

UNIVERSIDADE DE SÃO PAULO

Instituto de Ciências Matemáticas e de Computação

Algoritmos da aritmética básica e cálculo mental

Daniela Naves de Souza

Dissertação de Mestrado do Programa de Mestrado Profissional em
Matemática em Rede Nacional (PROFMAT)

SERVIÇO DE PÓS-GRADUAÇÃO DO ICMC-USP

Data de Depósito:

Assinatura: _____

Daniela Naves de Souza

Algoritmos da aritmética básica e cálculo mental

Dissertação apresentada ao Instituto de Ciências Matemáticas e de Computação – ICMC-USP, como parte dos requisitos para obtenção do título de Mestra em Ciências – Mestrado Profissional em Matemática em Rede Nacional. *VERSÃO REVISADA*

Área de Concentração: Mestrado Profissional em Matemática em Rede Nacional

Orientador: Prof. Dr. Alexandre Casassola Gonçalves

USP – São Carlos
Agosto de 2025

Ficha catalográfica elaborada pela Biblioteca Prof. Achille Bassi
e Seção Técnica de Informática, ICMC/USP,
com os dados inseridos pelo(a) autor(a)

S729a Souza, Daniela Naves de
Algoritmos da aritmética básica e cálculo mental
/ Daniela Naves de Souza; orientador Alexandre
Casassola Gonçalves. -- São Carlos, 2025.
82 p.

Dissertação (Mestrado - Programa de Pós-Graduação
em Mestrado Profissional em Matemática em Rede
Nacional) -- Instituto de Ciências Matemáticas e de
Computação, Universidade de São Paulo, 2025.

1. Algoritmos da aritmética. 2. Sistemas de
numeração. 3. Bases numéricas. 4. Operações
matemáticas. 5. Raiz quadrada. I. Gonçalves,
Alexandre Casassola, orient. II. Título.

Daniela Naves de Souza

Basic arithmetic and mental calculation algorithms

Master dissertation submitted to the Institute of Mathematics and Computer Sciences – ICMC-USP, in partial fulfillment of the requirements for the degree of Mathematics Professional Master's Program. *FINAL VERSION*

Concentration Area: Professional Master Degree Program in Mathematics in National Network

Advisor: Prof. Dr. Alexandre Casassola Gonçalves

USP – São Carlos
August 2025

*Este trabalho é dedicado às crianças que sonham com um futuro melhor e que não desistem
mesmo diante dos desafios,
e aos professores que transformam vidas todos os dias acreditando que o conhecimento é a
chave para mudar o mundo.*

AGRADECIMENTOS

Os meus agradecimentos vão, primeiramente, a Deus pela vida abençoada e por nunca me desamparar. Minha vida sempre foi e sempre será dele.

Agradeço também aos meus pais, Aduino e Rosângela, que não tiveram as mesmas oportunidades que eu, que não puderam concluir seus estudos, mas que lutaram incansavelmente para que eu pudesse ter um futuro diferente. Obrigada por serem meu chão e por tudo que fazem por mim.

Agradeço ainda à minha professora de matemática do ensino fundamental e médio, Mariza, que despertou em mim a paixão por essa área, me ensinou com maestria e sempre reconheceu o quanto eu era capaz.

Agradeço também aos diversos professores que tive ao longo da minha trajetória, nas graduações que cursei, e, em especial, aos professores do ICMC, que contribuíram para o meu aprendizado. Um agradecimento especial ao meu orientador, Professor Dr. Alexandre Casassola, que, com muita paciência, me ajudou a concluir esse sonho.

Gostaria de expressar minha gratidão à Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) pelo indispensável apoio financeiro e institucional que possibilitou a realização desta pesquisa.

Sou grata às várias pessoas que passaram pela minha vida até aqui e que contribuíram para que eu me tornasse a pessoa que sou hoje, ajudando tanto na minha formação acadêmica quanto na minha formação como ser humano. Ter apoio, incentivo e saber que não estamos sozinhos no mundo é essencial para seguir em frente.

Meus sinceros agradecimentos a todos que contribuíram direta ou indiretamente.

“A educação é a arma mais poderosa que você pode usar para mudar o mundo.”
(Nelson Mandela)

RESUMO

SOUZA, D. N. **Algoritmos da aritmética básica e cálculo mental**. 2025. 82 p. Dissertação (Mestrado em Ciências – Mestrado Profissional em Matemática em Rede Nacional) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos – SP, 2025.

Este é um projeto que busca compreender os algoritmos essenciais das operações aritméticas básicas: soma, subtração, multiplicação e divisão, com ênfase na demonstração da sua eficácia. Trabalhando na base arbitrária b , iremos recompor esses algoritmos, justificando sua validade. Em paralelo, discutiremos, para efeitos pedagógicos, a importância do cálculo mental simples, no que diz respeito à tabuada e a algumas operações mentais que otimizam os algoritmos acima, normalmente desenvolvidos com a escrita manual. Em sequência também será apresentado e demonstrado um outro algoritmo, bem menos conhecido, do cálculo da “raiz quadrada” de um número.

Palavras-chave: Algoritmos da aritmética, Raiz quadrada, Operações matemáticas, Sistemas de numeração, Bases numéricas.

ABSTRACT

SOUZA, D. N. **Basic arithmetic and mental calculation algorithms**. 2025. 82 p. Dissertação (Mestrado em Ciências – Mestrado Profissional em Matemática em Rede Nacional) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos – SP, 2025.

This project aims to understand the essential algorithms of basic arithmetic operations: addition, subtraction, multiplication, and division, with an emphasis on demonstrating their effectiveness. Working in an arbitrary base b , we will reconstruct these algorithms, justifying their validity. In parallel, for pedagogical purposes, we will discuss the importance of simple mental calculations, particularly regarding the multiplication table and certain mental operations that optimize the above algorithms, which are typically performed through handwriting. Additionally, another, much less known, algorithm for calculating the square root of a number will be presented and demonstrated.

Keywords: Arithmetic algorithms, Square root, Mathematical operations, Number systems, Number bases.

LISTA DE ILUSTRAÇÕES

Figura 1 – Sistema de numeração romano	23
Figura 2 – Sistema de numeração egípcio	24
Figura 3 – Sistema de numeração maia	25
Figura 4 – Sistema de numeração sumério	26

SUMÁRIO

1	INTRODUÇÃO	19
2	O SURGIMENTO DOS NÚMEROS	21
3	BASES NUMÉRICAS	27
3.1	Base decimal	27
3.2	Base arbitrária	29
3.3	Conversão Entre Bases	35
4	ADIÇÃO E SUBTRAÇÃO	37
4.1	Adição	37
4.1.1	<i>Algoritmo da Adição</i>	38
4.2	Subtração	46
4.2.1	<i>Algoritmo da Subtração</i>	46
5	MULTIPLICAÇÃO E DIVISÃO	53
5.1	Multiplicação	53
5.1.1	<i>Algoritmo da Multiplicação</i>	54
5.2	Divisão	61
5.2.1	<i>Algoritmo da Divisão</i>	61
6	RAIZ QUADRADA	69
6.1	Algoritmo da Raiz Quadrada	71
7	CONCLUSÃO	79
8	REFERÊNCIAS	81

INTRODUÇÃO

A Matemática é uma das disciplinas de extrema importância dentro do âmbito escolar e essencial para diversas situações da vida, contribuindo para o desenvolvimento lógico, para resolução de problemas do cotidiano e colaborando para o desenvolvimento de outras ciências como a tecnologia e a economia. As operações básicas, como adição, subtração, multiplicação e divisão, são a base para a construção de conteúdos e habilidades mais profundas da Matemática. Porém, muitos alunos ainda enfrentam dificuldades em compreender e aplicar os algoritmos de forma eficaz. Pensando nisso, esse trabalho busca explorar e compreender os algoritmos das operações básicas, explicando seu funcionamento e justificando por que são corretos e aplicáveis. Ao compreender esses algoritmos, professores podem adotar abordagens pedagógicas mais eficazes para que o aluno desenvolva um conhecimento sólido. Este trabalho também mostra e demonstra um algoritmo menos conhecido da raiz quadrada, trazendo um novo conhecimento com novas abordagens de ensino da matemática. Com isso, todos esses estudos poderão contribuir para o avanço do conhecimento teórico e melhorias do ensino da matemática, beneficiando professores e alunos.

Nesse trabalho buscamos revisar os algoritmos das operações aritméticas básicas, aprendidas normalmente na primeira parte do Ensino Fundamental, mas acrescentando uma *demonstração formal* para estes. Isso significa que procuramos justificar, com algum rigor matemático, porque quando somamos 2 números os dispomos um embaixo do outro, respeitando a posição dos dígitos - ou seja, os dígitos da unidade, dezena, centena ... de um número ficam abaixo respectivamente dos dígitos da unidade, dezena, centena ... do outro, fazemos a soma destes junto com algum *excesso* da etapa anterior, usamos apenas a unidade desta operação como parte da resposta e carregamos um possível excesso para a etapa seguinte. Porque o resultado deste algoritmo, ou seja, a sequência de dígitos resultantes, é de fato (representa) a soma dos números dados ?

A resposta à pergunta acima parece simples, para todas as pessoas com alguma formação

matemática. Mas quando vamos enxergar de perto o que está acontecendo . . . não é tão simples assim! Vários detalhes inicialmente não pensados necessitam ser bem entendidos para chegar-se a uma explicação satisfatória para a eficácia dos algoritmos. Não obstante, a formação fornecida pelo Profmat mostra-se totalmente satisfatória para prover essa argumentação, que não temos visto em quase nenhum livro de formação básica em Matemática. Esta é a motivação deste trabalho.

Um outro aspecto que esse trabalho busca, de forma mais implícita, é reacender a importância e a beleza do cálculo mental. Não nos referimos aqui a pessoas super habilidosas que realizam cálculos complexos, de muitos dígitos, em frações de segundo, mas sim a todos nós que usando tabuada elementar que aprendemos nos anos iniciais da formação escolar, e com *auxílio destes algoritmos*, efetuamos cálculos de alguma complexidade, obviamente com o recurso do papel e lápis, ou da lousa e giz. Frisamos que este pode ser considerado cálculo mental, pois os recursos materiais considerados funcionam como meros auxiliares de nossa memória e do senso de organização.

Este trabalho está assim organizado: no capítulo 2 fazemos uma breve apresentação da origem histórica e mitológica dos números, que já nascem vinculados a uma operação, a adição. No capítulo 3 desenvolvemos a ideia fundamental de base numérica, estabelecendo resultados básicos sobre a forma que representamos os números em *dígitos*. São os dígitos que vamos de fato operar nos algoritmos. Nos capítulos 4 e 5 tratamos respectivamente dos algoritmos de soma e subtração, e multiplicação e divisão, trazendo alguns exemplos diagramados, que são interpretados dentro dos algoritmos. O capítulo 6 apresenta uma exposição do bem pouco conhecido algoritmo da *raiz quadrada*, e no capítulo 7 uma breve conclusão desse texto.

O SURGIMENTO DOS NÚMEROS

Os sistemas de numeração sempre foram fundamentais para o desenvolvimento das civilizações. Diversos autores (IFRAH, 2001; TEIXEIRA, 1998; MATTOS, 2008) abordam como diferentes povos criaram símbolos e regras próprias para contar, calcular e registrar informações ao longo da história. A humanidade levou milhares e milhares de anos para construir a ideia de número. Na maior parte da existência humana, as pessoas não sabiam contar. Ainda na pré-história, os seres humanos eram nômades e viviam à base de pesca e caça. A necessidade de contar surgiu quando as antigas civilizações passaram a fixar residência em um local e, com isso, pararam de só caçar e colher frutos, começaram a plantar, criar animais e construir casas. Com essas mudanças na vida humana, houve a necessidade de registrar a quantidade de animais do rebanho, a quantidade de alimentos produzidos e colhidos, assim como contar os dias para se ter noção sobre o clima e as estações do ano, que interferiam diretamente na agricultura que estava começando a surgir. Controlar a quantidade das coisas passou a ser de grande importância.

Uma das histórias mais contadas sobre o surgimento da noção de números e de contagem é que o pastor, para controlar sua quantidade de ovelhas, usava pedrinhas. Ele separava uma pedrinha para cada ovelha que levava para pastar e as colocava em um saquinho. No final do dia, o pastor comparava a quantidade de ovelhas que voltava do pasto com a quantidade de pedrinhas que havia no saquinho. Se sobrasse pedrinhas, é porque estava faltando ovelhas. Porém, podemos imaginar também que nessa época surgiu uma das contagens mais intuitivas que ainda é usada para fazer pequenos cálculos, a contagem dos dedos. Os dedos eram objetos de fácil acesso em qualquer lugar que estivessem, e assim podemos supor que os seres humanos começaram a contar os dedos das mãos, percebendo que podiam associar cada dedo a uma ovelha ou coisa, podendo contar até dez usando as duas mãos uma única vez.

Porém, com as duas mãos, era possível contar apenas dez dedos, o que passou a ser insuficiente. Então, teve-se a ideia de recomençar a contagem, lembrando que um ou mais grupos de dez, ou seja, grupos de duas mãos inteiras, já haviam sido contados. Nessa forma de contagem,

agrupando de dez em dez, podemos ver a criação da base dez, assunto que trataremos em capítulos adiante. Essa é a base do nosso sistema numérico atual, sistema esse de contagem que permanece como um dos mais usados, visto a sua facilidade de contar nos dedos. Vamos lembrar que nessa época a contagem não era feita pensando nos símbolos que representam nossos atuais números, nem com os nomes que os conhecemos hoje: “um, dois, três, quatro, ...”, a contagem consistia em fazer apenas uma associação onde cada dedo ou pedrinha representava cada ovelha ou objeto que lhe pertencia.

Existem também registros históricos de madeiras ou ossos marcados com tracinhos, nós em cordas, marcas nas paredes, desenhos nas cavernas e outros tipos de marcações para realização das contagens. Mesmo sem saber o processo de cálculos usado hoje e sem ter conhecimentos dos símbolos numéricos atuais, eles estavam usando o conceito de associação da quantidade do que possuíam em relação à quantidade de pedrinhas ou dedos da mão, e começava aí uma noção de números e contagens.

Com a evolução humana, surgiu a palavra cálculo, que em latim "calculus" significa pedrinha, e começou a necessidade de fazer contas, de juntar ou separar coisas, na verdade, de adicionar ou subtrair. A adição na pré-história pode ser entendida como a prática de combinar e juntar objetos para criar algo que suprisse suas necessidades da época, para que se adaptassem ao ambiente e tivessem mais chance de sobrevivência. A adição começou a surgir com a união de diferentes materiais para criar ferramentas, por exemplo, ligar uma peça de osso a um pedaço de madeira para criar uma lança. Dessa forma, surgiu a noção de combinar e juntar diferentes materiais. À medida que a humanidade evoluía, as formas de adições se tornavam melhores e mais elaboradas, a adição não se limitava a ferramentas, mas a alimentação, tecidos, artefatos artesanais, como por exemplo a criação da cerâmica, que é a adição de argila e água.

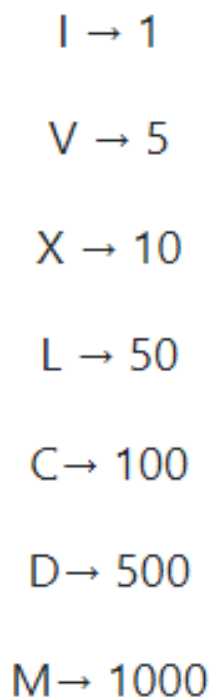
Com essa ideia de adição, onde sabia que podiam juntar coisas e materiais, percebeu-se que podiam combinar ou agrupar quantidades. À medida que a sociedade se desenvolvia, aumentava a necessidade de lidar com maiores quantidades, com o surgimento de trocas de objetos e bens entre as pessoas e a observância de fenômenos naturais. A mudança das fases das luas, a contagem dos dias e das estações do ano contribuíram também com a necessidade de combinar números. Vamos imaginar uma situação em que um homem possuía grande quantidade de gados, e que ao realizar uma troca com um vizinho pegou uma quantidade maior ainda de gados. Para não ter o trabalho de ir ao pasto contar todo seu gado, o que seria também uma tarefa difícil, ele viu a necessidade de fazer isso de dentro da sua casa, sentado em sua mesa, mas precisava desenvolver uma forma de agrupar essas grandes quantidades.

Os números fazem parte do nosso dia a dia e estão presentes em praticamente tudo ao nosso redor. Eles são fundamentais para a matemática e para muitas outras áreas do conhecimento, ajudando a representar situações, resolver problemas e organizar informações. Embora sejam associado a ideia de quantidade ou posições, eles vão muito além disso. Na verdade, um número é um conceito abstrato que pode assumir diferentes papéis, dependendo do contexto. Podemos

usá-los para contar, medir, ordenar ou até lidar com cálculos bem mais complexos, como os que aparecem na física, na engenharia, na contabilidade, na economia e na agricultura.

Com a necessidade de contagem e de fazer cálculos, os humanos desenvolveram símbolos e sistemas de numerações através de representação por algarismos. Há registros de vários sistemas de numeração, pois ao longo dos anos cada povo desenvolveu um tipo de grafia com quantidade de símbolos e sistemas numéricos distintos (IFRAH, 2001). O sistema de numeração mais conhecido atualmente é o sistema de numeração decimal, porém existiram alguns que se destacaram como o romano, maia, egípcio, sumérios etc.

- Sistema de numeração Romano: esse sistema de numeração é representado por letras. Para representar números diferentes, usa-se a repetição dos símbolos, onde os símbolos I, X, C e M podem ser repetidos no máximo três vezes. Escrever um símbolo menor à esquerda consiste em uma subtração e escrever o menor à direita, uma adição. Por exemplo, o número 9 é IX e o número 11 é XI. Esse sistema ainda é usado para contar os séculos.



I	→	1
V	→	5
X	→	10
L	→	50
C	→	100
D	→	500
M	→	1000

Figura 1 – Sistema de numeração romano

Fonte: Mundo Educação – *Sistema de numeração*. Acesso em: 03/04/2024.

- Sistema de numeração Egípcio: esse sistema possui sete símbolos que são agrupados de dez em dez, eles são repetidos e combinados para a representação de números maiores. Cada símbolo pode ser repetido nove vezes.

Símbolo Egípcio	Número na nossa notação
	1
∩	10
?	100
⌋	1 000
∩	10 000
⌋	100 000
⌋	1 000 000

Figura 2 – Sistema de numeração egípcio

Fonte: Portal Pedagógico – *Quem criou a Matemática?*. Acesso em: 03/04/2024.

- Sistema de numeração Maia: Os maias desenvolveram um sistema de numeração vigesimal posicional onde as “ordens maiores ficam em cima. O número 0 era representado por uma concha, o ponto sinalizava a unidade, podia ser empregado até quatro vezes, e o traço representava a quantidade cinco, até três vezes. O número 12, por exemplo, era escrito por dois traços (5 + 5) e dois pontos (1 + 1). Para representar o número 20, utilizava-se um ponto sobre uma concha, indicando $1 \cdot 20^1$. O 21 era expresso por um ponto acima $1 \cdot 20^1$ e um ponto embaixo $1 \cdot 20^0$ e assim sucessivamente.

				
0	1	2	3	4
				
5	6	7	8	9
				
10	11	12	13	14
				
15	16	17	18	19
				
				
20	21	22	30	33

Figura 3 – Sistema de numeração maia

Fonte: Mundo Educação – *Sistema de numeração maia*. Acesso em: 03/04/2024.

- Sistema de numeração Sumérios: foi um dos primeiros sistemas de numeração e é conhecido como sistema de numeração babilônico. Esse sistema possui dois símbolos que consistiam em traços e formatos simples que variavam de acordo com a posição do algarismo. O sistema numérico sumério é de base 60, ou seja, a cada nova posição o valor é multiplicado por 60. Um mesmo símbolo pode representar 1, 60, 3600 ou mais, dependendo da posição em que ele aparece. Como originalmente não existia um símbolo para o zero, a diferença de valor era indicada pelo espaço entre os símbolos: quanto mais à esquerda o símbolo está, maior seu valor posicional. Por exemplo, um símbolo isolado pode valer 1 se estiver na casa das unidades, mas valerá 60 se estiver uma posição à esquerda.

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

Figura 4 – Sistema de numeração sumério

Fonte: Mundo Educação – *Sistema de numeração*. Acesso em: 03/04/2024.

Entendemos como sistema de numeração seus algarismos e sua organização. No nosso sistema de numeração decimal temos 10 símbolos numéricos, os algarismos 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, que formam todos os outros números dentre as suas diversas combinações, ou seja, a posição de cada algarismo é importante. Esse sistema foi aperfeiçoado ao longo dos anos e sua origem é indo-arabica.

BASES NUMÉRICAS

Este capítulo baseia-se em obras que abordam a história e a estrutura dos sistemas de numeração, como Ifrah (2001), Mattos (2008), Wells (1999) e Teixeira (1998), além de autores que tratam da representação posicional e das bases numéricas de forma teórica, como Hefez (2016), Santos (1998) e Milies e Coelho (2001).

Uma base numérica é um sistema de numeração ou conjunto de símbolos, dígitos usados para representar números. Cada base numérica tem uma quantidade específica de símbolos e uma maneira que eles são organizados para representar diferentes valores, o valor de cada símbolo depende da sua posição em relação aos outros símbolos. Cada base numérica é fundamental porque determina diretamente a maneira pela qual cálculos e números são feitos. Bases numéricas são sistemas fundamentais usados para representar números em muitas disciplinas acadêmicas, especialmente matemática e computação. Eles diferem em termos de símbolos e regras usados para representar quantidades. A base decimal é um sistema de base usado diariamente, mas várias outras bases, incluindo binária, octal e hexadecimal, são críticas em áreas técnicas específicas.

3.1 Base decimal

A base decimal, também chamada de sistema de numeração base 10, é a maneira mais comum de representar números. Usando os dígitos de 0 a 9, essa base é usada em todo o mundo para atividades diárias e científicas. A história da base decimal está fortemente entrelaçada com o desenvolvimento das primeiras civilizações e importantes avanços na matemática em séculos (IFRAH, 2001). A aceitação da base decimal é historicamente significativa, uma vez que foi usada por antigas civilizações. De acordo com o Penguin Dictionary of Curious and Interesting Numbers, os maias usavam a base decimal e o Egito, em 300 a.C., também usava essa base.

Segundo Mattos (2008) durante a Idade Média, o sistema decimal foi introduzido na Europa, juntamente com o conceito de zero, pelo contato com o mundo islâmico. Isso ocorreu

em grande parte durante as Cruzadas e por meio de traduções de textos árabes para o latim. Na época do Renascimento, o sistema decimal foi amplamente introduzido na Europa pela primeira vez e rapidamente substituiu os sistemas de numeração romana e outros métodos locais. Devido à invenção da tipografia por Johann Gutenberg por volta de 1440, tornou-se mais fácil divulgar materiais propondo o uso do sistema decimal. Leonhard Pisano, conhecido como Fibonacci, foi um dos responsáveis por trazer o sistema para a Europa através de seu “Livro de 12 capítulos” de 1202.

Outro aspecto da base decimal que é bastante revolucionário é a introdução do zero. Antes dessa inovação, todos os sistemas de numeração disponíveis eram muito limitados e difíceis de manejar. Os indianos elaboraram o conceito de 0 e os árabes disseminaram pelo mundo, conceito esse que indica a ausência de um valor em determinada posição, por exemplo, o número 1024 indica que não possui centenas. O zero não apenas simplificou todos os cálculos, mas também possibilitou o desenvolvimento de algoritmos mais eficazes que permitiriam realizar cálculos complexos. Com ele, foi possível escrever números maiores de forma compacta e eficiente.

O sistema decimal de base dez, portanto, compreende os dez dígitos, ou seja, 0, 1, 2, 3, 4, 5, 6, 7, 8 e 9. Este sistema de contagem é amplamente usado no mundo moderno devido à simplicidade e eficiência na representação numérica e operações aritméticas. Na base decimal, no que diz respeito às operações básicas com números naturais — adição, subtração, multiplicação e divisão — manipular dez dígitos é muito familiar e simples, pois contar nos dedos (incitado pela natureza e tendo o total de dez dedos nas mãos) é muito básico. Em cada um dos números deste sistema, cada dígito representa uma potência de 10 dependendo de sua posição, começando da direita para a esquerda com 10^0 e aumentando em uma unidade no expoente para cada posição movida para a esquerda. O valor de um número vem da soma de todos os produtos obtidos da multiplicação do valor da posição de cada dígito por seu valor posicional.

Exemplo 1. No número 4572, vamos analisar cada dígito e seu valor posicional.

- Posição da unidade de milhar (10^3).

Dígito: 4

$$4 \times 10^3 = 4 \times 1000 = 4000.$$

O dígito 4 está na posição da unidade de milhar, representando 4000 unidades.

- Posição das centenas (10^2).

Dígito: 5

$$5 \times 10^2 = 5 \times 100 = 500.$$

O dígito 5 está na posição das centenas, representando 500 unidades.

- Posição das dezenas (10^1)

Dígito: 7

$$7 \times 10^1 = 7 \times 10 = 70.$$

O dígito 7 está na posição das dezenas, representando 70 unidades.

- Posição das unidades (10^0)

Dígito: 2

$$2 \times 10^0 = 2 \times 1 = 2.$$

O dígito 2 está na posição das unidades, representando unidades.

Para obter o valor total do número, somamos os valores posicionais de cada dígito:

$$4000 + 500 + 70 + 2 = 4572.$$

Portanto, o número 4572 é a soma de:

- 4000 (4 unidades de milhar)
- 500 (5 centenas)
- 70 (7 dezenas)
- 2 (2 unidades)

Dessa forma o número 15387 seria:

$$1 \times 10^4 + 5 \times 10^3 + 3 \times 10^2 + 8 \times 10^1 + 7 \times 10^0 =$$

$$= 10000 + 5000 + 300 + 80 + 7 = 15387.$$

3.2 Base arbitrária

A ideia usada na seção anterior, ou seja, de escrever um número como soma de potências de 10 agrupadas em quantidades que não excedem a 9 pode ser ampliada para um número natural b qualquer, que seja maior que 1. Um número n em uma base b é expresso como uma sequência de dígitos, onde cada dígito está posicionado de acordo com uma potência de b .

Definição 1. Seja $b > 1$ um número natural. Um **dígito** na base b é um conjunto de b símbolos distintos $\{s_0, s_1, \dots, s_{b-1}\}$ que são associados em correspondência biunívoca a cada um dos números $\{0, 1, 2, \dots, b-1\}$.

Normalmente, e por simplicidade, escolhemos os próprios números $0, 1, \dots, b-1$ para serem os dígitos nessa base, ou seja, $s_i = i$, $0 \leq i \leq b-1$.

Exemplo 2.

- Na base $b = 10$, os dígitos são os dez *algarismos indo-arábicos*: $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.
- Na base $b = 5$, os dígitos são os cinco primeiros *algarismos indo-arábicos*: $\{0, 1, 2, 3, 4\}$.
- Na base $b = 16$, os dígitos são os dez *algarismos indo-arábicos* $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ e as seis primeiras letras do alfabeto: $\{A, B, C, D, E, F\}$.

Definição 2. Um número natural n possui expressão na base b se pudermos escrever

$$n = a_k b^k + a_{k-1} b^{k-1} + \dots + a_2 b^2 + a_1 b + a_0 = \sum_{i=0}^k a_i b^i, \quad (3.1)$$

onde $a_0, a_1, \dots, a_k$ são dígitos na base b (que representam de fato números em $\{0, 1, \dots, b-1\}$).

Observação 1. Na representação (3.1), o dígito mais à esquerda a_k é normalmente tomado não nulo. Neste caso é chamado de dígito *mais significativo* (o dígito mais à direita a_0 é chamado de dígito *menos significativo*). Em algumas situações podemos “colocar zeros” à esquerda da representação de n , obtendo novas representações equivalentes, pois esses correspondem a potências mais altas que são somadas com coeficiente nulo, não alterando a soma inicial. Como exemplo, podemos escrever 1257 ou 001257 para o mesmo número.

Definição 3. O número de dígitos de um número a na base b é o número de dígitos que ocorrem na representação $a = (a_k a_{k-1} \dots a_0)_b$ desde que $a_k \neq 0$. Assim, nesse caso, o número de dígitos é $k+1$.

Um fato importante quanto à notação: a base 10 (dez), por ser a mais usada, dispensará os parênteses. Assim $(1324)_{10} = 1324$, enquanto $(243)_5 = 73$ e $(10111101)_2 = 189$.

Para entender como obter os dígitos de uma representação é necessário utilizar o Teorema da Divisão Euclidiana:

Teorema 1. Dados dois números inteiros n e b (com $b \neq 0$), existe um único par de inteiros (q, r) tais que:

$$n = q \cdot b + r \quad , \quad 0 \leq r < |b|,$$

onde q é o quociente e r é o resto da divisão.

Demonstração. Iniciemos apresentando o **Teorema de Eudoxius**, que afirma: Dados a e b inteiros, com $b \neq 0$, então a é um múltiplo de b ou se encontra entre dois múltiplos consecutivos de b . Mais precisamente, para cada par de inteiros a e $b \neq 0$, existe um inteiro q tal que:

- Para $b > 0$:

$$qb \leq a < (q+1)b. \quad (3.2)$$

- Para $b < 0$:

$$(q+1)b < a \leq qb. \quad (3.3)$$

De acordo com o Teorema de Eudoxius com $b > 0$, existe q satisfazendo a desigualdade (3.2). Dessa relação, obtemos:

$$0 \leq a - qb < b.$$

Se definirmos $r = a - qb$, temos $0 \leq r < b$. Assim, garantimos a existência de q e r tais que $a = qb + r$ com $0 \leq r < b$.

Agora, suponha que exista outro par de inteiros q_1 e r_1 que satisfaça $a = q_1b + r_1$, com $0 \leq r_1 < b$.

Subtraindo as duas expressões para a , temos:

$$(qb + r) - (q_1b + r_1) = 0 \implies b(q - q_1) = r_1 - r.$$

Logo, $b \mid (r_1 - r)$. Contudo, como $0 \leq r, r_1 < b$, segue que $|r_1 - r| < b$. Assim, a única possibilidade é $r_1 - r = 0$, ou seja, $r_1 = r$. Substituindo $r_1 = r$ na equação anterior, obtemos:

$$q_1b = qb \implies q_1 = q,$$

uma vez que $b \neq 0$. Portanto, q e r são únicos.

Demonstramos o Teorema no caso $b > 0$. O caso $b < 0$ pode ser provado de forma parecida, utilizando a desigualdade (3.3).

□

O Teorema da divisão nos garante que, dados inteiros a e b , sendo o último diferente de zero, podemos obter um par de inteiros (q, r) , quociente e resto, com as propriedades já aludidas. Vamos denotar tais inteiros com uma notação especial. Assim, escrevemos $a \bmod b$ para designar o resto da divisão de a por b , e $\lfloor \frac{a}{b} \rfloor$ para indicar o quociente desta divisão.

Representação de um número na base b

A expressão geral para um número n na base b é:

$$n = a_k \cdot b^k + a_{k-1} \cdot b^{k-1} + \cdots + a_1 \cdot b^1 + a_0 \cdot b^0. \quad (3.4)$$

Aqui, a_i representa os dígitos do número, e $0 \leq a_i < b$. O dígito a_0 é o dígito mais à direita e representa as unidades (ou b^0), a_1 é o próximo dígito à esquerda e representa b^1 , e assim por diante, até o dígito a_k que representa b^k .

Uma notação para representar n na base b é

$$n = (a_k a_{k-1} \cdots a_2 a_1 a_0)_b. \quad (3.5)$$

Ou seja, denotar o inteiro n na forma de (3.5) equivale a dizer que n se escreve como uma soma como na expressão (3.4).

Assim, é necessário nos certificarmos que qualquer número natural n está associado a uma sequência de dígitos (sua representação na base b) e essa representação é única.

Teorema 2. Para qualquer número inteiro positivo n e qualquer base $b > 1$, existe uma única sequência de dígitos $a_k, a_{k-1}, \dots, a_1, a_0$ tal que:

$$n = \sum_{i=0}^k a_i \cdot b^i,$$

onde $0 \leq a_i < b$ para todos os i , e $a_k \neq 0$.

Demonstração. Inicialmente, vamos supor que n possua uma representação na base b :

$$n = a_k \cdot b^k + a_{k-1} \cdot b^{k-1} + \cdots + a_1 \cdot b^1 + a_0 \cdot b^0, \quad (3.6)$$

onde a_i são os dígitos de n e $0 \leq a_i < b$ para todo i . Vamos apresentar um algoritmo que exhibe cada um dos a_i 's sucessivamente.

Usando a expressão (3.6) notamos que:

$$\begin{aligned} n &= (a_k \cdot b^{k-1} + a_{k-1} \cdot b^{k-2} + \cdots + a_1) b + a_0 = \\ &= n_1 \cdot b + a_0. \end{aligned}$$

Sendo $n_1 = a_k \cdot b^{k-1} + a_{k-1} \cdot b^{k-2} + \cdots + a_1$. Portanto, o dígito de menor ordem (unidades) é obtido como resto da divisão de n por b :

$$a_0 = n \mod b. \quad (3.7)$$

Vemos agora que n_1 já possui uma expressão na base b . E o coeficiente a_1 é o dígito das unidades de n_1 . Repetimos o argumento anterior e obtemos $n_1 = n_2 \cdot b + a_1$, com $n_2 = a_k \cdot b^{k-2} + a_{k-1} \cdot b^{k-3} + \cdots + a_2$, e assim

$$a_1 = n_1 \mod b. \quad (3.8)$$

O processo é repetido para obter os próximos coeficientes, dividindo sucessivamente o número reduzido por b e calculando o módulo b desse número. Na i -ésima etapa, calculamos o dígito a_i e o quociente n_{i+1} , que será usado na etapa seguinte:

$$n_i = n_{i+1} \cdot b + a_i \Rightarrow a_i = n_i \mod b, \text{ e } n_{i+1} = \left\lfloor \frac{n_i}{b} \right\rfloor = \frac{n_i - a_i}{b}. \quad (3.9)$$

Em cada etapa é claro que $n_{i+1} < n_i$. Cada iteração reduz n_i pela divisão por b . Como n é finito, e estamos dividindo continuamente por uma base $b > 1$, haverá um índice i tal que n_i será zero, após um número finito de passos. Isto ocorre quando $i = k + 1$, pois então $a_{k+1} = n_{k+1} \bmod b = 0$ e o mesmo ocorrendo para a_j com $j > k + 1$. Portanto não há mais contribuições de potências de b no número n .

Até aqui provamos que se n se escreve como na expressão (3.4), os coeficientes $a_0, a_1, \dots, a_k$ podem ser obtidos de forma única pelo algoritmo descrito acima, em especial pelas identidades (3.9). Isso implica na unicidade da representação. Pois suponha que n possa ser representado de duas maneiras diferentes:

$$n = \sum_{i=0}^k a_i \cdot b^i = \sum_{i=0}^m c_i \cdot b^i.$$

O algoritmo (3.9) nos dá $a_0 = n \bmod b = c_0, a_1 = n_1 \bmod b = c_1, \dots, a_i = n_i \bmod b = c_i, \dots, 0 \leq i \leq \max\{k, m\}$. As duas representações são portanto iguais.

Agora mostremos que qualquer $n \in \mathbb{N}$ possui uma representação na base b . Para tanto, usamos o mesmo algoritmo dado por (3.9), obtendo os números $n_0 = n, n_1, n_2, \dots$ e $a_0, a_1, a_2, \dots$. A sequência $\{n_i\}$ é decrescente enquanto n_i for positivo, portanto existe k tal que $n_k \neq 0$, e $n_{k+1} = 0$. A partir de $i > k$ os coeficientes a_i serão nulos.

Precisamos justificar que os coeficientes $a_k, a_{k-1}, \dots, a_1, a_0$ obtidos pelo processo descrito satisfazem a identidade (3.6). Começando com o número n , obtemos o primeiro dígito a_0 por (3.7). Isso significa que podemos escrever n na forma

$$n = b \cdot n_1 + a_0,$$

onde $n_1 = \left\lfloor \frac{n}{b} \right\rfloor$.

Ao calcular a_1 por (3.8) temos:

$$n_1 = b \cdot n_2 + a_1,$$

onde $n_2 = \left\lfloor \frac{n_1}{b} \right\rfloor$.

Continuando o processo, no passo i temos $n_i = n_{i+1} \cdot b + a_i$, sendo a_i calculado como $a_i = n_i \bmod b$.

Vamos recuperar n recursivamente. Começamos com $n = n_0$, logo

$$n = b \cdot n_1 + a_0.$$

Substituindo n_1 na expressão de n :

$$n = b \cdot (b \cdot n_2 + a_1) + a_0 = b^2 \cdot n_2 + b \cdot a_1 + a_0.$$

Repetindo esse processo até que n_i se torne zero, obtemos:

$$n = b^{k+1} \cdot 0 + b^k \cdot a_k + b^{k-1} \cdot a_{k-1} + \cdots + b^1 \cdot a_1 + b^0 \cdot a_0.$$

Portanto, a representação final de n é:

$$n = a_k \cdot b^k + a_{k-1} \cdot b^{k-1} + \cdots + a_1 \cdot b^1 + a_0 \cdot b^0,$$

onde $0 \leq a_i < b$ para todo i , e $a_k \neq 0$.

Dessa forma, demonstramos que os coeficientes $a_k, a_{k-1}, \dots, a_1, a_0$ obtidos pelo processo de divisão sucessiva representam a parte de n que corresponde a cada potência de b , e garante que a soma total, conforme expressa na forma $n = a_k \cdot b^k + a_{k-1} \cdot b^{k-1} + \cdots + a_1 \cdot b^1 + a_0 \cdot b^0$, é exatamente igual ao número original n . Portanto, todo $n \in \mathbb{N}$ possui uma representação na base b , que é única. Isso conclui a demonstração. $\square$

Proposição 1. Sejam a e $n \geq 1$ números inteiros não negativos. Então o número de dígitos de a na base b é menor ou igual a n se e somente se $a < b^n$. Em consequência, a tem exatamente n dígitos se e somente se

$$b^{n-1} \leq a < b^n. \quad (3.10)$$

Demonstração. Digamos $a = (a_k \dots a_0)_b$ com $a_k \neq 0$. Então a possui $k+1$ dígitos. Vamos supor $k+1 \leq n$. Então

$$a = \sum_{i=0}^k a_i b^i \leq \sum_{i=0}^k (b-1) b^i = (b-1)(1 + b + b^2 + \cdots + b^k).$$

Substituindo o termo entre parênteses na expressão acima pela fórmula da soma dos termos de uma progressão geométrica obtemos

$$a \leq (b-1) \cdot \frac{b^{k+1} - 1}{b-1} = b^{k+1} - 1 < b^{k+1} \leq b^n.$$

A desigualdade estrita na expressão acima implica $a < b^n$.

Agora suponhamos $k+1 > n$. Logo, $k \geq n$. Como $a_k > 0$ e na somatória que define a os demais termos são maiores ou iguais que zero, segue

$$a = \sum_{i=0}^k a_i b^i = a_k b^k + \sum_{i=0}^{k-1} a_i b^i \geq a_k b^n \geq b^n.$$

Isso conclui a primeira afirmação da proposição. A prova de (3.10) é consequência lógica dessa afirmação. $\square$

3.3 Conversão Entre Bases

Sejam b_1 e b_2 bases maiores que 1. A conversão de um número n da base b_1 para a base b_2 pode ser realizada por meio do algoritmo descrito no Teorema 2. Esse método consiste em realizar divisões repetidas do número pela base b_2 , registrando os restos obtidos em cada etapa até que o quociente seja zero. Os restos, lidos de baixo para cima, constituem a representação do número na base b_2 .

A seguir, exploraremos a conversão entre bases arbitrárias, com exemplos que ilustram a aplicação do algoritmo mencionado.

Conversão Entre Bases Arbitrárias

Na prática, para simplificar os cálculos, realiza-se a conversão em dois passos, utilizando a base decimal como intermediária:

- Converter o número da base b_1 para a base decimal (base 10).
- Converter o resultado da base decimal para a base b_2 .

Exemplo 3. Vamos converter o número $(615)_7$ para a base 5.

Por ser mais usual adotaremos o símbolo $\div$ para representar a divisão entre dois números, exemplo $6 \div 3 = 2$, onde 6 é o dividendo, 3 o divisor e 2 o quociente. Desta forma:

$$\left\lfloor \frac{6}{3} \right\rfloor = 6 \div 3 = 2.$$

1. Primeiramente, convertamos $(615)_7$ para decimal:

O número $(615)_7$ é interpretado como:

$$615_7 = 6 \cdot 7^2 + 1 \cdot 7^1 + 5 \cdot 7^0.$$

Calculamos cada termo:

$$6 \cdot 7^2 = 6 \cdot 49 = 294, \quad 1 \cdot 7^1 = 7, \quad 5 \cdot 7^0 = 5.$$

Somando:

$$(615)_7 = 294 + 7 + 5 = (306)_{10}.$$

Como mencionado acima a notação da base 10 (dez) dispensa os parênteses como em (??). Assim

$$(615)_7 = 294 + 7 + 5 = 306.$$

2. Em seguida, convertemos 306 para a base 5 utilizando divisões sucessivas:

$$306 \div 5 = 61, \text{ resto } 1,$$

$$61 \div 5 = 12, \text{ resto } 1,$$

$$12 \div 5 = 2, \text{ resto } 2,$$

$$2 \div 5 = 0, \text{ resto } 2.$$

3. Portanto, $(615)_7 = (2211)_5$.

Exemplo 4. Vamos converter o número 346 para a base 5:

$$346 \div 5 = 69, \text{ resto } 1,$$

$$69 \div 5 = 13, \text{ resto } 4,$$

$$13 \div 5 = 2, \text{ resto } 3,$$

$$2 \div 5 = 0, \text{ resto } 2.$$

Logo, $346 = (2341)_5$.

Exemplo 5. Considere o número $(2341)_5$. Para convertê-lo para a base decimal, utilizamos a expansão polinomial:

$$(2341)_5 = 2 \cdot 5^3 + 3 \cdot 5^2 + 4 \cdot 5^1 + 1 \cdot 5^0$$

Agora, calculamos cada termo individualmente:

$$2 \cdot 5^3 = 2 \cdot 125 = 250,$$

$$3 \cdot 5^2 = 3 \cdot 25 = 75,$$

$$4 \cdot 5^1 = 4 \cdot 5 = 20,$$

$$1 \cdot 5^0 = 1 \cdot 1 = 1.$$

Somamos os valores obtidos:

$$(2341)_5 = 250 + 75 + 20 + 1 = 346.$$

Portanto, o número $(2341)_5$ na base decimal é:

$$(2341)_5 = 346.$$

Observação 2. O método de divisões sucessivas funciona porque, em cada etapa, o resto obtido representa o coeficiente de uma potência da base b . Assim, os restos capturam a decomposição do número original em potências de b , permitindo reconstruir a representação correta na nova base ao lê-los na ordem inversa.

ADIÇÃO E SUBTRAÇÃO

Neste capítulo, vamos olhar com atenção para os algoritmos da adição e da subtração, buscando entender, de forma clara, o que acontece em cada etapa. A ideia é justificar teoricamente cada passo, com base na estrutura dos números naturais, e evidenciar a importância de conceitos como o excesso e o empréstimo. Ao formalizar essas operações, conseguimos enxergar melhor como os algoritmos ensinados na escola funcionam, por que funcionam e como podem ser adaptados para diferentes bases numéricas — um ponto essencial para ensinar aritmética de maneira mais compreensível e significativa.

4.1 Adição

A adição é uma das principais operações matemáticas e é a base de muitos cálculos mais complexos. Ela pode ser formalmente definida como uma função binária que combina dois valores numéricos para produzir um terceiro valor, conhecido como soma. Ela pode ser demonstrada de maneira prática através de objetos concretos ou de forma simbólica utilizando-se de símbolos como uma maneira de combinar quantidades.

Consideremos dois números inteiros a e b . A **adição** de a e b é a operação que resulta em um número S , tal que

$$S = a + b,$$

onde $a, b, S \in \mathbb{Z}$.

A adição no conjunto dos números inteiros possui as seguintes propriedades:

- **Comutatividade:** Para quaisquer inteiros a e b ,

$$a + b = b + a.$$

- **Associatividade:** Para quaisquer inteiros a , b , e c ,

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

- **Elemento Neutro:** Existe um número 0 tal que para qualquer inteiro a ,

$$a + 0 = a.$$

4.1.1 Algoritmo da Adição

O algoritmo da adição soma os dígitos de mesmo valor posicional. A adição de dois números inteiros a e c consiste em:

1. Considere as representações de a e c como uma sequência de dígitos.

$$a + c = (a_k a_{k-1} \dots a_0)_b + (c_k c_{k-1} \dots c_0)_b = \sum_{i=0}^k a_i b^i + \sum_{i=0}^k c_i b^i. \quad (4.1)$$

Onde a_i e c_i são os dígitos dos números a e c , respectivamente, e estão no intervalo $0 \leq a_i, c_i < b$.

2. Alinhar os números de forma que os dígitos correspondentes de a e c de acordo com sua posição i .
3. Para cada posição i , some os dígitos a_i e c_i correspondentes começando na menor ordem (unidades) para a maior ordem (centenas, milhares, etc.).
4. Se a soma $s_i = a_i + c_i$ for maior ou igual a base b do sistema numérico, o valor excedente é transferido para a próxima coluna à esquerda.
5. Continuar o processo até que todos os dígitos sejam somados incluindo os excessos.

Exemplo 6. Por exemplo, considerando a soma de dois números na base $b = 10$: $a = 569$ e $c = 254$, vamos executar o algoritmo da adição com o diagrama abaixo:

$$\begin{array}{r}
 1 1 \\
 5 6 9 \\
 + 2 5 4 \\
 \hline
 8 2 3
 \end{array}$$

Nesta seção nosso objetivo é estabelecer e justificar um algoritmo que opere nos dígitos de representações de números, e retorne a representação da soma destes números, em uma dada base numérica b . Supomos de início que temos dois inteiros positivos a e c , cujas representações são definidas em (4.1)

A primeira observação é que a e c não precisam ter o mesmo número de dígitos, ou seja, pode ocorrer $k \neq j$. Será conveniente contudo utilizar o mesmo número de coeficientes para ambos, o que é feito completando-se com zeros à esquerda para aquele com menos dígitos. Supondo sem perda de generalidade que $k \geq j$, definimos $b_i = 0$ para todo $k \geq i \geq j + 1$.

Em seguida reescrevemos os números na forma de somatórias, e as adicionamos.

$$a + c = (a_k a_{k-1} \dots a_0)_b + (c_k c_{k-1} \dots c_0)_b = \sum_{i=0}^k a_i b^i + \sum_{i=0}^k c_i b^i.$$

Agrupamos nas somatórias os termos semelhantes em b^i :

$$a + c = \sum_{i=0}^k (a_i + c_i) b^i.$$

Lembrando que buscamos a **representação** da soma $a + c$. A equação acima nos indica que bastaria considerar o i -ésimo dígito da representação da soma como $a_i + c_i$. No entanto, pode ocorrer que $a_i + c_i$ seja maior que $b - 1$, o que não é permitido na definição de representação para um número. Contornaremos isso, no algoritmo, com o conceito de **excesso**.

No que segue, fixamos $b \geq 2$ para ser a base do nosso sistema de numeração.

Definição 4. Sejam $a_1, a_2, \dots, a_r$ números inteiros não-negativos. O excesso da soma $a_1 + a_2 + \dots + a_r$ é o número e , dado por

$$e = \left\lfloor \frac{a_1 + a_2 + \dots + a_r}{b} \right\rfloor.$$

Ou seja, e é o quociente da divisão inteira de $a_1 + a_2 + \dots + a_r$ por b .

Por exemplo, o excesso, na base 10, da soma dos números 13, 25, 18 e 7 é 6, pois $13 + 25 + 18 + 7 = 63$. Pode-se ver também que o excesso dessa soma tem representação dada pela representação de s suprimindo-se o dígito das unidades: $s = 63 = (63)_{10}$, o excesso é $6 = (6)_{10}$.

Proposição 2. Dados $a_1, a_2, \dots, a_r$ números não-negativos. Fazamos $s = (a_1 + a_2 + \dots + a_r) \bmod b$, e seja e o excesso da soma $a_1 + a_2 + \dots + a_r$. Então,

$$0 \leq s \leq b - 1, \quad \text{e} \quad a_1 + a_2 + \dots + a_r = e \cdot b + s.$$

Demonstração. É imediata, aplicando-se o algoritmo da divisão Teorema(1). □

Teorema 3. Sejam $a_1, a_2, \dots, a_r$ números inteiros não-negativos. Suponha que todos esses números sejam representados na base b com o mesmo número de dígitos, ou seja, para todo $i \in \{1, 2, \dots, r\}$, tenhamos:

$$a_i = (a_{i,k}a_{i,k-1}a_{i,k-2} \dots a_{i,1}a_{i,0})_b,$$

onde $a_{i,j}$ é o j -ésimo dígito de a_i na base b .

Defina $e_0 = 0$ como o excesso inicial. E, para $j \geq 0$:

$$s_j = (a_{1,j} + a_{2,j} + \dots + a_{r,j} + e_j) \mod b \quad \text{e} \quad (4.2)$$

$$e_{j+1} = \text{excesso da soma } (a_{1,j} + a_{2,j} + \dots + a_{r,j} + e_j). \quad (4.3)$$

Então, o número

$$S = a_1 + a_2 + \dots + a_r,$$

é representado na base b como

$$S = (s_{l+k}s_{l+k-1} \dots s_{k+1}s_k \dots s_1s_0)_b,$$

sendo l o número de dígitos de r na base b .

Demonstração. Para cada $1 \leq i \leq r$, representamos a_i utilizando seus dígitos na base b :

$$a_i = \sum_{j=0}^k a_{i,j}b^j,$$

com os coeficientes $a_{i,j}$ satisfazendo $0 \leq a_{i,j} \leq b-1$.

Logo,

$$\begin{aligned} S &= \sum_{i=1}^r a_i = \sum_{i=1}^r \sum_{j=0}^k a_{i,j}b^j = \\ &= \sum_{j=0}^k \sum_{i=1}^r a_{i,j}b^j = \sum_{j=0}^k \left(\sum_{i=1}^r a_{i,j} \right) b^j. \end{aligned} \quad (4.4)$$

Consideremos, para cada $j \geq 0$, a soma dos números $a_{1,j}, a_{2,j}, \dots, a_{r,j}$, juntamente com o excesso e_j . Usando as equações (4.2) e (4.3) dadas anteriormente, e aplicando a Proposição (2), podemos escrever:

$$\sum_{i=1}^r a_{i,j} + e_j = e_{j+1} \cdot b + s_j, \quad (4.5)$$

com $0 \leq s_j \leq b-1$, onde:

- s_j é o dígito restante na posição j , e
- e_{j+1} é o excesso que será transferido para a posição seguinte.

Desenvolvendo (4.4) e usando (4.5) para alguns valores j , obtemos:

$$S = \sum_{j=0}^k \left(\sum_{i=1}^r a_{i,j} \right) b^j = \left(\sum_{i=1}^r a_{i,0} \right) b^0 + \sum_{j=1}^k \left(\sum_{i=1}^r a_{i,j} \right) b^j. \quad (4.6)$$

Para $j = 0$, temos

$$\sum_{i=1}^r a_{i,0} + e_0 = e_1 \cdot b + s_0,$$

como usamos $e_0 = 0$. Logo:

$$\sum_{i=1}^r a_{i,0} = e_1 \cdot b + s_0.$$

Substituindo esse resultado em:

$$\begin{aligned} S &= (e_1 b + s_0) \cdot b^0 + \sum_{j=1}^k \left(\sum_{i=1}^r a_{i,j} \right) b^j = \\ &= s_0 b^0 + e_1 b^1 + \sum_{j=1}^k \left(\sum_{i=1}^r a_{i,j} \right) b^j. \end{aligned}$$

Continuando o desenvolvimento de (4.6), obtemos:

$$\begin{aligned} S &= s_0 b^0 + e_1 b^1 + \left(\sum_{i=1}^r a_{i,1} \right) b^1 + \sum_{j=2}^k \left(\sum_{i=1}^r a_{i,j} \right) b^j = \\ &= s_0 b^0 + \left(e_1 + \sum_{i=1}^r a_{i,1} \right) b^1 + \sum_{j=2}^k \left(\sum_{i=1}^r a_{i,j} \right) b^j. \end{aligned} \quad (4.7)$$

Procedendo de forma análoga ao que fizemos em (4.6), com $j = 1$,

$$\sum_{i=1}^r a_{i,1} + e_1 = e_2 \cdot b + s_1.$$

Na última linha de (4.7) convertamos o termo :

$$\left(e_1 + \sum_{i=1}^r a_{i,1} \right) b^1 = (e_2 \cdot b + s_1) b^1 = s_1 b^1 + e_2 b^2.$$

E substituímos em S :

$$S = s_0b^0 + s_1b^1 + e_2b^2 + \sum_{j=2}^k \left(\sum_{i=1}^r a_{i,j} \right) b^j.$$

Repetindo esse processo para $j = 2$, temos:

$$\sum_{i=1}^r a_{i,2} + e_2 = e_3 \cdot b + s_2,$$

logo:

$$\begin{aligned} S &= s_0b^0 + s_1b^1 + s_2b^2 + e_3b^3 + \sum_{j=3}^k \left(\sum_{i=1}^r a_{i,j} \right) b^j = \\ &= \sum_{i=0}^2 s_ib^i + e_3b^3 + \sum_{j=3}^k \left(\sum_{i=1}^r a_{i,j} \right) b^j. \end{aligned}$$

Para mostrar a fórmula geral da soma S , utilizamos o princípio da indução finita (cujo detalhamento não será feito aqui). Primeiramente, temos que:

$$S = \sum_{i=0}^k s_ib^i + e_{k+1} \cdot b^{k+1}. \quad (4.8)$$

Note que em (4.8) não existe mais a somatória no índice j , pois ela se escreveria como

$$\sum_{j=k+1}^k,$$

que traduz uma soma nula, já que não apresenta nenhum termo.

Para finalizar, façamos uma estimativa no termo e_{k+1} . Esta decorre de estimativas recursivas nos termos $e_0, e_1, e_2, \dots$. Afirmamos que:

$$\forall j \geq 0, e_j < r. \quad (4.9)$$

Temos $e_0 = 0$, pela definição. Logo, $e_0 < r$.

Analisando a fração $\frac{a_{1,0} + a_{2,0} + \dots + a_{r,0}}{b}$, temos:

$$\begin{aligned} \frac{a_{1,0} + a_{2,0} + \dots + a_{r,0}}{b} &\leq \frac{(b-1) + (b-1) + \dots + (b-1)}{b} \\ &\leq \frac{r(b-1)}{b} < \frac{rb}{b} = r. \end{aligned}$$

Portanto,

$$e_1 = \left\lfloor \frac{a_{1,0} + a_{2,0} + \dots + a_{r,0}}{b} \right\rfloor \leq r - 1.$$

Logo, $e_1 < r$. Concluimos que (4.9) vale para $j = 0$ e $j = 1$.

Assuma que (4.9) é verdadeira para um índice j . Então, $e_j < r$, e:

$$\begin{aligned} \frac{a_{1,j} + a_{2,j} + \cdots + a_{r,j} + e_j}{b} &\leq \frac{(b-1) + (b-1) + \cdots + (b-1) + e_j}{b} \\ &\leq \frac{r(b-1) + e_j}{b} = \frac{rb - r + e_j}{b}. \end{aligned}$$

Mas $e_j \leq r-1$, e logo $rb - r + e_j \leq rb - 1$.

Então,

$$\frac{a_{1,j} + a_{2,j} + \cdots + a_{r,j} + e_j}{b} \leq \frac{rb - 1}{b} < r.$$

Donde

$$e_{j+1} = \left\lfloor \frac{a_{1,j} + a_{2,j} + \cdots + a_{r,j} + e_j}{b} \right\rfloor < r,$$

provando o passo de indução. Em particular, obtemos $e_{k+1} < r$.

Continuando o algoritmo para $j \geq k+1$ vemos que, para os índices $j \geq k+1$, os números $a_1, a_2, \dots, a_r$ não contribuem mais com novos dígitos, pois seus dígitos significativos estão restritos às posições $j \leq k$. A partir de $j \geq k+1$, a soma dos valores restantes depende apenas do excesso acumulado e_j , que foi propagado ao longo das iterações anteriores. Assim, para $j \geq k+1$, a fórmula para os novos dígitos s_j e para o excesso e_{j+1} fica dada por:

$$s_j = e_j \mod b,$$

$$e_{j+1} = \left\lfloor \frac{e_j}{b} \right\rfloor.$$

Isso significa que, para $j \geq k+1$, os dígitos s_j são, na verdade, os dígitos de e_{k+1} , lidos da direita para a esquerda, ou seja, a representação de e_{k+1} na base b .

Além disso, sabemos que $e_{k+1} < r$, pois o excesso nunca pode ultrapassar o número de termos r que estamos somando. Como o número r possui l dígitos na base b , o número e_{k+1} também terá no máximo l dígitos. Logo, podemos expressar e_{k+1} na forma:

$$e_{k+1} = (s_{k+l} s_{k+l-1} \cdots s_{k+2} s_{k+1})_b,$$

onde $s_j = 0$ para $j > k+l$, pois não há mais excesso a ser propagado após a última posição significativa.

Isso conclui a demonstração. □

Exemplo 7. Usando o Teorema (3) vamos considerar a soma de dois números na base $b = 10$: $n = 569$ e $m = 254$.

- Coluna das unidades ($j = 0$):

$$s_0 = (9 + 4 + 0) \mod 10 = 13 \mod 10 = 3,$$

$$e_1 = \left\lfloor \frac{13}{10} \right\rfloor = 1.$$

- Coluna das dezenas ($j = 1$):

$$s_1 = (6 + 5 + 1) \mod 10 = 12 \mod 10 = 2,$$

$$e_2 = \left\lfloor \frac{12}{10} \right\rfloor = 1,$$

- Coluna das centenas ($j = 2$):

$$s_2 = (5 + 2 + 1) \mod 10 = 8 \mod 10 = 8,$$

$$e_3 = \left\lfloor \frac{8}{10} \right\rfloor = 0.$$

A soma final é obtida com todos os dígitos calculados para cada coluna, sendo:

$$569 + 254 = 823.$$

Exemplo 8. Vamos calcular a soma de dois números na base $b = 10$: $n = 1532$ e $m = 729$.

- Coluna das unidades ($j = 0$):

$$s_0 = (2 + 9 + 0) \mod 10 = 11 \mod 10 = 1,$$

$$e_1 = \left\lfloor \frac{11}{10} \right\rfloor = 1.$$

- Coluna das dezenas ($j = 1$):

$$s_1 = (3 + 2 + 1) \mod 10 = 6 \mod 10 = 6,$$

$$e_2 = \left\lfloor \frac{6}{10} \right\rfloor = 0.$$

- Coluna das centenas ($j = 2$):

$$s_2 = (5 + 7 + 0) \mod 10 = 12 \mod 10 = 2,$$

$$e_3 = \left\lfloor \frac{12}{10} \right\rfloor = 1.$$

- Coluna dos milhares ($j = 3$):

$$s_3 = (1 + 0 + 1) \mod 10 = 2 \mod 10 = 2,$$

$$e_4 = \left\lfloor \frac{2}{10} \right\rfloor = 0.$$

A soma final é obtida com todos os dígitos calculados para cada coluna, sendo:

$$1532 + 729 = 2261.$$

Exemplo 9. Vamos calcular a soma de dois números na base $b = 5$: $n = (2342)_5$ e $m = (1244)_5$.

- Coluna para $j = 0$:

$$s_0 = (2 + 4 + 0) \mod 5 = 6 \mod 5 = 1,$$

$$e_1 = \left\lfloor \frac{6}{5} \right\rfloor = 1.$$

- Coluna para $j = 1$:

$$s_1 = (4 + 4 + 1) \mod 5 = 9 \mod 5 = 4,$$

$$e_2 = \left\lfloor \frac{9}{5} \right\rfloor = 1.$$

- Coluna para $j = 2$:

$$s_2 = (3 + 2 + 1) \mod 5 = 6 \mod 5 = 1,$$

$$e_3 = \left\lfloor \frac{6}{5} \right\rfloor = 1.$$

- Coluna para $j = 3$:

$$s_3 = (2 + 1 + 1) \mod 5 = 4 \mod 5 = 4,$$

$$e_4 = \left\lfloor \frac{4}{5} \right\rfloor = 0.$$

A soma final é obtida com todos os dígitos calculados para cada coluna, sendo:

$$(2342)_5 + (1244)_5 = (4141)_5.$$

4.2 Subtração

A subtração é uma das quatro operações básicas da matemática, que consiste em remover uma quantidade de outra, podendo ser entendida como a operação de descobrir a diferença entre dois números. Podemos dizer que a subtração apresenta a seguinte forma:

$$a - c = d,$$

sendo: a o *minuendo*, c o *subtraendo* e d o resultado da subtração, que é chamado de *diferença*. Aqui a , c , e d pertencem ao conjunto dos números inteiros $\mathbb{Z}$.

A subtração apresenta as seguintes propriedades:

- **Não comutativa:** a ordem dos números influencia o resultado, ou seja, $a - c \neq c - a$.
- **Não associativa:** a subtração também não é associativa, ou seja, $(a - c) - x \neq a - (c - x)$.
- **Inverso da Adição:** a subtração pode ser vista como o inverso da adição. Ou seja, se $d + c = a$, então $a - c = d$.

4.2.1 Algoritmo da Subtração

O algoritmo da subtração subtrai os dígitos de mesmo valor posicional. A subtração de dois números inteiros a e c , com $a \geq c$, consiste em:

1. Considere as representações de a e c como uma sequência de dígitos, definidas em (4.1)
2. Alinhar os números de forma que os dígitos correspondentes de a e c fiquem de acordo com sua posição i .

3. Para cada posição i , subtraia o dígito c_i de a_i , começando na menor ordem (unidades) para a maior ordem (centenas, milhares, etc.).
4. Se a subtração $s_i = a_i - c_i$ resultar em um valor negativo, realiza-se o empréstimo da próxima posição à esquerda, diminuindo a posição emprestada em 1 unidade e adicionando b à posição atual.
5. Continuar o processo até que todos os dígitos sejam subtraídos corretamente, levando em consideração os empréstimos necessários.

Exemplo 10. Vamos considerar a subtração $4125 - 1874$ na base 10 e ilustrar o algoritmo da subtração com o diagrama abaixo.

$$\begin{array}{r}
 ^3 ^{10} \\
 ^4 ^1 ^2 ^5 \\
 - ^1 ^8 ^7 ^4 \\
 \hline
 ^2 ^2 ^5 ^1
 \end{array}$$

Nesta seção vamos estabelecer e justificar um algoritmo que opere nos dígitos de representações de dois números, e retorne a representação da diferença destes números, em uma dada base numérica b . Supomos de início que temos dois inteiros positivos a e c , cujas representações são :

$$a = (a_k a_{k-1} \dots a_0)_b \text{ e } c = (c_j c_{j-1} \dots c_0)_b.$$

Onde a_i e c_i são os dígitos dos números a e c , respectivamente, e estão no intervalo $0 \leq a_i, c_i < b$.

Vamos considerar $a \geq c$, para que a operação obtenha como resultado um número não negativo.

Os números a e c não precisam ter o mesmo número de dígitos, ou seja, pode ocorrer $k \neq j$. Será conveniente contudo utilizar o mesmo número de dígitos para ambos, o que é feito completando-se com zeros à esquerda para aquele com menos dígitos. Uma vez que $a \geq c$ deve ser $k \geq j$, e definimos $c_i = 0$ para todo $k \geq i \geq j + 1$.

Em seguida reescrevemos os números na forma de somatórias, e as subtraímos.

$$a - c = (a_k a_{k-1} \dots a_0)_b - (c_k c_{k-1} \dots c_0)_b = \sum_{i=0}^k a_i b^i - \sum_{i=0}^k c_i b^i. \quad (4.10)$$

Agrupamos nas somatórias os termos semelhantes em b^i :

$$a - c = \sum_{i=0}^k (a_i - c_i) b^i. \quad (4.11)$$

O algoritmo de subtração é parecido ao da adição no sentido de que opera dígito a dígito, começando pela menor ordem. No entanto, ao contrário da adição, ele envolve o conceito de "empréstimo" quando o valor do minuendo é menor que o do subtraendo.

Teorema 4. Sejam a e c dois números com $a \geq c$, representados conforme (4.10), e $d = a - c$ a sua diferença. Definamos a sequência $\{\varepsilon_i\}$, onde cada ε_i representa o empréstimo da posição i para a posição $i - 1$, sendo $\varepsilon_0 = 0$. Para $i \geq 0$ fazemos recursivamente

$$\varepsilon_{i+1} = \begin{cases} 1, & \text{se } a_i - \varepsilon_i - c_i < 0, \\ 0, & \text{se } a_i - \varepsilon_i - c_i \geq 0. \end{cases} \quad (4.12)$$

E façamos para $i \geq 0$

$$d_i = (a_i + \varepsilon_{i+1} \cdot b) - \varepsilon_i - c_i. \quad (4.13)$$

Então as sequências $\{\varepsilon_i\}$ e $\{d_i\}$ serão nulas para $i \geq k + 1$, $0 \leq d_i < b$ para todo $i \geq 0$ e

$$d = \sum_{i=0}^k d_i b^i = (d_k d_{k-1} \dots d_0)_b. \quad (4.14)$$

Demonstração. Primeiro mostremos que

$$0 \leq d_i \leq b - 1, \quad (4.15)$$

para todo $i \geq 0$. Temos dois casos a considerar, de acordo com $a_i - c_i - \varepsilon_i \geq 0$ e $a_i - c_i - \varepsilon_i < 0$.

Para o caso em que $a_i - \varepsilon_i - c_i \geq 0$ sabemos por (4.12) que $\varepsilon_{i+1} = 0$. Assim, substituindo em (4.13), temos:

$$d_i = a_i - \varepsilon_i - c_i \geq 0.$$

Por outro lado, c_i e ε_i são números não negativos, logo,

$$d_i = a_i - c_i - \varepsilon_i \leq a_i \leq b - 1.$$

E disto segue

$$0 \leq d_i \leq b - 1.$$

Para o caso em que $a_i - \varepsilon_i - c_i < 0$ sabemos por (4.12) que $\varepsilon_{i+1} = 1$. Assim, substituindo em (4.13), temos:

$$d_i = (a_i + b) - \varepsilon_i - c_i.$$

Como $a_i - \varepsilon_i - c_i < 0$, somando b aos dois lados dessa desigualdade, obtemos:

$$d_i = a_i + b - \varepsilon_i - c_i < b. \quad (4.16)$$

Mas $c_i \leq b - 1$ e $\varepsilon_i \leq 1$, portanto $c_i + \varepsilon_i \leq b$, e logo $b - c_i - \varepsilon_i \geq 0$. Daí decorre

$$d_i = a_i + b - \varepsilon_i - c_i \geq 0. \quad (4.17)$$

Das relações (4.16) e (4.17) segue imediatamente a relação (4.15).

Agora vamos trabalhar a expressão em (4.11)

$$d = a - c = \sum_{i=0}^k (a_i - c_i)b^i = (a_0 - c_0)b^0 + \sum_{i=1}^k (a_i - c_i)b^i.$$

Como $\varepsilon_0 = 0$ podemos subtrair ε_0 e somar e subtrair $\varepsilon_1 b$ nessa expressão:

$$\begin{aligned} d &= (a_0 - \varepsilon_0 - c_0)b^0 + \varepsilon_1 b - \varepsilon_1 b + \sum_{i=1}^k (a_i - c_i)b^i = \\ &= (a_0 - c_0 - \varepsilon_0 + \varepsilon_1 b)b^0 - \varepsilon_1 b + \sum_{i=1}^k (a_i - c_i)b^i. \end{aligned} \quad (4.18)$$

O termo entre parênteses na primeira parcela do último membro de (4.18) equivale a d_0 . Logo, podemos escrever

$$d = d_0 b^0 - \varepsilon_1 b + \sum_{i=1}^k (a_i - c_i)b^i.$$

Repetindo a construção acima para $i = 1$:

$$\begin{aligned} d &= d_0 b^0 - \varepsilon_1 b + (a_1 - c_1)b^1 + \sum_{i=2}^k (a_i - c_i)b^i = \\ &= d_0 b^0 + (a_1 - c_1 - \varepsilon_1 + \varepsilon_2 b)b^1 - \varepsilon_2 b^2 + \sum_{i=2}^k (a_i - c_i)b^i. \end{aligned} \quad (4.19)$$

O termo entre parênteses na segunda parcela do último membro de (4.19) é igual a d_1 . Assim, podemos reescrever:

$$d = d_0 b^0 + d_1 b^1 - \varepsilon_2 b^2 + \sum_{i=2}^k (a_i - c_i)b^i.$$

Continuando essa propagação até $i = k$ podemos expressar a diferença como:

$$\begin{aligned} d &= d_0 b^0 + d_1 b^1 + d_2 b^2 + \cdots + d_{k-1} b^{k-1} - \varepsilon_k b^k + (a_k - c_k)b^k \\ &= \sum_{i=0}^{k-1} d_i b^i + (a_k - c_k - \varepsilon_k + \varepsilon_{k+1} b)b^k - \varepsilon_{k+1} b^{k+1} \\ &= \sum_{i=0}^k d_i b^i - \varepsilon_{k+1} b^{k+1}. \end{aligned} \quad (4.20)$$

Para finalizar mostremos que $\varepsilon_{k+1} = 0$. Isto pode ser visto da seguinte forma. Se ocorrer $\varepsilon_{k+1} \neq 0$ então deve ser $\varepsilon_{k+1} = 1$, logo $\varepsilon_{k+1} b^{k+1} = b^{k+1}$. O número dado pela soma $\sum_{i=0}^k d_i b^i$ é um número de $k + 1$ dígitos, portanto necessariamente menor que b^{k+1} . Daí segue que o último termo de (4.20) é negativo.

Mas esse termo é igual a $a - c$, que por hipótese é não-negativo. Essa contradição mostra-nos que deve ser $\varepsilon_{k+1} = 0$. Em consequência também obtemos

$$d = \sum_{i=0}^k d_i b^i.$$

Para $i \geq k + 1$ teremos sempre $a_i = c_i = 0$, logo ε_{i+1} será zero se $\varepsilon_i = 0$, recursivamente. E também $d_i = 0$, para todo $i \geq k + 1$.

□

Exemplo 11. Vamos considerar a subtração $4125 - 1874$ na base 10 e ilustrar o processo de cálculo dígito a dígito conforme o Teorema (4).

Fazemos a subtração dígito a dígito na direita para a esquerda.

- Unidades ($i = 0$)

Como o $\varepsilon_0 = 0$, temos:

$5 - 0 - 4 = 1 > 0$, não há necessidade de empréstimos, sendo $\varepsilon_1 = 0$, desta forma:

$$(5 + 0 \cdot 10) - 0 - 4 = 1.$$

- Dezenas ($i = 1$)

$2 - 0 - 7 = -5 < 0$, há necessidade de empréstimo, sendo $\varepsilon_2 = 1$, desta forma

$$(2 + 1 \cdot 10) - 0 - 7 = 5.$$

- Centenas ($i = 2$)

Como $1 - 1 - 8 = -8 < 0$, há necessidade de empréstimos, sendo $\varepsilon_3 = 1$, desta forma:

$$(1 + 1 \cdot 10) - 1 - 8 = 2.$$

- Milhares ($i = 3$)

Como $4 - 1 - 1 = 2 > 0$, não há necessidade de empréstimo, então.

$$4 - 1 - 1 = 2.$$

A subtração final é obtida com todos os dígitos calculados para cada coluna, sendo:

$$4125 - 1874 = 2251.$$

Exemplo 12. Vamos considerar a subtração de dois números na base 2: $(11110)_2 - (10011)_2$.

Fazemos a subtração dígito a dígito da direita para a esquerda.

- Unidades ($i = 0$)

Como $\varepsilon_0 = 0$, temos:

$$0 - 0 - 1 = -1 < 0$$

Há necessidade de empréstimo, sendo $\varepsilon_1 = 1$. Assim:

$$(0 + 1 \cdot 2) - 0 - 1 = 1.$$

- Dois ($i = 1$)

Como $1 - 1 - 1 = -1 < 0$, há necessidade de empréstimo, sendo $\varepsilon_2 = 1$. Assim:

$$(1 + 1 \cdot 2) - 1 - 1 = 1.$$

- Quatros ($i = 2$)

Como $1 - 1 - 0 = 0 \geq 0$, não há necessidade de empréstimo, sendo $\varepsilon_3 = 0$. Assim:

$$1 - 1 - 0 = 0.$$

- Oitos ($i = 3$)

Como $1 - 0 - 0 = 1 \geq 0$, não há necessidade de empréstimo, sendo $\varepsilon_4 = 0$. Assim:

$$1 - 0 - 0 = 1.$$

- Dezesesseis ($i = 4$)

Como $1 - 0 - 1 = 0 \geq 0$, não há necessidade de empréstimo. Assim:

$$1 - 0 - 1 = 0.$$

A subtração final é obtida com todos os dígitos calculados para cada coluna, sendo:

$$(11110)_2 - (10011)_2 = (01011)_2$$

MULTIPLICAÇÃO E DIVISÃO

A multiplicação e a divisão são operações fundamentais da aritmética que aprendemos desde cedo, elas não só ampliam as possibilidades de resolver problemas numéricos, como também estão na base de muitos algoritmos e processos matemáticos mais avançados.

Neste capítulo, vamos explorar com mais profundidade como essas operações funcionam, justificando os algoritmos utilizados para realizá-las. A multiplicação será tratada tanto como uma adição repetida quanto através de métodos formais que facilitam o cálculo com números grandes. Já a divisão será apresentada destacando o passo a passo para encontrar o quociente e o resto, sempre com explicações claras sobre o porquê de cada procedimento.

5.1 Multiplicação

A multiplicação é uma das quatro operações básicas da matemática, que consiste em adicionar uma quantidade a si mesma repetidamente, um número determinado de vezes. Em sua forma geral, a multiplicação pode ser representada da seguinte forma:

$$a \times f = p.$$

Onde: a é o *multiplicando*, f é o *multiplicador*, e p é o resultado da multiplicação, chamado de *produto*.

Os elementos a , f , e p pertencem ao conjunto dos números inteiros $\mathbb{Z}$. A multiplicação possui as seguintes propriedades:

- **Comutativa:** a ordem dos números não altera o resultado, ou seja, $a \times f = f \times a$.
- **Associativa:** a multiplicação também é associativa, ou seja, $(a \times f) \times c = a \times (f \times c)$.

- **Elemento Neutro:** o número 1 é o elemento neutro da multiplicação, ou seja, $a \times 1 = a$ para todo a .

5.1.1 Algoritmo da Multiplicação

A multiplicação de dois números inteiros a e f consiste em:

1. Considere as representações de a e f como uma sequência de dígitos.

$$a \times f = (a_k a_{k-1} \dots a_0)_b \times (f_k f_{k-1} \dots f_0)_b.$$

Onde a_i e f_i são os dígitos dos números a e f , respectivamente, e estão no intervalo $0 \leq a_i, f_i < b$.

2. Alinhar os números de forma que os dígitos correspondentes de a e f fiquem de acordo com sua posição i .
3. Para cada posição i de a , multiplique todos os dígitos de f por a_i , gerando um produto parcial.
4. Se o produto de $a_i \times f_i$ for maior ou igual à base b , o valor excedente é transportado para a próxima posição.
5. Os produtos parciais devem ser deslocados de acordo com a posição de a_i e então somados para obter o resultado final.

Exemplo 13. Vamos considerar a multiplicação de um número $a = 243$ por um número $f = 3$, ambos na base 10, e para representar o algoritmo da multiplicação usaremos o diagrama abaixo:

$$\begin{array}{r}
 1 \\
 2 4 3 \\
 \times 3 \\
 \hline
 7 2 9
 \end{array}$$

Portanto, $243 \times 3 = 729$.

Exemplo 14. Neste exemplo considerar a multiplicação de um número $a = 567$ por um número de dois dígitos $f = 14$, ambos na base 10:

$$\begin{array}{r}
 \begin{array}{cc} & 2 & 2 \\ & 5 & 6 & 7 \\ \times & & 1 & 4 \\ \hline & 1 & & \\ 2 & 2 & 6 & 8 \\ 5 & 6 & 7 & + \\ \hline 7 & 9 & 3 & 8 \end{array}
 \end{array}$$

Portanto, $567 \times 14 = 7938$.

Nesta seção, nosso objetivo é estabelecer e justificar um algoritmo que opere nos dígitos das representações de números e retorne a representação do produto destes números em uma dada base numérica b . Um caso elementar será quando um dos números for potência de b .

Proposição 3. Sejam $a = (a_k a_{k-1} \dots a_0)_b$ um número inteiro não-negativo, e $f = (100 \dots 0)_b$, ocorrendo exatamente $n \geq 0$ zeros nesta representação de f . Então uma representação para $a \times f$ é $(a_k a_{k-1} \dots a_0 00 \dots 0)_b$, onde os dígitos das posições $i = 0, i = 1, \dots, i = n - 1$ são todos nulos.

Demonstração. Com tal representação vemos que f é apenas a potência b^n . Assim

$$a.f = \left(\sum_{i=0}^k a_i b^i \right) . b^n = \sum_{i=0}^k a_i b^{i+n}.$$

Ou seja, o dígito da posição $i + n$ de $a.f$, para $0 \leq i \leq k$, é igual a a_i . E para cada $i < n$ o dígito da posição i de $a.f$ é zero, pois não ocorre a potência b^i na soma acima. Isso justifica a representação dada pela Proposição. $\square$

Teorema 5. Sejam a e f números naturais, e $p = a \times f$ o seu produto. Vamos supor que a e f têm como representação na base b : $a = (a_k a_{k-1} \dots a_1 a_0)_b$ e $f = (f)_b$. Defina recursivamente as sequências (e_i) e (p_i) para $i \geq 0$, com:

- $e_0 = 0, e_{i+1} = \left\lfloor \frac{f \cdot a_i + e_i}{b} \right\rfloor$ para $i \geq 0$,
- $p_i = (f \cdot a_i + e_i) \bmod b$.

Então $p = (p_k p_{k-1} \dots p_0)_b$.

Demonstração. A representação de f na base b tem apenas um dígito, que tomamos como o próprio f . Como $a = \sum_{i=0}^k a_i b^i$, obtemos:

$$\begin{aligned} p &= f \cdot a = f \cdot \left(\sum_{i=0}^k a_i b^i \right) = \\ &= \sum_{i=0}^k (f \cdot a_i) b^i. \end{aligned} \quad (5.1)$$

Devido às definições das sequências (e_i) e (p_i) , temos para todo $i \geq 0$:

$$f \cdot a_i + e_i = p_i + e_{i+1} \cdot b. \quad (5.2)$$

Separando a 1ª parcela da somatória no último membro de (5.1) dos demais, e aplicando a identidade (5.2), como $e_0 = 0$ chegamos em:

$$\begin{aligned} p &= (f \cdot a_0) b^0 + \sum_{i=1}^k (f \cdot a_i) b^i = \\ &= (p_0 + e_1 b) b^0 + \sum_{i=1}^k (f \cdot a_i) b^i = \\ &= p_0 b^0 + e_1 b^1 + \sum_{i=1}^k (f \cdot a_i) b^i. \end{aligned}$$

Agrupando o termo $e_1 b^1$ com a parcela $(i = 1)$ da somatória, em seguida obtemos:

$$\begin{aligned} p &= p_0 b^0 + e_1 b^1 + (f \cdot a_1) b^1 + \sum_{i=2}^k (f \cdot a_i) b^i = \\ &= p_0 b^0 + (f \cdot a_1 + e_1) b^1 + \sum_{i=2}^k (f \cdot a_i) b^i, \end{aligned}$$

Como por (5.2) $f \cdot a_1 + e_1 = p_1 + e_2 b$, temos

$$\begin{aligned} p &= p_0 b^0 + (p_1 + e_2 b) b^1 + \sum_{i=2}^k (f \cdot a_i) b^i = \\ &= p_0 b^0 + p_1 b^1 + e_2 b^2 + \sum_{i=2}^k (f \cdot a_i) b^i = \\ &= \sum_{j=0}^1 p_j b^j + e_2 b^2 + \sum_{i=2}^k (f \cdot a_i) b^i. \end{aligned}$$

Tal como na demonstração do Teorema (3), procedemos na próxima etapa em agrupar e_2b^2 com um termo da somatória que restou:

$$\begin{aligned} p &= \sum_{j=0}^1 p_j b^j + e_2 b^2 + (f \cdot a_2) b^2 + \sum_{i=3}^k (f \cdot a_i) b^i = \\ &= \sum_{j=0}^1 p_j b^j + (e_2 + f \cdot a_2) b^2 + \sum_{i=3}^k (f \cdot a_i) b^i = \\ &= \sum_{j=0}^2 p_j b^j + e_3 b^3 + \sum_{i=3}^k (f \cdot a_i) b^i. \end{aligned}$$

Assim, após um total de $k+1$ etapas, chegamos a:

$$p = \sum_{j=0}^k p_j b^j + e_{k+1} \cdot b^{k+1}. \quad (5.3)$$

Note que em (5.3) não existe mais a somatória no índice j , pois ela se escreveria como $\sum_{j=k+1}^k$, que traduz uma soma nula, já que não apresenta nenhum termo.

Neste ponto, observamos que a sequência dos excessos $e_0, e_1, e_2, \dots$ aqui obtida é a mesma que obteríamos seguindo o enunciado do Teorema (3) relativo a uma soma $a + a + \dots + a$ com f parcelas, pois essa soma é obviamente equivalente ao produto $f \times a$. Então, usando aquele teorema, temos para todo $i \geq 0$, $e_i < f$. Como $f < b$, segue que $0 \leq e_i < b$ e $0 \leq e_{k+1} < b$.

Logo, podemos na identidade (5.3) escrever:

$$\begin{aligned} p_{k+1} &= (f \cdot a_{k+1} + e_{k+1}) \mod b = \\ &= (e_{k+1}) \mod b = e_{k+1}, \end{aligned}$$

e

$$\begin{aligned} p &= \sum_{j=0}^k p_j b^j + p_{k+1} b^{k+1} = \sum_{j=0}^{k+1} p_j b^j = \\ &= (p_{k+1} \dots p_1 p_0)_b. \end{aligned}$$

Isso finaliza a demonstração. □

Teorema 6. Sejam a e f números inteiros não-negativos, com $a = (a_k \dots a_0)_b$ e $f = (f_r \dots f_0)_b$. Para cada $0 \leq i \leq r$ defina $s_i = a \cdot f_i$, com $s_i = (s_{i,q} s_{i,q-1} \dots s_{i,0})_b$. Então o produto $p = a \times f$, pode ser expresso como $p = s_0 + s_1 \cdot b^1 + \dots + s_r \cdot b^r$. Em consequência, utilizando o diagrama do algoritmo da soma, podemos perceber p como a soma dos números $s_0, s_1, \dots, s_r$, deslocando cada s_i de i posições para a esquerda.

Demonstração. Como $p = a \cdot f$, podemos escrever

$$p = a \cdot \left(\sum_{j=0}^r f_j \cdot b^j \right) = \sum_{j=0}^r (a \cdot f_j) b^j = \sum_{j=0}^r s_j \cdot b^j,$$

usando a definição dos números (s_j) . Pela proposição 3

$$\begin{aligned} s_j \cdot b^j &= (s_{j,q} s_{j,q-1} \dots s_{j,0})_b \times b^j = \\ &= (s_{j,q} s_{j,q-1} \dots s_{j,0} \underbrace{00 \dots 0}_j)_b. \end{aligned} \quad (5.4)$$

Logo p é expresso como a soma dos números cujas representações são dadas em (5.4). Isso conclui a demonstração. $\square$

Exemplo 15. Vamos considerar a multiplicação de dois números na base $b = 10$: $a = 243$ e $f = 3$, usando o Teorema (5).

- Multiplicação da unidade ($j = 0$):

$$s_0 = 3 \times 3 = 9.$$

- Multiplicação da dezena ($j = 1$):

$$s_1 = 3 \times 4 = 12,$$

dígito das dezenas: $d_1 = 12 \bmod 10 = 2$,

excesso: $e_2 = \left\lfloor \frac{12}{10} \right\rfloor = 1$.

- Multiplicação da centena ($j = 2$):

$$s_2 = 3 \times 2 + e_2 = 6 + 1 = 7.$$

A multiplicação final é obtida com todos os dígitos calculados para cada coluna.

$$243 \times 3 = 729.$$

Exemplo 16. Vamos considerar a multiplicação de dois números na base $b = 10$: $a = 154$ e $f = 6$.

- Multiplicação da unidade ($j = 0$):

$$s_0 = 6 \times 4 = 24,$$

dígito das unidades: $d_0 = 24 \bmod 10 = 4$,

excesso: $e_1 = \left\lfloor \frac{24}{10} \right\rfloor = 2$.

- **Multiplicação da dezena ($j = 1$):**

$$s_1 = 6 \times 5 + e_1 = 30 + 2 = 32,$$

dígito das dezenas: $d_1 = 32 \bmod 10 = 2,$

excesso: $e_2 = \left\lfloor \frac{32}{10} \right\rfloor = 3.$

- **Multiplicação da centena ($j = 2$):**

$$s_2 = 6 \times 1 + e_2 = 6 + 3 = 9,$$

dígito das centenas: $d_2 = 9.$

Assim, a multiplicação final é obtida reunindo os dígitos calculados para cada posição:

$$154 \times 6 = 924.$$

Exemplo 17. Vamos considerar a multiplicação de dois números na base $b = 6$: $a = (1243)_6$ e $f = (5)_6$.

- **Multiplicação na posição $j = 0$:**

$$s_0 = 5 \times a_0 = 5 \times 3 = 15,$$

$$d_0 = 15 \bmod 6 = 3, \quad e_1 = \left\lfloor \frac{15}{6} \right\rfloor = 2.$$

- **Multiplicação na posição $j = 1$:**

$$s_1 = 5 \times a_1 + e_1 = 5 \times 4 + 2 = 22,$$

$$d_1 = 22 \bmod 6 = 4, \quad e_2 = \left\lfloor \frac{22}{6} \right\rfloor = 3.$$

- **Multiplicação na posição $j = 2$:**

$$s_2 = 5 \times a_2 + e_2 = 5 \times 2 + 3 = 13,$$

$$d_2 = 13 \bmod 6 = 1, \quad e_3 = \left\lfloor \frac{13}{6} \right\rfloor = 2.$$

- **Multiplicação na posição $j = 3$:**

$$s_3 = 5 \times a_3 + e_3 = 5 \times 1 + 2 = 7,$$

$$d_3 = 7 \bmod 6 = 1, \quad e_4 = \left\lfloor \frac{7}{6} \right\rfloor = 1.$$

- **Excesso final:**

$$d_4 = e_4 = 1.$$

Reunindo os dígitos na ordem inversa da que foram obtidos, temos o resultado da multiplicação:

$$(1243)_6 \times (5)_6 = (11143)_6.$$

Exemplo 18. Vamos considerar a multiplicação de dois números na base $b = 10$: $a = 567$ e $f = 14$, usando o Teorema (6)

- Multiplicação da unidade ($j = 0$):

$$s_0 = 4 \times 567 = 2268.$$

- Multiplicação da dezena ($j = 1$):

$$s_1 = 1 \times 567 = 567,$$

deslocamento: multiplicamos por $b^1 = 10$, ou seja, 5670.

A multiplicação final é obtida somando os valores deslocados:

$$567 \times 14 = 2268 + 5670 = 7938.$$

Exemplo 19. Vamos considerar a multiplicação de dois números na base $b = 5$: $a = (1224)_5$ e $f = (32)_5$.

- Multiplicação na posição $j = 0$:

$$s_0 = (2)_5 \times (1224)_5 = (3003)_5.$$

- Multiplicação na posição $j = 1$:

$$s_1 = (3)_5 \times (1224)_5 = (4232)_5,$$

deslocamento: multiplicamos por $b^1 = 5^1 = 5$, ou seja, $(42320)_5$.

A multiplicação final é obtida somando os valores deslocados:

$$(1224)_5 \times (32)_5 = (42320)_5 + (3003)_5 = (100323)_5.$$

5.2 Divisão

A divisão é uma das operações fundamentais da aritmética, sendo o processo inverso da multiplicação. Dados dois números naturais a (dividendo) e c (divisor), a divisão pode ser expressa como:

$$a \div c = q, \quad \text{com resto } r, \text{ tal que } a = c \cdot q + r, \quad 0 \leq r < c.$$

Onde:

- a é o *dividendo*,
- c é o *divisor*,
- q é o *quociente*,
- r é o *resto*.

A divisão possui algumas propriedades importantes:

- **Não comutativa:** $a \div c \neq c \div a$ em geral.
- **Não associativa:** $(a \div c) \div x \neq a \div (c \div x)$.
- **Elemento neutro:** O número 1 atua como identidade na divisão quando $c = 1$, pois $a \div 1 = a$.

5.2.1 Algoritmo da Divisão

1. Considere a representação de dois números $a = (a_k a_{k-1} \dots a_0)_b$ e $c = (c_k c_{k-1} \dots c_0)_b$.
2. Escrevemos o dividendo a com seus dígitos alinhados e o divisor c dentro de chaves à direita do dividendo.
 - a) Selecione os primeiros k dígitos de a tal que o número formado seja maior ou igual a c .
 - b) Determine o maior dígito q_i tal que:

$$q_i \cdot c \leq \text{valor parcial do dividendo},$$

onde:

$$q_i = \left\lfloor \frac{\text{valor parcial do dividendo}}{c} \right\rfloor.$$

- c) Multiplique q_i por c e subtraia do valor parcial do dividendo.

d) Baixe o próximo dígito do dividendo e repita o processo até que todos os dígitos sejam processados.

3. **Resultado final:** Os dígitos do quociente q são a sequência dos q_i encontrados e o resto r é o valor final que não pôde ser dividido por c .

Exemplo 20. Vamos considerar os números $a = 1534$ e $c = 12$ e demonstrar o algoritmo da divisão entre eles através do diagrama abaixo:

$$\begin{array}{r} 1534 \quad | \quad 12 \\ 33 \quad 127 \\ 94 \\ 10 \end{array}$$

Neste caso o quociente da divisão de 1534 por 12 é 127 e o resto é 10.

Proposição 4. Sejam a e $c \neq 0$ números tais que c tenha exatamente $k + 1$ dígitos, e a tenha no máximo $k + 1$ dígitos, expressos na base b . Sejam q e r respectivamente, o quociente e o resto da divisão de a por c , ou seja,

$$q = \left\lfloor \frac{a}{c} \right\rfloor, \quad r = a \bmod c.$$

Então, o quociente q tem exatamente um dígito na base b , ou seja, $0 \leq q \leq b - 1$.

Além disso, se $q = 0$ e tomarmos um número da forma $ab + p$, onde p é um dígito qualquer na base b ($0 \leq p \leq b - 1$), então o quociente da divisão de $ab + p$ por c também terá exatamente um dígito na base b .

Demonstração. Como c tem $(k + 1)$ dígitos e a tem no máximo $(k + 1)$ dígitos, pela Proposição 1

$$\begin{aligned} b^{k+1} &> c \geq b^k, \\ b^{k+1} &> a. \end{aligned} \tag{5.5}$$

O quociente e resto da divisão de a por c satisfazem $a = q \cdot c + r$, com $r \geq 0$. Se q tivesse 2 ou mais dígitos, seria $q \geq b$, o que nos daria $q \cdot c \geq b \cdot c$. Como $c \geq b^k$, isso implica $q \cdot c \geq b^{k+1}$, e logo $a \geq b^{k+1}$, contradizendo (5.5). Portanto, q deve ter 1 dígito, ou seja, $0 \leq q \leq b - 1$.

Dado p um número de 1 dígito, e suponha $q = 0$. Isto só é possível se $a < c$. Dessa forma, denote $a' = a \cdot b + p$, e sejam q' e r' respectivamente o quociente e o resto da divisão de a' por c .

Então

$$a' = q' \cdot c + r' \Rightarrow a \cdot b + p = q' \cdot c + r',$$

Suponhamos, por absurdo, que $q' \geq b$.

Então,

$$q'c + r' \geq bc + r',$$

logo

$$ab + p \geq bc + r' \Rightarrow p - r' \geq b \cdot (c - a).$$

A última expressão acima gera o absurdo, pois $(c - a)$ é positivo, então $b \cdot (c - a) \geq b$, enquanto $p - r' \leq p < b$.

Para que não ocorra essa contradição, concluímos que $0 \leq q' < b$. □

Teorema 7. Agora, seja a e $c \neq 0$ números, com representações $a = (a_k \dots a_0)_b$ e $c = (c_\ell \dots c_0)_b$. Assuma $k \geq \ell$ (o caso $k < \ell$ se corrige completando com zeros à esquerda na representação de a). Defina os números p_0 , $q_{k-\ell}$ e r_0 por:

$$p_0 = (a_k a_{k-1} \dots a_{k-\ell})_b,$$

$$q_{k-\ell} = \left\lfloor \frac{p_0}{c} \right\rfloor, \quad r_0 = p_0 \mod c.$$

E defina as sequências finitas de números $\{p_i\}$, $\{q_{k-\ell-i}\}$ e $\{r_i\}$ para $1 \leq i \leq k - \ell$, por:

$$p_i = r_{i-1} \cdot b + a_{k-\ell-i},$$

$$q_{k-\ell-i} = \left\lfloor \frac{p_i}{c} \right\rfloor,$$

$$r_i = p_i \mod c.$$

Então,

1. Para cada $0 \leq i \leq k - \ell$ temos

$$0 \leq q_i \leq b - 1,$$

2. Chamando de q o número cuja representação na base b é $(q_{k-\ell} q_{k-\ell-1} \dots q_0)_b$ e tomando $r = r_{k-\ell}$, temos que q e r são, respectivamente, o quociente e o resto da divisão de a por c .

Demonstração. Provemos 1.

Para $i = k - \ell$, e do fato de p_0 ter o número de dígitos menor ou igual ao número de dígitos de c , a Proposição (4) assegura que $q_{k-\ell}$ tem 1 dígito, logo $0 \leq q_{k-\ell} \leq b - 1$. E sendo r_0 o resto de uma divisão por c , é dado que $\lfloor \frac{r_0}{c} \rfloor = 0$, e a Proposição (4) aplica-se novamente para concluir que $p_1 = r_0 \cdot b + a_{k-\ell-1}$, na divisão por c , dá quociente $q_{k-\ell-1}$ de 1 dígito, e resto $r_1 < c$.

Em geral, para $0 \leq i \leq k - \ell$, se $r_{i-1} < c$, então $p_i = r_{i-1} \cdot b + a_{k-\ell-i}$. E seu quociente por c , $q_{k-\ell-i}$, terá 1 dígito. Como r_i também será menor que c , esse passo se repete até atingirmos $i = k - \ell$, cobrindo todos os termos $q_{k-\ell}, q_{k-\ell-1}, \dots, q_1, q_0$. Isso prova (1).

A demonstração de (2) segue a ideia parecida com as demonstrações anteriores e consiste em manipular a somatória que define a como representação. Temos:

$$\begin{aligned} a &= \sum_{i=0}^k a_i b^i = \sum_{i=k-\ell}^k a_i \cdot b^i + \sum_{i=0}^{k-\ell-1} a_i b^i = \\ &= \left(\sum_{i=k-\ell}^k a_i b^{i-(k-\ell)} \right) \cdot b^{k-\ell} + \sum_{i=0}^{k-\ell-1} a_i b^i. \end{aligned} \quad (5.6)$$

A expressão entre parênteses em (5.6) corresponde a p_0 . E como $p_0 = q_{k-\ell} \cdot c + r_0$ podemos escrever:

$$\begin{aligned} a &= (q_{k-\ell} \cdot c + r_0) b^{k-\ell} + \sum_{i=0}^{k-\ell-1} a_i b^i = \\ &= q_{k-\ell} \cdot b^{k-\ell} \cdot c + r_0 b^{k-\ell} + \sum_{i=0}^{k-\ell-1} a_i b^i. \end{aligned} \quad (5.7)$$

Operando com o termo $i = k - \ell - 1$ da somatória no último membro de (5.7), chegamos a:

$$\begin{aligned} a &= q_{k-\ell} \cdot b^{k-\ell} c + r_0 \cdot b^{k-\ell} + a_{k-\ell-1} \cdot b^{k-\ell-1} + \sum_{i=0}^{k-\ell-2} a_i b^i = \\ &= q_{k-\ell} \cdot b^{k-\ell} c + r_0 \cdot b^{k-\ell-1} \cdot b + a_{k-\ell-1} \cdot b^{k-\ell-1} + \sum_{i=0}^{k-\ell-2} a_i b^i = \\ &= q_{k-\ell} b^{k-\ell} c + (r_0 b + a_{k-\ell-1}) \cdot b^{k-\ell-1} + \sum_{i=0}^{k-\ell-2} a_i b^i. \end{aligned} \quad (5.8)$$

O termo entre parênteses no último membro de (5.8) corresponde a p_1 . Dado que $p_1 = q_{k-\ell-1} \cdot c + r_1$ obtemos:

$$\begin{aligned}
q &= q_{k-\ell} \cdot b^{k-\ell} \cdot c + (q_{k-\ell-1}c + r_1) \cdot b^{k-\ell-1} + \sum_{i=0}^{k-\ell-2} a_i b^i = \\
&= \left(\sum_{j=k-\ell-1}^{k-\ell} q_j b^j \right) \cdot c + r_1 b^{k-\ell-1} + \sum_{i=0}^{k-\ell-2} a_i b^i.
\end{aligned}$$

Um argumento de indução irá repetir este processo até que todos os termos da somatória $\sum_{i=0}^{k-\ell-1} a_i b^i$ tenham sido operados e revertido para a expressão $\left(\sum_{j=k-\ell-1}^{k-\ell} q_j b^j \right) \cdot c$, com um termo residual. Na penúltima etapa desse processo resta apenas o termo $a_0 b_0$ na primeira somatória, e teremos:

$$\begin{aligned}
a &= \left(\sum_{j=1}^{k-\ell} q_j b^j \right) \cdot c + r_{k-\ell-1} \cdot b + a_0 b^0 = \\
&= \left(\sum_{j=1}^{k-\ell} q_j b^j \right) \cdot c + p_{k-\ell} = \\
&= \left(\sum_{j=1}^{k-\ell} q_j b^j \right) \cdot c + q_0 \cdot c + r_{k-\ell} = \\
&= \left(\sum_{j=0}^{k-\ell} q_j b^j \right) \cdot c + r_{k-\ell} = \\
&= q \cdot c + r.
\end{aligned}$$

Isso conclui a demonstração. □

Exemplo 21. Dado o número $a = 1534$ na base $b = 10$ e o divisor $c = 12$, aplicamos o teorema da divisão.

1. Definindo os números $p_0, q_{k-\ell}, r_0$:

A representação de $a = 1534$ tem 4 dígitos, portanto $k = 3$ (já que o índice começa de 0). A representação de $c = 12$ tem 2 dígitos, então $\ell = 1$. Calculamos p_0 tomando os primeiros $\ell + 1 = 2$ dígitos de a . Aqui, $p_0 = 15$.

$$p_0 = 15.$$

Agora, dividimos p_0 por $c = 12$:

$$q_2 = \left\lfloor \frac{15}{12} \right\rfloor = 1, \quad r_0 = 15 \mod 12 = 3.$$

Agora temos $q_2 = 1$ e $r_0 = 3$.

2. Definindo p_1, q_1, r_1 :

Usamos o valor $r_0 = 3$ e o próximo dígito de a , que é 3, para formar p_1 :

$$p_1 = r_0 \cdot 10 + 3 = 3 \cdot 10 + 3 = 33.$$

Agora, dividimos p_1 por $c = 12$:

$$q_1 = \left\lfloor \frac{33}{12} \right\rfloor = 2, \quad r_1 = 33 \bmod 12 = 9.$$

Então, temos $q_1 = 2$ e $r_1 = 9$.

3. Definindo p_2, q_2, r_2 :

Usamos o valor $r_1 = 9$ e o próximo dígito de a , que é 4, para formar p_2 :

$$p_2 = r_1 \cdot 10 + 4 = 9 \cdot 10 + 4 = 94.$$

Agora, dividimos p_2 por $c = 12$:

$$q_2 = \left\lfloor \frac{94}{12} \right\rfloor = 7, \quad r_2 = 94 \bmod 12 = 10.$$

Então, temos $q_2 = 7$ e $r_2 = 10$.

O número q é a sequência $(q_2 q_1 q_0)_b = (1 \ 2 \ 7)_{10}$. O resto r é $r_2 = 10$.

Portanto, a divisão de $a = 1534$ por $c = 12$ resulta em:

$$1534 \div 12 = 127 \quad \text{com resto} \quad 10.$$

Exemplo 22. Vamos fazer a divisão de dois números na base 7, dividendo $a = (12563)_7$ e o divisor $c = (26)_7$.

1. Definindo os números $p_0, q_{k-\ell}, r_0$:

A representação de $a = (12563)_7$ tem 4 dígitos, portanto $k = 3$ (já que o índice começa de 0). A representação de $c = (26)_7$ tem 2 dígitos, então $\ell = 1$. Calculamos p_0 tomando os primeiros $\ell + 1 = 2$ dígitos de a . Aqui, $p_0 = (12)_7$.

$$p_0 = (12)_7.$$

Agora, dividimos p_0 por $c = (26)_7$:

$$q_3 = \left\lfloor \frac{12}{26} \right\rfloor = 0, \quad r_0 = 12 \mod 26 = 12.$$

Agora temos $q_3 = 0$ e $r_0 = (12)_7$.

2. Definindo p_1, q_1, r_1 :

Usamos o valor r_0 e o próximo dígito de a , que é 5, para formar p_1 :

$$p_1 = r_0 \cdot 7 + 5 = 12 \cdot 7 + 5 = (125)_7.$$

Agora, dividimos $(125)_7$ por $c = (26)_7$:

Testando q_2 :

- para $q_1 = 2 : 2 \cdot (26)_7 = (55)_7$
- para $q_1 = 3 : 3 \cdot (26)_7 = (114)_7$
- para $q_1 = 4 : 4 \cdot (26)_7 = (143)_7$

Logo: $q_1 = 3$

$$r_1 = (125)_7 - (114)_7 = (11)_7$$

3. Definindo p_2, q_0, r_2 :

Usamos o valor r_1 e o próximo dígito de a , que é 6, para formar p_2 :

$$p_2 = r_1 \cdot 7 + 6 = 11 \cdot 7 + 6 = (116)_7.$$

Agora, dividimos $(116)_7$ por $c = (26)_7$:

Testando q_2 :

- para $q_0 = 2 : 2 \cdot (26)_7 = (55)_7$
- para $q_0 = 3 : 3 \cdot (26)_7 = (114)_7$
- para $q_0 = 4 : 4 \cdot (26)_7 = (143)_7$

Logo: $q_0 = 3$

$$r_2 = (116)_7 - (114)_7 = (2)_7$$

O número q é a sequência $(q_2 q_1 q_0)_b = (0 \ 3 \ 3)_7$. O resto r é $r_2 = 2$.

Portanto, a divisão de $a = (1256)_7$ por $c = (26)_7$ resulta em:

$$(1256)_7 \div (26)_7 = (033)_7 \quad \text{com resto } 2.$$

RAIZ QUADRADA

Neste capítulo, apresentaremos a definição formal de raiz quadrada inteira, acompanhada de proposições que garantem sua existência e unicidade. Em seguida, construiremos e demonstraremos um algoritmo geral para o cálculo da raiz quadrada em qualquer base b , destacando a validade de cada etapa e exemplificando sua aplicação prática.

Estamos acostumados com o conceito de "raiz quadrada" de um dado número α , como sendo um número β , que multiplicado por ele mesmo, forma o número dado,

$$\beta \times \beta = \beta^2 = \alpha.$$

Por exemplo, a raiz quadrada de 36 é 6, pois $6 \times 6 = 36$, e a raiz quadrada de 289 é 17, pois $17^2 = 289$.

Nesses exemplos, tanto o número como a sua raiz quadrada são inteiros. Este não é o caso mais comum, como se vê facilmente: os números 2, 3, 5, 8, 12, 24, 30, ... não possuem raízes quadradas inteiras, (tais números possuem raízes quadradas não exatas, mas não aprofundaremos esse assunto aqui). Não obstante, também torna-se interessante associar também a esse uma raiz quadrada aproximada, e inteira. Chamaremos a estas, assim como no caso das raízes quadradas exatas, de raiz quadrada, por simplicidade.

Definição 5. Seja a um número inteiro não negativo. A raiz quadrada de a é o maior número inteiro c com a propriedade:

$$c^2 \leq a < (c + 1)^2. \quad (6.1)$$

Proposição 5. Todo número inteiro não negativo possui uma única raiz quadrada.

Demonstração. Primeiramente vamos provar que a raiz existe.

Seja a um número inteiro não negativo ($a \geq 0$). Precisamos mostrar que existe um número inteiro c que verifica a relação (6.1).

Considere o conjunto $A = \{n \in \mathbb{Z} \mid n \geq 0 \text{ e } n^2 \leq a\}$. Esse conjunto é não vazio pois $0 \in A$. Argumentamos que ele é finito. Isto porque se $n^2 \leq a$ então $n \leq a$, uma vez que qualquer número inteiro é menor ou igual ao seu quadrado. Então $A \subset \{0, 1, 2, \dots, a\}$, o qual é finito.

Seja c o maior elemento de A . Então $c^2 \leq a$ e $(c+1)^2 > a$, pois $c+1 \notin A$. Assim:

$$c^2 \leq a < (c+1)^2,$$

o que prova que c é a raiz quadrada de a . A unicidade decorre do fato de que todo conjunto finito e não vazio tem um único maior elemento.

□

Proposição 6. Seja a um número não negativo e c sua raiz quadrada. Dado q um número qualquer com $0 \leq q < b^2$, define-se:

$$r = (a - c^2) \cdot b^2 + q. \quad (6.2)$$

Seja p o maior número tal que

$$p^2 + 2pbc \leq r. \quad (6.3)$$

Então $(bc + p)$ é a raiz quadrada de $ab^2 + q$ e p tem 1 dígito.

Demonstração. Expandindo $(bc + p)^2$ e usando a inequação (6.3), obtemos:

$$(bc + p)^2 = b^2c^2 + 2pbc + p^2 \leq b^2c^2 + r.$$

Da definição de r em (6.2), segue:

$$\begin{aligned} (bc + p)^2 &\leq b^2c^2 + (a - c^2)b^2 + q = \\ (bc + p)^2 &\leq b^2c^2 + ab^2 - c^2b^2 + q = ab^2 + q \end{aligned} \quad (6.4)$$

Mostremos que (6.4) não pode ser satisfeita se incrementarmos uma unidade em p .

Suponha, do contrário, que:

$$(bc + p + 1)^2 \leq ab^2 + q. \quad (6.5)$$

Então,

$$\begin{aligned}
&= b^2c^2 + 2bc(p+1) + (p+1)^2 \leq ab^2 + q \\
&\Rightarrow b^2c^2 + 2(p+1)bc + (p+1)^2 \leq ab^2 + q.
\end{aligned}$$

Da expressão acima, chegamos em

$$(p+1)^2 + 2(p+1)bc \leq ab^2 + q - b^2c^2 = (a - c^2)b^2 + q = r, \quad (6.11)$$

o que contradiz o fato de que p é o maior número que verifica a inequação (6.3). Para evitar essa contradição, devemos negar a hipótese (6.5), ou seja, deve ser.

$$(bc + p + 1)^2 > ab^2 + q. \quad (6.6)$$

As condições (6.4) e (6.6) equivalem a ser $(bc + p)$ a raiz quadrada de $ab^2 + q$.

Sabemos que p tem apenas 1 dígito e $0 \leq p \leq b - 1$, então vamos assumir por absurdo que $p \geq b$, desta forma temos

$$(bc + p)^2 \geq (bc + b)^2 = b^2(c + 1)^2.$$

Como $(bc + p)^2 \leq ab^2 + q$, obtemos

$$\begin{aligned}
b^2(c + 1)^2 &\leq ab^2 + q. \\
\Rightarrow b^2((c + 1)^2 - a) &\leq q.
\end{aligned} \quad (6.7)$$

A última desigualdade em (6.7) expressa uma contradição. Seu primeiro membro é maior ou igual a b^2 , já que $(c + 1)^2 - a$ é maior ou igual a 1 (lembre que c é a raiz quadrada de a). Seu segundo membro é menor que b^2 , pois essa é a hipótese sobre q . Tal contradição só pode ser evitada se $p \leq b$, logo p tem 1 dígito.

□

6.1 Algoritmo da Raiz Quadrada

Teorema 8. Seja a um número não-negativo. Representamos a com um número par de dígitos, $a = (a_{2k-1}a_{2k-2} \dots a_1a_0)_b$.

Fazemos $r_1 = (a_{2k-1}a_{2k-2})_b$, e c_{k-1} a raiz quadrada de r_1 . Para $2 \leq i \leq k$, definimos:

$$r_i = \left(r_{i-1} - c_{k-i+1}^2 - 2c_{k-i+1} \cdot b \cdot \left(\sum_{j=1}^{i-2} c_{k-j} \cdot b^{i-2-j} \right) \right) b^2 + (a_{2k-2i+1}a_{2k-2i})_b, \quad (6.8)$$

e c_{k-i} é o maior número tal que

$$c_{k-i}^2 + 2 \cdot c_{k-i} \cdot b \cdot \left(\sum_{j=1}^{i-1} c_{k-j} b^{i-1-j} \right) \leq r_i. \quad (6.9)$$

Então, para cada $1 \leq i \leq k$, o número c_{k-i} tem 1 dígito. E o número c cuja expressão na base b é $c = (c_{k-1}c_{k-2} \dots c_0)_b$ é a raiz quadrada de a . Vale também:

$$a - c^2 = r_k - c_0^2 - 2c_0b \sum_{j=1}^{k-1} c_{k-j} b^{k-1-j}. \quad (6.10)$$

Demonstração. Vamos mostrar que, para todo $1 \leq i \leq k$, o número $\alpha_i = \sum_{j=1}^i c_{k-j} b^{i-k}$ é a raiz quadrada de $(a_{2k-1}a_{2k-2} \dots a_{2k-2i})_b$. Como conclusão, obtemos que cada c_{k-i} é um dígito.

Para $i = 1$, $\alpha_1 = c_{k-1}$ e é a raiz quadrada de $(a_{2k-1}a_{2k-2})_b$, pela definição como r_1 tem (até) 2 dígitos, é fácil ver que c_{k-1} tem 1 dígito.

Antes de prosseguir, notamos que a expressão dentro dos parênteses mais amplo na primeira parcela do segundo membro de (6.8) é maior ou igual a zero. Isso decorre diretamente da definição de c_{k-i+1} em (6.9), usando $(i-1)$ no lugar de i . A importância disto é garantir que $r_i \geq 0$, e portanto, c_{k-1} está bem definido.

Vamos agora mostrar uma identidade que permitirá aplicar diretamente a proposição (6). Para todo $1 \leq i \leq k$ vale:

$$r_i - c_{k-1}^2 - 2c_{k-1} \cdot b \cdot \alpha_{i-1} = (a_{2k-1}a_{2k-2} \dots a_{2k-2i})_b - \alpha_i^2. \quad (6.11)$$

Esta identidade é verdadeira no caso $i = 1$, pois $r_1 - c_{k-1}^2 = (a_{2k-1} + a_{2k-2})_b - \alpha_1^2$ (tomamos aqui $\alpha_0 = 0$), o que é compatível com a definição de α_i ; dada pela somatória no início da demonstração.

Para $2 \leq i \leq k$ assuma que (6.11) é válida para $i-1$. Então, usando (6.8).

$$\begin{aligned} r_i - c_{k-i}^2 - 2c_{k-i} \cdot b \cdot \alpha_{i-1} &= \\ &= (r_{i-1} - c_{k-i+1}^2 - 2c_{k-i+1}b\alpha_{i-2})b^2 + (a_{2k-2i+1}a_{2k-2i})_b - c_{k-i}^2 - 2c_{k-i}b\alpha_{i-1}. \end{aligned} \quad (6.12)$$

Agora substituindo (6.11) para $i-1$ temos

$$\begin{aligned} &= ((a_{2k-1}a_{2k-2} \dots a_{2k-2i+2})_b - \alpha_{i-1}^2) b^2 + (a_{2k-2i+1}a_{2k-2i})_b - c_{k-i}^2 - 2c_{k-i}b\alpha_{i-1} = \\ &= (a_{2k-1}a_{2k-2} \dots a_{2k-2i+2})_b b^2 - \alpha_{i-1}^2 b^2 + (a_{2k-2i+1}a_{2k-2i})_b - c_{k-i}^2 - 2c_{k-i}b\alpha_{i-1} = \\ &= b^2(a_{2k-1}a_{2k-2} \dots a_{2k-2i+2})_b + (a_{2k-2i+1}a_{2k-2i})_b - (b^2\alpha_{i-1}^2 + 2c_{k-i}b\alpha_{i-1} + c_{k-1}^2). \end{aligned} \quad (6.13)$$

A soma das 2 primeiras parcelas do último membro de (6.13) é claramente $(a_{2k-1}a_{2k-2} \dots a_{2k-2i})_b$, enquanto a última parcela é igual a $-(c_{k-i} + b\alpha_{i-1})^2 = -\alpha_i^2$.

Assim mostramos que se (6.11) é válida para $i-1$, também é válida para i . O argumento da indução implica que (6.11) vale para $1 \leq i \leq k$.

Aplicando (6.11) à definição de r_i em (6.8), obtemos para $i \geq 2$

$$r_i = ((a_{2k-1}a_{2k-2} \dots a_{2k-2i+2})_b - \alpha_{i-1}^2) b^2 + (a_{2k-2i+1}a_{2k-2i})_b.$$

O número r_i estará nas condições do número r na proposição (6) dado que α_{i-1} seja raiz quadrada de $(a_{2k-1}a_{2k-2} \dots a_{2k-2i+2})_b$. Neste caso, a proposição nos garante que o maior número p com $p^2 + 2pb\alpha_{i-1} \leq r_i$ tem um dígito, e $(b\alpha_{i-1} + p)$ é raiz quadrada de $(a_{2k-1}a_{2k-2} \dots a_{2k-2i+2})_b b^2 + (a_{2k-2i+1}a_{2k-2i})_b = (a_{2k-1}a_{2k-2} \dots a_{2k-2i+2})_b$. Mas $p = c_{k-i}$ pela definição (6.9). E como $b\alpha_{i-1} + c_{k-i} = \alpha_i$, concluímos que se α_{i-1} é a raiz quadrada de $(a_{2k-1}a_{2k-2} \dots a_{2k-2i+2})_b$ então c_{k-i} tem um dígito e α_i é raiz quadrada de $(a_{2k-1}a_{2k-2} \dots a_{2k-2i})_b$. Já provamos no início da demonstração que c_{k-1} tem 1 dígito e é raiz de $(a_{2k-1}a_{2k-2})_b$, logo o princípio da indução finita conclui o argumento acima desenvolvido fornece que $\alpha_i = \sum_{j=1}^i c_{k-j} b^{i-j}$ é a raiz quadrada de $(a_{2k-1}a_{2k-2} \dots a_{2k-2i})_b$ e c_{k-i} é um dígito para todo $1 \leq i \leq k$.

Em particular, o número $\alpha_k = \sum_{j=1}^k c_{k-j} b^{k-j}$ é a raiz quadrada de $(a_{2k-1}a_{2k-2} \dots a_0)_b = a$.

Esse número é expresso na base b como $\alpha_k = (c_{k-1}c_{k-2} \dots c_1c_0)_b = c$. Por fim, a afirmação (6.10) é uma aplicação de (6.11) para $i = k$. Isso conclui a demonstração. $\square$

Exemplo 23. Vamos calcular a raiz quadrada aproximada de $a = 15227$ seguindo o método descrito no teorema. Para isso, vamos usar a base $b = 10$ e seguir os passos do algoritmo.

O número $a = 15227$ deve ser representado na base $b = 10$ com um número par de dígitos, como a tem 5 dígitos, adicionamos um zero à esquerda:

$$a = 015227$$

Agora, a tem 6 dígitos, que é um número par. Como $2k$ é a quantidade de dígitos do número $k = 3$

O número a é dividido em pares de dígitos:

$$a = 01' 52' 27$$

- Definição de r_1 e c_{k-1}

O primeiro par é:

$$r_1 = 01$$

Agora, c_{k-1} é a raiz quadrada de r_1 :

$$c_{k-1} = \sqrt{1} = 1$$

- Cálculo de r_2 e c_{k-2} Usamos a fórmula:

$$r_2 = (r_1 - c_{k-1}^2) \cdot b^2 + (a_{2k-3}a_{2k-4})_{10}$$

Substituindo os valores:

$$r_2 = (1 - 1^2) \cdot 10^2 + (52)_{10} = (0) \cdot 100 + 52 = 52$$

Agora, determinamos c_{k-2} :

$$c_{k-2}^2 + 2 \cdot c_{k-2} \cdot 10 \cdot c_{k-1} \leq r_2$$

Substituindo $c_{k-1} = 1$:

$$c_{k-2}^2 + 20c_{k-2} \leq 52$$

Testando valores:

- Se $c_{k-2} = 1$: $1^2 + 20 \times 1 = 1 + 20 = 21 \leq 52$
- Se $c_{k-2} = 2$: $2^2 + 20 \times 2 = 4 + 40 = 44 \leq 52$
- Se $c_{k-2} = 3$: $3^2 + 20 \times 3 = 9 + 60 = 69 > 52$

Portanto, $c_{k-2} = 2$.

- Cálculo de r_3 e c_{k-3} Agora, calculamos r_3 :

$$r_3 = (r_2 - c_{k-2}^2 - 2 \cdot c_{k-2} \cdot 10 \cdot c_{k-1}) \cdot 10^2 + (a_{2k-5}a_{2k-6})_{10}$$

Substituindo os valores:

$$r_3 = (52 - 2^2 - 2 \cdot 2 \cdot 10 \cdot 1) \cdot 100 + 27$$

$$r_3 = (52 - 4 - 40) \cdot 100 + 27 = 8 \cdot 100 + 27 = 827$$

Agora, determinamos c_{k-3} :

$$c_{k-3}^2 + 2 \cdot c_{k-3} \cdot 10 \cdot (c_{k-1} \cdot 10 + c_{k-2}) \leq r_3$$

Substituindo $c_{k-2} = 2$ e $c_{k-1} = 1$:

$$c_{k-3}^2 + 2 \cdot c_{k-3} \cdot 10 \cdot 12 \leq 827$$

$$c_{k-3}^2 + 240c_{k-3} \leq 827$$

Testando valores:

- Se $c_{k-3} = 1$: $1^2 + 240 \times 1 = 1 + 240 = 241 \leq 827$
- Se $c_{k-3} = 2$: $2^2 + 240 \times 2 = 4 + 480 = 484 \leq 827$
- Se $c_{k-3} = 3$: $3^2 + 240 \times 3 = 9 + 720 = 729 \leq 827$
- Se $c_{k-3} = 4$: $4^2 + 240 \times 4 = 16 + 960 = 976 > 827$

Portanto, $c_{k-3} = 3$.

Vamos calcular o resto do algoritmo:

$$r = (r_3 - c_{k-3}^2 - 2 \cdot c_{k-3} \cdot 10 \cdot (c_{k-1} \cdot 10 + c_{k-2}))$$

Substituindo os valores:

$$r = (827 - 3^2 - 2 \cdot 3 \cdot 10 \cdot 12)$$

$$r = 827 - 9 - 720 = 98$$

.

Então encontramos que a raiz quadrada de 15227 é a sequência formada por $c_{k-1} \cdot 10^2 + c_{k-2} \cdot 10 + c_{k-3} = 123$ com resto 98

$$\sqrt{15227} \approx 123$$

.

O exemplo acima pode ser descrito pelo diagrama abaixo.

$\sqrt{01'52'27}$	1 2 3
0 5 2	$\alpha^2 + 2\alpha \cdot 10 \cdot 1 \leq 52$
- 4 4	$\alpha = 2$
8 2 7	$2^2 + 2 \cdot 2 \cdot 10 \cdot 1 \leq 52$
- 7 2 9	$44 \leq 52$
9 8	$\alpha^2 + 2\alpha \cdot 10 \cdot 12 \leq 827$
	$\alpha = 3$
	$3^2 + 2 \cdot 3 \cdot 10 \cdot 12 \leq 827$
	$729 \leq 827$

Exemplo 24. Vamos calcular a raiz quadrada aproximada de $a = 32564$ seguindo o método descrito no teorema. Para isso, vamos usar a base $b = 10$ e seguir os passos do algoritmo.

O número $a = 32564$ deve ser representado na base $b = 10$ com um número par de dígitos. Como a tem 5 dígitos, adicionamos um zero à esquerda:

$$a = 032564$$

Agora, a tem 6 dígitos, que é um número par. Como $2k$ é a quantidade de dígitos, temos $k = 3$.

O número a é dividido em pares de dígitos:

$$a = 03' 25' 64$$

• **Definição de r_1 e c_{k-1}**

O primeiro par é:

$$r_1 = 03$$

Agora, c_{k-1} é a raiz quadrada inteira de r_1 :

$$c_{k-1} = \lfloor \sqrt{3} \rfloor = 1$$

• **Cálculo de r_2 e c_{k-2}**

Usamos a fórmula:

$$r_2 = (r_1 - c_{k-1}^2) \cdot b^2 + a_{2k-3}a_{2k-4}$$

Substituindo os valores:

$$r_2 = (3 - 1^2) \cdot 10^2 + 25 = (2) \cdot 100 + 25 = 225$$

Agora, determinamos c_{k-2} :

$$c_{k-2}^2 + 2 \cdot c_{k-2} \cdot 10 \cdot c_{k-1} \leq r_2$$

Substituindo $c_{k-1} = 1$:

$$c_{k-2}^2 + 20c_{k-2} \leq 225$$

Testando valores:

- Se $c_{k-2} = 7$: $7^2 + 20 \cdot 7 = 49 + 140 = 189 \leq 225$
- Se $c_{k-2} = 8$: $8^2 + 20 \cdot 8 = 64 + 160 = 224 \leq 225$
- Se $c_{k-2} = 9$: $9^2 + 20 \cdot 9 = 81 + 180 = 261 > 225$

Portanto, $c_{k-2} = 8$.

- **Cálculo de r_3 e c_{k-3}**

Agora, calculamos r_3 :

$$r_3 = (r_2 - c_{k-2}^2 - 2 \cdot c_{k-2} \cdot 10 \cdot c_{k-1}) \cdot 10^2 + a_{2k-5}a_{2k-6}$$

Substituindo os valores:

$$r_3 = (225 - 8^2 - 2 \cdot 8 \cdot 10 \cdot 1) \cdot 100 + 64$$

$$r_3 = (225 - 64 - 160) \cdot 100 + 64 = 1 \cdot 100 + 64 = 164$$

Agora, determinamos c_{k-3} :

$$c_{k-3}^2 + 2 \cdot c_{k-3} \cdot 10 \cdot (c_{k-1} \cdot 10 + c_{k-2}) \leq r_3$$

Substituindo $c_{k-1} = 1$ e $c_{k-2} = 8$:

$$c_{k-3}^2 + 2 \cdot c_{k-3} \cdot 10 \cdot 18 \leq 164$$

$$c_{k-3}^2 + 360c_{k-3} \leq 164$$

Testando valores:

$$\text{– Se } c_{k-3} = 0: \quad 0^2 + 360 \cdot 0 = 0 \leq 164$$

$$\text{– Se } c_{k-3} = 1: \quad 1^2 + 360 \cdot 1 = 1 + 360 = 361 > 164$$

Portanto, $c_{k-3} = 0$.

- **Cálculo do resto final**

$$r = (r_3 - c_{k-3}^2 - 2 \cdot c_{k-3} \cdot 10 \cdot (c_{k-1} \cdot 10 + c_{k-2}))$$

Substituindo $c_{k-3} = 0$:

$$r = 164 - 0^2 - 2 \cdot 0 \cdot 180 = 164$$

Assim, encontramos que a raiz quadrada de 32564 é:

$$c_{k-1} \cdot 10^2 + c_{k-2} \cdot 10 + c_{k-3} = 1 \cdot 100 + 8 \cdot 10 + 0 = 180$$

$$\sqrt{32564} \approx 180 \quad \text{com resto } 164.$$

CONCLUSÃO

Iniciamos nosso estudo sobre o surgimento dos números e a evolução dos sistemas de numeração. Essa contextualização histórica foi essencial para entender como a humanidade criou métodos para contar e calcular, resultando no sistema numérico que utilizamos hoje. Além disso, abordamos com mais detalhes o sistema de numeração e a representação de um número na base b que foi essencial para as demonstrações posteriores. Depois, exploramos e justificamos os algoritmos das operações básicas adição, subtração, multiplicação e divisão em uma base b , provando que eles não são apenas regras impostas a serem seguidas, mas um fundamento matemático sólido. Essa abordagem ajudou a entender que os princípios matemáticos por trás das operações são os mesmos e podem ser aplicados com eficácia em qualquer tipo de sistema de numeração. Além disso fizemos uma ligação de cada algoritmo com os diagramas e cálculos ensinados em sala de aula, mostrando porque cada etapa e regra deve ser seguida para obter um resultado correto.

Um ponto de destaque deste trabalho foi a apresentação de um algoritmo para o cálculo da raiz quadrada que, embora menos conhecido, mostrou-se eficiente e matematicamente correto. Esse algoritmo nos mostra que embora alguns cálculos pareçam ser complexos e trabalhosos eles podem ser simplificados, evidenciando a importância do cálculo mental como um poderoso método para otimizar processos e tornar os cálculos mais rápidos e simples.

Por fim esse trabalho mostra a importância de ensinar com métodos que considere não só a memorização de passos e etapas, mas também entender ideias. Ao explicar cada regra dos algoritmos em uma base qualquer, tentamos dar aos professores e alunos ferramentas para uma aprendizagem mais útil e flexível, que pode ser usada em vários lugares.

Como desdobramento futuro, sugere-se a exploração de aplicações práticas dentro da sala de aula para que o aluno entenda porque está realizando determinado cálculo, assim como a lógica e o raciocínio por trás de cada algoritmo, melhorando assim o aprendizado e o aprimorando o uso do cálculo mental em contextos específicos do seu dia a dia, tornando a matemática mais

aplicável e interessante.

REFERÊNCIAS

MUNDO EDUCAÇÃO. Sistema de numeração maia. Disponível em: <https://mundoeducacao.uol.com.br/sistema-numeracao-maia.htm>. Acesso em: 3 abr. 2024.

MUNDO EDUCAÇÃO. Sistema de numeração. Disponível em: <https://mundoeducacao.uol.com.br/mundoeducacao/numeracao.htm>. Acesso em: 3 abr. 2024.

PORTAL PEDAGÓGICO. Quem criou a Matemática? Disponível em: <https://portalpedagogico.com.br/quem-criou-a-matematica>. Acesso em: 3 abr. 2024.

MATTOS, João Ricardo da Costa. História da Matemática: uma abordagem crítica e epistemológica. São Paulo: Livraria da Física, 2008.

MATTOS, Eliezer Eustáquio de. História da matemática: uma visão crítica, desfazendo mitos e lendas. São Paulo: Livraria da Física, 2008.

GARDNER, David Wells. O dicionário Penguin de números curiosos e interessantes. Tradução de Vera Ribeiro. Rio de Janeiro: Jorge Zahar Editor, 1999.

IFRAH, Georges. Os números: A história de uma grande invenção. 2. ed. Rio de Janeiro: Record, 2001.

TEIXEIRA, Martins R. Contando com outros povos: sistemas de numeração. São Paulo: FTD, 1998.

SANTOS, José Plínio de Oliveira. **Introdução à Teoria dos Números**. Brasília: Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), 1998.

MILIES, C. P.; COELHO, S. P. **Números: Uma Introdução à Matemática**. São Paulo: Editora da Universidade de São Paulo (EDUSP), 2001.

MACHADO, N. J. **Matemática na Escola: Conteúdo e Forma**. São Paulo: Editora Scipione, 1993.

ALENCAR FILHO, E. **Teoria Elementar dos Números**. São Paulo: Nobel, 1996.

SILVA, C. M. **O Algoritmo da Raiz Quadrada**. Revista do Professor de Matemática (RPM), n. 2, p. 7, 1983. Disponível em: <<https://rpm.org.br/cdrpm/2/7.htm>>. Acesso em: 10 jan. 2025.

CARVALHO, J. B. P. **Algoritmos de Operações Aritméticas: Uma Abordagem Histórica e Didática**. Revista do Professor de Matemática (RPM), n. 49, p. 1-10, 2002.

DANTE, L. R. **Matemática: Contexto e Aplicações**. São Paulo: Editora Ática, 2009.

HEFEZ, Abramo. **Aritmética**. Rio de Janeiro: Sociedade Brasileira de Matemática (SBM), 2016. (Coleção PROFMAT). Disponível em: <https://loja.sbm.org.br/media/invate/product_attachment/Sum_rio__Aritm_tica.pdf>. Acesso em: 10 jun. 2024.

SILVA, A. O.; VILLELA, L. M. A. **A evolução dos algoritmos das operações aritméticas ao longo da história**. In: XII Encontro Nacional de Educação Matemática, 2016, São Paulo. *Educação Matemática na Contemporaneidade: desafios e possibilidades*. São Paulo: [s.n.], 2016. Disponível em: <https://www.sbemrasil.org.br/enem2016/anais/pdf/8264_4092_ID.pdf>. Acesso em: 15 mai. 2024.

SANTANA, G. S. **Algoritmos utilizados para as quatro operações elementares**. Dissertação (Mestrado) - Universidade Federal de Goiás, Programa de Pós-Graduação em Matemática, Goiânia, 2016.

DANTAS, Luiz Márcio Imenes; LELLIS, Marcelo. **A História da Matemática na Sala de Aula**. São Paulo: Atual, 1998.

