Universidade Federal de Uberlândia

Faculdade de Matemática

Programa de Mestrado Profissional em Matemática em Rede Nacional

ANALISANDO CRITÉRIOS DE DIVISIBILIDADE EM DIFERENTES BASES NUMÉRICAS

Fidélio Augustus Souki Gontijo

Uberlândia-MG

2025

Fidélio Augustus Souki Gontijo

ANALISANDO CRITÉRIOS DE DIVISIBILIDADE EM DIFERENTES BASES NUMÉRICAS

Dissertação apresentada ao Programa de Pós-Graduação em Matemática da Universidade Federal de Uberlândia, como parte dos requisitos para a obtenção de título de **MESTRE EM MATEMÁTICA**.

Área de concentração: Matemática
Linha de pesquisa: Teoria dos Números

Orientador(a): Marcus Augusto Bronzi

Uberlândia-MG
2025

Ficha Catalográfica Online do Sistema de Bibliotecas da UFU
com dados informados pelo(a) próprio(a) autor(a).

G641
2025

Gontijo, Fidélio Augustus Souki, 1996-
Analisando critérios de divisibilidade em diferentes bases numéricas [recurso eletrônico] / Fidélio Augustus Souki Gontijo. - 2025.

Orientador: Marcus Augusto Bronzi.
Dissertação (Mestrado) - Universidade Federal de Uberlândia, Pós-graduação em Matemática.
Modo de acesso: Internet.
Disponível em: http://doi.org/10.14393/ufu.di.2025.377
Inclui bibliografia.
Inclui ilustrações.

1. Matemática. I. Bronzi, Marcus Augusto,1982-, (Orient.). II. Universidade Federal de Uberlândia. Pós-graduação em Matemática. III. Título.

CDU: 51

Bibliotecários responsáveis pela estrutura de acordo com o AACR2:
Gizele Cristine Nunes do Couto - CRB6/2091
Nelson Marcos Ferreira - CRB6/3074

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
Coordenação do Programa de Pós-Graduação em Matemática em Rede Nacional
Av. João Naves de Ávila, 2121, Bloco 1F - Bairro Santa Mônica, Uberlândia-MG, CEP 38400-902
Telefone: (34) 3230-9452 - www.ime.ufu.br - profmat@ime.ufu.br

ATA DE DEFESA - PÓS-GRADUAÇÃO

Programa de Pós-Graduação em:	Mestrado Profissional em Matemática em Rede Nacional - PPGMPMAT UFU				
Defesa de:	Dissertação de Mestrado Profissional, 02, PPGMPMAT				
Data:	Vinte e sete de junho de dois mil e vinte e cinco	Hora de início:	14:00	Hora de encerramento:	16:00
Matrícula do Discente:	12312PFT006				
Nome do Discente:	Fidélio Augustus Souki Gontijo				
Título do Trabalho:	Analisando Critérios de Divisibilidade em Diferentes Bases Numéricas				
Área de concentração:	Matemática na Educação Básica				
Linha de pesquisa:	Matemática na Educação Básica e suas Tecnologias				
Projeto de Pesquisa de vinculação:	Não há				

Reuniu-se em webconferência pela plataforma ConferênciaWeb, a Banca Examinadora aprovada pelo Colegiado do Programa de Pós-graduação em Matemática - Mestrado Profissional em Matemática em Rede Nacional (PPGMPMAT). A Banca foi composta pelos professores doutores: Tatiana Miguel Rodrigues - UNESP, campus Bauru-SP; Aldicio José Miranda - IME/UFU e Marcus Augusto Bronzi - IME/UFU, orientador do candidato e presidente da sessão.

Iniciando os trabalhos, o presidente da mesa, Prof. Dr. Marcus Augusto Bronzi, apresentou os membros da Comissão Examinadora e, juntamente com o candidato, agradeceu a presença de todos os participantes. Posteriormente, o presidente concedeu a palavra ao discente para a exposição de sua dissertação e do produto educacional desenvolvido. A duração da apresentação do discente e o tempo de arguição e resposta foram conforme as normas do Programa.

Dando continuidade, o presidente da sessão concedeu a palavra aos examinadores, que procederam à arguição do discente. Ultimada a arguição, que se desenvolveu dentro dos termos regimentais, a Banca reuniu-se em sessão secreta e, após análise criteriosa, decidiu aprovar tanto a dissertação quanto o produto educacional apresentados pelo candidato.

A Banca, então, atribuiu o resultado final considerando o candidato:

Aprovado

Esta defesa faz parte dos requisitos necessários à obtenção do título de Mestre.

O competente diploma será expedido após cumprimento dos demais requisitos, conforme as normas do Programa, a legislação pertinente e a regulamentação interna da UFU

Nada mais havendo a tratar foram encerrados os trabalhos. Foi lavrada a presente ata que após lida e achada conforme foi assinada pela Banca Examinadora.

Documento assinado eletronicamente por **Marcus Augusto Bronzi**, **Presidente**, em 27/06/2025, às 15:35, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Aldicio José Miranda**, **Professor(a) do Magistério Superior**, em 27/06/2025, às 15:36, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Tatiana Miguel Rodrigues**, **Usuário Externo**, em 27/06/2025, às 15:37, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

"Uma máquina consegue fazer o trabalho de 50 homens ordinários. Nenhuma máquina consegue fazer o trabalho de um homem extraordinário.”
Elbert Hubbard

Agradecimentos

A realização deste trabalho não teria sido possível sem o apoio, incentivo e presença de pessoas fundamentais em minha vida.

Agradeço, em primeiro lugar, aos meus pais, que me ensinaram, com exemplo e dedicação, o valor do esforço, da educação e da persistência. Obrigado por nunca deixarem faltar apoio, por acreditarem em mim, mesmo nos momentos mais difíceis, e por serem a base sólida sobre a qual construí este caminho.

Ao meu irmão, minha referência de companheirismo e amizade, agradeço por estar sempre ao meu lado, com palavras de incentivo e gestos que me fortaleceram ao longo dessa jornada. Sua presença foi essencial para que eu mantivesse o foco e o equilíbrio.

À minha namorada, agradeço pela paciência, pelo carinho e pela compreensão nos momentos de ausência e cansaço. Sua companhia amorosa foi um alívio necessário nos dias mais exigentes e uma fonte constante de motivação.

Ao meu orientador, professor Marcos Augusto Bronzi, expresso minha profunda gratidão pelo apoio, pela disponibilidade e pelas contribuições valiosas ao longo deste percurso. Sua orientação atenta e segura foi decisiva para o amadurecimento deste trabalho e para meu crescimento acadêmico.

A todos que, direta ou indiretamente, contribuíram para a conclusão desta etapa tão importante, deixo aqui minha sincera gratidão.

GONTIJO, F. A. S. .*ANALISANDO CRITÉRIOS DE DIVISIBILIDADE EM DIFERENTES BASES NUMÉRICAS*. 2025. 106p. Dissertação de Mestrado, Universidade Federal de Uberlândia, Uberlândia-MG.

Resumo

Este trabalho propõe uma investigação teórica e didática sobre os critérios de divisibilidade em diferentes sistemas de numeração, com ênfase nos decimal, binário e hexadecimal. Partindo de uma contextualização histórica dos sistemas de numeração utilizados por diversas civilizações. Este estudo estabelece uma base conceitual sólida para a compreensão das estruturas posicionais e não posicionais. Serão desenvolvidos formalmente os principais algoritmos das operações aritméticas e os critérios de divisibilidade em cada base numérica estudada. O capítulo final apresenta uma abordagem generalizada para os critérios de divisibilidade em qualquer base numérica k, propondo uma estrutura que pode ser utilizada tanto para fins de pesquisa quanto para aplicações pedagógicas.

Palavras-chave: Critérios de divisibilidade; Sistemas de numeração; Base decimal; Base binária; Base hexadecimal; Educação matemática.

GONTIJO, F. A. S. .***Analyzing Divisibility Criteria in Different Numeral Bases***. **2025**. **106p**.
M. Sc. Dissertation , Federal University of Uberlândia, Uberlândia-MG.

Abstract

This work proposes a theoretical and didactic investigation into the criteria of divisibility across different numeral systems, with an emphasis on the decimal, binary, and hexadecimal systems. Beginning with a historical contextualization of numeral systems used by various civilizations, the study establishes a solid conceptual foundation for understanding positional and non-positional structures. The main algorithms of arithmetic operations and the divisibility criteria in each studied numeral base will be formally developed. The final chapter presents a generalized approach to divisibility criteria in any numeral base k, proposing a framework that can be used for both research purposes and pedagogical applications.

Keywords: Divisibility criteria; Numeral systems; Decimal base; Binary base; Hexadecimal base; Mathematics education.

Sumário

Lista de Figuras

Lista de Tabelas

Introdução

A humanidade, desde seus primórdios, estabelecia metodologias de contagem, dada a necessidade de determinar medidas de tempo e espaço para um melhor atendimento às questões básicas de sobrevivência e, é possível, tal necessidade continua atual. Tanto o labor quanto o ócio no que tange a humanidade estão atrelados à contagem.

De acordo com a professora de matemática, Tatiana Roque, em conjunto com o professor emérito, João Bosco Pitombeira [8], associa-se a história dos números à necessidade de contagem, relacionada a problemas de subsistência. Dessa forma, as primeiras civilizações começaram a desenvolver bases numéricas para uma melhor representação de tais quantidades.

Na antiguidade, temos como exemplo mais conhecido o sistema sexagesimal (base 60) posicional na antiga Babilônia, associado à escrita cuneiforme. Tal sistema ainda é utilizado nos nossos cálculos de horas, minutos e segundos, além das medidas dos ângulos na geometria. Além deste sistema, temos o sistema duodecimal (base 12), originário do número de falanges dos dedos da mão, o sistema quinário (base 5) originário de algumas tribos africanas, provavelmente baseado na quantidade de dedos em uma mão, o sistema vigesimal (base 20), usado por maias, astecas e celtas, entre outros.

Na nossa civilização contemporânea, utilizamos o sistema numérico hindu-arábico, nas mais diversas situações, em uma base numérica 10 e, portanto, utilizamos as operações básicas mais conhecidas (soma, subtração, multiplicação, divisão, potenciação e radiciação) tendo como referência tal base numérica.

Já na idade moderna, surgiram os sistemas de numeração binário e hexadecimal, ambos vinculados à informática e a computação, visto que, como visto na apostila do CEFET-SC [10], os computadores digitais trabalham internamente com dois níveis de tensão, pelo que o seu sistema de numeração natural é o sistema binário (ligado, desligado). Além disso, os computadores costumam utilizar o byte como unidade básica da memória. Um byte possui a informação de 8 bits e, então, um byte pode ser representado por 8 algarismos do sistema binário ou por dois algarismos do sistema hexadecimal.

A proposta deste trabalho surge da observação dos conteúdos presentes no 6º ano do Ensino Fundamental, em especial os que tratam da **História dos Sistemas de Numeração** e dos **Critérios de Divisibilidade**. Esses dois temas são tradicionalmente abordados de forma separada, muitas vezes de maneira descontextualizada ou superficial, o que pode dificultar a compreensão de sua importância e das conexões existentes entre eles.

A motivação principal, portanto, é oferecer uma abordagem mais significativa e interdisciplinar dos conteúdos curriculares, contribuindo para o desenvolvimento do raciocínio lógico, da alfabetização matemática e da valorização cultural da disciplina. Ao apresentar as bases numéricas de forma interligada com os critérios de divisibilidade e aplicá-las em um minicurso prático, espera-se ampliar o repertório didático de professores e despertar maior interesse dos alunos por temas tradicionalmente considerados abstratos.

Também apresentaremos um minicurso sobre as bases numéricas discutidas, onde trabalharemos a aritmética, com foco nas quatro operações básicas, nas diferentes bases numéricas vistas neste trabalho e com exercícios de fixação para os estudantes.

Dessa forma, o último capítulo deste texto se refere a um minicurso com imagens registrando sua aplicação e uma estrutura didática baseada em [7], de forma a facilitar a compreensão dos estudantes de Ensino Médio ou iniciantes na graduação.

CAPÍTULO 1

História dos Sistemas de Numeração

A necessidade de contar, registrar e comunicar quantidades levou diferentes civilizações a desenvolverem seus próprios sistemas de numeração. Ao longo da história, esses sistemas variaram bastante em estrutura e símbolos, mas dois aspectos principais os diferenciam: serem ou não posicionais, e a base numérica utilizada, como base decimal, base duodecimal, entre outras.

Neste trabalho a seguir, entenderemos o que são sistemas posicionais e não posicionais e veremos exemplos históricos notáveis: os sistemas egípcio, maia, babilônico, romano e grego. Para tal, utilizaremos como fontes principais o livro de Tatiana Roque e João Bosco Pitombeira [8] e a monografia de Wagner Yuwamamoto Miyaschita [6].

1.1 Sistema Posicional e Sistema Não Posicional

Os sistemas de numeração podem ser classificados, principalmente, em duas categorias: posicionais e não posicionais. Essa diferença diz respeito ao fato de que, nos sistemas posicionais, o valor de um símbolo depende da posição em que ele aparece no número. Já nos sistemas não posicionais, cada símbolo possui sempre o mesmo valor, independentemente de sua posição..

1.1.1 Sistema Posicional

Em um sistema posicional, o valor de cada símbolo depende da posição em que ele se encontra no número. Ou seja, o mesmo algarismo pode representar quantidades diferentes, conforme a sua ordem (veremos mais detalhadamente a seguir). Por exemplo, na nossa base decimal, considere o número 343. Da esquerda para a direita, o primeiro 3 representa trezentos, o 4 representa quarenta, e o último 3 representa três. Isso ocorre porque cada posição representa uma potência da base do sistema:

$$343 = 300 + 40 + 3 = 3 \times 100 + 4 \times 10 + 3 \times 1$$

Esse tipo de sistema permite representar grandes quantidades usando poucos símbolos. É o caso do sistema indo-arábico, usado atualmente, que utiliza apenas os algarismos de 0 a 9 e permite escrever qualquer número, por maior que seja, com uma sequência organizada de dígitos.

Sistemas como o babilônico, de base 60, o binário, de base 2, e o decimal de base 10, são alguns exemplos. Por serem posicionais, se provaram mais eficientes para cálculos e permitiram avanços importantes na ciência e na tecnologia.

1.1.2 Sistema Não Posicional

Já em um sistema não posicional, a posição dos símbolos não altera seu valor. Cada símbolo representa uma quantidade fixa, e os números são formados pela combinação ou repetição desses símbolos. Um exemplo bem conhecido é o sistema romano, um sistema que não possui símbolo para o zero, e realizar operações matemáticas um pouco mais elaboradas, como multiplicação ou divisão, é bem mais complexo.

Segundo Miyaschita [6], sistemas não posicionais atendiam bem às necessidades administrativas e religiosas, mas com o tempo mostraram limitações para o desenvolvimento de uma matemática mais abstrata.

A distinção entre sistemas posicionais e não posicionais é fundamental para entender a evolução histórica dos números. Os sistemas não posicionais foram os primeiros a surgir, mas com o tempo, os sistemas posicionais se mostraram mais eficazes para representar quantidades e realizar operações. Veja a operação de adição entre 1432 e 2468 utilizando números hindu-arábicos e números romanos:

Adição dos números hindu-arábicos

$$\begin{array}{ccccc} & 1 & 4 & 3 & 2 \\ + & 2 & 4 & 6 & 8 \\ \hline & 3 & 9 & 0 & 0 \end{array}$$

Adição dos números romanos (criado por analogia para fins de comparação)

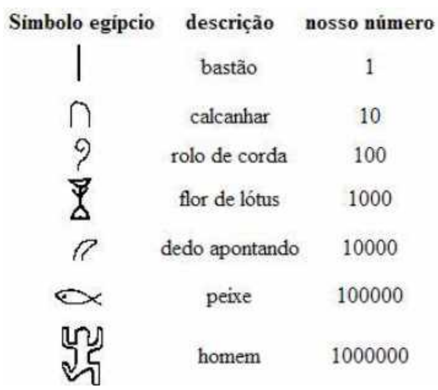
$$
\begin{array}{rcccccccccc}
 & & \mathrm{M} & \mathrm{C} & \mathrm{D} & \mathrm{X} & \mathrm{X} & \mathrm{X} & \mathrm{I} & \mathrm{I} & \\
+ & \mathrm{M} & \mathrm{M} & \mathrm{C} & \mathrm{D} & \mathrm{L} & \mathrm{X} & \mathrm{V} & \mathrm{I} & \mathrm{I} & \mathrm{I} \\
\hline
 & \mathrm{M} & \mathrm{M} & \mathrm{M} & \mathrm{C} & \mathrm{M} & & & & &
\end{array}
$$

Como todos os símbolos I estão ao final, podemos juntar cinco símbolos I, obtendo um símbolo V que, por sua vez, ao juntar com outro símbolo V, obtemos X. Em seguida juntamos cinco símbolos X para formar um símbolo L, que ao juntar com outro L, chegamos a um novo C. Por fim, ao unirmos CD com CD e C, obtemos CM (400+400+100=900) e isto junto aos três M's nos dá o resultado **MMMCM**. Mais a frente, explicaremos o porque da utilização de apenas sistemas posicionais ao realizar o algoritmo da adição.

A mudança do sistema posicional para o não posicional foi um dos grandes avanços da história da matemática e abriu caminho para os sistemas que usamos atualmente.

1.2O Sistema Egípcio

O sistema de numeração desenvolvido pelos egípcios na Antiguidade é um dos mais antigos de que se tem registro, de acordo com Roque e Pitombeira [8]. Ele surgiu por volta de 3000 a.C. e foi utilizado ao longo de mais de dois mil anos. Esse sistema foi essencial para o funcionamento da sociedade egípcia, especialmente para registros administrativos, tributários e religiosos. As inscrições com números eram comuns em papiros, monumentos, túmulos e templos.



Símbolo egípcio	descrição	nosso número
	bastão	1
	calcanhar	10
	rolo de corda	100
	flor de lótus	1000
	dedo apontando	10000
	peixe	100000
	homem	1000000

Figura 1.1: Símbolos Egípcios

Para escrever um número, bastava repetir o símbolo correspondente tantas vezes quantas fossem necessárias. Por exemplo, o número 243 era representado com:

Apesar de funcionar bem para registros simples e contagens, o sistema egípcio não era prático

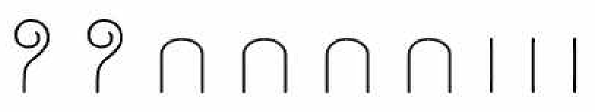


Figura 1.2: 243 no sistema egípcio

para operações matemáticas mais complexas. Por isso, os egípcios desenvolveram métodos próprios para adição, subtração e multiplicação, usando tabelas e dobramentos.

Ainda assim, Roque e Pitombeira [8] explicam que, mesmo com essas limitações, o sistema egípcio foi eficaz para a sua época e serviu como base para registros contábeis e arquitetônicos que eram essenciais para a construção de templos, pirâmides e sistemas de irrigação.

1.3O Sistema Romano

O sistema de numeração romano foi criado na Roma Antiga e se tornou amplamente utilizado em todo o Império Romano. Sua influência foi tão marcante que, ainda hoje, os números romanos continuam presentes em relógios, capítulos de livros, nomes de papas e monarcas, e em representação de séculos. Sua estrutura simples e visualmente distinta ajudava na leitura e escrita de números em monumentos, moedas e documentos oficiais.

O sistema romano é um sistema não posicional, ou seja, os símbolos têm sempre o mesmo valor, independentemente da posição em que aparecem. Além disso, ele é aditivo-subtrativo, o que significa que os números são formados a partir da soma ou subtração dos valores dos símbolos, dependendo da ordem em que aparecem.

Símbolo Romano	Valor
I	1
V	5
X	10
L	50
C	100
D	500
M	1000

Tabela 1.1: Símbolos Romanos

Para formar outros números, os romanos combinavam esses símbolos. Se um símbolo menor viesse antes de um maior, ele era subtraído (por exemplo, IV = 4) e se viesse depois, era somado (por exemplo, VI = 6).

Além disso, o mesmo símbolo não pode ser repetido mais do que três vezes seguidas (por isso, 4 é IV e não IIII) e apenas certos símbolos podem ser usados na subtração (I apenas antes de V e X, X antes de L e C, e C antes de D e M).

Por não ter símbolo para o zero e por ser não posicional, o sistema romano não era eficiente para cálculos matemáticos. Dessa forma, ele servia mais para registro de datas e contagens simples do que para realizar operações complexas.

No contexto do império, o sistema romano funcionava bem para contabilidade militar, impostos e engenharia, especialmente porque era fácil de ler e difícil de falsificar. No entanto, a falta de um sistema posicional e de um símbolo para o zero tornava-o inadequado para o desenvolvimento da matemática como ciência exata.

Assim, Miyaschita [6] aponta que o sistema romano, mesmo com suas limitações, teve grande impacto cultural e permaneceu em uso por séculos, mesmo após o surgimento de sistemas mais eficientes.

O sistema de numeração romano é um exemplo de como uma civilização pode criar uma forma útil de representação numérica com base em símbolos simples. Ainda que limitado em termos matemáticos, seu legado permanece vivo até hoje, servindo como uma ponte entre a matemática antiga e a simbologia moderna.

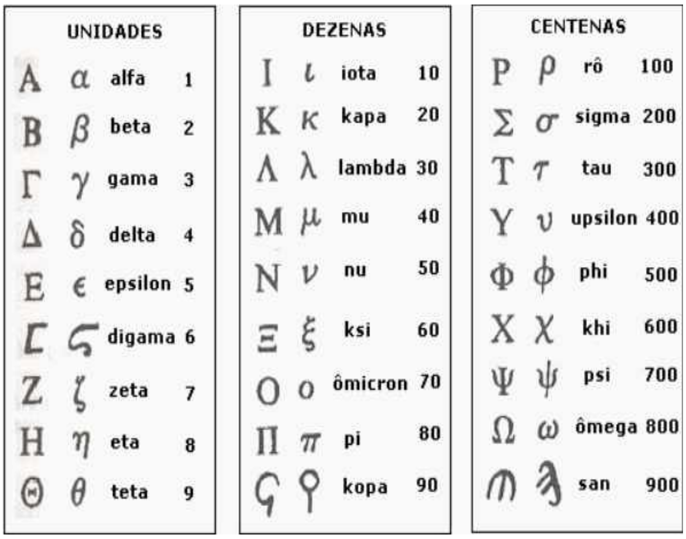
1.4O Sistema Grego

A Grécia antiga, conhecida por seus avanços em filosofia, ciência e matemática, também desenvolveu um sistema de numeração próprio. Apesar de sua grande contribuição para o pensamento lógico e matemático, o sistema numérico grego era relativamente limitado e não tão eficiente quanto os sistemas egípcio ou babilônico. Ainda assim, ele foi amplamente utilizado e reflete a engenhosidade e a cultura daquela civilização.

O sistema grego é um sistema não posicional e alfabético, também conhecido como **sistema jônico** ou **sistema ático** (dependendo do período e da forma de escrita). No sistema jônico, cada número era representado por uma letra do alfabeto grego e as letras eram associadas a valores fixos, o que significa que, como nos sistemas egípcio e romano, a posição da letra não alterava o seu valor.

Os gregos usavam as 24 letras do alfabeto grego, mais 3 letras arcaicas (digamma, qoppa e sampi) para completar os símbolos necessários para representar unidades, dezenas e centenas:

Quando um número ultrapassava 1000 era necessário colocar um pequeno sinal, semelhante ao



UNIDADES			
Α	α	alfa	1
Β	β	beta	2
Γ	γ	gama	3
Δ	δ	delta	4
Ε	ϵ	epsilon	5
Ϛ	ϛ	digama	6
Ζ	ζ	zeta	7
Η	η	eta	8
Θ	θ	teta	9

DEZENAS			
Ι	ι	iota	10
Κ	κ	kapa	20
Λ	λ	lambda	30
Μ	μ	mu	40
Ν	ν	nu	50
Ξ	ξ	ksi	60
Ο	ο	ômicron	70
Π	π	pi	80
Ϙ	ϙ	kopa	90

CENTENAS			
Ρ	ρ	rô	100
Σ	σ	sigma	200
Τ	τ	tau	300
Υ	υ	upsilon	400
Φ	ϕ	phi	500
Χ	χ	khi	600
Ψ	ψ	psi	700
Ω	ω	ômega	800
Ϡ	ϡ	san	900

Figura 1.3: Símbolos Gregos

acento agudo, abaixo ou acima, e à esquerda da sequência de símbolos. E as dezenas de milhares eram representadas de forma multiplicativa, eles usavam o M (10000) abaixo do numeral a ser multiplicado.

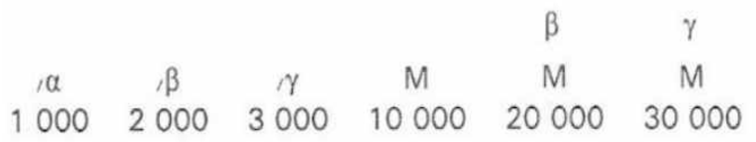


Figura 1.4: Símbolos Jônicos

Como era não posicional, esse sistema dificultava a realização de operações matemáticas complexas. A ausência de um símbolo para o zero e a dependência de muitas letras diferentes também tornavam o sistema pouco prático para cálculos. Por isso, os matemáticos gregos, como Euclides e Arquimedes, muitas vezes usavam letras e expressões algébricas ao lado dos numerais em seus tratados.

No entanto, podemos afirmar que os gregos fizeram avanços profundos na matemática teórica. Roque e Pitombeira [8] destacam que, apesar das limitações do sistema numérico, os gregos foram os primeiros a desenvolver uma geometria sistemática e a formalizar os axiomas e demonstrações, abrindo caminho para a matemática como ciência lógica.

1.5 O Sistema Maia

O sistema de numeração desenvolvido pela civilização maia, que floresceu na Mesoamérica (entre o sudeste do México, Guatemala e Belize) entre os séculos III e XV, é um dos mais sofisticados entre os povos pré-colombianos. Utilizado em atividades astronômicas, registros históricos e cálculos em calendários, o sistema maia é um excelente exemplo de sistema posicional e vigesimal, de base 20, além de ser um dos primeiros a utilizar um símbolo para o zero, algo bastante raro nas culturas antigas.

Enquanto o sistema decimal utiliza como base o número 10, o sistema maia era baseado em múltiplos de 20. Assim, a contagem seguia as potências de 20 (20^0, 20^1, 20^2, e assim por diante). A posição de cada número indicava sua multiplicação por uma potência de 20, o que confere ao sistema maia a característica **posicional**, algo que ele compartilha com o sistema decimal.

Uma exceção notável ocorre no calendário maia: em certos contextos, a segunda posição não representa 20^1, mas sim $18 \times 20 = 360$, para melhor ajustar o sistema ao ano solar. Vejamos os símbolos utilizados no sistema maia:

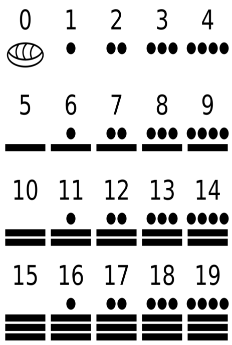


Figura 1.5: Símbolos Maias

O símbolo da concha, usado para indicar o zero, é um dos grandes marcos do sistema maia. Pouquíssimos povos antigos conseguiram conceber e representar o zero como valor numérico. Os maias o faziam com clareza, usando-o tanto para representar a ausência de quantidade quanto como parte essencial da estrutura posicional.

Assim Roque e Pitombeira [8], ressaltam que o uso do zero pelos maias, de forma sistemática, foi fundamental para a construção de calendários e previsões astronômicas complexas, demonstrando um pensamento matemático altamente avançado.

Como observa Miyaschita [6], o sistema maia não foi amplamente disseminado fora da região mesoamericana, mas é um testemunho poderoso da diversidade de formas que a matemática pode assumir em diferentes culturas. Seu uso de símbolos simples, organização posicional e zero mostra uma sofisticação comparável à dos sistemas mais avançados da história.

1.6O Sistema Sumério-Babilônico (Duodecimal)

O sistema duodecimal, também conhecido como sistema de base 12, é uma forma alternativa de contagem que utiliza doze unidades como base, em vez das dez do sistema decimal. Embora não tenha sido adotado como sistema padrão global, o duodecimal foi utilizado por diversas civilizações ao longo da história, com destaque para os sumérios e posteriormente os babilônios, que o empregavam em conjunto com o sistema sexagesimal, que trabalharemos à frente.

No sistema duodecimal, os números são organizados em potências de 12. Assim como no sistema decimal usamos as casas das unidades, dezenas, centenas (10^1, 10^2, $10^3 \ldots$), no sistema de base 12 usamos as unidades, dúzias, grosas (12^1, 12^2, $12^3 \ldots$) e assim por diante.

Segundo Miyaschita [6], o sistema de base 12 apresenta vantagens práticas em divisibilidade, pois o número 12 tem mais divisores inteiros do que o número 10. O número 12 pode ser dividido exatamente por 2, 3, 4 e 6, enquanto o 10 só é divisível por 2 e 5. Essa maior flexibilidade torna o duodecimal ideal para medições e partições. Não é por acaso que muitas unidades tradicionais de medida refletem o uso dessa base, como por exemplo:

- 12 polegadas = 1 pé;
- 12 meses = 1 ano;
- 2 dúzias = 24 itens;
- 1 grosa = 12 dúzias = 144 itens.

Nesse contexto, os exemplos mostram que, mesmo sem ser um sistema de numeração oficial como o decimal, o duodecimal está profundamente enraizado em práticas do cotidiano.

A base 12 foi especialmente importante para os sumérios, um dos primeiros povos da Mesopotâmia. Acredita-se que seu uso esteja relacionado à contagem com os dedos, já que é possível contar até 12 nas falanges dos dedos de uma única mão, usando o polegar como indicador.

Portanto, o sistema duodecimal é um exemplo fascinante de como diferentes civilizações experimentaram alternativas ao sistema decimal, buscando praticidade e eficiência. Embora não tenha se tornado o sistema predominante, seu uso em medidas, calendários e contagens reforça sua importância histórica e cultural.

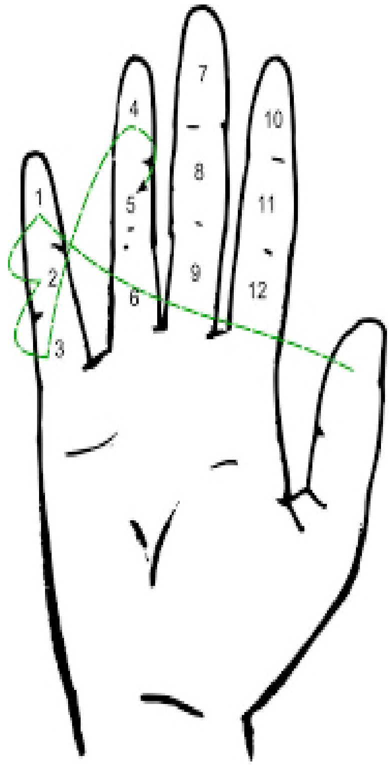


Figura 1.6: Contando até 12 com as Falanges

1.7 O Sistema Babilônico (Sexagesimal)

O sistema de numeração babilônico surgiu na antiga Mesopotâmia, especialmente entre os povos sumérios e acadianos, e foi posteriormente aperfeiçoado pelos babilônios por volta de 2000 a.C. Esse sistema é considerado um dos mais sofisticados da Antiguidade, tanto por sua estrutura quanto pela influência que exerceu sobre a matemática posterior, especialmente na astronomia.

Diferentemente dos sistemas anteriores, o sistema babilônico é posicional, ou seja, o valor de um símbolo depende de sua posição no número. Ele também é **sexagesimal**, o que significa que tem **base 60**. Em vez de contar de 0 a 9, como fazemos no sistema decimal, os babilônios contavam de 0 a 59, e depois passavam para a próxima ordem de grandeza, como fazemos ao completar uma dezena e passar para a casa das dezenas.

O uso da base 60 provavelmente surgiu da combinação de sistemas anteriores, como base 10 e base 12, e por razões práticas, já que o número 60 tem muitos divisores (2, 3, 4, 5, 6...), o que facilita a divisão e a medição de tempo e ângulos, práticas que os babilônios dominavam com precisão.

Os babilônios utilizavam dois tipos básicos de marcas em forma de cunha feitas com um estilete de junco em tabuletas de argila:

Observe a similaridade dos símbolos para 1 e 60, isso ocorre porque se diferenciavam pela posição.

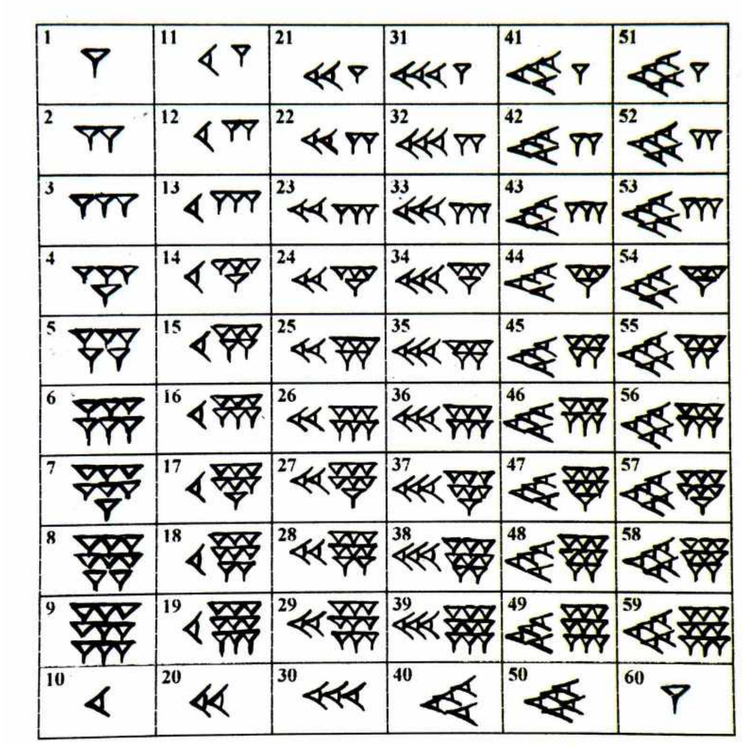


Figura 1.7: Sistema Sexagesimal

Inicialmente, não havia um símbolo para o zero, o que gerava ambiguidade em alguns casos. Mais tarde, os babilônios passaram a usar um marcador para indicar a ausência de valor em uma posição intermediária, embora esse símbolo não tivesse valor numérico próprio.

Apesar disso, o sistema babilônico foi amplamente usado em astronomia, calendário, agricultura e comércio. Muitos dos conhecimentos astronômicos dos gregos e até dos modernos se baseiam em registros babilônicos. O uso atual de 60 minutos em uma hora e 360 graus em um círculo é uma herança direta desse sistema.

Segundo Roque e Pitombeira [8], os babilônios foram capazes de resolver equações do segundo grau e de elaborar tabelas trigonométricas graças ao seu sistema numérico eficiente e à notação posicional.

1.8 O Sistema Hindu-Arábico

O sistema hindu-arábico é o sistema de numeração utilizado atualmente em praticamente todo o mundo. Sua importância é imensa, pois ele possibilita a realização de cálculos complexos com facilidade e eficiência. Esse sistema combina duas características fundamentais que o tornaram superior aos anteriores: é posicional e possui um símbolo para o zero.

O sistema foi desenvolvido originalmente na Índia, entre os séculos I e IV d.C., e posteriormente aperfeiçoado por matemáticos árabes durante a Idade Média. A partir daí, foi levado para a Europa por meio de traduções de obras árabes para o latim. Um dos responsáveis por sua disseminação no Ocidente foi Leonardo de Pisa, mais conhecido como Fibonacci, que em 1202 escreveu o Liber Abaci [4], introduzindo o sistema ao público europeu.

Vale ressaltar que o sistema hindu-arábico também é **posicional**, o que permite que o mesmo símbolo tenha significados diferentes dependendo da posição onde aparece, algo impossível nos sistemas egípcio, romano ou grego, por exemplo, que eram não posicionais. Além disso, a introdução do zero (0) como número foi uma inovação fundamental. No sentido que o zero tem dois papéis importantes: representa a ausência de valor e ocupa lugar na estrutura posicional (por exemplo, 204 é diferente de 24).

Dessa forma, são utilizados apenas dez símbolos: 0, 1, 2, 3, 4, 5, 6, 7, 8 e 9. Com esses símbolos, é possível formar qualquer número e realizar operações com rapidez, especialmente com a ajuda das regras da aritmética algébrica, que veremos mais adiante.

De acordo com Miyaschita [6], a combinação de posição e base 10 torna esse sistema extremamente versátil, eficiente e adequado para o ensino, a ciência e o comércio. Além disso, Tatiana Roque [8] aponta que a adoção do sistema hindu-arábico foi um divisor de águas na história da matemática, pois permitiu o desenvolvimento da álgebra e da aritmética moderna. Assim como a evolução mostrada na imagem abaixo:

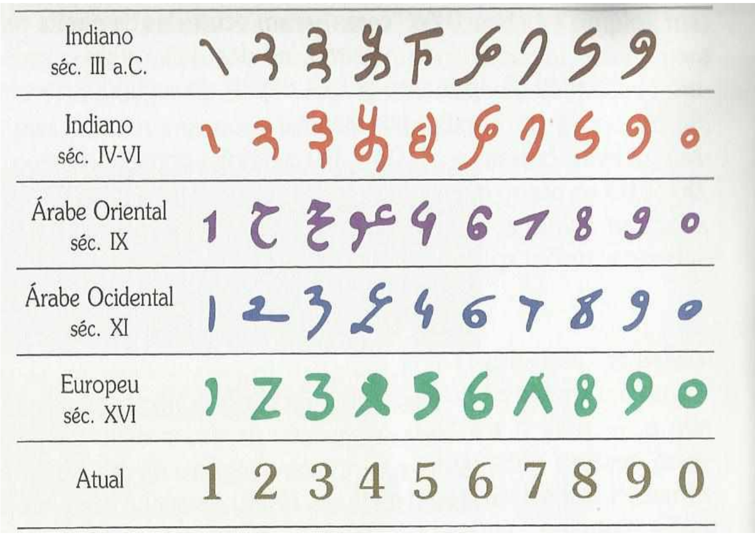


Figura 1.8: Evolução do Sistema Hindu-Arábico

Na Europa, o sistema demorou a ser aceito. Por muitos séculos, os números romanos continuaram em uso oficial, enquanto o sistema hindu-arábico era adotado principalmente por comerciantes e matemáticos. Eventualmente, porém, sua eficiência prevaleceu e ele se tornou o padrão numérico não apenas na Europa, mas também de maneira global.

Hoje, é o sistema universalmente utilizado em todos os campos: educação, ciência, engenharia, economia e vida cotidiana. Nesse contexto, a sua importância é tão grande que dificilmente conseguimos imaginar como seria viver sem ele.

Portanto, a história dos sistemas de numeração revela a diversidade e a criatividade com que diferentes povos lidaram com a necessidade de contar, calcular e registrar. Dos sistemas não posicionais como o egípcio e o romano, aos avançados sistemas posicionais como o maia e o hindu-arábico, cada um reflete aspectos culturais, tecnológicos e práticos de sua época.

CAPÍTULO 2

O Conjunto dos Números Inteiros ($\mathbb{Z}$)

Trataremos, neste capítulo, do conjunto dos números inteiros $\mathbb{Z}$ dado pela união dos números naturais, incluindo o elemento neutro (zero), $\mathbb{N}$ e seus opostos, utilizando como referência o livro de Nazaré Bezerra [1]. Além disso, as propriedades e axiomas relacionados aos números inteiros são válidas, independentemente, da base numérica com a qual se está trabalhando.

Este conjunto surge da necessidade da ampliação do conjunto dos números naturais, pois estes não eram suficientes para a resolução de situações cotidianas.

Como dito por Bezerra em [1], neste conjunto estão definidas duas operações:

(i) adição: que associa a todo par (a,b) de números inteiros, a soma $a+b \in \mathbb{Z}$;

(ii) multiplicação: que associa a todo par (a,b) de números inteiros, a produto $a \cdot b \in \mathbb{Z}$. Em geral, representamos o produto por ab.

Tais operações são definidas a partir de axiomas.

2.1Axiomas da Adição

De acordo com Bezerra [1], para que possamos definir a operação adição no conjunto dos números inteiros utilizamos os seguintes axiomas:

(A1) A adição é **comutativa**, ou seja, para quaisquer $a, b \in \mathbb{Z}$:

$$a+b=b+a;$$

(A2) A adição é **associativa**, ou seja, para quaisquer $a, b, c \in \mathbb{Z}$:

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

(A3) Existência e unicidade do **elemento neutro da adição**, ou seja, para qualquer $a \in \mathbb{Z}$:

$$a+0 = a;$$

(A4) Existência e unicidade do **oposto**, ou seja, para qualquer $a \in \mathbb{Z}$:

$$a+(-a) = 0.$$

2.2Axiomas da Multiplicação

Assim como a adição, Bezerra [1] define bem a multiplicação, no conjunto dos números inteiros, utilizando os seguintes axiomas:

(M1) A multiplicação é **comutativa**, ou seja, para quaisquer $a, b \in \mathbb{Z}$:

$$ab = ba;$$

(M2) A multiplicação é **associativa**, ou seja, para quaisquer $a, b, c \in \mathbb{Z}$:

$$(ab)c = a(bc);$$

(M3) Existência e unicidade do **elemento neutro da multiplicação**, ou seja, para qualquer $a \in \mathbb{Z}$:

$$a \cdot 1 = a;$$

(M4) Existência e unicidade do **elemento nulo**, ou seja, para quaisquer $a, b \in \mathbb{Z}$ se $ab = 0$, então $a = 0$ ou $b = 0$

(M5) Distributividade da multiplicação com relação à adição, ou seja, para quaisquer $a, b, c \in \mathbb{Z}$:

$$a(b+c) = ab+ac.$$

2.3 Divisor de um Inteiro e Divisibilidade

O conceito de divisor será um dos mais explorados neste trabalho e, portanto, devemos definir tal conceito muito bem. Portanto, de acordo com Bezerra [1], diremos que um número inteiro b divide outro inteiro a, se existe $c \in \mathbb{Z}$, tais que:

$$a = bc$$

Além disso, utilizaremos $b \mid a$ para simbolizar que b **divide** a e $b \nmid a$ para indicar que b **não divide** a. Se b divide a dizemos que b é um **divisor** de a ou que a é **múltiplo** de b.

A proposição a seguir é uma importante propriedade da divisibilidade.

Proposição 2.1

Sejam $a, b, c \in \mathbb{Z}$. Se $a \mid b$ e $a \mid c$, então $a \mid (bm + cn)$, com $m, n \in \mathbb{Z}$.

Demonstração. Como $a \mid b$ e $a \mid c$, existem $p, q \in \mathbb{Z}$, tais que:

$$b = a \cdot p$$
$$c = a \cdot q$$

Multiplicando a primeira por m e a segunda por n, obtemos:

$$bm = a(pm)$$
$$cn = a(qn)$$

Somando ambas igualdades, temos:

$$bm + cn = a(pm + qn)$$

Portanto, $a \mid bm + cn$, pois $pm + qn \in \mathbb{Z}$. $\square$

A próxima proposição fornece o intervalo no qual estão os possíveis divisores positivos de um número inteiro.

Proposição 2.2

Sejam a e b inteiros, com $a \neq 0$. Se $b \mid a$, então $|b| \leq |a|$.

Demonstração. Suponha que $b \mid a$. Então existe $c \neq 0$ e $c \in \mathbb{Z}$, tal que $a = bc$. Aplicando o módulo em ambos os lados da igualdade, obtemos:

$$|a| = |bc| = |b| \cdot |c| \geq |b| \cdot 1 = |b|$$

Pois, como $c \in \mathbb{Z}$ e $c \neq 0$ sabemos que $|c| \geq 1$ e, portanto, $|b| \leq |a|$. □

2.4Aritmética Modular

Existe uma área da matemática que trabalha com restos das divisões, chamada Aritmética Modular. Utilizaremos nesse trabalho, com o objetivo de demonstrar alguns critérios de divisibilidade. Para isso, é necessário definir seus conceitos fundamentais, baseando-nos na obra de Bezerra [1].

Definição 2.1

Sejam $a, b, m \in \mathbb{Z}$ com $m > 0$. Dizemos que:

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

Se, e somente se, $a - b = k \cdot m$, $k \in \mathbb{Z}$, ou seja, a e b deixam o mesmo resto na divisão por m.

Para operações com aritmética modular, devemos aplicar oito propriedades que veremos a seguir.

(P1) Reflexividade:

$$a \equiv a \pmod{m};$$

(P2) Simetria:

Se $a \equiv b \pmod{m}$, então:

$$b \equiv a \pmod{m};$$

(P3) Transitividade:

Se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então:

$$a \equiv c \pmod{m};$$

(P4) Adição:

Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então:

$$a + c \equiv b + d \pmod{m};$$

(P5) Subtração:

Se $a \equiv b \pmod{m}$, então:

$$a - c \equiv b - c \pmod{m};$$

(P6) Multiplicação:

Se $a \equiv b \pmod{m}$, então:

$$a \cdot c \equiv b \cdot c \pmod{m};$$

(P7) Potenciação:

Se $a \equiv b \pmod{m}$, então:

$$a^n \equiv b^n \pmod{m}, \quad \forall n \in \mathbb{Z}_+;$$

(P8) Cancelamento (se c e m forem coprimos):

Se $a \cdot c \equiv b \cdot c \pmod{m}$ e $mdc(c, m) = 1$, então:

$$a \equiv b \pmod{m}.$$

Agora, poderemos começar a explorar os sistemas numéricos e seus critérios de divisibilidade.

CAPÍTULO 3

Sistema de Numeração Decimal

O nosso atual sistema de numeração decimal será estudado neste capítulo, com o objetivo de entender os critérios de divisibilidade aplicados na base numérica usual, além de algumas propriedades das operações básicas. Para tal, utilizamos o livro de Álgebra Moderna [5].

3.1 O Sistema de Numeração Decimal

O sistema decimal é composto pelos algarismos 0, 1, 2, 3, 4, 5, 6, 7, 8 e 9, em ordem crescente. Dessa forma, como a nomenclatura de cada sistema é dada pela quantidade de algarismos utilizados, este sistema é chamado de decimal por possuir dez algarismos. Além disso, como todos os sistemas que serão estudados posteriormente neste trabalho, este é chamado sistema posicional, em que a posição do algarismo determina sua grandeza.

Vale mencionar, assim como foi lembrado por Rodrigues [7], que cada terna de ordens, da esquerda para a direita, compõe uma classe, de acordo com a seguinte tabela:

Classe	Ordem	Nome
Classe das unidades	1ª ordem	Unidades
	2ª ordem	Dezenas
	3ª ordem	Centenas
Classe do Milhar	4ª ordem	Unidades de milhar
	5ª ordem	Dezenas de milhar
	6ª ordem	Centenas de milhar
Classe do Milhão	7ª ordem	Unidades de milhão
	8ª ordem	Dezenas de milhão
	9ª ordem	Centenas de milhão
⋮	⋮	⋮

Representaremos um número na base 10 por $a_{(10)}$, em que:

$$a_{(10)} = a_0 \cdot 10^0 + a_1 \cdot 10^1 + a_2 \cdot 10^2 + \cdots + a_n \cdot 10^n, \text{ com } n \in \mathbb{Z}$$

Por exemplo, o número 15087 tem a seguinte representação decimal:

$$15087_{(10)} = 7 \cdot 10^0 + 8 \cdot 10^1 + 0 \cdot 10^2 + 5 \cdot 10^3 + 1 \cdot 10^4$$

Note que, como este sistema é **posicional**, a posição ocupada por cada algarismo interfere no seu valor numérico. Por exemplo, os números $87_{(10)} = 8 \cdot 10^1 + 7 \cdot 10^0$ e $78_{(10)} = 7 \cdot 10^1 + 8 \cdot 10^0$ são diferentes.

Assim, chegamos à notação utilizada hoje, em que o número $a_{(10)}$ pode ser representado apenas pelos seus coeficientes:

$$a_{(10)} = a_n a_{n-1} a_{n-2} \ldots a_2 a_1 a_0$$

Após entendermos a notação que é utilizada na nossa base numérica, resta entender os métodos de resolução das quatro operações básicas: adição, subtração, multiplicação e divisão.

3.2 Algoritmo da Adição no Sistema Decimal

O algoritmo da adição é um método sequencial de resolução da operação, baseado no sistema de classes e ordens, citado anteriormente. Ele foi desenvolvido com o objetivo de organizar e facilitar o processo de resolução, especialmente em cálculos com números maiores.

Para aplicar este algoritmo, o primeiro passo é alinhar os algarismos que compõem cada número de acordo com as respectivas ordens. Em seguida realizamos a operação entre ordens, da direita para a esquerda, iniciando pelas unidades.

Vale a observação que a adição com reagrupamento se faz necessária quando a soma obtida em determinada ordem excede 9. Dessa forma, o valor que representaria uma ordem superior à trabalhada é adicionado à próxima casa.

Exemplo 3.1

Por exemplo, vamos realizar a soma $145 + 273$, utilizando o algoritmo:

$$\begin{array}{r} \overset{1}{1}45 \\ +\ 273 \\ \hline 418 \end{array}$$

Demonstração. Para verificar a funcionalidade do método utilizaremos o método de indução. Inicialmente, tomemos dois números inteiros quaisquer na base decimal A e B de três algarismos. Ou seja:

$$A = a_0 + a_1 \cdot 10^1 + a_2 \cdot 10^2$$
$$B = b_0 + b_1 \cdot 10^1 + b_2 \cdot 10^2$$

Ao somarmos ambos os números obtemos:

$$A + B = (a_0 + b_0) + 10^1 \cdot (a_1 + b_1) + 10^2 \cdot (a_2 + b_2)$$

Por exemplo, se a soma $a_0 + b_0 \geq 10$, teremos que $(a_0 + b_0) = 10^1 + c_0$ e, portanto:

$$A + B = c_0 + 10^1(a_1 + b_1 + 1) + 10^2(a_2 + b_2)$$

De forma análoga e geral, para qualquer parcela $10^i \cdot (a_i + b_i), i \in \mathbb{Z}$ e $0 < i \leq n$, se $a_i + b_i \geq 10$, ou seja, $a_i + b_i = 10 + c_i$ teremos:

$$10^i \cdot (a_i + b_i) = 10^i \cdot (10^1 + c_i) = 10^{i+1} + 10^i \cdot c_i$$

Portanto, o algoritmo funciona para a adição de quaisquer dois números inteiros. □

3.3 Algoritmo da Subtração no Sistema Decimal

O algoritmo da subtração, assim como o anterior, é um método sequencial, baseado no sistema de classes e ordens e em alguns axiomas da adição. Também foi desenvolvido com o objetivo de auxiliar na resolução da operação.

Ao aplicar esse algoritmo, devemos alinhar os algarismos que fazem parte da composição do número respeitando as respectivas ordens. Em seguida realizamos a operação entre ordens, da direita para a esquerda, iniciando pelas unidades, assim como na adição.

Vale ressaltar que, ao subtrair os algarismos, quando uma dessas operações não é possível de se realizar em $\mathbb{N}$, é necessário "pegar emprestado" um da ordem seguinte, aumentando o valor em 10 e diminuindo o dígito da coluna da esquerda em 1.

Exemplo 3.2

Por exemplo, vamos realizar a subtração $732-561$, utilizando o algoritmo, alinhando o número de maior módulo por cima daquele que possui menor módulo:

$$\begin{array}{r} \scriptstyle 6\;13\; \\ \cancel{7}\cancel{3}2 \\ -561 \\ \hline 171 \end{array}$$

Para verificar a funcionalidade do método utilizaremos o método de indução. Inicialmente, tomemos dois números inteiros quaisquer na base decimal A e B de três algarismos. Ou seja:

$$A = a_0 + a_1 \cdot 10^1 + a_2 \cdot 10^2$$
$$B = b_0 + b_1 \cdot 10^1 + b_2 \cdot 10^2$$

Ao subtrairmos A por B, obtemos:

$$A - B = (a_0 - b_0) + 10^1 \cdot (a_1 - b_1) + 10^2 \cdot (a_2 - b_2)$$

Por exemplo, se $b_0 > a_0$, então $(a_0 - b_0) \notin \mathbb{N}$ e, daí, devemos "pegar emprestado" 1 de a_1. Isso transforma a_0 em $a_0 + 10$ e, como $0 \leq b_0 \leq 9$ então $a_0 + 10 \geq b_0$ e, agora temos $(a_0 + 10 - b_0) \in \mathbb{N}$. Por outro lado, agora também temos a parcela $10^1(a_1 - 1 - b_1)$, de forma a não alterar $A - B$. Generalizando, para qualquer parcela $10^i \cdot (a_i + b_i), i \in \mathbb{Z}$ e $0 < i \leq n$ se $b_i > a_i$ devemos "pegar emprestado" 1 de a_{i+1}, ou seja, teremos:

$$10^i(a_i - b_i) + 10^{i+1}(a_{i+1} - b_{i+1}) = 10^i(a_i - b_i + 10) + 10^{i+1}(a_{i+1} - b_{i+1} - 1)$$

Portanto, o algoritmo funciona na subtração de quaisquer dois números inteiros.

3.4Algoritmo da Multiplicação no Sistema Decimal

Este algoritmo, assim como os demais já vistos, também é um método sequencial baseado no sistema de classes e ordens, com a diferença de que este tem referências nos axiomas da multiplicação. Para realizar o algoritmo, alinhamos ambos os números e multiplicamos os dígitos individualmente, considerando a ordem, de um dos números pelo outro. Em seguida, somamos os resultados obtidos.

No caso deste algoritmo, assim como na adição, o reagrupamento se faz necessário quando o produto obtido em determinada ordem excede 9. Dessa forma, o valor que representaria uma ordem superior à trabalhada é adicionado à próxima casa.

Exemplo 3.3

Por exemplo, vamos realizar a multiplicação 123×45, utilizando o algoritmo:

$$\begin{array}{r} {\scriptstyle 1} \\ {\scriptstyle 1\,1} \\ 123 \\ \times \quad 45 \\ \hline 615 \\ {\scriptstyle 1} \\ +492 \\ \hline 5535 \end{array}$$

Para verificar a funcionalidade do método, tomemos um número inteiro A de três algarismos e outro número inteiro B de dois algarismos. Ou seja:

$$A = a_0 + a_1 \cdot 10^1 + a_2 \cdot 10^2$$
$$B = b_0 + b_1 \cdot 10^1$$

Ao multiplicar os dois números obtemos:

$$A \cdot B = a_0 b_0 + 10^1(a_1 b_0 + a_0 b_1) + 10^2(a_2 b_0 + a_1 b_1) + 10^3(a_2 b_1)$$

Por exemplo, se $a_0 b_0 \geq 10$ então $a_0 b_0 = 10c_1 + c_0$, com $c_1 > 0$, daí:

$$AB = c_0 + 10^1(a_1 b_0 + a_0 b_1 + c_1) + 10^2(a_2 b_0 + a_1 b_1) + 10^3(a_2 b_1)$$

Então, generalizando, para qualquer parcela $10^i \cdot (a_i + b_i), i \in \mathbb{Z}$ e $0 < i \leq n$, se $a_i b_i \geq 10$, ou seja, $a_i b_i = 10c_{i+1} + c_i$, com $c_{i+1} > 0$, teremos:

$$10^i \cdot (a_i b_i) = 10^i \cdot (10_{i+1} c_{i+1} + c_i) = 10^{i+1} c_{i+1} + 10^i c_i$$

Portanto, o algoritmo funciona na multiplicação de quaisquer dois números inteiros.

3.5Algoritmo da Divisão no Sistema Decimal

O algoritmo da divisão ensinado na maioria das instituições de ensino no Brasil possui referência no Algoritmo da Divisão de Euclides, porém possui uma própria estrutura sistemática do que chamamos de “divisão longa”.

Definimos que, em uma divisão de inteiros $A \div B = Q + R$, em que A é chamado dividendo, B é chamado divisor, Q o quociente e R o resto. Para realizar a divisão longa de A por B:

I. Primeiro alinhamos o dividendo e o divisor. O divisor é colocado dentro de uma "casinha"e o dividendo fica do lado de fora;

II. Em seguida, realizamos a divisão de cada dígito de A, da esquerda para a direita (e utilizando mais de um dígito se necessário), por B;

III. Na sequência multiplicamos o divisor pelo quociente encontrado e escrevemos o resultado abaixo da parte do dividendo que utilizamos;

IV. Subtraímos o resultado da multiplicação do dividendo, determinando, assim, um resto;

V. Trazemos o próximo dígito do dividendo para baixo, ao lado do restante;

VI. Repetimos os passos II a V até que todos os dígitos do dividendo tenham sido utilizados;

VII. O quociente ou resultado é o número formado abaixo da “casinha”.

Exemplo 3.4

Como exemplo, vamos realizar a divisão $569 \div 3$:

$$
\begin{array}{rr|l}
 & 569 & \underline{\;\;3\;\;} \\
(3\times 100) & \underline{-300} & 189 \;\; (100+80+9) \\
 & 269 & \\
(3\times 80) & \underline{-240} & \\
 & 29 & \\
(3\times 9) & \underline{-27} & \\
 & 2 &
\end{array}
$$

Vamos considerar este exemplo como o caso geral. Para entender o motivo da exatidão deste método, devemos associar a divisão como uma operação da multiplicação “invertida”.

3.6 Critérios de Divisibilidade na Base Decimal

Agora que já temos as quatro operações básicas bem definidas, bem como seus métodos de aplicação e algoritmos de resolução, podemos falar sobre alguns critérios de divisibilidade na base decimal. Esses critérios funcionam como regras práticas para decidir se um certo número é múltiplo, ou não, de um outro escolhido previamente.

Trataremos, neste capítulo, dos critérios de divisibilidade na base decimal mais conhecidos e utilizados: Divisibilidade por 2, 3, 5, 9 e 10. Além disso, trataremos o curioso caso de divisibilidade por 7 e 11, dois critérios pouco estudados nas escolas brasileiras e, para demonstrar estes critérios, utilizaremos o texto de Talysson Paulo da Silva [9] e o artigo de Ana Paula Chaves e Thiago Porto [3].

3.6.1 Divisibilidade por 2 na Base Decimal

Teorema 3.1

Um número é divisível por 2 se, e somente se, o dígito das unidades (a_0) for 0, 2, 4, 6 ou 8, ou seja, se o número terminar com algarismo par.

Demonstração. ($\Rightarrow$) Tomemos um número inteiro $a_{(10)}$, tal que:

$$a_{(10)} = a_0 \cdot 10^0 + a_1 \cdot 10^1 + a_2 \cdot 10^2 + \cdots + a_n \cdot 10^n, \text{ com } n \in \mathbb{N}$$

Podemos escrever $a_{(10)}$ da seguinte forma, colocando 10 em evidência:

$$a_{(10)} = a_0 + 10 \cdot (a_1 + a_2 \cdot 10^1 + \cdots + a_n \cdot 10^{n-1}), \text{ com } n \in \mathbb{N}$$

Tomaremos $k = (a_1 + a_2 \cdot 10^1 + \cdots + a_n \cdot 10^{n-1})$, daí:

$$a_{(10)} = a_0 + 10 \cdot k$$

Dessa forma, a parcela $10 \cdot k$ é divisível por 2, pois $2 \mid 10$ e, portanto, $a_{(10)}$ é divisível por 2 se a_0 o for.

($\Leftarrow$) Agora, nos resta mostrar a recíproca, ou seja, que se um número tem como algarismo das unidades 0, 2, 4, 6 ou 8, então este número é divisível por 2.

De fato, vamos escrever:

$$a_{(10)} = a_0 + 10 \cdot l,$$

onde $a_0 \in \{0, 2, 4, 6, 8\}$, ou seja, $a_0 = 2 \cdot b_0$. Dessa forma:

$$a_{(10)} = 2 \cdot (b_0 + 5l)$$

Portanto, $2 \mid a_{(10)}$. □

3.6.2 Divisibilidade por 5 na Base Decimal

Teorema 3.2

Um número é divisível por 5 se, e somente se, o dígito das unidades (a_0) for 0 ou 5, ou seja se terminar com 0 ou 5.

Demonstração. ($\Rightarrow$) Da mesma forma da demonstração do Teorema anterior, tomemos um número inteiro $a_{(10)}$, tal que:

$$a_{(10)} = a_0 \cdot 10^0 + a_1 \cdot 10^1 + a_2 \cdot 10^2 + \cdots + a_n \cdot 10^n, \text{ com } n \in \mathbb{N}$$

Podemos escrever $a_{(10)}$ da seguinte forma, colocando 10 em evidência:

$$a_{(10)} = a_0 + 10 \cdot (a_1 + a_2 \cdot 10^1 + \cdots + a_n \cdot 10^{n-1}), \text{ com } n \in \mathbb{N}$$

Tomaremos $k = (a_1 + a_2 \cdot 10^1 + \cdots + a_n \cdot 10^{n-1})$, daí:

$$a_{(10)} = a_0 + 10 \cdot k$$

Daí, sabemos que a parcela $10 \cdot k$ é divisível por 5, pois $5 \mid 10$ e, portanto, $a_{(10)}$ é divisível por 5 se $a_0 = 0$ ou $a_0 = 5$.

($\Leftarrow$) Reciprocamente,tomemos:

$$a_{(10)} = a_0 + 10 \cdot l$$

Se $a_0 = 5$ ou $a_0 = 0$ teremos $a_{(10)} = 5 \cdot (1 + 2l)$ ou $a_{(10)} = 5 \cdot (2l)$. Portanto, $5 \mid a_{(10)}$. □

3.6.3 Divisibilidade por 10 na Base Decimal

Teorema 3.3

Um número é divisível por 10 se, e somente se, o dígito das unidades (a_0) for 0.

Demonstração. ($\Rightarrow$) Assim como as outras demonstrações anteriores, tomemos um número inteiro $a_{(10)}$, tal que:

$$a_{(10)} = a_0 \cdot 10^0 + a_1 \cdot 10^1 + a_2 \cdot 10^2 + \cdots + a_n \cdot 10^n, \text{ com } n \in \mathbb{N}$$

Podemos escrever $a_{(10)}$ da seguinte forma, colocando 10 em evidência:

$$a_{(10)} = a_0 + 10 \cdot (a_1 + a_2 \cdot 10^1 + \cdots + a_n \cdot 10^{n-1}), \text{ com } n \in \mathbb{N}$$

Tomaremos $k = (a_1 + a_2 \cdot 10^1 + \cdots + a_n \cdot 10^{n-1})$, daí:

$$a_{(10)} = a_0 + 10 \cdot k$$

Portanto, $a_{(10)}$ é divisível por 10 se $a_0 = 0$.

($\Leftarrow$) Reciprocamente, tomemos:

$$a_{(10)} = a_0 + 10 \cdot l$$

Se $a_0 = 0$ teremos $a_{(10)} = 10 \cdot l$. Portanto, $10 \mid a_{(10)}$. □

3.6.4Divisibilidade por 3 e 9 na Base Decimal

Teorema 3.4

Um número natural n é divisível por 3 ou por 9 se, e somente se, a soma dos seus dígitos for divisível por 3 ou por 9.

Demonstração. ($\Rightarrow$) De início, vamos observar, na base decimal, que:

$$\begin{aligned} 10-1 &= 9 = 1\times 9 \\ 10^2-1 &= 99 = 11\times 9 \\ 10^3-1 &= 999 = 111\times 9 \\ 10^4-1 &= 9 = 1111\times 9 \end{aligned}$$

Generalizando, temos para $n\in\mathbb{N}$,

$$10^n-1=\underbrace{11\ldots1}_{n \text{ vezes}}\times 9$$

Ou seja, os números da forma 10^n-1 são divisíveis por 9 (donde também são divisíveis por 3).

Agora, tomemos um número inteiro $a_{(10)}$, tal que:

$$a_{(10)} = a_0\cdot 10^0 + a_1\cdot 10^1 + a_2\cdot 10^2+\cdots+a_n\cdot 10^n, \text{ com } n\in\mathbb{N}$$

Subtraindo de $a_{(10)}$ a soma de seus algarismos, temos:

$$\begin{aligned} a_{(10)}-(a_0+\cdots+a_n) &= a_0 10^0+a_1 10^1+a_2 10^2+\cdots+a_n 10^n-(a_0+\cdots+a_n) \\ &= a_0-a_0+a_1(10^1-1)+a_2(10^2-1)+\cdots+a_n(10^n-1) \end{aligned}$$

Pela nossa observação inicial, sabemos que o lado direito da igualdade é sempre divisível por 9 (e também por 3), ou seja, é da forma $9k$ com $k\in\mathbb{Z}$. Daí:

$$\begin{aligned} a_{(10)}-(a_0+\cdots+a_n) &= 9k \\ a_{(10)} &= 9k+(a_0+\cdots+a_n) \end{aligned}$$

Portanto, $a_{(10)}$ será divisível por 9 (e consequentemente por 3), quando $(a_0+\cdots+a_n)$ o for.

($\Leftarrow$) Reciprocamente, suponhamos que $a_{(10)}$ seja divisível por 9 e por 3. Dessa forma, temos que

$a_{(10)} = 9q$ com $q \in \mathbb{Z}$. Daí:

$$a_{(10)} - (a_0 + \cdots + a_n) = 9k$$
$$(a_0 + \cdots + a_n) = 9(q - k)$$

Logo, se $a_{(10)}$ é divisível por 9 e por 3, a soma $(a_0 + \cdots + a_n)$ também o é. □

3.6.5 Divisibilidade por 7 na Base Decimal

Teorema 3.5

Um número natural n é divisível por 7 se, ao considerar o último dígito, multiplicá-lo por 2 e subtraí-lo do número que restou, também seja divisível por 7.

Demonstração. Tomemos um número inteiro $a_{(10)}$, tal que:

$$a_{(10)} = a_0 + 10 \cdot (a_1 + a_2 \cdot 10^1 + \cdots + a_n \cdot 10^{n-1}), \text{ com } n \in \mathbb{N}$$

Tomaremos $k = (a_1 + a_2 \cdot 10^1 + \cdots + a_n \cdot 10^{n-1})$, daí:

$$a_{(10)} = a_0 + 10k$$

Note que 10 pode ser escrito como $7 + 3$. Substituindo isso em $a_{(10)}$:

$$a_{(10)} = 7k + 3k + a_0$$

Dessa forma:

$$a_{(10)} = 10k + a_0 \equiv 3k + a_0 \equiv 3k - 6a_0 \equiv k - 2a_0 \mod 7$$

Portanto, $a_{(10)}$ é divisível por 7 quando $k - 2a_0$ também o for. □

A Descoberta de Chika Ofili

Em 2019, Chika Ofili, um jovem estudante de 12 anos da Nigéria, fez uma descoberta surpreendente ao encontrar um novo critério de divisibilidade por 7. Sua descoberta ocorreu enquanto ele estudava um livro de matemática e percebeu um padrão diferente para testar a divisibilidade por 7.

Teorema 3.6: Teorema de Chika Ofili

Um número natural n é divisível por 7 se, e somente se, ao multiplicarmos o algarismo das unidades por 5 e somarmos ao restante do número, o resultado for divisível por 7.

Demonstração. Tomemos um número inteiro $a_{(10)}$ divisível por 7, tal que:

$$a_{(10)} = a_0 + 10 \cdot (a_1 + a_2 \cdot 10^1 + \cdots + a_n \cdot 10^{n-1}), \text{ com } n \in \mathbb{N}$$

Tomaremos $k = (a_1 + a_2 \cdot 10^1 + \cdots + a_n \cdot 10^{n-1})$, daí:

$$a_{(10)} = a_0 + 10k.$$

Sabemos, pela demonstração anterior que:

$$a_{(10)} \equiv 3k + a_0 \pmod 7$$

Multiplicando ambos os lados por 5, obtemos:

$$5a_{(10)} \equiv 15k + 5a_0 \pmod 7$$

Temos ainda que $15 \equiv 1 \pmod 7$ e, portanto, segue:

$$5a_{(10)} \equiv k + 5a_0 \pmod 7.$$

Como $5a_{(10)} \equiv a_{(10)} \equiv 0 \pmod 7$, então:

$$k + 5a_0 \equiv 0 \pmod 7.$$

Ou seja, chegamos à conclusão que $a_{(10)}$ divisível por 7 se, e somente se então $k + 5a_0$ também. □

Exemplo 3.5

Por exemplo, vamos utilizar o critério para verificar que 4788 é divisível por 7. Temos então que $5a_0 + k = 5 \cdot 8 + 478 = 40 + 478 = 518$. Por outro lado, aplicando o critério em 518, teremos $5a_0 + k = 5 \cdot 8 + 51 = 91$ e, em seguida, aplicando o mesmo critério em 91, teremos $5a_0 + k = 5 \cdot 1 + 9 = 14$. Como $7 \mid 14$, concluímos que $7 \mid 91$, $7 \mid 518$ e, portanto, 4788 é divisível por 7.

Exemplo 3.6

Agora, também como exemplo, vamos utilizar o critério para verificar que 6080 **não é divisível** por 7. Temos então que $5a_0+k=5\cdot 0+608=608$. Por outro lado, aplicando o critério em 608, teremos $5a_0+k=5\cdot 8+60=100$ e, em seguida, aplicando o mesmo critério em 100, teremos $5a_0+k=5\cdot 0+10=10$. Como $7\nmid 10$, concluímos que $7\nmid 100$, $7\nmid 608$ e, portanto, 6080 **não é divisível** por 7.

O critério de divisibilidade por 7 surgiu como parte dos esforços dos matemáticos ao longo da história para simplificar cálculos. Sua formalização ocorreu na era moderna, impulsionada pelo desenvolvimento da teoria dos números. A descoberta recente de Chika Ofili demonstrou que ainda há espaço para inovações matemáticas, mesmo em conceitos aparentemente bem estabelecidos.

3.6.6Divisibilidade por 11 na Base Decimal

Teorema 3.7

Um número natural n é divisível por 11 se , e somente se, a diferença entre a soma dos seus algarismos de posição ímpar (unidades, centenas, etc.) e a soma dos algarismos de posição par (dezenas, milhares, etc.) for divisível por 11.

Demonstração. $(\Rightarrow)$ Tomemos um número inteiro $a_{(10)}$, tal que:

$$a_{(10)}=a_0+10\cdot(a_1+a_2\cdot 10^1+\cdots+a_n\cdot 10^{n-1}),\ \text{com } n\in\mathbb{N}$$

Suponhamos que $a_{(10)}$ é divisível por 11 e, dessa forma, $a_{(10)}\equiv 0 \pmod{11}$. Podemos perceber um padrão nos restos das divisões das potências de 10 por 11:

$$\begin{aligned}
10^0 &\equiv 1 \pmod{11},\\
10^1 &\equiv 10\equiv -1 \pmod{11},\\
10^2 &\equiv 100\equiv 1 \pmod{11},\\
10^3 &\equiv 1000\equiv -1 \pmod{11},\\
10^4 &\equiv 10000\equiv 1 \pmod{11},\\
&\vdots
\end{aligned}$$

Logo, as potências de 10 com expoente par são congruentes a $1 \pmod{11}$ e as de expoente ímpar são congruentes a $-1 \pmod{11}$. Daí:

$$a_{(10)} \equiv a_0 \cdot 1 - a_1 \cdot 1 + a_2 \cdot 1 - a_3 \cdot 1 \cdots + a_{2k} \cdot 1 - a_{2k+1} \cdot 1 \pmod{11}$$

Tomando $S_{2k} = a_0 + a_2 + a_4 + \cdots + a_{2k}$ e também $S_{2k+1} = a_1 + a_3 + a_5 + \cdots + a_{2k+1}$, temos:

$$a_{(10)} \equiv S_{2k} - S_{2k+1} \pmod{11}$$

Pela hipótese, chegamos a:

$$S_{2k} - S_{2k+1} \equiv 0 \pmod{11}$$

Logo, se $a_{(10)}$ é divisível por 11, a diferença entre a soma dos seus algarismos de posição ímpar e a soma dos algarismos de posição par é divisível por 11.

($\Leftarrow$) Agora, tomemos um número $a_{(10)}$ em que a diferença entre a soma dos seus algarismos de posição ímpar e a soma dos algarismos de posição par for divisível por 11. Ou seja:

$$S_{2k} - S_{2k+1} \equiv 0 \pmod{11}.$$

Ou, como visto acima:

$$a_{(10)} \equiv S_{2k} - S_{2k+1} \equiv 0 \pmod{11}.$$

Portanto, se a diferença entre a soma dos seus algarismos de posição ímpar e a soma dos algarismos de posição par for divisível por 11, o número $a_{(10)}$ também o é. $\square$

CAPÍTULO 4

Sistema de Numeração Binário

Nesse capítulo, será abordado o sistema de numeração binário e alguns critérios de divisibilidade e, para introduzir a aritmética binária, utilizamos a apostila do CEFET-SC [10] por apresentar uma abordagem didática, clara e acessível sobre o sistema binário, especialmente voltada para estudantes do ensino técnico e médio. Estes números são, atualmente, a base de sistemas computacionais que trabalham internamente com dois níveis de tensão, razão pela qual o seu sistema de numeração natural é o sistema binário (aceso, apagado). Com efeito, num sistema simples como este é possível simplificar o cálculo, com o auxílio da lógica booleana, que abordaremos a seguir. Em computação, chama-se um dígito binário (0 ou 1) de bit, que vem do inglês Binary Digit. Um agrupamento de 8 bits corresponde a um byte (Binary Term).

4.1O Sistema de Numeração Binário

O sistema binário é base para a álgebra booleana (de George Boole - matemático inglês), que permite fazer operações lógicas e aritméticas usando-se apenas dois dígitos ou dois estados (sim e não, falso e verdadeiro, tudo ou nada, 1 ou 0, ligado e desligado). Ela lida com variáveis que assumem apenas dois valores, geralmente representados como 0 ou 1, e define três operações principais geralmente denotadas como “E” ($\wedge$) e “OU” ($\vee$), uma operação unária “NÃO” ($\neg$). Toda a eletrônica digital e computação está baseada no sistema binário e na lógica de Boole, que permite representar por circuitos eletrônicos digitais (portas lógicas) os números, caracteres, realizar operações lógicas e aritméticas. Os programas de computadores são codificados sob forma binária e armazenados nas mídias (memórias, discos, etc.) sob esse formato.

Representaremos um número na base 2 por $b_{(2)}$, em que:

$$b_{(2)} = b_0 \cdot 2^0 + b_1 \cdot 2^1 + b_2 \cdot 2^2 + \cdots + b_n \cdot 2^n \text{ com } n \in \mathbb{N}$$

Exemplo 4.1

Por exemplo, o número $75_{(10)}$ tem a seguinte representação binária:

$$75_{(10)} = 1 \cdot 2^6 + 0 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 64 + 8 + 2 + 1 = 1001011_{(2)}$$

Dessa forma, a notação utilizada, **também posicional**, com $b_i \in \{0, 1\}$, é a seguinte:

$$b_{(2)} = b_n b_{n-1} b_{n-2} \ldots b_2 b_1 b_0$$

Note que números com os algarismos nas mesmas posições, mas em bases diferentes, não possuem necessariamente o mesmo valor. Por exemplo $101_{(10)} \neq 101_{(2)} = 5_{(10)}$.

4.2 Conversão da Base Decimal para Base Binária

A conversão da Base Decimal para a Base Binária pode ser feita utilizando o **método das divisões sucessivas por 2**. Este consiste em realizar a divisão inteira por 2, registrando o resto obtido (será 0 ou 1). Em seguida, aplicamos o mesmo processo com os quocientes obtidos sucessivamente, até obter quociente zero. O número binário correspondente é formado pelos restos, escritos na ordem inversa em que foram obtidos (de baixo para cima).

Primeiramente faremos um exemplo, vamos converter o número $45_{(10)}$ para a Base Binária. Vamos escrever, com simplicidade, $x \div d = q$ resto r para representar

$$x = qd + r \tag{4.1}$$

Logo:

$$\begin{aligned}
45 \div 2 &= 22 \quad \text{resto: } 1,\\
22 \div 2 &= 11 \quad \text{resto: } 0,\\
11 \div 2 &= 5 \quad \text{resto: } 1,\\
5 \div 2 &= 2 \quad \text{resto: } 1,\\
2 \div 2 &= 1 \quad \text{resto: } 0,\\
1 \div 2 &= 0 \quad \text{resto: } 1.
\end{aligned}$$

Dessa forma, os restos obtidos (de baixo para cima) são 1, 0, 1, 1, 0, 1. Logo, obtemos:

$$45_{(10)} = 101101_{(2)}$$

Este método funciona, porque ele se baseia na representação posicional dos números em binário. Generalizando, tomemos $a_{(10)}$ um número escrito na Base Decimal e $a_{(2)}$ na Base Binária. Daí:

$$\begin{aligned}
a_{(2)} &= 2 \cdot Q_1 + r_0;\\
Q_1 &= 2 \cdot Q_2 + r_1;\\
Q_2 &= 2 \cdot Q_3 + r_2;\\
Q_3 &= 2 \cdot Q_4 + r_3;\\
&\vdots\\
Q_k &= 2 \cdot Q_{k+1} + r_k,
\end{aligned}$$

ou seja, teremos $a_{(2)} = a_0 + 2a_1 + 4a_2 + \cdots + 2^k a_k = a_0 \cdot 2^0 + a_1 \cdot 2^1 + a_2 \cdot 2^2 + \cdots + a_k \cdot 2^k$. Observe que a primeira divisão nos dá o coeficiente a_0, a segunda divisão nos dá a_1, e assim por diante, até determinarmos a_k.

Para facilitar as próximas seções deste capítulo, vamos utilizar a seguinte tabela:

Tabela 4.1: Tabela de Números de 0 a 63 em Decimal e Binário

Decimal	Binário	Decimal	Binário	Decimal	Binário	Decimal	Binário
0	000000	16	010000	32	100000	48	110000
1	000001	17	010001	33	100001	49	110001
2	000010	18	010010	34	100010	50	110010
3	000011	19	010011	35	100011	51	110011
4	000100	20	010100	36	100100	52	110100
5	000101	21	010101	37	100101	53	110101
6	000110	22	010110	38	100110	54	110110
7	000111	23	010111	39	100111	55	110111
8	001000	24	011000	40	101000	56	111000
9	001001	25	011001	41	101001	57	111001
10	001010	26	011010	42	101010	58	111010
11	001011	27	011011	43	101011	59	111011
12	001100	28	011100	44	101100	60	111100
13	001101	29	011101	45	101101	61	111101
14	001110	30	011110	46	101110	62	111110
15	001111	31	011111	47	101111	63	111111

4.3 Algoritmo da Adição no Sistema Binário

A adição no sistema binário segue princípios semelhantes à adição no sistema decimal, mas com base 2, onde os únicos dígitos possíveis são 0 e 1. O método se reduz a regras simples para combinar estes dois valores, considerando que $0+0=0$, $1+0=1$, $0+1=1$ e $1+1=10_{(2)}=2_{(10)}$. Assim, quando somamos $1+1$, o dígito 0 é escrito na posição atual, e o 1 é transportado para a coluna seguinte. Este “vai 1” é o equivalente binário ao transporte usado na adição decimal.

Exemplo 4.2

Como exemplo, vamos somar $1011_{(2)}$ e $1101_{(2)}$ (equivalentes a 11 e 13, respectivamente, na base decimal):

$$\begin{array}{rr} & {\scriptstyle 1\,1\,1} \\ & 1011 \\ + & 1101 \\ \hline & 11000 \end{array}$$

Observe que:

$$11000_{(2)} = 1\cdot 2^4 + 1\cdot 2^3 + 0\cdot 2^2 + 0\cdot 2^1 + 0\cdot 2^0 = 16+8=24$$

Portanto, temos em binário $1011_{(2)} + 1101_{(2)} = 11000_{(2)}$ (em decimal seria $11+13=24$).

Para verificar a funcionalidade do método, tomemos dois números inteiros quaisquer A e B na base binária que contenham quatro algarismos. Ou seja:

$$A = a_0 + a_1 \cdot 2^1 + a_2 \cdot 2^2 + a_3 \cdot 2^3$$
$$B = b_0 + b_1 \cdot 2^1 + b_2 \cdot 2^2 + b_3 \cdot 2^3$$

Ao somarmos ambos os números obtemos:

$$A + B = (a_0 + b_0) + 2^1(a_1 + b_1) + 2^2(a_2 + b_2) + 2^3(a_3 + b_3).$$

Por exemplo, se a soma $a_0 + b_0 \geq 2$, teremos que $(a_0 + b_0) = 2^1 + c_0$ e, portanto:

$$A + B = c_0 + 2^1(a_1 + b_1 + 1) + 2^2(a_2 + b_2) + 2^3(a_3 + b_3).$$

Generalizando, para qualquer parcela $2^i \cdot (a_i + b_i), i \in \mathbb{N}$ e $0 < i \leq n$, se $a_i + b_i \geq 2$, ou seja, $a_i + b_i = 2 + c_i$ teremos:

$$2^i \cdot (a_i + b_i) = 2^i \cdot (2 + c_i) = 2^{i+1} + 2^i \cdot c_i.$$

Portanto, o algoritmo funciona para a adição de quaisquer dois números inteiros escritos na Base Binária.

É importante mencionar que o método da adição binária é fundamental para sistemas digitais e computação, sendo uma adaptação direta da adição posicional para a base. Sua simplicidade e eficiência tornam possível o funcionamento de computadores modernos e outros dispositivos eletrônicos.

4.4Algoritmo da Subtração no Sistema Binário

A subtração de números binários é semelhante à do sistema decimal, mas segue as regras da aritmética binária. O processo é feito ordem por ordem, comparando os dígitos de cima com os de baixo. Quando o dígito de cima é menor que o dígito correspondente de baixo, é necessário fazer um "empréstimo"da próxima ordem à esquerda, assim como ocorre na subtração decimal.

Exemplo 4.3

Por exemplo, vamos subtrair $10110_{(2)}$ de $11101_{(2)}$ (equivalentes a 22 e 29, respectivamente, na base decimal):

$$\begin{array}{r} 1\ \overset{0}{\cancel{1}}\ \overset{10}{\cancel{1}}\ \overset{10}{\cancel{0}}\ 1 \\ -1\ 0\ 1\ 1\ 0 \\ \hline 0\ 0\ 1\ 1\ 1 \end{array}$$

Observe que:

$$111_{(2)} = 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 4 + 2 + 1 = 7.$$

Portanto, temos em binário que $11101_{(2)} - 10110_{(2)} = 111_{(2)}$ (em decimal seria $29 - 22 = 7$).

Para verificar a funcionalidade do método, tomemos dois números inteiros A e B quaisquer na base binária que contenham quatro algarismos. Ou seja:

$$A = a_0 + a_1 \cdot 2^1 + a_2 \cdot 2^2 + a_3 \cdot 2^3$$
$$B = b_0 + b_1 \cdot 2^1 + b_2 \cdot 2^2 + b_3 \cdot 2^3.$$

Ao subtrairmos A por B, obtemos:

$$A - B = (a_0 - b_0) + 2^1(a_1 - b_1) + 2^2(a_2 - b_2) + 2^3(a_3 - b_3).$$

Por exemplo, se $b_0 > a_0$ (ou seja, $b_0 = 1$ e $a_0 = 0$), então $(a_0 - b_0) \notin \mathbb{N}$ e, daí, devemos "pegar emprestado" de a_1. Feito isso, teremos $a_0 = 10_{(2)} = 2_{(10)}$ e $a_1 = 0$, de forma a não alterar $A - B$. Generalizando, para qualquer parcela $2^i \cdot (a_i + b_i), i \in \mathbb{N}$ e $0 < i \leq n$ se $b_i > a_i$ devemos “pegar emprestado” 1 de a_{i+1}, ou seja, teremos:

$$2^i(a_i - b_i) + 2^{i+1}(a_{i+1} - b_{i+1}) = 2^i(a_i - b_i + 2) + 2^{i+1}(a_{i+1} - b_{i+1} - 1)$$

Portanto, o algoritmo funciona na subtração de quaisquer dois números inteiros na Base Binária.

4.5 Algoritmo da Multiplicação no Sistema Binário

Assim como as demais operações vistas anteriormente, a multiplicação de números binários é um processo simples baseado em regras fundamentais semelhantes às da multiplicação no sistema decimal, utilizando as propriedades de adição e deslocamento para calcular o produto. No entanto, as operações são realizadas apenas com os dígitos 0 e 1, tornando o método direto e eficiente, pois

$0 \times 0 = 0$, $0 \times 1 = 0$, $1 \times 0 = 0$ e $1 \times 1 = 1$. Dessa forma, o produto pela multiplicação de dois dígitos é sempre menor ou igual a 1 e não se faz necessária a adição de valores em ordens posteriores.

Exemplo 4.4

Por exemplo, vamos realizar a multiplicação $10101_{(2)}$ com $101_{(2)}$ (equivalentes a 21 e 5 respectivamente na base decimal):

$$\begin{array}{r}
10101 \\
\times \quad 101 \\
\hline
1\overset{1}{0}101 \\
\overset{1}{0}0000 \\
+10101 \\
\hline
1101001
\end{array}$$

Observe que:

$$1101001_{(2)} = 1 \cdot 2^6 + 1 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 = 64 + 32 + 8 + 1 = 105$$

Portanto, temos em binário que $10101_{(2)} \times 101_{(2)} = 1101001_{(2)}$ (em decimal seria $21 \times 5 = 105$).

Para verificar a funcionalidade do método, tomemos um número inteiro na base binária A de três algarismos e outro número inteiro B de dois algarismos. Ou seja:

$$A = a_0 + a_1 \cdot 2^1 + a_2 \cdot 2^2$$
$$B = b_0 + b_1 \cdot 2^1.$$

Ao multiplicar os dois números obtemos:

$$A \cdot B = a_0 b_0 + 2^1(a_1 b_0 + a_0 b_1) + 2^2(a_2 b_0 + a_1 b_1) + 2^3(a_2 b_1).$$

Por exemplo, se $a_1 b_0 = a_0 b_1 = 1$ então temos que $a_1 b_0 + a_0 b_1 = 2 > 1$. Neste caso, teremos:

$$AB = a_0 b_0 + 2^1(0) + 2^2(a_2 b_0 + a_1 b_1 + 1) + 2^3(a_2 b_1).$$

Generalizando, teremos $AB = \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} a_i b_j \cdot 2^k$ com $k = i + j$. Portanto, o algoritmo funciona na multiplicação de quaisquer dois números inteiros.

Observe que, diferentemente do sistema decimal (em que existia a possibilidade de $a_0b_0 \geq 10$), no sistema binário temos que $a_0b_0 < 2$. Isto ocorre, pois $a_0 = 1$ ou $a_0 = 0$, $b_0 = 1$ ou $b_0 = 0$ e, como $0 \times 0 = 0$, $0 \times 1 = 0$, $1 \times 0 = 0$ e $1 \times 1 = 1$, temos que qualquer produto $a_ib_i < 2$, com $a_ib_i \in \mathbb{Z}$ e $0 \leq i \leq n$.

4.6 Algoritmo da Divisão no Sistema Binário

A divisão de números no sistema binário segue um processo semelhante ao da divisão no sistema decimal, utilizando o método da "divisão longa" baseando em subtrações sucessivas e deslocamentos.

Exemplo 4.5

Como exemplo, vamos realizar a divisão de $111010_{(2)}$ por $101_{(2)}$ (equivalentes a 58 e 5 respectivamente na base decimal):

$$
\begin{array}{r|l}
111010 & \underline{\;101\;} \\
\underline{-101\;\;\;} & 1011 \\
1001 & \\
\underline{-101} & \\
1000 & \\
\underline{-101} & \\
11 &
\end{array}
$$

Apesar da execução deste método ser semelhante à do sistema decimal, vamos determinar alguns passos a seguir para resolver esta divisão.

I. Primeiro alinhamos 111010 (dividendo) e 101 (divisor) de forma que o divisor é colocado dentro de uma "casinha"e o dividendo fica do lado de fora;

II. Em seguida, verificamos que $111 > 101$ (equivalentes respectivamente a 7 e 5 na base decimal), logo subtraímos 101 de 111 obtendo 10 e colocamos o dígito 1 no quociente (abaixo do divisor);

III. Na sequência acrescentamos o próximo dígito de 111010 de forma que 10 se torne 100;

IV. Como $100 < 101$, acrescentamos 0 ao quociente e utilizamos o próximo dígito de 111010 e, então, 100 se torna 1001;

V. Agora, temos que $1001 > 101$ (equivalentes respectivamente a 9 e 5 na base decimal), logo subtraímos 101 de 1001 obtendo 100 e colocamos o dígito 1 no quociente;

VI. Na sequência acrescentamos o próximo dígito de 111010 de forma que 100 se torne 1000;

VII. Por fim, como $1000 > 101$ (equivalentes respectivamente a 8 e 5 na base decimal), subtraímos 101 de 1000 obtendo 11 e colocamos o dígito 1 no quociente;

IX. O quociente, ou resultado da divisão é 1011.

Logo, como escrito em 4.1 temos que $111010_{(2)} \div 101_{(2)} = 1011_{(2)}$ resto $11_{(2)}$ (em decimal seria $58 \div 5 = 11$ resto 3 como em 4.1).

Vamos considerar este exemplo como o caso geral. Para entender o motivo da exatidão deste método, devemos associar a divisão como uma operação da multiplicação "invertida".

4.7 Critérios de Divisibilidade na Base Binária

Após definir bem os métodos de aplicação de cada uma das quatro operações neste sistema, vamos analisar os critérios de divisibilidade. No sistema binário, esses critérios são particularmente importantes devido à sua aplicação em computação e eletrônica digital, onde operações binárias são fundamentais.

Neste capítulo trataremos dos critérios de divisibilidade por 2, 3, 5 e 7 na Base Binária. Em cada uma destas passagens, para uma melhor compreensão dos critérios de divisibilidade, utilizaremos a palavra "bit"ao invés de "dígito". Além disso, para verificar mais precisamente a funcionalidade de cada critério, aplicaremos em exemplos numéricos na base binária e verificaremos na base decimal.

4.7.1 Divisibilidade por 2 na Base Binária ($10_{(2)}$)

Teorema 4.1

Na base binária, um número é divisível por $2_{(10)} = 10_{(2)}$ se, e somente se, o dígito das unidades, a_0, for 0.

Demonstração. ($\Rightarrow$) Tomemos um número inteiro na base binária $a_{(2)}$, expresso na forma:

$$a_{(2)} = a_0 \cdot 2^0 + a_1 \cdot 2^1 + a_2 \cdot 2^2 + \cdots + a_n \cdot 2^n, \text{ com } n \in \mathbb{N}, a_i \in \{0,1\}.$$

Podemos escrever $a_{(2)}$ da seguinte forma, colocando 2 em evidência:

$$a_{(2)} = a_0 + 2 \cdot (a_1 + a_2 \cdot 2^1 + \cdots + a_n \cdot 2^{n-1}), \text{ com } n \in \mathbb{N}, a_i \in \{0,1\}.$$

Tomaremos $k = (a_1 + a_2 \cdot 2^1 + \cdots + a_n \cdot 2^{n-1})$, daí:

$$a_{(2)} = a_0 + 2 \cdot k.$$

Como $2 \cdot k$ é divisível por 2, e a_0 só pode ser igual a 1 ou 0, temos que $a_{(2)}$ será divisível por 2 somente se $a_0 = 0$.

($\Leftarrow$) Agora, nos resta mostrar a recíproca, ou seja, que se um número tem como último bit 0, então este número é divisível por 2.

De fato, vamos escrever:

$$a_{(2)} = a_0 + 2 \cdot l,$$

onde $a_0 = 0$, ou seja, $a_{(2)} = 2 \cdot l$ e, portanto, $2 \mid a_{(2)}$. □

Exemplo 4.6

Por exemplo, vamos utilizar o critério para verificar a divisibilidade de $11010_{(2)}$ por 2, na base binária. Neste caso, $a_0 = 0$ e, portanto, $11010_{(2)}$ é divisível por 2. Entretanto, sabemos que:

$$11010_{(2)} = 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0 = 16 + 8 + 2 = 26_{(10)}.$$

E, de fato, $2 \mid 26$.

Exemplo 4.7

Agora, também como exemplo, vamos utilizar o critério para verificar que $10011_{(2)}$ **não é divisível** por 2, na base binária. Neste caso, $a_0 \neq 0$ e, portanto, $10011_{(2)}$ **não é divisível** por 2.

Entretanto, sabemos que:

$$10011_{(2)} = 1 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 16 + 2 + 1 = 19_{(10)}.$$

E, de fato, $2 \nmid 19$.

4.7.2 Divisibilidade por 3 na Base Binária ($11_{(2)}$)

Teorema 4.2

Na base binária, um número é divisível por $3_{(10)} = 11_{(2)}$ se, e somente se, a diferença entre a soma de seus bits nas posições pares e a soma de seus bits nas posições ímpares for divisível por 3.

Demonstração. $(\Rightarrow)$ Da mesma forma da demonstração do teorema anterior, tomemos um número inteiro na base binária $a_{(2)}$, escrito na forma:

$$a_{(2)} = a_0 \cdot 2^0 + a_1 \cdot 2^1 + a_2 \cdot 2^2 + \cdots + a_n \cdot 2^n, \text{ com } n \in \mathbb{N}, a_i \in \{0, 1\}$$

Suponhamos que $a_{(2)}$ é divisível por 3 e, dessa forma, $a_{(2)} \equiv 0 \pmod 3$.

Podemos perceber um padrão nos restos das divisões das potências de 2 por 3:

$$\begin{aligned}
2^0 &\equiv 1 \pmod 3,\\
2^1 &\equiv 2 \pmod 3,\\
2^2 &\equiv 4 \equiv 1 \pmod 3,\\
2^3 &\equiv 8 \equiv 2 \pmod 3,\\
2^4 &\equiv 16 \equiv 1 \pmod 3,\\
&\vdots
\end{aligned}$$

Logo, as potências de 2 com expoente par são congruentes a $1 \pmod 3$ e as de expoente ímpar são congruentes a $2 \pmod 3$. Daí:

$$a_{(2)} \equiv a_0 \cdot 1 + a_1 \cdot 2 + a_2 \cdot 1 + a_3 \cdot 2 \cdots + a_{2k} \cdot 1 + a_{2k+1} \cdot 2 \pmod 3.$$

Colocando 1 e 2 em evidência:

$$a_{(2)} \equiv 1 \cdot (a_0 + a_2 + a_4 + \cdots + a_{2k}) + 2 \cdot (a_1 + a_3 + a_5 + \cdots + a_{2k+1}) \pmod 3.$$

Tomando $S_{2k} = a_0 + a_2 + a_4 + \cdots + a_{2k}$ e também $S_{2k+1} = a_1 + a_3 + a_5 + \cdots + a_{2k+1}$, temos:

$$a_{(2)} \equiv S_{2k} + 2 \cdot S_{2k+1} \pmod 3.$$

Como $a_{(2)} \equiv 0 \pmod 3$ então:

$$\begin{aligned} S_{2k} + 2 \cdot S_{2k+1} \equiv 0 &\pmod 3; \\ S_{2k} \equiv -2 \cdot S_{2k+1} &\pmod 3; \\ S_{2k} \equiv 1 \cdot S_{2k+1} &\pmod 3; \\ S_{2k} - S_{2k+1} \equiv 0 &\pmod 3. \end{aligned}$$

Logo, se $a_{(2)}$ é divisível por 3, então a diferença entre a soma dos bits nas posições pares e a soma dos bits nas posições ímpares deve ser divisível por 3.

($\Leftarrow$) Agora, tomemos um número binário em que a diferença entre a soma dos bits nas posições pares e a soma dos bits nas posições ímpares é divisível por 3. Ou seja:

$$S_{2k} - S_{2k+1} \equiv 0 \pmod 3$$

Ou, como visto acima:

$$S_{2k} + 2 \cdot S_{2k+1} \equiv 0 \pmod 3.$$

Além disso, temos que $a_{(2)} \equiv S_{2k} + 2 \cdot S_{2k+1} \pmod 3$ e, portanto, $a_{(2)} \equiv 0 \pmod 3$. Ou seja, se a diferença entre a soma dos bits nas posições pares e a soma dos bits nas posições ímpares é divisível por 3, o número $a_{(2)}$ também o é. □

Exemplo 4.8

Por exemplo, vamos utilizar o critério para verificar a divisibilidade de $11011_{(2)}$ por 3, na base binária. Temos então que $S_{2k} = a_0 + a_2 + a_4 = 1 + 0 + 1 = 2$ e $S_{2k+1} = a_1 + a_3 = 1 + 1 = 2$. Daí $S_{2k} - S_{2k+1} = 2 - 2 = 0$. Como $3 \mid 0$, temos que $11011_{(2)}$ é divisível por 3. Entretanto, sabemos que:

$$11011_{(2)} = 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 16 + 8 + 2 + 1 = 27_{(10)}.$$

E, de fato, $3 \mid 27$.

Exemplo 4.9

Agora, também como exemplo, vamos utilizar o critério para verificar que $110111_{(2)}$ **não é divisível** por 3, na base binária. Temos então que $S_{2k} = a_0 + a_2 + a_4 = 1 + 1 + 1 = 3$ e, além disso, $S_{2k+1} = a_1 + a_3 + a_5 = 1 + 0 + 1 = 2$. Daí $S_{2k} - S_{2k+1} = 3 - 2 = 1$. Como $3 \nmid 1$, temos que $110111_{(2)}$ **não é divisível** por 3. Entretanto, sabemos que:

$$110111_{(2)} = 1 \cdot 2^5 + 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 32 + 16 + 4 + 2 + 1 = 55_{(10)}.$$

E, de fato, $3 \nmid 55$.

É interessante observar que o critério de divisibilidade por 3 na base binária é análogo ao critério de divisibilidade por 11 na base decimal.

4.7.3 Divisibilidade por 5 na Base Binária ($101_{(2)}$)

Teorema 4.3

Na base binária, um número é divisível por 5 se, e somente se, diferença entre o número formado pelos seus últimos dois dígitos e o número formado pelos dígitos restantes for divisível por 5.

Demonstração. $(\Rightarrow)$ Assim como nas demonstrações anteriores, tomemos um número binário $a_{(2)}$, escrito na forma:

$$a_{(2)} = a_0 \cdot 2^0 + a_1 \cdot 2^1 + a_2 \cdot 2^2 + \cdots + a_n \cdot 2^n, \text{ com } n \in \mathbb{N}, a_i \in \{0, 1\}$$

Suponhamos que $a_{(2)}$ é divisível por 5 e, dessa forma, $a_{(2)} \equiv 0 \pmod 5$. Além disso, se tomarmos $b = (a_2 + a_3 \cdot 2^1 + a_4 \cdot 2^2 + \cdots + a_n \cdot 2^{n-2})$ e $a = (a_0 \cdot 2^0 + a_1 \cdot 2^1)$ temos:

$$a_{(2)} = a + 2^2 \cdot b = 4b + a$$

Ou seja, a representa os "dois últimos dígitos" do número $a_{(2)}$ e b os "dígitos restantes". Daí:

$$\begin{aligned} a_{(2)} &\equiv 0 \pmod 5; \\ 4b + a &\equiv 0 \pmod 5; \\ -b + a &\equiv 0 \pmod 5; \\ a - b &\equiv 0 \pmod 5. \end{aligned}$$

Portanto, se $a_{(2)}$ é divisível por 5, então a diferença entre o número formado pelos seus dois últimos dígitos e o número formado pelos dígitos restantes é divisível por 5.

($\Leftarrow$) Agora, tomemos $a_{(2)}$ de forma que a diferença entre o número formado pelos seus dois últimos dígitos e o número formado pelos dígitos restantes seja divisível por 5. Daí, como antes, obtemos:

$$\begin{aligned} a - b &\equiv 0 \pmod 5; \\ a + 4b &\equiv 0 \pmod 5; \\ a_{(2)} &\equiv 0 \pmod 5. \end{aligned}$$

Logo, se a diferença entre o número formado pelos seus dois últimos dígitos e o número formado pelos dígitos restantes for divisível por 5, temos que $a_{(2)}$ é divisível por 5. $\square$

Exemplo 4.10

Por exemplo, vamos utilizar o critério para verificar a divisibilidade de $110010_{(2)}$ por 5, na base binária. Ao separar os dois últimos dígitos dos restantes teremos $1100_{(2)} - 10_{(2)} = 1010_{(2)}$, mas $1010_{(2)} = 10$. Como $5 \mid 10$, temos que $110010_{(2)}$ é divisível por 5. Entretanto, sabemos que:

$$110010_{(2)} = 1 \cdot 2^5 + 1 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0 = 32 + 16 + 2 = 50_{(10)}.$$

E, de fato, $5 \mid 50$.

Exemplo 4.11

Agora, também como exemplo, vamos utilizar o critério para verificar que $111111_{(2)}$ **não é divisível** por 5, na base binária. Ao separar os dois últimos dígitos dos restantes teremos $1111_{(2)} - 11_{(2)} = 1100_{(2)}$, mas $1100_{(2)} = 12$. Como $5 \nmid 12$, temos que $111111_{(2)}$ **não é divisível** por 5. Entretanto, sabemos que:

$$111111_{(2)} = 1 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 32 + 16 + 8 + 4 + 2 + 1 = 63_{(10)}.$$

E, de fato, $5 \nmid 63$.

4.7.4 Divisibilidade por 7 na Base Binária ($111_{(2)}$)

Teorema 4.4

Um número binário é divisível por 7 se, e somente se, a soma dos números formados pelos seus bits, agrupados de três em três (da direita para a esquerda), for divisível por 7 (no sistema binário).

Demonstração. ($\Rightarrow$) Como nas demonstrações dos critérios anteriores, tomemos um número inteiro na base binária $a_{(2)}$, escrito na forma:

$$a_{(2)} = a_0 \cdot 2^0 + a_1 \cdot 2^1 + a_2 \cdot 2^2 + \cdots + a_n \cdot 2^n, \text{ com } n \in \mathbb{N}, a_i \in \{0, 1\}$$

Suponhamos que $a_{(2)}$ é divisível por 7 e, dessa forma, $a_{(2)} \equiv 0 \pmod 7$.

Podemos perceber um padrão nos restos das divisões das potências de 2 por 7:

$$\begin{aligned}
2^0 &\equiv 1 \pmod 7, \\
2^1 &\equiv 2 \pmod 7, \\
2^2 &\equiv 4 \pmod 7, \\
2^3 &\equiv 8 \equiv 1 \pmod 7, \\
2^4 &\equiv 16 \equiv 2 \pmod 7, \\
2^5 &\equiv 32 \equiv 4 \pmod 7, \\
&\vdots
\end{aligned}$$

De forma geral, para considerar qualquer expoente inteiro, tomemos $k \in \mathbb{Z}$, daí:

$$\begin{aligned}
2^{3k} &\equiv 8^k \equiv 1 \pmod 7, \\
2^{3k+1} &\equiv 8^k \cdot 2^1 \equiv 2 \pmod 7, \\
2^{3k+2} &\equiv 8^k \cdot 2^2 \equiv 4 \pmod 7.
\end{aligned}$$

Como $a_{(2)} = a_0 \cdot 2^0 + a_1 \cdot 2^1 + a_2 \cdot 2^2 + \cdots + a_{3k} \cdot 2^{3k} + a_{3k+1} \cdot 2^{3k+1} + a_{3k+2} \cdot 2^{3k+2}$, teremos:

$$a_{(2)} \equiv a_0 + 2a_1 + 4a_2 + \cdots + a_{3k} + 2a_{3k+1} + 4a_{3k+2} \pmod 7$$
$$a_{(2)} \equiv (a_0 + a_3 + \cdots + a_{3k}) + 2(a_1 + a_4 + \cdots + a_{3k+1}) + 4(a_2 + a_5 + \cdots + a_{3k+2}) \pmod 7$$

Tomando $S_1 = (a_0 + a_3 + \cdots + a_{3k})$, $S_2 = (a_1 + a_4 + \cdots + a_{3k+1})$ e $S_3 = 4(a_2 + a_5 + \cdots + a_{3k+2})$:

$$a_{(2)} \equiv S_1 + 2S_2 + 4S_3 \equiv 0 \pmod 7$$

Portanto, se $a_{(2)}$ é divisível por 7, então a soma $S_1 + 2^1 \cdot S_2 + 2^2 \cdot S_3$ também o é.

($\Leftarrow$) Agora, tomemos $a_{(2)}$ de forma que a soma dos números formados pelos seus bits, agrupados de três em três (da direita para a esquerda), seja divisível por 7, ou seja:

$$S_1 + 2^1 \cdot S_2 + 2^2 \cdot S_3 \equiv 0 \pmod 7.$$

Entretanto, $a_{(2)} = S_1 + 2S_2 + 4S_3$ e, portanto, $a_{(2)}$ também é divisível por 7. $\square$

Exemplo 4.12

Por exemplo, vamos utilizar o critério para verificar que $110001_{(2)}$ é divisível por 7, na base binária. Temos então que $a_5a_4a_3 + a_2a_1a_0 = 110 + 001 = 111_{(2)} = 7_{(10)}$ e $7 \mid 7_{(10)}$.
Portanto, $110001_{(2)}$ é divisível por 7. Entretanto, sabemos que:

$$110001_{(2)} = 1 \cdot 2^5 + 1 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 = 32 + 16 + 1 = 49_{(10)}.$$

E, de fato, $7 \mid 49$.

Exemplo 4.13

Agora, também como exemplo, vamos utilizar o critério para verificar que $111101_{(2)}$ **não é divisível** por 7, na base binária. Temos então que $a_5a_4a_3 + a_2a_1a_0 = 111 + 101 = 1100_{(2)} = 12_{(10)}$ e $7 \nmid 12_{(10)}$. Portanto, $111101_{(2)}$ **não é divisível** por 7. Entretanto, sabemos que:

$$111101_{(2)} = 1 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 = 32 + 16 + 8 + 4 + 1 = 61_{(10)}.$$

E, de fato, $7 \nmid 61$.

Observação: o critério de divisibilidade por 7 na base binária é análogo ao critério de divisibilidade por 111 na base decimal. Além disso, ao estudarmos os critérios de divisibilidade por $3_{(10)} = 11_{(2)}$ e

$7_{(10)} = 111_{(2)}$, percebemos que os restos das divisões das potências de 2 pelos respectivos números resultavam em $2^k \pmod{n}$, onde k pode assumir como valor máximo o número de bits que compõe n na base binária. Daí, percebemos uma área de estudo com todos os números formados somente por bits 1 (ou seja, na forma $2^m - 1$, com $m \in \mathbb{Z}_+$), como por exemplo $15_{(10)} = 1111_{(2)}$, $31_{(10)} = 11111_{(2)}$, $63_{(10)} = 111111_{(2)}$, etc.

CAPÍTULO 5

Sistema de Numeração Hexadecimal

Nesse capítulo trabalharemos o sistema de numeração hexadecimal e alguns critérios de divisibilidade e, para introduzir a aritmética hexadecimal, utilizamos a apostila do CEFET-SC [10]. O sistema hexadecimal (base 16) é amplamente utilizado em computação e eletrônica digital devido à sua relação direta com o sistema binário e à sua eficiência na representação de números. Isso porque ele permite escrever valores longos usando menos dígitos, o que facilita tanto o armazenamento quanto o processamento de dados. No capítulo anterior, ao estudarmos o sistema binário, ficou evidente que sua principal desvantagem é a grande quantidade de bits necessária para representar mesmo números relativamente pequenos. Nesse contexto, o estudo da base hexadecimal se torna relevante, pois ela permite representar esses mesmos valores de forma mais enxuta e legível, contribuindo para a organização e interpretação de informações na área da computação e da eletrônica.

5.1O Sistema de Numeração Hexadecimal

De acordo com Scotti e Ferreira, o sistema hexadecimal está vinculado à informática, pois os computadores costumam utilizar o byte como unidade básica da memória. Sabendo que 1 byte = 8 bits, um byte pode ser representado por 8 algarismos do sistema binário ou por 2 algarismos do sistema hexadecimal.

Este sistema é essencial para a computação moderna, pois oferece uma maneira mais legível e eficiente de lidar com dados binários, como endereços de memória, cores e codificação de informações, já que cada dígito hexadecimal representa quatro bits, permitindo representar grandes quantidades de dados com menos caracteres.

Representaremos um número inteiro positivo na base 16 por $h_{(16)}$, em que:

$$h_{(16)} = h_0 \cdot 16^0 + h_1 \cdot 16^1 + h_2 \cdot 16^2 + \cdots + h_n \cdot 16^n, \text{ com } n \in \mathbb{N}$$

Exemplo 5.1

Por exemplo, o número $600_{(10)}$ tem a seguinte representação hexadecimal:

$$600_{(10)} = 2 \cdot 16^2 + 5 \cdot 16^1 + 8 \cdot 16^0 = 2 \cdot 256 + 5 \cdot 16 + 8 \cdot 1 = 258_{(16)}.$$

Portanto, a notação utilizada, **também posicional**, com $h_i \in \{0, 1, \ldots, 15\}$, é a seguinte:

$$h_{(16)} = h_n h_{n-1} h_{n-2} \ldots h_2 h_1 h_0.$$

No caso do sistema numérico hexadecimal, teremos bits maiores do que 9 e, se continuássemos apenas com números, usaríamos dois dígitos para estes bits. Então, para evitar confusão, foram escolhidas as letras A, B, C, D, E e F para representar 10 a 15. Por exemplo, o número $175_{(10)}$ será representado por:

$$175_{(10)} = 10 \cdot 16^1 + 15 \cdot 16^0 = AF_{(16)}.$$

Note também que, assim como nos sistema binário, números com os algarismos nas mesmas posições, mas em bases diferentes, não possuem necessariamente o mesmo valor. Por exemplo $142_{(10)} \neq 142_{(16)} = 322_{(10)}$.

5.2 Conversão da Base Decimal para a Base Hexadecimal

De forma semelhante ao capítulo anterior, a conversão da Base Decimal para a Base Hexadecimal pode ser feita utilizando o **método das divisões sucessivas por 16**, que consiste em realizar a divisão inteira por 16, registrando o resto obtido. Aplicamos o método sucessivamente com os quocientes obtidos até se obter zero como resultado. O número hexadecimal correspondente é formado pelos restos, escritos na ordem inversa em que foram obtidos (de baixo para cima).

Exemplo 5.2

Como exemplo, vamos converter o número $450_{(10)}$ para a Base Hexadecimal:

$$\begin{aligned} 450 \text{ dividido por } 16 \text{ tem quociente } 28 \text{ e resto } 2,\\ 28 \text{ dividido por } 16 \text{ tem quociente } 1 \text{ e resto } 12,\\ 1 \text{ dividido por } 16 \text{ tem quociente } 0 \text{ e resto } 1. \end{aligned}$$

Dessa forma, os restos obtidos de baixo para cima foram 1, 12 e 2.

Como o algarismo equivalente a 12 é a letra C, obtemos:

$$450_{(10)} = 1C2_{(16)}$$

Demonstração. Este método funciona, porque, assim como nos sistemas estudados anteriormente, ele se baseia na representação posicional dos números hexadecimais. Generalizando, tomemos $a_{(10)}$ um número escrito na Base Decimal e $a_{(16)}$ na Base Binária. Daí:

$$\begin{aligned} a_{(16)} &= 16 \cdot Q_1 + r_0;\\ Q_1 &= 16 \cdot Q_2 + r_1;\\ Q_2 &= 16 \cdot Q_3 + r_2;\\ Q_3 &= 16 \cdot Q_4 + r_3;\\ &\vdots\\ Q_k &= 16 \cdot Q_{k+1} + r_k. \end{aligned}$$

Ou seja, teremos $a_{(16)} = a_0 + 16a_1 + 256a_2 + \cdots + 16^k a_k = a_0 \cdot 16^0 + a_1 \cdot 16^1 + a_2 \cdot 16^2 + \cdots + a_k \cdot 16^n$. Observe que a primeira divisão nos dá o coeficiente a_0, a segunda divisão nos dá a_1, e assim por diante, até determinarmos a_k. $\square$

Para facilitar as próximas seções deste capítulo, vamos utilizar a seguinte tabela:

Tabela 5.1: Tabela de Números de 0 a 63 em Decimal e Hexadecimal

Base 10	Base 16	Base 10	Base 16	Base 10	Base 16	Base 10	Base 16
0	0	16	10	32	20	48	30
1	1	17	11	33	21	49	31
2	2	18	12	34	22	50	32
3	3	19	13	35	23	51	33
4	4	20	14	36	24	52	34
5	5	21	15	37	25	53	35
6	6	22	16	38	26	54	36
7	7	23	17	39	27	55	37
8	8	24	18	40	28	56	38
9	9	25	19	41	29	57	39
10	A	26	1A	42	2A	58	3A
11	B	27	1B	43	2B	59	3B
12	C	28	1C	44	2C	60	3C
13	D	29	1D	45	2D	61	3D
14	E	30	1E	46	2E	62	3E
15	F	31	1F	47	2F	63	3F

5.3 Algoritmo da Adição no Sistema Hexadecimal

A adição na base hexadecimal segue princípios semelhantes aos das bases decimal e binário, mas usa 16 símbolos ($0-9$ e $A-F$). Como nos demais sistemas numéricos posicionais, alinha-se os algarismos que compõem cada número e soma-se dígito a dígito, da direita para a esquerda, transportando o valor excedente quando a soma dos dígitos excede 16.

Exemplo 5.3

Como exemplo, vamos somar $F3A_{(16)} = 15 \cdot 16^2 + 3 \cdot 16^1 + 10 \cdot 16^0 = 3840 + 48 + 10 = 3898_{(10)}$ e $B9C_{(16)} = 11 \cdot 16^2 + 9 \cdot 16^1 + 12 \cdot 16^0 = 2816 + 144 + 12 = 2972_{(10)}$:

$$\begin{array}{rr} & F\overset{1}{3}A \\ + & B9C \\ \hline & 1AD6 \end{array}$$

Podemos observar que $A + C = 10 + 12 = 22 = 16 + 6$ e, portanto, explica o resultado 6 nas unidades com 1 sendo transportado para a casa seguinte. Além disso, $F + B = 15 + 11 = 26 = 16 + 10$, explicando o resultado $F + B = 1A$ em hexadecimal. Na base decimal temos:

$$1AD6_{(16)} = 1 \cdot 16^3 + 10 \cdot 16^2 + 13 \cdot 16^1 + 6 \cdot 16^0 = 4096 + 2560 + 208 + 6 = 6870_{(10)}.$$

Portanto, a soma hexadecimal $F3A_{(16)} + B9C_{(16)} = 1AD6_{(16)}$, em decimal seria $3898 + 2972 =$

6870.

Para verificar a funcionalidade do método, tomemos dois números inteiros quaisquer na base hexadecimal A e B de três algarismos. Ou seja:

$$A = a_0 + a_1 \cdot 16^1 + a_2 \cdot 16^2$$
$$B = b_0 + b_1 \cdot 16^1 + b_2 \cdot 16^2$$

Ao somarmos ambos os números obtemos:

$$A + B = (a_0 + b_0) + 16^1 \cdot (a_1 + b_1) + 16^2 \cdot (a_2 + b_2).$$

Por exemplo, se a soma $a_0 + b_0 \geq 16$, teremos que $(a_0 + b_0) = 16^1 + c_0$ e, portanto:

$$A + B = c_0 + 16^1(a_1 + b_1 + 1) + 16^2(a_2 + b_2).$$

De forma análoga e geral, para qualquer parcela $16^i \cdot (a_i + b_i), i \in \mathbb{N}$ com $0 < i \leq n$, se $a_i + b_i \geq 16$, ou seja, $a_i + b_i = 16 + c_i$ teremos:

$$16^i \cdot (a_i + b_i) = 16^i \cdot (16^1 + c_i) = 16^{i+1} + 16^i \cdot c_i.$$

Portanto, o algoritmo funciona para a adição de quaisquer dois números inteiros hexadecimais.

5.4Algoritmo da Subtração no Sistema Hexadecimal

A subtração de números hexadecimais é similar à aplicada no sistema decimal, e assim como o método anterior, é sequencial, ou seja dígito a dígito. O método se baseia em regras específicas para a subtração ordem por ordem. Quando uma dessas operações não é possível de se realizar em $\mathbb{N}$, é necessário “pegar emprestado” uma unidade da ordem seguinte, e neste caso, aumentando o valor em 16 e diminuindo o dígito da coluna da esquerda em 1.

Exemplo 5.4

Por exemplo, vamos realizar a subtração $D5A_{(16)} - B1C_{(16)}$(equivalentes a $3418_{(10)}$ e $2844_{(10)}$)

$$\begin{array}{r} D\overset{4}{\cancel{5}}\overset{1A}{\cancel{A}} \\ -B1C \\ \hline 23E \end{array}$$

Observe que:

$$23E_{(16)} = 2 \cdot 16^2 + 3 \cdot 16^1 + 14 \cdot 16^0 = 512 + 48 + 14 = 574_{(10)}.$$

Portanto, temos que $D5A_{(16)} - B1C_{(16)} = 23E_{(16)}$ (em decimal seria $3418 - 2844 = 574$).

Para verificar a funcionalidade do método, tomemos dois números inteiros quaisquer na base decimal A e B de três algarismos. Ou seja:

$$A = a_0 + a_1 \cdot 16^1 + a_2 \cdot 16^2$$
$$B = b_0 + b_1 \cdot 16^1 + b_2 \cdot 16^2$$

Ao subtrairmos A por B, obtemos:

$$A - B = (a_0 - b_0) + 16^1 \cdot (a_1 - b_1) + 16^2 \cdot (a_2 - b_2).$$

Por exemplo, se $b_0 > a_0$, então $(a_0 - b_0) \notin \mathbb{N}$ e, daí, devemos "pegar emprestado" 1 de a_1. Isso transforma a_0 em $a_0 + 16$ e, como $0 \leq b_0 \leq 15$ então $a_0 + 16 \geq b_0$ e, agora temos $(a_0 + 16 - b_0) \in \mathbb{N}$. Por outro lado, agora também temos a parcela $16^1(a_1 - 1 - b_1)$, de forma a não alterar $A - B$. Generalizando, para qualquer parcela $16^i \cdot (a_i + b_i), i \in \mathbb{Z}$ e $0 < i \leq n$ se $b_i > a_i$ devemos “pegar emprestado” 1 de a_{i+1}, ou seja, teremos:

$$16^i(a_i - b_i) + 16^{i+1}(a_{i+1} - b_{i+1}) = 16^i(a_i + 16 - b_i) + 16^{i+1}(a_{i+1} - 1 - b_{i+1}).$$

Portanto, o algoritmo funciona na subtração de quaisquer dois números inteiros hexadecimais.

5.5 Algoritmo da Multiplicação no Sistema Hexadecimal

A multiplicação no sistema hexadecimal segue os mesmos princípios da multiplicação no sistema decimal, entretanto possui diferença no reagrupamento que se faz necessário quando o produto obtido em determinada ordem excede 15.

Para realizar o algoritmo, alinhamos ambos os números e multiplicamos os dígitos individualmente, considerando a ordem, de um dos números pelo outro. Em seguida, somamos os resultados obtidos. Recomendamos, de início, que ao aplicar este algoritmo verifique a tabela de conversão de decimal para hexadecimal.

Exemplo 5.5

Por exemplo, vamos realizar a multiplicação $2F_{(16)}$ com $1A_{(16)}$ (equivalentes a 47 e 26 respectivamente na base decimal):

$$\begin{array}{r} \overset{\color{red}9}{2}F \\ \times \quad 1A \\ \hline \overset{\color{red}1}{1}D6 \\ +2F \\ \hline 4C6 \end{array}$$

Analisando detalhadamente a multiplicação com alguns dígitos:

$$F \cdot A = 15 \cdot 10 = 150 = {\color{red}9} \cdot 16 + {\color{red}6}$$

$$2 \cdot A + 9 = 2 \cdot 10 + 9 = 29 = {\color{red}1} \cdot 16 + {\color{red}13} = 1D$$

Agora, analisando a soma:

$$D + F = 13 + 15 = 28 = 16 + 12 = 16 \cdot {\color{red}1} + {\color{red}C}.$$

Portanto, temos em hexadecimal que $2F_{(16)} \times 1A_{(16)} = 4C6_{(16)}$ (em decimal $47 \times 26 = 1.222$).

Para verificar a funcionalidade do método, tomemos um número hexadecimal A de dois algarismos e outro número hexadecimal B de dois algarismos. Ou seja:

$$A = a_0 + a_1 \cdot 16^1 + a_2 \cdot 16^2$$
$$B = b_0 + b_1 \cdot 16^1$$

Ao multiplicar os dois números obtemos:

$$AB = a_0 b_0 + 16^1(a_1 b_0 + a_0 b_1) + 16^2(a_2 b_0 + a_1 b_1) + 16^3(a_2 b_1).$$

Por exemplo, se $a_0 b_0 \geq 16$ então $a_0 b_0 = 16c_1 + c_0$, com $c_1 > 0$, daí:

$$AB = c_0 + 16^1(a_1 b_0 + a_0 b_1 + c_1) + 16^2(a_2 b_0 + a_1 b_1) + 16^3(a_2 b_1).$$

Então, generalizando, para qualquer parcela $16^i \cdot (a_i \cdot b_i), i \in \mathbb{Z}$ e $0 < i \leq n$, se $a_i b_i \geq 16$, ou seja, $a_i b_i = 16 \cdot c_{i+1} + c_i$, com $c_{i+1} > 0$, teremos:

$$16^i \cdot (a_i b_i) = 16^i \cdot (16^{i+1} c_{i+1} + c_i) = 16^{i+1} \cdot c_{i+1} + 16^i c_i.$$

Portanto, o algoritmo funciona na multiplicação de quaisquer dois números hexadecimais e de forma semelhante ao algoritmo na base decimal.

5.6 Algoritmo da Divisão no Sistema Hexadecimal

A divisão no sistema hexadecimal segue os mesmos princípios da divisão no sistema decimal, mas utilizando a base 16. Isto é, possui referência no Algoritmo da Divisão de Euclides, porém possui uma própria estrutura sistemática do que chamamos de “divisão longa”.

Exemplo 5.6

Como exemplo, vamos realizar a divisão de $7D2_{(16)}$ por $1E_{(16)}$ (equivalentes a 2002 e 30, respectivamente, na base decimal):

$$
\begin{array}{rr|l}
 & 7D2 & \underline{\;1E\;\;} \\
(4\times16+4\times14) & \underline{-78} & 42 \quad (4\times16+2) \\
 & 52 & \\
(2\times16+2\times14) & \underline{-46} & \\
 & 16 &
\end{array}
$$

Apesar da execução deste método ser semelhante à do sistema decimal, vamos determinar alguns passos a seguir para resolver esta divisão.

I. Primeiro alinhamos $7D2$ (dividendo) e $1E$ (divisor) de forma que o divisor é colocado dentro de uma "casinha"e o dividendo fica do lado de fora;

II. Em seguida, verificamos que $7D > 4 \times 1E$ (equivalentes, respectivamente, a 125 e 4×30 na base decimal), logo subtraímos 78 de $7D$ obtendo 5 e colocamos o dígito 4 no quociente (abaixo do divisor);

III. Na sequência descemos o próximo dígito de $7D2$, de forma que 5 se torne 52;

IV. Agora, temos que $52 > 2 \times 1E$ (equivalentes respectivamente a 82 e 2×30 na base decimal), logo subtraímos 46 de 52 obtendo 16 e colocamos o dígito 2 no quociente;

V. O quociente, ou resultado da divisão é 42.

Logo, temos que $7D2_{(16)} \div 1E_{(16)} = 42_{(16)}$ com resto $16_{(16)}$ (em decimal seria $2002 \div 30 = 66$ com resto 22).

5.7 Critérios de Divisibilidade na Base Hexadecimal

Após definir bem os métodos de aplicação de cada uma das quatro operações neste sistema, vamos analisar os critérios de divisibilidade. Como na computação a base hexadecimal é amplamente utilizada para representar grandes números binários utilizando uma quantidade menor de dígitos, os critérios de divisibilidade permitem a implementação de algoritmos mais eficientes para verificação rápida de múltiplos em sistemas de criptografia e redes.

Neste capítulo trataremos, assim como no capítulo anterior, dos critérios de divisibilidade por 2, 15 (e portanto 3 e 5), 7, 11, 13 e 17 na Base Hexadecimal. Em cada uma destas passagens, para uma melhor compreensão dos critérios de divisibilidade, utilizaremos a palavra "bit"ao invés de "dígito". Além disso, para verificar mais precisamente a funcionalidade de cada critério, aplicaremos em exemplos numéricos na base hexadecimal e verificaremos na base decimal.

5.7.1 Divisibilidade por 2 na Base Hexadecimal

Teorema 5.1

Na base hexadecimal, um número é divisível por 2 se, e somente se, o último bit da esquerda para a direita $a_0 \in \{0,2,4,6,8,10,12,14\}$, ou seja, se o número terminar com algarismo par.

Demonstração. $(\Rightarrow)$ Tomemos um número inteiro na base hexadecimal $a_{(16)}$, expresso na forma:

$$a_{(16)} = a_0 \cdot 16^0 + a_1 \cdot 16^1 + a_2 \cdot 16^2 + \cdots + a_n \cdot 16^n, \text{ com } n \in \mathbb{N}, a_i \in \{0,1,2,\ldots,15\}.$$

Podemos escrever $a_{(16)}$ da seguinte forma, colocando 16 em evidência:

$$a_{(16)} = a_0 + 16 \cdot (a_1 + a_2 \cdot 16^1 + \cdots + a_n \cdot 16^{n-1}), \text{ com } n \in \mathbb{N}, a_i \in \{0,1,2,\ldots,15\}.$$

Tomaremos $k = (a_1 + a_2 \cdot 16^1 + \cdots + a_n \cdot 16^{n-1})$, daí:

$$a_{(16)} = a_0 + 16 \cdot k.$$

Como $16 \cdot k$ é divisível por 2, temos que $a_{(16)}$ será divisível por 2 somente se $a_0 \in \{0,2,4,6,8,10,12,14\}$.

$(\Leftarrow)$ Agora, nos resta mostrar a recíproca, ou seja, que se um número tem como último bit $a_0 \in \{0,2,4,6,8,10,12,14\}$, então este número é divisível por 2.

De fato, vamos escrever:

$$a_{(16)} = a_0 + 16 \cdot k,$$

onde $a_0 \in \{0,2,4,6,8,10,12,14\}$, ou seja, $a_0 = 2 \cdot b_0$. Dessa forma:

$$a_{(16)} = 2 \cdot (b_0 + 8l).$$

Portanto, $2 \mid a_{(16)}$. □

Exemplo 5.7

Por exemplo, vamos utilizar o critério para verificar a divisibilidade de $1AC_{(16)}$ por 2, na base hexadecimal. Neste caso, $a_0 = C = 12_{(10)}$, par e, portanto, $1AC_{(16)}$ é divisível por 2. Entretanto, sabemos que:

$$1AC_{(16)} = 1 \cdot 16^2 + 10 \cdot 16^1 + 12 \cdot 16^0 = 256 + 160 + 12 = 428_{(10)}.$$

E, de fato, $2 \mid 428$.

Exemplo 5.8

Agora, também como exemplo, vamos utilizar o critério para verificar que $15B_{(16)}$ **não é divisível** por 2, na base hexadecimal. Neste caso, $a_0 = B = 11_{(10)}$, não é par e, portanto, $15B_{(16)}$ **não é divisível** por 2. Entretanto, sabemos que:

$$15B_{(16)} = 1 \cdot 16^2 + 5 \cdot 16^1 + 11 \cdot 16^0 = 256 + 80 + 11 = 347_{(10)}.$$

E, de fato, $2 \nmid 347$.

5.7.2 Divisibilidade por 3 e 5 na Base Hexadecimal

Teorema 5.2

Na base hexadecimal, um número é divisível por 3 ou por 5 se, e somente se, a soma dos seus dígitos for divisível por 3 ou por 5.

Demonstraremos, simultaneamente, a divisibilidade por 3 ou 5, através da divisibilidade por 15, visto que $15 = 3 \cdot 5$.

Demonstração. $(\Rightarrow)$ De início, da mesma forma da demonstração do teorema anterior, tomemos um número inteiro na base hexadecimal $a_{(16)}$, escrito na forma:

$$a_{(16)} = a_0 \cdot 16^0 + a_1 \cdot 16^1 + a_2 \cdot 16^2 + \cdots + a_n \cdot 16^n, \text{ com } n \in \mathbb{N}, a_i \in \{0, 1, 2, \ldots, 15\}.$$

Suponhamos, então, que $a_{(16)}$ é divisível por 15 e, portanto, $a_{(16)} \equiv 0 \pmod{15}$. Além disso, observamos que $16 \equiv 16^i \equiv 1^i \equiv 1 \pmod{15}$, com $i \in \mathbb{Z}$. Daí:

$$a_{(16)} \equiv a_0 \cdot 1 + a_1 \cdot 1 + a_2 \cdot 1 + \cdots + a_n \cdot 1 \pmod{15}.$$

Pela hipótese, teremos então:

$$a_{(16)} \equiv a_0 + a_1 + a_2 + \cdots + a_n \equiv 0 \pmod{15}$$

Logo, se $a_{(16)}$ for divisível por 15 (e, portanto, por 3 ou 5), então a soma dos seus algarismos também será.

($\Leftarrow$) Agora, vamos supor que a soma dos algarismos de $a_{(16)}$ é divisível por 15, ou seja:

$$a_0 + a_1 + a_2 + \cdots + a_n \equiv 0 \pmod{15}.$$

Por outro lado:

$$a_{(16)} \equiv a_0 \cdot 16^0 + a_1 \cdot 16^1 + \cdots + a_n \cdot 16^n \equiv a_0 \cdot 1 + a_1 \cdot 1 + a_2 \cdot 1 + \cdots + a_n \cdot 1 \pmod{15}.$$

E pelo que foi visto anteriormente:

$$a_{(16)} \equiv a_0 + a_1 + a_2 + \cdots + a_n \equiv 0 \pmod{15}.$$

Logo, se a soma dos algarismos de $a_{(16)}$ for divisível por 15 (e, portanto, por 3 ou 5), então o próprio $a_{(16)}$ também será. $\square$

Exemplo 5.9

Por exemplo, vamos utilizar o critério para verificar a divisibilidade de $24F_{(16)}$ por 3, na base hexadecimal. Temos então que $a_2 + a_1 + a_0 = 2 + 4 + 15 = 21$ e $3 \mid 21$. Portanto, $24F_{(16)}$ é divisível por 3. Por outro lado, sabemos que:

$$24F_{(16)} = 2 \cdot 16^2 + 4 \cdot 16^1 + 15 \cdot 16^0 = 512 + 64 + 15 = 591_{(10)}.$$

E, de fato, $3 \mid 591$.

Exemplo 5.10

Também como exemplo, vamos utilizar o critério para verificar a divisibilidade de $25D_{(16)}$ por 5, na base hexadecimal. Temos então que $a_2 + a_1 + a_0 = 2 + 5 + 13 = 20$ e $5 \mid 20$. Portanto, $25D_{(16)}$ é divisível por 5. Por outro lado, sabemos que:

$$25D_{(16)} = 2 \cdot 16^2 + 5 \cdot 16^1 + 13 \cdot 16^0 = 512 + 80 + 13 = 605_{(10)}.$$

E, de fato, $5 \mid 605$.

Exemplo 5.11

Agora, também como exemplo, vamos utilizar o critério para verificar que $1E2_{(16)}$ **não é divisível** por 3, na base hexadecimal. Temos então que $a_2 + a_1 + a_0 = 1 + 14 + 2 = 17$ e $3 \nmid 17$. Portanto, $1E2_{(16)}$ **não é divisível** por 3. Por outro lado, sabemos que:

$$1E2_{(16)} = 1 \cdot 16^2 + 14 \cdot 16^1 + 2 \cdot 16^0 = 256 + 224 + 2 = 482_{(10)}.$$

E, de fato, $3 \nmid 482$.

Exemplo 5.12

Por fim, como exemplo, vamos utilizar o critério para verificar que $1AA_{(16)}$ **não é divisível** por 5, na base hexadecimal. Temos então que $a_2 + a_1 + a_0 = 1 + 10 + 10 = 21$ e $5 \nmid 21$. Portanto, $1AA_{(16)}$ **não é divisível** por 5. Por outro lado, sabemos que:

$$1AA_{(16)} = 1 \cdot 16^2 + 10 \cdot 16^1 + 10 \cdot 16^0 = 256 + 160 + 10 = 426_{(10)}.$$

E, de fato, $5 \nmid 426$.

5.7.3 Divisibilidade por 7 na Base Hexadecimal

Teorema 5.3

Na base hexadecimal, um número é divisível por 7 se, e somente se, a soma dos números formados pelos seus algarismos, agrupados de três em três, da direita para a esquerda, for divisível por 7 (no sistema hexadecimal).

Demonstração. ($\Rightarrow$) Como nas demonstrações dos critérios anteriores, tomemos um número inteiro na base hexadecimal $a_{(16)}$, escrito na forma:

$$a_{(16)} = a_0 \cdot 16^0 + a_1 \cdot 16^1 + a_2 \cdot 16^2 + \cdots + a_n \cdot 16^n, \text{ com } n \in \mathbb{N}, a_i \in \{0, 1, 2, \ldots, 15\}.$$

Suponhamos que $a_{(16)}$ é divisível por 7 e, dessa forma, $a_{(16)} \equiv 0 \pmod 7$. Por outro lado, como $16^1 = 2^4$, $16^2 = 2^8$, $16^3 = 2^{12}$, $16^4 = 2^{16}$, e assim por diante, podemos nos basear num padrão de restos semelhantes ao da base binária:

$$\begin{aligned}
(2^4)^0 &\equiv 1 \pmod 7, \\
(2^4)^1 &\equiv 16 \equiv 2 \pmod 7, \\
(2^4)^2 &\equiv 256 \equiv 4 \pmod 7, \\
(2^4)^3 &\equiv 4.096 \equiv 1 \pmod 7, \\
(2^4)^4 &\equiv 65.536 \equiv 2 \pmod 7, \\
&\vdots
\end{aligned}$$

De forma geral, para considerar qualquer expoente inteiro, tomemos $k \in \mathbb{Z}$, daí:

$$\begin{aligned}
(2^4)^{3k} &\equiv 4096^k \equiv 1 \pmod 7, \\
(2^4)^{3k+1} &\equiv 4096^k \cdot 16^1 \equiv 2 \pmod 7, \\
(2^4)^{3k+2} &\equiv 4096^k \cdot 16^2 \equiv 4 \pmod 7.
\end{aligned}$$

Como $a_{(16)} = a_0 \cdot (2^4)^0 + a_1 \cdot (2^4)^1 + a_2 \cdot (2^4)^2 + \cdots + a_{3k} \cdot (2^4)^{3k} + a_{3k+1} \cdot (2^4)^{3k+1} + a_{3k+2} \cdot (2^4)^{3k+2}$, teremos:

$$\begin{aligned}
a_{(16)} &\equiv a_0 + 2a_1 + 4a_2 + \cdots + a_{3k} + 2a_{3k+1} + 4a_{3k+2} \pmod 7. \\
a_{(16)} &\equiv (a_0 + a_3 + \cdots + a_{3k}) + 2(a_1 + a_4 + \cdots + a_{3k+1}) + 4(a_2 + a_5 + \cdots + a_{3k+2}) \pmod 7.
\end{aligned}$$

Tomando $S_1 = (a_0 + a_3 + \cdots + a_{3k})$, $S_2 = (a_1 + a_4 + \cdots + a_{3k+1})$ e $S_3 = 4(a_2 + a_5 + \cdots + a_{3k+2})$:

$$a_{(16)} \equiv S_1 + 2S_2 + 4S_3 \equiv 0 \pmod 7.$$

Portanto, se $a_{(16)}$ é divisível por 7, então a soma $S_1 + 2^1 \cdot S_2 + 2^2 \cdot S_3$ também o é.

($\Leftarrow$) Agora, tomemos $a_{(16)}$ de forma que a soma dos números formados pelos seus bits, agrupados de três em três (da direita para a esquerda), seja divisível por 7, ou seja:

$$S_1 + 2^1 \cdot S_2 + 2^2 \cdot S_3 \equiv 0 \pmod 7.$$

Entretanto, $a_{(16)} = S_1 + 2S_2 + 4S_3$ e, portanto, $a_{(16)}$ também é divisível por 7. □

Exemplo 5.13

Por exemplo, vamos utilizar o critério para verificar que $12B4_{(16)}$ é divisível por 7, na base hexadecimal. Temos então que $a_5a_4a_3 + a_2a_1a_0 = 001 + 2B4 = 2B5_{(16)}$ e $7 \mid 2B5_{(16)} = 693_{(10)}$, pois $693 = 7 \cdot 99$. Portanto, $12B4_{(16)}$ é divisível por 7. Por outro lado, sabemos que:

$$12B4_{(16)} = 1 \cdot 16^3 + 2 \cdot 16^2 + 11 \cdot 16^1 + 4 \cdot 16^0 = 4096 + 512 + 176 + 4 = 4788_{(10)}.$$

E, de fato, $7 \mid 4788$, pois $4788 = 7 \cdot 684$ (Veja Exemplo 3.5).

Exemplo 5.14

Agora, também como exemplo, vamos utilizar o critério para verificar que $17C0_{(16)}$ **não é divisível** por 7, na base hexadecimal. Temos então que $a_5a_4a_3 + a_2a_1a_0 = 001 + 7C0 = 7C1_{(16)}$ e $7 \nmid 7C1_{(16)} = 1985_{(10)}$, pois $1985 = 7 \cdot 283 + 4$. Portanto, $17C0_{(16)}$ **não é divisível** por 7. Por outro lado, sabemos que:

$$17C0_{(16)} = 1 \cdot 16^3 + 7 \cdot 16^2 + 12 \cdot 16^1 + 0 \cdot 16^0 = 4096 + 1792 + 192 + 0 = 6080_{(10)}.$$

E, de fato, $7 \nmid 6080$, pois $6080 = 7 \cdot 868 + 4$ (Veja Exemplo 3.6).

É importante ressaltar a semelhança deste critério de divisibilidade do critério de divisibilidade por 7 na base binária, visto que $16 = 2^4$ e, dessa forma, o padrão de repetição dos restos é o mesmo.

5.7.4 Divisibilidade por 11 na Base Hexadecimal ($B_{(16)}$)

Inspirado no critério de divisibilidade por 7 na base decimal desenvolvido pelo nigeriano Chika Ofili, desenvolvemos este critério de divisibilidade por 11 na base hexadecimal.

Teorema 5.4

Na base hexadecimal, um número será divisível por 11 se, e somente se, ao multiplicarmos o algarismo das unidades por 9 e somarmos ao restante do número, o resultado for divisível por 11.

Demonstração. Tomemos um número inteiro $a_{(16)}$ divisível por $B_{(16)} = 11_{(10)}$, na forma:

$$a_{(16)} = a_0 \cdot 16^0 + a_1 \cdot 16^1 + a_2 \cdot 16^2 + \cdots + a_n \cdot 16^n, \text{ com } n \in \mathbb{N}, a_i \in \{0, 1, 2, \ldots, 15\}.$$

Tomaremos $k = (a_1 + a_2 \cdot 16^1 + \cdots + a_n \cdot 16^{n-1})$, daí:

$$a_{(16)} = a_0 + 16k.$$

Além disso, como $16k = 11k + 5k$:

$$a_{(16)} \equiv 11k + 5k + a_0 \equiv 5k + a_0 \pmod{11}.$$

Multiplicando ambos os lados por 9, obtemos:

$$9a_{(16)} \equiv 45k + 9a_0 \pmod{11}.$$

Temos ainda que $45 \equiv 1 \pmod{11}$ e, portanto, segue:

$$9a_{(16)} \equiv k + 9a_0 \pmod{11}.$$

Além disso, por hipótese, temos $a_{(16)} \equiv 0 \pmod{11}$. Logo, ao multiplicar ambos os lados da equivalência por 9, obtemos:

$$9a_{(16)} \equiv 9 \cdot 0 \equiv 0 \pmod{11}.$$

Por fim, por transitividade:

$$k + 9a_0 \equiv 0 \pmod{11}.$$

Ou seja, chegamos à conclusão que $a_{(16)}$ divisível por $B_{(16)} = 11_{(10)}$ se, e somente se $k + 9a_0$ também for divisível por $B_{(16)} = 11_{(10)}$. □

Exemplo 5.15

Vamos utilizar o critério para verificar que $25D_{(16)}$ é divisível por $B_{(16)} = 11_{(10)}$, na base hexadecimal. Temos então que $9a_0 + k = 9 \cdot D_{(16)} + 25_{(16)} = 75_{(16)} + 25_{(16)} = 9A_{(16)} = 154_{(10)}$.
Como $B_{(16)} \mid 9A_{(16)}$, concluímos que $25D_{(16)}$ é divisível por $B_{(16)}$. Entretanto, sabemos que:

$$25D_{(16)} = 2 \cdot 16^2 + 5 \cdot 16^1 + 13 \cdot 16^0 = 512 + 80 + 13 = 605_{(10)}.$$

E, de fato, $11 \mid 605$, pois $605 = 11 \cdot 55$.

Exemplo 5.16

Agora, também como exemplo, vamos utilizar o critério para verificar que $22B_{(16)}$ **não é divisível** por $B_{(16)} = 11_{(10)}$, na base hexadecimal. Temos então que $9a_0 + k = 9 \cdot B_{(16)} + 22_{(16)} = 63_{(16)} + 22_{(16)} = 85_{(16)} = 133_{(10)}$.

Como $B_{(16)} \nmid 85_{(16)}$, concluímos que $22B_{(16)}$ **não é divisível** por $B_{(16)}$. Entretanto, sabemos que:

$$22B_{(16)} = 2 \cdot 16^2 + 2 \cdot 16^1 + 11 \cdot 16^0 = 512 + 32 + 11 = 555_{10}.$$

E, de fato, $11 \nmid 555$.

5.7.5 Divisibilidade por 13 na Base Hexadecimal ($D_{(16)}$)

Após verificar o critério de divisibilidade por 7 na base binária, desenvolvemos este critério de divisibilidade por 13 na base hexadecimal, utilizando uma metodologia análoga.

Teorema 5.5

Na base hexadecimal, um número é divisível por 13 se, e somente se, a soma dos números formados pelos seus bits, agrupados de três em três (da direita para a esquerda), for divisível por 13 (no sistema hexadecimal).

Demonstração. ($\Rightarrow$) Como nas demonstrações dos critérios anteriores, tomemos um número inteiro na base hexadecimal $a_{(16)}$, escrito na forma:

$$a_{(16)} = a_0 \cdot 16^0 + a_1 \cdot 16^1 + a_2 \cdot 16^2 + \cdots + a_n \cdot 16^n, \text{ com } n \in \mathbb{N}, a_i \in \{0, 1, 2, \ldots, 15\}.$$

Suponhamos que $a_{(16)}$ é divisível por $D_{(16)} = 13_{(10)}$ e, dessa forma, $a_{(16)} \equiv 0 \pmod{13}$.

Podemos perceber um padrão nos restos das divisões das potências de 16 por 13:

$$\begin{aligned}
16^0 &\equiv 1 \pmod{13},\\
16^1 &\equiv 16 \equiv 3 \pmod{13},\\
16^2 &\equiv 256 \equiv 9 \pmod{13},\\
16^3 &\equiv 4.096 \equiv 1 \pmod{13},\\
16^4 &\equiv 65.536 \equiv 3 \pmod{13},\\
16^5 &\equiv 1.048.576 \equiv 9 \pmod{13},\\
&\vdots
\end{aligned}$$

De forma geral, para considerar qualquer expoente inteiro, tomemos $k \in \mathbb{Z}$, daí:

$$\begin{aligned} 16^{3k} &\equiv 4096^k \equiv 1 \pmod{13} \\ 16^{3k+1} &\equiv 4096^k \cdot 16^1 \equiv 3 \pmod{13} \\ 16^{3k+2} &\equiv 4096^k \cdot 16^2 \equiv 9 \pmod{13}. \end{aligned}$$

Como $a_{(16)} = a_0 \cdot 16^0 + a_1 \cdot 16^1 + a_2 \cdot 16^2 + \cdots + a_{3k} \cdot 16^{3k} + a_{3k+1} \cdot 16^{3k+1} + a_{3k+2} \cdot 16^{3k+2}$, teremos:

$$\begin{aligned} a_{(16)} &\equiv a_0 + 3a_1 + 9a_2 + \cdots + a_{3k} + 3a_{3k+1} + 9a_{3k+2} \pmod{13} \\ a_{(16)} &\equiv (a_0 + a_3 + \cdots + a_{3k}) + 3(a_1 + a_4 + \cdots + a_{3k+1}) + 9(a_2 + a_5 + \cdots + a_{3k+2}) \pmod{13}. \end{aligned}$$

Tomando $S_1 = (a_0 + a_3 + \cdots + a_{3k})$, $S_2 = (a_1 + a_4 + \cdots + a_{3k+1})$ e $S_3 = 4(a_2 + a_5 + \cdots + a_{3k+2})$:

$$a_{(16)} \equiv S_1 + 3S_2 + 9S_3 \equiv 0 \pmod{13}.$$

Portanto, se $a_{(16)}$ é divisível por 13, então a soma $S_1 + 3 \cdot S_2 + 9 \cdot S_3$ também o é.

($\Leftarrow$) Agora, tomemos $a_{(16)}$ de forma que a soma dos números formados pelos seus bits, agrupados de três em três (da direita para a esquerda), seja divisível por 13, ou seja:

$$S_1 + 3 \cdot S_2 + 9 \cdot S_3 \equiv 0 \pmod{13}.$$

Entretanto, $a_{(16)} = S_1 + 3S_2 + 9S_3$ e, portanto, $a_{(16)}$ também é divisível por 13. □

Exemplo 5.17

Por exemplo, vamos utilizar o critério para verificar que $19A5_{(16)}$ é divisível por $D_{(16)} = 13_{(10)}$, na base hexadecimal. Temos então que $a_5a_4a_3 + a_2a_1a_0 = 001_{(16)} + 9A5_{(16)} = 9A6_{(16)} = 2470_{(10)}$ e $D_{(16)} \mid 9A6_{(16)}$, ou seja, $13_{(10)} \mid 2470_{(10)}$, pois $2470 = 13 \cdot 190$.
Portanto, $19A5(16)$ é divisível por $D_{(16)} = 13_{(10)}$. Entretanto, sabemos que:

$$19A5_{(16)} = 1 \cdot 16^3 + 9 \cdot 16^2 + 10 \cdot 16^1 + 5 \cdot 16^0 = 4096 + 2304 + 160 + 5 = 6565_{(10)}.$$

E, de fato, $13 \mid 6565$, pois $6565 = 13 \cdot 505$.

Exemplo 5.18

Agora, também como exemplo, vamos utilizar o critério para verificar que $22C4_{(16)}$ **não é divisível** por 13, na base hexadecimal. Temos então que $a_5a_4a_3 + a_2a_1a_0 = 002 + 2C4 = 2C6$ e $D_{(16)} \nmid 2C6_{(16)}$, ou seja, $13_{(10)} \nmid 710_{(10)}$, pois $710 = 13 \cdot 54 + 8$. Portanto, $22C4_{(16)}$ **não é divisível** por 13. Entretanto, sabemos que:

$$22C4_{(16)} = 2 \cdot 16^3 + 2 \cdot 16^2 + 12 \cdot 16^1 + 4 \cdot 16^0 = 8192 + 512 + 192 + 4 = 8900_{(10)}.$$

E, de fato, $13 \nmid 8900$, pois $8900 = 13 \cdot 684 + 8$.

5.7.6 Divisibilidade por 17 na Base Hexadecimal ($11_{(16)}$)

Teorema 5.6

Na base hexadecimal, um número é divisível por 17 se, e somente se, a diferença entre a soma de seus bits nas posições pares e a soma de seus bits nas posições ímpares for divisível por 17.

Demonstração. ($\Rightarrow$) Seja um número inteiro na base hexadecimal $a_{(16)}$, escrito na forma:

$$a_{(16)} = a_0 \cdot 16^0 + a_1 \cdot 16^1 + a_2 \cdot 16^2 + \cdots + a_n \cdot 16^n, \text{ com } n \in \mathbb{N}, a_i \in \{0, 1, \ldots, 15\}.$$

Suponhamos que $a_{(16)}$ é divisível por $11_{(16)} = 17_{(10)}$, ou seja, $a_{(16)} \equiv 0 \pmod{17}$.

Podemos observar um padrão nos restos das divisões das potências de 16 por 17:

$$\begin{aligned}
16^0 &\equiv 1 \pmod{17}, \\
16^1 &\equiv -1 \pmod{17}, \\
16^2 &\equiv 1 \pmod{17}, \\
16^3 &\equiv -1 \pmod{17}, \\
16^4 &\equiv 1 \pmod{17}, \\
&\vdots
\end{aligned}$$

Observamos que as potências de 16 com expoente par são congruentes a $1 \pmod{17}$, enquanto as de expoente ímpar são congruentes a $-1 \pmod{17}$. Assim, podemos escrever:

$$a_{(16)} \equiv a_0 \cdot 1 + a_1 \cdot (-1) + a_2 \cdot 1 + a_3 \cdot (-1) + \cdots + a_{2k} \cdot 1 + a_{2k+1} \cdot (-1) \pmod{17}.$$

Colocando os termos comuns em evidência:

$$a_{(16)} \equiv 1 \cdot (a_0 + a_2 + a_4 + \cdots + a_{2k}) + (-1) \cdot (a_1 + a_3 + a_5 + \cdots + a_{2k+1}) \pmod{17}.$$

Definindo:

$$S_{2k} = a_0 + a_2 + a_4 + \cdots + a_{2k}, \quad S_{2k+1} = a_1 + a_3 + a_5 + \cdots + a_{2k+1},$$

temos:

$$a_{(16)} \equiv S_{2k} - S_{2k+1} \pmod{17}.$$

Como assumimos que $a_{(16)} \equiv 0 \pmod{17}$, então:

$$S_{2k} - S_{2k+1} \equiv 0 \pmod{17}.$$

Ou seja, se $a_{(16)}$ é divisível por $11_{(16)} = 17_{(10)}$, então a diferença entre a soma dos dígitos hexadecimais nas posições pares e a soma dos dígitos nas posições ímpares deve ser divisível por 17.

($\Leftarrow$) Agora, suponha que a diferença entre a soma dos dígitos nas posições pares e a soma dos dígitos nas posições ímpares seja divisível por 17. Ou seja:

$$S_{2k} - S_{2k+1} \equiv 0 \pmod{17}.$$

Como já mostramos que:

$$a_{(16)} \equiv S_{2k} - S_{2k+1} \pmod{17}.$$

segue-se que:

$$a_{(16)} \equiv 0 \pmod{17}$$

Ou seja, se a diferença entre a soma dos dígitos nas posições pares e a soma dos dígitos nas posições ímpares for divisível por $11_{(16)} = 17_{(10)}$, então o número $a_{(16)}$ também é divisível por $11_{(16)} = 17_{(10)}$. □

Exemplo 5.19

Por exemplo, vamos utilizar o critério para verificar que $1A6E_{(16)}$ é divisível por $11_{(16)} = 17_{(10)}$, na base hexadecimal. Temos então que $S_{2k} = a_2 + a_0 = A + E = 10 + 14 = 24$ e $S_{2k+1} = a_3 + a_1 = 1 + 6 = 7$. Daí, $S_{2k} - S_{2k+1} = 24 - 7 = 17$. Como $17 \mid 17$, temos que $1A6E_{(16)}$ é divisível por

$11_{(16)} = 17_{(10)}$. Por outro lado, sabemos que:

$$1A6E_{(16)} = 1 \cdot 16^3 + 10 \cdot 16^2 + 6 \cdot 16^1 + 14 \cdot 16^0 = 4096 + 2560 + 96 + 14 = 6766_{(10)}.$$

E, de fato, $17 \mid 6766$, pois $6766 = 17 \cdot 398$.

Exemplo 5.20

Agora, também como exemplo, vamos utilizar o critério para verificar que $1518_{(16)}$ **não é divisível** por $11_{(16)} = 17_{(10)}$, na base hexadecimal. Temos então que $S_{2k} = a_2 + a_0 = 5 + 8 = 13$ e $S_{2k+1} = a_3 + a_1 = 1 + 1 = 2$. Daí, $S_{2k} - S_{2k+1} = 13 - 2 = 11$. Como $17 \nmid 11$, temos que $1518_{(16)}$ **não é divisível** por $11_{(16)} = 17_{(10)}$. Por outro lado, sabemos que:

$$1518_{(16)} = 1 \cdot 16^3 + 5 \cdot 16^2 + 1 \cdot 16^1 + 8 \cdot 16^0 = 4096 + 1280 + 16 + 8 = 5400_{(10)}.$$

De fato, $17 \nmid 5400$, pois $5400 = 17 \cdot 317 + 11$.

Estes últimos critérios, por 11, por 13 e por 17, só existem, desta forma, na base hexadecimal, evidenciando que neste sistema de numeração, é mais simples verificar algumas divisibilidades.

CAPÍTULO 6

Critérios de Divisibilidade em Bases Genéricas

Para complementar este trabalho, traremos alguns critérios de divisibilidade para qualquer base numérica, visto que, assim como em Braga e Zini [2], a aritmética modular permite fazer essa análise para qualquer par de números inteiros e a facilidade ou dificuldade de um critério de divisibilidade de um número por outro está intimamente ligada à base numérica na qual esses números estão representados.

Neste capítulo, vamos verificar o que ocorre com os critérios de divisibilidade se mudarmos a base de representação de um número e, além disso, para quais bases numéricas temos critérios de divisibilidade mais simples de serem verificados. O objetivo é estender o raciocínio para uma base numérica k genérica e verificar o que é de fato geral e o que é intrínseco da base numérica escolhida.

Utilizaremos, para um melhor desenvolvimento das demonstrações, a notação $a_{(k)} = \sum_{i=0}^{q} a_i k^i$ para representar um número inteiro qualquer na base k.

6.1 Divisibilidade por uma base k

Um critério fundamental de divisibilidade em qualquer base numérica é a relação entre um número e sua base. Nesta proposição, analisamos a condição necessária para que um número escrito em uma base k seja divisível por k. Segue, baseado em Braga e Zini [2].

Proposição 6.1

Seja $a_{(k)} = \sum_{i=0}^{q} a_i k^i$, um número inteiro escrito em uma base numérica k. Então $a_{(k)}$ é divisível por k se, e somente se a_0 o for.

Demonstração. Como $a_{(k)} = \sum_{i=0}^{q} a_i k^i$, podemos rescrevê-lo na forma $a_{(k)} = a_0 + \sum_{i=1}^{q} a_i k^i$. Evidenciando o termo k, obtemos $a_{(k)} = a_0 + k\left(\sum_{i=1}^{q} a_i k^{i-1}\right)$. Portanto, $a_{(k)}$ será divisível por k somente quando a_0 o for. □

Nesta proposição, verificamos que um número será divisível pela base em que está escrito somente quando o algarismo das unidades também for. Entretanto, como $a_0 < k$, a única possibilidade em que temos a_0 divisível por k é quando $a_0 = 0$.

6.2 Divisibilidade por um divisor de k

Nesta proposição, exploramos a divisibilidade de um número escrito em uma base k por um divisor m dessa base. Mostraremos que, se m é um fator inteiro de k, a divisibilidade de um número $a_{(k)}$ por m depende exclusivamente do algarismo das unidades.

Proposição 6.2

Seja $a_{(k)} = \sum_{i=0}^{q} a_i k^i$, um número inteiro escrito em uma base k. Considere m um divisor inteiro de k, ou seja, $m = \frac{k}{p}$, com $p \in \mathbb{Z}$. Então $a_{(k)}$ é divisível por m se, e somente se a_0 o for.

Demonstração. Temos que $m = \frac{k}{p}$, então $k = mp$ e, portanto, $a_{(k)} = \sum_{i=0}^{q} a_i (mp)^i$. Assim, obtemos:

$$a_{(k)} = a_0 + \sum_{i=1}^{q} a_i m^i p^i$$

Evidenciando m, teremos $a_{(k)} = a_0 + m\left(\sum_{i=1}^{q} a_i m^{i-1} p^i\right)$ e então, $a_{(k)}$ será divisível por m se, e somente se quando a_0 o for. □

Observe que nesta proposição generalizamos o critério de divisibilidade para os divisores de k, visto que a escolha de p não pode ser arbitrária, pois m é inteiro. Além disso, quando $p = 1$ obtemos o critério de divisibilidade por k.

6.3 Divisibilidade por um divisor do antecessor de k

A seguir, nessa proposição, desenvolveremos um critério de divisibilidade para quaisquer que sejam os divisores do **antecessor** de uma base k, ou seja, do número imediatamente anterior a k, representado por $k-1$.

Proposição 6.3

Seja $a_{(k)} = \sum_{i=0}^{q} a_i k^i$, um número inteiro escrito em uma base k. Considere r um divisor inteiro de $k-1$, ou seja, $r = \dfrac{k-1}{n}$, com $n \in \mathbb{N}$. Então $r \mid a_{(k)}$ se, e somente se, $r \mid \sum_{i=0}^{q} a_i$.

Demonstração. ($\Rightarrow$) Tomemos $a_{(k)} \equiv 0 \pmod{r}$. Como $r = \dfrac{k-1}{n}$ temos, então, que $k = nr + 1$. Logo $k \equiv 1 \pmod{r}$ e, daí:

$$k^i \equiv 1^i \equiv 1 \pmod{r}.$$

Portanto, como $a_{(k)} = \sum_{i=0}^{q} a_i k^i$, obtemos:

$$a_{(k)} \equiv \sum_{i=0}^{q} a_i \cdot 1 \equiv \sum_{i=0}^{q} a_i \pmod{r}.$$

Dessa forma, se $r \mid a_{(k)}$ então $r \mid \sum_{i=0}^{q} a_i$.

($\Leftarrow$) Reciprocamente, se $\sum_{i=0}^{q} a_i \equiv 0 \pmod{r}$ e $k^i \equiv 1^i \equiv 1 \pmod{r}$, então:

$$a_{(k)} \equiv \sum_{i=0}^{q} a_i k^i \equiv 0 \cdot 1 \equiv 0 \pmod{r}.$$

Ou seja, concluímos que $r \mid a_{(k)}$. □

Note que os critérios de divisibilidade por 3 e 9 na base decimal são análogos aos critérios por 3, 5 e 15 na base hexadecimal, por exemplo (veja os Teoremas 3.4 e 5.2).

6.4 Divisibilidade por um divisor do sucessor de k

Agora, nessa proposição, desenvolveremos um critério de divisibilidade para quaisquer que sejam os divisores do **sucessor** de uma base k, ou seja, do número imediatamente posterior a k, representado por $k+1$.

Proposição 6.4

Seja $a_{(k)} = \sum_{i=0}^{q} a_i k^i$, um número inteiro escrito em uma base k. Considere t um divisor inteiro de $k+1$, ou seja, $t = \dfrac{k+1}{n}$, com $n \in \mathbb{N}$. Então $t \mid a_{(k)}$ se, e somente se, $t \mid \sum_{i=0}^{q} a_i(-1)^i$.

Demonstração. ($\Rightarrow$) Tomemos $a_{(k)} \equiv 0 \pmod{t}$. Como $t = \dfrac{k+1}{n}$ temos, então, que $k = tn-1$. Logo $k \equiv -1 \pmod{t}$ e, daí:

$$k^i \equiv (-1)^i \pmod{t}.$$

Portanto, como $a_{(k)} = \sum_{i=0}^{q} a_i k^i$, obtemos:

$$a_{(k)} \equiv \sum_{i=0}^{q} a_i(-1)^i \pmod{t}.$$

Dessa forma, se $t \mid a_{(k)}$ então $t \mid \sum_{i=0}^{q} a_i(-1)^i \pmod{t}$.

($\Leftarrow$) Reciprocamente, se $\sum_{i=0}^{q} a_i(-1)^i \equiv 0 \pmod{t}$, e $(-1)^i \equiv k^i \pmod{t}$ então:

$$a_{(k)} \equiv \sum_{i=0}^{q} a_i k^i \equiv 0 \pmod{t}.$$

Ou seja, concluímos que $t \mid a_{(k)}$. □

Note que, por exemplo, os critérios de divisibilidade por 11 na base decimal, 3 na base binária e 17 na base hexadecimal são análogos, pois ambos são sucessores de 10, 2, e 16, respectivamente. Além disso, se observamos uma base octal por exemplo, ou seja, com $k = 8$, este critério se aplicaria ao 9 e 3.

6.5 Divisibilidade por um divisor de k^p

Por fim, traremos uma proposição que trata da divisibilidade dos divisores de uma potência de base k.

Proposição 6.5

Seja $a_{(k)} = \sum_{i=0}^{q} a_i k^i$, um número inteiro escrito em uma base k. Agora, tome $u \in \mathbb{N}$, tal que $u \mid k^p$, com $p \in \mathbb{N}$. Então $a_{(k)}$ será divisível por u, se u dividir o número formado pelos dois p últimos dígitos de $a_{(k)}$.

Demonstração. Tomemos $u \in \mathbb{N}$, tal que $u \mid k^p$, com $p \in \mathbb{N}$ e $a_{(k)} = \sum_{i=0}^{q} a_i k^i$. Podemos escrever $a_{(k)}$ em duas parcelas:

$$a_{(k)} = \underbrace{\sum_{i=0}^{p-1} a_i k^i}_{\text{Últimos } p \text{ algarismos}} + \underbrace{\sum_{i=p}^{q} a_i k^i}_{\text{Algarismos restantes}} .$$

Por outro lado, podemos colocar k^p em evidência nos algarismos restantes:

$$a_{(k)} = \sum_{i=0}^{p-1} a_i k^i + k^p \left(\sum_{i=p}^{q} a_i k^{i-p} \right).$$

Como $u \mid k^p$, então u divide $a_{(k)}$ se também dividir $\sum_{i=0}^{p-1} a_i k^i$. □

Observação: vale o destaque de que, ao trabalhar com os critérios de divisibilidade na base decimal para alunos do 6° ano do Ensino Fundamental, trabalhamos os critérios de divisibilidade por 4, em que um número é divisível por 4 se, e somente se, os dois últimos algarismos formarem um número divisível por 4, e por 8, em que um número é divisível por 8 se, e somente se, os três últimos algarismos formarem um número divisível por 8. Agora, graças à proposição acima, como $4 \mid 100 = 10^2$ e $8 \mid 1000 = 10^3$, entendemos estes critérios que trabalhamos na escola.

Ao final desse capítulo, observamos que a facilidade da aplicação de um critério de divisibilidade por um número é maior ou menor dependendo da base escolhida. Por exemplo, na base decimal é mais difícil utilizar um critério de divisibilidade por 7 do que na base octal. Critérios de divisibilidade, como afirmam Braga e Zini [2], dependem essencialmente da base numérica escolhida.

CAPÍTULO 7

Produto Técnico-Tecnológico: Minicurso

Informações Gerais

- **Título do Minicurso:** Decifrando os Códigos do Mundo Digital: Aritmética nas Bases Binária e Hexadecimal
- **Público-alvo:** Professores da Educação Básica, Licenciandos em Matemática, Graduandos da Computação e Alunos do Ensino Médio
- **Carga horária:** 4 horas
- **Datas de realização:** 23 e 24 de Abril de 2025
- **Local:** Auditória 5R-A da Universidade Federal de Uberlândia
- **Ministrante:** Fidélio Augustus Souki Gontijo
- **Material utilizado:** Projetor, notebook, cadernos, caneta, quadro branco e pincéis
- **Conhecimento prévio:** As quatro operações no sistema decimal, decomposição de um número na base decimal

Descrição

Como parte da aplicação prática dos resultados obtidos nesta pesquisa, foi elaborado e ministrado um minicurso intitulado "*Decifrando os Códigos do Mundo Digital: Aritmética nas Bases Binária e Hexadecimal*" no auditório 5R-A, no campus Santa Mônica da Universidade Federal de Uberlândia, para alunos no início do curso de Licenciatura em Matemática, ou interessados na temática. O minicurso teve como objetivos:

- Introduzir conceitos fundamentais de sistemas numéricos posicionais e não posicionais
- Demonstrar técnicas de conversão entre bases (decimal, binária, hexadecimal)
- Explorar operações aritméticas em binário e hexadecimal
- Apresentar aplicações tecnológicas na computação, programação e eletrônica digital

Principais Tópicos Abordados

1. História e evolução dos sistemas numéricos (egípcio, romano, maia, babilônico, hindu-arábico);
2. Diferença entre sistemas posicionais e não posicionais;
3. Conversão entre bases:
   - Método das divisões sucessivas;
   - Tabelas comparativas (0 a 63 em decimal, binário e hexadecimal);
4. Operações matemáticas em binário e hexadecimal:
   - Adição, subtração, multiplicação e divisão;
   - Atividades passadas para os presentes;
5. Aplicações na tecnologia:
   - Armazenamento e transmissão de dados

     Binário: Todo dado digital (texto, imagem, vídeo, som) é convertido em sequências de 0s e 1s, porque os computadores funcionam com circuitos eletrônicos que só reconhecem dois estados: ligado (1) e desligado (0). Exemplo: A letra “A” - 01000001 em código binário

     Hexadecimal: Como as sequências binárias são longas e difíceis de ler, os dados muitas vezes são representados em hexadecimal para facilitar a visualização. Cada dígito hexadecimal representa 4 bits. Exemplo: o byte 11110000 = F0 em hexadecimal.
   - Endereçamento de memória e depuração

Binário: Os endereços de memória são representados internamente em binário, pois a arquitetura do processador opera diretamente com bits. Exemplo: 0000111110101000 (endereço binário real).

Hexadecimal: Para os programadores, é muito mais fácil ler e escrever os endereços em hexadecimal. O endereço binário acima pode ser representado como 0x0FA8. O prefixo 0x indica "número hexadecimal".

- Representação de cores em HTML/CSS;

  Binário: Cada cor RGB (no inglês: vermelho, verde, azul) pode ser representada com 8 bits. Exemplo: vermelho puro: 11111111 00000000 00000000 (255, 0, 0).

  Hexadecimal: Como é padrão na web, essa cor seria escrita como FF0000. Cada par hexadecimal representa uma das cores (R, G, B). O vermelho puro representado em hexadecimal: FF = 255 (vermelho); 00 = 0 (verde); 00 = 0 (azul)

Materiais Disponibilizados

- Slides didáticos com exemplos e exercícios;
- Tabelas de conversão (decimal-binário-hexadecimal);
- Roteiro de atividades práticas;

Registro da Atividade

Fotografias de atividades realizadas:

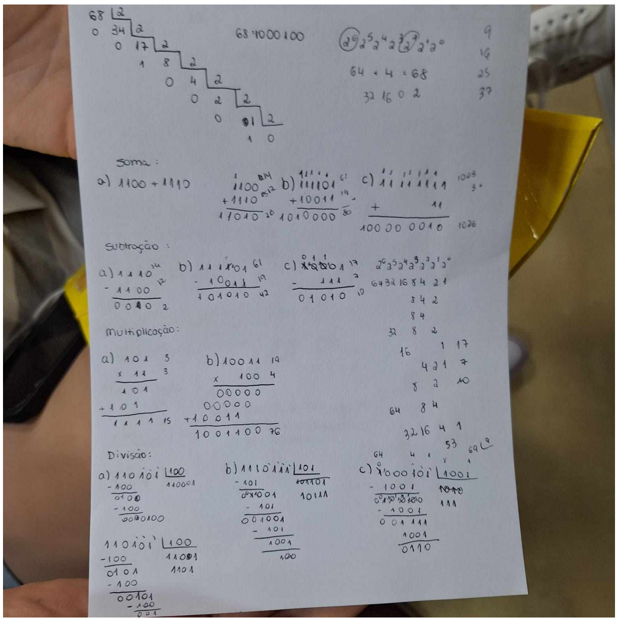


Figura 7.1: Registro de atividades em caderno de participante 1

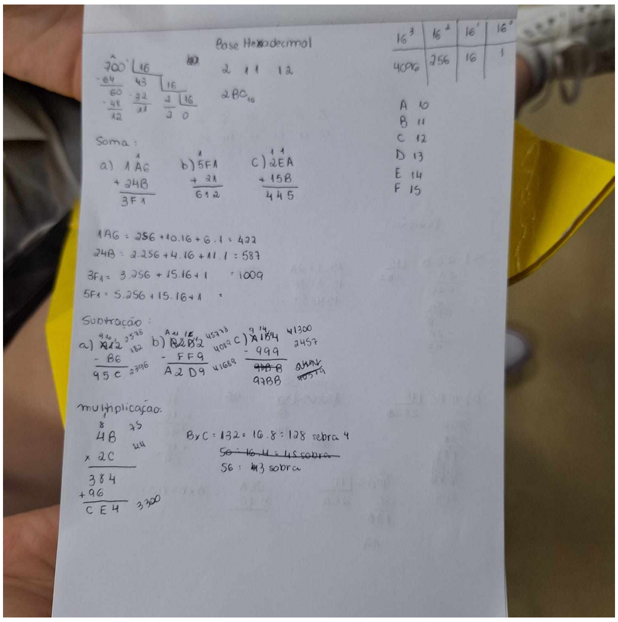


Figura 7.2: Registro de atividades em caderno de participante 2

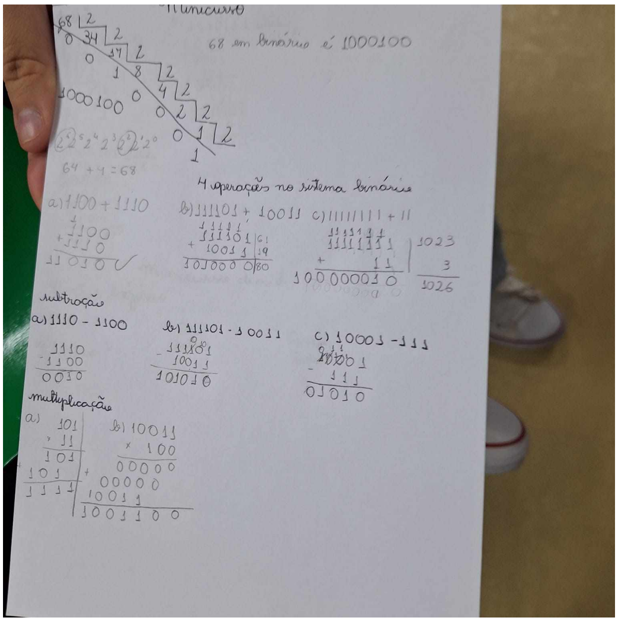


Figura 7.3: Registro de atividades em caderno de participante 3

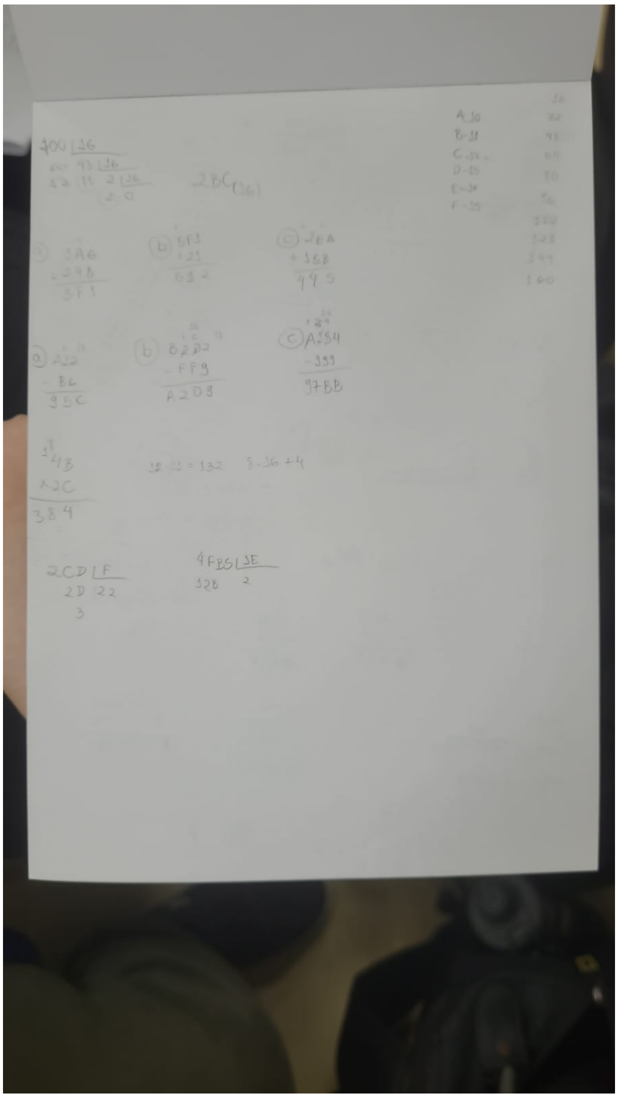


Figura 7.4: Registro de atividades em caderno de participante 4

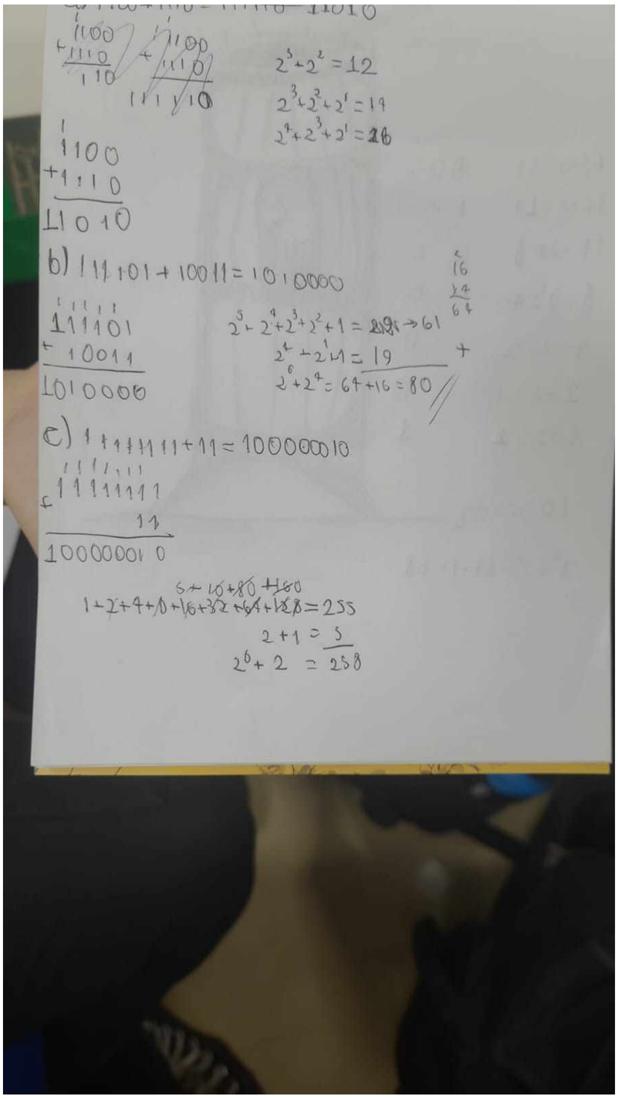


Figura 7.5: Registro de atividades em caderno de participante 5

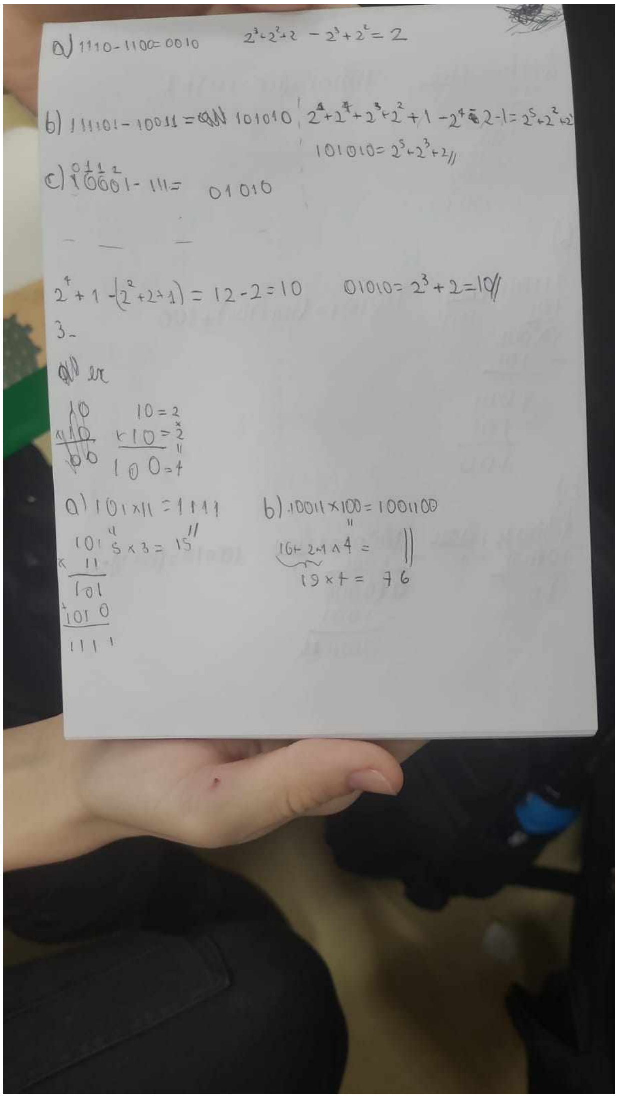


Figura 7.6: Registro de atividades em caderno de participante 6

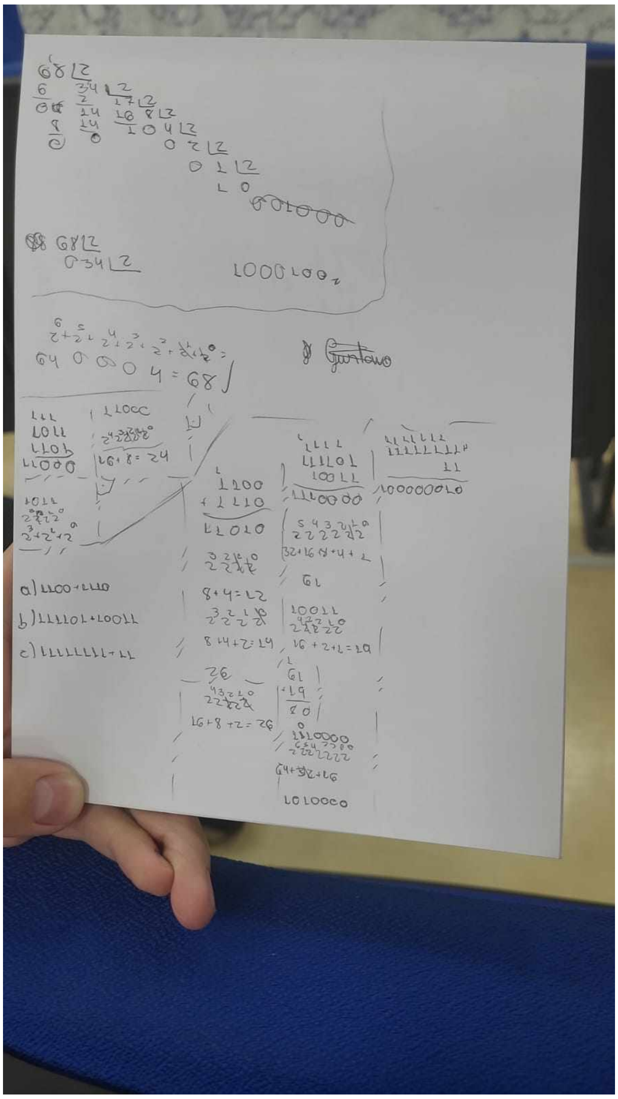


Figura 7.7: Registro de atividades em caderno de participante 7

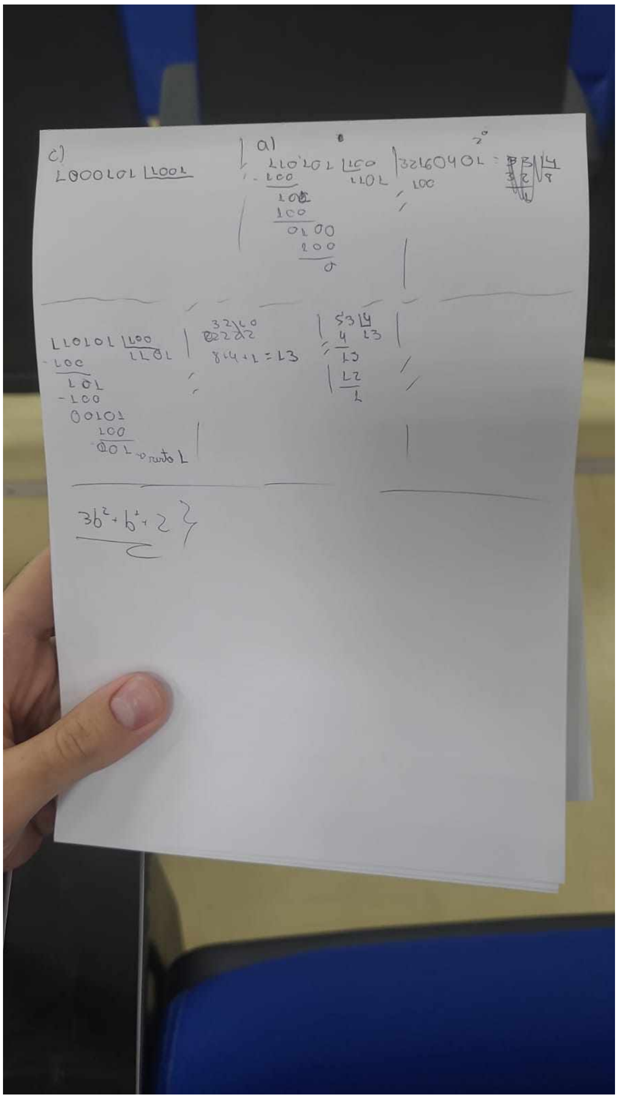


Figura 7.8: Registro de atividades em caderno de participante 8

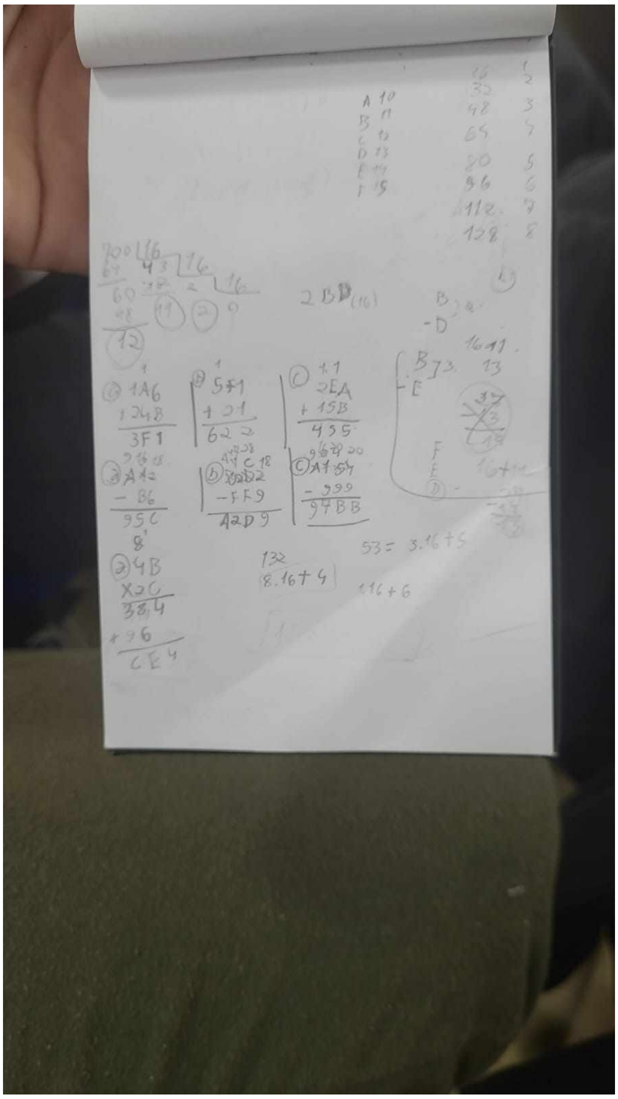


Figura 7.9: Registro de atividades em caderno de participante 9

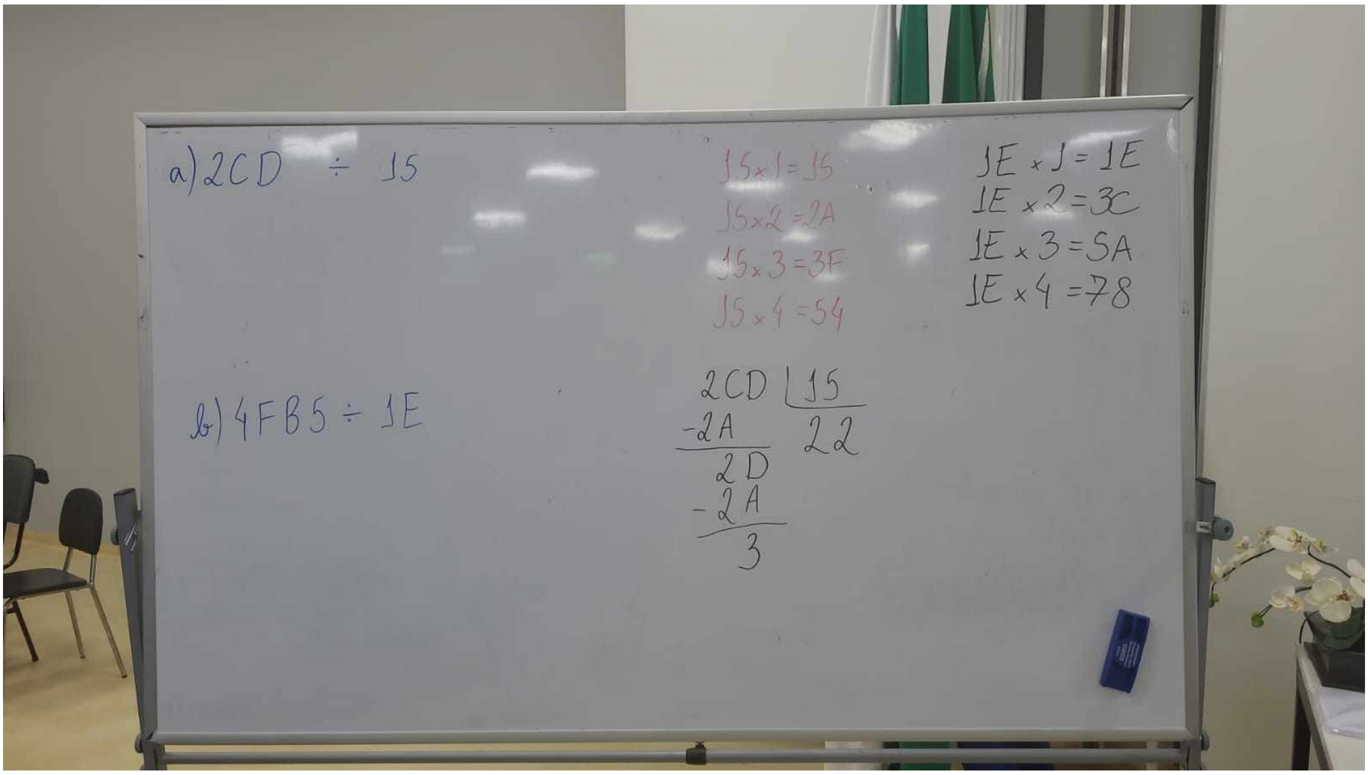


Figura 7.10: Registro de atividades em lousa

Alguns dos principais slides:

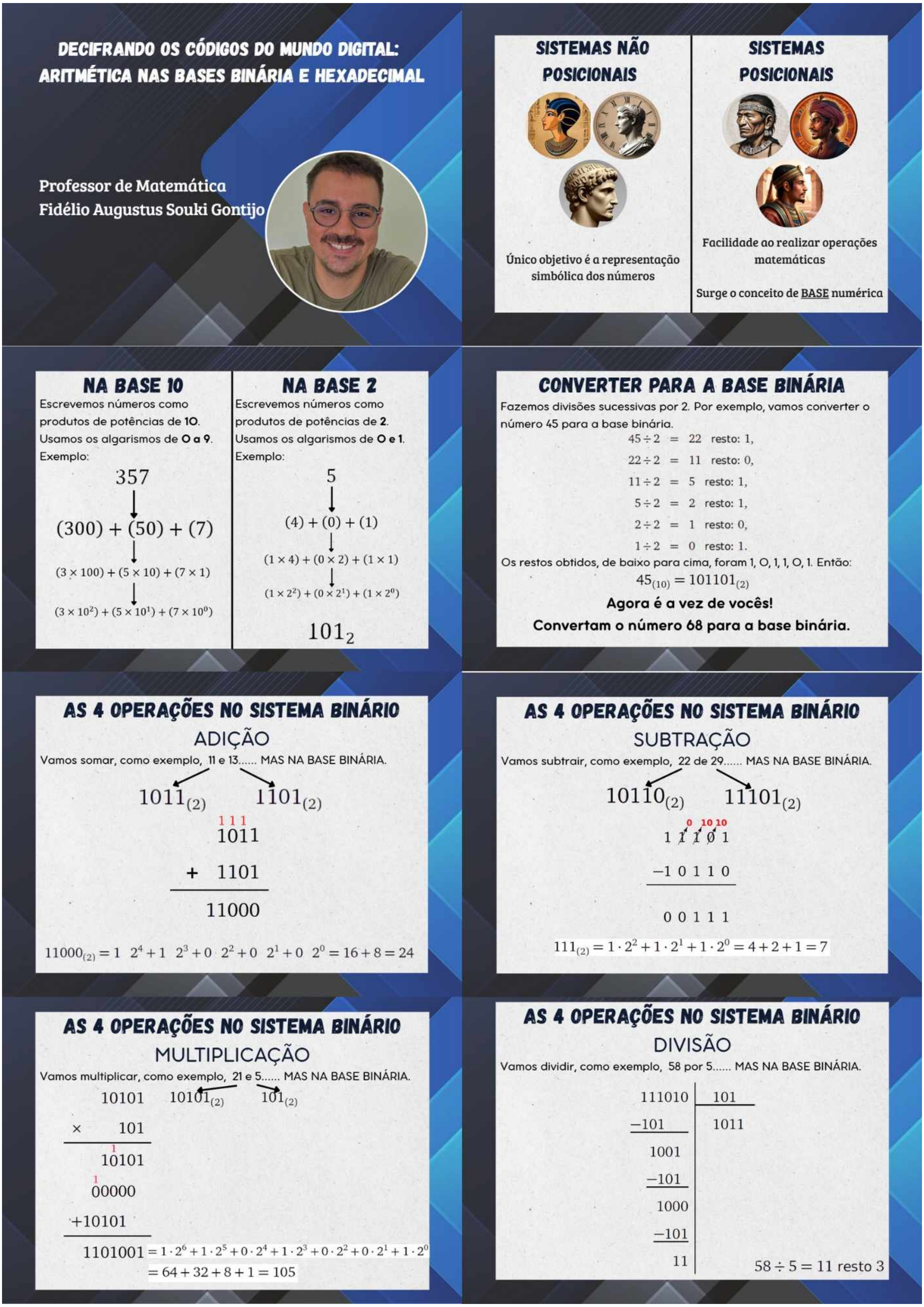


Figura 7.11: Slide do minicurso – parte 1

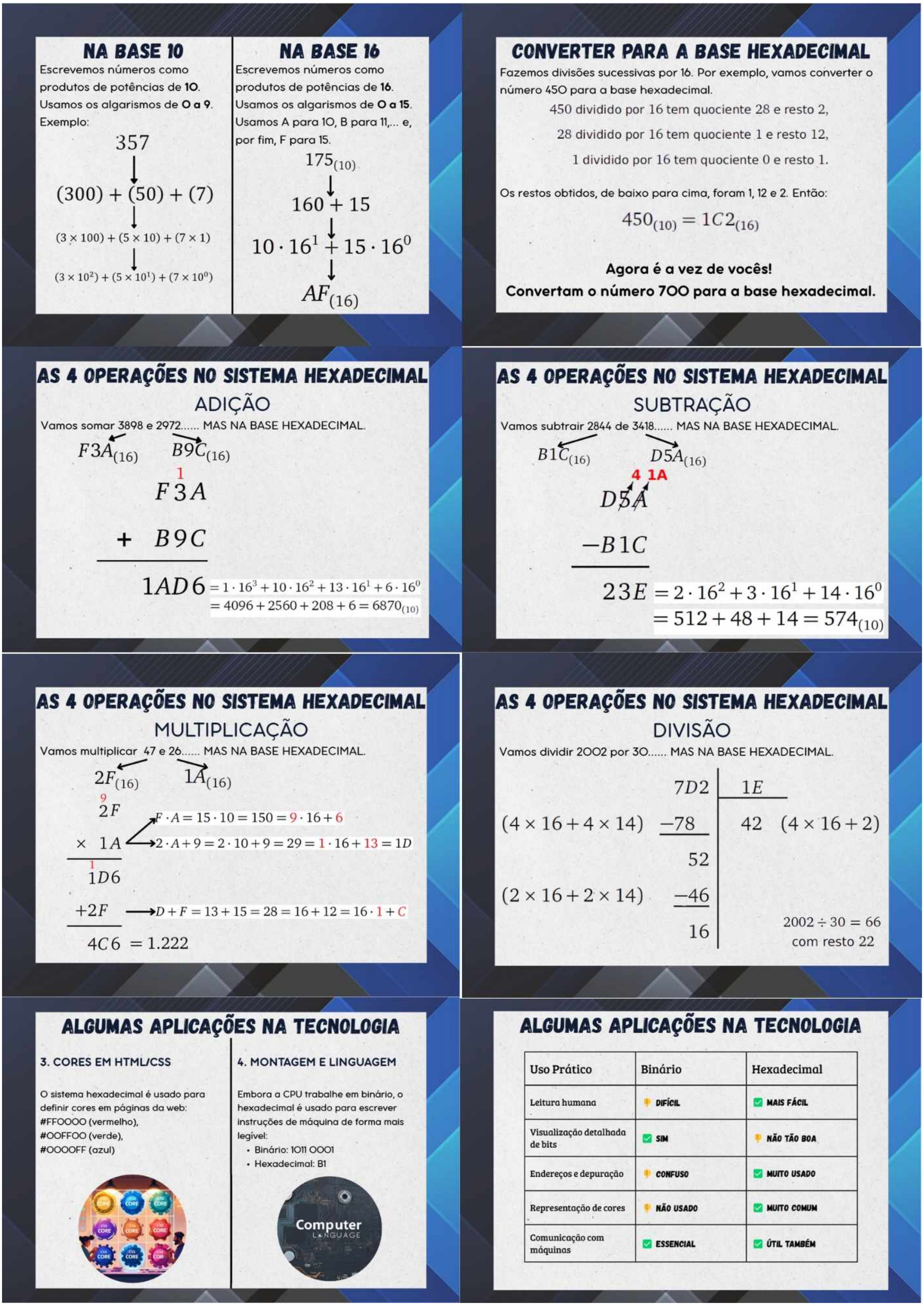


Figura 7.12: Slide do minicurso – parte 2

Conexão com a Pesquisa

Este minicurso representa uma ação de extensão e validação prática dos conhecimentos produzidos na pesquisa, destacando:

Continuidade Teórico-Metodológica

O minicurso opera como extensão didática da pesquisa, traduzindo seus fundamentos teóricos para uma abordagem acessível. Enquanto a dissertação demonstra formalmente critérios de divisibilidade através de Aritmética modular, Sistemas posicionais e Operações em diferentes bases numéricas, o minicurso introduz esses conceitos de forma intuitiva, com ênfase nas bases binária e hexadecimal.

Aplicação Pedagógica

A dissertação propõe sequências didáticas para o ensino de divisibilidade, materializadas no minicurso através de:

Tabela 7.1: Correspondência entre dissertação e minicurso

Dissertação	**Minicurso**
Critérios formais de divisibilidade	Fundamentos de sistemas posicionais
Operações em bases arbitrárias	Aritmética binária e hexadecimal
Aplicações teóricas	Exemplos tecnológicos práticos

Configura-se como um produto técnico-tecnológico relevante para programas de pós-graduação profissional, promovendo a integração entre academia e educação básica.

CAPÍTULO 8

Considerações Finais

Ao elaborar este trabalho, nosso objetivo principal era investigar os critérios de divisibilidade em diferentes bases numéricas, com ênfase nos sistemas decimal, binário e hexadecimal. No entanto, ao longo da pesquisa, ficou evidente que, embora os princípios fundamentais da divisibilidade sejam universais, sua aplicação prática varia significativamente conforme a base adotada. Os critérios de divisibilidade, baseados em propriedades algébricas e aritméticas, independem da representação numérica, mas sua formulação e uso tornam-se mais ou menos simples dependendo da base utilizada. Em particular, nas bases binária e hexadecimal, alguns critérios assumem formas mais compactas e eficientes, o que reforça sua utilidade em aplicações computacionais.

No âmbito educacional, os critérios desenvolvidos podem ser adaptados ao ensino básico, auxiliando na compreensão de conceitos fundamentais da aritmética. O minicurso apresentado neste trabalho, voltado para as quatro operações básicas nas bases binária e hexadecimal, contextualiza historicamente as bases posicionais e não posicionais, e proporciona a experiência de revisitar conteúdos da educação infantil sob uma nova perspectiva, mais madura e atenta aos métodos de resolução em cada operação, destacando os detalhes específicos de cada base.

Em síntese, reforçamos a importância de se estudar a teoria dos números em diferentes contextos, evidenciando como a escolha da base numérica influencia a eficiência e clareza dos critérios de divisibilidade. Também destacamos que o tema abre caminho para novas investigações, tanto no campo matemático quanto em aplicações tecnológicas e pedagógicas. Acreditamos que a abordagem proposta pode servir como base para futuras pesquisas e como ferramenta de ensino, promovendo uma compreensão mais profunda e interdisciplinar da matemática. Além disso, o minicurso permitiu aos futuros professores revisar e compreender melhor os algoritmos ensinados nas operações básicas dos anos iniciais da formação escolar.

Referências Bibliográficas

[1] BEZERRA, Nazaré. ***Teoria dos Números: Um Curso Introdutório***. 1ª ed. Vol. 1. AEDI/UFPA, 2018 (citado nas páginas 15–18).

[2] BRAGA, Clezio A. e ZINI, Jhoni Marcelo. ***Criterios de divisibilidade em bases numéricas genéricas***. URL: https://projetos.unioeste.br/cursos/cascavel/matematica/xxivsam/artigos/63.pdf (acesso em 29/09/2024) (citado nas páginas 72, 76).

[3] CHAVES, Ana Paula e PORTO, Thiago. "**O Rei Maligno e a Princesa Generosa: Sobre bases numéricas e critérios de divisibilidade**". Em: ***Revista da Olimpíada de Matemática do Estado de Goiás*** (2014) (citado na página 26).

[4] FIBONACCI, Leonardo. ***Liber Abaci***. 2002ª ed. Vol. 1. Obra histórica seminal sobre aritmética e álgebra, escrita em latim. Springer, 2003 (citado na página 13).

[5] IEZZI, Gelson et al. ***Álgebra Moderna: Volume 1***. 1ª ed. Vol. 1. Atual Editora, 2002 (citado na página 20).

[6] MIYASCHITA, Wagner Yuwamamoto. ***Sistemas de Numeração: Como Funcionam e Como São Estruturados os Números***. Monografia de Graduação em Licenciatura Plena em Matemática. 2002 (citado nas páginas 3, 4, 7, 9, 10, 13).

[7] RODRIGUES, Renato. "**Aplicações da Teoria dos Números na Educação Básica com Enfoque em Divisibilidade e na Aritmética dos Restos**". Dissertação de Mestrado. Universidade Federal de Uberlândia, 2024 (citado nas páginas 2, 20).

[8] ROQUE, Tatiana e PITOMBEIRA, João Bosco. ***Tópicos de História da Matemática***. 1ª ed. Vol. 1. SBM, 2012 (citado nas páginas 1, 3, 5, 6, 8, 9, 12, 13).

[9] SILVA, Talysson Paulo da. "**Critérios de divisibilidade: usuais, incomuns e curiosos**". Dissertação de Mestrado. Universidade Federal da Paraíba - UFPB, 2019 (citado na página 26).

[10] ***Sistemas de Numeração em Eletrônica Digital***. CEFET-SC. 2024 (citado nas páginas 1, 34, 51).