UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO
DEPARTAMENTO DE MATEMÁTICA
Mestrado Profissional em Matemática em Rede Nacional

Marcelo José Celestino

Representação dos Números Reais em uma Base Arbitrária

RECIFE
2021

UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO
DEPARTAMENTO DE MATEMÁTICA
Mestrado Profissional em Matemática em Rede Nacional

Marcelo José Celestino

Representação dos Números Reais em uma Base Arbitrária

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

Orientador: Prof. Dr. Rodrigo Gondim

RECIFE
2021

Dados Internacionais de Catalogação na Publicação
Universidade Federal Rural de Pernambuco
Sistema Integrado de Bibliotecas
Gerada automaticamente, mediante os dados fornecidos pelo(a) autor(a)

C392r Celestino, Marcelo José
Representação dos Números Reais em uma Base Arbitrária / Marcelo José Celestino. - 2021.
111 f. : il.

Orientador: Rodrigo Jose Gondim Neves.
Inclui referências e apêndice(s).

Dissertação (Mestrado) - Universidade Federal Rural de Pernambuco, Programa de Mestrado Profissional em Matemática (PROFMAT), Recife, 2021.

1. Representação. 2. Sistema de Numeração. 3. Base Arbitrária. 4. Transcendentes. I. Neves, Rodrigo Jose Gondim, orient. II. Título

CDD 510

DECLARAÇÃO

Eu, Marcelo José Celestino, declaro, para devidos fins e efeitos, que a dissertação sob título REPRESENTAÇÃO DOS NÚMEROS REAIS EM UMA BASE ARBITRÁRIA, entregue como Trabalho de Conclusão de curso para obtenção do título de mestre, com exceção das citações diretas e indiretas claramente indicadas e referenciadas, é um trabalho original. Eu estou consciente que a utilização de material de terceiros incluindo uso de paráfrase sem a devida indicação das fontes será considerado plágio, e estará sujeito à processos administrativos da Universidade Federal Rural de Pernambuco e sanções legais. Declaro ainda que respeitei todos os requisitos dos direitos de autor e isento a Pós-graduação PROFMAT/UFRPE, bem como o professor orientador Rodrigo José Gondim Neves, de qualquer ônus ou responsabilidade sobre a sua autoria.

Recife, 04 de junho 2021.

Assinatura: _____

MARCELO JOSÉ CELESTINO

Representação dos Números Reais em uma Base Arbitrária

Trabalho apresentado ao Programa de Mestrado Profissional em Matemática – PROFMAT do Departamento de Matemática da UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO, como requisito parcial para obtenção do grau de Mestre em Matemática.

Aprovado em 04/06/2021

BANCA EXAMINADORA

_____

Prof. Dr. Rodrigo José Gondim Neves (Orientador)– UFRPE

_____

Prof. Dr. Airton Temístocles Gonçalves de Castro – DMat/UFPE

_____

Profa. Dra. Anete Soares Cavalcanti– PROFMAT/UFRPE

À minha família

Agradecimentos

Agradeço a Deus primeiramente, por ter me ajudado em toda a trajetória deste curso. Sem Ele, eu não teria chegado até aqui.

À minha família, esposa e filhos, pelo apoio, encorajamento, sacrifícios que fizeram para que eu pudesse estudar.

Ao meu orientador Dr. Rodrigo Gondim, por ter sido peça importante para a conclusão deste curso e pelas orientações.

Aos professores do Profmat que, com dedicação, nos transmitiram o ensino de forma que pudéssemos aprender.

Ao professor Eudes Mendes, da disciplina Tópicos de Matemática, pela grande contribuição para que eu pudesse desenvolver o TCC, aprendendo projeto de pesquisa e látex.

Aos meus colegas de classe, pelas trocas de ideias.

À coordenação do Profmat da UFRPE, pelo apoio recebido.

A todos que, direta ou indiretamente, me ajudaram e se tornaram peças importantes para a conclusão deste curso.

À CAPES, pelo apoio financeiro.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

"Não vos conformeis com este mundo,
mas transformai-vos pela renovação
do vosso entendimento,
para que experimenteis qual seja a boa,
agradável e perfeita vontade de Deus.
(Bíblia Sagrada, Romanos 12.2)

Resumo

Este trabalho visa aprofundar o estudo sobre representação dos números, partindo do pressuposto que todo número possui uma representação, isto é, os naturais, os racionais, os irracionais e os reais. Observaremos como se representa um número em determinado conjunto e procuraremos extrair algumas propriedades. E, visando um método de ensino eficaz, lúdico e atrativo, faremos uma implementação da representação de um número na base binária utilizando os dedos das mãos, servindo assim, de auxílio pedagógico. E, por fim, descreveremos alguns problemas olímpicos que fazem jus ao que estamos estudando.

Palavras-chave: Representação, sistema de numeração, base arbitrária, transcendentes.

Abstract

This work aims to deepen the study on the representation of numbers, assuming that every number has a representation, that is, the natural, the rational, the irrational and the real. We will observe how a number is represented in a given set and we will try to extract some properties. And, aiming at an effective, playful and attractive teaching method, we will implement the representation of a number on the binary basis using the fingers, thus serving as a pedagogical aid. And, finally, we will describe some olympic problems that do justice to what we are studying.

Keywords: Representation, numbering system, arbitrary basis, transcendent.

Lista de ilustrações

Sumário

Introdução

Atualmente vivemos no "mundo dos números", mas foram necessários muitos anos de descobertas e aperfeiçoamento para chegarmos à forma atual de como escrevê-los. Se faziam marcas em madeira, em osso, nós em corda, utilizavam pedras, dedos das mãos, gravetos, entre outros, para registrar as quantidades. Com o passar do tempo, povos de diversas civilizações criaram e aperfeiçoaram vários sistemas de numeração. Com esses sistemas de numeração surgiram as representações dos números naturais, seguidas dos racionais e dos reais.

O foco do nosso trabalho é tratar a representação dos números reais em uma base arbitrária. O tema justifica-se pelos seguintes:

Observando livros da educação básica, constatamos que o tema em curso é abordado, mas de forma superficial, em que se faz representação dos números apenas na base decimal praticamente e, na base binária, raramente, sem haver a preocupação no ensino da representação dos números em outras bases.

Durante toda educação básica, os alunos não são instigados a reconhecerem um objeto matemático em diversas representações, sejam elas simbólicas, algébricas, gráficas ou em linguagem natural. Os alunos aprendem os objetos matemáticos em um único sentido de conversão, o que os impedem de coordenar estes registros de representação dificultando a aprendizagem matemática.

Outro fato é que podemos correlacionar a matemática com outras áreas afins, como por exemplo, a informática, que utiliza sistema binário e sistema hexadecimal para representar dados.

A BNCC (Base Nacional Comum Curricular), tratando acerca do desenvolvimento do letramento matemático, o define como as competências e habilidades de raciocinar, representar, comunicar e argumentar matematicamente, de modo a favorecer o estabelecimento de conjecturas, a formulação e a resolução de problemas em uma variedade de contextos, utilizando conceitos, procedimentos, fatos e ferramentas matemáticas. Ou seja, entre as competências e habilidades do letramento matemático está o representar matematicamente, o que tem sido alvo de dificuldade para muitas pessoas.

Diante do exposto, problematizamos: Como representar números reais em uma base arbitrária?

Nosso objetivo é representar números reais em uma base arbitrária e, nesse ínterim, almejamos conhecer a representação de um número natural, racional e real em uma base arbitrária; descrever a representação de um número real em uma base arbitrária e verificar

propriedades e, entender a representação de um número real em uma base arbitrária.

Para alcançar nosso objetivo, usamos como método a pesquisa bibliográfica feita em livros, artigos, sites de internet e outros que tratam do tema proposto.

Pois bem, observaremos o que outras pessoas escreveram acerca do tema proposto, o que irá aclarar ainda mais a importância do tema. Em seguida, observaremos o que a BNCC tem descrito a respeito do assunto em pauta, como também observaremos o embasamento matemático, isto é, a teoria matemática que dá base ao objeto de estudo.

1 Referencial Teórico

De acordo com (1), representar tem vários sentidos, entre esses estão "substituir", "estar em lugar de", "significar"e "denotar". Quando estamos representando números, estamos trazendo significado, denotação de um número por um símbolo.

Patrício (2) diz que "as representações assumem um papel decisivo na aprendizagem e no ensino da matemática, muito importante e peculiar, haja vista, os objetos matemáticos serem de natureza abstrata, ou seja, não possuem existência física".

De acordo com (3) não há como um sujeito mobilizar qualquer conhecimento sem realizar uma atividade de representação. Desta forma a noção de representação torna-se fundamental para qualquer estudo psicológico que investigue a forma como se processa a aquisição de conhecimento e de como se processam transformações de representações. Duval, quando trata de representações, o faz em três concepções diferentes, a saber: representação mental, representação interna ou computacional e representação semiótica. Esta última se diferencia por serem produzidas por um sistema particular de signos e também por poderem ser convertidas em representações equivalentes em outro sistema semiótico, dando ao sujeito a possibilidade de atribuir significações diferentes a essas representações.

Vale salientar que um objeto matemático pode ter diversas representações.

> Há uma palavra às vezes importante e marginal em matemática, é a palavra “representação”. Ela é, na maioria das vezes, empregada sob a forma verbal “representar”. Uma escrita, uma notação, um símbolo representam um objeto matemático: um número, uma função, um vetor... Do mesmo modo, os traçados e figuras representam objetos matemáticos: um segmento, um ponto, um círculo. Isto quer dizer que os objetos matemáticos não devem ser jamais confundidos com a representação que se faz dele. De fato, toda confusão acarreta, em mais ou menos a longo termo, uma perda de compreensão e os conhecimentos adquiridos tornam-se rapidamente inutilizáveis ao longo de seu contexto de aprendizagem: seja por não lembrar ou porque permanecem como representações “inertes” que não sugerem nenhum tratamento. A distinção entre um objeto e sua representação é, portanto, um ponto estratégico para a compreensão da matemática. (4)

Na teoria de Duval observamos que os registros de representações são procendências típicas de representar um objeto matemático, e o sistema no qual podemos representar um objeto matemático, denomina-se sistema ou registro semiótico. A importância dos registros semióticos se dá não somente por se constituírem num sistema de comunicação, mas também por possibilitarem a organização de informações a respeito do objeto representado.

Em matemática, é importante separar, distinguir o objeto de sua representação.

Exemplo 1.1. Observe algumas representações do número nove: $9, 13 - 4, \frac{18}{2}$ e 3^2.

Note que essas representações referem-se ao mesmo número, ao mesmo objeto matemático, a mesma referência. Entretanto, os objetos nestas representações distintas, não possuem o mesmo significado operatório. De fato, um aluno, pode reconhecer o 9 em $13 - 4$, mas pode ser que não consiga fazer o mesmo em 3^2 ou em $\frac{18}{2}$.

Duval em seus registros esclarece que a distinção entre sentido e referência está estreitamente ligado ao princípio da substituição, que é essencial nos procedimentos de cálculo ou de dedução, ou seja, duas expressões tendo a mesma referência podem ser trocadas uma pela outra, em uma frase ou fórmula, sem que o valor mude.

Exemplo 1.2. Efetuar a operação $1 + \frac{1}{5}$.

Podemos efetuar a operação da seguinte forma:

$1 + \frac{1}{5} = \frac{5}{5} + \frac{1}{5} = \frac{6}{5}$.

Mas observe que podemos efetuar esta mesma operação de outra forma, mantendo a mesma referência:

$1 + \frac{1}{5} = 1 + 0,2 = 1,2$.

Note que, no primeiro caso, nos mantivemos na mesma rede semiótica de representação, enquanto que no segundo caso, há uma mudança de sistema de representação.

A isto, Duval esclarece que a pluralidade de sistemas de representação permite uma diversificação de representação de um mesmo objeto, o que aumenta as capacidades cognitivas do sujeito e consequentemente potencializa as suas representações mentais.

Em suma, tratando-se dos sistemas semióticos, Patrício (2) resume que

> Os sistemas semióticos são sistemas de representação que cumprem três atividades cognitivas de toda representação. A primeira é a **formação** de uma marca, que possa ser identificada como representação de um objeto; a segunda, o **tratamento**, é a transformação de representação, uma mudança de forma, mas preservando as características próprias do sistema onde foi criada. E a terceira, a possibilidade de **conversão** da representação com sua passagem a outro sistema, mas mantendo o mesmo objeto de referência (2).

Pensando como Duval, observamos que tanto as atividades mais simples quanto as atividades mais elaboradas envolvendo matemática, requerem uma certa complexidade ao funcionamento cognitivo. E muitas análises acerca da compreensão matemática reproduz na imaginação as complexidades epistemológicas dos conceitos, mas estas podem ser explicadas pela história de suas descobertas. Duval ainda aponta duas características que fazem diferença entre a atividade requerida pela atividade matemática e a requerida nos

domínios do conhecimento, embora ambas exijam um conjunto de conceitos com certo grau de complexidade. São elas:

1. A importância que as representações semióticas têm para a matemática; em primeira instância, porque as operações de cálculo, por exemplo, dependem do sistema de representação utilizado; em segunda instância, pelo fato de os objetos necessitarem de um sistema de representação que lhes permitam ser acessados.

2. A grande variedade de representações semióticas utilizadas em matemática: os sistemas de numeração, as figuras geométricas, escritas algébricas e formais, as representações gráficas e a língua natural mesmo quando ela não é utilizada no seu uso comum.

Já vimos que, em matemática, há uma diversidade de representações, ou seja, existem diversos registros que possibilitam a mobilização simultânea de várias representações de um objeto e a troca entre essas representações e, isso pode ser feito a qualquer momento, de acordo com a necessidade. A originalidade da atividade matemática está justamente nessas características. Sabe-se que em determinadas ocasiões um tipo de registro pode ser colocado em evidência, mas deve existir sempre a possibilidade de passar de um registro para outro.

De acordo com (4), no decorrer do processo educativo, existem algumas indicações que os alunos dão de aprendizado. As mobilizações das representações dos objetos matemáticos, indicam se eles estão aprendendo ou não. Também indicam em que pontos eles estão com dificuldades. Se estas representações forem coordenadas de forma eficiente, podem facilitar o aprendizado nas aulas de matemática, cabendo ao professor direcionar o aluno a este novo pensar. Além das representações, Duval traz a definição de congruência entre representações. É por meio dessas e outras definições que é possível ao professor ministrar suas aulas e ainda verificar nos alunos as conversões e tratamentos realizados por estes durante a produção dos conteúdos em sala de aula.

Observando (5), vemos que a área da matemática nos seus diversos campos - Aritmética, Álgebra, Geometria, Estatística e Probabilidade - precisa garantir que os alunos relacionem observações empíricas do mundo real a **representações** (tabelas, figuras e esquemas) e associem essas representações a uma atividade matemática (conceitos e propriedades), fazendo induções e conjecturas. Na fase do ensino fundamental espera-se também o desenvolvimento de habilidades no que se refere à leitura, escrita e ordenação de números naturais e números racionais por meio da identificação e compreensão de características do sistema de numeração decimal, sobretudo o valor posicional dos algarismos. Na perspectiva de que os alunos aprofundem a noção de número, é importante colocá-los diante de tarefas, como as que envolvem medições, nas quais os números naturais não são suficientes para resolvê-las, indicando a necessidade dos números racionais tanto na representação decimal

quanto na fracionária. Nessa fase, precisa ser destacada a importância da comunicação em linguagem matemática com o uso da linguagem simbólica, da **representação** e da argumentação.

A BNCC enfatiza bem a importância da representação de um determinado objeto matemático.

> As competências que estão diretamente associadas a representar pressupõem a elaboração de registros para evocar um objeto matemático. Apesar de essa ação não ser exclusiva da Matemática, uma vez que todas as áreas têm seus processos de representação, é em especial nessa área que podemos verificar de forma inequívoca a importância das representações para a compreensão de fatos, de ideias e de conceitos, uma vez que o acesso aos objetos matemáticos se dá por meio delas. Nesse sentido, na Matemática, o uso dos registros de representação e das diferentes linguagens é, muitas vezes, necessário para a compreensão, resolução e comunicação de resultados de uma atividade. Por sua vez, o trânsito entre os diversos registros de representação pode favorecer que os estudantes tenham maior flexibilidade e fluidez na área e, ainda, promover o desenvolvimento do raciocínio (5).

Dentre os objetos de conhecimentos descritos em (5) descatacamos as seguintes habilidades que fazem jus ao tema em estudo:

- (EF06MA01) Comparar, ordenar, ler e escrever números naturais e números racionais cuja representação decimal é finita, fazendo uso da reta numérica.
- (EF06MA02) Reconhecer o sistema de numeração decimal, como o que prevaleceu no mundo ocidental, e destacar semelhanças e diferenças com outros sistemas, de modo a sistematizar suas principais características (base, valor posicional e função do zero), utilizando, inclusive, a composição e decomposição de números naturais e números racionais em sua representação decimal.
- (EF06MA08) Reconhecer que os números racionais positivos podem ser expressos nas formas fracionária e decimal, estabelecer relações entre essas representações, passando de uma representação para outra, e relacioná-los a pontos na reta numérica.
- (EF07MA10) Comparar e ordenar números racionais em diferentes contextos e associá-los a pontos da reta numérica.
- (EF08MA01) Efetuar cálculos com potências de expoentes inteiros e aplicar esse conhecimento na representação de números em notação científica.
- (EF09MA02) Reconhecer um número irracional como um número real cuja representação decimal é infinita e não periódica, e estimar a localização de alguns deles na reta numérica.

- (EM13MAT306) Resolver e elaborar problemas em contextos que envolvem fenômenos periódicos reais (ondas sonoras, fases da lua, movimentos cíclicos, entre outros) e comparar suas representações com as funções seno e cosseno, no plano cartesiano, com ou sem apoio de aplicativos de álgebra e geometria.
- (EM13MAT401) Converter representações algébricas de funções polinomiais de 1º grau em representações geométricas no plano cartesiano, distinguindo os casos nos quais o comportamento é proporcional, recorrendo ou não a softwares ou aplicativos de álgebra e geometria dinâmica.
- (EM13MAT501) Investigar relações entre números expressos em tabelas para representá-los no plano cartesiano, identificando padrões e criando conjecturas para generalizar e expressar algebricamente essa generalização, reconhecendo quando essa representação é de função polinomial de 1º grau.

Pois bem, é com base nesses referenciais que vamos dar sequência ao nosso trabalho, esperando contribuir com um maior esclarecimento do tema proposto.

No capítulo seguinte descrevemos a teoria matemática que dá base ao objeto de estudo. Para isso, nos apoiamos em (6), (7) e (8).

2 Aritmética

2.1 Divisão Euclidiana

Euclides, nos seus *Elementos*, quando definiu o conceito de divisibilidade, o fez com uma visão geométrica. De fato, quando um segmento, utilizado como unidade de medida podia medir outro, nesse caso ele dizia que um número era parte do outro. Em geral, apesar da ideia geométrica de Euclides se aplicar a segmentos, ele considerava número apenas os números naturais, entretanto, aqui estenderemos para os inteiros.

Definição 2.1. *Sejam a e b inteiros. Dizemos que a é múltiplo de b se existe um k pertencente a $\mathbb{Z}$ tal que $a = kb$.*

Nestas condições, dizemos que a é divisível por b ou que b é divisor de a ou ainda que b divide a. Usaremos a notação $b \mid a$ para indicar que b divide a.

Proposição 2.1. *A relação de divisibilidade nos inteiros satisfaz as seguintes propriedades:*

(i) Qualquer que seja $a \in \mathbb{Z}$, tem-se:
$a \mid a, \quad a \mid -a, \quad 1 \mid a, \quad -1 \mid a, \quad a \mid 0$;

(ii) Se $a \mid b$ e $b \mid c$, então $a \mid c$;

(iii) Se $d \mid a$ e $d \mid b$, então $d \mid ax + by$ para quaisquer $x, y \in \mathbb{Z}$;

(iv) Se $a \mid b$ e $b \neq 0$, então $|a| \leq |b|$;

(v) Se $a \mid b$ e $b \mid a$, então $a = \pm b$.

Demonstração. (i) Trivial, pois decorre das igualdades $a = 1 \cdot a$, $a = -1 \cdot a$, $a = a \cdot 1$, $a = (-1) \cdot (-a)$ e $0 = 0 \cdot a$.

(ii) Se $a \mid b$ e $b \mid c$, então existem k e $t \in \mathbb{Z}$ tais que $b = k \cdot a$ e $c = t \cdot b$. Substituindo o valor de b da primeira equação na segunda, temos
$c = t \cdot b = t \cdot (k \cdot a) = (t \cdot k) \cdot a$, o que nos mostra que $a \mid c$.

(iii) Se $d \mid a$ e $d \mid b$, então existem k e $t \in \mathbb{Z}$ tais que $a = k \cdot d$ e $b = t \cdot d$. Assim,
$ax + by = (k \cdot d) \cdot x + (t \cdot d) \cdot y = (k \cdot x + t \cdot y) \cdot d$ e, portanto, $d \mid ax + by$ para quaiquer $x, y \in \mathbb{Z}$.

(iv) De fato, se $a \mid b$, então existe $k \in \mathbb{Z}$ tal que $b = k \cdot a$. Tomando módulos, temos que $|b| = |k| \cdot |a|$. Como $b \neq 0$, temos que $k \neq 0$, logo $1 \leq |k|$ e, por consequência, $|a| \leq |k| \cdot |a| = |b|$.

(v) Se $a \mid b$ e $b \mid a$, então existem $k, t \in \mathbb{Z}$ tais que $b = k \cdot a$ e $a = t \cdot b$. Substituindo o valor de b da primeira equação na outra, temos $a = t \cdot k \cdot a$. Se $a = 0$, então $b = 0$ e, se $a \neq 0$, então $t \cdot k = 1$, o que implica que $t = k = 1$ ou $t = k = -1$, daí $a = b$ ou $a = -b$, portanto $a = \pm b$. ■

2.1.1 O algoritmo da divisão euclidiana

Euclides, nos seus *Elementos*, não enunciou explicitamente, mas utilizou o fato de que sempre é possível efetuar a divisão de a por b, $b \neq 0$, mesmo que essa divisão não seja exata; nesse caso, chamamos divisão com resto. A ideia do algoritmo da divisão, no caso de inteiros positivos, é encontrar o maior múltiplo de b que é menor que a. Para isso fazemos subtrações sucessivas de b em a até enquanto o resultado for positivo. O algoritmo da divisão euclidiana não só é um importante instrumento na obra de Euclides, mas também é um resultado central da teoria.

Teorema 2.1. *Sejam a e b números inteiros com $b \neq 0$. Existem dois únicos números inteiros q e r tais que*

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

Para a demonstração deste teorema usaremos o Princípio da Boa Ordenação enunciado a seguir.

Teorema 2.2. *(Princípio da Boa Ordenação) Todo subconjunto não vazio de $\mathbb{N}$ possui um menor elemento.*

Demonstração. Faremos a demonstração por redução ao absurdo. Seja X um subconjunto não vazio de $\mathbb{N}$ e suponha que X não possui um menor elemento. Queremos mostrar que X é vazio, conduzindo a uma contradição. Considere um conjunto T, complementar de X em $\mathbb{N}$. Queremos, portanto, mostrar que $T = \mathbb{N}$.
Defina o conjunto

$$I_n = \{k \in \mathbb{N}; k \leq n\},$$

e considere a sentença aberta

$$p(n) : I_n \subset T.$$

Como $0 \leq n$ para todo n, segue que $0 \in T$, pois, caso contrário, 0 seria um menor elemento de X. Logo, $p(0)$ é verdade.

Suponha agora que $p(n)$ seja verdade. Se $n + 1 \in X$, como nenhum elemento de I_n está em X, teríamos que $n + 1$ é um menor elemento de X, o que não é permitido. Logo, $n + 1 \in T$, seguindo daí que

$$I_{n+1} = I_n \cup \{n+1\} \subset T,$$

o que prova que $\forall n$, $I_n \subset T$; portanto, $\mathbb{N} \subset T \subset \mathbb{N}$ e, consequentemente, $T = \mathbb{N}$. ■

Agora estamos aptos a demonstrar o teorema relativo ao algoritmo da divisão euclidiana.

Demonstração. Existência: Considere, inicialmente, $a, b > 0$. Se $a < b$, então $q = 0$ e $r = a$ satisfazem as condições do enunciado. Se $a \geq b$, então considere o conjunto $S = \{x = a - by; y \in \mathbb{N} \text{ e } a \geq yb\} \subset \mathbb{N}$. Note que S é um subconjunto não vazio dos naturais e, portanto, pelo Princípio da Boa Ordenação, possui um menor elemento em $\mathbb{N}$. Seja $r \in S$ o menor elemento de S, então existe $q \in \mathbb{N}$ tal que $a - bq = r \Rightarrow a = bq + r$. Vamos mostrar que $r < b$.
Suponha, por absurdo que $r \geq b$. Como $r = a - bq$ temos $r - b = a - (q+1)b$. Pela nossa hipótese, $r - b \in S$, por outro lado, $r - b < r$ e isso contraria a nossa escolha de r como menor elemento de S. Portanto $r < b$.

Para $a < 0$ e $b > 0$, divida $-a$ por b obtendo $-a = bq + r$, com $0 \leq r < b$, assim temos $a = b(-q) + (-r)$; se $r = 0$ conseguimos o desejado, caso contrário temos $-b < -r < 0$ e, então, podemos escrever $a = b(-q) - b + b + (-r) = b(-q-1) + (b - r)$, onde o resto é $r' = b - r$, com $0 < r' < b$, provando o desejado.

Para $b < 0$, divida a por $-b$ obtendo $a = (-b)q + r = b(-q) + r$, assim temos $0 \leq r < -b = |b|$.

Unicidade: Suponha que dados $a, b \in \mathbb{Z}$ tenham sido encontrados dois pares de quociente e resto satisfazendo

$$a = bq + r = bq' + r'$$

onde q, q', r, $r' \in \mathbb{Z}$, e que $0 \leq r < |b|$ e $0 \leq r' < |b|$. Então, supondo r diferente de r', digamos $r > r'$, temos que $r - r' = bq - bq' = b(q - q') > 0$. Como $r - r' < b$ e pela igualdade $r - r'$ é múltiplo de b, devemos ter necessariamente $r - r' = 0$, o que contradiz a hipótese. Daí concluímos que $r = r'$ e, então, $b(q' - q) = 0$ e, portanto, $q = q'$. ■

Temos então que os números q e r são chamados, respectivamente, de quociente e resto da divisão de a por b. Da divisão euclidiana, temos que o resto da divisão de a por b é zero se, e somente se, b divide a.

A seguir, para ilustrar aplicações do Algoritmo de Euclides, passaremos a alguns exemplos.

Exemplo 2.1. *Mostrar que o resto da divisão de* 10^n *por* 9 *é sempre* 1*, qualquer que seja o número natural* n*.*

Faremos a demonstração por indução. Para $n = 1$, temos $10^1 = 9 \cdot 1 + 1$; portanto o resultado vale. Suponha, agora, que o resultado vale para algum $n \in \mathbb{N}$, isto é, $10^n = 9q+1$, vamos mostrar que vale para $n + 1$.

Ora, $10^{n+1} = 10 \cdot 10^n = (9 + 1) \cdot 10^n = 9 \cdot 10^n + 10^n$. Por hipótese, $10^n = 9q + 1$, então substituindo temos, $9 \cdot 10^n + 10^n = 9 \cdot 10^n + 9q + 1 = 9(10^n + q) + 1 = 9q' + 1$.

Logo, o resultado vale para $n + 1$. Portanto, pelo Princípio de Indução, temos que o resultado vale para todo $n \in \mathbb{N}$.

Exemplo 2.2. *Qual o quinquagésimo termo da sequência EUCLIDESEUCLIDESEUCLI...?*

Note que os termos dessa sequência se repetem de 8 em 8. Como $50 = 8 \cdot 6 + 2$, ou seja, o resto da divisão de 50 por 8 é 2, temos que o quinquagésimo termo da sequência será a letra U.

Exemplo 2.3. *Se hoje é quarta-feira, que dia da semana será daqui a* 90 *dias? Quantas semanas completas terão passado?*

Como sabemos a semana tem 7 dias, portanto, a cada 7 dias estaremos novamente em uma quarta-feira. Assim sendo, gostaríamos de saber qual o maior múltiplo de 7 menor que 90 e depois ver quantos dias ainda devemos passar para atingir 90. A resposta está codificada em

$$90 = 84 + 6 = 7 \cdot 12 + 6$$

Portanto, será terça-feira e terão sido passadas 12 semanas completas.

2.2 MDC e o Algoritmo Estendido de Euclides

Embora conhecendo propriedades teóricas do MDC entre dois números inteiros a e b, encontrá-lo pode não ser uma tarefa fácil se não utilizarmos as ferramentas corretas. Poderíamos, por exemplo, encontrar o conjunto dos divisores de a, o conjunto dos divisores de b e verificar qual o maior elemento comum aos dois conjuntos. No entanto, podemos nos utilizar do Algoritmo de Euclides e encontrar de forma rápida e prática o mdc de a e b.

Definição 2.2. *Sejam a e b números inteiros não simultaneamente nulos. Um número d será dito um divisor comum de a e b se $d \mid a$ e $d \mid b$.*

Definição 2.3. *Diremos que d é um máximo divisor comum de a e b se possuir as seguintes propriedades:*

(i) d é divisor comum de a e de b;

(ii) d é divisível por todo divisor comum de a e b.
A condição (ii) pode ser reenunciada como se segue:
ii') Se c é um divisor comum de a e b, então $c \mid d$.

Denotamos $d = mdc(a, b)$ ou $d = (a, b)$.

Lema 2.1. *Sejam $a, b, n \in \mathbb{Z}$. Se existe $(a, b - na)$, então (a, b) existe e $(a, b) = (a, b - na)$.*

Demonstração. Seja $d = (a, b - na)$. Como $d \mid a$ e $d \mid (b - na)$, segue que d divide $b = b - na + na$. Logo d é um divisor comum de a e b. Suponha agora que c seja um divisor comum de a e b. Logo c é um divisor comum de a e $b - na$ e, portanto, $c \mid d$. Isso prova que $d = (a, b)$. ■

2.2.1 Algoritmo Estendido de Euclides

Dados $a, b \in \mathbb{N}$, podemos supor $b \leq a$. Se $b = 1$ ou $b = a$, ou ainda $b \mid a$, sabemos trivialmente que $mdc(a, b) = b$. Suponhamos, então, que $1 < b < a$ e que $b \nmid a$. Logo, pela divisão euclidiana, podemos escrever

$$a = bq_1 + r_1, \text{ com } 0 < r_1 < b.$$

Temos duas possibilidades:

1. $r_1 \mid b$. Em tal caso, $r_1 = (b, r_1)$ e, pelo Lema 2.1, temos que

$$r_1 = (b, r_1) = (b, a - q_1 b) = (b, a) = (a, b),$$

e o algoritmo termina.

2. $r_1 \nmid b$. Em tal caso, podemos efetuar a divisão de b por r_1, obtendo

$$b = r_1 q_2 + r_2, \text{ com } 0 < r_2 < r_1.$$

Novamente, temos duas possibilidades:

a) $r_2 \mid r_1$. Nesse casso, $r_2 = (r_1, r_2)$ e novamente, pelo Lema 2.1,

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

e paramos, pois termina o algoritmo.

b) $r_2 \nmid r_1$. Nesse caso, podemos efetuar a divisão de r_1 por r_2, obtendo

$$r_1 = r_2 q_3 + r_3, \text{ com } 0 < r_3 < r_2.$$

Continuamos esse procedimento até que pare. Isto sempre ocorre, pois, caso contrário, teríamos uma sequência de números naturais $b > r_1 > r_2 > \ldots$ que não possui menor elemento, o que não é possível pelo Princípio da Boa Ordenação. Logo, para algum n, temos que $r_n \mid r_{n-1}$, o que implica que $(a, b) = r_n$.

Exemplo 2.4. *Em uma determinada escola, o professor de matemática de uma turma do sexto ano pediu aos alunos que se reunissem em grupos para fazer um trabalho escolar. Nessa turma há* 44 *alunos, sendo* 24 *meninas e* 20 *meninos. Sabendo que em cada grupo só pode ter apenas meninos ou apenas meninas e que nos grupos deve haver a mesma quantidade de alunos, qual a quantidade máxima de alunos que pode ter em cada grupo?*

O que queremos é calcular o máximo divisor comum entre 20 e 24. De acordo com o algoritmo de Euclides obtemos
$24 = 20 \times 1 + 4$
$20 = 4 \times 5 + 0$

Observe que o último quociente foi 4, portanto pelo algoritmo de Euclides, temos $(24, 20) = 4$.

2.3 Relações de Equivalência

Quando pensamos em aritmética modular, pensamos numa maneira moderna de introduzi-la e, essa maneira é através das relações de equivalência. Seja X um conjunto, que pode ser finito ou infinito. Definimos uma relação em X dizendo como comparar dois elementos deste conjunto. Observe que para definir a relação, precisamos dizer quem é o conjunto subjacente; isto é, o conjunto cujos elementos estão sendo comparados.

No conjunto dos números inteiros, por exemplo, temos duas relações naturais, a relação de igualdade e a relação de desigualdade. Em um conjunto de bolas coloridas, temos a relação bolas de uma mesma cor. Esse é um ótimo exemplo para se ter em mente, porque é muito concreto. As relações de equivalência são de um tipo muito especial.

Definição 2.4. *Seja X um conjunto onde está definida uma relação, que denotaremos por $\equiv$. Esta é uma relação de equivalência se, quaisquer que sejam $x, y, z \in X$, as seguintes propriedades são satisfeitas:*

1. $x \equiv x$
2. *Se* $x \equiv y$ *então* $y \equiv x$
3. *Se* $x \equiv y$ *e* $y \equiv z$ *então* $x \equiv z$

A propriedade 1 chama-se propriedade reflexiva e nos diz apenas que se a relação é de equivalência então um elemento pode ser comparado a si próprio. É o caso, por exemplo, da igualdade dos inteiros. No entanto, a relação $<$ (estritamente menor) no conjunto dos inteiros não satisfaz esta propriedade.

A propriedade 2 chama-se simétrica. Mais uma vez a relação $<$ nos inteiros não a satisfaz; $5 < 7$, mas não é verdade que $7 < 5$. Observe ainda que a relação $\leq$ (menor ou igual) nos inteiros é reflexiva, mas não é simétrica.

A propriedade 3 chama-se transitiva. Tanto a igualdade, quanto as relações $<$ e $\leq$ nos inteiros são transitivas. Um exemplo de relação que não é transitiva é a relação $\neq$ (diferente) nos inteiros. De fato, temos que $5 \neq 7$ e $7 \neq 5$, mas não é verdade que $5 \neq 5$. Note que $\neq$ é simétrica, mas não é reflexiva.

Tencionamos dar exemplos onde alguma destas propriedades é falsa, porque esta é a única forma de entender o que realmente elas significam. Exemplos de relações de equivalência não faltam: igualdade nos inteiros, a relação **bolas de uma mesma cor** em um conjunto de bolas coloridas, a relação **mesmo número de lados** no conjunto dos polígonos, a relação **mesmo volume** no conjunto dos sólidos geométricos e assim por diante.

2.4 Classes de Equivalência

As relações de equivalência são usadas para classificar os elementos de um conjunto em subconjuntos com propriedades semelhantes. As subdivisões de um conjunto produzidas por uma relação de equivalência são conhecidas como classes de equivalência.

Definição 2.5. *Seja X um conjunto e $\equiv$ uma relação de equivalência definida em X. Se $x \in X$ então a classe de equivalência de x é o conjunto dos elementos de X que são equivalentes a x por $\equiv$. Denotando por $\overline{x}$ a classe de equivalência de x, temos em símbolos*

$$\overline{x} = [y \in X; y \equiv x]$$

Por exemplo, escolha uma bola azul em um conjunto B de bolas coloridas. A classe de equivalência desta bola pela relação bolas de uma mesma cor é o subconjunto das bolas azuis contidas no conjunto B.

Existe uma propriedade das classes de equivalência muito importante e vamos enunciá-la como um princípio: *qualquer elemento de uma classe de equivalência é um representante de toda a classe*. Ou seja, se conhecemos um elemento da classe podemos reconstruir a classe inteira. Imagine que, no exemplo das bolas coloridas, alguém nos diz que o subconjunto que temos diante de nós é uma classe de equivalência. Para saber que

classe é esta, basta tomar uma bola e ver qual a sua cor, isto é, com somente um elemento identificamos a classe inteira.

Para o conjunto X, o princípio acima nos diz que se y é um elemento da classe de x então as classes de x e y são iguais. Em símbolos, enunciamos a proposição:

Proposição 2.2. *Se $x \in X$ e $y \in \overline{x}$ então $\overline{x} = \overline{y}$.*

Demonstração. Podemos provar isto usando as propriedades das relações de equivalência. Se $y \in \overline{x}$, então, por definição, $y \equiv x$; e pela propriedade simétrica, $x \equiv y$. Mas se $z \in \overline{x}$ então também temos $z \equiv x$. Logo, pela propriedade transitiva $z \equiv y$. Portanto, $z \in \overline{y}$. Mostramos assim que $\overline{x} \subseteq \overline{y}$. Um argumento análogo mostra que $\overline{y} \subseteq \overline{x}$. ■

Considere as seguintes propriedades do conjunto X com a relação de equivalência $\equiv$:

1. X é a união de todas as classes de equivalência.

2. Duas classes de equivalência distintas não podem tem um elemento em comum.

A propriedade 1 segue do fato de que cada elemento pertence à sua própria classe de equivalência. A propriedade 2 segue do princípio enunciado acima.

O conjunto das classes de equivalência de $\equiv$ em X tem um nome especial, é chamado de conjunto quociente de X por $\equiv$. Observe que os elementos do conjunto quociente são subconjuntos de X, as classes de equivalência. Isto é, o conjunto quociente não é um subconjunto de X, mas sim do conjunto das partes de X. Lembre-se que o conjunto das partes de X é aquele cujos elementos são todos os subconjuntos de X.

2.5 Congruências

Vamos agora construir uma relação de equivalência no conjunto dos inteiros. Vamos escolher um número inteiro positivo, que estará fixado a partir deste momento. Chamemos de n este número. O número n será o módulo ou período da nossa construção. Diremos que, pulando de n em n, todos os inteiros são equivalentes; ou ainda, dois inteiros cuja diferença é um múltiplo de n são equivalentes. Formalmente, temos a seguinte definição:

Definição 2.6. *Seja $n > 0$. Diremos que dois inteiros a e b são congruentes módulo n se $a - b$ é múltiplo de n. Em outras palavras, a e b são congruentes módulo n, se os restos de sua divisão euclidiana por n são iguais, e escrevemos*

$$a \equiv b \mod n.$$

Quando a e b não são congruentes, diremos que eles são incongruentes módulo n. Nesse caso escrevemos $a \not\equiv b \mod n$.

Não podemos deixar de verificar que a congruência módulo n é uma relação de equivalência, para isso enunciamos a seguinte proposição:

Proposição 2.3. *Seja $n \in \mathbb{N}$. Para quaisquer $a, b, c \in \mathbb{Z}$, tem-se que*

(i) $a \equiv a \mod n$;

(ii) *se* $a \equiv b \mod n$, *então* $b \equiv a \mod n$;

(iii) *se* $a \equiv b \mod n$ *e* $b \equiv c \mod n$, *então* $a \equiv c \mod n$.

Demonstração. (i) Seja a um inteiro. Para mostrar que $a \equiv a \mod n$, temos que verificar, por definição, que a diferença $a - a$ é múltiplo de n. Mas isto é óbvio, pois 0 é múltiplo de qualquer inteiro.

(ii) Se $a \equiv b \mod n$, então $a - b$ é um múltiplo de n. Mas $b - a = -(a - b)$; logo $b - a$ também é múltiplo de n. Portanto, $b \equiv a \mod n$.

(iii) Suponhamos que $a \equiv b \mod n$ e $b \equiv c \mod n$, onde a, b e c são inteiros. A primeira congruência nos diz que $a-b$ é múltiplo de n; a segunda nos diz que $b-c$ é múltiplo de n. Somando múltiplos de n temos de volta múltiplos de n; logo $(a-b)+(b-c) = (a-c)$ é múltiplo de n. Portanto $a \equiv c \mod n$.

Assim, verificamos as três propriedades e podemos concluir que a congruência módulo n é uma relação de equivalência. ■

Observemos alguns exemplos numéricos para compreendermos melhor o que está sendo enunciado.

Exemplo 2.5. $15 \equiv 1 \mod 7$ *pois* $15 - 1 = 14$ *é múltiplo de* 7.

Exemplo 2.6. $6 \equiv 16 \mod 5$ *pois* 6 *e* 16 *deixam o mesmo resto na divisão por* 5.

A princípio, o conjunto que nos interessa é o conjunto quociente de $\mathbb{Z}$ pela relação de congruência módulo n. Este conjunto tem uma notação própria, $\mathbb{Z}_n$; e um nome especial, conjunto dos inteiros módulo n. Precisamos identificar os elementos de $\mathbb{Z}_n$. Sabemos, por definição, que são subconjuntos de $\mathbb{Z}$, as classes de equivalência da congruência módulo n. Seja $a \in \mathbb{Z}$. A classe de a é formada pelos $b \in \mathbb{Z}$ que satisfazem $b - a$ é múltiplo de n; isto é, $b - a = kn$, para algum $k \in \mathbb{Z}$. Podemos assim descrever a classe de a na forma

$$\overline{a} = \{a + kn; k \in \mathbb{Z}\}$$

Em particular $\overline{0}$ é o conjunto dos múltiplos de n. Isto produz uma situação curiosa. Se $a \in \mathbb{Z}$, então podemos dividi-lo por n, obtendo q e r inteiros tais que

$$a = nq + r \text{ e } 0 \leq r \leq n - 1.$$

Logo, $a - r = nq$ é um múltiplo de n. Portanto, $a \equiv r \mod n$. Isto é, um inteiro qualquer é congruente módulo n a um inteiro no intervalo que vai de 0 a $n - 1$. Em outras palavras, o conjunto quociente $\mathbb{Z}_n$ é formado pelas classes $\overline{0}, \overline{1}, \ldots \overline{n-1}$. Além disso, duas destas classes não podem ser iguais; a única maneira de dois números entre 0 e $n - 1$ serem congruentes módulo n é se forem iguais. Em suma, $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots \overline{n-1}\}$.

Quando uma classe de $\mathbb{Z}_n$ estiver representada na forma $\overline{a}$ com $0 \leq a \leq n - 1$, diremos que está na forma reduzida.

Para somar duas classes em $\mathbb{Z}_n$ fazemos da seguinte maneira: sejam $\overline{a}$ e $\overline{b}$ duas classes de $\mathbb{Z}_n$ que desejamos somar. A fórmula para a operação é a seguinte:

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

Chamamos a atenção para a interpretação correta desta fórmula. De um lado da igualdade temos a soma de duas classes; do outro lado temos a classe da soma de dois números inteiros. Assim definimos a operação soma de classes usando uma operação que já é nossa conhecida, a soma de inteiros. Tomemos um exemplo em $\mathbb{Z}_7$. De acordo com esta fórmula, para somar $\overline{6}$ a $\overline{4}$, somamos os inteiros 6 e 4, obtendo o resultado 10; logo $\overline{6} + \overline{4} = \overline{10}$. Como $10 - 3 = 7$ temos que 10 e 3 estão na mesma classe de equivalência módulo 7, isto é, $\overline{10} = \overline{3}$.

Note que isto que estamos observando aponta para um problema importante. Estamos definindo a soma de classes, que são subconjuntos de $\mathbb{Z}$, mas a soma foi definida usando um elemento de cada subconjunto. Quem nos garante que escolhendo elementos distintos de cada classe não obtemos um resultado diferente? Este é um ponto relativamente sutil, mas é essencial compreender o que está acontecendo. Observe que somamos as classes $\overline{6}$ e $\overline{4}$ usando os elementos 6 e 4. Mas $\overline{13} = \overline{6}$ e $\overline{11} = \overline{4}$. O que aconteceria se somássemos as classes $\overline{13}$ e $\overline{11}$? Se estamos mesmo somando as classes o resultado tem que dar $\overline{3}$. Lembre-se que estamos trabalhando em $\mathbb{Z}_7$. De acordo com a fórmula temos

$$\overline{13} + \overline{11} = \overline{24}.$$

Mas $24 - 3 = 21$ é múltiplo de 7, então $\overline{24} = \overline{3}$ e obtivemos o mesmo resultado.
Afirmação: Quaisquer que sejam os representantes escolhidos para efetuar a soma de duas classes, o resultado sempre é a mesma classe.

Demonstração. Suponha que em $\mathbb{Z}_n$ temos duas classes $\overline{a}$ e $\overline{b}$. Suponha ainda que $\overline{a} = \overline{a'}$ e $\overline{b} = \overline{b'}$. Queremos verificar que $\overline{a + b} = \overline{a' + b'}$.

Mas $\overline{a} = \overline{a'}$ é equivalente a dizer que $a - a'$ é múltiplo de n; analogamente, $\overline{b} = \overline{b'}$ é equivalente a dizer que $b - b'$ é múltiplo de n. Somando dois múltiplos de n temos um múltiplo de n, logo

$$(a - a') + (b - b') = (a + b) - (a' + b')$$

é múltiplo de n. Portanto, $\overline{a + b} = \overline{a' + b'}$, como queríamos mostrar. ■

Da mesma forma, a fórmula para a multiplicação das classes $\overline{a}$ e $\overline{b}$ de $\mathbb{Z}_n$ é

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

Analogamente à soma, temos que verificar que esta fórmula dá um resultado que não depende da escolha de representantes para as classes. Digamos que $\overline{a} = \overline{a'}$ e $\overline{b} = \overline{b'}$. Queremos mostrar que $\overline{a} \cdot \overline{b} = \overline{a' \cdot b'}$.

Mas $\overline{a} = \overline{a'}$, é equivalente a dizer que $a - a'$ é um múltiplo de n; digamos que $a = a' + tn$, para algum inteiro t. De forma análoga, $b = b' + qn$, para algum inteiro q. Multiplicando temos,

$$a \cdot b = (a' + tn)(b' + qn) = a'b' + (a'q + tb' + qtn)n.$$

Logo, $ab - a'b'$ é um múltiplo de n. Portanto, $\overline{a \cdot b} = \overline{a' \cdot b'}$, que é o que queríamos provar.

Tomemos um exemplo em $\mathbb{Z}_8$. As classes $\overline{2}$ e $\overline{4}$ são, evidentemente, diferentes da classe $\overline{0}$. No entanto,

$$\overline{2} \cdot \overline{4} = \overline{8} = \overline{0}.$$

Note que o produto de duas classes não nulas pode ser a classe $\overline{0}$. Vejamos uma aplicação destas ideias, mas antes enunciaremos um teorema muito importante para a resolução de congruências.

Teorema 2.3 (Pequeno Teorema de Fermat)**.** *Seja p um número primo e a um inteiro que não é divisível por p. Então, $a^{p-1} \equiv 1 \mod p$.*

Para a demonstração do teorema usaremos o lema a seguir.

Lema 2.2. *(Lei do Corte) Se $ax \equiv ay \mod n$ e $mdc(a, n) = 1$, então $x \equiv y \mod n$.*

Demonstração. Pela hipótese, temos que $\exists q \in \mathbb{Z}$, tal que

$$ax = nq + ay, \text{ daí } nq = ax - ay = a(x - y).$$

Assim, temos que $n \mid a(x - y)$, mas como o $mdc(a, n) = 1$, segue $n \mid (x - y)$, garantindo que $x \equiv y \mod n$. ■

Vamos à demonstração do teorema de Fermat.

Demonstração. Seja o conjunto de valores a, $2a$, $3a$, ..., $(p-1)a$. Sabemos que $mdc(a,p) = 1$, pelo fato de que p não divide a e, daí, nenhum dos números deste conjunto é divisível por p. Além disso, pelo lema 2.2 temos que, se $aj \equiv ak \mod p$, então $j \equiv k \mod p$ e, portanto, podemos estabelecer uma relação biunívoca entre os "aj", $j = 1, 2, \ldots, p-1$ e o conjunto $1, 2, \ldots, (p-1)$ em termos de congruência, isto é, cada um dos termos do primeiro conjunto é congruente a um diferente do segundo. Deste argumento, e da propriedade de que se $a \equiv b \mod m$, então $ac \equiv bc \mod m$, segue a seguinte equivalência:
$a \cdot (2a) \cdot (3a) \cdot \ldots \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \mod p$, ou seja,
$a^{p-1} \cdot (p-1)! \equiv (p-1)! \mod p \rightarrow a^{p-1} \cdot (p-1)! \equiv (p-1)! \cdot 1 \mod p$.

Como $mdc((p-1)!, p) = 1$, pelo lema 2.2 segue que $a^{p-1} \equiv 1 \mod p$. ■

Vejamos uma aplicação importante das congruências no cálculo de restos da divisão de uma potência por um número qualquer.

Exemplo 2.7. *Qual o resto da divisão de* 9^{57} *por* 7*?*

Sabemos pelo Teorema de Fermat que $9^6 \equiv 1 \mod 7$. Dividindo 57 por 6 temos $57 = 6 \cdot 9 + 3$. Temos então as seguintes congruências módulo 7

$$9^{57} \equiv (9^6)^9 \cdot 9^3 \equiv 1^9 \cdot 9^3 \equiv 9^3 \mod 7, \text{ mas } 9 \equiv 2 \mod 7, \text{ então } 9^3 \equiv 2^3 \equiv 8 \equiv 1 \mod 7.$$

Portanto, o resto da divisão de 9^{57} por 7 é 1.

2.6 Inverso Multiplicativo em $\mathbb{Z}_n$

Suponha que $\overline{a} \in \mathbb{Z}_n$. Diremos que a classe $\overline{\alpha} \in \mathbb{Z}_n$ é o inverso de $\overline{a}$ se a equação $\overline{a} \cdot \overline{\alpha} = \overline{1}$ é verificada em $\mathbb{Z}_n$. É óbvio que se $\overline{a} = \overline{0}$ então $\overline{a}$ não tem inverso. Cabe observar que em $\mathbb{Z}_n$ pode haver outros elementos sem inverso além da classe $\overline{0}$.

Suponhamos que $\overline{a} \in \mathbb{Z}_n$ tem inverso $\overline{\alpha}$. A equação $\overline{a} \cdot \overline{\alpha} = \overline{1}$ corresponde a dizer que $a\alpha - 1$ é divisível por n. Ou seja, $a\alpha + kn = 1$ para algum $k \in \mathbb{Z}$. Note que esta última equação implica que $mdc(a,n) = 1$. Concluímos então que se $\overline{a}$ tem inverso em $\mathbb{Z}_n$, então $mdc(a,n) = 1$. A recíproca é verdadeira.

Suponhamos que $a \in \mathbb{Z}$ e que $mdc(a,n) = 1$. A equação anterior sugere que apliquemos o algoritmo euclidiano estendido aos números a e n para obter inteiros α e k tais que $a\alpha + kn = 1$.

Esta equação é equivalente a $\overline{a} \cdot \overline{\alpha} = \overline{1}$ em $\mathbb{Z}_n$. Logo, a classe $\overline{\alpha}$ calculada pelo algoritmo euclidiano estendido é o inverso de $\overline{a}$ em $\mathbb{Z}_n$. Concluímos assim que se $mdc(a,n) = 1$ então $\overline{a}$ tem inverso em $\mathbb{Z}_n$. O próximo teorema resume isso que nós acabamos de ver.

Teorema 2.4. *A classe $\overline{a}$ tem inverso em $\mathbb{Z}_n$ se, e somente se, a e n são primos entre si.*

Demonstração. Encontrado em (6) pág. 83.

Exemplo 2.8. *Qual é o inverso de $\overline{3}$ em $\mathbb{Z}_7$?*

A primeira pergunta é se o inverso existe mesmo. Usando o algoritmo estendido de Euclides, não só descobrimos se o inverso existe, mas também qual é o inverso.

No exemplo, é óbvio que $mdc(3,7) = 1$, portanto o inverso existe. Aplicando o algoritmo estendido obtemos $3 \cdot 5 - 7 = 1$, que é equivalente a $\overline{3} \cdot \overline{5} = \overline{1}$ em $\mathbb{Z}_7$. Logo, $\overline{5}$ é o inverso de $\overline{3}$ em $\mathbb{Z}_7$. É claro que *qual é o inverso* e até mesmo sua existência depende de modo crucial do valor do módulo. Por exemplo, a classe $\overline{3}$ em $\mathbb{Z}_{27}$ não tem inverso.

O conjunto dos elementos de $\mathbb{Z}_n$ que tem inverso é muito importante. Vamos denotá-lo por $U(n)$. Em símbolos

$$U(n) = \{\overline{a} \in \mathbb{Z}_n; mdc(a,n) = 1\}.$$

Não temos dificuldade de calcular $U(p)$ quando p é um número primo. Neste caso $mdc(a,p) = 1$ significa que p não divide a. Mas se p não divide a então $\overline{a} \neq \overline{0}$. Portanto, quando p é primo, todas as classes diferente de $\overline{0}$ tem inverso. Assim

$$U(p) = \mathbb{Z}_p \setminus \{\overline{0}\}.$$

Mas isto vale apenas quando p é primo. O que acontece quando n é um número composto é ilustrado nos seguintes exemplos:

$$U(6) = \{\overline{1}, \overline{5}\} \text{ e } U(8) = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}.$$

Uma propriedade importante do conjunto $U(n)$ é que o produto de dois elementos de $U(n)$ é um elemento de $U(n)$. Outrossim, se $\overline{a}$ e $\overline{b}$ em $\mathbb{Z}_n$ tem inverso, então $\overline{a} \cdot \overline{b}$ também tem inverso em $\mathbb{Z}_n$. Digamos que $\overline{a}$ tem inverso $\overline{a'}$ e $\overline{b}$ tem inverso $\overline{b'}$ em $\mathbb{Z}_n$. O inverso de $\overline{a} \cdot \overline{b}$ será $\overline{b'} \cdot \overline{a'}$. A verificação é imediata

$$(\overline{a} \cdot \overline{b})(\overline{b'} \cdot \overline{a'}) = \overline{a} \cdot \overline{1} \cdot \overline{a'} = \overline{a} \cdot \overline{a'} \cdot \overline{1} = \overline{1} \cdot \overline{1} = \overline{1}.$$

Podemos usar o que vimos até agora para resolver congruências lineares em $\mathbb{Z}_n$. Uma congruência linear é uma equação do tipo

$$ax \equiv b \mod n,$$

onde $a, b \in \mathbb{Z}$. Um método para resolver uma equação deste tipo é multiplicar pelo inverso de $a \mod n$, mas isto só é possível se $mdc(a,n) = 1$. Digamos que esta última hipótese é satisfeita. Então existe $\alpha \in \mathbb{Z}$ tal que $\alpha \cdot a \equiv 1 \mod n$. Multiplicando a equação

$ax \equiv b \mod n$ por α, obtemos $\alpha \cdot ax \equiv \alpha \cdot b \mod n$. Como $\overline{\alpha}$ é o inverso de $\overline{a}$ em $\mathbb{Z}_n$ esta equação se reduz a

$$x \equiv \alpha \cdot b \mod n.$$

Exemplo 2.9. *Resolver a congruência* $4x \equiv 3 \mod 15$.

Ora, como $mdc(4, 15) = 1$ então existe $\alpha \in \mathbb{Z}$ tal que $4\alpha \equiv 1 \mod 15$. Como $4 \cdot 4 - 15 = 1$, o inverso de $\overline{4}$ é o próprio $\overline{4}$. Multiplicando a congruência por 4, temos

$$x \equiv 4 \cdot 3 \equiv 12 \mod 15.$$

Portanto, a solução da equação é $x \equiv 12 \mod 15$. De fato $4 \cdot 12 = 48 \equiv 3 \mod 15$.

2.7 Anéis e Grupos

Nesta seção trataremos acerca de anéis e grupos tendo em vista uma importante contribuição para o que iremos tratar sobre o tema proposto neste trabalho. Em se tratando de anel, iremos tratar, mais precisamente do anel $\mathbb{Z}_n$ relacionando-o com congruência módulo n.

2.7.1 Anéis

Definição 2.7. *Denominamos anel A um conjunto dotado de duas operações, adição e multiplicação, cujos elementos satisfazem as seguintes condições:*

1. *(Comutatividade da soma). Para todo $a, b \in A$, temos $a + b = b + a$.*
2. *(Associatividade da soma). Para todo $a, b, c \in A$, temos $(a + b) + c = a + (b + c)$.*
3. *(Elemento neutro da adição). Existe um elemento $0 \in A$ tal que $a + 0 = a$ para todo $a \in A$.*
4. *(Elemento simétrico). Se $a \in A$, então existe um elemento $b \in A$ tal que $a + b = 0$. (Notação: o simétrico de a será denotado $-a$.)*
5. *(Associatividade da multiplicação). Para todo $a, b, c \in A$, temos $(ab)c = a(bc)$.*
6. *(Distributividade da multiplicação). Para todo $a, b, c \in A$, temos $a(b + c) = ab + ac$ e $(b + c)a = ba + ca$.*

Observações:

1. A multiplicação não é, necessariamente, comutativa. Quando isso ocorrer A será denominado anel comutativo.

2. Um anel não necessita ter elemento neutro da multiplicação (chamado identidade do anel e denotado por 1). Caso isso ocorra, dizemos que A é um anel com unidade.

3. Os elementos de um anel A que possuem inverso multiplicativo são chamados invertíveis ou unidades de A (notação: $U(A) = \{x \in A \mid x \text{ é uma unidade de } A\}$). Note que não é necessário que os elementos de um anel tenham inversos multiplicativos. É fácil ver que os conjuntos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, M_m(\mathbb{Z})$ (matrizes $m \times m$ com entradas inteiras) e $\mathbb{Z}[x]$ (polinômios na variável x com coeficientes inteiros) - com a soma e o produto usuais - satisfazem a definição acima. Portanto, representam alguns exemplos de anéis.

Definição 2.8 (Divisor de zero)**.** *Um elemento não nulo a em um anel comutativo A é chamado um divisor de zero se existe um elemento não nulo b em A tal que $a \cdot b = 0$.*

Definição 2.9 (Domínio integral)**.** *Um anel comutativo com unidade é chamado de domínio integral ou simplesmente domínio se ele não tem divisor de zero. Assim, num domínio integral $a \cdot b = 0 \Leftrightarrow a = 0$ ou $b = 0$.*

Exemplo 2.10. *$\mathbb{Z}, \mathbb{Q}, \mathbb{C}, \mathbb{R}$ são domínios. $\mathbb{Z}_6$ não é um domínio, pois $\overline{2} \cdot \overline{3} = \overline{0}$ e $\overline{2}, \overline{3} \neq \overline{0}$.*

Definição 2.10 (Corpos)**.** *Um anel comutativo com unidade é chamado corpo se todo elemento não nulo é invertível.*

Exemplo 2.11. *Os conjuntos $\mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ são corpos.*

Proposição 2.4. *Todo corpo é um domínio.*

Demonstração. De fato, dados a e b pertencentes a um corpo com $a \neq 0$ e $a \cdot b = 0$, podemos multiplicar ambos os lados da última expressão por a^{-1} obtendo $b = 0$. ■

Observação: Nem todo domínio é um corpo. Se tomarmos o anel dos inteiros, observamos que $\mathbb{Z}$ é um domínio, mas não é um corpo. Pois, os únicos inversíveis em $\mathbb{Z}$ são 1 e -1.

2.7.1.1 O Anel $\mathbb{Z}_n$

Sendo n um inteiro positivo, sabemos que $n\mathbb{Z} = \{na \mid a \in \mathbb{Z}\}$ é um ideal de $\mathbb{Z}$, esse fato nos permite definir o anel $\mathbb{Z}/n\mathbb{Z} = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, n - 1 + n\mathbb{Z}\}$, com as operações:

$$(a + n\mathbb{Z}) + (b + n\mathbb{Z}) = (a + b) + n\mathbb{Z} \text{ e } (a + n\mathbb{Z})(b + n\mathbb{Z}) = (ab) + n\mathbb{Z}.$$

Esse anel é comutativo, pois $\mathbb{Z}$ o é, com unidade $1 + n\mathbb{Z}$. Com o objetivo de simplificarmos a notação, representaremos $\mathbb{Z}/n\mathbb{Z}$ por $\mathbb{Z}_n$ e $a + n\mathbb{Z}$ por $\overline{a}$, ou simplesmente a. Note que podemos relacionar o anel $\mathbb{Z}/n\mathbb{Z}$ com congruência módulo n. Dessa forma, o anel quociente $\mathbb{Z}/n\mathbb{Z}$ será denotado por $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ com as operações: $\overline{a} + \overline{b} = \overline{a + b}$

e $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$. Nem todos os elementos de $\mathbb{Z}_n$ possuem inverso multiplicativo. Por exemplo, em $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$ não existe nenhuma classe $\overline{a}$ tal que $\overline{a} \cdot \overline{2} = \overline{1}$.

Proposição 2.5. *$\mathbb{Z}_n$ é corpo se, e somente se n é primo.*

Demonstração. Suponha, por absurdo, que $\mathbb{Z}_n$ é corpo e $n = xy$ com $x, y \in \mathbb{Z}$ tais que $0 < x, y < n$. Dessa forma, $\overline{xy} = \overline{0}$ donde $\overline{x} = \overline{0}$ ou $\overline{y} = \overline{0}$, pois $\mathbb{Z}_n$ é corpo, isto é, domínio. Assim, $n|x$ ou $n|y$, o que é um absurdo. Logo n é primo. Por outro lado, se n é primo, então $\forall \overline{a} \in \mathbb{Z}_n \setminus \{\overline{0}\}$ temos que $mdc(n, a) = 1$. Temos, assim, $ax + ny = 1$. Usando classes de equivalência, $\overline{ax + ny} = \overline{1} \Rightarrow \overline{ax} = \overline{1}$, donde $\overline{a} \cdot \overline{x} = \overline{1}$. Assim, $\overline{a}$ possui inverso, ou seja, $\mathbb{Z}_n$ é corpo. ■

2.7.2 Grupos

Chamamos de grupo um conjunto G munido de uma operação $*$ definida neste conjunto, satisfazendo algumas propriedades. Por operação estamos entendendo uma regra que a cada dois elementos $a, b \in G$ associa um terceiro elemento $a * b$ que também está em G.

A associação **conjunto e operação** é extremamente comum em matemática. Como exemplos podemos observar os números naturais e a soma, os inteiros e a soma, os inteiros e o produto, os racionais e a soma, os racionais e o produto, os vetores no espaço e o produto vetorial e muitos mais.

Mas note que nem toda associação **conjunto e operação** constitui um grupo. Para termos um grupo é necessário que a operação satisfaça algumas propriedades. A seguir, uma definição mais formal.

Definição 2.11. *Um conjunto G onde está definida uma operação $*$ é um grupo se a operação satisfaz as seguintes propriedades:*

1. *Associatividade: dados $a, b, c \in G$ temos que $a * (b * c) = (a * b) * c$.*
2. *Elemento neutro: existe um elemento $e \in G$ tal que para todo $a \in G$ temos $a * e = e * a = a$.*
3. *Elemento inverso: dado um elemento $a \in G$ qualquer, existe um elemento $a' \in G$ tal que $a * a' = a' * a = e$.*

Se além dessas condições ainda tivermos que para todo $a, b \in G$, $a * b = b * a$, ou seja, a operação é comutativa, então $(G, *)$ é um grupo abeliano.

Existem muitos exemplos importantes da associação **conjunto e operação** que não satisfazem as propriedades acima e, portanto não são grupos. Como exemplo temos a soma de números naturais que é associativa e tem elemento neutro (o zero), no entanto, o

único natural a ter inverso para a soma é o zero. Outro exemplo: o conjunto dos vetores no espaço com o produto vetorial não satisfaz sequer a propriedade associativa.

Observe que os inteiros, racionais, reais e complexos são grupos para a soma. Os racionais, reais e complexos não nulos são grupos para o produto. O conjunto $\mathbb{Z}_n$ com a soma é um grupo, para qualquer $n \in \mathbb{Z}_+^*$.

O número de elementos de um grupo é a sua ordem. A maior parte dos grupos mencionados anteriormente tem ordem infinita. O único exemplo de grupo finito que vimos foi $\mathbb{Z}_n$ com a soma; este grupo tem ordem n. Um outro grupo finito fácil de descrever é $\{-1, 1\}$ com a operação de produto de inteiros; neste caso a ordem é 2.

2.7.2.1 Grupos Aritméticos

Anteriormente comentamos sobre $U(n)$, o conjunto dos elementos inversíveis de $\mathbb{Z}_n$. Ou seja, $U(n) = \{\overline{a} \in \mathbb{Z}_n; mdc(a, n) = 1\}$. Este conjunto é um grupo para a operação de multiplicação de classes de $\mathbb{Z}_n$.

Ora, sabemos que o produto de dois elementos de $\mathbb{Z}_n$ é um elemento de $\mathbb{Z}_n$, mas nada nos garante que isto também vale para $U(n)$. Isto é, precisamos saber se, quando multiplicamos dois elementos de $U(n)$, o resultado ainda é um elemento de $U(n)$ - caso contrário não temos uma operação em $U(n)$.

De outra forma, precisamos verificar que o produto de dois elementos inversíveis de $\mathbb{Z}_n$ é um elemento inversível de $\mathbb{Z}_n$. Já fizemos isso em seções anteriores e vamos repeti-lo aqui.

Digamos que $\overline{a}$ e $\overline{b}$ são elementos de $U(n)$ e que seus inversos são $\overline{a}'$ e $\overline{b}'$, respectivamente. Então, $\overline{ab}$ é inversível e seu inverso é $\overline{a'b'}$, como é fácil verificar multiplicando estes dois elementos

$$\overline{ab} \cdot \overline{a'b'} = \overline{aa'} \cdot \overline{bb'} = 1.$$

Daí, temos um conjunto $U(n)$, onde está definida uma operação, o produto de classes. Temos que verificar que esta operação satisfaz as propriedades requeridas. A associatividade é fácil verificar, pois já sabemos que o produto em $\mathbb{Z}_n$ é associativo. O elemento neutro é 1, que é inversível em $\mathbb{Z}_n$, e portanto está em $U(n)$. É consequência da própria definição de $U(n)$ que cada elemento de $U(n)$ tem inverso. Portanto, o conjunto $U(n)$ é um grupo para o produto de classes.

Agora será importante determinar a ordem de $U(n)$, tendo em vista as aplicações que virão a seguir. Começamos definindo a função ϕ que, a cada número inteiro positivo n, associa um outro inteiro positivo, a ordem de $U(n)$. Esta é a função ϕ de Euler. Assim, a ordem de $U(n)$ é denotada por $\phi(n)$. Vejamos como calcular ϕ.

Seja p um número primo, então todos os inteiros positivos menores que p são primos com p. Logo, $U(p) = \mathbb{Z}_p \setminus \{\overline{0}\}$ tem $p-1$ elementos. Portanto, $\phi(p) = p-1$.

Também não é difícil calcular $\phi(p^k)$. Para isto temos que contar os inteiros positivos menores que p^k cujo máximo divisor comum com p^k é 1. Mas $mdc(a, p^k) = 1$ significa que p não divide a. Então, basta contar os inteiros positivos menores que p^k que não são divisíveis por p. De fato é mais fácil contar aqueles que são divisíveis. Se a é divisível por p com $0 \leq a < p^k$, então $a = p \cdot b$ para algum $b \in \mathbb{Z}$ e $0 \leq b < p^{k-1}$.

Portanto, há p^{k-1} inteiros positivos menores que p^k que são divisíveis por p. Logo, há $p^k - p^{k-1}$ que não são divisíveis por p. Isto é,

$$\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1).$$

O próximo teorema nos ajuda a encontrar ϕ do produto de dois números primos entre si.

Teorema 2.5. *Se m, n são inteiros positivos tais que $mdc(m, n) = 1$, então $\phi(mn) = \phi(m) \cdot \phi(n)$.*

Antes de demonstrarmos, enunciaremos o Teorema Chinês do Resto, útil em nossa demonstração.

Teorema 2.6 (Teorema Chinês do Resto)**.** *Sejam $n_1, n_2, \cdot n_k$ inteiros positivos dois a dois primos entre si. Então o sistema*

$x \equiv a_1 \mod n_1$

$x \equiv a_2 \mod n_2$

$\vdots$

$x \equiv a_k \mod n_k$

tem solução única em $\mathbb{Z}_{n_1 \ldots n_k}$.

Demonstração. encontrado em (8).

Vamos à demonstração do Teorema 2.5.

Demonstração. (Encontrado em (6)) Para provar isto usaremos o teorema chinês do resto interpretado em forma de tabela. Temos dois inteiros positivos m, n que satisfazem $mdc(m, n) = 1$. Escrevemos na horizontal os números de 0 a $m-1$ e na vertical de 0 a $n-1$. Assim, a tabela tem $m \cdot n$ casas, cada uma endereçada por dois números a, b, onde $0 \leq a \leq m-1$ e $0 \leq b \leq n-1$. Vamos preencher a casa a, b da tabela com o inteiro x entre 0 e $mn-1$ que satisfaz

$$x \equiv a \mod m$$
$$x \equiv b \mod n$$

Consideremos a tabela

$$\begin{array}{cccccc} linha\,1 & 1 & m+1 & 2m+1 & \dots & (n-1)m+1 \\ linha\,2 & 2 & m+2 & 2m+2 & \dots & (n-1)m+2 \\ linha\,3 & 3 & m+3 & 2m+3 & \dots & (n-1)m+3 \\ \vdots & \vdots & \vdots & \vdots & \dots & \vdots \\ linha\,m & m & 2m & 3m & \dots & nm \end{array}$$

De acordo com o teorema chinês do resto, cada casa é preenchida por exatamente um número entre 0 e $mn-1$. Assim não há casas em branco, e nenhum número aparece repetido. Usando a notação acima, vamos dizer que o número x da tabela tem coordenadas (a,b).

Digamos que $\overline{x} \in \mathbb{Z}_{mn}$, onde $0 \leq x \leq mn-1$. Sejam a e b as coordenadas de x na tabela. Vamos começar mostrando a seguinte afirmação:
Afirmação: $\overline{x} \in U(mn)$ se, e somente se, $\overline{a} \in U(m)$ e $\overline{b} \in U(n)$.

É fácil ver que se $\overline{x} \in U(mn)$ então $\overline{a} \in U(m)$ e $\overline{b} \in U(n)$. De fato, se $\overline{x} \in U(mn)$ tem inverso $\overline{x'} \in U(mn)$, então $xx' \equiv 1 \mod mn$. Portanto, $xx'-1$ é divisível por mn. Em particular, $xx'-1$ é divisível por m; donde $xx' \equiv 1 \mod m$. De $x \equiv a \mod m$ concluímos que $ax' \equiv 1 \mod m$; logo, $\overline{a}$ é inversível em $\mathbb{Z}_m$. A demonstração de que $\overline{b} \in U(n)$ é análoga.

Vejamos como provar a recíproca. Seja $\overline{x}$ um elemento de $\mathbb{Z}_{mn}$, e suponhamos que suas coordenadas satisfazem $\overline{a} \in U(m)$ e $\overline{b} \in U(n)$. Queremos mostrar que $\overline{x}$ é inversível módulo mn. Seja $\overline{a'}$ o inverso de $\overline{a}$ em $\mathbb{Z}_m$ e $\overline{b'}$ o inverso de $\overline{b}$ em $\mathbb{Z}_n$. O inverso de $\overline{x}$, se existir, deve ocupar alguma posição na tabela. Pelo teorema chinês do resto, tem que existir um inteiro y tal que $0 \leq y \leq mn-1$ e

$$\begin{aligned} y &\equiv a' \mod m \\ y &\equiv b' \mod n \end{aligned}$$

Vamos mostrar que $\overline{y} \in \mathbb{Z}_{mn}$ é o inverso de $\overline{x}$. Como $x \equiv a \mod m$ e $y \equiv a' \mod m$, temos que, $xy = aa' = 1 \mod m$. Logo, $xy-1$ é divisível por m. Um argumento análogo mostra que $xy-1$ é divisível por n. Como $mdc(m,n)=1$ podemos concluir, que $xy-1$ é divisível por mn. Isto é, $\overline{x} \cdot \overline{y} = \overline{1}$ em $\mathbb{Z}_{mn}$, como queríamos mostrar. Provamos assim a afirmação feita anteriormente.

Usando a afirmação fica fácil provar o teorema. Queremos calcular $\phi(mn)$. Por definição, isto é o número de elementos de $U(mn)$. Portanto, usando a afirmação anterior, o que queremos é contar o número de casas da tabela cujas coordenadas estão, respectivamente, em $U(m)$ e $U(n)$. Mas este número é igual ao produto do número de elementos de $U(m)$ pelo número de elementos de $U(n)$, que é $\phi(m) \cdot \phi(n)$. Portanto $\phi(mn) = \phi(m) \cdot \phi(n)$.
■

Definição 2.12. *Seja G um grupo multiplicativo. Dado $a \in G$, define-se potência m-ésima de a, para todo inteiro m, da seguinte maneira:*

- *se $m \geq 0$, por recorrência da seguinte forma*
  $a^0 = e$ (elemento neutro de G)
  $a^m = a^{m-1}a$, se $m > 1$
- *se $m < 0$, $a^m = (a^{-m})^{-1}$.*

Proposição 2.6. *Seja G um grupo multiplicativo. Se m e n são números inteiros e $a \in G$, então:*

1. $a^m a^n = a^{m+n}$;
2. $a^{-m} = (a^m)^{-1}$;
3. $(a^m)^n = a^{mn}$.

Demonstração. 1. Inicialmente vamos demonstrar por indução sobre n o caso particular, em que $n \geq 0$ e $m + n \geq 0$. De fato, $n = 0 \Rightarrow a^m a^n = a^m a^0 = a^m e = a^m = a^{m+0} = a^{m+n}$. Logo, a propriedade é válida quando $n = 0$.

Agora, seja $r \geq 0$ e suponhamos que, para qualquer inteiro m tal que $m + r \geq 0$, seja válida a igualdade $a^{m+r} = a^m a^r$, então:

$a^m a^{r+1} = a^m(a^r a) = (a^m a^r)a = a^{m+r}a = a^{(m+r)+1} = a^{m+(r+1)}$.

Suponhamos agora que m e n são dois inteiros quaisquer. Tomemos um número inteiro $p > 0$ tal que $p + m > 0$, $p + n > 0$ e $p + m + n > 0$. Então, observando que $a^p a^{-p} = a^p(a^p)^{-1} = e$ (como consequência da definição) temos:

$a^{m+n} = a^{m+n}(a^p a^{-p}) = (a^{m+n}a^p)a^{-p} = a^{(m+n)+p}a^{-p} = a^{m+(n+p)}a^{-p}$.

Observe que na terceira igualdade acima foi usada a primeira parte da demonstração. Aplicando novamente o resultado da primeira parte temos:

$a^{m+(n+p)}a^{-p} = (a^m(a^n a^p))a^{-p} = ((a^m a^n)a^p)a^{-p} = (a^m a^n)(a^p a^{-p}) = (a^m a^n)e = a^m a^n$.

2. Note que devido ao primeiro item, $a^{-m}a^m = a^{(-m)+m} = a^0 = e$. De modo análogo, $a^m a^{-m} = e$; logo, cada uma dessas potências é inversa da outra , ou seja, $a^{-m} = (a^m)^{-1}$. Como queríamos demonstrar nesse item.

3. Vamos provar por indução o caso em que $n \geq 0$. Para $n = 0$, temos: $(a^m)^0 = e = a^0 = a^{m\cdot 0}$. Vamos supor que exista $r \geq 0$ que satisfaça $(a^m)^r = a^{mr}$, vamos mostrar que é válida a igualdade $(a^m)^{r+1} = a^{m(r+1)}$.

De fato, $(a^m)^{r+1} = (a^m)^r(a^m)^1 = a^{mr}a^m = a^{mr+m} = a^{m(r+1)}$ e, por fim, vamos supor que $n < 0$. Assim, por definição, $(a^m)^n = [(a^m)^{-n}]^{-1} = (a^{-mn})^{-1}$ e, pelo item anterior temos que $(a^{-mn})^{-1} = a^{mn}$. ■

2.7.2.2 Subgrupos Cíclicos

Definição 2.13. *Seja G um grupo com a operação $*$. Um subconjunto não vazio H de G é um subgrupo de G se:*

1. *Para todo $a \in H$ temos que $a * b \in H$.*
2. *O elemento neutro de G está em H.*
3. *Para todo $a \in H$, seu inverso a' também está em H.*

Seja G um grupo finito com uma operação $*$ e seja a um elemento de G. Consideremos o conjunto das potências de a

$$H = \{e, a, a^2, a^3, \ldots\}.$$

Note que, aparentemente, trata-se de um conjunto infinito. Aparentemente, porque $H \subseteq G$, que é um conjunto finito. Logo, H também tem que ser finito. Mas isto significa que potências muito grandes de a vão ter que ser iguais a potências menores. Assim vão existir inteiros positivos $n > m$, tais que $a^m = a^n$. Seja a' o inverso de a em G. Multiplicando esta equação por $(a')^m$, obtemos $a^{n-m} = e$, o elemento neutro. Concluímos duas coisas importantes:

1. Dado um elemento qualquer $a \in G$ existe um inteiro positivo k tal que $a^k = e$.
2. Se $a^k = e$, então o inverso de a é a^{k-1}, uma potência de a. Logo, o inverso de a pertence a H.

Em particular temos que H é um subgrupo de G. Qual a ordem de H? Digamos que k é o menor inteiro positivo tal que $a^k = e$. Se $n > k$, então podemos dividir n por k, obtendo $n = k \cdot q + r$, onde $0 \leq r \leq k - 1$. Então

$$a^n = a^{k \cdot q + r} = a^{k \cdot q} * a^r.$$

Como $a^k = e$, segue-se que $a^n = a^r$. Concluímos que não precisamos nos preocupar com as potências de a com expoente maior que $k - 1$, porque são iguais a outras potências, de expoentes menores. Logo,

$$H = \{e, a, a^2, a^3, \ldots, a^{k-1}\}.$$

Além disso, todos estes elementos são distintos. De fato, se $r \leq s < k$ e $a^r = a^s$, então $a^{s-r} = e$. Como $s - r < k$, que é a ordem de a, temos que $s - r = 0$; ou seja, $r = s$. Portanto, dois elementos do conjunto acima são iguais se, e só se, correspondem a potências com os mesmos expoentes. Assim, a ordem de H é k. Com isto temos um método simples para construir subgrupos de G. Dado um grupo finito G, escolha $a \in G$ diferente do elemento neutro e, então:

1. O conjunto H formado pelas potências de a em G é um subgrupo.

2. A ordem de H é igual ao menor inteiro positivo k tal que $a^k = e$.

Vamos, de forma conveniente, introduzir a seguinte terminologia. Se o subgrupo H é igual ao conjunto das potências de um elemento a, diremos que a é um gerador de H. O menor inteiro positivo k tal que $a^k = e$ é a ordem de a. Usaremos a notação $\text{ord}_n\, a = k$ para significar que k é a ordem de a módulo n. Portanto, se H tem a como gerador então a ordem de H (isto é, o número de elementos de H) é igual a ordem de a. Um subgrupo que admite um elemento gerador é chamado de cíclico.

2.8 Raiz Primitiva

Definição 2.14. *Sejam $n, a \in \mathbb{Z}$ com $n > 0$ e $mdc(a, n) = 1$. Dizemos que a é uma raiz primitiva módulo n se* $\text{ord}_n\, a = \phi(n)$.

Seja $p > 3$ um número primo. A ordem de $U(p)$ é $\phi(p) = p - 1$, um número par e composto; mesmo assim o grupo $U(p)$ é cíclico. Este resultado é conhecido como teorema da raiz primitiva. Uma raiz primitiva é o mesmo que um gerador de $U(p)$.

O nome raiz primitiva justifica-se pelo fato de que todos os elementos de $U(p)$ são raízes da equação $x^{p-1} - \overline{1} = \overline{0}$ em $\mathbb{Z}_p$. Um gerador de $U(p)$ é uma raiz primitiva porque obtemos as outras raízes da equação como potências da raiz primitiva.

Teorema 2.7 (Teorema da raiz primitiva)**.** *Se p é primo então o grupo $U(p)$ é cíclico.*

Na demonstração vamos utilizar o teorema a seguir.

Teorema 2.8. *Seja $f(x)$ um polinômio de grau k com coeficientes inteiros e coeficiente líder 1. Se p é um número primo, então $f(x)$ não pode ter mais de k raízes distintas em $\mathbb{Z}_p$.*

Demonstração. Encontrado em (6) pág. 97.

Lema 2.3. *Digamos que G é um grupo finito munido de uma operação $*$. Seja $a \in G$. Um inteiro positivo t satisfaz $a^t = e$ se, e somente se, t é divisível pela ordem de a.*

Demonstração. Encontrado em (6) pág. 156.

Lema 2.4. *Seja G um grupo abeliano finito munido de uma operação $*$. Se G tem elementos de ordens r e s, então G tem um elemento cuja ordem é igual ao mínimo múltiplo comum entre r e s.*

Demonstração. Encontrado em (6) pág 173.

Vamos à demonstração do Teorema da raiz primitiva.

Demonstração. Podemos supor que $p \geq 5$, já que o teorema é obviamente verdadeiro quando $p = 2$ ou $p = 3$. Escolha um elemento qualquer $\overline{a_1} \in U(p)$, onde $1 < a_1 < p - 1$. Podemos sempre começar escolhendo $a_1 = 2$. Seja k_1 a ordem de $\overline{a_1}$. Se $k_1 = p - 1$, então já encontramos um elemento que gera $U(p)$. Logo, $U(p)$ é cíclico. Suponha, então, que $k_1 < p - 1$. Temos que a_1 é uma das soluções em $\mathbb{Z}_p$ da equação $x^{k_1} - 1 = 0$. Como p é primo, pelo teorema 2.8 esta equação não pode ter mais de k_1 soluções distintas. Por outro lado, os elementos de

$$H = \{\overline{1}, \overline{a_1}, \overline{a_1}^2, \ldots, \overline{a_1}^{k_1 - 1}\}$$

são soluções de $x^{k_1} - 1 = 0$. Como H contém k_1 elementos distintos, então tem que conter todas as soluções de $x^{k_1} - 1 = 0$. Mas $k_1 < p - 1$, logo existe um elemento $\overline{b} \in U(p)$ que não pertence a H. Em particular $\overline{b}$ não é uma solução de $x^{k_1} - 1 = 0$. Assim, pelo lema 2.3 concluímos que a ordem de $\overline{b}$ não pode dividir k_1.

Seja r a ordem de $\overline{b}$. Há dois casos a considerar. Se $r = p - 1$, então $\overline{b}$ é um gerador de $U(p)$, e obtivemos o resultado desejado. Seja, então, $r < p - 1$. Pelo lema 2.4 concluímos que existe um elemento $\overline{a_2}$ que tem ordem k_2 igual ao mínimo múltiplo comum entre k_1 e r.

Como r não divide k_1, temos que $k_2 > k_1$. Continuando assim, ou obtemos um elemento de ordem $p - 1$, como queremos; ou construímos uma sequência estritamente crescente de inteiros positivos $k_1 < k_2 < k_3 < \ldots$ onde cada um destes números é a ordem de um elemento de $U(p)$. Em particular, cada inteiro desta sequência divide $p - 1$; portanto tem que ser menor ou igual a $p - 1$. Logo a sequência tem que parar, produzindo assim o gerador desejado para $U(p)$. ■

Observe que este método produz, de maneira sistemática, um gerador para $U(p)$, mas nem sempre produz o menor gerador. Observe também que a recíproca do teorema é falsa; por exemplo, $U(4)$ é cíclico. Com isso observamos que não basta que $U(n)$ seja

cíclico para que n seja primo. Na verdade, $U(n)$ é cíclico se, e somente se, n é igual a $1, 2, 4, p^k$ ou $2p^k$, onde p é um primo ímpar qualquer.

3 Representação dos Números Naturais

Ao escrever números naturais, geralmente escrevemos utilizando o sistema de numeração de base 10 ou sistema decimal. O sistema de numeração decimal é um sistema posicional, isto é, adota o princípio do valor posicional, diferentemente de outros sistemas de numeração, como o sistema de numeração romano. Nos primeiros sistemas numéricos, como os romanos, um algarismo tem apenas um valor: I significa um, V significa cinco, X significa dez e C cem (no entanto, o valor pode ser negado se colocado antes de outro algarismo). Em sistemas posicionais modernos, como o sistema decimal, a posição do algarismo significa que seu valor deve ser multiplicado por algum valor; no número 444 na base 10, por exemplo, os três símbolos idênticos representam quatro centenas, quatro dezenas e quatro unidades, respectivamente, devido a suas posições diferentes na sequência de dígitos.

Note que em 312, o primeiro algarismo representa 300, o segundo algarismo representa 10 e o terceiro representa 2 no sistema decimal, enquanto que em VII (sete em numeração romana) os dois I significam ambos 1. Daí, temos:

$$312 = 300 + 10 + 2 = 3 \cdot 100 + 1 \cdot 10 + 2 = 3 \cdot 10^2 + 1 \cdot 10^1 + 2 \cdot 10^0$$

No sistema de numeração decimal, utilizamos os algarismos $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$, ou seja, 10 algarismos que fazem jus ao nome decimal.

Num sistema de numeração de uma base qualquer, utilizamos os algarismos $0, 1, 2, 3, \ldots, b-1$, ou seja, b algarismos. Da mesma forma como acontece na base 10, o uso de um ponto basimal estende-se para incluir frações, permitindo representar os números reais em uma base arbitrária.

3.1 Existência e Unicidade da escrita

Observaremos aqui que todo número natural pode ser escrito em uma base $b \neq 1$, b qualquer, também natural e que essa escrita é única. Assim estaremos, ao mesmo tempo, representando os números naturais em uma base arbitrária.

Teorema 3.1. *Sejam $b, n \in \mathbb{N}$. Então existem naturais $a_0, a_1, \ldots, a_k$, univocamente determinados por b, n satisfazendo $0 \leq a_i < b$ para $i = 0, 1, \ldots, k$, $a_k \neq 0$ tais que*

$$n = a_k b^k + \ldots + a_1 b + a_0.$$

Além disso, os a_i podem ser efetivamente obtidos a partir de b e n.

Demonstração. Existência. Se $0 < n < b$, faça $k = 0$ e $a_0 = n$. Se $n > b$, utilizando o algoritmo de Euclides, divida n por b, obtendo $n = bq_0 + a_0, 0 \leq a_0 < b$. Se $q_0 < b$, então o resultado está provado fazendo $a_1 = q_0$, caso contrário, divida q_0 por b obtendo $q_0 = bq_1 + a_1$ com $0 \leq a_1 < b$ e $n = b^2q_1 + ba_1 + a_0$. Se $q_1 < b$, então o resultado está provado fazendo $a_2 = q_1$. Indutivamente, sempre que $q_{t-1} \geq b$, divida-o por b obtendo $q_{t-1} = bq_t + a_t$, com $0 \leq a_t < b$. Substituindo em n vamos obter

$$n = q_t b^t + a_{t-1}b^{t-1} + \ldots + a_2b^2 + a_1b + a_0.$$

Como a sequência dos coeficientes é uma sequência decrescente de números naturais, o algoritmo não é infinito, isto é, existe $k \in \mathbb{N}$ tal que $q_k < b$. Faça $a_k = q_k$ e, assim, obtemos a expressão desejada.

Unicidade. Suponhamos que n pudesse ser escrito de duas formas,

$$c_t b^t + \ldots + c_1 b + c_0 = n = a_k b^k + \ldots + a_t b^t + a_{t-1}b^{t-1} + a_1 b + a_0,$$

com $k \geq t$. Supondo $a_0 \geq c_0$ teríamos $0 \leq a_0 - c_0 < b$ e sendo múltiplo de b, necessariamente $a_0 = c_0$. Subtraindo a_0, dividindo por b e usando o mesmo argumento mostraríamos que $a_1 = c_1$, $a_2 = c_2, \ldots, a_k = c_k$. Se $k > t$, então teríamos $a_k b^k + \ldots + a_{t+1}b^{t+1} = 0$, o que é um absurdo, pois o lado direito é positivo. ■

Exemplo 3.1. *O número* $(5430)_6$*, que está representado na base* 6*, na base* 10 *corresponde à*

$$5 \times 6^3 + 4 \times 6^2 + 3 \times 6^1 + 0 = 1080 + 144 + 18 + 0 = 1242.$$

Exemplo 3.2. *Para converter o número* 4936 *da base* 10 *para a base* 4 *devemos proceder conforme o algoritmo descrito na demonstração do Teorema, isto é, fazendo divisões sucessivas por* 4*. Temos que* $4936 = 1234 \times 4 + 0$*, então o último algarismo da representação na base* 4 *será* 0*. Como* $1234 = 4 \times 308 + 2$*, o penúltimo algarismo será* 2*. Como* $308 = 77 \times 4 + 0$*, o ante-penúltimo algarismo será* 0*. Continuando com essas divisões sucessivas temos* $77 = 19 \times 4 + 1$ *e o próximo algarismo a ser escrito será* 1*. Como* $19 = 4 \times 4 + 3$*, o próximo algarismo a ser escrito será* 3*. Finalmente,* $4 = 4 \times 1 + 0$ *e os dois primeiros algarismos serão* 1 *e* 0*. Portanto,*

$$4936 = (1031020)_4$$

3.2 Conversão entre bases

Nos exemplos anteriores fizemos conversão entre base 10 e outras bases. De maneira geral, se queremos converter um número da base 10 para uma base b qualquer, fazemos divisões sucessivas por b e tomamos os restos da divisão que representa o número na nova base. Se queremos converter de uma base b qualquer para a base 10 escrevemos cada algarismo multiplicado pela base b, elevado à posição que ocupa. A soma de cada multiplicação de cada algarismo pelo valor das potências resulta no número desejado. Por exemplo, para $b \geq 10$ temos

$$(1597)_b = 1 \times b^3 + 5 \times b^2 + 9 \times b^1 + 7 \times b^0.$$

Se quisermos converter um número na base b diferente de 10 para outra base qualquer, o ideal é que façamos a mudança primeiro para a base 10 para depois converter para a outra base.

Exemplo 3.3. *Converter o número* $(2102)_3$ *da base* 3 *para a base* 7.

Primeiro fazemos a conversão para a base 10, conforme vimos anteriormente:

$$(2102)_3 = 2 \times 3^3 + 1 \times 3^2 + 0 \times 3^1 + 2 \times 3^0 = 54 + 9 + 0 + 2 = (65)_{10}.$$

Agora fazemos a conversão para a base 7, fazendo divisões sucessivas e anotando os restos.
$65 = 9 \times 7 + 2$
$9 = 1 \times 7 + 2$
$1 = 0 \times 7 + 1$
Logo, $(65)_{10} = (122)_7$ e, portanto, $(2102)_3 = (122)_7$.

Há um caso especialmente simples de mudança entre bases distintas de 10, que é quando uma das bases é uma potência da outra, neste caso, a ordem da potência funciona como o tamanho dos blocos. Inicialmente vamos exemplificar utilizando as bases 2 e 16 que são de extrema importância na informática. Os computadores geralmente utilizam o byte como unidade básica da memória. Ora, 1 byte = 8 bits, então um byte pode ser representado por 8 algarismos do sistema binário ou por 2 algarismos do sistema hexadecimal. Os algarismos utilizados na base 2 são 0 e 1, e os utilizados na base 16 são $0, 1, \ldots 9, A, B, C, D, E, F$, em que $A = 10, B = 11, C = 12, D = 13, E = 14$ e $F = 15$.

Exemplo 3.4. *Considere o número* $(10010010111)_2$ *na base* 2. *Vamos convertê-lo para a base* 16. *Como* $16 = 2^4$, *então cada dígito da base* 16 *equivale a* 4 *dígitos na base* 2, *daí separamos em blocos de* 4 *algarismos da direita para a esquerda. Quando um bloco tem menos de* 4 *algarismos, completamos com zeros à esquerda. Então obtemos* $([0100][1001][0111])_2$. *Como* $(0100)_2 = 4$, $(1001)_2 = 9$ *e* $(0111)_2 = 7$, *temos*

$$(10010010111)_2 = (497)_{16}.$$

Exemplo 3.5. *Considere o número* $(AF98)_{16}$*. Vamos convertê-lo para a base* 2*. Como* $A = (1010)_2$*,* $F = (1111)_2$*,* $9 = (1001)_2$ *e* $8 = (1000)_2$*, temos*

$$(AF98)_{16} = ([1010][1111][1001][1000])_2 = (1010111110011000)_2.$$

Exemplo 3.6. *Considere o número* $(6754)_8$ *na base* 8*. Vamos convertê-lo para a base* 2*. Como* $8 = 2^3$ *então cada dígito da base* 8 *equivale a* 3 *dígitos na base* 2*. Como* $6 = (110)_2$*,* $7 = (111)_2$*,* $5 = (101)_2$ *e* $4 = (100)_2$*, temos*

$$(6754)_8 = ([110][111][101][100])_2 = (110111101100)_2.$$

3.3 Operações

3.3.1 Adição

Quando somamos numa base b qualquer, o fazemos somando cada algarismo correspondente, isto é, algarismo da unidade com algarismo da unidade, algarismo da segunda ordem com algarismo da segunda ordem e, assim, por diante. Efetuamos a soma dois a dois de forma que, se a soma for maior ou igual a b no algarismo da unidade, então colocamos o que passa de b e adicionamos b unidades (1 grupo de b) na soma da segunda ordem; fazemos o mesmo no restante da soma toda vez que a soma em determinada ordem for maior ou igual a b.

Exemplo 3.7. *Somar os números* 367 *e* 489 *na base* 10*.*

$$\begin{array}{r} 367 \\ +489 \\ \hline 856 \end{array}$$

Somando 9 unidades com 7 unidades dá 16 unidades. Como a soma é maior ou igual a 10 unidades, pegamos a dezena, 1, e adicionamos na ordem das dezenas e deixamos 6 na ordem das unidades. Somando 8 dezenas com 6 dezenas dá 14 dezenas, mais uma dezena dá 15 dezenas. Como a soma é maior ou igual a 10 dezenas, pegamos as 10 dezenas, ou seja, 1 centena e adicionamos na ordem das centenas e deixamos 5 na ordem das dezenas. Somando 3 centenas com 4 centenas dá 7 centenas, mais 1 centena dá 8 centenas e terminamos a nossa soma.

Exemplo 3.8. *Somar os números* $(11011)_2$ *e* $(1101)_2$ *que representam* 27 *e* 13*, respectivamente, na base* 10*.*

$$\begin{array}{r} 1^1 1^1 0^1 1^1 1 \\ +\ 1\ 1\ 0\ 1 \\ \hline 1\,0\,1\,0\,0\,0 \end{array}$$

Quando somamos na base 2, procedemos da mesma forma, somando os algarismos de ordem 1, depois somando os algarismos de ordem 2 e, assim, por diante. Caso a soma seja maior ou igual a 2 no algarismo de ordem 1, adicionamos 1 unidade na soma dos algarismos de ordem 2; nesse caso, 1 unidade não significa número 1, mas um grupo de 2, assim como na base 10 quando adicionamos 1, na verdade estamos adicionando 1 grupo de 10.

Note, primeiramente, que $1 + 1 = 2$ na base 10, mas na base 2, $2 = 10$, assim $1 + 1 = 10$; então temos 0 unidades e 1 grupo de 2. Esse grupo de 2 adicionamos na soma dos algarismos de ordem 2. No segundo passo temos $1 + 1 + 0 = 10$, colocamos 0 e adicionamos 1 grupo de 2^2 na soma dos algarismos de ordem 3. No terceiro passo temos $1 + 0 + 1 = 10$, novamente colocamos 0 e adicionamos 1 grupo de 2^3 na soma dos algarismos de ordem 4. No quarto passo temos $1 + 1 + 1 = 3$ e $3 = 11$ na base 2, então colocamos 1 e adicionamos 1 grupo de 2^4 na soma dos algarismos de ordem 5. Finalmente temos $1 + 1 = 10$. Portanto $(11011)_2 + (1101)_2 = (101000)_2$ que equivale a 40 na base 10.

Exemplo 3.9. *Somar os números* $(A28)_{16}$ *e* $(739)_{16}$.

$$\begin{array}{r} A28 \\ \underline{+739} \\ 1161 \end{array}$$

No primeiro passo temos $8 + 9 = 17$, ou seja, 1 grupo de 16 e mais 1 unidade. Então, colocamos 1 e adicionamos 1 na soma dos algarismos de ordem 2. Agora, temos $3 + 2 + 1 = 6$ e colocamos 6. No próximo passo temos $A + 7$, como $A = 10$, então fica $10 + 7 = 17$, ou seja, 1 grupo de 16 e mais 1 unidade, e colocamos 11, encerrando assim a soma. Portanto,

$$(A28)_{16} + (739)_{16} = (1161)_{16}.$$

3.3.2 Subtração

Quando subtraímos numa base b qualquer, se o minuendo for maior do que o subtraendo, não temos dificuldade para realizar a subtração. No entanto, se o minuendo for menor do que o subtraendo, então temos que fazer reagrupamento, isto é, "pedir emprestado" da casa do minuendo mais próxima à esquerda. Se estivermos na casa das unidades, "pedimos emprestado"1 unidade de ordem 2, somamos com a unidade do minuendo e efetuamos a diferença, o mesmo acontecendo com a casa das unidades de ordem $3, 4$ e, assim, por diante. Quando falamos de reagrupamento, estamos querendo dizer que podemos extrair unidades de uma ordem e reagrupar em outra ordem, facilitando, assim, a nossa operação.

Exemplo 3.10. *Subtrair os números* $(11011)_2$ *e* $(1101)_2$ *escritos na base* 2*.*

$$\begin{array}{r} 1\overset{0}{\not 1}\overset{1}{1}0\,1\,1 \\ -\ 1\,1\,0\,1 \\ \hline 1\,1\,1\,0 \end{array}$$

No primeiro e no segundo passo não temos dificuldade, fazemos $1-1=0$ e $1-0=1$. No terceiro passo não temos como tirar 1 de 0, então como no sistema decimal "pedimos emprestado" à casa do minuendo mais próxima à esquerda, isto é, fazemos reagrupamento, extraímos uma unidade de ordem 4 e reagrupamos com a de ordem 3, ficando agora, $10-1$. Mas $10=2$, então fazemos $2-1=1$. Por fim, no quarto passo, ficamos com $10-1$; novamente, temos $10=2$, ficando $2-1=1$ e concluímos a subtração.

Podemos tirar a prova real transformando para a base 10. Temos $(11011)_2 = 27$ e $(1101)_2 = 13$, $27-13=14$ e $(1110)_2 = 14$. Portanto, temos que $(11011)_2-(1101)_2 = (1110)_2$.

Exemplo 3.11. *Subtrair os números* $(5746)_9$ *e* $(4857)_9$ *escritos na base* 9*.*

$$\begin{array}{r} 5746 \\ \underline{-4857} \\ 0778 \end{array}$$

No primeiro passo não podemos tirar 7 de 6, então "*pedimos emprestado*"à casa do minuendo mais próxima à esquerda, isto é, fazemos reagrupamento, extraímos uma unidade de ordem 2 (ficando agora com 3 unidades de ordem 2) e reagrupamos com a de ordem 1. O 1 que "pedimos emprestado"equivale a 9, pois estamos operando na base 9, então temos $9+6=15$, e fazemos $15-7=8$.

$$\begin{array}{r} 57\overset{3}{\not 4}\overset{1}{6} \\ \underline{-4\,8\,5\,7} \\ 8 \end{array} \quad \Rightarrow \quad \begin{array}{r} 5\,7\,3\ 15 \\ \underline{-\,4\,8\,5\ \ 7} \\ 8 \end{array}$$

No segundo passo, novamente não temos como tirar 5 de 3, então extraímos uma unidade de ordem 3 (ficando agora com 6 unidades de ordem 3) e reagrupamos com a de ordem 2 e, temos, $9+3=12$, e fazemos $12-5=7$.

$$\begin{array}{r} 5\overset{6}{\not 7}\overset{1}{3}\ 15 \\ \underline{-4\,8\ 5\ \ 7} \\ 7\ \ 8 \end{array} \quad \Rightarrow \quad \begin{array}{r} 5\ 6\ 12\,15 \\ \underline{-\,4\ 8\ \ 5\ \ 7} \\ 7\ \ 8 \end{array}$$

No terceiro passo, de forma análoga, não temos como tirar 8 de 6, então extraímos uma unidade de ordem 4 (ficando agora com 4 unidades de ordem 4) e reagrupamos com

a de ordem 3 e, temos, $9 + 6 = 15$ e fazemos $15 - 8 = 7$. Finalmente, $4 - 4 = 0$.

$$\begin{array}{r} {}^{4}\not{5}^{1}6\ \ 12\ \ 15 \\ \underline{-4\ \ 8\ \ 5\ \ 7} \\ 0\ \ 7\ \ 7\ \ 8 \end{array} \quad \Rightarrow \quad \begin{array}{r} 4\ \ 15\ \ 12\ \ 15 \\ \underline{-\ \ 4\ \ 8\ \ 5\ \ 7} \\ 0\ \ 7\ \ 7\ \ 8 \end{array}$$

Portanto, $(5746)_9 - (4857)_9 = (778)_9$.

3.3.3 Multiplicação

Na base 10, quando multiplicamos os algarismos das unidades, se o produto for maior ou igual a 10, então adicionamos a/as dezena/s no produto com o algarismo da dezena; o mesmo fazemos quando multiplicamos as dezenas, as centenas, e assim por diante. Depois somamos os produtos realizados. O mesmo acontece quando operamos com uma base b qualquer.

Exemplo 3.12. *Efetuar a seguinte operação na base* 7*:* 4653×5.

$$\begin{array}{r} 4653 \\ \underline{\times 5} \\ 33561 \end{array}$$

No primeiro passo fazemos $5 \times 3 = 15$. Mas $15 = 2 \times 7 + 1$, então colocamos 1 e reservamos o 2 para adicionarmos no produto com o algarismo de ordem 2 que, nesse caso, é 5.

$$\begin{array}{r} 4653 \\ \underline{\times 5} \\ \underbrace{15}_{2\times 7+1} \end{array} \quad \Rightarrow \quad \begin{array}{r} 465^{2}3 \\ \underline{\times 5} \\ 1 \end{array}$$

No segundo passo, fazemos $5 \times 5 + 2 = 27$; mas $27 = 3 \times 7 + 6$, então colocamos 6 e reservamos o 3 para adicionarmos no produto com o algarismo de ordem 3 que, nesse caso, é 6.

$$\begin{array}{r} 4653 \\ \underline{\times 5} \\ \underbrace{27}_{3\times 7+6} \end{array} \quad \Rightarrow \quad \begin{array}{r} 46^{3}53 \\ \underline{\times 5} \\ 61 \end{array}$$

No terceiro passo, fazemos $5 \times 6 + 3 = 33$; mas $33 = 4 \times 7 + 5$, então colocamos 5 e reservamos o 4 para adicionarmos no produto com o algarismo de ordem 4 que, nesse caso, é 4.

$$\begin{array}{r} 4653 \\ \underline{\times 5} \\ \underbrace{33}_{4\times 7+5} \end{array} \quad \Rightarrow \quad \begin{array}{r} 4^4653 \\ \underline{\times 5} \\ 561 \end{array}$$

Finalmente, $5 \times 4 + 4 = 24$, mas $24 = 3 \times 7 + 3$, então colocamos 33 e concluímos a nossa operação.

$$\begin{array}{r} 4653 \\ \underline{\times 5} \\ \underbrace{24}_{3\times 7+3} \end{array} \quad \Rightarrow \quad \begin{array}{r} 4653 \\ \underline{\times 5} \\ 33561 \end{array}$$

Portanto, na base 7, $4653 \times 5 = 33561$.

3.3.4 Divisão

Como estamos trabalhando com números naturais, vamos nos ater a divisões exatas, isto é, divisões que não deixam restos. Dividir em outras bases é provavelmente o mais difícil, pois não apenas precisamos dividir, mas também multiplicar e subtrair, tudo em uma base diferente. Como exemplo vamos utilizar a base 6.

Exemplo 3.13. *Vamos efetuar a divisão* $(3241)_6 \div (5)_6$ *na base* 6.

$$\begin{array}{r|l} 3241 & \underline{5} \\ \underline{-32} & 405 \\ 041 & \\ \underline{-41} & \\ 0 & \end{array}$$

Observe que 3 não cabe em 5, então temos que pegar 32. Note que 5 cabe 4 vezes em 32, pois 5×4 na base 6 é $32 = 3 \times 6^1 + 2 \times 6^0$ (o que seria 20 na base 10) e o resto é 0. Agora subtraímos $32 - 32 = 0$ e baixamos o 4, ficando, agora, $04 \div 5 = 0$. Por fim, baixamos o 1 e temos $41 \div 5$.

Ora, 5 cabe 5 vezes em 41, pois 5×5 na base 6 é $41 = 4 \times 6^1 + 1 \times 6^0$ (o que seria 25 na base 10) e o resto é 0. Portanto, $(3241)_6 \div (5)_6 = (405)_6$.

Exemplo 3.14. *Consideremos e efetuemos a operação de divisão* $(5430)_6 \div (13)_6$ *na base* 6.

$$\begin{array}{r|l} 5430 & \underline{13} \\ \underline{-43} & 350 \\ 113 & \\ \underline{-113} & \end{array}$$

0

Note que 13 não cabe em 5, daí para começar a dividir pegamos 54. Vemos que 13 cabe 3 vezes em 54, pois 13×3 na base 6 é 43. Agora subtraímos $54 - 43 = 11$ e baixamos o 3, ficando, agora, $113 \div 13$.

13 cabe cinco vezes em 113, pois 13×5 na base 6 é 113 e o resto é zero. Finalmente, dividimos 0 por 13 obtendo 0 e, como resultado final 350. Portanto, $(5430)_6 \div (13)_6 = (350)_6$.

Uma maneira mais fácil de dividir numa base b seria converter o divisor e o dividendo para a base 10 e efetuar a divisão na base 10, depois converter o quociente dessa divisão para a base b.

Por exemplo, $(5430)_6 = (1242)_{10}$ e $(13)_6 = (9)_{10}$. Então fazemos $1242 \div 9 = 138$. Agora passamos 138 para a base 6, fazendo divisões sucessivas por 6. Então $(138)_{10} = (350)_6$ e, portanto, $(5430)_6 \div (13)_6 = (350)_6$.

3.4 Critérios de divisibilidade numa base arbitrária

Existem alguns critérios práticos para decidir quando um determinado número inteiro é divisível por outro e para determinar o resto da divisão. Esse conhecimento pode ser muito útil para realizar cálculos de maneira mais rápida, sem a necessidade de utilizar o algoritmo de divisão. Os critérios, por sua vez, são ensinados para números inteiros escritos na base 10, mas poderiam ser mais gerais estendendo-se a outras bases. Aqui vamos fazer de forma agrupada os critérios práticos de divisibilidade. Para prová-los, será necessário provar o Lema seguinte.

Lema 3.4.1. *Sejam $a, b, d \in \mathbb{Z}$. Então $d \mid a - b$ se, e somente se, a e b deixam o mesmo resto na divisão por d.*

Demonstração. Suponha que $d \mid a - b$. Dividindo a e b por d obtemos $a = dq + r$ e $b = dq' + r'$ com $0 \leq r, r' < d$. Queremos mostrar que $r = r'$. Se não for esse o caso, então vamos supor $r > r'$. Daí, $a - b = d(q - q') + (r - r')$ e, como $d \mid a - b$ obtemos $d \mid r - r'$ que é um absurdo, pois $0 < r - r' < d$, logo $r = r'$.
Reciprocamente, se $a = dq + r$ e $b = dq' + r$ é evidente que $a - b = d(q - q')$ e segue o resultado. ■

Em toda essa seção consideramos b uma base fixada e escrevemos os números naturais na base b:

$$n = a_s b^s + \ldots + a_k b^k + a_{k-1} b^{k-1} \ldots a_1 b + a_0$$

Onde os algarismos satisfazem $a_0, a_1, \ldots, a_k \in \{0, 1, \ldots, b-1\}$.

- **Primeiro Grupo**: Divisores de alguma potência da base

Considere n na base b,

$$n = a_s b^s + \ldots + a_k b^k + a_{k-1} b^{k-1} \ldots a_1 b + a_0$$

Suponha que $d \mid b^k$ e que essa é a menor potência de b cumprindo tal condição. Então $d \mid a_s b^s + \ldots + a_k b^k$, de modo que:

Proposição 3.1. *$d \mid n \Leftrightarrow d \mid a_{k-1} b^{k-1} \ldots a_1 b + a_0$. Além disso n e $a_{k-1} b^{k-1} \ldots a_1 b + a_0$ deixam o mesmo resto na divisão por d, uma vez que $d \mid n - (a_{k-1} b^{k-1} \ldots a_1 b + a_0)$.*

Demonstração. Como, por hipótese, $d \mid n - (a_{k-1} b^{k-1} \ldots a_1 b + a_0)$, usando o Lema 3.4.1, o resultado segue. ■

No caso especial em que $b = 10$, temos:

Exemplo 3.15. *$d \mid 10$ para $d = 2, 5, 10$ então, para estes valores de d temos o seguinte critério:*

$$d \mid n \Leftrightarrow d \mid a_0$$

Além disso n e a_0 deixam o mesmo resto na divisão por d.

Exemplo 3.16. *$d \mid 100$, mas $d \nmid 10$. Para $d = 4, 20, 25, 50, 100$ temos o seguinte critério:*

$$d \mid n \Leftrightarrow d \mid 10a_1 + a_0$$

Além disso n e $10a_1 + a_0$ deixam o mesmo resto na divisão por d.

Exemplo 3.17. *$d \mid 1000$, mas $d \nmid 100$. Para $d = 8, 40, 125, 200, 250, 500, 1000$ temos o seguinte critério:*

$$d \mid n \Leftrightarrow d \mid 100a_2 + 10a_1 + a_0$$

Além disso n e $100a_2 + 10a_1 + a_0$ deixam o mesmo resto na divisão por d.

- **Segundo Grupo**: Números que dividem o antecessor da base

Considere n na base b,

$$n = a_s b^s + \ldots + a_k b^k + a_{k-1} b^{k-1} \ldots a_1 b + a_0.$$

E considere que d é um inteiro positivo tal que $d \mid b - 1$, isto é, $b = dq + 1$. Então cada potência de b também será desta forma, isto é, $b^k = dQ + 1$. Defina $s = a^k + \ldots + a_1 + a_0$, a soma dos algarismos de n quando expresso em base b. Assim temos o seguinte critério de divisibilidade:

Proposição 3.2. *$d \mid n \Leftrightarrow d \mid s$. Além disso n e s deixam o mesmo resto na divisão por d.*

Demonstração. Como $d \mid n - s$, usando o Lema 3.4.1, o resultado segue. ■

Exemplo 3.18. *No caso especial $b = 10$ esse critério funciona para $d = 3$ e para $d = 9$.*

- **Terceiro Grupo**: Números que dividem o sucessor da base

Considere n na base b,

$$n = a_s b^s + \ldots + a_k b^k + a_{k-1} b^{k-1} \ldots a_1 b + a_0.$$

E considere que d é um inteiro positivo tal que $d \mid b + 1$, isto é, $b = dq - 1$. As potências de b com expotente par satisfazem $b^{2s} = Qd + 1$ e as potências de b com expoente ímpar satisfazem $b^{2s+1} = Ld - 1$. Definimos assim a soma alternada dos algarismos de n quando escrito em base b, $a = a_0 - a_1 + a_2 - \ldots + (-1)^k a_k$. Assim temos o seguinte critério de divisibilidade:

Proposição 3.3. *$d \mid n \Leftrightarrow d \mid a$ Além disso n e a deixam o mesmo resto na divisão por d.*

Demonstração. Como $d \mid n - a$, pelo Lema 3.4.1, o resultado segue. ■

Exemplo 3.19. *No caso especial $b = 10$ esse critério funciona para $d = 11$.*

4 Representação dos Racionais

O surgimento dos números racionais veio da necessidade de representar partes de um inteiro. Segundo historiadores, no Egito Antigo, durante inundações do Rio Nilo , muitas terras ficavam submersas, o que era favorável a que elas recebessem nutrientes. Tais terras tornavam-se muito férteis para a agricultura. Assim, quando as águas baixavam, havia a necessidade de remarcar os limites entre os terrenos de cada proprietário. Todavia, não encontravam um número inteiro para representar tais medidas, por mais eficientes que tentassem ser, o que os levou à utilização de frações.

Neste capítulo, observaremos a representação dos números racionais como também algumas propriedades peculiares.

Definição 4.1. *Sejam a e b inteiros, $b \neq 0$. Dizemos que r é racional se puder ser escrito na forma $r = \frac{a}{b}$.*

Dizemos que $\frac{a}{b}$ é a representação fracionária de r. Fazendo a divisão de a por b obtemos a representação decimal do número racional r. O conjunto dos números racionais inclui todos os números resultantes da divisão de inteiros. Em particular, $\frac{m}{1} = m$ e $\frac{m \cdot p}{p}$ são inteiros e racionais.

Definimos a relação de igualdade entre as frações da seguinte forma:

$$\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc$$

Essa relação independe das frações serem irredutíveis, pois $\frac{a}{b} = \frac{ac}{bc}$.

As operações de adição e multiplicação e a relação de ordem com os racionais são definidas como segue:

- **Adição**

A operação de adição de dois números racionais é bem definida, isto é:

$$\forall \ \frac{a}{b} \text{ e } \frac{c}{d} \in \mathbb{Q}, \text{ temos que } \frac{a}{b} + \frac{c}{d} \in \mathbb{Q}.$$

Isto significa que quaisquer que sejam $\frac{a}{b}$ e $\frac{c}{d}$ racionais, a soma $\frac{a}{b} + \frac{c}{d}$ é um número racional e temos:

$$\frac{a}{b} + \frac{c}{d} = \frac{a \cdot d}{b \cdot d} + \frac{c \cdot b}{d \cdot b} = \frac{ad + bc}{bd}$$

Exemplo 4.1. *A soma* $\frac{2}{3} + \frac{5}{7} = \frac{2 \cdot 7}{3 \cdot 7} + \frac{5 \cdot 3}{7 \cdot 3} = \frac{2 \cdot 7 + 5 \cdot 3}{3 \cdot 7} = \frac{29}{21}$ *é um número racional.*

Os racionais gozam de todas as propriedades dos inteiros. A adição tem as seguintes propriedades:

(i) (Associativa): $\frac{a}{b}+\left(\frac{c}{d}+\frac{e}{f}\right)=\left(\frac{a}{b}+\frac{c}{d}\right)+\frac{e}{f}$

(ii) (Comutativa): $\frac{a}{b}+\frac{c}{d}=\frac{c}{d}+\frac{a}{b}$

(iii) (Elemento neutro): o zero. $\frac{a}{b}+0=0+\frac{a}{b}=\frac{a}{b}$

(iv) (Simétrico): $\frac{a}{b}+\left(-\frac{a}{b}\right)=0$

- **Multiplicação**

A operação de multiplicação de dois números racionais é bem definida, isto é:

$$\forall \ \frac{a}{b} \text{ e } \frac{c}{d} \in \mathbb{Q}, \text{ temos que } \frac{a}{b}\cdot\frac{c}{d} \in \mathbb{Q}.$$

Isto significa que quaisquer que sejam $\frac{a}{b}$ e $\frac{c}{d}$ racionais, o produto $\frac{a}{b}\cdot\frac{c}{d}$ é um número racional e temos:

$$\frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}$$

Exemplo 4.2. *O produto* $\frac{3}{5}\cdot\frac{2}{7}=\frac{3\cdot 2}{5\cdot 7}=\frac{6}{35}$ *é um número racional.*

A multiplicação tem as seguintes propriedades:

(i) (Associativa): $\frac{a}{b}\cdot\left(\frac{c}{d}\cdot\frac{e}{f}\right)=\left(\frac{a}{b}\cdot\frac{c}{d}\right)\cdot\frac{e}{f}$

(ii) (Comutativa): $\frac{a}{b}\cdot\frac{c}{d}=\frac{c}{d}\cdot\frac{a}{b}$

(iii) (Elemento neutro): o um. $\frac{a}{b}\cdot 1=1\cdot\frac{a}{b}=\frac{a}{b}$

(iv) (Elemento Inverso): Para cada racional $\frac{a}{b}$, não nulo, existe um, e só um elemento inverso multiplicativo $\frac{b}{a}$ tal que $\frac{a}{b}\cdot\frac{b}{a}=1$

- **Relação de ordem**

Dizemos que $\frac{a}{b}>\frac{c}{d}$ se, e só se $\frac{a}{b}-\frac{c}{d}>0$
Isto significa que:

$$\frac{a}{b}-\frac{c}{d}=\frac{ad}{bd}-\frac{cb}{db}=\frac{ad-bc}{bd}>0$$

O que equivale a dizer: $\frac{a}{b} > \frac{c}{d}$ se, e só se $ad > bc$, com $b, d > 0$.

Exemplo 4.3. *Comparar os números* $\frac{4}{9}$ *e* $\frac{3}{7}$.

Temos $\frac{4}{9} - \frac{3}{7} = \frac{4 \cdot 7}{9 \cdot 7} - \frac{3 \cdot 9}{7 \cdot 9} = \frac{4 \cdot 7 - 3 \cdot 9}{9 \cdot 7} = \frac{28 - 27}{63} = \frac{1}{63} > 0$ Logo, $\frac{4}{9} > \frac{3}{7}$.
Ou podemos fazer $4 \cdot 7 = 28$ e $9 \cdot 3 = 27$, como $28 > 27$, segue que $\frac{4}{9} > \frac{3}{7}$.

4.1 Longa Divisão Euclidiana

Dado $n \in \mathbb{R}_+$ e uma base $b > 1$ qualquer, existem $a_0, a_1, \ldots, a_r, c_1, c_2, \ldots, c_s, \ldots \in \{0, 1, \ldots, b-1\}$, tais que $n = (a_r b^r + \ldots + a_1 b + a_0) + (c_1 b^{-1} + c_2 b^{-2} + \ldots + c_s b^{-s} + \ldots)$. As duas parcelas entre parênteses são, respectivamente, a parte inteira de n e a parte não-inteira de n. Denotamos $n = (a_r \ldots a_1 a_0, c_1 c_2 \ldots c_s \ldots)_b$.

Para a parte inteira, o procedimento para a demonstração é o mesmo que foi utilizado para os naturais. Utilizando divisão euclidiana, dividimos n por b e obtemos $n = bq_0 + a_0$, $0 \leq a_0 < b$. Se $q_0 < b$ o resultado está provado fazendo $a_0 = q_0$, senão, dividimos q_0 por b e obtemos $q_0 = bq_1 + a_1$, com $0 \leq a_1 < b$. Se $q_1 < b$ o resultado está provado fazendo $a_1 = q_1$, senão, continuamos com a divisão até que $q_r < b$. Então fazemos $a_r = q_r$ e obtemos a expressão desejada.

Para a parte não-inteira, multiplicamos por b, dessa forma encontramos c_1. Retiramos c_1 e multiplicamos por b novamente encontrando c_2. Retiramos c_2 e multiplicamos por b novamente. Continuando com esse processo vamos mostrar que tal expressão é periódica.

Exemplo 4.4. *No número* $(1, 57)_b$ *a parte inteira é* 1 *e a parte não inteira é* $0, 57$. *Conforme o enunciado,* $1, 57 = 1 + 5 \times b^{-1} + 7 \times b^{-2}$ *em que b é uma base qualquer,* $b > 7$.

Exemplo 4.5. *O número* $(45, 1212\ldots)_6$ *é igual a* $4 \times 6^1 + 5 \times 6^0 + 1 \times 6^{-1} + 2 \times 6^{-2} + 1 \times 6^{-3} + 2 \times 6^{-4} + \ldots$.

4.2 Frações × Dízimas

Utilizando a divisão continuada (ou a longa divisão) observaremos que a representação de um racional possui uma periodicidade. Considere $a, b \in \mathbb{Z}, b > 0$. Fazendo divisão continuada temos

$$\begin{array}{l|l} a & \underline{b} \\ a_1 & n, c_1 c_2 \ldots \\ a_2 & \\ a_3 & \end{array}$$

...

Como os únicos restos da divisão por b são $\{0, 1, 2, \dots b-1\}$, então podemos ter certeza de que haverá repetição no desenrolar da divisão. Quando a repetição ocorrer, um novo ciclo se iniciará e o resultado será uma dízima periódica.

Exemplo 4.6. $\frac{2}{3} = 0,666\ldots,$ $\frac{1}{7} = \overline{0,142857},$ $\left(\frac{1}{2}\right)_3 = 0,111\ldots$

Observe que nesses exemplos existem periodicidades, porém há outros, os decimais exatos (ou os que têm representação decimal finita) que, aparentemente, não tem periodicidade, mas veremos mais adiante que todo número racional pode ser escrito com periodicidade.

Os próximos teoremas e proposições desta seção, que tratam da representação dos racionais, foram referenciados e adaptados de (9).

Teorema 4.1. *Um número racional possui representação decimal finita se, e somente se, quando escrito na forma irredutível, a decomposição em fatores primos de seu denominador possui apenas os fatores* 2 *ou* 5.

Demonstração. Seja n um número com uma quantidade finita de casas decimais, ou seja,

$$n = a + 0, b_1 b_2 \dots b_k,$$

em que $a \in \mathbb{Z}$ é a parte inteira e cada b_i é uma casa decimal de n, ou seja, cada b_i é um inteiro entre 0 e 9.

Note que, se $b_i = 0$, para todo $i = 1, 2, \dots k$, então $n = a$ é um número inteiro e podemos escrevê-lo na forma fracionária como

$$n = \frac{n}{2^0 5^0}.$$

Daí podemos supor que $b_k \neq 0$, neste caso

$$0, b_1 b_2 \dots b_k \times 10^k = b_1 b_2 \dots b_k \Rightarrow 0, b_1 b_2 \dots b_k = \frac{b_1 b_2 \dots b_k}{10^k}$$

e então $n = a + 0, b_1 b_2 \dots b_k = a + \dfrac{b_1 b_2 \dots b_k}{10^k} = \dfrac{a \times 10^k + b_1 b_2 \dots b_k}{2^k 5^k}.$

Reciprocamente, seja $\frac{a}{b}$ uma fração irredutível com $a \in \mathbb{Z}$, $b = 2^p 5^q$ e $p, q \in \mathbb{Z}_+$. Suponha $p \geq q$, o caso $p < q$ é análogo. então temos

$$\frac{a}{b} = \frac{a}{2^p 5^q} = \frac{a}{2^p 5^q} \cdot \frac{5^{p-q}}{5^{p-q}} = \frac{a \times 5^{p-q}}{10^p}$$

o que podemos concluir que a representação decimal de $\frac{a}{b}$ possui p casas decimais. ■

Exemplo 4.7. *O número* $\frac{8}{25}$ *possui representação decimal finita, pois* $\frac{8}{25} = \frac{8}{2^0 5^2} = 0,32$

Quando n tem representação decimal infinita periódica dizemos que n é uma dízima periódica.

Teorema 4.2. *Seja* $\frac{a}{b}$ *a forma irredutível de um número racional. Se a decomposição de* b *em fatores primos contém fatores diferentes de* 2 *e* 5*, então sua representação decimal é uma dízima periódica. Além disso, o período possui no máximo* $b-1$ *algarismos.*

Demonstração. Sabemos pelo Teorema 4.1 que a representação decimal de $\frac{a}{b}$ é infinita. Então só precisamos mostrar que é periódica. Considere r_1 o resto da divisão de a por b. Note que $r_1 \neq 0$, pois se assim não fosse, a divisão resultaria em um número inteiro. Dessa forma $1 \leq r_1 \leq b-1$.

O próximo passo no algoritmo da divisão é dividir r_1 por b. Nesse passo obtemos um novo resto r_2, com $1 \leq r_2 \leq b-1$. Continuando com o processo de divisão obtemos a sequência de restos

$$r_1, r_2, r_3, \ldots, r_{b-1}, r_b, \text{ com } 1 \leq r_j \leq b-1 \text{ para todo } j = 1, 2, 3, \ldots, b.$$

Como há apenas $b-1$ possibilidades de restos diferentes para esta divisão, o resto r_b já apareceu pelo menos uma vez na sequência $r_1, r_2, r_3, \ldots, r_{b-1}$. Isso garante que o processo de divisão entrou em um ciclo de repetição e que o comprimento do período é de no máximo $b-1$ casas decimais. ■

Exemplo 4.8. *Em* $\frac{1}{3} = 0,333\ldots$ *o comprimento do período é de uma casa decimal.*

Exemplo 4.9. *Em* $\frac{1}{7} = 0,142857142857\ldots$ *o comprimento do período é de* 6 *casas decimais.*

4.3 Dízimas periódicas puras e impuras

Sabemos que as dízimas periódicas podem ser formadas de partes cujos algarismos se repetem, as quais chamamos de período, e partes cujos algarismos não se repetem. Às dízimas periódicas formadas apenas de partes cujos algarismos se repetem chamamos de dízimas periódicas puras e, as demais chamamos de dízimas periódicas impuras.

Exemplo 4.10. $\frac{31}{99} = 0,313131\ldots$ *é uma dízima periódica pura.*

Exemplo 4.11. $\frac{2}{15} = 0,13333\ldots$ *é uma dízima periódica impura.*

O teorema a seguir é uma generalização e esclarece melhor o que estamos estudando.

Teorema 4.3. *Seja* $q \in \mathbb{Q}$, $q = \frac{a}{b}$, $a, b \in \mathbb{Z}$, $b > 0$, $b = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ *com* $mdc(a, b) = 1$. *Então temos:*

(i) q *é decimal exato* $\Leftrightarrow b = 2^{e_i} 5^{e_j}$, $i, j \in \{1, 2, \dots, k\}$.

(ii) q *é dízima pura* $\Leftrightarrow 2 \nmid b$ *e* $5 \nmid b$.

(iii) q *é dízima impura se existir* $q_i \neq 2, 5$ *e* $2 \mid b$ *ou* $5 \mid b$.

Demonstração. (i) Decorre do Teorema 4.1

(ii) ($\Rightarrow$) Seja $\frac{a}{b} = q = 0, \overline{c_1 c_2 \dots c_k}$ uma dízima pura. Multiplicando por 10^k ambos os lados da igualdade, temos:

$$10^k q = c_1 c_2 \dots c_k, \overline{c_1 c_2 \dots c_k}$$

subtraindo q de ambos os lados da igualdade, temos:

$$(10^k - 1)q = 0, \overline{c_1 c_2 \dots c_k}$$

e, agora, dividindo tudo por $(10^k - 1)$, temos:

$$q = \frac{0, \overline{c_1 c_2 \dots c_k}}{(10^k - 1)} = \frac{0, \overline{c_1 c_2 \dots c_k}}{99 \dots 9}$$

ou seja, não há fatores 2 nem 5 no denominador, o que significa que $2 \nmid b$ e $5 \nmid b$.
($\Leftarrow$) Decorre do Teorema 4.2.

(iii) Seja $q = \frac{a}{b}$ uma dízima impura. Suponha por absurdo que $q_i = 2, 5$ ou $2 \nmid b$ e $5 \nmid b$. Se $q_i = 2, 5$ então, por i), q é decimal exato, o que é um absurdo e, se $2 \nmid b$ e $5 \nmid b$ então, por ii), q é dízima pura, novamente absurdo. Portanto, o resultado segue. ■

Agora observe que um número racional cuja representação decimal é finita pode ser escrito com uma representação decimal infinita, ou seja, como uma dízima, como no exemplo a seguir.

Exemplo 4.12. $2,47 = 2,46999\dots$, $\quad 2 = 1,999\dots$, $\quad 4,1538 = 4,1537999\dots$.

Isso tira a ambiguidade fornecendo uma bijeção entre as frações e as dízimas periódicas. O resultado geral segue da proposição a seguir.

Proposição 4.1. *Todo número racional admite uma representação decimal infinita periódica.*

Demonstração. Dado um número racional qualquer, se sua forma fracionária irredutível possui denominador com fatores primos distintos de 2 e 5, não há nada a provar. Caso contrário, sua representação decimal é finita, digamos que seja $a, b_1b_2b_3 \ldots b_k$ com $b_k \neq 0$. Vamos mostrar que

$$a, b_1b_2b_3 \ldots b_k = a, b_1b_2b_3 \ldots (b_k - 1)999 \ldots$$

De fato, seja $n = a, b_1b_2b_3 \ldots (b_k - 1)999 \ldots$. Multiplicando n por 10^{k+1} temos

$$10^{k+1}n = ab_1b_2b_3 \ldots (b_k - 1)9, 999 \ldots \qquad \text{(I)}$$

Multiplicando n por 10^k temos

$$10^k n = ab_1b_2b_3 \ldots (b_k - 1), 999 \ldots \qquad \text{(II)}$$

Subtraindo (II) de (I) temos

$$(10^{k+1} - 10^k)n = ab_1b_2b_3 \ldots (b_k - 1)9, 999 \ldots - ab_1b_2b_3 \ldots (b_k - 1), 999 \ldots,$$

$$\Rightarrow 10^k(10 - 1)n = ab_1b_2b_3 \ldots (b_k - 1)9 - ab_1b_2b_3 \ldots (b_k - 1)$$

$$\Rightarrow 9 \times 10^k n = ab_1b_2b_3 \ldots (b_k - 1)9 - ab_1b_2b_3 \ldots (b_k - 1)$$

Somando e subtraindo 1 no lado direito da igualdade, temos

$$9 \times 10^k n = (ab_1b_2b_3 \ldots (b_k - 1)9 + 1) - (ab_1b_2b_3 \ldots (b_k - 1) + 1)$$

$$= 10 \times ab_1b_2b_3 \ldots b_k - ab_1b_2b_3 \ldots b_k = 9 \times ab_1b_2b_3 \ldots b_k$$

$$\Rightarrow 10^k n = ab_1b_2b_3 \ldots b_k \Rightarrow n = \frac{ab_1b_2b_3 \ldots b_k}{10^k}$$

Portanto, $n = a, b_1b_2b_3 \ldots b_k$. ■

Exemplo 4.13. *Considere o exemplo anterior para* $n = 2, 46999 \ldots$

Observe que $k = 2$. *Então multiplicando por* 10^3 *temos* $1000n = 2469, 999 \ldots$.
Multiplicando por 10^2 *temos* $100n = 246, 999 \ldots$.
Subtraindo ambas as equações temos $1000n - 100n = 2469, 999 \ldots - 246, 999 \ldots$

$$\Rightarrow 900n = 2469 - 246 \Rightarrow 900n = 2469 - 246 + 1 - 1 \Rightarrow 900n = (2469 + 1) - (246 + 1)$$

$$\Rightarrow 900n = 2470 - 247 \Rightarrow 9 \times 10^2 n = 10 \times 247 - 247$$

$$\Rightarrow 9 \times 10^2 n = 9 \times 247 \Rightarrow 10^2 n = 247 \Rightarrow n = \frac{247}{10^2} \Rightarrow n = 2, 47$$

4.4 Ciclos de Dígitos

No estudo das representações decimais de números racionais, especificamente das dízimas periódicas, observamos que existe um padrão de repetição quando olhamos para

uma fração e seus múltiplos, frações essas que representam as dízimas periódicas, isto é, frações cujo denominador é um número primo.

Considerando o número primo $p = 7$, olhemos para a fração $\frac{1}{7}$. Fazendo divisão longa obtemos

$$
\begin{array}{r|l}
10 & 7 \\
\cline{2-2}
-7 & 0,142857\ldots \\
\cline{1-1}
30 & \\
-28 & \\
\cline{1-1}
20 & \\
-14 & \\
\cline{1-1}
60 & \\
-56 & \\
\cline{1-1}
40 & \\
-35 & \\
\cline{1-1}
50 & \\
-49 & \\
\cline{1-1}
10 & \\
\ldots &
\end{array}
$$

Note que a sequência $1, 3, 2, 6, 4, 5, 1$ em destaque é composta do primeiro dígito do dividendo seguido pelos restos em cada etapa da divisão longa. Quando chegamos ao resto 1 o decimal começa a se repetir. Chegamos a 1 no sexto resto, razão pela qual o período tem 6 dígitos; na verdade, este período é tão longo quanto deveria ser.

Dizemos que uma fração $\frac{1}{p}$ tem período máximo se seu período for $p - 1$, isto é, se seu período for tão longo quanto deveria ser. No nosso exemplo, $\frac{1}{7}$ tem período máximo. Algo mais esclarecedor como veremos é que a sequência $1, 3, 2, 6, 4, 5$ são as potências de 10 reduzidas módulo 7.

4.4.1 Entendendo repetições decimais

Seguindo com o nosso exemplo da divisão longa de 1 por 7, observamos que a sequência de restos é realmente a sequência de potências de 10 em U_7. As potências de 10 reduzidas módulo 7 são:

$$10^1 \equiv 3, \qquad 10^2 \equiv 2, \qquad 10^3 \equiv 6, \qquad 10^4 \equiv 4, \qquad 10^5 \equiv 5, \qquad 10^6 \equiv 1, \ldots$$

Note que a ordem de 10 em U_7 é 6, pois 6 é o menor inteiro positivo tal que $10^6 \equiv 1 \mod 7$. É por esta causa que são necessários seis passos da longa divisão antes de encontrarmos um resto 1, mais precisamente, antes de encontrarmos qualquer resto repetido. Nós dizemos que 10 é um gerador de U_7, ou que $10 \equiv 3 \mod 7$ é uma raiz primitiva módulo 7.

Um raciocínio semelhante a esse vale para $\frac{1}{n}$ sempre que n e 10 forem coprimos; ou seja, sempre que n não tiver quaisquer fatores de 2 ou 5. O teorema a seguir esclarece com mais formalidade.

Teorema 4.4. *Se* 10 *é relativamente primo com* n*, então o período de* $\frac{1}{n}$ *é igual à ordem de* 10 $\mod n$ *em* U_n*.*

Demonstração. Se o período de $\frac{1}{n}$ é k, então isso significa que k é o menor inteiro positivo tal que $\frac{10^k - 1}{n}$ é um número inteiro. (Considere o método para converter um dízima periódica em uma fração - multiplicando por 10^k e subtraindo a parte decimal). Isso significa que k é o menor inteiro positivo tal que n divide $10^k - 1$, ou equivalentemente, $10^k \equiv 1 \mod n$. Mas esta última afirmação é precisamente a definição da ordem de 10 em U_n. ■

4.4.2 Números primos com inversos de período máximo

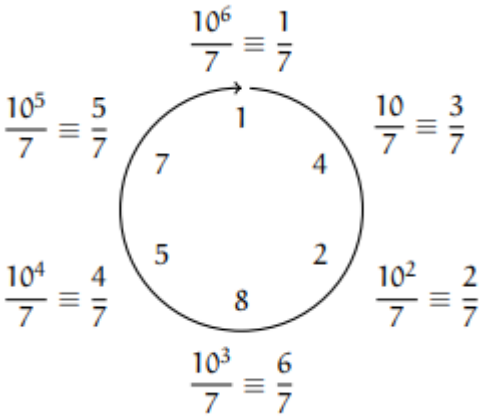
A partir de agora que sabemos como encontrar o período de $\frac{1}{n}$ para n relativamente primo com 10, podemos entender as permutações cíclicas exibidas pelos múltiplos de algumas frações como $\frac{1}{7}$. Acontece que permutações cíclicas de dígitos ocorrem nos múltiplos de muitas frações $\frac{1}{p}$, onde p é primo.

Suponha que p seja um primo ímpar e a ordem de 10 em U_p seja $p-1$. Isso significa que todos os números $1, 2, \ldots, p-1$ aparecem como potências de 10 em U_p. Ou seja, para cada $m \in \{1, 2, \ldots, p-1\}$, podemos encontrar algum número inteiro positivo r tal que $m \equiv 10^r \mod p$. Daí $m \equiv 10^r \mod p$ implica que as partes fracionárias (ou seja, os dígitos à direita do ponto decimal) de $\frac{m}{p}$ e $\frac{10^r}{p}$ são os mesmos. Isso significa que $\frac{m}{p}$ tem a mesma sequência de dígitos repetidos que $\frac{1}{p}$, mas começando com um dígito diferente.

Retomando nosso exemplo, vimos anteriormente que $\frac{1}{7} = 0,\overline{142857}$, onde a barra superior indica que os dígitos se repetem. Considere o numerador um dígito diferente, digamos 5. Agora, $5 \equiv 10^5 \mod 7$, então a partes fracionárias de $\frac{5}{7}$ e $\frac{10^5}{7}$ são as mesmas. Já que sabemos a representação decimal de $\frac{1}{7}$, simplesmente deslocamos o ponto decimal para descobrir que $\frac{10^5}{7} = 14285,\overline{714285}$. Portanto, $\frac{5}{7} = 0,\overline{714285}$, que é a mesma sequência de dígitos repetidos como em $\frac{1}{7}$, mas começando com um dígito diferente. Podemos ilustrar esse padrão em um diagrama de círculo como na Figura 1, inspirado em (10).

Em suma, quando p é primo, todos os inteiros positivos menores do que p são relativamente primos com p, então $U_p = \{1, 2, 3, \ldots, p-1\}$. Um teorema básico em álgebra abstrata (Teorema de Lagrange, (6) pág. 148) diz que a ordem de um elemento em um

Figura 1 – Ciclos de Dígitos



Fonte: Dan Kalman, 1996.

grupo sempre divide a ordem do próprio grupo. Isso significa que a ordem de 10 em U_p e, portanto, o período de $\frac{1}{p}$, sempre divide $p-1$. Já vimos que para $p=7$, a ordem de 10 em U_7 é 6, que é o maior que poderia ser. Claro, isso corresponde ao fato previamente observado de que o período de $\frac{1}{7}$ é tão longo quanto poderia ser. Números primos como 7 são chamados primos com inversos de período máximo. Na base 10, o 7 é o primeiro primo com inverso de período máximo.

Definição 4.2. *Um número primo p é um primo com inverso de período máximo se a ordem de* 10 *em U_p é $p-1$.*

Denotamos ordem de 10 por $|10|$. Em resumo, um primo p é um primo com inverso de período máximo se, e somente se, $|10| = p-1$ em U_p, que é o caso em que a representação decimal de $\frac{1}{p}$ tem período $p-1$. Isso também ocorre exatamente quando 10 gera U_p. Além disso, para qualquer primo com inverso de período máximo, os múltiplos $\frac{1}{p}, \frac{2}{p}, \ldots, \frac{p-1}{p}$ exibem permutações cíclicas de uma sequência de $p-1$ dígitos.

Baseando-se no que estudamos até agora em relação aos primos com inverso de período máximo, observamos as seguintes propriedades que serão demonstradas a seguir:

1. O número de uns na sequência $11, 111, 1111, 11111, \ldots$ é igual ao comprimento da repetição de $\frac{1}{p}$ e divisível por p.

2. Os números internos ao círculo diametralmente somam 9 na base 10 ou $b-1$ na base b.

3. As frações externas ao círculo diametralmente somam 1.

4. O número cíclico quando multiplicado pelo seu primo gerador, resulta em uma sequência de $b-1$ dígitos, em que b é a base em que o número está escrito.

5. Quando dividido em dois, três, quatro, ... partes em relação à base por seus dígitos e somadas essas partes, o resultado é uma sequência de $b-1's$.

6. Todos os números cíclicos são divisíveis por $b-1$, em que b é a base em que o número está escrito.

Para a demonstração da propriedade 1 utilizamos o método para converter as dízimas periódicas em fração. Se houver k dígitos na repetição, multiplique o decimal por 10^k e subtraia a parte decimal para obter a repetição como um número inteiro, ou seja, se x é a parte decimal, então $(10^k-1)x = n$ em que n é o número inteiro cuja representação na base 10 é a repetição (ignorando qualquer zeros à esquerda). Agora, se $x = \frac{1}{p}$, descobrimos que p deve ser um divisor de 10^k-1, mas $10^k-1 = 9\times 111\ldots1$ (k vezes). Como p é primo e é maior do que 3, então p não divide 9, logo p divide $111\ldots1$ (k vezes). Isso mostra que p é um divisor de $111\ldots1$, onde o número de uns é igual a k, o comprimento da repeticão de p.

Um argumento semelhante, mas ao contrário, mostra que p não pode dividir $111\ldots1$ com menos que k uns. De fato, se p divide $111\ldots1$ (k vezes) para alguns $k' < k$, seria possível expressar $\frac{1}{p}$ como uma repetição decimal com um comprimento k', contradizendo nossa suposição de que o comprimento da repetição de $\frac{1}{p}$ é k. Isso completa a demonstração e mostra que p é um primo com inverso de período máximo se, e somente se for um divisor de $111\ldots1$ ($p-1$ vezes).

Exemplo 4.14. $\frac{1}{7} = 0,142857\ldots$ *tem período de comprimento* 6*, então o número* 111111 *composto de* 6 *uns é divisível por* 7*.*

Exemplo 4.15. $\frac{1}{5} = \overline{0,1463}_8$ *tem período de comprimento* 4*, então o número* $(1111)_8$ *composto de* 4 *uns é divisível por* 5*.*

A propriedade 2 decorre do seguinte teorema cuja demonstração está em (10):

Teorema 4.5. *Seja p um primo com inverso de período máximo. Se a repetição de $\frac{1}{p}$ é a sequência dos dígitos $d_1, d_2, \ldots, d_{2k}$, então $d_1 + d_{k+1} = d_2 + d_{k+2} = \ldots = d_k + d_{2k} = 9$.*

Demonstração. Se p for um primo com inverso de período máximo, então o período terá comprimento $p-1$. Como p é ímpar, podemos denotar o período por $2k$. Daí p divide $111\ldots1$ ($2k$ vezes), mas falha ao dividir qualquer sequência mais curta de uns. Em particular, p não divide $111\ldots1$ (k vezes). Agora, $111\ldots1$ ($2k$ vezes) $= (10^k+1)\times 111\ldots1$

(k vezes), o que implica que p divide $(10^k + 1)$. Isso mostra que $10^k \cdot \frac{1}{p} + \frac{1}{p}$ é um número inteiro. A expansão decimal de $\frac{1}{p}$ é $\frac{1}{p} = 0, d_1 d_2 \ldots d_{2k} d_1 d_2 \ldots$, portanto a adição $10^k \cdot \frac{1}{p} + \frac{1}{p}$ pode ser representada desta maneira:

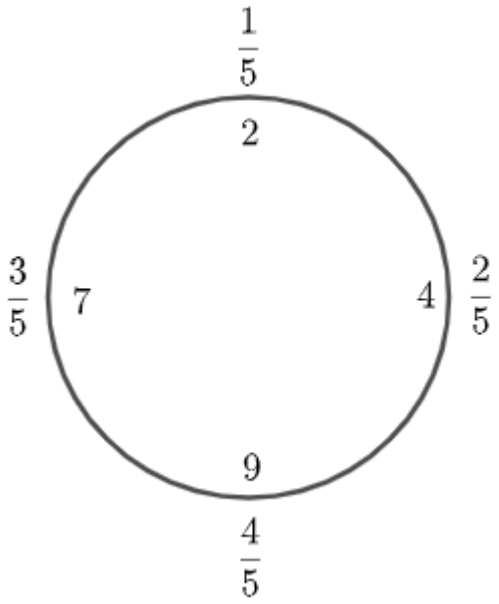
$$\begin{array}{rccccccc} & d_1 d_2 \ldots d_k, & d_{k+1} & d_{k+2} \ldots d_{2k} & & d_1 & d_2 & \ldots \\ + & & 0, d_1 & d_2 & \ldots & d_k & d_{k+1} & d_{k+2} \ldots \\ \hline \end{array}$$

A única maneira de essas casas decimais produzirem uma soma inteira é se $d_i + d_{k+i} = 9$ para cada $1 \leq i \leq k$, o que conclui a demonstração. ■

Observação: O teorema é uma prova para a base 10, mas a propriedade estende-se para qualquer base b.

Exemplo 4.16. *Considere* $\left(\frac{1}{5}\right)_{12} = 0, \overline{2497}$. *Observe na Figura 2 que os números internos ao círculo diametralmente somam* 11.

Figura 2 – Ciclos de Dígitos na base 12



Fonte: O autor

A propriedade 3 é um corolário do Teorema 4.5. Tudo o que precisamos fazer é somar as expansões decimais dessas frações. Pelo teorema, o resultado será $0,999\ldots = 1$. Novamente, como visto na Figura 2, a propriedade estende-se a outras bases.

Para a elucidação da propriedade 4 considere os exemplos a seguir.

Exemplo 4.17. *Ora,* $\frac{1}{7} = 0,142857, \ldots$, *na base* 10, *então* $142857 \times 7 = 999999$.

Exemplo 4.18. $\left(\frac{1}{5}\right)_{12} = 0, \overline{2497}$, *na base* 12, *então* $2497 \times 5 = \underbrace{11}\,\underbrace{11}\,\underbrace{11}\,\underbrace{11}$.

As propriedades 5 e 6 decorrem do Teorema de Midy, demonstrado em (11).

Teorema 4.6 (de Midy)**.** *Seja p um inteiro positivo, q primo $\neq 2$ e 5, p primo com q e $p < q$. Seja s a ordem de 10 módulo q e $s = 2s'$, com s' inteiro positivo, então tem-se que $\frac{p}{q} = 0, u_1u_2$ onde $u_1 = a_1a_2 \dots a_{s'}$ e $u_2 = a_{s'+1}a_{s'+2} \dots a_{2s'}$, com $0 \leq a_i < 10$, (para qualquer $1 \leq i \leq 2s'$ e $u_1 + u_2 = 10^{s'} - 1$.*

Exemplo 4.19 (propriedade 5)**.** *Utilizando o período de $\frac{1}{7} = 0,142857\dots$ temos $14+28+57 = 99$, $142 + 857 = 999$, $1428 + 5714 + 2857 = 9999$ e, assim, por diante.*

Na base 12, utilizando o período de $\frac{1}{5} = 0,2497\dots$ temos $24 + 97 = \underbrace{11}\,\underbrace{11}$, $249724 + 972497 = \underbrace{11}\,\underbrace{11}\,\underbrace{11}\,\underbrace{11}\,\underbrace{11}\,\underbrace{11}$.

Exemplo 4.20 (propriedade 6)**.** 142857 *na base* 10 *é divisível por* 9. 2497 *na base* 12 *é divisível por* 11.

4.4.3 Permutações Cíclicas em outras bases

Observamos que as permutações cíclicas também aparecem em outras bases. Lembremos que o valor de qualquer algarismo em um número é determinado pela sua posição. Na base dez, o valor de qualquer posição é uma potência de dez. Por exemplo,

$$347,85 = 3 \cdot 10^2 + 4 \cdot 10^1 + 7 \cdot 10^0 + 8 \cdot 10^{-1} + 5 \cdot 10^{-2}.$$

No entanto, se $347,85$ é interpretado como um número de base b, então seu valor é:

$$347,85 = 3 \cdot b^2 + 4 \cdot b^1 + 7 \cdot b^0 + 8 \cdot b^{-1} + 5 \cdot b^{-2}.$$

Note que cada algarismo de um número em uma base b deve ser menor do que o próprio b.

Assim como na base dez, o grupo U_n indica quais permutações cíclicas aparecem quando os múltiplos de $\frac{1}{n}$ são escritos na base b, sempre que n e b são relativamente primos. Nós simplesmente olhamos para o comportamento de b no grupo U_n. Em particular, os múltiplos de $\frac{1}{p}$ exibem permutações cíclicas de período máximo na base b, se e somente se, b é um gerador de U_n.

Exemplo 4.21. *Considere a representação de $\frac{1}{5}$ na base 8. Como $8 \equiv 3 \mod 5$, nós examinamos o comportamento das potências de 3 em U_5:*

$$3^1 \equiv 3, \quad 3^2 \equiv 4, \quad 3^3 \equiv 2 \quad e \quad 3^4 \equiv 1.$$

Observe que, em U_5 a ordem de 8 é 4, que é tão grande quanto poderia ser. Isso significa que os múltiplos de $\frac{1}{5}$ exibem permutações cíclicas de período máximo quando expressos na base 8. Explicitamente, esses múltiplos são:

$$\frac{1}{5} = 0,\overline{1463}_8, \qquad \frac{2}{5} = 0,\overline{3146}_8, \qquad \frac{3}{5} = 0,\overline{4631}_8 \qquad e \qquad \frac{4}{5} = 0,\overline{6314}_8.$$

Dizemos que 5 é um primo com inverso de período máximo na base 8, pois 8 tem ordem máxima em U_5.

Retomando o exemplo de $\frac{1}{5}$ na base 12 vemos que $12 \equiv 2 \mod 5$, então examinamos o comportamento das potências de 2 em U_5:

$$2^1 \equiv 2, \qquad 2^2 \equiv 4, \qquad 2^3 \equiv 3 \qquad \text{e} \qquad 2^4 \equiv 1.$$

Vemos que a ordem de 12 é 4 em U_5 e os múltiplos de $\frac{1}{5}$ exibem permutações cíclicas de período máximo quando expressos na base 12. Esses múltiplos são:

$$\frac{1}{5} = 0,\overline{2497}_{12}, \qquad \frac{2}{5} = 0,\overline{4972}_{12}, \qquad \frac{3}{5} = 0,\overline{7249}_{12} \qquad \text{e} \qquad \frac{4}{5} = 0,\overline{9724}_{12}.$$

Note que, na base 10 a fração $\frac{1}{5}$ tem representação decimal finita, mas nas bases 8 e 12 a fração $\frac{1}{5}$ e seus múltiplos exibem permutações cíclicas dos algarismos.

De acordo com (10), para qualquer primo p, existem bases nas quais p é um primo com inverso de período máximo. Além disso, os matemáticos pensam que para qualquer base b, existem infinitos primos com inversos de período máximo na base b, mas isto não foi comprovado nem mesmo para uma única base.

A seguir, conforme (12), mostramos alguns primeiros primos com inversos de período máximo em suas respectivas bases.
Para $b = 10$ os primos são $7, 17, 19, 23, 29, 47, 59, 61, 97, 109, \ldots$
Para $b = 12$ os primos são $5, 7, 17, 31, 41, 43, 53, 67, 101, 103, \ldots$
Para $b = 3$ os primos são $2, 5, 7, 17, 19, 29, 31, 43, 53, 79, 89, 101, 113, \ldots$
Para $b = 2$ os primos são $3, 5, 11, 13, 19, 29, 37, 53, 59, 61, 67, 83, 101, 107, \ldots$

Observamos que as permutações cíclicas de dígitos não são incomuns, mas ocorrem nas representações de muitas frações. Talvez a principal razão pela qual não observamos com frequência essas permutações cíclicas, seja porque dificilmente escrevemos dígitos suficientes. Por exemplo, as permutações cíclicas dos múltiplos de $\frac{1}{17}$ podem ser virtualmente desconhecidas porque, quase nunca, calculamos decimais para 16 dígitos. Quanto mais raramente observados são os padrões que aparecem em primos com inversos de período máximo maiores!

5 Os Números Reais

Temos visto as representações dos naturais e dos racionais. A passagem de $\mathbb{Q}$ para $\mathbb{R}$ de fato é a mais complicada conceitualmente e a representação de um número real está ligada de forma direta à própria noção de número de real. Dizer o que é um número real não é uma tarefa fácil, mas uma propriedade essencial dos números reais é que todo número real pode ser bem aproximado por números racionais. Na seção anterior, vimos a representação dos racionais, então vamos nos ater apenas aos irracionais.

Uma maneira simples que nos possibilita entender os números reais é pensar neles como sendo a medida dos segmentos de reta, isto é, números que expressam a medida dos segmentos de uma reta orientada.

Seja $\overline{AB}$ um segmento de reta. Fixemos um segmento padrão u, chamado segmento unitário. Se u cabe n vezes em $\overline{AB}$ diremos que a medida de $\overline{AB}$ será igual a n, com $n \in \mathbb{N}$. Agora, se ocorrer que o segmento unitário não caiba em $\overline{AB}$ um número exato de vezes, então a medida de $\overline{AB}$ não será um número natural. Daí, procuramos um segmento menor v que caiba n vezes em u e m vezes em $\overline{AB}$. Encontrado esse segmento v, diremos que v é uma medida comum de u e $\overline{AB}$ e que u e $\overline{AB}$ são comensuráveis. A medida de v será a fração $\frac{1}{n}$ e a medida de $\overline{AB}$, por sua vez será m vezes $\frac{1}{n}$, isto é, igual a $\frac{m}{n}$.

Todavia, se não existir v que seja medida comum de u e $\overline{AB}$, diremos que u e $\overline{AB}$ são incomensuráveis. A esses números que representam segmentos incomensuráveis chamamos de números irracionais.

5.1 Números Reais como Aproximações Sucessivas

Como já vimos, um número real positivo é o resultado de uma medição. Assim sendo, todo número real X pode ser representado por uma sucessão de aproximações sucessivas utilizando racionais $x_1, x_2, x_3, \ldots$ de modo o erro $\mathcal{E}_n = |x - x_n|$ seja cada vez menor, ou seja, $\mathcal{E}_n \to 0$.

O Teorema de Cauchy ((13), pp. 125-129) garante que toda sequência de racionais $x_1, x_2, x_3, \ldots$ tais que $|x_m - x_n| \to 0$ é convergente.

Outrossim, dado $x \in \mathbb{R}$, existe $k = \lfloor x \rfloor \in \mathbb{Z}$ tal que $0 \leq x - k < 1$. Podemos escrever a representação decimal de

$$x - k = 0, a_1 a_2 \ldots a_n \ldots, \qquad a_i \in \{0, 1, 2, \ldots, 9\},$$

o que significa que se $r_n = a_n + 10 \cdot a_{n-1} + 100 \cdot a_{n-2} + \ldots + 10^{n-1} \cdot a_1$, então

$\frac{r_n}{10^n} \leq x - k < \frac{r_n + 1}{10^n}$, e daí $k + \frac{r_n}{10^n}$ é uma boa aproximação racional de x, ou seja, o erro $\left| x - \left(k + \frac{r_n}{10^n} \right) \right|$ é menor do que $\frac{1}{10^n}$, o que de fato é um número bem pequeno se n for grande. A representação decimal de um número real fornece pois uma sequência de aproximações por racionais cujos denominadores são potências de 10.

Dado $x \in \mathbb{R}$ e q natural não nulo, existe $p \in \mathbb{Z}$ tal que $\frac{p}{q} \leq x < \frac{p+1}{q}$(basta tomar $p = \lfloor qx \rfloor$) e, portanto $\left| x - \frac{p}{q} \right| < \frac{1}{q}$ e $\left| x - \frac{p+1}{q} \right| \leq \frac{1}{q}$. Em particular, há aproximações de x por racionais com denominador q com erro menor do que $\frac{1}{q}$. A representação decimal de x equivale a dar essas aproximações para os denominadores q que são potências de 10.

O uso de um ponto decimal na base dez estende-se para incluir frações e permite representar todos os números reais até uma precisão arbitrária. Com a notação posicional, os cálculos aritméticos são muito mais simples do que com qualquer sistema numérico mais antigo, e isso explica a rápida disseminação da notação quando foi introduzida na Europa Ocidental.

Observamos que os racionais tem uma limitação que os torna insuficientes para medidas simples: há números que queremos representar, mas que não é possível expressar como razão entre dois inteiros. Um exemplo de extrema simplicidade é $\sqrt{2}$, solução de $x^2 = 2$ e medida da diagonal do quadrado unitário.

Afirmação: $\sqrt{2}$ é irracional.

Demonstração. Considere d a diagonal do quadrado de lado 1, ou seja, $d = \sqrt{2}$. Suponha que $d = \frac{p}{q}$, com $p, q \in \mathbb{Z}$ e $mdc(p, q) = 1$. Então temos $\frac{p^2}{q^2} = 2 \Rightarrow p^2 = 2q^2 \Rightarrow p^2$ é par $\Rightarrow p$ é par. Daí $p = 2k$.
Como $p^2 = 2q^2$, substituindo o valor de p temos $(2k)^2 = 2q^2 \Rightarrow 4k^2 = 2q^2 \Rightarrow 2k^2 = q^2 \Rightarrow q^2$ é par $\Rightarrow q$ é par, ou seja, p é par e q é par, o que é um absurdo, pois $mdc(p, q) = 1$. Logo, $\sqrt{2}$ é irracional. ■

Sendo $\sqrt{2}$ irracional, possui infinitas casas decimais e podemos fazer sucessivas aproximações até uma precisão arbitrária.

Um modo de se obter valores aproximados de $\sqrt{2}$ é usar a forma decimal

$$\sqrt{2} = 1,41421\ldots .$$

Os números 1; $1,4$; $1,41$; $1,414$; $1,4142$; $1,41421$; ... formam uma sequência de aproximações cada vez mais precisas de $\sqrt{2}$. Os números da sequência são todos racionais e temos, assim, uma sequência infinita de aproximações racionais de $\sqrt{2}$:

$$\frac{1}{1}, \frac{14}{10}, \frac{141}{100}, \frac{1414}{1000}, \frac{14142}{10000}, \frac{141421}{100000}, \ldots . \qquad \text{(I)}$$

À proporção que avançamos na sequência, estes números vão se aproximando cada vez mais de $\sqrt{2}$. Além disso, podemos escrever as desigualdades

$$\frac{1}{1} < \sqrt{2} < \frac{2}{1},$$

$$\frac{14}{10} < \sqrt{2} < \frac{15}{10},$$

$$\frac{141}{100} < \sqrt{2} < \frac{142}{100},$$

$$\frac{1414}{1000} < \sqrt{2} < \frac{1415}{1000},$$

$$\frac{14142}{10000} < \sqrt{2} < \frac{14143}{10000},$$

$$\frac{141421}{100000} < \sqrt{2} < \frac{141422}{100000},$$

$$\ldots < \sqrt{2} < \ldots$$

Ou na representação decimal:

$$1 < \sqrt{2} < 2,$$

$$1,4 < \sqrt{2} < 1,5,$$

$$1,41 < \sqrt{2} < 1,42,$$

$$1,414 < \sqrt{2} < 1,415,$$

$$1,4142 < \sqrt{2} < 1,4143,$$

$$1,41421 < \sqrt{2} < 1,41422,$$

$$\ldots < \sqrt{2} < \ldots$$

de forma que $x_1 = 1$, $x_2 = 1,4$, $x_3 = 1,41$, $x_4 = 1,414$, $x_5 = 1,4142$, $x_6 = 1,41421$ e, assim, por diante. Estas desigualdades mostram que uma infinidade de termos da sequência (I) estão tão próximos de $\sqrt{2}$ quanto se deseje especificar.

Se quisermos, por exemplo, nos certificar de que existem infinitos números racionais diferindo de $\sqrt{2}$ a menos de $0,0001$, podemos obter estes números escolhendo todos os termos da sequência (I), exceto os quatro primeiros.

Diante do exposto, temos o seguinte: todo número real pode ser representado por uma dízima não necessariamente periódica.

Como vimos nos racionais, dado $n \in \mathbb{R}_+$ e uma base $b > 1$ qualquer, existem $a_0, a_1, \ldots, a_r, c_1, c_2, \ldots, c_s, \ldots \in \{0, 1, \ldots, b-1\}$, tais que
$n = (a_r b^r + \ldots + a_1 b + a_0) + (c_1 b^{-1} + c_2 b^{-2} + \ldots + c_s b^{-s} + \ldots) = (a_r \ldots a_1 a_0, c_1 c_2 \ldots c_s \ldots)_b$,
sendo que agora a parte não inteira de n é infinita e não periódica.

Exemplo 5.1. $\pi = 3,141592\ldots = 3 + 1 \cdot 10^{-1} + 4 \cdot 10^{-2} + 1 \cdot 10^{-3} + 5 \cdot 10^{-4} + \ldots$.

Note que o valor de π tem infinitas casas decimais, mas que não se repetem, isto é, os dígitos não seguem um padrão de repetição.

5.2 Irracionais em outras bases

A representação dos irracionais em outras bases é análogo ao que fizemos com os irracionais, separamos a parte inteira e efetuamos a divisão pela base b; para a parte não inteira, multiplicamos pela base e pegamos a parte inteira. Fazemos isso até um número desejado de casas decimais.

Exemplo 5.2. *Representar o número* $\pi = 3,141592\ldots$ *na base* 2.

Separamos a parte inteira, que é 3, e efetuamos a divisão longa por 2 e encontramos

$$3 = (11)_2.$$

Para a parte não inteira, multiplicamos por 2 e pegamos a parte inteira

$$\begin{array}{r} 0,141592\ldots \\ \underline{\qquad\quad \times 2} \\ 0,283184\ldots \end{array}$$

nesse caso a parte inteira é zero. E temos $\pi = 11,0\ldots$

Continuamos multiplicando por 2 e pegando a parte inteira. Esse processo nunca termina, pois π é irracional.

Temos então

$$\pi = (11,00100100001111110110101010001\ldots)_2.$$

Agora observe π em outras bases:
Base 3
$\pi = 10,01021101222201\ldots$
Base 4

$\pi = 3,02100333122220\ldots$
Base 8
$\pi = 3,11037552421026\ldots$
Base 16
$\pi = 3,243F6A8885A300\ldots$

Note que da base 4 em diante, a representação de π sempre começa com 3. Isso é justificado pelo fato de 3 pertencer ao conjunto $\{0,1,2,3,4,\ldots b-1\}$ dos restos da divisão por b, com $b \geq 4$.

Exemplo 5.3. *Representar o número* $\sqrt{2} = 1,414213\ldots$ *na base* 5.

Separamos a parte inteira, que é 1. Como $1 < 5$ então é sua própria representação na base 5.

Para a parte não inteira, multiplicamos por 5 e pegamos a parte inteira

$$\begin{array}{r} 0,414213\ldots \\ \times 5 \\ \hline 2,071065\ldots \end{array}$$

nesse caso a parte inteira é 2. E temos $\sqrt{2} = 1,2\ldots$.

Multiplicamos novamente por 5 a parte não inteira e pegamos a parte inteira

$$\begin{array}{r} 0,071065\ldots \\ \times 5 \\ \hline 0,355325 \end{array}$$

nesse caso a parte inteira é zero. E temos $\sqrt{2} = 1,20\ldots$.

Continuamos com esse processo até obtermos um número desejado de casas decimais.

Temos então

$$\sqrt{2} = (1,2013420143403224\ldots)_5.$$

Os números irracionais também podem ser representados por frações contínuas infinitas, mas não será o nosso foco aqui.

A seguir, vamos descrever acerca dos números transcendentes.

5.3 Os Números Transcendentes

De acordo com (14), a teoria dos números transcendentais foi originada por Liouville em seu famoso livro de memórias de 1844 em que ele obteve, pela primeira vez, uma

classe, *très-étendue*, como foi descrito no título do artigo, de números que não satisfazem nenhuma equação algébrica com coeficientes inteiros. Alguns problemas isolados relativos ao assunto, no entanto, foram formulados muito antes dessa data, e o estudo intimamente relacionado dos números irracionais constituiu um grande foco de atenção pelo menos um século antes. De fato, em 1744, Euler já havia estabelecido a irracionalidade de e, e, em 1761, Lambert havia confirmado a irracionalidade de π. Além disso, os primeiros estudos de frações contínuas revelaram várias características básicas relativas à aproximação de números irracionais por racionais. Sabia-se, por exemplo, que para qualquer α irracional existe uma seqüência infinita de racionais $\frac{p}{q}$ $(q > 0)$ tais que $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$, e também se sabia que a fração contínua de um irracional quadrático é, em última instância, periódica, de onde existe $c = c(\alpha) > 0$ tal que $\left|\alpha - \frac{p}{q}\right| > \frac{c}{q^2}$ para todos os racionais $\frac{p}{q}$ $(q > 0)$. Liouville observou que um resultado do último tipo é mais geral, e que existe de fato um limite para a precisão com que qualquer número algébrico, não racional, pode ser aproximado por racionais. Foi essa observação que forneceu o primeiro critério prático pelo qual os números transcendentais poderiam ser construídos.

Antes de definirmos número transcendente, definiremos número algébrico.

Definição 5.1. *Um número α é um número algébrico, quando α é solução de alguma equação polinomial da forma:*

$$a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0,$$

onde $n \in \mathbb{N}$, $a_i \in \mathbb{Q}$ para todo $i = 1, 2, 3, \ldots, n$, $a_n \neq 0$.

Isto é, os algébricos são o conjunto das raízes de todos os polinômios com coeficientes racionais, e denotamos por $\overline{Q}$.

O polinômio minimal de α algébrico é o polinômio de menor grau tendo α como raiz. Desta feita observamos que qualquer número racional $r = \frac{p}{q}$ é algébrico, pois é raiz da equação $qx - p = 0$, onde p e q são inteiros e $q \neq 0$.

Quando tratamos dos irracionais, vemos que há irracionais que são algébricos e outros que não são algébricos.

Exemplo 5.4. *$\sqrt{3}$ é algébrico, pois é raiz da equação $x^2 - 3 = 0$.*

Na realidade, quando p é primo então $\sqrt{p}$ é irracional e algébrico, pois é raiz da equação $x^2 - p = 0$.

Definição 5.2. *Dizemos que um número $t \in \mathbb{R}$ é transcendente quando ele não é algébrico, isto é, quando não existe nenhum polinômio P com coeficientes racionais tal que $P(t) = 0$.*

Observação: Se t é transcendente, então t não pertence a $\overline{\mathbb{Q}}$.

Teorema 5.1 (Liouville)**.** *Para qualquer número algébrico α com grau $n > 1$, existe $c = c(\alpha) > 0$ tal que $\left|\alpha - \frac{p}{q}\right| > \frac{c}{q^n}$ para todos os racionais $\frac{p}{q}$, $q > 0$.*

Demonstração. Considere $f(x) = a_0 + a_1x + \ldots + a_nx^n$ polinômio não nulo minimal de α, com $a_n \neq 0$.
Ora, sabemos que todo polinômio não nulo só tem uma quantidade finita de raízes. Sendo assim, existe $\delta > 0$ tal que $[\alpha - \delta, \alpha + \delta] \cap R_f = \{\alpha\}$, onde $R_f = \{x \in \mathbb{R} \mid f(x) = 0\}$.

Dado $\frac{p}{q} \in \mathbb{Q}$ só temos duas possibilidades:

$$\frac{p}{q} \in [\alpha - \delta, \alpha + \delta] \qquad \text{ou} \qquad \frac{p}{q} \notin [\alpha - \delta, \alpha + \delta]$$

Caso 1. $\frac{p}{q} \notin [\alpha - \delta, \alpha + \delta] \Rightarrow \left|\alpha - \frac{p}{q}\right| > \delta$. Mas $\delta \geq \frac{\delta}{q^n}$, já que $q \geq 1$. Então temos $\left|\alpha - \frac{p}{q}\right| > \frac{\delta}{q^n}$.

Faça $c = \delta$ e o resultado segue.

Caso 2. $\frac{p}{q} \in [\alpha - \delta, \alpha + \delta]$. Ora, não sabemos se $\frac{p}{q}$ está entre $\alpha - \delta$ e α ou entre α e $\alpha + \delta$.

Mas a função f é contínua e derivável no intervalo com extremos α e $\frac{p}{q}$ (pois $f(x)$ é um polinômio). Logo, pelo Teorema do Valor Médio, existe ξ entre α e $\frac{p}{q}$ tal que

$$f(\alpha) - f\left(\frac{p}{q}\right) = f'(\xi)\left(\alpha - \frac{p}{q}\right).$$

Mas, $f(\alpha) = 0$, então aplicando o módulo a ambos os lados da igualdade, temos:

$$\left|f\left(\frac{p}{q}\right)\right| = |f'(\xi)|\left|\alpha - \frac{p}{q}\right|$$

Como f' é contínua no intervalo fechado com extremos α e $\frac{p}{q}$, então ela tem que admitir um máximo. Daí, existe $M \in \mathbb{Q}$ tal que $|f'(x)| \leq M$ para todo x nesse intervalo. Então temos

$$\left|f\left(\frac{p}{q}\right)\right| = |f'(\xi)|\left|\alpha - \frac{p}{q}\right| \leq M\left|\alpha - \frac{p}{q}\right| \qquad \text{(I)}$$

Agora, sabemos que $f\left(\frac{p}{q}\right) \neq 0$ e que $f\left(\frac{p}{q}\right) = \left|a_0 + a_1 \cdot \frac{p}{q} + \ldots + a_n \cdot \frac{p^n}{q^n}\right|$

$$= \left| \frac{a_0 q^n + a_1 p q^{n-1} + \ldots + a_n p^n}{q^n} \right|$$

Mas note que $a_0 q^n + a_1 p q^{n-1} + \ldots + a_n p^n$ é um inteiro e não nulo e, o menor valor que pode assumir é 1. Assim,

$$\frac{a_0 q^n + a_1 p q^{n-1} + \ldots + a_n p^n}{q^n} \geq \frac{1}{q^n}. \qquad \text{(II)}$$

Combinando as desigualdades (I) e (II) temos que

$$\left| \alpha - \frac{p}{q} \right| > \frac{1}{M \cdot q^n}$$

Mas não podemos garantir que δ é igual a $\frac{1}{M}$, então pegamos o c como o menor deles, $c = min\left\{\delta, \frac{1}{M}\right\}$.

Portanto, $\left| \alpha - \frac{p}{q} \right| > \frac{c}{q^n}$, $\forall\ \frac{p}{q} \in \mathbb{Q}$. ■

Segundo (15), números algébricos não são bem aproximados por racionais, no sentido da teoria das frações contínuas, então Liouville definiu uma classe de números que são muito bem aproximados por racionais de uma maneira muito rápida. Esses números são chamados números de Liouville.

5.3.1 Números de Liouville

Definição 5.3. *Um número ξ é chamado número de Liouville, se existe uma sequência $\left(\frac{p_j}{q_j}\right) \in \mathbb{Q}$, infinita, com $q_j > 1$ tal que*

$$\left| \xi - \frac{p_j}{q_j} \right| < \frac{1}{q_j^j}, \quad \forall j \geq 1.$$

Observe que esses números de Liouville tem uma ótima aproximação por racionais, a menos que a sequência q_j fosse limitada, pois assim essa convergência não seria tão rápida.

Proposição 5.1. *(q_j) é ilimitada.*

Demonstração. Suponha que (q_j) é limitada, isto é, existe $M \in \mathbb{Q}$ tal que $q_j \leq M$. Daí multiplicando a desigualdade $\left| \xi - \frac{p_j}{q_j} \right| < \frac{1}{q_j^j}$ por q_j, temos

$$|\xi q_j - p_j| < q_j \leq M.$$

Pela desigualdade triangular, temos

$$|p_j| - |\xi q_j| \leq |\xi q_j - p_j| \leq M \quad \Rightarrow \quad p_j \leq M + |\xi||q_j| \leq (|\xi| + 1) \cdot M.$$

Mas isso é um absurdo, pois existem infinitos $\dfrac{p_j}{q_j}$.
Note que supomos q_j limitada e obtivemos p_j limitada, pois $p_j \leq (|\xi| + 1) \cdot M$. ■

O teorema de Liouville foi uma ferramenta muito importante, culminando com esses números de Liouville. Mas como provar que esses números são transcendentes? A resposta pra isso decorre do teorema a seguir.

Teorema 5.2. *Todo número de Liouville é transcendente.*

Demonstração. Suponha que ξ é um número de Liouville e algébrico de grau n. Como ξ é de Liouville, então por definição, existe $\left(\dfrac{p_j}{q_j}\right)$ tal que

$$\left|\xi - \frac{p_j}{q_j}\right| < \frac{1}{q_j^j}, \quad \forall j \geq 1.$$

Como ξ é algébrico, pelo Teorema 5.1 de Liouville, temos:

$$\frac{c}{q_j^n} < \left|\xi - \frac{p_j}{q_j}\right| < \frac{1}{q_j^j} \quad \Rightarrow \quad \frac{c}{q_j^n} < \frac{1}{q_j^j} \quad \Rightarrow \quad q_j^{j-n} < \frac{1}{c}$$

Note que, se $j \geq n + 1$, então $q_j \leq q_j^{j-n} < \dfrac{1}{c}$, o que implica que q_j seria limitada, contradizendo a proposição 5.1. Portanto, todo número de Liouville é transcendente. ■

Liouville construiu uma classe infinita de números que satisfazem essa relação, isto é, de números transcendentes e, um desses números é o descrito no teorema a seguir.

Teorema 5.3. *O número*

$$l = \sum_{n=1}^{\infty} 10^{-n!} = 0,110001000000000000000010\ldots$$

é transcendente.

Demonstração. Para demonstrarmos que l é transcendente, basta mostrarmos que l é número de Liouville. Para isso, definamos

$$p_j = \sum_{n=1}^{j} 10^{j!-n!} \qquad e \qquad q_j = 10^{j!}.$$

Observe que p_j e q_j são inteiros, pois $n \leq j$. Note também que

$$\frac{p_j}{q_j} = \sum_{n=1}^{j} 10^{-n!},$$

ou seja, é a j-ésima soma parcial da série l. Daí

$$\left| l - \frac{p_j}{q_j} \right| = \sum_{n=1}^{\infty} 10^{-n!} - \sum_{n=1}^{j} 10^{-n!} = \sum_{n=j+1}^{\infty} 10^{-n!}.$$

Vamos provar que

$$\sum_{n=j+1}^{\infty} 10^{-n!} < \frac{1}{q_j^j}.$$

Ora,

$$\sum_{n=j+1}^{\infty} 10^{-n!} = \frac{1}{10^{(j+1)!}} + \frac{1}{10^{(j+2)!}} + \ldots = \frac{1}{10^{(j+1)!}} \left(1 + \frac{1}{10^{(j+2)!-(j+1)!}} + \frac{1}{10^{(j+3)!-(j+1)!}} + \ldots \right).$$

Agora observe que $(j+k)! - (j+1)! \geq k-1$, para $k \geq 2$. De fato,

$(j+k)!-(j+1)! = (j+1)![(j+k)\ldots(j+2)-1]$. Como $j \geq 1$, temos $j+k > k$. Assim,

$(j+1)![(j+k)\ldots(j+2)-1] > k-1$. O que implica

$$\left| l - \frac{p_j}{q_j} \right| < \frac{1}{10^{(j+1)!}} \left(1 + \frac{1}{10} + \frac{1}{10^2} + \ldots \right) = \frac{1}{10^{(j+1)!}} \cdot \left(\frac{1}{1 - \frac{1}{10}} \right) = \frac{10}{9 \cdot 10^{(j+1)!}} < \frac{1}{10^{(j+1)!-1}}.$$

Se mostrarmos que $\frac{1}{10^{(j+1)!-1}} < \frac{1}{q_j^j}$ o nosso problema estará resolvido.

Ora, para mostrar que $\frac{1}{10^{(j+1)!-1}} < \frac{1}{q_j^j} = \frac{1}{10^{j!j}}$, basta mostrar que $(j+1)!-1 \geq j!j$. De fato,

$$(j+1)! - 1 = (j+1) \cdot j! - 1 = j!j + j! - 1 \geq j!j.$$

Portanto, $\left| l - \frac{p_j}{q_j} \right| < \frac{1}{q_j^j}$, ou seja, l é número de Liouville. Consequentemente,

$$l = \sum_{n=1}^{\infty} 10^{-n!} = 0,110001000000000000000010\ldots$$

é transcendente. ■

Este número é um exemplo de que existem números transcendentes. Na verdade, nós provamos mais que isso, pois podemos trocar o 10 por qualquer número maior ou igual a 2, inteiro, que teríamos a representação de um número de Liouville em outra base. Ou seja,

$$l = \sum_{n=1}^{\infty} b^{-n!}.$$

Georg Cantor mostrou que quase todo número é transcendente. De fato, se colocarmos os números transcendentes e os algébricos na reta real, veremos que os algébricos

são invisíveis dentro da reta. Para isso Cantor mostrou que a cardinalidade dos números algébricos é a mesma de $\mathbb{N}$, enquanto a cardinalidade dos números transcendentes é a mesma de $\mathbb{R}$.

Outros exemplos, bem mais conhecidos, de números transcendentes, são:

$$e = 2,718281\ldots, \quad \pi = 3,141592\ldots, \quad e^{\pi} = 23,140692\ldots, \quad \log\alpha, \alpha \neq 1.$$

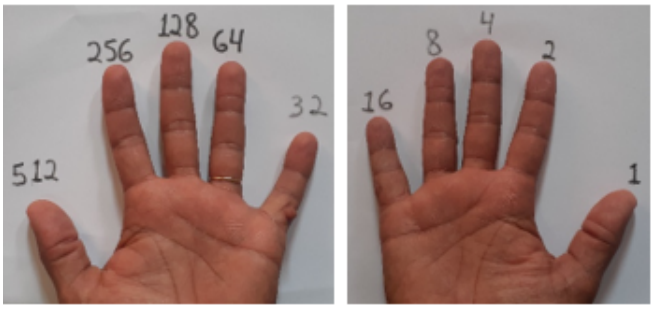
Alguns problemas em aberto: $e + \pi$ é transcendente? π^e é transcendente? e^e é transcendente? π^{π} é transcendente? Para maiores informações sobre números transcendentes, veja (15).

6 Implementação

Diante do que temos visto até agora, não podemos deixar de contemplar o ensino na sala de aula, tendo em vista o objetivo deste curso que é o aperfeiçoamento do professor e da transmissão do conhecimento de forma compreensível e atrativa. Para isso, de forma a otimizar o aprendizado da matemática em sala de aula, intencionamos fazer uma implementação da representação dos números binários com os dedos das mãos, isto é, contar em binário com as mãos. E, ao fazer isso, temos a intenção de familiarizar os alunos com os números binários, suas representações e operações e, isto, de forma compreensível e atrativa.

Pois bem, como tratamos em capítulos anteriores, os números binários são representados por apenas dois algarismos: 0 e 1, que são os possíveis restos da divisão por 2. Utilizando as mãos, representamos os zeros com os dedos abaixados e os uns com os dedos levantados. No nosso exemplo, diremos que o 1 é representado pelo polegar direito e, que cada dedo das mãos representa uma potência de 2, como é visto na figura 3 a seguir, onde o dedo 1 representa o número 1, o dedo 2 representa o número 2, o dedo 3 representa o número 4, o dedo 4 representa o número 8 e, assim, por diante.

Figura 3 – Potências de 2 representadas pelos dedos



Fonte: O autor

Com isso podemos combinar os dedos para representar os números naturais na base 2, visto que todo número natural pode ser representado como soma de potências de 2.

Observe na tabela 1 a representação e a expansão de alguns primeiros números na base 2, tendo em vista que queremos apenas exemplificar e esclarecer a representação de um número decimal como soma de potências de 2, o que também vale para todo número natural.

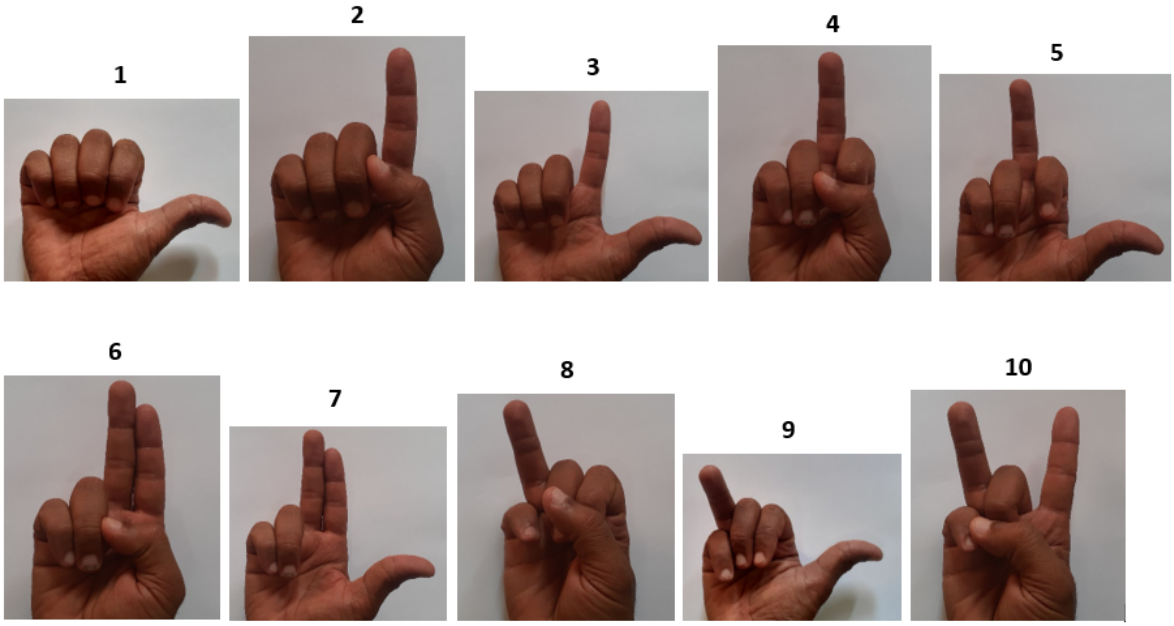
Note que cada número na base 10 tem representação na base 2 cuja expansão é formada por potências de 2. Se somarmos todos os números da expansão resultará no número na base 10.

Base decimal	Base binária	Expansão
0	0	0 uns
1	1	1 um
2	10	1 dois e 0 uns
3	11	1 dois e 1 um
4	100	1 quatro, 0 dois e 0 uns
5	101	1 quatro, 0 dois e 1 um
6	110	1 quatro, 1 dois e 0 uns
7	111	1 quatro, 1 dois e 1 um
8	1000	1 oito, 0 quatros, 0 dois e 0 uns
9	1001	1 oito, 0 quatros, 0 dois e 1 um
10	1010	1 oito, 0 quatros, 1 dois e 0 uns
11	1011	1 oito, 0 quatros, 1 dois e 1 um
12	1100	1 oito, 1 quatro, 0 dois e 0 uns
13	1101	1 oito, 1 quatro, 0 dois e 1 um
14	1110	1 oito, 1 quatro, 1 dois e 0 uns
15	1111	1 oito, 1 quatro, 1 dois e 1 um
16	10000	1 dezesseis, 0 oitos, 0 quatros, 0 dois e 0 uns
...	...	...

Tabela 1 – Decimal, binário e expansão.

A seguir, observamos a representação dos números de 1 a 10 na base 2, utilizando os dedos das mãos.

Figura 4 – Números de 1 a 10 na base 2



Fonte: O autor

Com os dedos da mão direita podemos representar até o número 31, que é quando todos os dedos estão levantados. Para representar o número 32 utilizamos a mão esquerda

e, continuamos contando utilizando as duas mãos. O máximo que podemos contar em binário com os dedos das mãos é até 1023, que é quando todos os dedos das mãos estão levantados, como é mostrado na figura 5.

Figura 5 – 1023 na base 2

Fonte: O autor

Este valor é resultado da soma dos valores correspondentes a todos os dedos, isto é, $512 + 256 + 128 + 64 + 32 + 16 + 8 + 4 + 2 + 1 = 1023$.

Vejamos mais alguns exemplos.

Exemplo 6.1. *Representar o número 95 na base 2.*

Sabemos que para representar na base 2 fazemos a divisão sucessiva por 2, separamos os restos e continuamos dividindo até chegar em quociente 1 e resto zero. Pegamos o último quociente e todos os restos e escrevemos, nessa ordem, a representação. Outrossim, quando estamos dividindo, o que estamos fazendo é pegando a maior potência de 2 menor que o número e subtraindo do número. Neste caso, a maior potência de 2 menor que 95 é 64 e sobram 31; agora, a maior potência de 2 menor que 31 é 16 e sobram 15; continuamos até obtermos $64 + 16 + 8 + 4 + 2 + 1 = 95$. Dessa forma, basta levantar os dedos representados por esses números, como está indicado na figura 6. Em números, $95 = (1011111)_2$.

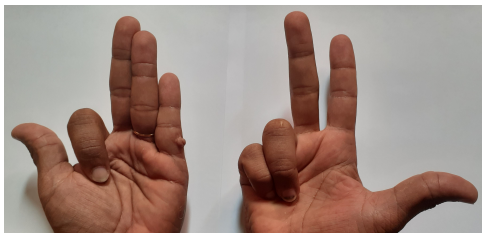
Figura 6 – 95 na base 2

Fonte: O autor

Exemplo 6.2. *Representar o número 743 na base 2.*

Analogamente, como no exemplo 6.1, obtemos a soma $512+128+64+32+4+2+1 = 743$ e chegamos à representação como na figura 7. Em números, $743 = (1011100111)_2$.

Figura 7 – 743 na base 2



Fonte: O autor

Deixamos no Apêndice A um questionário como sugestão de atividade que pode ser respondido livremente pelo leitor ou por qualquer aluno coagido a isso.

6.1 Sequência Didática

Nesta seção sugerimos uma sequência didática, que pode ser aplicada nas aulas em turmas dos sextos anos, como estratégia de melhoria do aprendizado dos estudantes, visando dar mais sentido ao processo de ensino e aumentar o engajamento dos estudantes nas atividades pedagógicas.

Sequência Didática

Turma: 6^o ano

Duração: 04 aulas de 50 minutos

Recursos: Livros didáticos, revistas, artigos, jornais, sites de internet, entre outros.

Disciplina: Matemática

Tema: Representação dos números binários com os dedos das mãos

Justificativa

O mundo onde vivemos se constitui um conjunto de fenômenos naturais e sociais. Sendo assim, pretende-se conduzir uma série de atividades que facilitem a aquisição e a construção de conhecimentos acerca da representação dos números binários, onde o interesse se desenvolva através das diversidades sociais históricas e culturais, bem como, nas representações das diversas linguagens, na curiosidade, nos jogos, nas habilidades: físicas, motoras e perceptivas, na leitura de imagens e de sons, buscando integrar as diversas áreas de ensino.

Uma das maneiras de auxiliar os estudantes a enfrentarem as dificuldades de suas vidas, é proporcionar experiências que incentivem as descobertas de suas habilidades e atitudes essenciais para perceber a importância de uma linguagem simbólica universal na representação e modelagem de situações matemáticas como forma de comunicação.

Objetivos

- Despertar o interesse pela pesquisa.
- Ampliar a compreensão que o estudante tem acerca dos números binários e suas representações.
- Oferecer oportunidades para que os estudantes possam expor o que sabem sobre os números binários e suas representações.
- Relacionar a matemática com outras áreas de ensino.

Sequência

1^a aula

- Leitura do livro didático.
- Explicitação, em primeira instância, dos números binários; fatos históricos.

2^a aula

- Pesquisa sobre a utilização dos números binários em áreas afins, como computação.
- Escrever um trabalho em pautado ou cartolina sobre os números binários e sua utilização.

3^a aula

- Representação dos números binários com os dedos das mãos.
- Interação com os alunos.

4^a aula

- Fechamento.
- Apresentação dos trabalhos.

Avaliação (através de:)

- Exercícios
- Participação
- Interpretação

Vale salientar que, para a aplicação dessa sequência, é necessário que, em aulas anteriores tenha se tratado acerca do sistema de numeração decimal, para só então falar de outros sistemas de numeração, como o sistema binário. Sendo assim, faz-se referência à habilidade (EF06MA02) da BNCC.

7 Problemas Olímpicos Envolvendo Sistemas de Numeração

Observamos que as Olimpíadas de Matemática vêm se destacando de forma crescente nas escolas, vêm ganhando mais espaço e atração por parte daqueles que amam a matemática. Sendo assim, neste capítulo descreveremos alguns problemas de Olimpíadas de Matemática que fazem jus ao que estamos estudando.

Problema 1

(Olimpíada do Canadá 1977 P3) O número N é um inteiro que possui representação na base b igual a 777, ou seja, $N = (777)_b$. Calcule o menor inteiro positivo b tal que N é a quarta potência de algum inteiro.
Solução:

Se reescrevermos N na base 10, temos o seguinte:

$$N = 7b^2 + 7b + 7 = 7(b^2 + b + 1)$$

Conforme o enunciado, N é a quarta potência de algum inteiro, ou seja, $N = 7(b^2+b+1) = a^4$, para algum inteiro a. Temos, então, que $7 \mid a^4$.
Como $7 \mid a^4$ e 7 é um número primo, então $a^4 \geq 7^4$. Sendo assim, queremos o menor inteiro positivo b que satisfaça o enunciado e, para tal podemos verificar que $a = 7$ funciona. Portanto, quando $a = 7$, temos

$$7(b^2 + b + 1) = 7^4 \Rightarrow b^2 + b + 1 = 7^3$$

Resolvendo a equação do segundo grau em b, encontramos $b = 18$.

Problema 2

(SL IMO 1998 N8) Seja $a_0, a_1, a_2, \ldots$ uma sequência crescente de inteiros não negativos tal que cada número inteiro não negativo possa ser escrito de forma única como

$$a_i + 2a_j + 4a_k \qquad (7.1)$$

onde i, j, k não são necessariamente diferentes. Determine a_{1998}.
Solução: Adaptado de (16).

Observe que, o que devemos fazer é escrever, de forma única, os números inteiros não negativos como uma combinação linear dos elementos da sequência (a_n). Isto leva a que, dada a sequência até o termo de ordem $n-1$, isto é, $a_0, a_1, \ldots, a_{n-1}$, então o termo de ordem n, ou seja, a_n, é o menor inteiro positivo que não seja da forma $a_i + 2a_j + 4a_k$, com $i, j, k < n$.
Vamos encontrar os primeiros termos da sequência de forma intuitiva. O primeiro inteiro não negativo é o zero. Para escrever zero na forma (7.1) devemos ter $a_0 = 0$:

$$0 = a_0 + 2a_0 + 4a_0 = 0 + 2 \cdot 0 + 4 \cdot 0$$

Não temos como escrever 1 usando somente $a_0 = 0$. Isto leva a adicionar o número 1 na sequência (a_n), logo $a_1 = 1$. Com isso podemos escrever os números do 1 ao 7 usando somente dois elementos da sequência $a_0 = 0$, $a_1 = 1$:

$$\begin{aligned}
1 &= a_1 + 2a_0 + 4a_0 = 1 + 2 \cdot 0 + 4 \cdot 0,\\
2 &= a_0 + 2a_1 + 4a_0 = 0 + 2 \cdot 1 + 4 \cdot 0,\\
3 &= a_1 + 2a_1 + 4a_0 = 1 + 2 \cdot 1 + 4 \cdot 0,\\
4 &= a_0 + 2a_0 + 4a_1 = 0 + 2 \cdot 0 + 4 \cdot 1,\\
5 &= a_1 + 2a_0 + 4a_1 = 1 + 2 \cdot 0 + 4 \cdot 1\\
6 &= a_0 + 2a_1 + 4a_1 = 0 + 2 \cdot 1 + 4 \cdot 1,\\
7 &= a_1 + 2a_1 + 4a_1 = 1 + 2 \cdot 1 + 4 \cdot 1.
\end{aligned}$$

O número 8 não pode ser escrito usando somente dois elementos da sequência: $a_0 = 0$, $a_1 = 1$. Isto leva a adicionar o número 8 na sequência (a_n), logo $a_2 = 8$:

$$8 = a_2 + 2a_0 + 4a_0 = 8 + 2 \cdot 0 + 4 \cdot 0$$

O número 9 não pode ser escrito usando somente três elementos da sequência: $a_0 = 0$, $a_1 = 1$, $a_2 = 8$. Isto leva a adicionar o número 9 na sequência (a_n), logo $a_3 = 9$. Com quatro elementos da sequência é possível escrever os números do 9 até o 63:

$$\begin{aligned}
9 &= a_3 + 2a_0 + 4a_0 = 9 + 2 \cdot 0 + 4 \cdot 0,\\
63 &= a_3 + 2a_3 + 4a_3 = 9 + 2 \cdot 9 + 4 \cdot 9.
\end{aligned}$$

Segue que $a_4 = 64$ e $a_5 = 65$. Depois dessas pequenas experimentações descobrimos os primeiros termos da sequência que são $(a_n) = (0, 1, 8, 9, 64, 65, \ldots)$.

Sabemos que todo número inteiro não negativo m pode ser escrito de forma única na base binária:

$$m = 2^0 t_0 + 2^1 t_1 + 2^2 t_2 + 2^3 t_3 + \ldots + 2^r t_r \qquad (7.2)$$

com $t_i \in \{0, 1\}$ e $i = 0, 1, 2, \ldots, r$. Outrossim, queremos escrever m como em (7.1):

$$m = 2^0 a_i + 2^1 a_j + 2^2 a_k \qquad (7.3)$$

Comparando (7.2) e (7.3) sugere-se escolher a_i, a_j e a_k como somas finitas, como seguem:

$$\begin{aligned} a_i &= t_0 + 2^3 t_3 + 2^6 t_6 + \ldots = t_0 + 8t_3 + 8^2 t_6 + \ldots \\ a_j &= t_1 + 2^3 t_4 + 2^6 t_7 + \ldots = t_1 + 8t_4 + 8^2 t_7 + \ldots \\ a_k &= t_2 + 2^3 t_5 + 2^6 t_8 + \ldots = t_2 + 8t_5 + 8^2 t_8 + \ldots \end{aligned}$$

Podemos reescrever essas três equações anteriores como

$$a_n = s_0 + 8s_1 + 8^2 s_2 + \ldots + 8^r s_r \qquad (7.4)$$

onde $s_i \in \{0, 1\}$ e $i = 0, 1, 2, \ldots, r$. Em palavras, a sequência (a_n) consiste dos números inteiros não negativos que podem ser escritos em base 8 usando somente zeros e uns. Para encontrar um termo arbitrário de (a_n) devemos escrever primeiro n em base 2:

$$n = s_0 + 2s_1 + 2^2 s_2 + \ldots + 2^r s_r \qquad (7.5)$$

Os s_i em (7.5) coincidem com os s_i em (7.4). Observe os primeiros termos já encontrados

$$\begin{aligned} 0 = 0 + 2 \cdot 0 \ , \ a_0 &= 0 + 8 \cdot 0 = 0, \\ 1 = 1 + 2 \cdot 0 \ , \ a_1 &= 1 + 8 \cdot 0 = 1, \\ 2 = 0 + 2 \cdot 1 + 2^2 \cdot 0 \ , \ a_2 &= 0 + 8 \cdot 1 + 8^2 \cdot 0 = 8, \\ 3 = 1 + 2 \cdot 1 + 2^2 \cdot 0 \ , \ a_3 &= 1 + 8 \cdot 1 + 8^2 \cdot 0 = 9, \\ 4 = 0 + 2 \cdot 0 + 2^2 \cdot 1 + 2^3 \cdot 0 \ , \ a_4 &= 0 + 8 \cdot 0 + 8^2 \cdot 1 + 8^3 \cdot 0 = 64, \\ 5 = 1 + 2 \cdot 0 + 2^2 \cdot 1 + 2^3 \cdot 0 \ , \ a_5 &= 1 + 8 \cdot 0 + 8^2 \cdot 1 + 8^3 \cdot 0 = 65. \end{aligned}$$

Como queremos encontrar a_{1998} escreveremos primeiro $1998 = (11111001110)_2$ em base 2:

$$1998 = 0 + 2 \cdot 1 + 2^2 \cdot 1 + 2^3 \cdot 1 + 2^4 \cdot 0 + 2^5 \cdot 0 + 2^6 \cdot 1 + 2^7 \cdot 1 + 2^8 \cdot 1 + 2^9 \cdot 1 + 2^{10} \cdot 1$$

Segue que

$$a_{1998} = 0 + 8 \cdot 1 + 8^2 \cdot 1 + 8^3 \cdot 1 + 8^4 \cdot 0 + 8^5 \cdot 0 + 8^6 \cdot 1 + 8^7 \cdot 1 + 8^8 \cdot 1 + 8^9 \cdot 1 + 8^{10} \cdot 1 = 1227096648.$$

Problema 3

(OBM 2020 P3 Nível 2) Consideremos uma sequência infinita $x_1, x_2, \ldots$ de números inteiros positivos tais que, para todo inteiro $n \geq 1$:

- Se x_n é par, então $x_{n+1} = \dfrac{x_n}{2}$;
- Se x_n é ímpar, então $x_{n+1} = \dfrac{x_n - 1}{2} + 2^{k-1}$, onde k é o inteiro tal que $2^{k-1} \leq x_n < 2^k$.

Determine o menor valor possível de x_1 para o qual a sequência contenha algum termo igual a 2020.

Solução:

Observe que, se dizemos que um inteiro positivo y é tal que $10^{m-1} \leq y < 10^m$, onde m também é inteiro e positivo, sabemos que y possui m algarismos na base 10. Mas, se dizemos que $2^{m-1} \leq y < 2^m$, então sabemos que y possui m algarismos na base 2. Portanto, sabemos que x_n possui k algarismos na base decimal (note que $2 = (10)_2$).

Com isso, podemos dizer que $x_n = (\overline{a_1a_2a_3a_4\ldots a_k})_2$, com $a_1, a_2, \ldots, a_k \in \{0, 1\}$. Colocamos a barra para não confundir com o produto dos a_i. Agora, temos que analisar dois casos:

$a_k = 0 \Rightarrow x_n$ é par, ou $a_k = 1 \Rightarrow x_n$ é ímpar.

No primeiro caso, temos que

$x_{n+1} = \dfrac{(\overline{a_1a_2a_3\ldots a_{k-1}0})_2}{2} \Rightarrow x_{n+1} = \left(\dfrac{\overline{a_1a_2a_3\ldots a_{k-1}0}}{10}\right)$

$\Rightarrow x_{n+1} = (\overline{a_1a_2a_3\ldots a_{k-1}})_2$. Ou seja, dividir por 2 é apagar o último algarismo, o zero.

Agora, se $a_k = 1$, temos que $x_{n+1} = \dfrac{(\overline{a_1a_2a_3\ldots a_{k-1}1})_2 - 1}{2} + 2^{k-1}$

$\Rightarrow x_{n+1} = \left(\dfrac{\overline{a_1a_2a_3\ldots a_{k-1}0}}{10}\right)_2 + (10^{k-1})_2 \Rightarrow x_{n+1} = (\overline{a_1a_2a_3\ldots a_{k-1}})_2 + (10^{k-1})_2$.

Observe que 10^{k-1} possui k algarismos, e que o seu k-ésimo algarismo é o 1, e $a_1a_2a_3\ldots a_{k-1}$ possui $k-1$ algarismos. Logo, $x_{n+1} = (\overline{1a_1a_2a_3\ldots a_{k-1}})_2$. No primeiro caso, x_{n+1} possui $k-1$ algarismos na base 2, enquanto, no segundo caso, x_{n+1} possui k algarismos na base 2. Isso nos diz que, para qualquer x_n, formamos um número que possui a mesma quantidade de algarismos na base 2 ou que tem menos algarismos na base 2. Observe um exemplo pra entendermos melhor o que está acontecendo:

Se $x_n = 1101001$, então $k = 7$

então $\dfrac{x_n - 1}{2} = 110100$ e $2^{k-1} = 2^6 = 1000000$. Daí

$\dfrac{x_n - 1}{2} + 2^{k-1} = 1000000 + 110100 = 1110100$. Ou seja, o que essa soma faz é transferir o último algarismo de x_n para o início.

Fazendo divisões sucessivas por 2 encontramos $2020 = (11111100100)_2$, que tem 11 algarismos. Daí, se quisermos começar com um número menor possível, então devemos começar com 11 algarismos. Esse número de 11 algarismos tem que ter, em algum lugar, um termo igual a 2020.

Se $x_{n+1} = 2020$, temos duas possibilidades para x_n : 4040 ou 1993. No entanto,

se $x_n = 4040 = (111111001000)_2$, isso significa que x_{n-1} teria mais algarismos na base binária que x_{n+1}, ou seja, x_{n-1} seria maior que x_{n+1}, o que não pode ocorrer. O mesmo ocorre para $x_{n-2}, x_{n-3}, \ldots, x_1$. Logo, vamos dizer que $x_n = 1993 = (11111001001)_2$. Assim, basta realizarmos os passos inversos das condições dadas, e encontraremos que $x_1 = (10010011111)_2 = 1183$. Logo, o menor x_1 que determina uma sequência onde 2020 aparece é $x_1 = 1183$.

Conclusão e Projetos Futuros

Observamos que o professor é desafiado constantemente em sala de aula, no sentido de que, a cada dia o mesmo precisa inovar, renovar, trazer brilho às suas aulas de forma que os alunos se sintam atraídos pelo conhecimento. Sendo assim, neste trabalho buscamos uma forma de diminuir a formalidade ou a monotonicidade quando fazemos uma implementação do tema proposto.

Pensando na importância, buscamos referências que o justificassem, foi o que fizemos no Capítulo 1 quando mencionamos autores que trataram acerca do tema proposto, bem como fizemos menção da BNCC, documento pelo qual devemos nos guiar para lecionar no ensino básico.

No capítulo 2 descrevemos a teoria matemática, isto é, a aritmética que introduz de forma elementar conceitos e propriedades que usamos em capítulos posteriores.

No capítulo 3 começamos a tratar do tema com mais precisão quando descrevemos acerca da representação dos números naturais, vimos conversão entre bases e as principais operações, como também alguns critérios de divisibilidade, tudo isso em uma base arbitrária.

No capítulo 4 descrevemos acerca da representação dos números racionais, da importância da Longa Divisão Euclidiana para representá-los numa base qualquer e extraímos algumas propriedades interessantes inerentes aos números racionais.

No capítulo 5, para atingirmos nosso objetivo final, descrevemos acerca da representação dos números reais, mais precisamente os irracionais. Vimos que os números reais são resultados de medições e que todo número real pode ser representado por aproximações sucessivas utilizando racionais. Vimos que a representação dos irracionais em uma base arbitrária se constrói de forma análoga aos racionais e demos exemplos em que isso se justifica. Por fim, descrevemos acerca dos números transcendentes, até então desconhecidos do autor, mas que aclarou um pouco mais acerca dos números reais. Fizemos menção do número de Liouville que nos fornece uma forma de saber se um número é transcendente. Além disso, o número de Liouville é uma prova de que existem números transcendentes.

No capítulo 6 fizemos uma implementação da representação dos números binários com os dedos das mãos, servindo de auxílio pedagógico a todos que quiserem adotar essa implementação para abrilhantar suas aulas. É importante que o professor que queira utilizar essa implementação em suas aulas tenha pleno domínio acerca do tema e se adeque à sua realidade na sala de aula.

Por fim, no capítulo 7 descrevemos alguns problemas de olimpíadas de matemática fazendo jus ao que estamos estudando.

Pois bem, diante do exposto descrevemos acerca da representação dos números reais de forma a conscientizar o leitor sobre o importante papel que as representações assumem na aprendizagem e no ensino da matemática, pois, como aprendemos com Duval, não há como um sujeito mobilizar qualquer conhecimento sem realizar uma atividade de representação. A respeito disso é importante lembrar que um objeto matemático pode ter diversas representações. Daí, o professor, ao representar um objeto, deve fazê-lo nas suas diversas representações, pois assim aumentará as capacidades cognitivas do aluno e, consequentemente, potencializará as suas representações mentais.

Referências

1 FERREIRA, A. B. d. H. *Dicionário Eletrônico Aurélio Século XXI, Versão 3.0.1 CD-ROM*. Rio de Janeiro: Editora Nova Fronteira e Lexikon Informática, 1999.

2 PATRICIO, R. S. *As dificuldades relacionadas à aprendizagem do conceito de vetor à luz da teoria dos registros de representação semiótica. Dissertação (Mestrado) - Curso de Mestrado em Educação em Ciências e Matemática, Universidade Federal do Pará*. Belém: [s.n.], 2011.

3 DUVAL, R. *Quel cognitif retenir en didactique des mathématiques? RDM, v.16, n.3, p.349-382*. Disponível em: https://revue-rdm.com/1996/quel-cognitif-retenir-en/. Acessado em: 21/01/2021: [s.n.], 1996.

4 DUVAL, R. *Registros de Representação Semiótica e Funcionamento Cognitivo do Pensamento. Trad. MORETTI, M.T.* ***Revemat****, v.7 n.2*. Disponível em: https://dx.doi.org/10.5007/1981-1322.2012v7n2p266. Acessado em: 21/01/2021: [s.n.], 2012.

5 BRASIL. *Ministério da Educação. Base Nacional Comum Curricular*. Brasília: [s.n.], 2018.

6 COUTINHO, S. C. *Números Inteiros e Criptografia RSA*. Rio de Janeiro: IMPA, 2009.

7 CELESTINO, M. J. *Criptografia El Gamal. Monografia (Graduação) - Curso de Licenciatura Plena em Matemática, Universidade Federal Rural de Pernambuco*. Recife: [s.n.], 2014.

8 HEFEZ, A. *Aritmética - Coleção Profmat*. Rio de Janeiro: SBM, 2016.

9 KIRILOV, E. L. *Representação decimal dos números racionais*. Disponível em: https://docs.ufpr.br/∼ akirilov/ensino/2017/docs/racionais_kirilov_linck.pdf. Acessado em: 13/01/2021: UFPR, 2017.

10 KALMAN, D. *Fractions with Cyclic Digit Patterns*. [S.l.]: College Math Journal 27, 1996 pp. 109–115.

11 LEAVITT, W. G. *A THEOREM ON REPEATING DECIMALS*. [S.l.]: Faculty Publications, Department of Mathematics. 48, 1967.

12 WIKIPEDIA. *Cyclic Number*. Disponível em https://pt.qaz.wiki/wiki/Cyclic-number. Acessado em 04/01/2021: [s.n.], 2021.

13 LIMA, E. L. *Curso de análise v.1 13. ed.* Rio de Janeiro: Associação Instituto Nacional de Matemática Pura e Aplicada, 2011.

14 BACKER, A. *Transcendental Number Theory*. [S.l.]: Cambrigde University Press, 1975.

15 MARQUES, D. *Teoria dos Números Transcendentes. Coleção Matemática Universitária*. Rio de Janeiro: SBM, 2013.

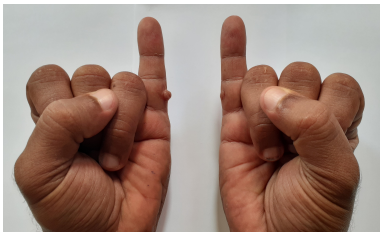
16 LINARES, J. L. *Problemas Resolvidos sobre Sequências no Treinamento de Estudantes do Ensino Médio para Olimpíadas Internacionais de Matemática. Dissertação - Mestrado Profissional em Matemática em Rede Nacional, Universidade Federal de São Carlos.* São Carlos: [s.n.], 2019.

Apêndices

APÊNDICE A – Sugestão de Atividade

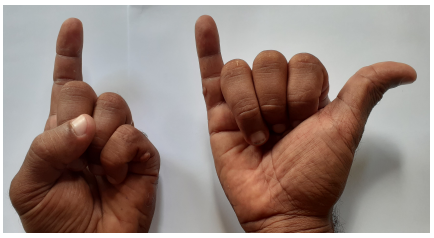
1. Como representar com os dedos das mãos o número 387 na base 2?

2. Qual número na base 10 está representado pelos dedos das mãos na figura a seguir?



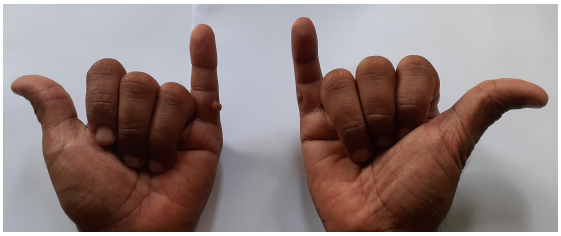
   a) 33
   b) 36
   c) 48
   d) 64

3. Qual número na base 10 está representado pelos dedos das mãos na figura a seguir?



   a) 81
   b) 141
   c) 217
   d) 273

4. Qual número na base 10 está representado pelos dedos das mãos na figura a seguir?



a) 34

b) 561

c) 657

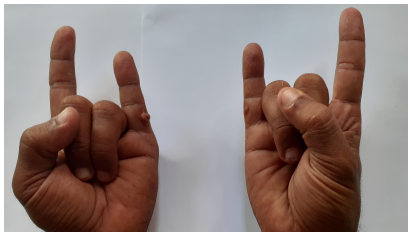
d) 705

5. Qual número na base 10 é representado quando apenas os dedos 1 e 5 estão levantados?

6. Qual número na base 10 é representado quando apenas todos os dedos da mão esquerda estão levantados?

7. Como representamos o número duzentos, na base 2, com os dedos das mãos?

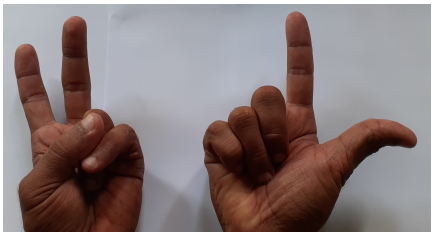
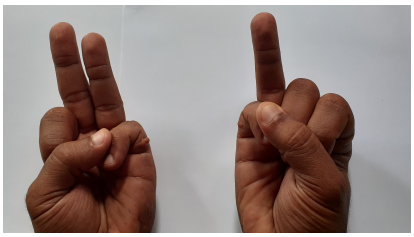
8. Qual número na base 10 está representado pelos dedos das mãos na figura a seguir?



9. Se dos dez dedos baixarmos os dois maiores dedos, qual número estará representado na base 2?

10. Zé Carlos foi ao mercado levando 10 reais e comprou dois salgadinhos de mesmo valor. Quando chegou em casa, foi indagado pelo seu irmão Cristiano sobre quanto custou cada salgadinho. Zé Carlos preferiu responder quanto sobrou do seu dinheiro. Para isso, ele fez o sinal de vitória utilizando dois dedos da mão direita, embora seu irmão não tenha entendido muito. Se Zé Carlos representou o valor que sobrou na base 2, pergunta-se: quanto custou cada salgadinho?

Gabarito

1. 
2. C
3. D
4. B
5. 17
6. 992
7. 
8. 306
9. 891
10. 2 reais