  
de Graduação em Matemática  
Bacharelado da Universidade Federal  
do Amazonas

Aprovada em: \_\_\_/\_\_\_/\_\_\_\_\_.

BANCA EXAMINADORA

---

Prof. Dr. Jorge Fernandes de Lima Neto (Orientador)  
Universidade Federal do Amazonas (UFAM)

---

Prof. Dr. Germán Benitez Monsalve  
Universidade Federal do Amazonas (UFAM)

---

Prof. Dr. Stefan Josef Ehbauer  
Universidade Federal do Amazonas (UFAM)

## RESUMO

Este trabalho foi baseado no artigo do professor Alfredo Wagner Martins Pinto [1]. Seja  $x$  um número real, existem únicos  $[x]$  inteiro e  $0 \leq \{x\} < 1$  real tal que  $x = [x] + \{x\}$ , onde  $[x]$  é a parte inteira de  $x$  e  $\{x\}$  mantissa de  $x$ . A partir dessa informação, pode-se desenvolver a representação decimal desse número real, que é o primeiro objetivo deste trabalho. A mantissa pode ser escrita como uma série, tal que se um número é racional a mantissa desse número real é periódica. Logo em seguida, será necessário conhecimento da função  $\phi$  de Euler. Através de manipulações algébricas e conceitos analíticos, prossegue que todo número racional é periódico. Daí a necessidade de determinar o tamanho do período desse número racional, o segundo objetivo do trabalho. Ou seja, iremos determinar quantos dígitos tem o período de um número racional não inteiro. Isso nos dirá, por exemplo, por que o período de  $\frac{5}{7} = 0, \overline{714285}$  tem seis dígitos. Através de Teoria dos grupos, foi tentado determinar uma forma menos cansativa de encontrar o tamanho desse período. E por fim, encontrada uma melhor estimativa para o segundo objetivo do trabalho.

. A mantissa pode ser escrita como uma série, tal que se um número é racional a mantissa desse número real é periódica. Logo em seguida, será necessário conhecimento da função  $\phi$  de Euler.

**Palavras-chave:** Parte inteira; Mantissa; número racional; período.

## SUMÁRIO

|  |    |
|--|----|
| 1 INTRODUÇÃO .....   | 6  |
| 2 CONCEITOS PRELIMINARES .....                                 | 8  |
| 2.1 ALGUNS CONCEITOS DE SÉRIES E SEQUÊNCIAS .....              | 8  |
| 2.2 ANÉIS .....  | 8  |
| 2.3 GRUPOS .....   | 9  |
| 2.4 CONGRUÊNCIAS .....   | 9  |
| 2.5 RELAÇÕES DE EQUIVALÊNCIA .....                             | 10 |
| 2.6 CLASSES DE EQUIVALÊNCIAS .....                             | 10 |
| 2.7 OPERAÇÕES EM $\mathbb{Z}_n$ .....                          | 11 |
| 2.8 SUBGRUPOS .....  | 11 |
| 2.9 A FUNÇÃO $\phi$ .....                                      | 12 |
| 3 PARTE INTEIRA E MANTISSA DE UM NÚMERO REAL .....             | 14 |
| 4 REPRESENTAÇÃO DECIMAL .....                                  | 15 |
| 4.1 REPRESENTAÇÃO DA MANTISSA E PARTE INTEIRA COMO SÉRIE ..... | 17 |
| 5 REPRESENTAÇÃO PERIÓDICA .....                                | 18 |
| 6 TAMANHO DO PERÍODO .....                                     | 21 |
| 7 CONSIDERAÇÕES FINAIS .....                                   | 24 |
| REFERÊNCIAS .....  | 25 |

## 1 INTRODUÇÃO

Simon Stevin foi a figura principal para a história da matemática, e se destaca com as contribuições para os números decimais. E a partir de suas contribuições, surgiu a ideia de frações decimais. Sobre as frações decimais, John de Seville, trabalhando com as raízes, foi o pioneiro na história das frações decimais. Na época, François Viète recomendou o uso de frações decimais em vez de frações sexagesimais.

A ideia de frações decimais faz sua primeira aparição em métodos de aproximação às raízes quadradas de números. Segundo Cajori (2007, apud Jucá, 2008, p. 26).

Apesar do trabalho de Seville com as raízes quadradas, foi o francês François Vieté (1540 - 1603) quem fez a recomendação favorecendo o uso de frações decimais em lugar das frações sexagesimais usadas na época. (BOYER, 1996).

Simon Stevin (1548 – 1620) deve a sua popularização ao uso do sistema decimal de frações, o que veio a viabilizar o uso divisionário das moedas, pesos e medidas em geral. Segundo Jucá (2008) foi o primeiro a explicar o sistema com frações decimais de forma mais completa, pois ele queria ensinar como efetuar as computações com mais facilidade por meio de inteiros sem frações.

A partir das frações decimais, podemos estender este assunto a fim de determinar a quantidade de dígitos de um período de um número racional, que é o objetivo principal deste trabalho, e que frações de números inteiros são periódicas. Para isso, é preciso ter conhecimentos de conceitos básicos de teoria dos grupos, Análise, Séries convergentes, congruências, classes de equivalência, entre outros.

Primeiro mostraremos que todo número real  $x$  pode ser escrito como um número inteiro somado com um número no intervalo  $[0,1)$ , ou seja  $x = [x] + \{x\}$ , onde  $[x]$  é a parte inteira de  $x$  e  $\{x\} \in [0,1)$  é chamada mantissa de  $x$ . A mantissa pode ser escrita como uma série tal que, se um número é racional a mantissa desse número real é periódica.

Trabalhando com o conjunto  $\mathbb{Z}_n$ , que é um anel das classes de equivalência módulo  $n$ , ocorrerá que  $\mathbb{Z}_n^*$  o conjunto das classes dos invertíveis módulo  $n$ , obedece as condições de grupo. Estudaremos o conjunto  $\mathbb{Z}_n^*$ , e veremos que a sua cardinalidade, ou seja, sua quantidade de elementos, trará uma grande ajuda para o

propósito deste trabalho. Logo em seguida, será necessário conhecimento da função  $\phi$  de Euler e suas respectivas propriedades.

Nosso principal teorema é:

Seja um número racional  $m = \frac{p}{q}$ , com  $0 < p < q$ ,  $\text{mdc}(p, q) = 1$  e  $\text{mdc}(q, 10) = 1$ . Então  $m$  é um número periódico (dízima periódica) de tamanho  $k = \text{ord}_q 10$ .

Observe que estamos excluindo as frações decimais irredutíveis  $\frac{p}{q}$  com  $\text{mdc}(q, 10) = 1$ , pois se  $q = 2^a 5^b q_1$ , onde  $\text{mdc}(q_1, 10) = 1$ , teremos  $\frac{p}{q} = \frac{1}{10^{a+b}} \frac{2^a 5^b p}{q_1}$ ; como multiplicar por  $\frac{1}{10^{a+b}}$  só acrescenta “zeros após a vírgula” e não altera outros dígitos, basta analisar a fração  $\frac{2^a 5^b p}{q_1}$ , onde vale:  $\text{mdc}(q_1, 10) = 1$ .

Então, com o estudo da função  $\phi$  de Euler, descobriremos que é possível determinar o valor desse  $k$ , pois  $k = \text{ord}_n 10$  é divisor de  $\phi(q)$ . Ou seja,  $k$  é um dos divisores de  $\phi(q)$ .

## 2 CONCEITOS PRELIMINARES

### 2.1 ALGUNS CONCEITOS DE SÉRIES E SEQUÊNCIAS

A série de números reais  $\sum_{k=0}^{\infty} ar^k$ , com  $r \neq 0$ ,  $a \neq 0$  é chamada série geométrica. O número  $r$  é chamado razão. Sabemos que uma série geométrica converge se  $|r| < 1$ .

Se  $S_k = a + ar^2 + \dots + ar^k$ ,  $k \geq 0$ , são as somas parciais da série  $\sum_{k=0}^n a_k$ , o cálculo nos diz que

$$\sum_{k=0}^{\infty} ar^k = \lim_{n \rightarrow \infty} S_k = \frac{a}{1-r}$$

Uma série  $\sum_{k=0}^n a_k$  é absolutamente convergente se  $\sum_{k=0}^n |a_k|$  for convergente.

Uma sequência  $\{a_k\}$  é dita monótona crescente se  $a_k \leq a_{k+1}$  para todo  $k$  pertencente aos naturais, e se a sequência  $\{a_k\}$  tiver  $a_k \geq a_{k+1}$  com  $k$  natural é dita monótona decrescente. Além disso, a Análise Matemática nos diz que toda sequência monótona limitada é convergente.

Observe que a sequência  $S_k = \frac{a_1}{10} + \frac{a_2}{100} + \dots + \frac{a_k}{10^k}$ , com  $a_k \in \{0, 1, \dots, 9\}$  é monótona e limitada, pois  $S_k \geq S_{k+1}$  e

$$S_k = \frac{a_1}{10} + \frac{a_2}{100} + \dots + \frac{a_k}{10^k} < \frac{9}{10} + \dots + \frac{9}{10^k} = 1 - \frac{1}{10^k} < 1$$

Ou seja,  $S_k < 1$

Portanto, uma sequência monótona e limitada é uma sequência convergente, e esta sequência converge para um número real.

### 2.2 ANÉIS

Um anel é uma estrutura algébrica que consiste num conjunto  $A$  com um elemento  $0$  e duas operações binárias  $+$  e  $*$  que satisfazem as seguintes condições:

Associatividade da  $+$ , para todo  $a, b, c \in A$ :  $(a + b) + c = a + (b + c)$ ;

Existência de elemento neutro ( $0$ ) em relação a  $+$ , para todo  $a \in A$ :  $a + 0 = 0 + a = a$ ;

Existência de simétrico em relação a  $+$ , para todo  $a \in A$  existe um  $b \in A$ :  $a + b = 0$ ;

Comutatividade da  $+$ , para todo  $a, b \in A$ :  $a + b = b + a$ ;

Associatividade de  $*$ : para todo  $a, b, c \in A$ :  $(a*b)*c = a*(b*c)$ ;

Distributividade de  $*$  em relação a  $+$ : para todo  $a, b, c \in A$ :  $a*(b+c) = a*b + a*c$ .

### 2.3 GRUPOS

**Definição 2.1:** Seja  $G$  um conjunto e  $*$  uma operação binária sobre  $G$ .

O par ordenado  $(G,*)$  é um grupo se satisfizer as propriedades:

Associatividade: Seja  $a, b, c \in G$ , tal que:  $(a*b)*c = a*(b*c)$ ;

Existência do elemento neutro: Existe um  $e$  tal que:  $e*a = a*e = a$  ;

Elemento simétrico: para qualquer elemento  $a$  em  $G$  existe outro elemento  $s$  tal que:  $a*s = s*a = e$ , onde  $e$  é o elemento neutro.

**Definição 2.2:** Um grupo multiplicativo  $G$  será chamado grupo cíclico se, para algum elemento  $a \in G$ , se verificar a igualdade  $G = \langle a \rangle$ , onde  $\langle a \rangle$  é o conjunto das potências de  $a$ . Nessas condições, o elemento  $a$  é chamado gerador do grupo  $G$ .

### 2.4 CONGRUÊNCIAS

**Definição 2.3:** Sejam  $a, b$  inteiros quaisquer e  $n$  um número inteiro estritamente positivo. Diz-se que  $a$  é cômruo a  $b$  módulo  $n$  se  $n \mid (a - b)$ , isto é, se  $a - b = n.q$  para um conveniente inteiro  $q$ . Para indicar que  $a$  é cômruo a  $b$ , módulo  $n$ , usa-se a notação:

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

Seguem as propriedades básicas da congruência de inteiros:

- ( i )  $a \equiv a \pmod{n}$  (**reflexividade**);
- ( ii )  $a \equiv b \pmod{n}$ , então  $b \equiv a \pmod{n}$  (**simetria**);
- ( iii )  $a \equiv b \pmod{n}$  e  $b \equiv c \pmod{n}$ , então  $a \equiv c \pmod{n}$  (**transitividade**);
- ( iv )  $a \equiv b \pmod{n}$  e  $0 \leq b < n$ , então  $b$  é o resto da divisão euclidiana de  $a$  por  $n$ ;
- ( v )  $a \equiv b \pmod{n}$  se, e somente se  $a$  e  $b$  dão o mesmo resto na divisão euclidiana por  $n$ ;
- ( vi )  $a \equiv b \pmod{n}$  se e somente se  $a \pm c \equiv b \pm c \pmod{n}$ ;
- ( vii )  $a \equiv b \pmod{n}$  e  $c \equiv d \pmod{n}$ , então  $a + c \equiv b + d \pmod{n}$ ;
- ( viii )  $a \equiv b \pmod{n}$ , então  $ac \equiv bc \pmod{n}$ ;
- ( ix )  $a \equiv b \pmod{n}$  e  $c \equiv d \pmod{n}$ , então  $ac \equiv bd \pmod{n}$ ;
- ( x ) Se  $ca \equiv cb \pmod{n}$  e  $\text{mdc}(c,n) = d > 0$ , então  $a \equiv b \pmod{(n/d)}$ .

## 2.5 RELAÇÕES DE EQUIVALÊNCIA

**Definição 2.4:** Uma relação  $R$  sobre um conjunto  $E$  não vazio é chamada relação de equivalência sobre  $E$  se, e somente se,  $R$  é reflexiva, simétrica e transitiva. Ou seja,  $R$  deve cumprir, respectivamente, as seguintes propriedades:

- ( i ) Se  $x$  pertence a  $E$ , então  $xRx$ ;
- ( ii ) Se  $x, y$  pertencem a  $E$  e  $xRy$ , então  $yRx$ ;
- ( iii ) Se  $x, y, z$  pertencem a  $E$  e  $xRy$  e  $yRx$ , então  $xRz$ .

Exemplo:

A relação de congruência módulo  $n$  (com  $n$  inteiro e maior que 1) sobre  $\mathbb{Z}$ , é uma relação de equivalência, pois:

- ( i ) Para todo  $x \in \mathbb{Z}$  temos  $x \equiv x \pmod{n}$ ;
- ( ii ) Para todo  $x, y \in \mathbb{Z}$ ,  $x \equiv y \pmod{n}$  temos  $y \equiv x \pmod{n}$ ;
- ( iii ) Para todo  $x, y, z \in \mathbb{Z}$ ,  $x \equiv y \pmod{n}$  e  $y \equiv z \pmod{n}$  temos  $x \equiv z \pmod{n}$ ;

## 2.6 CLASSES DE EQUIVALÊNCIAS

**Definição 2.5:** Seja  $R$  uma relação de equivalência sobre  $E$ . Dado  $a$ , com  $a \in E$ , chama-se classe de equivalência determinada por  $a$ , módulo  $R$ , o subconjunto de  $E$  constituído pelos elementos  $x$  tais que  $xRa$ . Em símbolos:

$$\bar{a} = \{ x \in E ; xRa \}$$

Com  $a, n$  inteiros, com  $n > 1$ .

**Exemplo:**

O conjunto  $\bar{a} = \{ y \in E ; y \equiv a \pmod{n} \}$  é chamado de classes residuais módulo  $n$ .

De fato, seja  $n \in \mathbb{Z}$ ,  $\mathbb{Z}_n = \{ \bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1} \}$ .

Onde

$$\bar{0} = \{ y \in \mathbb{Z} ; y \equiv 0 \pmod{n} \}, \bar{1} = \{ y \in \mathbb{Z} ; y \equiv 1 \pmod{n} \},$$

$$\bar{2} = \{ y \in \mathbb{Z} ; y \equiv 2 \pmod{n} \}, \dots, \overline{n-1} = \{ y \in \mathbb{Z} ; y \equiv (n-1) \pmod{n} \}.$$

Assim por diante:

$$\bar{n} = \{ y \in \mathbb{Z} ; y \equiv n \pmod{n} \}, \overline{n+1} = \{ y \in \mathbb{Z} ; y \equiv 1 \pmod{n} \}, \dots$$

$$\overline{n+(n-1)} = \{ y \in \mathbb{Z} ; y \equiv (n-1) \pmod{n} \},$$

$$\text{Logo, } \bar{0} = \bar{n}, \bar{1} = \overline{n+1}, \dots, \overline{n-1} = \overline{n+(n-1)}.$$

Temos apenas  $n$  classes mod  $n$ .

## 2.7 OPERAÇÕES EM $\mathbb{Z}_n$

$\mathbb{Z}_n = \{\bar{0}, \dots, \overline{n-1}\}$ , onde  $\bar{0}, \dots, \overline{n-1}$  são os restos da divisão inteira de um  $t$  por um  $n$ , onde  $t \in \mathbb{Z}$  e  $n \in \mathbb{N}$ .

**Definição 2.6:** Dadas duas classes  $\bar{a}$  e  $\bar{b} \in \mathbb{Z}_n$ , chama-se soma  $\bar{a} + \bar{b}$  à classe  $\overline{a+b}$ .

Observe que essa operação soma está bem definida:

Seja  $\bar{a}, \bar{a}' \in \mathbb{Z}_n$ , tal que  $\bar{a} = \bar{a}'$ ,  $a \equiv a' \pmod{n}$ .

Seja  $\bar{b}, \bar{b}' \in \mathbb{Z}_n$ , tal que  $\bar{b} = \bar{b}'$ ,  $b \equiv b' \pmod{n}$ .

Pela propriedade (vii) de congruências:  $a + b \equiv a' + b' \pmod{n}$ . Logo, a operação está bem definida, ou seja:  $\bar{a} + \bar{b} = \overline{a+b}$ .

A operação soma satisfaz a associatividade, comutatividade, existência do elemento neutro e simétrico.

**Definição 2.7:** Dadas duas classes  $\bar{a}$  e  $\bar{b} \in \mathbb{Z}_n$ , chama-se produto  $\bar{a} \cdot \bar{b}$  a classe  $\overline{a \cdot b}$ .

A operação multiplicação está bem definida:

Seja  $\bar{a}, \bar{a}' \in \mathbb{Z}_n$ , tal que  $\bar{a} = \bar{a}'$ ,  $a \equiv a' \pmod{n}$ .

Seja  $\bar{b}, \bar{b}' \in \mathbb{Z}_n$ , tal que  $\bar{b} = \bar{b}'$ ,  $b \equiv b' \pmod{n}$ .

Pela propriedade (ix) de congruências:  $a \cdot b \equiv a' \cdot b' \pmod{n}$ . Logo, a operação está bem definida, ou seja:  $\bar{a} \cdot \bar{b} = \overline{a \cdot b}$ .

A operação multiplicação satisfaz a associatividade, comutatividade, existência do elemento neutro.

## 2.8 SUBGRUPOS

**Definição 2.8:** Seja  $(G, *)$  grupo e  $H$  um subconjunto não vazio de  $G$ .  $H$  é um subgrupo de  $G$  se  $H$  é fechado com a operação de  $G$  e é grupo.

**Notação:**  $H \leq G$  ( $H$  é subgrupo de  $G$ )

**Definição 2.9:** Dizemos que  $a$  é divisor de  $b$  se, e somente se existe  $c \in \mathbb{Z}$ ;  $b = a \cdot c$ . ou seja,  $a \mid b$ , diz-se que  $a$  divide  $b$ .

## 2.9 A FUNÇÃO $\phi$

**Definição 2.10:** Um conjunto  $A$  contido nos inteiros é um sistema completo de resíduos módulo  $n$  se  $A$  tem  $n$  elementos, e o conjunto dos restos das divisões dos elementos de  $A$  por  $n$  é  $\{0,1,2,\dots, n-1\}$  neste caso, dado  $k$  natural, existe único  $m \in A$  tal que  $m \equiv k \pmod{n}$ .

**Definição 2.11:** Um sistema reduzido de resíduos módulo  $n$  é um conjunto de  $\phi(n)$  inteiros,  $r_1, r_2, \dots, r_{\phi(n)}$ , tais que cada elemento deste conjunto é relativamente primo com  $n$ , e se  $i \neq j$  então  $r_i \not\equiv r_j \pmod{n}$ .

Exemplos:

$A = \{0,1,2,3,4,5,6,7\}$  é um sistema completo de resíduos módulo 8.

$B = \{1,3,5,7\}$  é um sistema reduzido de resíduos módulo 8.

**Teorema 2.12:** Sejam  $m, n \in \mathbb{Z}$ ,  $\text{mdc}(m,n) = 1$ ,  $\phi(m.n) = \phi(m) \phi(n)$

Demonstração:

Dispondo os números de 1 até  $mn$  da seguinte forma:

$$\begin{array}{l} 1, m + 1, 2m + 1, \dots, (n-1)m + 1 \\ 2, m + 2, 2m + 2, \dots, (n-1)m + 2 \\ \dots\dots\dots \\ m, 2m, 3m, \dots\dots\dots, (n-1)m + 3 \end{array}$$

Se na linha  $r$ , onde temos os termos  $r, m + r, 2m + r, \dots, (n-1)m + r$

Tivermos  $\text{mdc}(m,r) = d > 1$ , então nenhum termo nesta linha será primo com  $mn$ , uma vez que estes termos, sendo da forma  $km + r$ ,  $0 \leq k \leq n - 1$ , são todos divisíveis por  $d$  que é o máximo divisor comum de  $m$  e  $r$ . Logo, para encontrarmos os inteiros desta tabela que são primos com  $n$ , devemos olhar na linha  $r$  somente se  $\text{mdc}(m,r) = 1$ . Portanto temos  $\phi(m)$  linhas onde todos os elementos são primos com  $m$ .

Devemos procurar em cada uma dessas  $\phi(m)$  linhas quantos elementos são primos com  $n$ , uma vez que todos são primos com  $m$ . Como  $\text{mdc}(m,n) = 1$  os elementos  $r, m + r, 2m + r, \dots, (n-1)m + r$  formam um sistema completo de resíduos módulo  $n$ . Logo, cada uma destas linhas possui  $\phi(n)$  elementos primos com  $n$  e, portanto, como eles são primos com  $m$ , são primos com  $mn$ . Isto garante que  $\phi(m.n) = \phi(m) \phi(n)$ .

Exemplo:

Seja  $m = 2, n = 3 \Rightarrow \text{mdc}(2,3) = 1$ .

$\mathbb{Z}_2^* = \{\bar{a} \in \mathbb{Z}_2; \text{mdc}(a,2) = 1\}$ , então  $\mathbb{Z}_2^* = \{\bar{1}\}$ , logo  $|\mathbb{Z}_2^*| = \phi(2) = 1$ ,

$\mathbb{Z}_3^* = \{\bar{a} \in \mathbb{Z}_3; \text{mdc}(a,3) = 1\}$ , então  $\mathbb{Z}_3^* = \{\bar{1}, \bar{2}\}$ , logo  $|\mathbb{Z}_3^*| = \phi(3) = 2$ ,

$\mathbb{Z}_6^* = \{\bar{1}, \bar{5}\}$ , logo  $|\mathbb{Z}_6^*| = 2$ .

Portanto,  $\phi(2.3) = \phi(6) = \phi(2)\phi(3)$ .

Seja  $n = p_1^{r_1} \dots p_s^{r_s}$  decomposição em fatores primos. Se  $p$  é primo  $\phi(n) = p - 1 = p$

$(1 - \frac{1}{p})$  e  $\phi(p^r) = p^r - p^{r-1}$ .

Exemplos:

$\mathbb{Z}_3^* = \{\bar{a} \in \mathbb{Z}_3; \text{mdc}(a,3) = 1\}$ , então  $\mathbb{Z}_3^* = \{\bar{1}, \bar{2}\} \Rightarrow \phi(3) = 3 - 1 = 2$

$\mathbb{Z}_{11}^* = \{\bar{a} \in \mathbb{Z}_{11}; \text{mdc}(a,11) = 1\}$ , então  $\mathbb{Z}_{11}^* = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}, \bar{10}\}$

$\phi(11) = 11 - 1 = 10$ .

**Teorema 2.13:**  $\phi(p^r) = p^r - p^{r-1} = p^{r-1}(p - 1) = p^r \left(1 - \frac{1}{p}\right)$ .

Demonstração:

Pela definição de  $\phi(n)$ , sabemos que  $\phi(p^r)$  é o número de inteiros positivos não-superiores a  $p^r$  e relativamente primos com  $p^r$ . Mas os únicos números não-primos menores ou iguais a  $p^r$  são, em número  $p^{r-1}$ , logo, segue que  $\phi(p^r) = p^r - p^{r-1} = p^{r-1}(p - 1) = p^r \left(1 - \frac{1}{p}\right)$ .

$$\phi(n) = n \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_s}\right)$$

**Corolário 2.14:**  $\phi(n) = n \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_s}\right)$ . Considerando  $n = p_1^{r_1} \dots p_s^{r_s}$

decomposição em fatores primos.

Demonstração:

Utilizando o teorema anterior:

$$\phi(n) = (p_1^{r_1} - p_1^{r_1-1}) \dots (p_s^{r_s} - p_s^{r_s-1}) = p_1^{r_1-1}(p_1 - 1) \dots p_s^{r_s-1}(p_s - 1) =$$

$$p_1^{r_1} \left(1 - \frac{1}{p_1}\right) \dots p_s^{r_s} \left(1 - \frac{1}{p_s}\right) = p_1^{r_1-1} \dots p_s^{r_s-1} \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_s}\right) =$$

$$n \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_s}\right)$$

### 3 PARTE INTEIRA E MANTISSA DE UM NÚMERO REAL

**Princípio da Boa Ordenação:** Todo subconjunto não-vazio formado por números naturais possui um menor elemento.

**Notação:** (parte inteira de um número real  $x$ )

$$\lfloor x \rfloor = \max[(-\infty, x] \cap \mathbb{Z}]$$

Para entender melhor vejamos o que significa a interseção do conjunto  $(-\infty, x]$  com o conjunto dos inteiros  $\mathbb{Z}$ .

O maior elemento de  $(-\infty, x]$  é o próprio elemento  $x$ , mas a interseção com os inteiros, faz com que o maior elemento de  $(-\infty, x] \cap \mathbb{Z}$  seja sempre inteiro e menor ou igual a  $x$ , enfim,  $\max[(-\infty, x] \cap \mathbb{Z}]$ , quer dizer escolher o maior elemento inteiro menor ou igual a  $x$ .

**Proposição 3.1:** Seja  $x$  um número real, existem únicos  $\lfloor x \rfloor$  inteiro e  $0 \leq \{x\} < 1$  real tal que:

$$x = \lfloor x \rfloor + \{x\}$$

Onde  $\lfloor x \rfloor$  é a parte inteira de  $x$  e  $\{x\}$  será chamada mantissa de  $x$ .

Demonstração:

Consideremos o conjunto de números  $A = \{n \in \mathbb{Z}; x - n \geq 0\}$ ,  $A$  é limitado superiormente, pois  $\lim_{n \rightarrow \infty} x - n = -\infty$  e  $\lim_{n \rightarrow -\infty} x - n = +\infty$ .

Pelo princípio da Boa ordenação, o conjunto  $A$  possui um maior elemento que chamaremos  $\lfloor x \rfloor$ .

Seja  $\{x\} = x - \lfloor x \rfloor$ , então  $\{x\}$  é maior ou igual a zero, pois  $\lfloor x \rfloor \in A$ , além disso,  $\{x\} < 1$ , pois caso contrário:

$$\{x\} - 1 \geq 0 \text{ temos } x - \lfloor x \rfloor - 1 \geq 0 \text{ portanto } x - (\lfloor x \rfloor + 1) \geq 0$$

Neste caso teríamos o inteiro  $\lfloor x \rfloor + 1$  pertencendo a  $A$ , contrariando o fato de  $\lfloor x \rfloor$  ser o máximo de  $A$ . Contradição.

**Definição 3.2:** Para um  $n$  real, tal que  $n = \frac{p}{q}$ , com  $p, q$  inteiros, e  $q \neq 0$ , podemos usar a definição para obter a parte inteira e a mantissa.  $p = cq + r$ , com  $0 \leq r < q$ ,  $c$  quociente e  $r$  o resto da divisão.

$$\lfloor n \rfloor = \left\lfloor \frac{p}{q} \right\rfloor = c \quad \{ n \} = \left\{ \frac{p}{q} \right\} = \frac{r}{q}$$

$\frac{r}{q}$  sempre será menor que 1 e maior ou igual a zero, satisfazendo a definição de mantissa de  $n$ , e  $c$  pertencente aos inteiros, satisfazendo a definição de parte inteira de  $n$ .

**Exemplo:**  $n = \frac{p}{q} = \frac{73}{8}$ ,  $73 = 9 \cdot 8 + 1 \Rightarrow c = 9$  e  $\frac{r}{q} = \frac{1}{8}$

Dessa forma  $\left\lfloor \frac{73}{8} \right\rfloor = 9$  e  $\left\{ \frac{73}{8} \right\} = \frac{1}{8}$

**Corolário 3.3:** Se  $x \in \mathbb{Z}$ ,  $\{x\} = 0$  se, e somente se  $\lfloor x \rfloor = x$ .

Demonstração:

( $\Rightarrow$ ) Com  $x$  inteiro, se  $\{x\} = 0$ , pela proposição anterior.

$$x = \lfloor x \rfloor + \{x\} \text{ implica que } x = \lfloor x \rfloor + 0 \text{ logo } \lfloor x \rfloor = x.$$

( $\Leftarrow$ ) Com  $x$  inteiro, se  $\lfloor x \rfloor = x$ , novamente pela proposição, se  $x = \lfloor x \rfloor + \{x\}$  então  $x = \lfloor x \rfloor + 0$ ,  $\{x\} = 0$ .

Também vale  $\{x\} = 0$  se e somente se  $\lfloor x \rfloor = x$ ,  $x \in \mathbb{Z}$ .

Diretamente da proposição, pelo fato da parte inteira já pertencer aos inteiros.

**Corolário 3.4:** Sejam  $x, y \in \mathbb{Z}$ ,  $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor \leq \lfloor x \rfloor + \lfloor y \rfloor + 1$ .

Demonstração:

$$\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x \rfloor + \lfloor y \rfloor + \lfloor \{x\} + \{y\} \rfloor = \lfloor \lfloor x \rfloor + \lfloor y \rfloor + \{x\} + \{y\} \rfloor = \lfloor x + y \rfloor$$

Como  $\{x\} + \{y\} < 2$ ,  $\lfloor \{x\} + \{y\} \rfloor \leq 1$ , segue que:

$$\lfloor x + y \rfloor = \lfloor x \rfloor + \lfloor y \rfloor + \lfloor \{x\} + \{y\} \rfloor \leq \lfloor x \rfloor + \lfloor y \rfloor + 1.$$

Portanto,  $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor \leq \lfloor x \rfloor + \lfloor y \rfloor + 1$ .

#### 4 REPRESENTAÇÃO DECIMAL

Seja  $x$  real. Como vimos  $x = I + m$ , com  $I \in \mathbb{Z}$  e  $m \in [0, 1)$ . Deve-se obter a representação de  $m \in (0, 1)$ .

Seja  $m \in (0, 1)$

- $10m = [10m] + \{10m\} = a_1 + m_0$ ,  $a_1 = [10m]$  e  $m_0 = \{10m\}$
- $m = \frac{a_1}{10} + \frac{m_0}{10} = \frac{a_1}{10} + m_1$ , onde  $m_1 = \frac{m_0}{10}$  se  $m_0 = 0$  o processo é encerrado.

**Exemplo:**

Se  $x = 0.9$ ,  $m = 0.9 \Rightarrow 10m = 9$  Logo  $10m = [10m] + \{10m\} = a_1 + m_0 = 9 + 0$ .

$$m = \frac{[a_1]}{10} + \frac{\{m_0\}}{10} = \frac{[a_1]}{10} + \frac{0}{10} \text{ logo, } m_0 = 0.$$

O processo é encerrado,  $m = \frac{a_1}{10} \Rightarrow m = \frac{9}{10}$ .

Caso contrário:

$m = \frac{a_1}{10}$ , com  $0 \leq a_1 \leq 9$ , inteiro, pois  $0 < m \leq 1$ , pois  $\Rightarrow 0 < 10m < 10$ ,

então  $0 \leq [10m] \leq 9$ . Se não,  $m_1$  é diferente de zero.

Escrevemos  $100m_1 = [100m_1] + \{100m_1\} = a_2 + \{100m_1\}$ .

$$m_1 = \frac{a_2}{100} + \frac{\{m_1\}}{10} = \frac{a_2}{100} + m_2, m_2 = \frac{\{100m_1\}}{100} \text{ e } a_2 = [100m_1].$$

Observe que  $100m_1 = 10m_0$ , como  $0 < m_0 < 1$ , pelo mesmo argumento anterior,  $0 \leq a_2 \leq 9$ .

- $m = \frac{a_1}{10} + \frac{a_2}{100} + m_2$ , se  $m_2 = 0$  encerramos o processo.

**Exemplo:**

Se  $x = \frac{30}{24}$ ,  $x = \frac{24}{24} + \frac{6}{24}$  então,  $m = \frac{6}{24}$ . Logo,  $10m = \frac{60}{24} = \frac{48}{24} + \frac{12}{24}$ .

$$10m = [10m] + \{10m\} = a_1 + m_0 = 2 + \frac{1}{2}$$

$$m = \frac{[10m]}{10} + \frac{\{10m\}}{10} = \frac{2}{10} + \frac{1}{20}, \text{ logo } m_1 = \frac{m_0}{10} = \frac{1}{20}, \text{ como } m_0 \neq 0, \text{ o processo}$$

continua.

$$100m_1 = [100m_1] + \{100m_1\} = a_2 + m_1 = \frac{100}{20} = 5$$

$$m_1 = \frac{[100m_1]}{100} + \frac{\{100m_1\}}{100} = \frac{5}{100} + 0, \text{ com } m_2 = \frac{\{100m_1\}}{100} = 0.$$

Então processo é encerrado com  $m = \frac{a_1}{10} + \frac{a_2}{100} = \frac{2}{10} + \frac{5}{100}$ , caso contrário repetimos o processo novamente.

Podemos seguir com o processo indefinidamente, e para cada  $k$ :

$$m = \frac{a_1}{10} + \frac{a_2}{100} + \dots + \frac{a_k}{10^k} = + m_k, \quad a_k \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

$$m = \sum_{k=1}^{\infty} \frac{a_k}{10^k}, \quad \text{onde } m_k = \frac{\{10^k m_{k-1}\}}{10^k}, \quad \text{com } a_k = \lfloor 10^k m_{k-1} \rfloor$$

#### 4.1 REPRESENTAÇÃO DA MANTISSA E PARTE INTEIRA COMO SÉRIE

Seja,  $m = (0, a_1 a_2 \dots a_k, \dots) = \sum_{k=1}^{\infty} \frac{a_k}{10^k}$

Fazendo um processo análogo como no início do capítulo:

$$10m = a_1 + \sum_{k=1}^{\infty} \frac{a_{k+1}}{10^k} = a_1 + (0, a_2 a_3 \dots) = a_1 + \frac{a_2}{10} + \frac{a_3}{100} + \dots$$

Segue que  $\{10m\} = \sum_{k=1}^{\infty} \frac{a_{k+1}}{10^k} = (0, a_2 a_3 \dots)$ .

Então,  $m_1 = \frac{\{10m\}}{10} = \sum_{k=1}^{\infty} \frac{a_{k+1}}{10^{k+1}} = \sum_{k=2}^{\infty} \frac{a_k}{10^k} = (0, 0 a_2 a_3 \dots)$

Prosseguindo,  $10^2 m_1 = \sum_{k=2}^{\infty} \frac{a_k}{10^{k-2}} = a_2 + \frac{a_3}{10} + \dots = a_2 + (0, a_3 a_4 \dots)$

$$\{10^2 m_1\} = \sum_{k=1}^{\infty} \frac{a_{k+2}}{10^k}$$

$$m_2 = \frac{\{10^2 m_1\}}{10^2} = \sum_{k=1}^{\infty} \frac{a_{k+2}}{10^{k+2}} = \sum_{k=3}^{\infty} \frac{a_k}{10^k} = (0, 00 a_3 a_4 \dots)$$

O processo se repete até:

$$m_j = \frac{\{10^j m_{j-1}\}}{10^j} = \sum_{k=1}^{\infty} \frac{a_{k+j}}{10^{k+j}} = \sum_{k=j+1}^{\infty} \frac{a_k}{10^k} = (0, 00 \dots 0 a_j a_{j+1} a_{j+2} \dots)$$

Chegamos a conclusão que:

$$10^{j+1} m_j = \sum_{k=1}^{\infty} \frac{a_{k+j}}{10^{k-1}} = a_{j+1} + (0, a_{j+2} a_{j+3} \dots)$$

$$\lfloor 10^{j+1} m_j \rfloor = a_{j+1} \quad \text{e} \quad \{10^{j+1} m_j\} = (0, a_{j+2} a_{j+3} \dots)$$

Algumas informações obtidas nesse processo serão de grande utilidade para demonstrações seguintes.

## 5 REPRESENTAÇÃO PERIÓDICA

No capítulo anterior vimos que  $m$  pode ser representado da seguinte forma:

$$m = \sum_{k=1}^{\infty} \frac{a_k}{10^k} = (0, a_1 a_2 \dots)$$

Agora veremos como é a representação periódica de  $m$ , como exemplo, suponha  $m = (0,121212\dots)$ , percebemos que esse número tem representação infinita e “12” repetirá infinitamente para a sua representação. Isso é chamado de período da representação de  $m$ .

**Definição 5.1:** Seja  $m = (0, a_1 a_2 \dots)$  a representação infinita de  $m \in (0,1]$ . Dizemos que a representação é periódica, se existirem  $k_0 \geq 1$  e  $t \geq 1$  inteiros tal que  $a_{k+t} = a_k$  para todo  $k \geq k_0$ .

$$m = (0, a_1 \dots a_{k_0-1} a_{k_0} \dots a_{k_0+t-1} a_{k_0} \dots a_{k_0+t-1} a_{k_0} \dots a_{k_0+t-1} a_{k_0} \dots a_{k_0+t-1} \dots).$$

O período da representação de  $m$  é denotado por  $P$ .

$P = a_{k_0} \dots a_{k_0+t-1}$  é chamado um período da representação.

$t$  é o tamanho desse período.

Assim,  $m = (0, a_1 \dots a_{k_0-1} PPP\dots)$ .

Podemos escrever  $m = (0, a_1 \dots a_{k_0-1} \overline{a_{k_0} \dots a_{k_0+t-1}}) = (0, a_1 \dots a_{k_0-1} \bar{P})$ .

Exemplo:  $m = (0,1232323\dots)$ , temos que  $m = (0,1\overline{23})$ , ou seja,  $P = 23$ , com tamanho do período igual a 2.

**Definição 5.2:** Seja  $m = (0, a_1 a_2 \dots a_k)$ , com  $a_k \neq 0$ , com representação finita. Sua representação infinita é  $m = (0, a_1 a_2 \dots a_{k-1} (a_k - 1)999\dots)$ .

Exemplo: Se  $m = 0,25$ , sua representação finita é  $m = 0,24999\dots = 0,24\bar{9}$ .

**Definição 5.3:** Seja  $m$  periódico, Diremos que  $m$  é uma dízima periódica se uma das condições abaixo for satisfeita:

- O tamanho do período é maior que 1.
- Se o tamanho do período é igual a 1, então  $a_{k_0} < 9$ .

No segundo caso, se  $a_{k_0} = 9$ , pelo corolário anterior, teríamos que:

$$m = (0, a_1 \dots a_{k_0-2} (a_{k_0-1} - 1) a_{k_0} a_{k_0} a_{k_0} \dots)$$

O que teria a mesma representação de  $m = (0, a_1 \dots a_{k_0-1})$ , uma representação finita.

**Proposição 5.4:** Se  $m = (0, a_1 \dots a_{k_0-1} \overline{a_{k_0} \dots a_{k_0+t-1}})$  é periódico então  $m$  é racional.

Demonstração:

Fazendo  $10^{k_0-1}m = (0, a_1 \dots a_{k_0-1}) + (0, \overline{a_{k_0} \dots a_{k_0+t-1}})$ ,  $m$  é racional se, e somente se  $(0, \overline{a_{k_0} \dots a_{k_0+t-1}})$  for racional.

Considerando um caso ilustrativo  $(0, \overline{a_1 a_2 a_3})$  :

$$\text{Segue que } (0, \overline{a_1 a_2 a_3}) = \frac{a_1}{10} + \frac{a_2}{100} + \frac{a_3}{1000} + \frac{a_1}{10000} + \frac{a_2}{100000} + \frac{a_3}{1000000} +$$

... =

$$= \frac{a_1}{10} \left(1 + \frac{1}{100} + \frac{1}{100} + \dots\right) + \frac{a_2}{100} \left(1 + \frac{1}{100} + \frac{1}{100} + \dots\right) +$$

$$\frac{a_3}{1000} \left(1 + \frac{1}{100} + \frac{1}{100} + \dots\right)$$

Como  $\left(1 + \frac{1}{100} + \frac{1}{100} + \dots\right)$  representa a soma de uma série geométrica absolutamente convergente, a associatividade pode ser feita.

$$(0, \overline{a_1 a_2 a_3}) = \frac{a_1}{10} \left(1 + \frac{1}{10^3} + \frac{1}{10^6} + \dots\right) + \frac{a_2}{100} \left(1 + \frac{1}{10^3} + \frac{1}{10^6} + \dots\right)$$

$$+ \frac{a_3}{1000} \left(1 + \frac{1}{10^3} + \frac{1}{10^6} + \dots\right)$$

$$= \left(\frac{a_1}{10} + \frac{a_2}{100} + \frac{a_3}{1000}\right) \left(\frac{1}{1 - \frac{1}{10^3}}\right) = \left(\frac{a_1}{10} + \frac{a_2}{100} + \frac{a_3}{1000}\right) \left(\frac{10^3}{10^3 - 1}\right)$$

$$= \frac{(a_1 10^2 + a_2 10 + a_3)}{10^3 - 1}$$

$$\text{Então } (0, \overline{a_1 a_2 a_3}) = \frac{(a_1 10^2 + a_2 10 + a_3)}{10^3 - 1} = \frac{(a_1 10^2 + a_2 10 + a_3)}{999} = \frac{(a_1 a_2 a_3)}{999}.$$

No caso geral  $(0, \overline{a_1 a_2 \dots a_n}) = \frac{(a_1 a_2 \dots a_n)}{9 \dots 9}$  com  $n$  “noves”.

Portanto,  $m$  é racional.

**Exemplos:**

$$\frac{432}{999} = (0, \overline{432}) \quad \frac{43}{99} = (0, \overline{43})$$

**Proposição 5.5 :** Seja  $m = (0, a_1 a_2 \dots)$   $m$  é periódico se, e somente se existem inteiros  $1 \leq j < k$ , tais que  $\{ 10^j m_{j-1} \} = \{ 10^k m_{k-1} \}$ , onde  $m_{j-1}$  e  $m_{k-1}$  são obtidos de  $m$  na determinação de sua representação decimal.

Demonstração:

( $\Rightarrow$ ) Seja  $m = (0, a_1 \dots a_{k_0-1} \overline{P})$  periódico.

$$\{ 10^{k_0+t-1} m_{k_0+t-2} \} = (0, PPP\dots) \text{ e } \{ 10^{k_0+2t-1} m_{k_0+2t-2} \} = (0, PPP\dots).$$

( $\Leftarrow$ ) Supondo  $\{ 10^j m_{j-1} \} = \{ 10^k m_{k-1} \}$ , temos  $(0, a_{j+2} a_{j+3} \dots) = (0, a_{k+2} a_{k+3} \dots)$

logo,  $a_{j+2} = a_{k+2}$ ,  $a_{j+3} = a_{k+3}, \dots$ , como  $1 \leq j < k$ ,  $t = k - j \geq 1 \Rightarrow k = j + t$ .

Então  $a_{j+2} = a_{j+t+2}$ ,  $a_{j+3} = a_{j+t+3}$  e mais geralmente  $a_{j+s} = a_{j+t+s}$ , para todo  $s \geq 2$ .

Portanto  $m$  é periódico.

**Proposição 5.6:** Todo número racional é periódico.

Demonstração: Seja  $m = \frac{p}{q}$ , racional,  $p < q$ ,  $\text{mdc}(p, q) = 1$  e  $\text{mdc}(10, q) = 1$  logo,

$\text{mdc}(10^k p, q) = 1$ . Pela divisão euclidiana, temos  $10^k p = a_1 q + r_1$ ,  $r_1 \in \{1, 2, \dots, q - 1\}$ ;  $\text{mdc}(10^k p, q) = 1$ , então  $\frac{p}{q} = \frac{a_1}{10} + \frac{r_1}{10q}$ .

$$\frac{p}{q} = \frac{a_1}{10} + \frac{r_1}{10q}$$

Pela representação decimal,  $m = \frac{a_1}{10} + m_1$ , onde  $a_1 = \lfloor 10m \rfloor$  e  $m_1 = \frac{r_1}{10q}$ .

$$\text{Seguindo, } 10^2 m_1 = \frac{10r_1}{q} = \frac{a_2 q + r_2}{q} = a_2 + \frac{r_2}{q}$$

De maneira indutiva, obtemos  $\{ 10^k m_{k-1} \} = \frac{r_k}{q}$ , onde  $r_k \in \{1, 2, \dots, q - 1\}$ .

O conjunto  $\{ \frac{r_k}{q} \}$  é finito, pois  $\frac{r_k}{q} \in \{ \frac{1}{q}, \dots, \frac{q-1}{q} \}$ . Portanto o conjunto

$\{ \{ 10^k m_{k-1} \} \}$  é finito, logo, pela proposição 5.5, existem  $k$  e  $j$  tal que  $\{ 10^j m_{j-1} \} = \{ 10^k m_{k-1} \}$ , então  $m$  é periódico.

## 6 TAMANHO DO PERÍODO

Nesta seção veremos como determinar o tamanho do período de um número racional

$$m = \frac{p}{q} \text{ com } \text{mdc}(p, q) = 1.$$

Segue alguns conceitos fundamentais:

Seja  $\mathbb{Z}_n = \{\overline{0}, \dots, \overline{n-1}\}$  anel das classes de equivalência módulo  $n$ ;

$\mathbb{Z}_n^* = \{\overline{1}, \dots, \overline{n-1}\}$  conjunto das classes dos invertíveis módulo  $n$ .  $\bar{a} \in \mathbb{Z}_n^*$  se, e somente se  $\text{mdc}(a, n) = 1$ ;

$\phi(n) = |\mathbb{Z}_n^*|$  é a ordem (número de elementos do grupo multiplicativo  $\mathbb{Z}_n^*$ );

Seja  $\mathbb{Z}_n^* = \{\overline{1}, \dots, \overline{a_{\phi(n)}}\}$  o conjunto das classes dos invertíveis módulo  $n$ ;

**Proposição 6.1:** Para inteiros  $a$  e  $b$  sejam primos entre si, é necessário e suficiente que se possam encontrar  $x_0$  e  $y_0$  inteiros, tal que  $ax_0 + by_0 = 1$ .

Demonstração:

( $\Rightarrow$ ) Se  $a$  e  $b$  são primos entre si, existem  $x_0$  e  $y_0$  inteiros tais que  $d = ax_0 + by_0$ , onde  $d$  é o máximo divisor comum de  $a$  e  $b$ , logo, pondo  $d = 1$ , temos  $ax_0 + by_0 = 1$ .

( $\Leftarrow$ ) Supondo que se possam encontrar  $x_0$  e  $y_0$  inteiros, tal que  $ax_0 + by_0 = 1$

Então qualquer divisor comum de  $a$  e  $b$  também é divisor comum de 1. Logo, os únicos divisores comuns aos elementos  $a$  e  $b$  são  $+1$  e  $-1$ . De onde o máximo divisor comum de  $a$  e  $b$  é 1.

**Corolário 6.2:** Seja  $\bar{a}$  invertível,  $\bar{a} \in \mathbb{Z}_n^*$  se, e somente se  $\text{mdc}(a, n) = 1$

Demonstração:

( $\Rightarrow$ ) Se  $\bar{a} \in \mathbb{Z}_n^*$  é invertível, existe  $\bar{a}^{-1} \in \mathbb{Z}_n^*$ , então  $\bar{a} \cdot \bar{a}^{-1} = \bar{1}$ .  $\bar{a} = 1$ , logo  $a \cdot a^{-1} \equiv 1 \pmod{n}$  ou  $a \cdot a^{-1} - 1 = nq$ ,  $q \in \mathbb{Z}$ . Pela proposição anterior, temos que  $a \cdot a^{-1} - nq = 1$ , logo  $\text{mdc}(a, n) = 1$ .

( $\Leftarrow$ ) Se  $\text{mdc}(a, n) = 1$ , novamente pela proposição anterior, existem  $x_0$  e  $y_0$ , tal que:

$ax_0 + ny_0 = 1$ . Dessa igualdade segue que  $ax_0 - 1 = n(-y_0)$  portanto  $ax_0 \equiv 1 \pmod{n}$ . De onde  $\overline{ax_0} = \bar{1}$ , ou  $\bar{a} \cdot \overline{x_0} = \bar{1}$ , logo  $\bar{a}$  é invertível e  $\overline{x_0}$  é seu inverso. Dessa forma, temos que o conjunto  $\mathbb{Z}_n^*$  também pode ser escrito como  $\mathbb{Z}_n^* = \{\bar{a} \in \mathbb{Z}_n; \text{mdc}(a, n) = 1\}$ .

Exemplos:

$$\mathbb{Z}_{10}^* = \{\bar{a} \in \mathbb{Z}_{10}; \text{mdc}(a, 10) = 1\} \text{ então, } \mathbb{Z}_{10}^* = \{\bar{1}, \bar{3}, \bar{7}, \bar{9}\}.$$

$$\mathbb{Z}_{11}^* = \{\bar{a} \in \mathbb{Z}_{11}; \text{mdc}(a, 11) = 1\} \text{ então, } \mathbb{Z}_{11}^* = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}, \bar{10}\}$$

Conceitos de ordem de um elemento e ordem de um grupo:

$\text{ord}_n a = |\langle \bar{a} \rangle|$ , onde  $\langle \bar{a} \rangle$  é subgrupo de  $\mathbb{Z}_n^*$  das potências de  $a$ ;

$\text{ord}_n a$  é o menor inteiro positivo  $k$ , tal que  $a^k \equiv 1 \pmod{n}$  ou o menor inteiro tal que  $a^k - 1 = t \cdot n$ , com  $t \in \mathbb{Z}$ . Se  $a = 10$ , temos  $a^k - 1 = 9 \dots 9 = t \cdot n$ , com  $k$  “noves”.

$\text{ord}_n a$  divide  $\phi(n) = |\mathbb{Z}_n^*|$ . Um exemplo:  $\mathbb{Z}_6^*$ , como  $\bar{a} \in \mathbb{Z}_6^*$  se, e somente se  $\text{mdc}(a, 6) = 1$ , podemos definir  $\mathbb{Z}_6^* = \{\bar{a} \in \mathbb{Z}_6; \text{mdc}(a, 6) = 1\}$ , com cada elemento invertível, ou seja  $\mathbb{Z}_6^* = \{1, 5\}$ , temos que  $\text{ord}_6 1 = 1$ , pois 1 é o menor natural que satisfaz  $1^1 \equiv 1 \pmod{6}$ , e como  $\phi(6) = |\mathbb{Z}_6^*| = 2$ , temos que  $1 \mid 2$ , logo  $\text{ord}_6 1$  divide  $\phi(6)$ , completando,  $\text{ord}_6 5 = 2$ , pois  $5^2 = 25 \equiv 1 \pmod{6}$ , e  $2 \mid 2$ , logo  $\text{ord}_6 5$  divide  $\phi(6)$ .

**Proposição 6.3:** Se  $a^w \equiv 1 \pmod{n}$ , então  $\text{ord}_n a$  divide  $w$ ;

**Teorema 6.4:** Seja  $m = \frac{p}{q}$  racional  $0 < p < q$ ,  $\text{mdc}(p, q) = 1$  e  $\text{mdc}(q, 10) = 1$ .

Então é um número periódico (dízima periódica) de tamanho  $k = \text{ord}_q 10$ .

Demonstração:

Como  $\text{mdc}(q, 10) = 1$ , logo existe  $t \in \mathbb{Z}$  tal que  $qt = 10^k - 1$ , onde  $k = \text{ord}_q 10$ .

Então  $\frac{p}{q} = \frac{tp}{tq} = \frac{tp}{10^k - 1}$ . Tomando a representação decimal  $tp = \frac{a_1 10^{k-1} + \dots + a_k}{10^k - 1} =$

$(0, \overline{a_1 a_2 \dots a_k})$  mostra que  $m$  é periódico com um período de tamanho  $k$ .

Determinar o valor de  $\text{ord}_q 10$  é mais trabalhoso. Temos que fazer por tentativas entre divisores de  $\phi(n)$ .

**Exemplos:**

$$\phi(51) = 32 \text{ e } \text{ord}_{51} 10 = 16$$

$$\phi(97) = 96 \text{ e } \text{ord}_{97} 10 = 96$$

$$\phi(21) = 12 \text{ e } ord_{21} 10 = 6$$

Se  $n = 91$  segue que  $\phi(91) = \phi(7 \cdot 13) = \phi(7) \cdot \phi(13) = 6 \cdot 12 = 72$ . Verificando os divisores de  $n$  temos que  $ord_{91} 10 = 6$ .

Seja  $q = 91$ . Tomando  $0 < p < 91$ ,  $p \in \mathbb{Z}$  e  $mdc(p, 91) = 1$ ,  $m = \frac{p}{91}$  é periódico, com período de tamanho 6.

**Exemplos:**

$$p = 90, \text{ então } m = \frac{90}{91} = 0.989010989010\dots = 0,\overline{989010}.$$

$$p = 89, \text{ então } m = \frac{89}{91} = 0.978021978021\dots = 0,\overline{978021}.$$

$$p = 87, \text{ então } m = \frac{87}{91} = 0.956043956043\dots = 0,\overline{956043}.$$

## 7 CONSIDERAÇÕES FINAIS

A função  $\phi(n)$ , com  $n$  inteiro positivo é importante para determinar o tamanho do período de um número racional, mas fazer por tentativas entre os divisores de  $\phi(n)$ , é trabalhoso. Chegamos a conclusão que o período depende somente do denominador, e apesar de conseguirmos alcançar o objetivo trabalhando com  $\phi(n)$ , há maneiras mais fáceis de determinar o tamanho do período de um número racional, pois, logicamente no caso de  $n$  “grande” indicará que o número de divisores de  $\phi(n)$  também poderá ser grande, custando mais tempo a quem for tentar encontrar o tamanho do período. Uma alternativa é melhorar a estimativa de  $ord_n 10$  usando as próprias propriedades de  $\phi(n)$ . Isso tudo significa que  $\phi(n)$  é de muita importância para determinar o tamanho do período de um número racional.

## REFERÊNCIAS

BOYER, C. B. **História da matemática**. Tradução do inglês para o português de Elza Gomide. São Paulo: Edgard Blucher Ltda, 1974.

DIAS, Sandy da Conceição. Simon Stevin e os números decimais. **Sociedade Brasileira de Educação Matemática**, São Paulo, 13-16 julho. 2016. Disponível em: [http://www.sbemrasil.org.br/enem2016/anais/pdf/6717\\_2854\\_ID.pdf](http://www.sbemrasil.org.br/enem2016/anais/pdf/6717_2854_ID.pdf). Acesso em: 21 dez. 2020.

IEZZI, Gelson; DOMINGUES, Hygino H. **Álgebra Moderna**. 2 ed. São Paulo: Atual, 1982.

JUCÁ, R. de S. **Uma sequência didática para o ensino das operações com os números decimais**. Dissertação. Universidade do Estado do Pará. Belém, 2008.

LIMA, Elon Lages. **Análise real**. 2.ed. Rio de Janeiro: Instituto de Matemática Pura e Aplicada, CNPQ, 1993. 189 p. (Matemática universitária)

SANTOS, José Plínio de Oliveira. **Introdução à teoria dos números**. 2. ed. Rio de Janeiro: IMPA; CNPQ, 2000. 196 p.

WAGNER, Alfredo. **Frações Decimais**. (comunicação pessoal com o autor, 2018)