UNIVERSIDADE FEDERAL DE ALAGOAS

Mestrado Profissional em Matemática em Rede Nacional

PROFMAT

DISSERTAÇÃO DE MESTRADO

O Algoritmo do Par Binário:

Um estudo da representação decimal do quociente

$$a/2^n,\ a \in \mathbb{R} \text{ e } n \in \mathbb{N}^*$$

José Elizângelo Lopes Luna

Instituto de Matemática

Maceió, Abril de 2013

PROFMAT

UNIVERSIDADE FEDERAL DE ALAGOAS

INSTITUTO DE MATEMÁTICA

O Algoritmo do Par Binário:

Um estudo da Representação decimal do quociente

$a/2^n, a \in \mathbb{R}$ e $n \in \mathbb{N}^*$

José Elizângelo Lopes Luna

Dissertação apresentada ao programa de Mestrado Profissional em Matemática em Rede Nacional, coordenado pela Sociedade Brasileira de Matemática e ofertado pelo Instituto de Matemática da Universidade Federal de Alagoas como requisito parcial para obtenção do grau de mestre em matemática.

Banca Examinadora:

Prof. Dr. André Luiz Flores (Orientador - UFAL)

Prof. Dr. Ediel Azevedo Guerra (UFAL)

Prof. Dr Givaldo Oliveira dos Santos (IFAL)

Catalogação na fonte
Universidade Federal de Alagoas
Biblioteca Central
Divisão de Tratamento Técnico
Bibliotecária Responsável: Fabiana Camargo dos Santos

L961a Luna, José Elizângelo Lopes.
O algoritmo do par binário : um estudo da representação decimal do quociente $a/2^n$, $a \in R$ e $n \in N^*$ / José Elizângelo Lopes Luna. – 2013.
119 f.

Orientador: André Luiz Flores.
Dissertação (Mestrado profissional em Matemática em Rede Nacional) – Universidade Federal de Alagoas. Instituto de Matemática. Maceió, 2013.

Bibliografia: f. 118-119.

1. Representação decimal. 2. Quociente divisor 2. 3. Par binário. 4. Matemática – Ensino. I. Título.

CDU: 511

Aos meus pais, José Lopes de Luna e Maria Rosa Lopes Luna, por me guiarem desde cedo pelo caminho da verdade e sabedoria. A eles nunca serei suficientemente grato.

Agradecimentos

Agradeço a Deus, que em sua infinita misericórdia me deu forças para superar as limitações que me impediam de chegar até aqui: *Gratias agimus tibi propter magnam gloriam tuam sempiterne omnipotens Dei Sancti*!

Aos meus pais, meus irmãos Rejane, Rolângela e Mário e meus sobrinhos, especialmente Lívia e Letícia, e aos amigos que tanto me apoiaram nessa fase de minha vida, em especial, Adelmo Camilo, Joyce Cardoso, Vanderléia Paes, Adilma Lopes e Jéssica Santos.

Aos meus colegas e ex-colegas de trabalho, em especial, os Professores Mário Gama, Márcio Soares, Iran Carvalho, Cleyton Almeida, Fábio Henrique e Valdiran Souza, verdadeiros amigos com quem pude contar em diversos momentos difíceis.

Ao Prof. Dr. André Luiz Flores, pela valiosa orientação e paciência inabalável; em suas aulas pude reavivar o entusiasmo pela Álgebra e Teoria dos Números.

Ao Prof. Dr. Ediel Guerra e Prof. Dr. Givaldo Oliveira, pelas importantes sugestões para o enriquecimento deste trabalho.

Ao grande amigo e Prof. Vicente Bezerra Filho, da UPE, com quem aprendi não apenas a amar a matemática, mas também, e sobretudo, a amar ser professor.

Ao Prof. Dr. Paulo Figueiredo de Lima, da UFPE, que há dez anos atrás me encorajou a lutar pelo sonho do mestrado. Jamais esquecerei a confiança que depositou em mim.

A todos os professores do PROFMAT- UFAL, de maneira especial aos professores Ediel Guerra, Fernando Micena, Marcus Bronzi e André Contiero. Levarei comigo o grande exemplo de Matemáticos e seres humanos que mostraram ser ao longo do curso.

Aos meus ex-alunos e ex-integrantes do Programa de Qualificação Discente em Matemática de Nível Médio da EREM Francisco Pereira da Costa e do Programa NEPSO: Vaniele Barros, Edjane Pereira, Marta Michelly, Edlânia Félix, Francielly Bezerra e Ramón Miranda, atualmente alunos da graduação em Matemática da Universidade de Pernambuco- UPE, com quem tive a primeira oportunidade de compartilhar as ideias que aqui exponho.

A Camila Martinez Toledo, aluna do Programa NEPSO- Polo Chile e do *Programa Educacional para Niños, Niñas y Jóvenes con Talentos Académicos de la Universidad de La Frontera* (PROENTA-UFRO), pela preciosa ajuda na língua espanhola.

Aos colegas alagoanos do PROFMAT, que me receberam em seu Estado e não pouparam esforços para que eu e os demais colegas de Pernambuco nos sentíssemos em casa.

Aos colegas e amigos pernambucanos Paulo Sérgio e Alex Gomes com quem pude compartilhar mais de perto as dificuldades desses dois anos, e com o apoio de quem as pude superar.

À CAPES, pelo apoio financeiro.

"Deus criou os números naturais. Todo o resto é obra do Homem."

—L. KRONECKER (1823-1891)

Resumo

No contexto tradicional, a unívoca determinação do quociente e do resto da divisão euclidiana se faz por meio de algoritmos baseados na determinação de aproximações máximas do dividendo pelo produto entre o divisor e o número candidato a quociente, e então pela diferença entre a aproximação dada e o dividendo original, num processo permeado pela obtenção de quocientes parciais, obtidos considerando-se grupos convenientes de dígitos do dividendo, tomados no sentido da maior para a menor ordem. No caso específico do divisor 2, é possível desviar o processo de cálculo dessa recorrência clássica, mediante o definir de uma função que relaciona cada algarismo do dividendo ao seu congênere de mesma ordem no quociente. Neste trabalho provamos a existência de tal função definida em $\mathbb{Z}_2 \times \{0,1,2,3,4,5,6,7,8,9\}$, que usaremos chamar de "Função par binário", ao tempo que oferecemos uma contribuição adicional ao estudo das regularidades da representação decimal no contexto da divisão pelos inteiros na forma 2^n, com $n \in \mathbb{N}$ e, extensivamente, $2^n \cdot 10^m$ com $m \in \mathbb{Z}$. Adicionalmente, expomos aplicações aritméticas da técnica exposta, dentre as quais é destacada a relação entre as bases binária e decimal, e propomos, como produto de nosso trabalho, uma sequência didática na qual o sistema binário de numeração em $\mathbb{Z}$ é introduzido de maneira lúdica com o conhecido jogo matemático "Matemágica dos cartões numerados", cujo funcionamento fundamenta-se na conversão binária das expressões decimais dos números inteiros.

Palavras-chave: <REPRESENTAÇÃO DECIMAL. DIVISOR 2. PAR BINÁRIO.>

Abstract

In the traditional context, the unequivocal determination of the quotient and the remainder of the Euclidean division takes place by means of algorithms based approaches in determining the maximum dividend by the product of the divisor and quotient candidate number, then the difference between the approach and the dividend paid original, a process permeated by obtaining partial quotients obtained considering convenient groups of digits of the dividend taken in order from largest to smallest order. In the specific case of the divider 2, you can bypass the process of calculating this recurrence classic, by defining a function that relates each digit of the dividend to its counterpart of the same order in the quotient. In this paper we prove the existence of such a function defined on $\mathbb{Z}_2 \times \{0,1,2,3,4,5,6,7,8,9\}$, we use to call "function binary pair"to time we offer an additional contribution to the study of the regularities of the decimal representation in the context of the division by integers of the form 2^n, with $n \in \mathbb{N}$ and, extensively, $2^n \cdot 10^m$ with $m \in \mathbb{Z}$. Additionally, we expose arithmetic applications of the binary pair algorithm, among which highlight the relationship between binary and decimal bases, and propose, as a product of this work, a didactic sequence about the binary numbering system on $\mathbb{Z}$ in playful way with the known mathematical game "Matemágica dos cartões numerados", whose operation is based on the conversion of binary decimal expressions of integers.

Keywords: <DECIMAL REPRESENTATION. DIVIDER 2. BINARY PAIR>

Sumário

1 INTRODUÇÃO 12

2 NOÇÕES ELEMENTARES DA TEORIA DOS NÚMEROS 16

2.1 Sistema de Numeração Decimal 16

2.2 Divisibilidade 21

2.3 Congruências 23

2.4 Classes de restos 27

3 O ALGORITMO DO PAR BINÁRIO EM $\mathbb{Z}$ 29

3.1 Motivação 29

3.2 O Algoritmo do Par binário: Enunciado e Exemplos 30

3.3 Demonstração do Algoritmo do par binário 36

4 O ALGORITMO DO PAR BINÁRIO EM $\mathbb{R}$ 45

4.1 Expressões decimais de números reais 45

4.2 O Algoritmo do Par Binário para dividendos reais quaisquer 51

4.2.1 Dividendos que admitem representação decimal finita 51

4.2.2 Dividendos expressos em representação decimal infinita 54

5 ITERAÇÃO DE QUOCIENTES 60

5.1 Quocientes Iterados 60

5.2 Par Binário Composto 62

5.3 Matriz associada a um dividendo 66

5.4 Matriz do dividendo inteiro 68

5.4.1 Divisão euclidiana por 2^n 68

5.5 Matriz complementar do dividendo inteiro 73

5.5.1 Redutibilidade de quocientes 73

5.5.2 Parte Fracionária de um Quociente Irredutível 76

5.6 Construção da Matriz do Dividendo Inteiro 82

5.7 Dividendos Reais Quaisquer 85

5.7.1 Forma Produto de um Quociente 85

5.7.2 Matriz Inteira Associada a Dízimas Infinitas 87

6 APLICAÇÕES 89
6.1 Sobre o Uso do Presente Trabalho na Escola Básica 89
6.2 Representação Binária de um Inteiro Dado na Base Decimal 90
6.3 Representação Decimal de Expressões Binárias Finitas 93
6.4 Representação Binária de Quocientes do tipo $q = \frac{a}{2^n},\ a \in \mathbb{Z}, n \in \mathbb{N}^*$ 97
6.5 Aplicações com a Forma Produto 103

7 PROPOSTA DE SEQUÊNCIA DIDÁTICA: JOGO DOS CARTÕES NUMERADOS 107
7.1 Descrição e Regras 107
7.2 O Segredo 107
7.3 Análise do Jogo 109
7.4 Construção dos Cartões 109
7.5 Sequência didática 113
Objetivo 113
Público-alvo 113
Metodologia e Tempo Pedagógico 113
Avaliação 114

1 INTRODUÇÃO

Possuem considerável valor na matemática os resultados relacionados à relação de divisibilidade dos inteiros e à divisão com resto, conceitos fundamentais da Teoria dos Números que derivam do teorema milenar conhecido como *Algoritmo da divisão de Euclides*, que estabelece a existência e unicidade do quociente $b \in \mathbb{Z}$ e do resto $r \in \{0, 1, \cdots, b-1\}$ na divisão entre um dividendo $a \in \mathbb{Z}$ e um divisor não-nulo $d \in \mathbb{Z}$.

No caso específico do divisor $d = 2$, encontramos o desdobrar mais singelo da teoria, que chama a atenção pela sua simplicidade, contrastando com a importância de suas aplicações: de fato, se por um lado tal simplicidade contribui para que o divisor 2 seja tradicionalmente a via pela qual estabelecemos o primeiro contato com a divisão, ainda na infância, por outro, é dela que derivam aplicações de grande relevância na atualidade, sobretudo nas ciências da computação e engenharias, que se valem amplamente de tais conceitos. Nesse contexto, os quocientes de divisor 2 ocupam um lugar especial, uma vez que é do processo de se determinar o quociente e o resto para tal divisor que se baseia a conversão da linguagem humana convencional na linguagem binária, própria das máquinas, e reciprocamente. Comumente, tal processo consiste na aplicação do método conhecido como *algoritmo da chave*, que se baseia na obtenção de aproximações máximas do dividendo a partir do produto entre um inteiro conveniente e o divisor: a diferença entre a aproximação obtida (quando máxima) e o dividendo, resulta no resto procurado.

Em geral, esse processo e vários outros de mesma natureza são tratados no ensino básico de maneira mecânica, sem nenhuma justificativa que explique seu funcionamento ou que o relacione às propriedades da representação decimal dos inteiros, de onde provém. Segundo BRASIL [5], o trabalho com as operações deve se concentrar "na compreensão dos diferentes significados de cada uma delas, nas relações existentes entre elas e no estudo reflexivo do cálculo "(p. 55). Nesse contexto, a articulação com o funcionamento do sistema decimal é imprescindível, pois

> "as técnicas operatórias usualmente ensinadas na escola (...) apoiam-se nas regras do sistema de numeração decimal e na existência de propriedades e de regularidades

> presentes nas operações. (...) Muitos dos erros cometidos pelos alunos são provenientes da não-disponibilidade desses conhecimentos ou do não-reconhecimento de sua presença no cálculo"(idem, p.120).

Apesar disso, nos últimos anos tem ganhado força no meio docente o abandono sistemático do ensino das propriedades do sistema decimal e dos algoritmos , em detrimento do uso exclusivo e irreflexivo das calculadoras e computadores, às vezes sob a alegação de se tratarem de práticas anacrônicas e inúteis.

De acordo com os PCN do Ensino Fundamental (BRASIL ,[4]),isto constitui uma falha importante no ensino da matemática na escola básica. Com efeito,

> [são] aspectos do tratamento habitualmente dado ao estudo dos naturais nos ciclos finais do ensino fundamental [que] também comprometem sua aprendizagem:
>
> (...)
>
> - ausência de um trabalho com estimativas e com cálculo mental e o abandono da exploração dos algoritmos das operações fundamentais;
>
> (...)
>
> - trabalho centrado nos algoritmos, como o cálculo do mmc e do mdc sem a compreensão dos conceitos e das relações envolvidos e da identificação de regularidades que possibilitem ampliar a compreensão acerca dos números. "(p.97)

Na verdade, a representação decimal de um número inteiro constitui um terreno fértil para a observação de regularidades aritméticas interessantes e inesperadas, sobretudo no contexto educacional do Ensino básico. De fato, com a popularização recente da matemática recreativa, protagonizada pelos jogos matemáticos, e responsável pela disseminação cada vez mais comum de laboratórios de matemática nas escolas públicas, não é difícil encontrarem-se materiais didáticos que se prestam a explorar ou a ilustrar conceitos aritméticos a partir da manipulação de jogos ou da curiosidade suscitada por procedimentos de cálculo inusitados, como as "matemágicas"[1] das adivinhações numéricas ou os métodos algorítmicos de manipulação mais cômoda do que os tradicionais. Como exemplo, citamos Hefez ([14]: pp.47-52), que se utiliza de tais expedientes para ilustrar a aritmética da representação dos números naturais recorrendo ao Jogo de Nim e ao jogo de adivinhação "O nove misterioso".

[1]Termo comumente usado no contexto da matemática recreativa para se referir às "mágicas"que se utilizam de propriedades aritméticas dos números naturais para causar o efeito de adivinhação.

Segundo BRASIL [4], esse tipo de abordagem exploratória, em que se privilegia a investigação de padrões e a formulação de hipóteses, embora seja o meio pelo qual ocorre a gênese em matemática, não é devidamente destacada no ensino básico:

> "A partir da observação de casos particulares, as regularidades são desvendadas, as conjecturas e teorias matemáticas são formuladas. Esse caráter indutivo é, em geral, pouco destacado quando se trata da comunicação ou do ensino do conhecimento matemático."(p.26)

e enfatiza que, em tal abordagem, a Álgebra (e, por extensão, a aritmética) possui o papel de sistematizadora do conhecimento:

> "É interessante (...) propor situações em que os alunos possam investigar padrões, tanto em sucessões numéricas como em representações geométricas e identificar suas estruturas, construindo a linguagem algébrica para descrevê-los simbolicamente. Esse processo favorece a que o aluno construa a ideia de Álgebra como uma linguagem para expressar regularidades."(p.117)

Neste trabalho, apresentamos uma técnica algorítmica que objetiva, em sua forma mais elementar, determinar o quociente da divisão euclidiana por 2 recorrendo ao relacionar de cada algarismo do dividendo com o seu correspondente de ordem no quociente a partir da análise de paridade de dois algarismos vizinhos na representação decimal do dividendo e segundo o quadro 1, que usaremos chamar de *tabuada do par binário*[2], compondo um curioso processo, supostamente desprovido de cálculos intermediários e que pretende, a partir da curiosidade quanto ao seu funcionamento, eventualmente suscitada pelo seu manuseio, predispor o estudante a procurar padrões e regularidades ligadas às expressões decimais dos números e à sua divisão euclidiana por 2, característica normalmente presente nos materiais que integram os laboratórios de matemática das escolas básicas.

No decorrer do texto, pretendemos provar e generalizar a validade da tabuada do par binário, inicialmente considerando dividendos em $\mathbb{Z}$ (Capítulo 2), e a partir daí, procedendo a duas ampliações naturais: a primeira, usando dividendos reais dados pelas dízimas que os representam (Capítulo 3); e a segunda, considerando divisores do tipo $2^n, n \in \mathbb{N}^*$ (Capítulo 4). Uma vez de posse dos resultados obtidos nessa etapa, queremos expor aplicações do algoritmo obtido em algumas situações comuns no estudo da aritmética do ensino básico, com destaque para os processos relacionados à conversão entre os sistemas decimal e binário de numeração (Capítulo 5). Finalmente, apresentaremos uma sugestão de sequência didática que utiliza o algoritmo do par binário

[2] Assim a chamaremos pelo fato de tornar possível a determinação do algarismo do quociente procurado em função do par a_i e a_{i+1} de algarismos do dividendo, e da paridade de a_{i+1}, o que significa que o resto deste por 2 pode assumir um dos valores do conjunto $\{0,1\}$, que são os dígitos do sistema binário de numeração. A conexão do algoritmo com tal sistema ficará mais evidente nos capítulos posteriores, e receberá um tratamento completo no capítulo final. Em vista disso, usamos chamar o método aqui apresentado de *Algoritmo do Par Binário.*

Quadro 1: Tabuada do par binário

DIVIDENDO	QUOCIENTE	
a_i	para a_{i+1} par	para a_{i+1} ímpar
0 ou 1	0	5
2 ou 3	1	6
4 ou 5	2	7
6 ou 7	3	8
8 ou 9	4	9

Fonte: Autor, 2003

e o conhecido jogo "A matemática dos cartões numerados"para introduzir o sistema binário de numeração no ensino básico (Capítulo 6).

2 NOÇÕES ELEMENTARES DA TEORIA DOS NÚMEROS

Neste capítulo, estabeleceremos notações e resultados fundamentais da aritmética que usaremos durante todo o decurso de nosso trabalho. Tomaremos como axiomas o Algoritmo da divisão de Euclides, o Princípio da indução finita em suas duas versões e a existência do conjunto dos números inteiros, que denotaremos por $\mathbb{Z}$, cuja definição admitiremos conhecida. Além disso, definimos o conjunto $\mathbb{N}$, dos naturais, pondo

$$\mathbb{N} = \{n \in \mathbb{Z} : n \geqslant 0\}$$

2.1 Sistema de Numeração Decimal

Segundo Hefez ([14], p.43), o nosso sistema de numeração deriva do sistema sexagesimal dos babilônios (1700 A.C.) e se desenvolveu na China e na Índia, em virtude do que é chamado, às vezes, de "Sistema de numeração Indo-Arábico".

Esse sistema, que se espalhou pela Europa por volta de 1202, devido à publicação da obra *Liber Abacci*, de Fibonacci, apesar de sua notável superioridade sobre os sistemas de numeração usados na época, não gozou de notoriedade imediata, talvez devido à sua grande aceitação junto aos povos árabes, cuja cultura era rejeitada pelos europeus:

> "A introdução do sistema decimal na Europa foi tardia por causa dos preconceitos da Idade Média. Por exemplo, num documento de 1299, os banqueiros de Florença condenavam o seu uso. (...) Vários séculos se passaram para que, finalmente, esse sistema fosse usado sem restrições pelos europeus."(idem)

Na atualidade, os dez símbolos que usamos na representação decimal de um número costumam

ser chamados de *Algarismos*[1] ou *Dígitos* [2]. São eles:

$$0,1,2,3,4,5,6,7,8,9$$

que representam também os primeiros 9 números inteiros positivos mais o zero. Por força da tradição, diremos que o número inteiro que cada algarismo representa é o seu *valor absoluto*. Devido à constante menção que faremos do conjunto dos valores absolutos durante o trabalho, o indicaremos com a notação

$$\mathbb{A} = \{0,1,2,3,4,5,6,7,8,9\}$$

Por outro lado, a representação decimal de um número inteiro positivo se faz indicando o número de agrupamentos de 10 unidades, chamado de dezenas; de 10 dezenas, chamados de centenas; e de 10 centenas, chamados de unidade de milhar, para citar apenas os primeiros. Evidentemente, não faz sentido empreender a (impossível) tarefa de se nomear cada um dos infinitos agrupamentos possíveis. De modo geral, dizemos que um agrupamento de ordem n é um agrupamento de 10^n unidades, e $a \in \mathbb{A}$ agrupamentos desses expressam-se como o produto

$$a \cdot 10^n \tag{2.1}$$

Desse modo, a quantidade que conhecemos pelo nome de "três mil, oitocentos e vinte e três", por exemplo, significa que estamos "batizando" um grupo de 3 unidades de milhar, 8 centenas, 2 dezenas e 3 unidades; ou ainda, utilizando a convenção 2.1,

$$3 \cdot 10^3 + 8 \cdot 10^2 + 2 \cdot 10 + 3$$

Essa última representação costuma ser chamada de *Forma polinomial*[3] do número inteiro, devido à quantidade de termos que usamos para descrever os muitos agrupamentos, e é equivalente à notação usual "3823" que expressa, numa sequência de dígitos, as quantidades respectivas de cada tipo de agrupamento. A ausência de determinado grupo é indicada pelo zero. Voltaremos a falar dessa importante notação em breve.

Tradicionalmente, quando indica-se genericamente um dígito a, convém indexá-lo com o número da ordem que ele ocupa na forma decimal de que faz parte e que é, por definição, o expoente da potência de dez de quem é coeficiente. Também aqui adotaremos essa convenção e passaremos

[1] Deriva do sobrenome do matemático persa Buchafar Mohamed Abenmusa Al-Kuarizmi, que descreveu completamente o sistema hindu num livro do ano 825 d.C. (ver [11], p.40)

[2] Deriva do latim *Digitus*, que significa "dedo": uma clara alusão aos antigos métodos de contagem, que utilizavam os dedos das mãos, o que justifica o fato da adoção da base dez para o sistema hindu.

[3] Etimologicamente, do grego *poli*: "muitos"e do latim *nominalis*: "nomes".

a representar expressões como 2.1 na forma

$$a_n 10^n \tag{2.2}$$

Aliás, (2.2) é a expressão que define o *Valor posicional* ou *Relativo* de um algarismo a_n. Ademais, ao valor $n \in \mathbb{N}$ chamaremos de *ordem de* a_n.

Com essa notação, a forma polinomial pode ser vista como uma soma de valores relativos de algarismos, e se escreve, de maneira geral, na forma do somatório

$$\sum_{i=0}^{n} a_i 10^i \tag{2.3}$$

onde $i \in \mathbb{N}$.

Chamamos agora atenção para o fato de que (2.3) certamente expressa um número inteiro, uma vez que $\mathbb{Z}$ é fechado para a multiplicação e para a adição[4]. No entanto, isto não nos garante que todos os números inteiros possam ser representados assim. De fato, essa garantia se nos fornece por meio do conhecido resultado que enunciamos a seguir:

Teorema 2.1 (Martinez et al:[23], p.37)**.** *Se $a, b \in \mathbb{N}$ com $b > 1$, então existem inteiros positivos $a_i \in \{0, 1, 2, \cdots, b-1\}$ univocamente determinados tais que*

$$a = \sum_{i=0}^{n} a_i b^i$$

com $n \in \mathbb{N}$.

Demonstração. Provaremos o resultado pela segunda forma do princípio de indução finita:

(Existência): Se $0 \leq a < b$, basta escrever $a = a_0$ e o teorema é válido neste caso. Seja então $a \geq b$ e suponha que a proposição seja válida para $q \in \mathbb{N}$ tal que

$$1 \leq q < a. \tag{2.4}$$

Provemos que vale também para $q = a$: De fato, pelo Algoritmo de Euclides, existe $q \in \mathbb{N}$ e

[4]Um conjunto A é dito fechado para uma operação $*$ quando para quaisquer a e b elementos de A se tem $a * b \in A$. A multiplicação e a adição possuem essa propriedade em $\mathbb{Z}$. Para detalhes, recomendamos [10], p.121

$a_0 \in \{0,1,2,\cdots,b-1\}$ tais que

$$a = bq + a_0 \tag{2.5}$$

Agora, note que (2.5) implica $q < a$, e daí, a hipótese de indução (2.4) nos diz que existem inteiros r_0, r_1, $\cdots$, $r_m \in \{0,1,2,\cdots,b-1\}$ tais que

$$q = r_m b^m + \cdots + r_1 b + r_0. \tag{2.6}$$

Substituindo (2.6) em (2.5), temos

$$a = (r_m b^m + \cdots + r_1 b + r_0)\cdot b + a_0 = r_m b^{m+1} + \cdots + r_1 b^2 + r_0 b + a_0.$$

Daí, basta definir $a_i = r_{i-1}$ para todo $i \geq 1$ e $m = n-1$.

(Unicidade): Para $0 \leq a < b$ é trivial. Seja então $a \geq b$ e suponha que o resultado seja válido para todo $q \in \mathbb{N}$ tal que

$$1 \leq q < a \tag{2.7}$$

Provemos que também ele o é para $q = a$: para isto, considere as seguintes representações para a, a saber:

$$a = a_n b^n + \cdots + a_1 b + a_0 \tag{2.8}$$

e

$$a = a'_n b^n + \cdots + a'_1 b + a'_0. \tag{2.9}$$

Então, como se tratam do mesmo inteiro a, podemos escrever:

$$a = b(a_n b^{n-1} + \cdots + a_1) + a_0 = b(a'_n b^{n-1} + \cdots + a'_1) + a'_0.$$

Agora, pondo $q = a_n b^{n-1} + \cdots + a_1$ e $q' = a'_n b^{n-1} + \cdots + a'_1$, é fácil ver que $q < a$ e $q' < a$, e daí a hipótese de indução (2.7) nos diz que as representações de q e q' são univocamente determinadas. Por outro lado, como $0 \leq a_0, a'_0 < b$, segue que (2.8) e (2.9) expressam a divisão euclidiana de a com divisor b e restos respectivamente iguais a a_0 e a'_0; daí, a unicidade do quociente e do resto nos garante que

$$q = q' \quad e \quad a_0 = a'_0,$$

e as representações são indistintas. □

Neste ponto, cabe uma observação importante: apesar de termos enunciado o Teorema 2.1 em $\mathbb{N}$, ele evidentemente vale em $\mathbb{Z}$; a prova para esse caso geral é análoga, pois em termos de notação, a e $-a$ diferem entre si tão somente pelo acréscimo do sinal "$-$"[5]. Na verdade, em todo o nosso texto nos valeremos dessa observação para nos abstermos de provar cada resultado para $\mathbb{Z}_-$ e para

[5] Ver, por exemplo, [13]: p. 62.

$\mathbb{Z}_+$.

Corolário 2.1. *Se a é um número inteiro, então existem dígitos $a_i \in \mathbb{A}$ univocamente determinados tais que*

$$a = \sum_{i=0}^{n} a_i 10^i$$

com $n \in \mathbb{N}$.

Demonstração. Basta fazer $b = 10$ no teorema 2.1. □

Definição 2.1. Seja $a \in \mathbb{Z}$ o número inteiro definido pela soma

$$a = \sum_{i=0}^{n} a_i 10^i$$

Damos o nome de *expressão decimal* de a, à representação

$$a = a_n a_{n-1} \cdots a_1 a_0$$

em que $a_i \in \mathbb{A}$ para todo $i \in \{0,1,2,3,\cdots,n\}$.

Corolário 2.2. *: As expressões decimais $a = a_n a_{n-1} \cdots a_1 a_0$ e $b = b_n b_{n-1} \cdots b_1 b_0$ representam o mesmo número inteiro se, e somente se, $a_i = b_i$, para todo $i \in \{0,1,2,3,...,n\}$.*

Demonstração. Decorre imediatamente da unicidade da representação de um inteiro numa base b qualquer.

□

Corolário 2.3. *: Se $a = a_n a_{n-1} \cdots a_1 a_0$ e $a' = 0a_n a_{n-1} \cdots a_1 a_0$, então $a = a'$*

Demonstração. Pela definição 2.1, temos:

$$a' = 0a_n a_{n-1} \cdots a_1 a_0 = 0 \cdot 10^{n+1} + a_n 10^n + \cdots + a_1 10 + a_0 = 0 + a_n 10^n + \cdots + a_1 10 + a_0 =$$

$$= a_n 10^n + \cdots + a_1 10 + a_0 = a_n a_{n-1} \cdots a_1 a_0 = a.$$ □

Em virtude desse corolário, é costume dizer-se que o zero, ao ser escrito na extrema esquerda da expressão decimal, é um *algarismo não significativo*, pois sua omissão não altera o valor da expressão decimal considerada. Isto nos diz que dados a e b inteiros distintos, sempre podemos considerar ambos com o mesmo número de algarismos, bastando para isso que completemos com zeros não significativos a expressão decimal com menor número de dígitos.

2.2 Divisibilidade

Definição 2.2 (Martinez et al:[23], p.15)**.** Sejam a e b dois números inteiros tais que $a \leqslant b$. Dizemos que a divide b quando existe um inteiro $q \in \mathbb{Z}$ tal que $b = q \cdot a$. Nesse caso, escrevemos

$$a \mid b.$$

Se isto não ocorre, dizemos que a não divide b, e escrevemos $a \nmid b$.

Proposição 2.1 (Hefez:[14], pp.31-32)**.** *Sejam a, b, c, d, m, n números inteiros. São válidas as seguintes propriedades:*

(i) $1 \mid a$, $a \mid a$ e $a \mid 0$.

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

(iii) Se $a \mid b$ e $b \mid c$, então $a \mid c$.

(iv) Se a, b, c, m e n são inteiros, $c \mid a$ e $c \mid b$, então $c \mid ma + nb$.

Demonstração. :
(i) Como $a = 1$, segue que $a \mid a$ e $1 \mid a$; por outro lado, $0 = 0 \cdot a$; logo, $a \mid 0$.

(ii) Se $a \mid b$ e $b \mid a$, então existem q e q' inteiros tais que

$$a = qb \quad e \quad b = q'a.$$

Daí, $a = qq'a$, e daí, $qq' = 1$ e $q = q' = 1$, donde $a = b$.

(iii) Se $a \mid b$ e $b \mid c$, então existem $q, q' \in \mathbb{Z}$ tais que

$$b = aq \quad e \quad c = bq' \tag{2.10}$$

do que segue, de 2.10, que $bq' = aqq'$ e $c = aqq'$, o que significa que $a \mid c$.

(iv) Por hipótese, existem q e q' inteiros tais que

$$a = cq \quad e \quad b = cq'.$$

Então, temos que

$ma + nb = mcq + ncq' = c(mq + nq')$, o que implica $c \mid ma + nb$.

□

Dissemos que se não existe $q \in \mathbb{Z}$ tal que $a = bq$, então a não divide b. Isto significa que a divisão de a por b não é exata; daí, pelo algoritmo de Euclides, existe $r \in \{1, 2, 3, \cdots, b-1\}$ tal que

$$a = bq + r$$

A essa expressão chamaremos de *Forma Euclidiana de a com divisor b*. No caso $b = 2$, por exemplo, para escrever um inteiro positivo a existem somente duas formas euclidianas possíveis: $a = 2b$ ou $a = 2b + 1$. No primeiro caso temos que $2 \mid a$, e no segundo, $2 \nmid a$. É costume denominar os números do primeiro tipo de *pares*, e os do segundo tipo de *ímpares*.

A seguir provamos o conhecido critério de divisibilidade por 2, de que faremos uso posteriormente.

Proposição 2.2 (Critério de divisibilidade por 2)**.**

$a = a_n a_{n-1} \cdots a_1 a_0$ *é divisível por 2 se, e somente se,* $2 \mid a_0$.

Demonstração. Podemos escrever:

$$a = a_n \cdot 10^n + \cdots + a_1 10 + a_0 = 10 \left(\sum_{i=1}^{n} a_i 10^{i-1} \right) + a_0$$

ou ainda, pondo $Q = \sum_{i=1}^{n} a_i 10^{i-1}$,

$$a = 10Q + a_0. \tag{2.11}$$

($\Rightarrow$) Se $2 \mid a_0$, então, como $2 \mid 10$, a Proposição 2.1 (iv) nos garante que $2 \mid a$.

($\Leftarrow$) Se $2 \mid a$, então existe $q \in \mathbb{Z}$ tal que $a = 2q$. Então, temos que

$2q = 10Q + a_0$, e daí, $a_0 = 2q - 10Q = 2(q - 5Q)$ donde $2 \mid a_0$. □

2.3 Congruências

A classificação dos inteiros conforme o resto que deixam na divisão por outro inteiro é fundamental na aritmética, e não são poucas as situações interessantes na Teoria dos números cujo tratamento adequado requer sua consideração. Segundo [11] (p. 520), deve-se a Gauss [6] a notação que tornou a discussão de tais situações mais exequível, introduzindo uma nova aritmética em seu livro *Disquisitiones Arithmeticae*, de 1801 . Trata-se da relação de congruência, cuja definição enunciamos a seguir:

Definição 2.3 (Hefez:[14], p.110)**.** Seja $m \in \mathbb{N} \setminus \{0,1\}$ e $a,\ b \in \mathbb{Z}$.

Dizemos que *a é congruente a b módulo m* quando a deixa o mesmo resto que b na divisão por m. Nesse caso, escrevemos

$$a \equiv b \mod m$$

Se isto não ocorre, dizemos que *a não é congruente a b módulo m*, e escrevemos $a \not\equiv b \mod m$

Exemplo 2.1. *Temos, de acordo com a definição 2.3, por exemplo:*

$23 \equiv 13 \mod 10$, *pois* $23 = 2 \cdot 10 + 3$ *e* $13 = 10 \cdot 1 + 3$*;*

$240 \equiv 8 \mod 2$, *pois* 240 *e 8 deixam resto zero quando divididos por 2;*

$5 \not\equiv 2 \mod 2$, *pois 5=2*$\cdot 2 + 1$. □

A proposição a seguir nos fornece uma definição equivalente para a relação de congruência:

[6] Carl Friedrich Gauss: 1777-1855

Proposição 2.3 (Hefez:[13], p. 111)**.** *: Sejam a e b inteiros quaisquer e $m \in \mathbb{N} \setminus \{0,1\}$. Nessas condições, vale*

$$a \equiv b \mod m \text{ se, e somente se, } m \mid a-b$$

Demonstração. :
($\Rightarrow$) Se $a \equiv b \mod m$, então, por definição, existem inteiros q e q' e $r \in \{0,1,\cdots,m-1\}$ tais que

$$a = mq + r \qquad e \qquad b = mq' + r.$$

Subtraindo membro a membro, temos

$a - b = mq - mq' + r - r,$ ou ainda $a - b = m(q-q')$, e daí, $m \mid a-b$.

($\Leftarrow$) Por hipótese, existe $q \in \mathbb{Z}$ tal que

$$a - b = mq, \text{ que podemos escrever } a = mq + b \tag{2.12}$$

Mas, pelo algoritmo de Euclides, existe $r \in \{0,1,\cdots,m-1\}$ e $q' \in \mathbb{Z}$ tais que

$$a = mq' + r \tag{2.13}$$

Então, de 2.12 e de 2.13, temos

$$mq + b = mq' + r \text{ , ou ainda, } b = m(q'-q) + r \tag{2.14}$$

Como $0 \leq r < m$, segue que 2.14 é a forma euclidiana de b com divisor m. Então, temos de 2.13 e de 2.14 que a e b deixam o mesmo resto na divisão por 2. □

Proposição 2.4 (Santos:[27], pp.32-35)**.** *: Sejam a, b, c e d inteiros quaisquer e $m \in \mathbb{N} \setminus \{0,1\}$. Temos:*

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

(ii) Se $a \equiv b \mod m$, *então* $b \equiv a \mod m$;

(iii) Se $a \equiv b \mod m$ *e* $b \equiv c \mod m$, *então* $a \equiv c \mod m$;

(iv) Se $a \equiv b \mod m$ *e* $c \equiv d \mod m$, *então* $a + c \equiv b + d \mod m$;

(v) Se $a \equiv b \mod m$ *e* $c \equiv d \mod m$, *então* $ac \equiv bd \mod m$;

(vi) *Se* $a \equiv b \mod m$, *então* $a+c \equiv b+c \mod m$;

(vii) *Se* $a \equiv b \mod m$, *então* $ac \equiv bc \mod m$;

(viii) *Se* $a \equiv b \mod m$, *então* $a^n \equiv b^n \mod m$ *para todo* $n \in \mathbb{N}$

Demonstração. :
(i) De fato, como $m \mid 0$, temos $m \mid a-a$, e daí, $a \equiv a \mod m$.

(ii) $a \equiv b \mod m$ implica $m \mid a-b$, e daí, $m \mid -(b-a)$, ou ainda, $m \mid b-a$, do que segue que $b \equiv a \mod m$.

(iii) Por hipótese, $m \mid a-b$ e $b \mid b-c$. Então existem $q, q' \in \mathbb{Z}$ tais que

$$a-b = mq \quad e \quad b-c = mq'.$$

Então, escrevendo $b = a-mq \quad e \quad b = c+mq'$, segue que $a-mq = c+mq'$, o que implica $a-c = m(q+q')$, e daí, $m \mid a-c$ o que equivale, segundo a Proposição 2.3, que $a \equiv c \mod m$.

(iv) Por hipótese, temos que $m \mid a-b$ e $m \mid c-d$. Daí, existem inteiros q e q' tais que

$$a-b = mq \quad e \quad c-d = mq'. \tag{2.15}$$

Somando essas igualdades membro a membro, temos $a-b+c-d = mq+mq'$, que pode ser reescrita como $a+c-(b+d) = m(q+q')$, o que equivale a dizer que $m \mid (a+c)-(b+d)$ ou ainda, pela Proposição 2.3, que $a+c \equiv b+d \mod m$

(v) De 2.15, temos que

$$a-b = mq \quad e \quad c-d = mq'$$

ou ainda,

$$a = b+mq \qquad e \qquad c = d+mq' \tag{2.16}$$

Multiplicando membro a membro, as igualdades 2.16, temos:

$ac = (b+mq)(d+mq') = bd+bmq'+dmq+m^2qq'$. Logo, $ac-bd = m(bq'+dq+mqq')$, e a Proposição 2.3 nos dá que $ac \equiv bd \mod m$.

(vi) Basta fazer $c = d$ em (iv).

(vii) Basta fazer $c = a$ e $b = d$ em (v), e obtemos $a^2 \equiv b^2 \mod m$. O resultado geral segue por indução. □

Para ilustrar a eficácia da notação de congruência, considere o exemplo a seguir:

Exemplo 2.2. *Vamos determinar o algarismo das unidades de* 12^{45}*:*

Antes de qualquer coisa, observe que

$$a = a_n 10^n + \cdots + a_1 10^1 + a_0 = 10\left(\sum_{i=1}^{n} a_i 10^i\right) + a_0 \equiv 0 + a_0 \equiv a_0 \mod 10, \tag{2.17}$$

o que nos diz que a é côngruo ao seu algarismo das unidades, módulo 10. Nosso trabalho, então, se reduz a encontrar o menor valor positivo x tal que $12^{45} \equiv x \mod 10$*. Para isso, podemos escrever*

$$12^{45} = 12^{2\cdot 22+1} = (12^2)^{22} \cdot 12 = 144^{22} \cdot 12.$$

Agora, pela proposição 2.4 (vii) *e* $(viii)$ *e por* 2.17, temos que

$144^{22} \cdot 12 \equiv 4^{22} \cdot 2 \equiv (4^2)^{11} \cdot 2 \equiv (16)^{11} \cdot 2 \equiv (6)^{11} \cdot 2 \equiv 6^{2\cdot 5+1} \cdot 2 \equiv (6^2)^5 6 \cdot 2 \equiv 36^5 \cdot 12 \equiv$

$\equiv 6^5 \cdot 2 \equiv 36^2 \cdot 6 \cdot 2 \equiv 6^2 \cdot 6 \cdot 2 \equiv 36 \cdot 12 \equiv 6 \cdot 2 \equiv 12 \equiv 2 \mod 10$, e daí, segue que $a_0 = 2$ □

2.4 Classes de restos

Para concluir o capítulo, introduziremos o conceito de classes de restos. Para tanto, apresentamos três definições algébricas que nos ajudarão a tornar seu tratamento mais conciso:

Definição 2.4 (Relação de equivalência)**.** Seja $\mathscr{U}$ um conjunto não vazio.
Uma relação $\sim$ definida em $\mathscr{U} \times \mathscr{U}$ é chamada de *Relação de equivalência sobre* $\mathscr{U}$ quando, para quaisquer elementos $a, b, c \in \mathscr{U}$ valem as seguintes propriedades:

1. (Reflexiva) $a \sim a$;
2. (Simétrica) Se $a \sim b$, então $b \sim a$;
3. (Transitiva) Se $a \sim b$ e $b \sim c$, então $a \sim c$

Definição 2.5 (Classe de equivalência)**.** Seja $\mathscr{U} \neq \emptyset$ e $\sim$ uma relação de equivalência sobre $\mathscr{U}$.

Damos o nome de classe de equivalência de a pela relação $\sim$ ao subconjunto $\overline{a}$ formado por todos os elementos x de $\mathscr{U}$ tais que $x \sim a$, isto é,

$$\overline{a} = \{x \in \mathscr{U} : x \sim a\}$$

Definição 2.6 (Quociente de um conjunto por uma relação de equivalência)**.** Seja $\mathscr{U} \neq \emptyset$ e $\sim$ uma relação de equivalência sobre $\mathscr{U}$.
Ao conjunto de todas as classes de equivalência determinadas por uma relação de equivalência $\sim$ dá-se o nome de *Quociente de* $\mathscr{U}$ por $\sim$, e indica-se por

$$\mathscr{U} / \sim = \{\overline{x} : x \in \mathscr{U}\}$$

As relações de equivalência são importantes porque permitem classificar os elementos de um conjunto $\mathscr{U}$ em grupos que são equivalentes entre si (daí o nome atribuído a elas) segundo uma dada propriedade. Em outras palavras, esses grupos de elementos equivalentes, no contexto da relação considerada, formam o que se chama de classe equivalência, e podem ser considerados indistintos entre si, de modo que um representante qualquer deles pode ser usado para se definir objetos relacionados a toda classe, bem como concluir resultados gerais para esta. Finalmente,

o conjunto das classes de elementos equivalentes é o que definimos como conjunto quociente do conjunto $\mathscr{U}$ pela relação $\sim$ em questão. Essas considerações permitem um tratamento mais geral e mais sintético das propriedades de $\mathscr{U}$.

Atentando para a Proposição 2.4, as afirmações (i), (ii) e (iii) caracterizam a congruência módulo m como uma relação de equivalência sobre $\mathbb{Z}$. Tal relação particiona, pois, o conjunto dos inteiros em grupos de números que possuem o mesmo resto na divisão pelo m considerado; isto é, considerando que os restos possíveis na divisão por m são $0,1,2,\cdots,m-1$, podemos definir:

Definição 2.7 (Classes de Restos)**.** : Seja $m \in \mathbb{Z} \setminus \{0,1\}$ e $a \in \{0,1,2,\cdots,m-1\}$.
A classe de resto a módulo m é o conjunto denotado por $\overline{a}$ cujos elementos são todos os números inteiros que deixam resto a na divisão euclidiana por m; isto é,

$$\overline{a} = \{x \in \mathbb{Z} : x \equiv a \mod m\}$$

Nessas condições, o conjunto $\mathbb{Z}$ fica particionado em m classes distintas, que são os elementos do conjunto quociente de $\mathbb{Z}$ pela relação $\equiv \mod m$, que tradicionalmente é chamado de *conjunto dos inteiros módulo m*, conforme definimos a seguir:

Definição 2.8 (Conjunto dos inteiros módulo m)**.** : Seja $m \in \mathbb{Z} \setminus \{0,1\}$.
Damos o nome de Conjunto dos inteiros módulo m ao conjunto quociente de $\mathbb{Z}$ pela relação de congruência módulo m, e o indicamos por

$$\mathbb{Z}_m = \left\{\overline{0},\overline{1},\overline{2},\overline{3},\cdots,\overline{m-1}\right\}.$$

3 O ALGORITMO DO PAR BINÁRIO EM $\mathbb{Z}$

3.1 Motivação

Queremos aqui tratar da divisão euclidiana por 2 de um inteiro qualquer definido por sua expressão decimal $a = a_n a_{n-1} \cdots a_1 a_0$, isto é, supondo o quociente $b = b_n b_{n-1} \cdots b_1 b_0$ e o resto $r \in \{0,1\}$ queremos escrever

$$a = 2b + r, \tag{3.1}$$

e a partir daí estudar como se dá a "transformação "de cada algarismo a_k de a no seu correspondente b_k de mesma ordem em b. A exemplo de Lima ([16], p.59), faremos uso exclusivamente de inteiros positivos em nossa abordagem, uma vez que para tratar dos números negativos basta acrescentar o sinal de menos.

A título de ilustração, considere o inteiro $a = 231247859$, para o qual temos $b = 115623929$ e $r = 1$. Para facilitar nossa exposição, relacionaremos cada algarismo b_k da expressão decimal de b ao seu correspondente de ordem a_k na expressão decimal de a por meio da notação

$$\beta(a_k) = b_k \tag{3.2}$$

Temos então, neste caso,

$$\begin{array}{lllll}
a_8 = 2 & \mapsto & b_8 = 1, & \text{ou} & \beta(2) = 1 \\
a_7 = 3 & \mapsto & b_7 = 1, & \text{ou} & \beta(3) = 1 \\
a_6 = 1 & \mapsto & b_6 = 5, & \text{ou} & \beta(1) = 5 \\
a_5 = 2 & \mapsto & b_5 = 6, & \text{ou} & \beta(2) = 6 \\
a_4 = 4 & \mapsto & b_4 = 2, & \text{ou} & \beta(1) = 2 \\
a_3 = 7 & \mapsto & b_3 = 3, & \text{ou} & \beta(7) = 3 \\
a_2 = 8 & \mapsto & b_2 = 9, & \text{ou} & \beta(8) = 9 \\
a_1 = 5 & \mapsto & b_1 = 2, & \text{ou} & \beta(5) = 2 \\
a_0 = 9 & \mapsto & b_0 = 9, & \text{ou} & \beta(9) = 9.
\end{array} \tag{3.3}$$

Para nossos objetivos, gostaríamos que a relação $\beta = \{(a_i, b_i) \in \mathbb{A} \times \mathbb{A}\}$ definida por (3.2) definisse uma função de $\mathbb{A}$ em $\mathbb{A}$. Isto, no entanto, não ocorre. De fato, para os números a e b de nosso exemplo, temos um par de valores distintos para $a_i = 2$: $\beta(2) = 1$ na ordem $i = 8$ e $\beta(2) = 6$, na ordem $i = 5$.

Nosso primeiro objetivo aqui será o de estabelecer meios para eliminar essa ambiguidade, redefinindo a relação 3.2 num domínio mais adequado, no qual β expresse uma associação unívoca. Isto nos dará o nosso principal resultado, e é do que trataremos na seção a seguir.

3.2 O Algoritmo do Par binário: Enunciado e Exemplos

A função que definiremos a seguir ocupará um papel central em toda a nossa exposição:

Definição 3.1 (Função Par Binário)**.** Damos o nome de *Par Binário* à função

$$\langle\ ,\ \rangle : \mathbb{Z}_2 \times \mathbb{A} \longrightarrow \mathbb{A}$$

$$(a,b) \mapsto \langle a,b \rangle$$

definida por

$$\langle a,b \rangle = \begin{cases} \dfrac{b}{2}, & \text{se} \quad a = 0 \\ \dfrac{b}{2} + 5, & \text{se} \quad a = 1 \end{cases}$$

quando $2 \mid b$, e

$$\langle a,b \rangle = \langle a, b-1 \rangle, \qquad \text{caso contrário.}$$

A título de ilustração, calculemos essa função para alguns valores particulares de a e de b:

Exemplo 3.1. *De acordo com a Definição 3.1, devemos ter:*

$$\langle 0,2 \rangle = \frac{2}{2} = 1$$

$$\langle 1,4 \rangle = \frac{4}{2} + 5 = 7$$

$$\langle 0,3 \rangle = \langle 0,2 \rangle = \frac{2}{2} = 1$$

$$\langle 1,9\rangle = \langle 1,8\rangle = \frac{8}{2}+5 = 9 \qquad \square$$

Estamos agora em condições de enunciar nosso principal resultado, que expressa a relação 3.2 em termos da Definição 3.1 com $m = 2$. No que segue, usaremos a notação "$\overline{*}$" com o significado da Definição 2.8, isto é, representando a função

$$\overline{*} : \mathbb{A} \longrightarrow \mathbb{Z}_2$$

tal que

$$\overline{a} = \begin{cases} 1, & se \quad a \equiv 1 \ mod\ 2 \\ \\ 0, & se \quad a \equiv 0 \ mod\ 2 \end{cases} .$$

Teorema 3.1 (Algoritmo do Par Binário)**.** *Se $a = a_n a_{n-1} \cdots a_1 a_0$ e $b = b_n b_{n-1} \cdots b_1 b_0$ são inteiros tais que $a = 2b + r$ com $r \in \{0,1\}$, então*

$$b_i = \langle \overline{a_{i+1}}, a_i \rangle$$

com $i \in \{0,1,\cdots,n\}$

O resultado que enunciado identifica a relação (3.2) com o conceito de par binário dado na Definição 3.1. Em outras palavras, definindo β no domínio $\mathbb{Z}_2 \times \mathbb{A}$, a função que associa cada algarismo a_i do dividendo ao seu correspondente de mesma ordem no quociente identifica-se com a função par binário aplicada na dupla $(\overline{a_{i+1}}, a_i)$. Apesar de os elementos do novo domínio considerado serem pares ordenados, para maior concisão do texto optaremos por manter a notação (3.2), ficando subtendida a presença do elemento de $\mathbb{Z}_2$ que corresponde à paridade do algarismo de ordem imediatamente superior àquele que nos interessa. Em vista dessa convenção, escreveremos

$$\beta(a_i) = \langle \overline{a_{i+1}}, a_i \rangle$$

e passaremos a chamar o símbolo $\beta(a_i)$ de "par binário"de a_i.

Passaremos agora a ilustrar o uso do Teorema 3.1 com alguns exemplos antes de procedermos à sua demonstração.

Exemplo 3.2. .

1. *Para* $a = 15323$, *podemos escrever (corolário 2.3)* $a = 015323$, *e o Teorema 3.1 nos dá*

$$b = \beta(1)\beta(5)\beta(3)\beta(2)\beta(3) =$$

$$= \langle\overline{0},1\rangle\langle\overline{1},5\rangle\langle\overline{5},3\rangle\langle\overline{3},2\rangle\langle\overline{2},3\rangle =$$

$$= \langle 0,0\rangle\langle 1,4\rangle\langle 1,2\rangle\langle 1,2\rangle\langle 0,2\rangle =$$

$$= \frac{0}{2}\left(\frac{4}{2}+5\right)\left(\frac{2}{2}+5\right)\left(\frac{2}{2}+5\right)\frac{2}{2} =$$

$$= 0(2+5)(1+5)(1+5)1 =$$

$$= 7661$$

2. *Para* $a = 3142 = 03142$, *temos*

$$b = \langle\overline{0},3\rangle\langle\overline{3},1\rangle\langle\overline{1},4\rangle\langle\overline{4},2\rangle =$$

$$= \langle 0,1\rangle\langle 1,1\rangle\langle 1,4\rangle\langle 0,2\rangle =$$

$$= \langle 0,0\rangle\langle 1,0\rangle\langle 1,4\rangle\langle 0,2\rangle =$$

$$= \left(\frac{0}{2}\right)\left(\frac{0}{2}+5\right)\left(\frac{4}{2}+5\right)\left(\frac{2}{2}\right) =$$

$$= 0(0+5)(2+5)1 =$$

$$= 0571$$

□

Conforme visto, o Teorema 3.1 possibilita transferir o trabalho da divisão por 2 de um número inteiro com um número qualquer de algarismos para o equivalente (mais simples) de operar com pares binários obtidos a partir de algarismos de ordens consecutivas. Conforme veremos a seguir, os pares binários $\langle a,b\rangle$, quando escritos em sua forma mais simples, isto é, na forma tal que $2 \mid b$ e $a \in \{0,1\}$, se comportam como um quociente exato com divisor 2 de números inteiros pares entre 0 e 18. Essa correspondência nos permite formular uma definição alternativa para a função Par binário (Definição 3.1), e torna o processo de cálculo mais intuitivo, facilitando sua manipulação. Na proposição a seguir estabelecemos essa equivalência:

Proposição 3.1. *Com as hipóteses do Teorema 3.1, se* $\langle \overline{a_{i+1}}, a_i \rangle = \langle c_1, c_0 \rangle$, *com* $c_0 \equiv 0 \ mod\ 2$, $c_1 \in \{0,1\}$ *e* $c = c_1 10 + c_0 = c_1 c_0$ *é o inteiro cujos algarismos são* c_1 *e* c_0, *então*

$$\langle \overline{a_{i+1}}, a_i \rangle = \frac{c}{2}$$

Demonstração. :
Se $c_1 = 0$ e $2 \mid a_i$, então:
$\langle 0, a_i \rangle = \dfrac{a_i}{2} = \dfrac{0a_i}{2}$ daí, basta fazer $c_1 = 0$ e $c_0 = a_i$
Se $c_1 = 0$ e $2 \nmid a_i$, então:
$\langle 0, a_i \rangle = \langle 0, a_i - 1 \rangle = \dfrac{a_i - 1}{2} = \dfrac{0(a_i - 1)}{2}$ daí, $c_1 = 0$ e $c_0 = a_i - 1$.

Se $c_1 = 1$ e $2 \mid a_i$, então:
$\langle 1, a_i \rangle = \dfrac{a_i}{2} + 5 = \dfrac{a_i + 10}{2} = \dfrac{1a_i}{2}$. Analogamente, $c_1 = 1$ e $c_0 = a_i$.

Se $c_1 = 1$ e $2 \nmid a_i$, então:
$\langle 1, a_i \rangle = \langle 1, a_i - 1 \rangle = \dfrac{a_i - 1}{2} + 5 = \dfrac{a_i - 1 + 10}{2} = \dfrac{1(a_i - 1)}{2}$ e $c_1 = 1$ e $c_0 = a_i - 1$.

Portanto, em qualquer caso, $\langle \overline{a_{i+1}}, a_i \rangle = \dfrac{c}{2}$ □

Usando este resultado, o cálculo do par binário $\langle \overline{a_{i+1}}, a_i \rangle$ reduz-se, portanto, a encontrar sua forma simplificada $\langle c_1, c_0 \rangle$ e considerá-la como sendo o quociente $\dfrac{c_1 c_0}{2}$, o que torna o processo mais natural. De fato, é o que ilustramos no exemplo a seguir:

Exemplo 3.3. *Para* $a = 997766$ *e* $a = 2b + r$, $r \in \{0,1\}$, *a Proposição 3.1 nos dá:*

$$b = \langle \overline{0}, 9 \rangle \langle \overline{9}, 9 \rangle \langle \overline{9}, 7 \rangle \langle \overline{7}, 7 \rangle \langle \overline{7}, 6 \rangle \langle \overline{6}, 6 \rangle =$$

$$= \langle 0, 8 \rangle \langle 1, 8 \rangle \langle 1, 6 \rangle \langle 1, 6 \rangle \langle 1, 6 \rangle \langle 0, 6 \rangle =$$

$$= \left(\frac{8}{2}\right)\left(\frac{18}{2}\right)\left(\frac{16}{2}\right)\left(\frac{16}{2}\right)\left(\frac{16}{2}\right)\left(\frac{6}{2}\right) =$$

$$= 498883;$$

Para $a = 125478$, *temos*

$$b = \langle \overline{0}, 1 \rangle \langle \overline{1}, 2 \rangle \langle \overline{2}, 5 \rangle \langle \overline{5}, 4 \rangle \langle \overline{4}, 7 \rangle \langle \overline{7}, 8 \rangle =$$

$$= \langle 0,0\rangle \langle 1,2\rangle \langle 0,4\rangle \langle 1,4\rangle \langle 0,6\rangle \langle 1,8\rangle =$$

$$= \left(\frac{0}{2}\right)\left(\frac{12}{2}\right)\left(\frac{4}{2}\right)\left(\frac{14}{2}\right)\left(\frac{6}{2}\right)\left(\frac{18}{2}\right) =$$

$$= 62739$$ □

Para concluir a seção, mostraremos uma aplicação da Proposição 3.1 no cálculo do dobro de um número inteiro qualquer a partir do Algoritmo do par binário, e em seguida, mostraremos como obter o algoritmo tradicional da multiplicação por 2 como corolário do Teorema 3.1.

Exemplo 3.4 (Aplicação do par binário na multiplicação por 2)**.** .
Seja $b = 652415$. o Teorema 3.1 nos garante que a cada algarismo b_i de b corresponde um algarismo de $2b$, univocamente determinado pelo par binário $\langle \overline{a_{i+1}}, a_i\rangle$. Por outro lado, a Proposição 3.1 nos ensina como b_i é obtido a partir do seu a_i correspondente: de fato, $b_i = \dfrac{c_1c_0}{2} = \langle c_1, c_0\rangle$. Dito isto, temos:

$$652415 = \left(\frac{12}{2}\right)\left(\frac{10}{2}\right)\left(\frac{4}{2}\right)\left(\frac{8}{2}\right)\left(\frac{2}{2}\right)\left(\frac{10}{2}\right) = \langle 1,2\rangle \langle 1,0\rangle \langle 0,4\rangle \langle 0,8\rangle \langle 0,2\rangle \langle 1,0\rangle$$

Agora, sabemos do Teorema 3.1 que a sequência de pares binários acima representa b se, e somente se, o primeiro algarismo de cada par for côngruo mod 2 ao segundo algarismo do par de ordem imediatamente inferior, o que sempre pode ocorrer, segundo a Definição 3.1, segundo a qual temos $\langle a,b\rangle = \langle a, b-1\rangle$, se $2 \nmid b$. Sendo assim, podemos escrever:

$$\langle 1,2\rangle \langle 1,0\rangle \langle 0,4\rangle \langle 0,8\rangle \langle 0,2\rangle \langle 1,0\rangle =$$

$$= \langle 1,3\rangle \langle 1,0\rangle \langle 0,4\rangle \langle 0,8\rangle \langle 0,3\rangle \langle 1,0\rangle =$$

$$= \langle \overline{1},3\rangle \langle \overline{3},0\rangle \langle \overline{0},4\rangle \langle \overline{4},8\rangle \langle \overline{8},3\rangle \langle \overline{3},0\rangle =$$

$$= \frac{1304830}{2} \Rightarrow 2 \times 652415 = 1304830.$$ □

Generalizaremos este resultado no corolário seguinte:

Corolário 3.1 (Algoritmo tradicional da multiplicação por 2)**.** *Seja $a = a_n a_{n-1} \cdots a_1 a_0$ e $b = b_n b_{n-1} \cdots b_1 b_0 = 2a$. Sejam também c_1c_0 e $c_1'c_0'$ números inteiros tais que $c_1, c_1' \in \{0,1\}$.*
Se $2a_k = c_1c_0$ e $2a_{k-1} = c_1'c_0'$, então

$$b_0 = c_0,$$

e

$$b_k = \begin{cases} c_0, & se\ \overline{c_0} = \overline{c_1'} \\ c_0 + 1, & se\ \overline{c_0} \neq \overline{c_1'} \end{cases}$$

Demonstração. Temos $2a_k = c_1c_0$; logo, $a_k = \dfrac{c_1c_0}{2}$, e a Proposição 3.1 nos diz que $a_k = \langle c_1, c_0 \rangle$.

Analogamente, $2a_{k-1} = c_1'c_0' \Rightarrow a_{k-1} = \dfrac{c_1c_0}{2} = \langle c_1', c_0' \rangle$

Agora, pelo Teorema 3.1, temos:

$$\langle \overline{b_{k+1}}, b_k \rangle = a_k = \langle c_1, c_0 \rangle$$

e

$$\langle \overline{b_k}, b_{k-1} \rangle = a_{k-1} = \langle c_1', c_0' \rangle$$

Segue disto que

$$\overline{b_{k+1}} = c_1$$

Além disso, se $r \in \{0,1\}$, então

$$b_{k-1} - r = c_0'$$

e

$$\overline{b_k} = c_1'. \tag{3.4}$$

Então, se $\overline{c_0} = c_1'$, segue de 3.4 que $\overline{c_0} = \overline{b_k}$, e daí, $c_0 = b_k$.

Por outro lado, se $\overline{c_0} \neq c_1'$, temos, por 3.4, que $\overline{c_0 + 1} = c_1' = \overline{b_k}$.

E daí, $b_k = c_0 + 1$. □

Note que o corolário formaliza a sistemática do "vai um"presente no algoritmo usual de multiplicação. O exemplo a seguir ilustra isto:

Exemplo 3.5. *Dobrar o número* $a = 15723546$*:*

Dobrando os algarismos e aplicando o Corolário 3.1, podemos escrever:

$2a = (02)(10)(14)(04)(06)(10)(08)(12) =$

$= (2+1)(0+1)44(6+1)0(8+1)2 =$

$= 31447092.$ □

3.3 Demonstração do Algoritmo do par binário

Concluiremos este capítulo apresentando uma demonstração para o Teorema 3.1. Para tanto, enunciaremos e provaremos alguns resultados essenciais que se farão necessários no decorrer da prova. Iniciamos com o lema a seguir, que se presta ao objetivo de reduzir toda a prova ao caso em que o dividendo é múltiplo do quociente. Os demais lemas objetivam estabelecer equivalências entre características das expressões decimais do dividendo e do quociente, de modo a transferir o foco da prova do primeiro para o segundo, o que torna possível a demonstração que iremos apresentar.

Lema 3.1. *Se* $2 \mid a$*, então* a *e* $a+1$ *possuem o mesmo quociente* b *na divisão euclidiana por 2*

Demonstração. :

Se $2 \mid a$, então existe $b \in \mathbb{N}$ tal que $a = 2b$. Então, $a+1 = 2b+1$, e como $1 \in \{0,1\}$, segue que b é o quociente da divisão euclidiana de $a+1$ por 2. □

Lema 3.2. *Seja* $b = b_n b_{n-1} \cdots b_1 b_0$ *e* a_k *o dígito de ordem* $k \geq 1$ *na expressão decimal de* $2b$*.*

(i) $b_k \in \{0,1,2,3,4\}$ *se, e somente se,* $a_k = 2b_k + s$*;*

(ii) $b_k \in \{5,6,7,8,9\}$ *se, e somente se,* $a_k = (2b_k - 10) + s$*,*

$$\text{Em que } s = \begin{cases} 0, & se \quad b_{k-1} \in \{0,1,2,3,4\} \\ 1, & se \quad b_{k-1} \in \{5,6,7,8,9\} \end{cases}$$

Demonstração. ($\Rightarrow$)

(Indução sobre k) Seja $k = 1$. Há dois casos a se considerar, a depender da paridade de b_0:

Caso I: Se $0 \leq b_0 \leq 4$, segue que

$$0 \leq 2b_0 \leq 8 \text{ e daí, } a_0 = 2b_0 \tag{3.5}$$

Então,

(i)

$$0 \leq b_1 \leq 4 \text{ implica } 0 \leq 2b_1 \leq 8 \tag{3.6}$$

Logo, de 3.5 e 3.6, temos que

$2(b_1b_0) = 2b_110 + 2b_0 = (2b_1)(2b_0) = a_1a_0,$ donde $a_1 = 2b_1 + 0.$

(ii)

$$\text{Se } 5 \leq b_1 \leq 9, \text{ então } 10 \leq 2b_1 \leq 18, \text{ e temos } 0 \leq 2b_1 - 10 \leq 8. \tag{3.7}$$

Disto segue que $2(b_1b_0) = 2b_110 + 2b_0 = (2b_1 - 10 + 10)10 + b_0 = (2b_1 - 10) \cdot 10 + 10^2 + b_0 =$

$= 10^2 + (2b_1 - 10) \cdot 10 + b_0,$ e, usando a desigualdade 3.7, temos então $a_1 = 2b_1 - 10.$

Caso II: Se $5 \leq b_0 \leq 9$ temos

$$10 \leq 2b_0 \leq 18, \text{ ou ainda } 0 \leq 2b_0 - 10 \leq 8, \text{ o que nos dá } a_0 = 2b_0 - 10 \tag{3.8}$$

Então,

$(i) \quad 2(b_1b_0) = 2b_110 + 2b_0 = 2b_110 + 2b_0 - 10 + 10 \Rightarrow (2b_1 + 1)10 + 2b_0 - 10$

e, de 3.6, temos

$1 \leq 2b_1 + 1 \leq 9,$ que implica $a_1 = 2b_1 + 1.$

$(ii) \quad 2(b_1b_0) = 2b_110 + 2b_0 = (2b_1 - 10 + 10)10 + 2b_0 - 10 + 10 =$

$= (2b_1 - 10)10 + 10^2 + 10 + 2b_0 - 10 = 10^2 + [(2b_1 - 10) + 1]10 + 2b_0 - 10,$

e de 3.7 e 3.8, segue que $a_1 = (2b_1 - 10) + 1.$

Logo, o resultado vale para $k = 1$. Suponha agora que valha para todo $1 \leq k \leq n$, onde n é algum inteiro. Provaremos que vale para $k + 1$, e daí, para todo $k \in \mathbb{N}$. Para tanto, dividiremos a prova em dois casos, como antes:

Caso I: Se $0 \leq b_{k+1} \leq 4$, temos:

$$0 \leq 2b_{k+1} \leq 8, \tag{3.9}$$

e supondo $s \in \{0,1\}$, temos

(i)

$$0 \leq b_k \leq 4, \text{ ou } 0 \leq 2b_k \leq 8, \text{ ou ainda } 0 \leq 2b_k + s \leq 9. \tag{3.10}$$

Agora, usando 3.9 e 3.10, a hipótese de indução nos garante que $a_k = 2b_k + s$, e daí,

$2b = 2 \cdot (b_{k+1}b_k \cdots b_0) = 2b_{k+1}10^{k+1} + (2b_k + s)10^k + \cdots + a_0$, o que nos dá $a_{k+1} = 2b_{k+1} + 0$.

(ii) Se $5 \leq b_{k+1} \leq 9$, então

$$0 \leq 2b_k - 10 \leq 8, \text{ donde } 0 \leq (2b_k - 10) + s \leq 9. \tag{3.11}$$

Além disso, podemos escrever

$2b = 2 \cdot (b_{k+1}b_k \cdots b_0) = 2b_{k+1}10^{k+1} + 2b_k10^k + \cdots + a_0 =$

$= 2b_{k+1}10^{k+1} + (2b_k - 10 + 10)10^k + \cdots + a_0 =$

$= 2b_{k+1}10^{k+1} + (2b_k - 10)10^k + 10^{k+1} + \cdots + a_0 =$

$= (2b_{k+1} + 1)10^{k+1} + (2b_k - 10)10^k + \cdots + a_0.$

Agora, pela hipótese de indução e por 3.11, temos

$$a_k = (2b_k - 10) + s \leq 9$$

o que nos dá

$$2b = 2 \cdot (b_{k+1}b_k \cdots b_0) = (2b_{k+1} + 1)(2b_k - 10 + s) \cdots a_0$$

e daí, $a_{k+1} = 2b_{k+1} + 1$.

Caso II: Se $5 \leq b_{k+1} \leq 9$ temos

$$0 \leq 2b_{k+1} - 10 \leq 8, \tag{3.12}$$

e usando 3.10, 3.12, a hipótese de indução e um raciocínio análogo ao caso I, temos:

(i) $2b = 2 \cdot (b_{k+1}b_k \cdots b_0) =$

$= (2b_{k+1} - 10)10^{k+1} + 10^{k+2} + 2b_k 10^k + \cdots + a_0 =$

$= 10^{k+2} + [(2b_{k+1} - 10)(2b_k + s)\cdots a_0]$

$\Rightarrow\ a_{k+1} = 2b_{k+1} - 10 + 0.$

Da mesma forma, de 3.11, 3.12 e da hipótese de indução decorre:

$(ii)\quad 2b = 2 \cdot (b_{k+1}b_k \cdots b_0) =$

$= (2b_{k+1} - 10 + 1)10^{k+1} + 10^{k+2} + (2b_k - 10 + s)10^k + \cdots + a_0 =$

$= 10^{k+2} + [(2b_{k+1} - 10 + 1)(2b_k - 10 + s)\cdots a_0]$

$\Rightarrow\ a_{k+1} = 2b_{k+1} - 10 + 1$ [1]

$(\Leftarrow)$
$(i)\quad$ Se $a_k = 2b_k + s \in \mathbb{A}$, então $b_k = \dfrac{a_k - s}{2}$. Como $b_k \in \mathbb{A}$ e $s \in \{0,1\}$, segue que

$$a_k - s \in \{0,2,4,6,8\} \ \Rightarrow\ b_k = \frac{a_k - s}{2} \in \{0,1,2,3,4\} \tag{3.13}$$

$(ii)\quad$ Analogamente, se $a_k = (2b_k - 10) + s$, então $b_k = \dfrac{a_k - s}{2} + 5 \in \{5,6,7,8,9\}$, por 3.13. □

Lema 3.3. *Sejam $a = a_n a_{n-1} \cdots a_1 a_0$ e $b = b_n b_{n-1} \cdots b_1 b_0$ inteiros tais que $a = 2b + r$, com $r \in \{0,1\}$. Então, para $k \in \{1,2,\cdots,n\}$ temos que*

$$\textit{se}\ \ 2 \mid a_k \quad \textit{e} \quad 2 \mid a_{k+1},\ \textit{então}\ \ 0 \le b_{k-1} \le 4 \quad \textit{e} \quad 0 \le b_k \le 4$$

Demonstração. :

Sejam $a = \sum_{i=0}^{n} a_i 10^i$, $b = \sum_{i=0}^{n} b_i 10^i$ e a_{k-1}, a_k e a_{k+1} dígitos consecutivos de a. Pelo Lema 3.1 é suficiente considerarmos o caso $a = 2b$. Disto segue que $b = \dfrac{a}{2}$, e daí,

$$b = \sum_{i=0}^{n} \frac{a_i}{2} 10^i = \frac{a_n}{2}10^n + \cdots + \frac{a_{k+1}}{2}10^{k+1} + \frac{a_k}{2}10^k + \frac{a_{k-1}}{2}10^{k-1} + \cdots + \frac{a_0}{2}$$

[1] pois $0 \le 2b_k - 10 + s \le 9$

Por hipótese, temos que $2 \mid a_{k+1}$ e $2 \mid a_k$ implica que existem $b'_k \in \mathbb{A}$ e $b'_{k+1} \in \mathbb{A}$ tais que

$$a_{k+1} = 2b'_{k+1} \text{ , que nos dá } \; b'_{k+1} = \frac{a_{k+1}}{2}$$

e

$$a_k = 2b'_k \text{ , donde } \; b'_k = \frac{a_k}{2}. \tag{3.14}$$

Como $a_k, a_{k+1} \in \{0,2,4,6,8\}$, segue que $b'_k, b'_{k+1} \in \{0,1,2,3,4\}$.

Para a_{k-1} há duas situações possíveis: a primeira, em que $2 \mid a_{k-1}$ e a segunda, em que $2 \nmid a_{k-1}$. A seguir apresentamos a prova para o primeiro caso. A prova do segundo pode ser obtida de maneira inteiramente análoga.

Dito isto, temos que:

$$\text{Se } 2 \mid a_{k-1}, \text{ então existe } b'_{k-1} = \frac{a_{k-1}}{2} \in \{0,1,2,3,4\},$$

e b'_{k+1}, b'_k e b'_{k-1} são dígitos entre 0 e 4.

Afirmamos que $b'_k = b_k$; isto é, que b'_k é, efetivamente, o algarismo de ordem k em b:

De fato, como $2 \mid a_k$, o Lema 3.2 nos diz que

$$(i) \quad a_k = 2b_k \quad \text{ou} \quad (ii) \quad a_k = 2b_k - 10 \quad .$$

Suponha por absurdo que ocorre (ii). Então temos que

$a_k = 2b_k - 10 = 2b'_k$ implica $\; b_k = b'_k + 5$, e temos, por 3.14, que $\; b_k \in \{5,6,7,8,9\}$;

logo, pelo Lema 3.2, segue que $\; a_{k+1} = 2b_{k+1} - 10 + 1$ ou $a_{k+1} = 2b_{k+1} + 1$.

Em qualquer caso, teremos que $2 \nmid a_{k+1}$, contradição. Portanto,

$$a_k = 2b_k = 2b'_k \text{ , e daí, } \; b_k = b'_k \in \{0,1,2,3,4\}.$$

Além disso, $a_k = 2b_k$ e pelo Lema 3.2, segue que $b_{k-1} \in \{0,1,2,3,4\}$. □

Lema 3.4. *Sejam* $a = a_n a_{n-1} \cdots a_1 a_0$ *e* $b = b_n b_{n-1} \cdots b_1 b_0$ *inteiros tais que* $a = 2b + r$, *com* $r \in \{0,1\}$. *Então, para* $k \in \{1,2,\cdots,n\}$, *temos que*

$$\text{se } 2 \mid a_k \quad e \quad 2 \nmid a_{k+1}, \text{ então } 0 \leq b_{k-1} \leq 4 \quad e \quad 5 \leq b_k \leq 9$$

Demonstração. :

Sejam $a = \sum_{i=0}^{n} a_i 10^i$ e $b = \sum_{i=0}^{n} b_i 10^i$. Como antes, e sem perda de generalidade, suponha $a = 2b$. Isto nos dá:

$$b = \frac{a}{2} = \sum_{i=0}^{n} \frac{a_i}{2} 10^i = \frac{a_n}{2} 10^n + \cdots + \frac{a_{k+1}}{2} 10^{k+1} + \frac{a_k}{2} 10^k + \frac{a_{k-1}}{2} 10^{k-1} + \cdots + \frac{a_0}{2} \tag{3.15}$$

Por outro lado, seguindo a ideia da demonstração anterior,

$$\text{se } 2 \nmid a_{k+1} \text{ então existe } b'_{k+1} \in \{0,1,2,3,4\} \text{ tal que } a_{k+1} = 2b'_{k+1} + 1 \tag{3.16}$$

e

$$\text{se } 2 \mid a_k, \text{ então existe } b'_k \in \{0,1,2,3,4\} \text{ tal que } a_k = 2b'_k \tag{3.17}$$

Além disso, o Lema 3.2 nos diz que $2 \mid a_k$ implica $s = 0$ e nos aponta as duas seguintes possibilidades:

$$(i) \quad a_k = 2b_k \quad \text{ou} \quad (ii) \quad a_k = 2b_k - 10 \quad .$$

Afirmamos que $a_k = 2b_k - 10$. De fato, supondo (i), temos que

$a_k = 2b_k$ e $a_k = 2b'_k$, e dai $b_k = b'_k \in \{0,1,2,3,4\}$;

logo, pelo Lema 3.2 devemos ter $a_{k+1} = 2b_{k+1} + 0$ ou $a_{k+1} = 2b_{k+1} - 10$, e daí, $2 \mid a_{k+1}$ (contradição).

Portanto, $a_k = 2b_k - 10 = 2b'_k$, que é o mesmo que $b_k = b'_k + 5$ em vista do que temos $b_k \in \{5,6,7,8,9\}$.

Para completar a demonstração, observemos que $a_k = 2b_k - 10$, e o Lema 3.2 nos diz que $b_{k-1} \in \{0,1,2,3,4\}$. □

Lema 3.5. *Sejam $a = a_n a_{n-1} \cdots a_1 a_0$ e $b = b_n b_{n-1} \cdots b_1 b_0$ inteiros tais que $a = 2b + r$, com $r \in \{0,1\}$. Então, para $k \in \{1,2,\cdots,n\}$, temos que*

$$\text{Se } 2 \mid a_{k+1} \quad \text{e} \quad 2 \nmid a_k \text{ , então } 0 \leq b_k \leq 4 \quad \text{e} \quad 5 \leq b_{k-1} \leq 9.$$

Demonstração. : Supondo $a = 2b$ (Lema 3.1), podemos escrever

$$b = \frac{a}{2} = \frac{a_n}{2}10^n + \cdots + \frac{a_{k+1}}{2}10^{k+1} + \frac{a_k}{2}10^k + \frac{a_{k-1}}{2}10^{k-1} + \cdots + \frac{a_0}{2}$$

Por hipótese, existem b'_k e $b'_{k+1} \in \{0,1,2,3,4\}$ tais que

$$a_{k+1} = 2b'_{k+1}$$

e

$$a_k = 2b'_k + 1$$

Além disso, o Lema 3.2 nos diz que

$$(i) \quad a_k = 2b_k + 1 \quad \text{ou} \quad (ii) \quad a_k = (2b_k - 10) + 1$$

Supondo que ocorre (ii), temos

$a_k = 2b_k - 10 + 1 = 2b'_k + 1$, ou ainda $b_k = b'_k + 5 \in \{5,6,7,8,9\}$, e o Lema 3.2 nos diz que $s = 1$, e daí devemos ter $a_{k+1} = 2b_{k+1} + 1$ ou $a_{k+1} = (2b_{k+1} - 10) + 1$ donde $2 \nmid a_{k+1}$ (contradição).

Logo, $a_k = 2b_k + 1 = 2b'_k + 1$ e temos $b_k = b'_k$ que implica $b_k \in \{0,1,2,3,4\}$.

Além disso, se $a_k = 2b_k + 1$, então $s = 1$, e daí, $b_{k-1} \in \{5,6,7,8,9\}$. □

Lema 3.6. *Sejam $a = a_n a_{n-1} \cdots a_1 a_0$ e $b = b_n b_{n-1} \cdots b_1 b_0$ inteiros tais que $a = 2b + r$, com $r \in \{0,1\}$. Então, para $k \in \{1,2,\cdots,n\}$, temos que*

$$\text{se } 2 \nmid a_{k+1} \quad \text{e} \quad 2 \nmid a_k \text{ , então } 5 \leq b_{k-1}, b_k \leq 9.$$

Demonstração. Supondo $a = 2b$ (Lema 3.1), podemos escrever, como o fizemos antes:

$$b = \frac{a}{2} = \frac{a_n}{2}10^n + \cdots + \frac{a_{k+1}}{2}10^{k+1} + \frac{a_k}{2}10^k + \frac{a_{k-1}}{2}10^{k-1} + \cdots + \frac{a_0}{2}.$$

Por hipótese, existem b'_k e $b'_{k+1} \in \{0,1,2,3,4\}$ tais que

$$a_{k+1} = 2b'_{k+1} + 1$$

e

$$a_k = 2b'_k + 1.$$

Do Lema 3.2 temos que

$2 \nmid a_k$, e daí, $s = 1$, o que implica

$$(i) \quad a_k = 2b_k + 1 \quad \text{ou} \quad (ii) \quad a_k = (2b_k - 10) + 1 \quad .$$

Se $a_k = 2b_k + 1$, então temos $b_k = b'_k \in \{0,1,2,3,4\}$, e daí temos

$a_{k+1} = 2b_{k+1}$ ou $a_{k+1} = 2b_{k+1} - 10$, e $2 \mid a_{k+1}$ (absurdo).

Logo, $a_k = (2b_k - 10) + 1 = 2b'_k + 1$, do que segue que $b_k = b'_k + 5 \in \{5,6,7,8,9\}$.

Por outro lado,

se $a_k = 2b_k + 1$, então $s = 1$ e daí, $b_{k-1} \in \{5,6,7,8,9\}$. □

Estamos agora em condições de efetuar a prova do Teorema 3.1:

Demonstração. (do Teorema 3.1):

Sejam $a = \sum_{i=0}^{n} a_i 10^i$ e $b = \sum_{i=0}^{n} b_i 10^i$ inteiros tais que $a = 2b + r, \quad r \in \{0,1\}$. Sem perda de generalidade, suponhamos $r = 0$. Sejam também a_k e a_{k+1} dois algarismos consecutivos de a e $b_i = \beta(a_i)$:

Se $2 \mid a_k$ e $2 \mid a_{k+1}$, o Lema 3.3 nos diz que $0 \leq b_{k-1} \leq 4$ e $0 \leq b_k \leq 4$ e daí, pelo Lema 3.2 e a Definição 3.1, temos:

$$a_k = 2b_k \text{ , donde } b_k = \frac{a_k}{2} = \langle 0, a_k \rangle = \langle \overline{a_{k+1}}, a_k \rangle \text{ , pois } 2 \mid a_{k+1}.$$

Se $2 \mid a_k$ e $2 \nmid a_{k+1}$, o Lema 3.4 nos diz que $0 \leq b_{k-1} \leq 4$ e $5 \leq b_k \leq 9$ e daí, pelo Lema 3.2 e a

Definição 3.1, segue que

$$a_k = 2b_k - 10 \text{ , ou ainda } b_k = \frac{a_k}{2} + 5 = \langle 1, a_k \rangle = \langle \overline{a_{k+1}}, a_k \rangle \text{ , pois } 2 \nmid a_{k+1}.$$

Se $2 \nmid a_k$ e $2 \mid a_{k+1}$, o Lema 3.5 nos diz que $5 \leq b_{k-1} \leq 9$ e $0 \leq b_k \leq 4$, e daí, pelo Lema 3.2 e a Definição 3.1 segue que

$a_k = 2b_k + 1$ ou, equivalentemente, $b_k = \dfrac{a_k - 1}{2} = \langle 0, a_k - 1 \rangle = \langle \overline{a_{k+1}}, a_k \rangle$,

pois $2 \mid a_{k+1}$ e $\langle 0, a_k - 1 \rangle = \langle 0, a_k \rangle$. Se $2 \nmid a_k$ e $2 \nmid a_{k+1}$, o Lema 3.6 nos diz que $5 \leq b_{k-1}, b_k \leq 9$ e daí, pelo Lema 3.2 e a Definição 3.1, segue que

$a_k = 2b_k - 10 + 1$, que implica $b_k = \dfrac{a_k - 1}{2} + 5 = \langle 1, a_k - 1 \rangle = \langle \overline{a_{k+1}}, a_k \rangle$, por razões análogas às anteriores.

Logo, em qualquer caso, concluímos que $\beta(a_k) = \langle \overline{a_{k+1}}, a_k \rangle$, como queríamos demonstrar. □

4 O ALGORITMO DO PAR BINÁRIO EM $\mathbb{R}$

Queremos, no presente capítulo, estabelecer a validade da generalização do Teorema 3.1 obtida quando ampliamos o conjunto de definição do dividendo de $\mathbb{Z}$ para $\mathbb{R}$. Para tanto, dedicaremos a presente seção às considerações prévias a respeito da representação decimal dos números reais, bem como às convenções que usaremos, e que julgamos necessárias ao que pretendemos.

4.1 Expressões decimais de números reais

No que segue, assumiremos conhecidos os conceitos de série de números reais e o critério de convergência de séries de termos positivos, de que precisaremos para a definição a seguir:

Definição 4.1. Seja $a \in \mathbb{R}$ o número real definido pela série

$$a' + \sum_{i=1}^{\infty} \frac{a_{-i}}{10^i} \tag{4.1}$$

onde $a' = a_n a_{n-1} \cdots a_1 a_0 \in \mathbb{Z}$ e $a_{-1}, a_{-2}, \cdots \in \mathbb{A}$. Damos o nome de *expressão decimal de* a à representação

$$a = a', a_{-1} a_{-2} a_{-3} \cdots a_{-m} \cdots$$

Adicionalmente, dizemos que a' é a *parte inteira de* a e que $a_{-1} a_{-2} \cdots a_{-m} \cdots$ é sua *parte fracionária*. Nessas condições, a vírgula cumpre o papel de separação entre as partes inteira e fracionária de a. Além disso, por simplicidade, usaremos chamar os algarismos a_i tais que $i < 0$ *de algarismos fracionários*, ao passo que designaremos os algarismos a_i tais que $i \geq 0$ de *algarismos inteiros de* a.

Por outro lado, vale mencionar que a definição está bem justificada. De fato, se $a' \geq 0$ e

$a_i > 0$ para todo $i \in \mathbb{N}$, (4.1) é uma série de termos positivos cuja n-ésima soma parcial é dada por

$$a' + S_n = a' + \frac{a_{-1}}{10} + \frac{a_{-2}}{10^2} + \cdots + \frac{a_{-n}}{10^n}$$

Mas do fato de que $\frac{a_{-k}}{10^k} \leq \frac{1}{10^{k-1}}$, segue que

$$a' + S_n \leq a' + 1 + \frac{1}{10} + \cdots + \frac{1}{10^{n-1}}$$

Mas $\sum_{i=1}^{\infty} \frac{1}{10^{i-1}}$ é uma série geométrica de primeiro termo 1 e razão $r = \frac{1}{10}$. É fato conhecido que tal série converge para $\frac{1}{1-r}$ (Para uma prova deste fato, recomendamos consultar Ávila ([2], p.109), donde obtemos

$$\sum_{i=1}^{\infty} \frac{1}{10^{i-1}} = \frac{1}{1-1/10} = \frac{10}{9}.$$

Segue disto que

$$0 < a' + S_n \leq a' + \sum_{i=1}^{n} \frac{1}{10^{i-1}} < a' + \frac{10}{9}$$

e a sequência de somas parciais $a' + S_n$ é monótona limitada, logo, convergente (Ver [17] p.26, Teo. 4), e daí, (4.1) também converge e $a > 0$.

Se $a' = 0$ e $a_k = 0$ para todo $k \leq -1$, segue-se trivialmente que $a = 0$, e se $a' + \sum \frac{a_{-i}}{10^i} < 0$ segue que $-\left(a' + \sum \frac{a_{-i}}{10^i}\right) > 0$ e este caso se reduz ao primeiro, donde $-a > 0$ implica $a < 0$.

Logo, a série 4.1 sempre define um número real a, de modo que podemos escrever

$$a', a_{-1}a_{-2}a_{-3}\cdots a_{-m}\cdots = a.$$

Menos trivial e mais importante é a implicação contrária, isto é, a afirmação de que para cada número real a existe uma expressão decimal que o define. Tal afirmação constitui uma generalização do Teorema 2.1 a $\mathbb{R}$, e devido à sua importância no que se segue, o provaremos a seguir, utilizando o método apresentado por Dominguez ([9], p.264). Para tanto, admitiremos conhecida a definição analítica de limite de uma sequência de números reais [1].

Teorema 4.1 (cf. [9], p.264)**.** *Se $a \in \mathbb{R}$, então existem $a' \in \mathbb{Z}$ e dígitos $a_{-1}, a_{-2}, \cdots a_{-m}, \cdots$*

[1] Dizemos que uma sequência $(a_i)_{i\in\mathbb{N}}$ possui limite a quando, dado um $\varepsilon > 0$ arbitrário, existir $r \in \mathbb{N}$ tal que $n \geq r \Rightarrow |a_n - a| < \varepsilon$. Nesse caso, escrevemos $\lim a_i = a$ (cf. [17], p.24)

tais que

$$a = a', a_{-1}a_{-2}a_{-3}\cdots a_{-m}\cdots$$

Demonstração. Seja $a' \in \mathbb{Z}$ tal que $a' \leq a < a' + 1$.

Se $a' = a$, recaímos no caso $a \in \mathbb{Z}$ já provado anteriormente (Teorema 2.1).

Suponha então $a' < a < a' + 1$ e seja $a_{-1} \in \mathbb{A}$ *o maior dígito tal que*

$$S_1 = a' + \frac{a_{-1}}{10} \leq a \leq a' + \frac{a_{-1}+1}{10} = S_1'. \tag{4.2}$$

Se $a = S_1$, a demonstração está concluída e $a = a', a_{-1}$.

Caso contrário, seja $a_{-2} \in \mathbb{A}$ o maior dígito tal que

$$S_2 = S_1 + \frac{a_{-2}}{10^2} \leq a \leq S_1 + \frac{a_{-2}+1}{10^2} = S_2'.$$

Se $a = S_2$, então $a = a', a_{-1}a_{-2}$ e a demonstração termina. Caso contrário, repete-se o processo.

A partir daí, temos duas situações possíveis:
I) Para algum $r \in \mathbb{N}$ se tem $a = a', a_{-1}a_{-2}a_{-3}\cdots a_{-r}$, e a demonstração está completa.

II) O processo não termina.

Nesse caso, consideremos os subconjuntos de $\mathbb{R}$:

$$S = \{S_1, S_2, \cdots\} \qquad \text{e} \qquad S' = \{S_1', S_2', \cdots\}$$

onde os elementos $S_k \in S$ definem-se recursivamente pondo $S_k = S_{k-1} + \dfrac{a_{-k}}{10^k}$, e os elementos $S_k' \in S'$, de maneira análoga, pondo $S_k' = S_{k-1} + \dfrac{a_{-k}+1}{10^k}$, e S_1 e S_1' definidos como em 4.2.

Por construção, para todo $i \in \mathbb{N}$ se tem $S_i < S_i'$.

Por outro lado, temos

$$0 < S_r' - S_r = a' + \sum_{i=1}^{r-1} \frac{a_i}{10^i} + \frac{a_r+1}{10^r} - \left(a' + \sum_{i=1}^{r} \frac{a_i}{10^i}\right) = \frac{1}{10^r}. \tag{4.3}$$

Agora, dado $\varepsilon > 0$, seja $r \in \mathbb{N}$ tal que $\frac{1}{10^r} < \varepsilon$. Por 4.3, temos que $S'_r - S_r = \frac{1}{10^r}$.

Mas $S_r \leq a \leq S'_r$, e daí,

$$a - S_r < S'_r - S_r = \frac{1}{10^r} < \varepsilon. \tag{4.4}$$

Entretanto, sabemos que para todo $n \geq r$ vale a desigualdade

$$S_r \leq S_n \leq a.$$

Então, de 4.4, temos:

$$a - S_n \leq a - S_r < \varepsilon \tag{4.5}$$

Mas $a - S_n = |a - S_n|$, e daí temos de 4.5 que

$$n \geq r \;\Rightarrow\; |a - S_n| < \varepsilon,$$

o que significa, pela, definição de limite, que $\lim S_n = a$ ou, equivalentemente, que

$a = a', a_{-1}a_{-2}a_{-3}\cdots a_{-m}\cdots$ □

Observemos que apesar de ser um resultado mais geral do que seu equivalente em $\mathbb{Z}$, o Teorema 4.1 não assegura a unicidade da representação decimal, ao contrário do seu caso particular. Com efeito, apesar de cada expressão decimal definir um único número real, a afirmação recíproca não é necessariamente verdadeira. De fato, consideremos, a título de ilustração, as expressões decimais a seguir:

$a = 0,23000\cdots$ tal que $a_i = 0$ para todo $i < -2$

e

$b = 0,22999\cdots$ em que $a_i = 9$ para todo $i < -2$.

Afirmamos que a e b definem o mesmo número $\alpha \in \mathbb{R}$. De fato, por definição, temos

$$a = 0,23000\cdots = \frac{2}{10} + \frac{3}{10^2} + \frac{0}{10^3} + \frac{0}{10^4} + \cdots = \frac{20}{10^2} + \frac{3}{10^2} + \cdots + 0 + 0 + \cdots = \frac{23}{100},$$

e

$$b = 0,22999\cdots = \frac{2}{10} + \frac{2}{10^2} + \frac{9}{10^3} + \frac{9}{10^4} + \cdots = \frac{20}{10^2} + \frac{2}{10^2} + \frac{\frac{9}{10^3}}{1 - \frac{1}{10}} = \frac{22}{100} + \frac{9/10^3}{9/10} =$$

$$= \frac{22}{100} + \frac{1}{100} = \frac{23}{100}$$

Logo, as expressões a e b definem o mesmo número real $\alpha \in \mathbb{R}$.

Em vista dessa duplicidade de notação, diremos que $a = 0,23000\cdots$ é a representação de α em *expansão finita* e que $b = 0,22999\cdots$ a sua representação em *expansão infinita*. Apesar disso, concordando com Lima ([16], pp. 59-60), adotaremos escrever $a = b = \alpha$, não fazendo distinção entre α e qualquer de suas representações decimais. Além disso, no primeiro caso, dispensaremos os zeros à direita de a e escreveremos $a = 0,23$.

Generalizando, temos a definição a seguir:

Definição 4.2 (Dízima finita e dízima infinita)**.** Seja $a = a', a_{-1}a_{-2}a_{-3}\cdots a_{-m}\cdots$ uma expressão decimal real. Dizemos que a é uma *dízima de expansão finita*, ou, simplesmente, *dízima finita*, se para algum $m \in \mathbb{N}$ se tenha $a_i = 0$ para todo $i < -m$, e escrevemos

$$a = a', a_{-1}a_{-2}a_{-3}\cdots a_{-m}.$$

Caso contrário, dizemos que a é uma *dízima de expansão infinita*, ou, simplesmente, uma *dízima infinita*.

Exemplo 4.1. *São exemplos de dízimas finitas:*

$$0,50000\cdots = 0,5 \quad e \quad 1,21000\cdots = 1,21,$$

e são exemplos de dízimas infinitas

$$3,14159265\cdots (= \pi) \quad e \quad 0,3333\cdots \left(= \frac{1}{3}\right) \qquad \square$$

A observação feita antes da Definição 4.2 referente à equivalência entre as dízimas $0,23$ e $0,22999\cdots$, bem como a segunda parte do Exemplo 4.1 referentes aos números π e $\frac{1}{3}$ nos dão evidências de que os números que admitem representação em dízima finita também possuem uma representação na forma de dízima infinita tal que $a_i = 9$ para todo $i \leq -m$, para algum $m \in \mathbb{N}$, ao passo que alguns números, tais como o $\frac{1}{3}$, que apresenta uma expansão infinita periódica, ou o π, que apresenta uma expansão infinita e aperiódica não possuem uma representação alternativa finita.

De fato, segundo Lima ([16], p.64), a função que associa cada número real a à sua expressão decimal é sobrejetiva, mas não injetiva, e ainda, o único caso em que há a quebra da injetividade é aquele em que a dízima possui infinitos algarismos fracionários iguais a 9. Desse modo, um número real admite uma expressão decimal infinita se, e somente se, admitir uma representação infinita do tipo $a', a_{-1}a_{-2}a_{-3}\cdots a_{-m}9999\cdots$, o que não ocorre com as dízimas periódicas de período diferente de 9. Na proposição a seguir caracterizaremos os números reais que possuem tal propriedade:

Proposição 4.1. *Um número real a admite uma representação decimal em dízima finita se, e somente se, existem $\alpha \in \mathbb{Z}$ e $n \in \mathbb{N}$ tais que*

$$a = \frac{\alpha}{10^n}$$

Demonstração. Seja $a = a', a_{-1}a_{-2}a_{-3}\cdots a_{-n}$ e suponha que $a_i = 0$ para todo $i < -n$. Podemos escrever:

$$a = a', a_{-1}a_{-2}a_{-3}\cdots a_{-n} = a' + \sum_{i=1}^{n} \frac{a_{-i}}{10^i} = \frac{a'10^n + a_{-1}10^{n-1} + \cdots + a_{-n}}{10^n} = \frac{a'a_{-1}a_{-2}\cdots a_{-n}}{10^n}$$

onde $a' = a_m a_{m-1}\cdots a_1 a_0$

Reciprocamente, seja $\alpha = a_m a_{m-1}\cdots a_1 a_0 \in \mathbb{Z}$.

Então,

$$a = \frac{a_m a_{m-1}\cdots a_1 a_0}{10^n} = \frac{\sum_{i=0}^{m} a_i 10^i}{10^n} = \frac{a_m}{10^{n-m}} + \frac{a_{m-1}}{10^{n-m+1}} + \cdots + \frac{a_1}{10^{n-1}} + \frac{a_0}{10^n} \tag{4.6}$$

Agora, se $n = m$ temos:

$$a = a_m + \frac{a_{m-1}}{10} + \frac{a_{m-2}}{10^2} + \cdots + \frac{a_1}{10^{m-1}} + \frac{a_0}{10^m} = a_m, a_{m-1}a_{m-2}\cdots a_1 a_0.$$

Se $n > m$, então existe $k \in \mathbb{N}$ tal que $n = m + k$.

Então, de 4.6 vem:

$$a = \frac{a_m}{10^k} + \frac{a_{m-1}}{10^{k+1}} + \cdots + \frac{a_1}{10^{m-1}} + \frac{a_0}{10^m} = 0, \underbrace{0\cdots 0}_{k-zeros} a_m a_{m-1}\cdots a_1 a_0.$$

Se $n < m$, então existe $k \in \mathbb{N}$ tal que $n = m - k$.

Então,

$$a = \frac{a_m}{10^{-k}} + \frac{a_{m-1}}{10^{-k+1}} + \cdots + \frac{a_1}{10^{m-(k+1)}} + \frac{a_0}{10^{m-k}} =$$

$$= a_m 10^k + a_{m-1} 10^{k-1} + \cdots + a_1 10^{k-(m-1)} + a_0 10^{k-m} =$$

$$= a_m a_{m-1} \cdots a_{m-k}, a_{m-(k+1)} \cdots a_1 a_0.$$

Em qualquer caso, a dízima resultante é finita. □

Decorre desse resultado que toda expressão decimal de um número inteiro é um caso particular de uma dízima finita. De fato, dado $a = a_m a_{m-1} \cdots a_1 a_0 \in \mathbb{Z}$, basta pôr $\alpha = a_m a_{m-1} \cdots a_1 a_0 0$ e $n = 1$, e teremos

$$\frac{a_m a_{m-1} \cdots a_1 a_0 0}{10^1}$$

Por outro lado, segue da Definição 4.2 que a dízima finita $a_m a_{m-1} \cdots a_1 a_0, 0$ coincide com a expressão decimal do inteiro a acima. Com efeito,

$$a_m a_{m-1} \cdots a_1 a_0, 0 = a + \sum_{i=1}^{\infty} \frac{0}{10^i} = a + 0 = a$$

Com isto, temos provado que toda expressão decimal real a de parte não-inteira nula representa um número inteiro de expressão decimal igual a parte inteira de a, resultado que destacamos a seguir, e determina uma "imersão"das expressões decimais inteiras no conjunto das expressões decimais reais:

Corolário 4.1. *Se $a = a', 0$ é o número real tal que $a' = a_n a_{n-1} \cdots a_1 a_0$, então $a = a' \in \mathbb{Z}$, ou, equivalentemente,*

$$a', 0 = a'$$

4.2 O Algoritmo do Par Binário para dividendos reais quaisquer

4.2.1 Dividendos que admitem representação decimal finita

Uma vez de posse dos resultados da seção precedente referentes à natureza finita ou infinita das expressões decimais, abordaremos agora o problema de generalizar o Teorema 3.1 a dividendos

reais. No caso das expansões finitas, o que temos em mente é associar uma dada expressão decimal real a uma expressão decimal em $\mathbb{Z}$ que lhe seja equivalente num sentido que se tornará claro no decorrer desta seção.

Para tanto, dadas duas dízimas $a \in \mathbb{R}$ e $b \in \mathbb{R}^*$, precisamos ainda investigar qual a relação entre as finitudes de a e de b com a finitude do quociente $\frac{a}{b}$. Nesse problema mais geral, o questionamento chave seria: Sendo a finita, é $\frac{a}{b}$ sempre finita? A resposta geral, evidentemente, é não. De fato, pondo $a = 1$ e $b = 3$, temos a finita enquanto $\frac{a}{b} = 0,333\cdots$ é infinita. Por outro lado, se $a = 0,333\cdots$ e $b = 0,666\cdots$ temos $\frac{a}{b} = \frac{1}{2} = 0,5$, que é uma dízima finita. Além disso, já vimos que sendo $a \in \mathbb{Z}$ e $n \in \mathbb{N}$, $\frac{a}{10^n}$ é finita, e concluímos que a finitude do quociente não está condicionada à finitude do dividendo, em geral.

Na proposição a seguir, veremos que, felizmente, não é esse o caso dos quocientes de divisor 2. Nela provaremos que dada uma expressão decimal a finita, a expressão decimal de $\frac{a}{2}$ também será finita, valendo a recíproca; isto é: se $b \in \mathbb{R}$ admite uma representação finita, então existe $a \in \mathbb{R}$ decimal finita tal que $b = \frac{a}{2}$.

Proposição 4.2. *$a = a', a_{-1}a_{-2}a_{-3}\cdots a_{-m}\cdots$ é uma dízima finita se, e somente se,*

$$\frac{a}{2} = b', b_{-1}b_{-2}b_{-3}\cdots b_{-m}\cdots$$

é uma dízima finita

Demonstração. ($\Rightarrow$) Seja $a = a', a_{-1}a_{-2}a_{-3}\cdots a_{-m}\cdots$. Pela Proposição 4.1, existe $\alpha \in \mathbb{Z}$ tal que

$$a = \frac{\alpha}{10^m}. \tag{4.7}$$

Dividindo os dois membros de 4.7 por 2, segue que

$$\frac{a}{2} = \frac{\alpha}{2 \cdot 10^m} = \frac{5\alpha}{10 \cdot 10^m} = \frac{5\alpha}{10^{m+1}} \tag{4.8}$$

Como $5\alpha \in \mathbb{Z}$, segue pela Proposição 4.1 que (4.8) é uma dízima finita, e daí, $\frac{a}{2}$ é uma dízima finita.

($\Leftarrow$) Seja $\frac{a}{2} = b', b_{-1}b_{-2}b_{-3}\cdots b_{-m}$. Pela Proposição 4.1 existe $\alpha' \in \mathbb{Z}$ tal que

$$\frac{a}{2} = \frac{\alpha'}{10^m} \text{ e daí, } a = \frac{2\alpha'}{10^m}.$$

Como $\alpha' \in \mathbb{Z}$, segue que $2\alpha' \in \mathbb{Z}$, e daí a mesma proposição nos garante que a é uma dízima finita. □

Em outras palavras, o resultado nos diz que a finitude de uma dízima é invariante pela divisão por 2. Em particular, se a admite uma representação em dízima finita, o uso da representação finita de a nos retornará um $\frac{a}{2}$ em representação finita; ao passo que se tomarmos a em representação infinita, a dízima $\frac{a}{2}$ também o será. No primeiro caso, a proposição a seguir estende o algoritmo do par binário às dízimas finitas:

Proposição 4.3. *Seja $a = a', a_{-1}a_{-2}a_{-3}\cdots a_{-m}$ uma dízima finita. Se $\gamma = c_{n+m+1}c_{n+m}\cdots c_1 0$ é um inteiro tal que $\gamma = a \cdot 10^{m+1}$, então*

$$\frac{a}{2} = \frac{a'}{2} + 0, \beta(c_m)\beta(c_{m-1})\cdots\beta(c_1)\beta(0) = \frac{a'}{2} + 0, \beta(a_{-1})\beta(a_{-2})\cdots\beta(a_{-m})\beta(0)$$

onde $\beta(a_i) = \langle \overline{a_{i+1}}, a_i \rangle$

Demonstração. Podemos escrever:

$$\frac{a}{2} = \frac{a', a_{-1}a_{-2}a_{-3}\cdots a_{-m} \cdot 10^{m+1}}{2} \cdot \frac{1}{10^{m+1}} = \frac{\gamma}{2} \cdot 10^{-m-1}.$$

Como $\gamma \in \mathbb{Z}$, o Teorema 3.1 nos dá

$$\frac{a}{2} = (\beta(c_{n+m+1})\beta(c_{n+m})\cdots\beta(c_1)\beta(0)) \cdot 10^{-m-1} =$$

$$= \left[\sum_{i=1}^{n+m+1} \beta(c_i)10^i + \beta(0) \right] \cdot 10^{-m-1} =$$

$$= \left\langle \overline{0}, c_{n+m+1} \right\rangle \langle \overline{c_{n+m+1}}, c_{n+m} \rangle \cdots \langle \overline{c_1}, 0 \rangle \cdot 10^{-m-1} =$$

$$= \left\langle \overline{0}, c_{n+m+1} \right\rangle \cdots \langle \overline{c_{2+m}}, c_{1+m} \rangle, \langle \overline{c_{1+m}}, c_m \rangle \cdots \langle \overline{c_1}, 0 \rangle =$$

$$= \frac{a'}{2} + 0, \beta(c_m)\cdots\beta(c_1)\beta(0).$$

Agora, basta observar que para cada i se tem $a_i = c_{m+i+1}$ □

Em termos práticos, a proposição 4.3 nos ensina que, para fins de cálculo de pares binários, podemos tratar dízimas finitas como se fossem expressões decimais inteiras, respeitando a posição da vírgula decimal e consequente distinção entre algarismos inteiros e fracionários.

Exemplo 4.2. *Para* $a = 8933,432$*, temos*

$$\frac{a}{2} = \frac{8933,4320}{2} = \langle\overline{0},8\rangle\langle\overline{8},9\rangle\langle\overline{9},3\rangle\langle\overline{3},3\rangle,\langle\overline{3},4\rangle\langle\overline{4},3\rangle\langle\overline{3},2\rangle\langle\overline{2},0\rangle = \frac{08}{2}\frac{08}{2}\frac{12}{2}\frac{12}{2},\frac{14}{2}\frac{02}{2}\frac{12}{2}\frac{00}{2} =$$

$$= 4466,7160.$$

Para $a = 1047$*, temos*

$$\frac{1047}{2} = \frac{1047,0}{2} = \langle\overline{0},1\rangle\langle\overline{1},0\rangle\langle\overline{0},4\rangle\langle\overline{4},7\rangle,\langle\overline{7},0\rangle = 0523,5.$$

Para $a = 3,123$*, temos:*

$$\frac{3,123}{2} = \frac{3,1230}{2} = \langle\overline{0},3\rangle\langle\overline{3},1\rangle\langle\overline{1},2\rangle\langle\overline{2},3\rangle,\langle\overline{3},0\rangle = 1,5615$$ □

4.2.2 Dividendos expressos em representação decimal infinita

Conforme observa Lima ([16], p. 66), não é possível efetuar as quatro operações com as dízimas infinitas usando-as integralmente. Em particular, se $a = a',a_{-1}a_{-2}a_{-3}\cdots a_{-m}\cdots$ é uma dízima infinita, não é possível recorrer ao algoritmo tradicional no cálculo de $\frac{a}{2}$, já que este se desenvolve da direita para a esquerda, ao passo que as dízimas denotam-se no sentido oposto. Tal inconveniente, no entanto, não constitui uma barreira à aplicação do algoritmo do par binário, uma vez que este não baseia-se na adoção de uma ordem fixa de manipulação, podendo, pois, ser desenvolvido da esquerda para a direita, se assim o quisermos.

Nesse contexto, a única barreira que persiste refere-se à impossibilidade óbvia de se calcularem os infinitos pares binários provenientes da expansão infinita do dividendo. A solução clássica para tal entrave, como observa Lima ([16]), consiste na obtenção de aproximações sucessivas do quociente real por meio de racionais expressos em dízimas finitas, com cada vez mais algarismos não-inteiros, "tanto mais aproximados quanto maior for m [o número de algarismos adotados no dividendo]" (idem, p.66).

É esta a estratégia de que faremos uso a partir de então. Para tanto, definimos:

Definição 4.3 (Aproximação e Erro)**.** Seja $a = a', a_{-1}a_{-2}a_{-3}\cdots a_{-m}\cdots$ e $q = b', b_{-1}b_{-2}b_{-3}\cdots b_{-m}\cdots$ dízimas infinitas tais que $q = \frac{a}{2}$. Dizemos que uma dízima finita $q' < q$ é uma aproximação por falta de q se existe uma função

$$E : [0,q) \cap \left\{ \frac{\alpha}{10^k} : \alpha \in \mathbb{N} \; e \; k \in \mathbb{N}^* \right\} \longrightarrow (0,q] \tag{4.9}$$

Tal que

$$E(q') = q - q'$$

Nessas condições, dizemos que E é o *Erro por falta* na aproximação de q por q'.

Neste ponto cabem duas observações: a primeira é a de que E está bem definida. De fato, a proposição 4.2 nos assegura que sempre é possível obter dízimas infinitas a e q como acima. A segunda, é a de que poderíamos definir, de maneira análoga ao que fizemos, a *aproximação por excesso* e o *erro por excesso*. Não o faremos, entretanto, por não haver nenhum ganho sensível teórica ou praticamente no que segue, se assim o fizermos.

Finalmente, a função E nos fornece a "distância"entre o valor real de q e a sua aproximação racional (e de expansão finita) q'. Em particular, dadas duas aproximações distintas q' e q'' de q, dizemos que q' é melhor aproximação (por falta) de q do que q'' quando $E(q') < E(q'')$.

Evidentemente, sendo q uma dízima infinita, o processo de obtenção de aproximações finitas cada vez melhores de q que citamos acima e de que trata Lima (idem) pode ser repetido infinitamente, bastando, para isso, tomarmos a próxima aproximação com mais algarismos do que a sua precedente. No entanto, se fixarmos um número de algarismos para a aproximação desejada, podemos obter uma aproximação melhor do que qualquer outra tomada com o mesmo número de algarismos. É disto que trata a definição que propomos a seguir:

Definição 4.4. Seja q uma dízima infinita. Damos o nome de *m-aproximação ótima* de q, e denotaremos por "$A_m(q)$"(ou simplesmente "A_m"quando não houver possibilidade de confusão quanto à dízima a que estamos nos referindo) à dízima finita com m algarismos fracionários tal que

$$E(A_m(q)) < E(q')$$

Para toda aproximação q' do domínio de E com m algarismos fracionários.

A proposição a seguir assegura a existência de $A_m(q)$ e nos mostra como a obter a partir de qualquer q.

Proposição 4.4. *Se $q = b', b_{-1}b_{-2}b_{-3}\cdots b_{-m}\cdots$ é uma dízima infinita, então a m-aproximação ótima de q é dada por*

$$A_m(q) = b', b_{-1}b_{-2}b_{-3}\cdots b_{-m}$$

Demonstração. :

Seja $q' = b', b_{-1}\cdots\tilde{b}_{-m}$ tal que $\tilde{b}_{-m} \neq b_m$. Se $\tilde{b}_{-m} > b_{-m}$, temos que $q' > q$ e q' não é uma aproximação por falta de q. Suponhamos então $\tilde{b}_{-m} < b_{-m}$.
Então,

$$E(q') = q - q' = 0,0\cdots(b_m - \tilde{b}_{-m})\cdots > 0,0\cdots(b_{-m} - b_{-m})\cdots = q - A_m(q) = E(A_m(q))$$

Logo, $E(A_m(q)) < E(q')$ para todo $q' \neq A_m(q)$ □

O ponto fundamental da proposição 4.4 é o fato de que ela nos diz que os m algarismos de uma m-aproximação ótima são todos exatos; isto é, a sequência $b_{-1}, b_{-2}, \cdots, b_{-m}$ dos algarismos fracionários de $A_m(q)$ coincide com a sequência dos m primeiros dígitos não-inteiros de q. Tal fato será importante na demonstração do próximo resultado:

Proposição 4.5. *Se $a = a', a_{-1}a_{-2}a_{-3}\cdots a_{-m}\cdots$ é uma dízima infinita e $q = \dfrac{a}{2}$, então*

$$A_m(q) = \frac{a'}{2} + 0, \beta(a_{-1})\cdots\beta(a_{-m})$$

é a m-aproximação ótima de q, onde $\beta(a_i) = \langle\overline{a_{i+1}}, a_i\rangle$

Demonstração. :

Pela Proposição 4.4, $A_m(q) = a', a_{-1}a_{-2}a_{-3}\cdots a_{-m}$ é a $m-$aproximação ótima de a. Sendo $A_m(q)$ uma dízima finita, o Teorema 4.3 nos diz que

$$\frac{A_m(a)}{2} = \frac{a'}{2} + 0, \beta(a_{-1})\cdots\beta(a_{-m})\beta(0).$$

Ainda pela Proposição 4.4, os m primeiros algarismos não-inteiros de $\frac{A_m(a)}{2}$ são exatos, e daí, $\frac{a'}{2} + 0,\beta(a_{-1})\cdots\beta(a_{-m}) = A_m(q)$ é a m-aproximação ótima de q. □

Exemplo 4.3. *A 4-aproximação ótima do quociente* $q = \frac{a}{2}$ *onde* $a = 0,333\cdots$ *é*

$$A_4(a) = \frac{0,3333}{2} = \langle\overline{0},0\rangle, \langle\overline{0},3\rangle \langle\overline{3},3\rangle \langle\overline{3},3\rangle \langle\overline{3},3\rangle = 0,1666$$ □

Para fins práticos, a proposição 4.5 já nos possibilita determinar a aproximação de quocientes com qualquer precisão desejada, o que já seria suficiente para os objetivos a que nos propusemos neste capítulo. No entanto, para tornar este estudo mais completo, gostaríamos de mostrar que a sequência de aproximações $(A_n(q))_{n\in\mathbb{N}}$ de fato define o número real q. Com isto, obteremos a generalização definitiva do nosso algoritmo ao universo $\mathbb{R}$. Para esse fim, precisaremos antes provar o lema seguinte:

Lema 4.1. *Seja* $q = a', a_{-1}a_{-2}a_{-3}\cdots a_{-m}\cdots$ *uma dízima infinita. O erro* $E(A_k(q))$ *cometido quando substituímos* q *por* $A_k(q)$ *é menor do que* $\frac{1}{10^k}$

Demonstração. :

Pela Proposição 4.4, temos $A_k(q) = a', a_{-1}a_{-2}a_{-3}\cdots a_{-m}\cdots$. Nessas condições, temos

$$E(A_k(q)) = q - A_k(q) = 0, \underbrace{0\cdots0}_{k-ordens}\ a_{-k-1}\cdots < 0, \underbrace{0\cdots01}_{k-ordens} = \frac{1}{10^k}$$

□

Estamos agora em condições de provar o resultado principal do capítulo:

Teorema 4.2 (Algoritmo do par binário para dízimas infinitas)**.** *:*
Com as notações anteriores, se $a = a', a_{-1}a_{-2}a_{-3}\cdots a_{-m}\cdots$, *então*

$$q = \frac{a'}{2} + 0,\beta(a_{-1})\cdots\beta(a_{-m})\cdots$$

onde $\beta(a_i) = \langle\overline{a_{i+1}}, a_i\rangle$

Demonstração. :

Seja $A_k = A_k(q)$ a k-aproximação ótima de q e considere a sequência $(A_1, A_2, \cdots, A_n, \cdots)$. Pela Definição 4.3, temos

$$0 \leq A_1 \leq A_2 \leq \cdots < q \quad \text{e} \quad q \geq E(A_1) \geq E(A_2) \geq \cdots \geq E(A_n) \geq \cdots > 0 \tag{4.10}$$

e daí, as sequências $(A_n)_{n\in\mathbb{N}}$ e $(E(A_n))_{n\in\mathbb{N}}$ são monótonas limitadas, logo, convergentes (ver [17],p.26, Teo.4).

Por outro lado, de 4.10 e do Lema 4.1 que

$$0 < E(A_n) < \frac{1}{10^n} \tag{4.11}$$

e o *teorema do confronto de limites* (idem, p.27, Teo. 6)[2], nos dá

$$0 = \lim 0 < \lim E(A_n) < \lim \frac{1}{10^n} = 0 \text{ , o que implica que } \lim E(A_n) = 0.$$

Daí segue que $\lim(q - A_n) = 0$.

Agora, como a sequência constante converge, temos então[3]:

$\lim q - \lim A_n = 0$, do que decorre $q - \lim A_n = 0$ e, finalmente, $\lim A_n = q$.

Logo, a sequência $(A_n)_{n\in\mathbb{N}}$ converge para q, o que equivale a dizer que

$$q = \frac{a'}{2} + 0, \beta(a_{-1}) \cdots \beta(a_{-m}) \cdots .$$

□

Exemplo 4.4. *Para* $a = 53,121212\cdots$, *temos*

$$\frac{a}{2} = \langle\overline{0},5\rangle \langle\overline{5},3\rangle, \langle\overline{3},1\rangle \langle\overline{1},2\rangle \langle\overline{2},1\rangle \langle\overline{1},2\rangle \langle\overline{2},1\rangle \langle\overline{1},2\rangle \cdots = 26,560606\cdots$$

Para $a = 0,10110011\cdots$, *temos*

$$\frac{a}{2} = 0, \langle\overline{0},1\rangle \langle\overline{1},0\rangle \langle\overline{0},1\rangle \langle\overline{1},1\rangle \langle\overline{1},0\rangle \langle\overline{0},0\rangle \langle\overline{0},1\rangle \langle\overline{1},1\rangle \cdots = 0,05055005\cdots$$

[2]Teorema do confronto (ou do sanduíche): "Se $\lim x_n = \lim y_n = a$ e $x_n \leq z_n \leq y_n$ para todo n suficientemente grande, então $\lim z_n = a$"

[3]Se duas sequências x_n e y_n convergem, então $lim(x_n + y_n) = limx_n + limy_n$ (ver [17]: p. 28, Teorema 8).

Para $a = \pi = 3,1415926\cdots$, *temos*

$$\frac{a}{2} = \langle\overline{0},3\rangle, \langle\overline{3},1\rangle \langle\overline{1},4\rangle \langle\overline{4},1\rangle \langle\overline{1},5\rangle \langle\overline{5},9\rangle \langle\overline{9},2\rangle \langle\overline{2},6\rangle \cdots = 1,5707963\cdots \qquad \square$$

Para concluir o capítulo, gostaríamos de estabelecer uma notação que unificasse os teoremas 3.1, 4.2 e a proposição 4.3. Isto é possível se considerarmos que uma expressão decimal em $\mathbb{Z}$ é um caso particular de uma expressão decimal finita (corolário 4.1), e esta, por sua vez, admite uma representação em dízima infinita.

Para tanto, seja $a = a', a_{-1}a_{-2}a_{-3}\cdots a_{-m}\cdots$ uma expressão decimal genérica com $a' = a_n a_{n-1} \cdots a_1 a_0$. Podemos escrever

$$a = \sum_{i\in I} a_i 10^i \tag{4.12}$$

desde que definamos:

- $I = \{n, \cdots, 1, 0\} \subset \mathbb{N}$, quando a for uma expressão decimal em $\mathbb{Z}$;
- $I = \{n, \cdots, 1, 0, -1, \cdots -m\} \subset \mathbb{Z}$, quando a for uma dízima finita; e
- $I = \{n, \cdots, 1, 0, -1, \cdots -m\cdots\} \subset \mathbb{Z}$ quando a uma dízima infinita.

Nessas condições, reescreveremos os três teoremas anteriores de maneira unificada como se segue:

Teorema 4.3. *Seja* $a = \sum_{i\in I} a_i 10^i \in \mathbb{R}$ *e* $I \subset \mathbb{Z}$ *um conjunto de índices adequado à representação decimal de* a. *Se* $\beta(a_i) = \langle\overline{a_{i+1}}, a_i\rangle$, *então*

$$\frac{a}{2} = \sum_{i\in I} \beta(a_i) 10^i.$$

Tal notação sintética será útil no prosseguir do trabalho, sempre que precisarmos apresentar definições ou resultados que independam da expansão de a.

5 ITERAÇÃO DE QUOCIENTES

5.1 Quocientes Iterados

Tendo ampliado o raio de ação de nosso algoritmo no capítulo precedente, generalizando de $\mathbb{Z}$ para $\mathbb{R}$ o domínio dos dividendos aos quais se aplica, voltamos nossa atenção agora para a aplicação da teoria desenvolvida até aqui à determinação de quocientes cujo divisor não seja necessariamente igual a 2. Conscientes, no entanto, de que uma generalização a todo divisor $b \in \mathbb{R}^*$ é impossível no âmbito das fronteiras naturalmente impostas ao nosso trabalho, nos limitaremos a tratar do caso $b = 2^n,\ n \in \mathbb{N}^*$, que se constitui, como se sabe, uma aplicação natural e imediata da divisão por 2. De fato, dividir por 4 equivale a dividir duas vezes consecutivas por 2 (pois $\frac{a}{4} = \frac{a}{2^2} = a \cdot \frac{1}{2} \cdot \frac{1}{2}$); dividir por 8 equivale a dividir três vezes consecutivas por 2 (pois $\frac{a}{8} = \frac{a}{2^3} = a \cdot \frac{1}{2} \cdot \frac{1}{2} \cdot \frac{1}{2}$), e dividir por 16 equivale a dividir quatro vezes seguidas por 2 (pois $\frac{a}{16} = \frac{a}{2^4} = a \cdot \frac{1}{2} \cdot \frac{1}{2} \cdot \frac{1}{2} \cdot \frac{1}{2}$), por exemplo.

Mais geralmente, para $q = \frac{a}{2^n}$, $a \in \mathbb{R}$, $n \in \mathbb{N}^*$, considere a sequência $(q_i)_{i \geq 1}$ tal que

$$q_i = \begin{cases} \frac{a}{2} & \text{se} \quad i = 1 \\ \\ \frac{q_{i-1}}{2} & \text{se} \quad i > 1 \end{cases} \tag{5.1}$$

isto é, considere a sequência iniciada pela metade do dividendo $a \in \mathbb{R}$ e cujos termos posteriores são sempre iguais à metade de seu antecessor na sequência. É imediato que (q_i) assim definida é uma progressão geométrica de primeiro termo $q_1 = \frac{a}{2}$ e razão $r = \frac{1}{2}$, do que segue (ver Morgado: [24], p.21) que podemos expressar seu termo geral na forma

$$q_i = \frac{a}{2} \cdot \left(\frac{1}{2}\right)^{i-1} = \frac{a}{2} \cdot \frac{1}{2^{i-1}} = \frac{a}{2^i}$$

Do exposto, segue que $q_n = \frac{a}{2^n} = q$, e daí, a iteração n vezes da operação de divisão por 2 a partir

de $a \in \mathbb{R}$ nos retorna o quociente desejado. Em vista disso, definimos:

Definição 5.1. Seja $a \in \mathbb{R}$. Damos o nome de *Iteração sobre a* à sequência definida por

$$q_i(a) = \frac{a}{2^i}, \quad i \in \mathbb{N}^*$$

e de k-iterado de a ao seu k-ésimo termo $q_k(a)$.

Usando essa nomenclatura [1], sintetizamos o raciocínio anterior na proposição seguinte:

Proposição 5.1. *Sejam $a \in \mathbb{R}$ e $n \in \mathbb{N}^*$ tais que $q = \frac{a}{2^n}$. Se $(q_i(a))_{i\geq 1}$ é a iteração sobre a, então o valor de q coincide com o do n-iterado de a; isto é,*

$$q = q_n$$

Demonstração. (Indução sobre n) Para $n = 1$, é imediato. Supondo que $q = q_n$ para algum $n \in \mathbb{N}^*$, então temos $q = \frac{a}{2^{n+1}} = \frac{\left(\frac{a}{2^n}\right)}{2} = \frac{q_n}{2} \overset{(5.1)}{=} q_{n+1}$, donde a proposição é verdadeira para $n+1$, e, por indução, para todo $n \in \mathbb{N}^*$ □

Exemplo 5.1. *Para $q = \frac{115}{2^3}$ temos, pelo Teorema 4.3:*

$q_1 = \beta(1)\beta(1)\beta(5), \beta(0) = 057,5$
$q_2 = \beta(5)\beta(7), \beta(5)\beta(0) = 28,75$
$q_3 = \beta(2)\beta(8), \beta(7)\beta(5)\beta(0) = 14,375,$

e daí, segue que $q = 14,375$. □

Vale comentar que o processo de iteração que fizemos acima e provamos na proposição 5.1 possui a vantagem teórica de possibilitar a omissão de uma série de considerações preliminares referentes à finitude das expansões de a e de $q = \frac{a}{2^n}$. De fato, uma vez que $q = q_n$ e $q_i = \frac{q_{i-1}}{2}$ para $2 \leq$

[1] Sempre que não houver possibilidade de confusão usaremos indicar o k-iterado $q_k(a)$ simplesmente pela notação mais limpa "q_k", reservando a notação completa para quando precisarmos tratar de mais de um dividendo no mesmo contexto.

$i \leq n$, a aplicação repetida da proposição 4.2 nos diz que q admite representação em dízima finita se, e somente se, q_{n-1} admite representação em dízima finita, se, e somente se, q_{n-2} admite representação em dízima finita, e, prosseguindo com esse raciocínio, concluímos que isto ocorre se, e somente se, a admite representação em dízima finita.

Desse modo, para calcularmos $q = \dfrac{a}{2^n}$ basta que procedamos como no exemplo 5.1 aplicando n vezes seguidas o teorema 4.3. Além disso, a finitude da expansão decimal de $q_n = q$ será a mesma da expansão de a.

5.2 Par Binário Composto

Na discussão acima, vimos que a proposição 5.1 estende o teorema 4.3 aos quocientes com divisores do tipo 2^n, sem a necessidade de quaisquer considerações adicionais, a não ser o uso do raciocínio recursivo. Na verdade, tendo em vista os objetivos iniciais deste capítulo, isto seria o suficiente para considerarmos nossa meta atingida. No entanto, gostaríamos de obter uma técnica mais refinada e eficiente para a obtenção de quocientes a partir da iteração. De fato, apesar do uso dessa técnica tal como a fizemos no exemplo 5.1 ser um procedimento eficaz, a necessidade de determinar cada q_{i-1} antes de cada q_i pode revelar-se um trabalho penoso, sobretudo nos casos em que o número de algarismos de a ou a quantidade de iterações for grande. Isso deve-se ao fato de o processo apresentado ser um procedimento "horizontal"; isto é, imaginando cada q_i como uma linha de uma matriz, a linha q_{i+1} só pode ser obtida após a determinação completa da linha q_i; em particular, se q_i expressa uma dízima infinita, o procedimento descrito não nos permite obter q_{i+1}.

Queremos agora estabelecer um procedimento "vertical"; isto é, um procedimento que em lugar da iteração dos quocientes, foque na iteração de cada algarismo do dividendo em separado, de modo a que a determinação de uma coluna fique condicionada à completa determinação de sua vizinha imediata de ordem superior. Para tanto, precisaremos da introdução de alguns conceitos complementares de cuja discussão nos ocuparemos em todo o restante do capítulo: o primeiro deles o definiremos a seguir, e consiste numa generalização do conceito de par binário:

Definição 5.2. Seja $n \in \mathbb{N}^*$ e $I \subset \mathbb{Z}$ um conjunto de índices e $a = \sum_{i \in I} a_i 10^i \in \mathbb{R}$. Damos o nome de *Par Binário Composto* à função $\beta^n : \mathbb{A} \longrightarrow \mathbb{A}$ definida pela recorrência

$$\beta^n(a_i) = \begin{cases} \beta(a_i) = \langle \overline{a_{i+1}}, a_i \rangle, & \text{se} \quad n = 1 \\ \beta(\beta^{n-1}(a_i)) = \left\langle \overline{\beta^{n-1}(a_{i+1})}, \beta^{n-1}(a_i) \right\rangle, & \text{se} \quad n > 1 \end{cases}.$$

Para referência futura, diremos que

$$(\beta^n(a_i))_{n\geq 1} \tag{5.2}$$

é a sequência de pares binários gerada por a_i . No entanto, quando quisermos nos referir aos k primeiros termos de 5.2, escreveremos

$$[a_i]_k = \Big(\beta(a_i), \beta^2(a_i), \beta^3(a_i), \cdots, \beta^k(a_i)\Big) \tag{5.3}$$

Na proposição a seguir, apresentaremos algumas propriedades do par binário composto:

Proposição 5.2 (Propriedades)**.** *O Par Binário Composto possui as seguintes propriedades:*

(i) $\beta(\beta^n(a_i)) = \beta^n(\beta(a_i))$, *para todo* $n \in \mathbb{N}^*$;

(ii) $\beta^n(\beta^m(a_i)) = \beta^m(\beta^n(a_i))$, *para todo* $m, n \in \mathbb{N}^*$;

(iii) $\beta^n(\langle\overline{a_{i+1}}, a_i\rangle) = \Big\langle\overline{\beta^n(a_{i+1})}, \beta^n(a_i)\Big\rangle$;

(iv) Se $\beta(1) = 0$, *então* $\langle 0, \beta^n(1)\rangle = 0$ *para todo* $n \in \mathbb{N}^*$.

Demonstração. :

(i) Para $n = 1$, é imediato. Suponha que para certo $n \in \mathbb{N}^*$ a propriedade se verifique; então, para $n+1$ temos, por definição:

$$\beta(\beta^{n+1}(a_i)) = \beta(\beta(\beta^n(a_i))),$$

e pela hipótese de indução e Definição 5.2, por sua vez,

$$\beta(\beta(\beta^n(a_i))) = \beta(\beta^n(\beta(a_i))) = \beta^{n+1}(\beta(a_i))$$

e a propriedade é válida para $n+1$ e, consequentemente, para todo $n \in \mathbb{N}^*$.

(ii) Para $n = 1$ a validade é garantida por (i). Supondo que exista $n \in \mathbb{N}^*$ tal que a propriedade seja válida, segue então, pela Definição 5.2, que

$$\beta^{n+1}(\beta^m(a_i)) = \beta(\beta^n(\beta^m(a_i))),$$

e daí,pela hipótese de indução e pela Definição 5.2, temos

$$\beta(\beta^n(\beta^m(a_i))) = \beta(\beta^{n+m}(a_i)) = \beta^{n+m+1}(a_i).$$

e daí, a propriedade é verdadeira para todo $n \in \mathbb{N}^*$.

(iii) Pelo Teorema 4.3 e por (i), temos $\beta^n(\langle\overline{a_{i+1}}, a_i\rangle) = \beta^n(\beta(a_i)) = \beta(\beta^n(a_i)) =$

$= \left\langle\overline{\beta^n(a_{i+1})}, \beta^n(a_i)\right\rangle$.

(iv) Para $n = 1$, temos $\langle 0, \beta(1)\rangle = \langle 0, 0\rangle = 0$.

Supondo que $\langle 0, \beta^n(1)\rangle = 0$ para certo $n \in \mathbb{N}^*$, temos então, de (i) e de (iii), que

$$\left\langle 0, \beta^{n+1}(1)\right\rangle = \langle \beta(1), \beta(\beta^n(1))\rangle = \langle \beta(0), \beta(\beta^n(1))\rangle = \beta(\langle 0, \beta^n(1)\rangle),$$

e a hipótese de indução nos diz que $\beta(\langle 0, \beta^n(1)\rangle) = \beta(0) = 0$. Logo, a propriedade é válida para $n+1$, e daí, para todo $n \in \mathbb{N}^*$. □

Queremos, com a Definição 5.2, introduzir algo similar à iteração de quocientes em $\mathbb{R}$ ao universo de $\mathbb{A}$, o que transferirá o cálculo de $q_k(a)$ à determinação de cada um de seus algarismos tomados isoladamente, o que trará consigo alguns benefícios, de que trataremos no momento adequado. Para tanto, enunciamos, a seguir, o teorema que confirma tal possibilidade:

Teorema 5.1 (Algoritmo do Par Binário Composto)**.** *: Sejam $a \in \mathbb{R}$ e I um conjunto de índices adequado à expansão decimal de a.*

$$\textit{Se } a = \sum_{i\in I} a_i 10^i \textit{ e } \frac{a}{2^n} = \sum_{i\in I} b_i 10^i, \textit{ então } b_i = \beta^n(a_i) \textit{ para todo } i \in I.$$

Demonstração. (Indução sobre n):

Se $n = 1$, temos o Teorema 4.3, que sabemos ser verdadeiro.

Suponhamos então que para certo $n \in \mathbb{N}^*$ o resultado seja válido. Então, para $n+1$ devemos ter:

$$q = \frac{a}{2^{n+1}} = \frac{\left(\frac{a}{2^n}\right)}{2},$$

ou ainda, usando a hipótese de indução:

$$q = \frac{\sum_{i\in I} \beta^n(a_i) 10^i}{2}.$$

Agora, pelo Teorema 4.3 e Definição 5.2, temos:

$$q = \sum_{i \in I} \beta(\beta^n(a_i))10^i = \sum_{i \in I} \beta^{n+1}(a_i)10^i,$$

donde decorre que o resultado é válido para todo $n \in \mathbb{N}^*$ □

Antes de ilustrarmos o uso do Teorema 5.1, cabe uma observação, referente ao fato (óbvio) de que o resultado que provamos trata-se de uma releitura da Proposição 5.2 em termos de pares binários compostos, o que pode parecer redundante numa primeira análise. Perceba-se, no entanto, que ao contrário daquela proposição, que focava na iteração de quocientes tomando cada iterado a partir do seu precedente, o teorema que provamos foca na sequência $[a_i]$. De fato, ao afirmar que $\beta^n(a_i)$ é o dígito de ordem i em q, o teorema nos autoriza a usar a definição 5.2, segundo a qual teremos $\beta^n(a_i) = \beta(\beta^{n-1}(a_i))$, iniciando um processo recursivo sobre a ordem i em cada iterado de a, conforme ilustraremos a seguir:

Exemplo 5.2. *Calculemos* $q = \dfrac{358}{2^4}$*:*

Usando o teorema 5.1 e a proposição 5.2 (i)*, temos:*

$q = \beta^4(3)\beta^4(5)\beta^4(8), \beta^4(0) =$

$= \beta^3(1)\beta^3(7)\beta^3(9), \beta^3(0)\beta^3(0) =$

$= \beta^2(0)\beta^2(8)\beta^2(9), \beta^2(5)\beta^2(0) =$

$= \beta(0)\beta(4)\beta(4), \beta(7)\beta(5)\beta(0) =$

$= 022,375$ □

Pelo exposto, note que agora poderíamos determinar cada algarismo a_i de q, a partir de a, sem a necessidade de se determinar os iterados q_k completamente a cada passo, isto é, o Teorema 5.1 nos permite fazer um cálculo "vertical", calculando-se os 4 primeiros termos de $[a_i]$, ao invés do cálculo "horizontal", baseado na construção da sequência $(q_j(a))_{1 \leq j \leq 4}$.

Assim, teríamos, no exemplo anterior:

$[a_2]_4 = (1,0,0,0) \Rightarrow \beta^4(3) = 0$

$[a_1]_4 = (7,8,4,2) \Rightarrow \beta^4(5) = 2$

$[a_0]_4 = (9,9,4,2) \Rightarrow \beta^4(8) = 2$

$$[a_{-1}]_4 = (0,5,7,3) \;\Rightarrow\; \beta^4(0_{-1}) = 3$$

$$[a_{-2}]_4 = (0,0,5,7) \;\Rightarrow\; \beta^4(0_{-2}) = 7$$

$$[a_{-3}]_4 = (0,0,0,5) \;\Rightarrow\; \beta^4(0_{-3}) = 5$$

Nosso objetivo, a partir de então, será o de otimizar essa técnica de cálculo, o que faremos introduzindo uma notação mais adequada, da qual trataremos em seguida.

5.3 Matriz associada a um dividendo

Nas seções 4.1 e 4.2 orientamos o processo de cálculo do quociente $q = \dfrac{a}{2^n}$ segundo a construção da iteração $(q_j(a))_{1\leq j\leq n}$ de a, o que chamamos de "cálculo horizontal"de q, e mais tarde mostramos, com o Teorema 5.1, que a expressão decimal de q poderia ser obtida mediante a construção das sequências $[a_i]_n$, com $i \in I$, o que então apelidamos de "cálculo vertical"de q.

Queremos agora dar sentido mais preciso às expressões "horizontal"e "vertical"que usamos, e mostrar, como prometemos, a vantagem do uso do processo a que se refere a última expressão. Para tanto, pondo $a = \sum_{i\in I} a_i 10^i$, doravante representaremos a sequência $[a_i]_n$ dos n primeiros pares binários do dígito a_i na forma da matriz coluna

$$[a_i]_n = \begin{pmatrix} \beta(a_i) \\ \beta^2(a_i) \\ \vdots \\ \beta^n(a_i) \end{pmatrix} \tag{5.4}$$

Por outro lado, fixando $k \in \{1,\cdots,n\}$, o Teorema 5.1 nos assegura que $q_k = \sum_{i\in I} \beta^k(a_i)10^i$, cuja expressão decimal pode ser vista como a matriz

$$\left[\beta^k(a_i)\right]_{1\times(\#I)} = [q_k] \tag{5.5}$$

que é a matriz linha usual, com tantas colunas quantas forem os elementos de I. Em particular, se $I = \{r,\cdots,1,0,-1,\cdots,-m\}$, temos

$$[q_k] = \left(\beta^k(a_r)\cdots\beta^k(a_1)\beta^k(a_0)\beta^k(a_{-1})\cdots\beta^k(a_{-m})\right). \tag{5.6}$$

Admitindo certo abuso de notação[2], a partir daqui não distinguiremos o k-iterado q_k e sua matriz associada $[q_k]$, e escreveremos $q_k = [q_k]$.

Estamos agora em condições de definir a matriz associada a um dividendo:

Definição 5.3 (Matriz associada a um dividendo)**.** Seja $q = \dfrac{a}{2^n}$, $n \in \mathbb{N}^*$ e $a = \sum_{i \in I} a_i 10^i$.

Daremos o nome de *Matriz n−ésima associada ao dividendo a* à matriz denotada por

$$[a]_n = (\alpha_{ij}) \tag{5.7}$$

com $i \in \{1, \cdots, n\}$ e $j \in I$ definida por

$$\alpha_{ij} = \beta^i(a_{k+1-j})$$

Em outras palavras, a matriz $[a]_n$ é tal que sua i-ésima linha é dada pelo iterado q_i, e sua j-ésima coluna é a matriz $[a_j]_n$, o que significa que calcular q equivale a se determinar a linha q_n de (5.7), o que, por sua vez, pode ser feito determinando-se as sequências $[a_i]_n$ que são as colunas de (5.7), o que justifica a denominação de "cálculo vertical"que fizemos, opondo-se à determinação linha a linha, que chamamos de "cálculo horizontal"por razões análogas. A titulo de ilustração, consideremos o exemplo a seguir:

Exemplo 5.3. *: Sendo* $q = \dfrac{800}{2^4}$, *temos*

$$[800]_4 = \begin{pmatrix} \beta(8) & \beta(0) & \beta(0) \\ \beta^2(8) & \beta^2(0) & \beta^2(0) \\ \beta^3(8) & \beta^3(0) & \beta^3(0) \\ \beta^4(8) & \beta^4(0) & \beta^4(0) \end{pmatrix} = \begin{pmatrix} [a_2]_4 & [a_1]_4 & [a_0]_4 \end{pmatrix} \tag{5.8}$$

Mas

[2] A identificação que fazemos aqui entre q_k e $[q_k]$ refere-se aos valores absolutos dos algarismos de q_k. A rigor, trata-se de uma bijeção entre o conjunto das matrizes-linha $1 \times k$ e $\mathbb{R}$ que associa a cada expressão decimal q a matriz cujos termos são os dígitos de q tomados ordenadamente da esquerda para direita.

$$[a_2]_4 = \begin{pmatrix} 4 \\ 2 \\ 1 \\ 0 \end{pmatrix} \tag{5.9}$$

e usando 5.9, temos

$$[a_1] = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 5 \end{pmatrix} \tag{5.10}$$

e usando 5.10, por sua vez, segue que:

$$[a_0] = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \tag{5.11}$$

E substituindo 5.9, 5.10 e 5.11 em 5.8, temos:

$$[800]_4 \overset{(5.9)}{=} \begin{pmatrix} 4 & \beta(0) & \beta(0) \\ 2 & \beta^2(0) & \beta^2(0) \\ 1 & \beta^3(0) & \beta^3(0) \\ 0 & \beta^4(0) & \beta^4(0) \end{pmatrix} = \begin{pmatrix} 4 & 0 & \beta(0) \\ 2 & 0 & \beta^2(0) \\ 1 & 0 & \beta^3(0) \\ 0 & 5 & \beta^4(0) \end{pmatrix} = \begin{pmatrix} 4 & 0 & 0 \\ 2 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 5 & 0 \end{pmatrix},$$

e daí, segue que $q = q_5 = 50$. □

5.4 Matriz do dividendo inteiro

5.4.1 Divisão euclidiana por 2^n

Interessa-nos agora abordar a divisão euclidiana por 2^n e o cálculo do quociente nessa divisão, em particular. A matriz que definiremos como resultado das considerações desta seção será muito útil em nossa proposta de otimizar o nosso algoritmo para o divisor específico que temos estudado neste capítulo.

A definição da função *Parte inteira*[3] será útil nesse contexto, em razão do que a enunciaremos a seguir:

[3]Também chamada por alguns autores de "Função maior inteiro": ver por exemplo, [27], p. 76.

Definição 5.4. Damos o nome de *Parte Inteira* à função

$$\lfloor \quad \rfloor : \mathbb{R} \longrightarrow \mathbb{Z}$$

que a cada número real $x = x' + \sum_{i \in I} x_i 10^i,\ x_i \in \mathbb{A},\ I \subset \mathbb{Z}_-$ associa a parte inteira x' de sua expressão decimal, e indicamos

$$\lfloor x \rfloor = x'$$

Assim, por exemplo, $\lfloor 2,5 \rfloor = 2$; $\lfloor 0,125 \rfloor = 0$; e $\lfloor 5 \rfloor = 5$.

Enunciaremos na proposição a seguir algumas propriedades da função parte inteira. A prova destas decorrem imediatamente da Definição 5.4 e optaremos por sua omissão:

Proposição 5.3. *: A Função Parte inteira de x possui as seguintes propriedades:*

(i) $x \in (0,1) \ \Rightarrow\ \lfloor x \rfloor = 0$;

(ii) $\lfloor x - y \rfloor = 0 \ \Rightarrow\ \lfloor x \rfloor = \lfloor y \rfloor$;

(iii) $\lfloor x \rfloor = x \Leftrightarrow x \in \mathbb{Z}$.

O problema da determinação do quociente da divisão euclidiana por 2^n está diretamente relacionado à função parte inteira. De fato, sejam $a \in \mathbb{Z}$ e $n \in \mathbb{N}$ tais que $q = \dfrac{a}{2^n}$.

Se $2^n \mid a$, então existe $b \in \mathbb{Z}$ tal que $a = 2^n b$, e daí, temos:

$$b = \frac{a}{2^n} = q \in \mathbb{Z} \text{ e } \lfloor q \rfloor = q.$$

Caso contrário, existe $b \in \mathbb{Z}$ e $r \in \mathbb{Z}$ com $0 < r < 2^n$ tais que

$$a = 2^n b + r \tag{5.12}$$

donde

$$b = \frac{a-r}{2^n} = \frac{a}{2^n} - \frac{r}{2^n} = q - \frac{r}{2^n}.$$

Note que $q \notin \mathbb{Z}$ pois 5.12 implica que

$$q - b = \frac{r}{2^n} \in (0,1) \tag{5.13}$$

e disto segue que $b = q - \frac{r}{2^n} \Rightarrow q - b = \frac{r}{2^n}$.

Agora, pela Proposição 5.3 (i) e por 5.12, temos $\lfloor q - b \rfloor = \left\lfloor \frac{r}{2^n} \right\rfloor = 0$.

Logo, da Proposição 5.3 (ii) e (iii) temos $\lfloor q \rfloor = \lfloor b \rfloor$,

e finalmente, $b = \lfloor q \rfloor$, o que nos dá o resultado seguinte:

Proposição 5.4. *Sejam $a \in \mathbb{Z}$, $b \in \mathbb{Z}, r \in \mathbb{N}^*$. Se $a = 2^n b + r$ com $0 \leq r < 2^n$, então*

$$b = \left\lfloor \frac{a}{2^n} \right\rfloor.$$

Demonstração. Efetuada. □

Corolário 5.1. *Com as hipóteses anteriores, se $a = a_k a_{k-1} \cdots a_1 a_0$ então*

$$b = \beta^n(a_k)\beta^n(a_{k-1}) \cdots \beta^n(a_0).$$

Demonstração. : Basta usar a Proposição 5.2, segundo a qual $q = q_n$. Daí, $b = \lfloor q \rfloor = \lfloor q_n \rfloor = \beta^n(a_k)\beta^n(a_{k-1}) \cdots \beta^n(a_0)$. □

O que a Proposição 5.4 nos diz, e mais propriamente o seu corolário, em termos de representação decimal, é que o quociente na divisão euclidiana de a por 2^n é dado pela n-ésima linha da matriz

$$\alpha_{ij} = \left(\beta^i(a_{k+1-j})\right)_{\substack{1 \leq i \leq n \\ 0 \leq j \leq k}}$$

obtida a partir da supressão dos termos $\beta^i(a_j)$ de $[a]_n$ tais que $j < 0$. Pela sua importância no que segue, a definiremos formalmente a seguir:

Definição 5.5. Seja $q = \dfrac{a}{2^n}$ com $a = a_k a_{k-1} \cdots a_1 a_0 \in \mathbb{Z}$ e $n \in \mathbb{N}^*$. Damos o nome de *Matriz inteira n-ésima de a* à matriz que indicaremos por $\lfloor a \rfloor_n$ tal que

$$\lfloor a \rfloor_n = \begin{pmatrix} \beta(a_k) & \cdots & \beta(a_0) \\ \vdots & & \vdots \\ \beta^n(a_k) & \cdots & \beta^n(a_0) \end{pmatrix}$$

Exemplo 5.4. *Vamos calcular o quociente da divisão euclidiana de 2417 por 2^4. Isto equivale a determinar a 4.ª linha da matriz $\lfloor 2417 \rfloor_4$:*

$$\lfloor 2417 \rfloor_4 = \begin{bmatrix} 1 & 2 & 0 & 8 \\ 0 & 6 & 0 & 4 \\ 0 & 3 & 0 & 2 \\ 0 & 1 & 5 & 1 \end{bmatrix}$$

Portanto, $\left\lfloor \dfrac{2417}{2^4} \right\rfloor = 151$ □

A proposição a seguir pode ser útil na construção de $\lfloor a \rfloor_n$, sobretudo para maiores valores de n:

Proposição 5.5. *Se $a = a_k a_{k-1} \cdots a_1 a_0 \in \mathbb{Z}$, $n \in \mathbb{N}^*$ e $\lfloor a \rfloor_n = (\alpha_{ij})_{\substack{1 \le i \le n \\ 1 \le j \le k+1}}$, então:*

(i) $\alpha_{(i+1)1} = \langle 0, \alpha_{i1} \rangle$ *para todo* $i \in \{1, \cdots, n-1\}$.
Em particular, se $\alpha_{r1} = 1$, *então,* $\alpha_{(i+1)1} = 0$ *para todo* $i \ge r$

(ii) *Se* $2 \mid \alpha_{i(s-1)}$ *para todo* $i \ge r$ *e* $r \in \{1, \cdots, n-1\}$, *então* $\alpha_{(i+1)s} = \langle 0, \alpha_{is} \rangle$.
Em particular, se $\alpha_{rs} = 1$ *e* $\alpha_{i(s-1)} = 0$ *para todo* $i \ge r$, *então* $\alpha_{(i+1)s} = 0$ *para todo* $i \ge r$

Demonstração. :

(i) Pela Proposição 5.2 e pelo Teorema 4.3, temos:

$$\alpha_{(i+1)1} = \beta^{i+1}(a_k) = \beta\left(\beta^i(a_k)\right) = \beta^i(\beta(a_k)) = \beta^i(\langle \overline{a_{k+1}}, a_k \rangle) = \left\langle \overline{\beta^i(a_{k+1})}, \beta^i(a_k) \right\rangle.$$

Mas $a_{k+1} = 0$ implica que $\beta^i(a_{k+1}) = 0$ para todo $i \in \mathbb{N}$.

Logo, $\alpha_{(i+1)1} = \langle 0, \beta^i(a_k) \rangle = \langle 0, \alpha_{i1} \rangle$.

Em particular, se $\alpha_{r1} = 1$ com $i > r$, temos que

$\alpha_{(i+1)1} = \langle 0, \beta^{i+1}(a_k) \rangle$,

e a Proposição 5.2 (ii) nos dá

$\langle 0, \beta^{i+1}(a_k) \rangle = \langle 0, \beta^{i+1-r}(\beta^r(a_k)) \rangle = \langle 0, \beta^{i+1-r}(\alpha_{r1}) \rangle = \langle 0, \beta^{i+1-r}(1) \rangle$.

E daí, da Proposição 5.2 (iv) obtemos $\langle 0, \beta^{i+1-r}(1) \rangle = 0$.

$(ii) \quad \alpha_{(i+1)s} = \beta^{i+1}(a_{k+1-s}) = \beta^i(\beta(a_{k+1-s})) = \beta^i\left(\langle \overline{a_{k+1-(s-1)}}, a_{k+1-s} \rangle\right) =$

$= \left\langle \overline{\beta^i(a_{k+1-(s-1)})}, \beta^i(a_{k+1-s}) \right\rangle = \langle \overline{\alpha_{i(s-1)}}, \alpha_{is} \rangle$.

Mas, por hipótese, $2 \mid \alpha_{i(s-1)}$, e daí, $\alpha_{(i+1)s} = \langle 0, \alpha_{is} \rangle$.

Em particular, se $\alpha_{rs} = 1$ e $\alpha_{i(s-1)} = 0$ para todo $i \geq r$, temos, então, para $i \geq r$:

$\alpha_{(i+1)s} = \langle 0, \alpha_{is} \rangle = \langle 0, \beta^i(a_{k-1+s}) \rangle = \langle 0, \beta^{i-r}(\beta^r(a_{k-1+s})) \rangle = \langle 0, \beta^{i-r}(\alpha_{rs} \rangle =$

$= \langle 0, \beta^{i-r}(1) \rangle = 0$ □

Dito de outra forma, a proposição 5.5 nos diz que, para construir $\lfloor a \rfloor_n$ é conveniente:

1. Preparar uma tabela (Matriz) cuja quantidade de linhas seja igual ao expoente do divisor e a quantidade de colunas seja igual à quantidade dígitos do dividendo;
2. Ao proceder o cálculo por colunas, perceber que o cálculo dos pares binários da primeira coluna se faz dividindo por dois o par binário precedente, se este for par, ou subtraindo uma unidade e então dividindo-o, caso seja ímpar;
3. Ao se encontrar o dígito 1 na primeira coluna, dispensar o cálculo dos demais termos, que serão todos nulos;
4. A partir da linha em que a primeira coluna se anular, tudo o que foi dito dela em (2) e (3) se aplica à segunda coluna; quando esta se anular, o mesmo se aplicará à terceira, e assim por diante.

Ilustraremos o processo no exemplo a seguir:

Exemplo 5.5. *Vamos construir a matriz* $\lfloor 312 \rfloor_7$, *e determinar* $\left\lfloor \frac{312}{2^7} \right\rfloor$ *em seguida. Para melhor visualizar a aplicação da técnica, marcaremos com pontos as células da tabela cujo cálculo é dispensável:*

$$\lfloor 312 \rfloor_7 = \begin{bmatrix} 1 & 5 & 6 \\ . & 7 & 8 \\ . & 3 & 9 \\ . & 1 & 9 \\ . & . & 9 \\ . & . & 4 \\ . & . & 2 \end{bmatrix}$$

Portanto, $\left\lfloor \frac{312}{2^7} \right\rfloor = 2$. □

5.5 Matriz complementar do dividendo inteiro

5.5.1 Redutibilidade de quocientes

No que segue, gostaríamos de admitir apenas quocientes de dividendos ímpares em nossas considerações. Para que possamos fazer isto sem prejuízo para a generalidade de nossa exposição, mostraremos que todo quociente do tipo considerado neste capítulo admite tal representação, salvo casos particulares que não requerem a teoria desta seção para o seu tratamento.

Com este objetivo, definimos:

Definição 5.6. Sejam $q = \frac{a}{2^n}$ e $p = \frac{b}{2^m}$ tais que $n, m \in \mathbb{N}^*$ e $a, b \in \mathbb{Z}$. Dizemos que p é equivalente a q, e escrevemos $p \sim q$, se p e q admitem a mesma representação decimal. Além disso, se $m > n$, dizemos que p é redutível a q.

Decorre dessa definição que se $p \sim q$ e $m > n$, temos que $\lfloor a \rfloor_n$ possui menor quantidade de linhas e colunas do que $\lfloor b \rfloor_m$, embora possuam, a menos de zeros à esquerda, a mesma linha final, já que $p_m = q_n$.

De fato, por definição, $p = q$, e daí, temos

$$a = \frac{2^n b}{2^m} = \frac{b}{2^{m-n}} \tag{5.14}$$

e a última linha de $\lfloor b \rfloor_{m-n}$ coincide com a.

Por outro lado, de (5.14),

$$q = \frac{\left(\dfrac{b}{2^{m-n}}\right)}{2^n} \text{ implica } \lfloor a \rfloor_n = \left\lfloor \frac{b}{2^{m-n}} \right\rfloor_n . \tag{5.15}$$

Mais rigorosamente, se $a = a_r a_{r-1} \cdots a_1 a_0$ e $b = b_s b_{s-1} \cdots b_1 b_0$ com $s \geq r$, temos

$$\lfloor b \rfloor_n = \left(\begin{array}{ccc|ccc} b_s & \cdots & b_{r+1} & b_r & \cdots & b_0 \\ \vdots & & \vdots & \vdots & & \vdots \\ \beta^{m-n}(b_s) & \cdots & \beta^{m-n}(b_{r+1}) & \beta^{m-n}(b_r) & \cdots & \beta^{m-n}(b_0) \\ \hline 0 & \cdots & 0 & \beta(a_r) & \cdots & \beta(a_0) \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & \beta^n(a_r) & \cdots & \beta^n(a_0) \end{array}\right) \tag{5.16}$$

E daí, considerando as matrizes

$M_{n\times r} = \lfloor a \rfloor_n$;

$N_{(m-n)\times s} = \lfloor b \rfloor_{m-n}$; e

$O_{n\times(r-s)}$ a matriz nula, podemos escrever sinteticamente:

$$\lfloor b \rfloor_n = \left(\begin{array}{c|c} N_{(m-n)\times s} & \\ \hline O_{n\times(r-s)} & M_{n\times r} \end{array}\right) \tag{5.17}$$

e daí, a matriz $\lfloor a \rfloor_n$ coincide com a matriz obtida da supressão das $m-n$ primeiras linhas e $r-s$ primeiras colunas de $\lfloor b \rfloor_n$.

Ilustrando:

Exemplo 5.6. $\dfrac{3072}{2^7}$ *é equivalente a* $\dfrac{96}{2^2}$. *Temos:*

$$\lfloor 3072 \rfloor_7 = \left(\begin{array}{cc|cc} 1 & 5 & 3 & 6 \\ 0 & 7 & 6 & 8 \\ 0 & 3 & 8 & 4 \\ 0 & 1 & 9 & 2 \\ 0 & 0 & 9 & 6 \\ \hline 0 & 0 & 4 & 8 \\ 0 & 0 & 2 & 4 \end{array}\right)$$

e

$$\lfloor 96 \rfloor_2 = \begin{pmatrix} 4 & 8 \\ 2 & 4 \end{pmatrix}$$

que pode ser obtida suprimindo-se as 5 primeiras linhas e 2 primeiras colunas de $\lfloor 3072 \rfloor_7$ □

Um quociente $q = \dfrac{a}{2^n}$ é dito irredutível quando para todo $p = \dfrac{b}{2^m}$, $m < n$, se tem $q \nsim p$. Pelas considerações anteriores, sabemos que isto equivale a dizer que $b = \dfrac{a}{2^{n-m}} \notin \mathbb{Z}$, o que ocorre se, e somente se, $2^{n-m} \nmid a$ para todo $n - m \in \mathbb{N}$.

Em particular, para $m = n - 1$ temos $2 \nmid a$, o que nos dá o resultado seguinte:

Proposição 5.6. *: $q = \dfrac{a}{2^n}$, $n \in \mathbb{N}^*$ é irredutível se, e somente se, $2 \nmid a$*

Decorre desse resultado que nem todo quociente admite um equivalente irredutível. De fato, se $2 \mid a$, então existe $R \in \mathbb{N}^*$ tal que $2^R \mid a$ e $2^{R+1} \nmid a$, donde segue que

$$\frac{a}{2^R} = q_R$$

é um inteiro ímpar, e daí,

$$q = \frac{q_R}{2^{n-R}}.$$

Nessas condições, se $n = R$, temos $q = q_R \in \mathbb{Z}$ e se $n < R$, então $q = 2^{R-n} q_R \in \mathbb{Z}$.

Por outro lado, se temos $n > R$, segue que após R iterações de a obteremos o dividendo q_R da forma irredutível de q. Em vista disso, definimos:

Definição 5.7. Seja $q = \frac{a}{2^n}$ com $a \in \mathbb{Z}$ e $n \in \mathbb{N}^*$ um quociente irredutível.
Damos o nome de *Iterações de redução de q* ao valor natural $R < n$ tal que

$$\tilde{q} = \frac{q_R}{2^{n-R}}$$

é o equivalente irredutível de q.

Exemplo 5.7. *O quociente* $q = \frac{192}{2^5}$ *não possui equivalente irredutível, pois* $\lfloor 192 \rfloor_5$ *não possui linha com dígito final ímpar:*

$$\lfloor 192 \rfloor_5 = \begin{bmatrix} 0 & 9 & 6 \\ . & 4 & 8 \\ . & 2 & 4 \\ . & 1 & 2 \\ . & . & 6 \end{bmatrix}.$$

□

Exemplo 5.8. *O quociente* $q = \frac{76}{2^4}$ *é redutível, e como*

$$\lfloor 76 \rfloor_2 = \begin{bmatrix} 3 & 8 \\ 1 & 9 \end{bmatrix}$$

segue que $\tilde{q} = \frac{19}{2^2}$ *e* $R = 2$. □

5.5.2 Parte Fracionária de um Quociente Irredutível

No exposto, vimos que dado um quociente redutível $q = \frac{a}{2^n}$, se o menor $R \in \mathbb{N}$ tal que $q = \frac{q_R}{2^{n-R}}$ com q_R ímpar é tal que $n < R$, então $q \in \mathbb{Z}$, o que significa que se q não admite forma irredutível, então $\lfloor q \rfloor = q$ e a expressão decimal de q possui parte fracionária nula.

Na verdade, a recíproca deste fato também é válida; de fato, se $q = \frac{a}{2^n}$ é irredutível, então pela proposição anterior, $2 \nmid a$, e daí, $2^n \nmid a$, donde $q \notin \mathbb{Z}$. Enunciamos a seguir esse resultado como corolário da Proposição 5.6

Corolário 5.2. *q admite parte fracionária se, e somente se, q possui equivalente irredutível.*

Tal resultado nos assegura que para tratarmos da parte fracionária de q é suficiente considerarmos quocientes de dividendos ímpares.

Assim como fizemos no cálculo de $\lfloor q \rfloor$, trataremos o cálculo da parte não-inteira do ponto de vista matricial. Para isso, introduzimos a seguinte definição:

Definição 5.8. Seja $q = \dfrac{a}{2^n}$ um quociente irredutível e $N(q)$ o número de algarismos fracionários da forma decimal de q. Damos o nome de *Matriz complementar n-ésima* de a à matriz que denotaremos por

$$\lceil a \rceil_n = \left(\Delta_{ij}\right)_{n \times N(q)}$$

tal que $\Delta_{ij} = \beta^i(a_{-j})$

A seguir listamos as propriedades da matriz complementar tendo em vista facilitar o seu processo de construção:

Teorema 5.2 (Propriedades da matriz complementar)**.** *Seja $q = \dfrac{a}{2^n}$ irredutível com $n \in \mathbb{N}^*$. Se $\lceil a \rceil_n = \left(\Delta_{ij}\right)_{n \times N(q)}$, então são válidas as seguintes propriedades:*

(i) $N(q) = n$

(ii) $\Delta_{ii} = 5$ *para todo* $1 \leq i \leq n$;

(iii) $\Delta_{i(i-1)} = \Delta_{21}$ *para todo* $3 \leq i \leq n$

(iv) $\Delta_{i(i-2)} = \begin{cases} \Delta_{31} & \text{se } 2 \nmid i \quad e \quad 5 \leq i \leq n \\ \Delta_{42} & \text{se } 2 \mid i \quad e \quad 6 \leq i \leq n \end{cases}$

(v) $\Delta_{ij} = 0 \quad$ *se* $\quad i < j$ *para todo* $1 \leq i \leq n$

Demonstração. :

(i) Seja $a = a_r a_{r-1} \cdots a_1 a_0$ com a_0 ímpar. Vamos provar que $N(q_k) = k$ para todo $k \in \mathbb{N}^*$:

Para $k = 1$, temos

$q_1 = \dfrac{a}{2} = \dfrac{a,0}{2} = \beta(a_r)\beta(a_{r-1}) \cdots \beta(a_0), \beta(0) = \beta(a_r)\beta(a_{r-1}) \cdots \beta(a_0), 5$, e daí, $N(q_1) = 1$,

pois $\langle \overline{a_0}, 0\rangle = \langle 1, 0\rangle = 5$

Agora, se para algum $k \in \mathbb{N}^*$ temos $N(q_k) = k$, então

$$q_k = \frac{a}{2^k} = \left\lfloor \frac{a}{2^k} \right\rfloor, \beta^k(a_{-1})\beta^k(a_{-2})\cdots\beta^k(a_{-k+1})5 \tag{5.18}$$

e daí,

$$q_{k+1} = \frac{a}{2^{k+1}} = \left\lfloor \frac{a}{2^{k+1}} \right\rfloor, \beta(\beta^k(a_{-1}))\cdots\beta(\beta^k(a_{-k+1}))\beta(5)\left\langle \overline{5}, 0\right\rangle \tag{5.19}$$

Como $\left\langle \overline{5}, 0\right\rangle = 5 \neq 0$, temos disto e de (5.18) que

$$N(q_{k+1}) = N(q_k) + 1 = k + 1 \tag{5.20}$$

e daí, para todo $k \in \mathbb{N}^*$ vale $N(q_n) = n$.

(ii) Decorre da prova de (i). De fato, vimos que $N(q_k) = k$, e que, além disso,

$$\beta^k(a_{-k}) = 5 \text{ para todo } k \in \mathbb{N}^*$$

Mas $\beta^k(a_{-k}) = \Delta_{kk}$ por definição. Em particular, se $1 \leq i \leq n$, temos $\Delta_{ii} = 5$.

(iii) Suponhamos inicialmente que $2 \mid \beta(a_0)$.

Então

$$\Delta_{21} = \left\langle \overline{\beta(a_0)}, \Delta_{11} \right\rangle = \langle 0, 5\rangle = 2 \tag{5.21}$$

Daí, para $i = 3$, temos, de (ii) e de (5.21), que

$$\Delta_{32} = \left\langle \overline{\Delta_{21}}, \Delta_{22} \right\rangle = \left\langle \overline{2}, 5\right\rangle = \langle 0, 5\rangle = 2 \tag{5.22}$$

Supondo que para certo $k \in \mathbb{N}^*$ se tenha

$$\Delta_{k(k-1)} = \Delta_{21} = 2 \tag{5.23}$$

temos, de (ii) e de (5.23) que, para $k+1$ vale:

$$\Delta_{(k+1)k} = \left\langle \overline{\Delta_{k(k+1)}}, \Delta_{kk} \right\rangle = \left\langle \overline{2}, 5\right\rangle = 2.$$

Logo, se $2 \mid \beta(a_0)$, então $\Delta_{i(i-1)} = \Delta_{21}$ para todo $i \in \mathbb{N}^*$.

Se isto não ocorre, então teremos $\Delta_{21} = 7$ e o restante da prova e análoga.

(iv) Há 4 casos a serem considerados, conforme seja

$$\left\langle \overline{\beta^2(a_0)}, \Delta_{21} \right\rangle \in \{\langle 0,2\rangle, \langle 1,2\rangle, \langle 0,7\rangle, \langle 1,7\rangle\}$$

Provaremos o caso $\beta^2(a_0) = 0$ e $\Delta_{21} = 2$. Os demais casos se provam de forma exatamente idêntica.

Supondo isso, temos então

$$\Delta_{31} = \left\langle \overline{\beta^2(a_0)}, \Delta_{21} \right\rangle = \langle 0,2\rangle = 1$$

e

$$\Delta_{42} = \left\langle \overline{\Delta_{31}}, \Delta_{32} \right\rangle = \langle 1,2\rangle = 6 \tag{5.24}$$

Então, para $i = 5$, teremos

$$\Delta_{53} = \left\langle \overline{\Delta_{42}}, \Delta_{43} \right\rangle = \left\langle \overline{6}, 2 \right\rangle = 1$$

e, para $i = 6$, teremos

$$\Delta_{64} = \left\langle \overline{\Delta_{53}}, \Delta_{54} \right\rangle = \left\langle \overline{1}, 2 \right\rangle = 6$$

Suponha agora que a propriedade seja válida para certo $n \in \mathbb{N}^*$; isto é, que

$$\Delta_{k(k-2)} = \begin{cases} \Delta_{31} = 1 \quad se\ 2 \nmid k \\ \\ \Delta_{42} = 6 \quad se\ 2 \mid k \end{cases} \tag{5.25}$$

Então, de (iii) e de (5.25) teremos, para $k+1$, se k é par:

$$\Delta_{(k+1)(k-1)} = \left\langle \overline{\Delta_{k(k-2)}}, \Delta_{k(k-1)} \right\rangle = \langle 1,2\rangle = 6$$

ou, analogamente,

$$\Delta_{(k+1)(k-1)} = \left\langle \overline{6}, 2 \right\rangle = \left\langle \overline{0}, 2 \right\rangle = 1, \quad se \quad 2 \nmid k$$

Logo, (iv) é válida para todo $k \in \mathbb{N}^*$.

(v) Suponha por absurdo que exista $i \in \{1, \cdots, n\}$ e $j > i$ tal que $\Delta_{ij} \neq 0$.

Então, $N(q_i) \geq j > i$. Absurdo. □

De acordo com o teorema, a matriz complementar de a é uma matriz quadrada (propriedade 1) e triangular inferior (propriedade 5). Sua diagonal principal é formada por n dígitos iguais a 5 (propriedade 2), a diagonal imediatamente inferior à principal é formada por $n-1$ dígitos iguais a 2 ou a 7 (propriedade 3), e a diagonal inferior a esta última, por sua vez, é uma sequência cujos termos alternam-se entre os valores 1 e 6 ou 3 e 8 (propriedade 4).

Em consequência disto, temos que para cada $n \in \mathbb{N}^*$ existe apenas um número finito de matrizes complementares $\lceil a \rceil_n$. De fato, construindo as matrizes para alguns valores de n, temos:

$$\lceil a \rceil_1 = (5) \tag{5.26}$$

$$\lceil a \rceil_2 \in \left\{ \begin{pmatrix} 5 & 0 \\ 2 & 5 \end{pmatrix}, \begin{pmatrix} 5 & 0 \\ 7 & 5 \end{pmatrix} \right\} \tag{5.27}$$

$$\lceil a \rceil_3 \in \left\{ \begin{pmatrix} 5 & 0 & 0 \\ 2 & 5 & 0 \\ 1 & 2 & 5 \end{pmatrix}, \begin{pmatrix} 5 & 0 & 0 \\ 2 & 5 & 0 \\ 6 & 2 & 5 \end{pmatrix}, \begin{pmatrix} 5 & 0 & 0 \\ 7 & 5 & 0 \\ 3 & 7 & 5 \end{pmatrix}, \begin{pmatrix} 5 & 0 & 0 \\ 7 & 5 & 0 \\ 8 & 7 & 5 \end{pmatrix} \right\} \tag{5.28}$$

É fácil ver que cada matriz do tipo $\lceil a \rceil_n$ pode ser estendida à ordem $(n+1) \times (n+1)$ de duas maneiras diferentes, conforme seja $\overline{\beta^n(a_0)} = 1$ ou $\overline{\beta^n(a_0)} = 0$. Desse modo, para $n = 4$, devemos ter

$$\lceil a \rceil_4 \in \left\{ \begin{pmatrix} 5 & 0 & 0 & 0 \\ 2 & 5 & 0 & 0 \\ 1 & 2 & 5 & 0 \\ d_1 & 6 & 2 & 5 \end{pmatrix}, \begin{pmatrix} 5 & 0 & 0 & 0 \\ 2 & 5 & 0 & 0 \\ 6 & 2 & 5 & 0 \\ d_2 & 1 & 2 & 5 \end{pmatrix}, \begin{pmatrix} 5 & 0 & 0 & 0 \\ 7 & 5 & 0 & 0 \\ 3 & 7 & 5 & 0 \\ d_3 & 8 & 7 & 5 \end{pmatrix}, \begin{pmatrix} 5 & 0 & 0 & 0 \\ 7 & 5 & 0 & 0 \\ 8 & 7 & 5 & 0 \\ d_4 & 3 & 7 & 5 \end{pmatrix} \right\}$$

com $d_1 \in \{0,5\}$, $d_2 \in \{3,8\}$, $d_3 \in \{1,6\}$ e $d_4 \in \{4,9\}$ Desse modo, temos que

$$\#\{\lceil a \rceil_1\} = 1, \quad \#\{\lceil a \rceil_2\} = 2, \quad \#\{\lceil a \rceil_3\} = 4, \quad e \quad \#\{\lceil a \rceil_4\} = 8$$

Afirmamos que essa regularidade se mantém para $n > 4$, isto é, afirmamos que $\#\{\lceil a \rceil_n\} = 2^{n-1}$.

De fato, supondo que isto acontece para algum $n \in \mathbb{N}^*$, provemos que assim também o é para $n+1$:

Para tanto, seja $\lceil a \rceil_n = (\Delta_{ij})_{n \times n}$. Estendendo para $\lceil a \rceil_{n+1}$, devemos ter

$$\Delta_{(n+1)1} = \left\langle \overline{\beta^n(a_0)}, \Delta_{n1} \right\rangle = \begin{cases} \langle 0, \Delta_{n1} \rangle, & se \quad \overline{\beta^n(a_0)} = 0 \\ \\ \langle 1, \Delta_{n1} \rangle, & se \quad \overline{\beta^n(a_0)} = 1 \end{cases}.$$

Então,

$$\Delta_{(n+1)j} = \left\langle \overline{\Delta_{n(j+1)}}, \Delta_{nj} \right\rangle \text{ para todo } j \neq 1,$$

do que segue que apenas o termo $\Delta_{(n+1)1}$ admite duplicidade de valores, e daí,

$$\#\left\{\lceil a\rceil_{n+1}\right\} = 2\#\left\{\lceil a\rceil_n\right\} = 2(2^{n-1}) = 2^n, \tag{5.29}$$

e a afirmação é válida para $n+1$, e daí, por indução, também o é para todo $n \in \mathbb{N}^*$. Logo, a quantidade de matrizes complementares é finita para cada $n \in \mathbb{N}^*$, valendo o resultado obtido, que destacamos a seguir:

Proposição 5.7. *Se $n \in \mathbb{N}^*$ então $\#\left\{\lceil a\rceil_n\right\} = 2^{n-1}$*

Demonstração. Efetuada. □

Isto nos diz que apesar de existirem infinitos dividendos ímpares para o quociente $\frac{a}{2^n}$, as possibilidades para $\lceil a\rceil_n$, e, consequentemente, para $q - \lfloor q \rfloor$ são finitas.

Exemplo 5.9. *Construamos $\lceil 3\rceil_7$:*

$$\lceil 3\rceil_7 = \begin{bmatrix} 5 & 0 & 0 & 0 & 0 & 0 & 0 \\ 7 & 5 & 0 & 0 & 0 & 0 & 0 \\ 3 & 7 & 5 & 0 & 0 & 0 & 0 \\ 1 & 8 & 7 & 5 & 0 & 0 & 0 \\ 0 & 9 & 3 & 7 & 5 & 0 & 0 \\ 0 & 4 & 6 & 8 & 7 & 5 & 0 \\ 0 & 2 & 3 & 4 & 3 & 7 & 5 \end{bmatrix}$$

O que obtemos construindo uma tabela quadrada 7×7 e em seguida preenchendo sua diagonal principal com o dígito 5 e, sem se preocupar com os termos acima desta, que são todos nulos, calculamos $\Delta_{21} = \left\langle \overline{\beta(3)}, 5 \right\rangle = 7$ que será o valor a ser preenchido em toda a primeira diagonal abaixo da principal.

Em seguida, calculamos $\Delta_{31} = \left\langle \overline{\beta^2(3)}, 7 \right\rangle = \langle 0, 6\rangle = 3$, e daí alternamos o restante dessa diagonal com os valores 3 e 8.

Finalmente, calculamos os termos restantes. Em particular, a última linha nos dá a parte fracionária de $\frac{3}{2^7}$, e do fato de que $\beta^n(3) = 0$ para $n \geq 2$, temos $\frac{3}{2^7} = 0,0234375$ □

5.6 Construção da Matriz do Dividendo Inteiro

Reunimos tudo o que vimos até aqui no resultado a seguir, que estabelece a construção da matriz de um dividendo inteiro em termos da matriz inteira, matriz complementar e iterações de redução de q:

Teorema 5.3. *Seja* $q = \dfrac{a}{2^n}$ *com* $a = a_r a_{r-1} \cdots a_1 a_0 \in \mathbb{Z}$, $n \in \mathbb{N}^*$.

Se $R < n$ *é o número de iterações de redução de* q *à forma irredutível, então a matriz associada ao dividendo* a *é a matriz de ordem* $n \times (n - R + r + 1)$ *tal que*

$$[a]_n = \left(\begin{array}{c|c} \lfloor a \rfloor_R & O \\ \hline \lfloor q_R \rfloor_{n-R} & \lceil q_R \rceil_{n-R} \end{array}\right)$$

onde

$\lfloor a \rfloor_R$ *é do tipo* $R \times (r+1)$;
$\lfloor q_R \rfloor_{n-R}$ *é do tipo* $(n-R) \times (r+1)$;
$\lceil q_R \rceil_{n-R}$ *é quadrada de ordem* $n - R$; *e*
O *é a matriz nula* $R \times (n-R)$

Demonstração. :

Pela Definição 5.5, as primeiras $r+1$ colunas de $[a]_n$ coincidem com a matriz $\lfloor a \rfloor_n$. Em particular, se R é o número de iterações de redução de q, então $\tilde{q} = \dfrac{q_R}{2^{n-R}}$ é a forma irredutível de q e daí podemos escrever

$$\lfloor a \rfloor_n = \left(\begin{array}{c} \lfloor a \rfloor_R \\ \hline \lfloor q_R \rfloor_{n-R} \end{array}\right) \tag{5.30}$$

Mas $q_k = \dfrac{a}{2^k}$ é inteiro par para todo $1 \leq k < R$ e q_R é inteiro ímpar $(*)$

Segue disso que as últimas $n - R$ linhas a partir da coluna $r+2$ de $[a]_n$ coincidem com a matriz $\lceil q_R \rceil_{n-R}$ que possui $n - R$ colunas (Teorema 5.2 (1)) $(**)$

Finalmente, de $(*)$ temos que $q_k \in \mathbb{Z}$ para todo $1 \leq k \leq R$, donde $q_k - \lfloor q_k \rfloor = 0$, e de (5.30) e de $(**)$ segue que

$$\begin{pmatrix} \alpha_{1(r+2)} & \cdots & \alpha_{1(n-R+r+1)} \\ \vdots & & \vdots \\ \alpha_{R(r+2)} & \cdots & \alpha_{R(n-R+r+1)} \end{pmatrix} = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{pmatrix}_{R\times(n-R)} \tag{5.31}$$

e então,

$$[a]_n = \left(\begin{array}{c|c} \lfloor a \rfloor_R & O \\ \hline \lfloor q_R \rfloor_{n-R} & \lceil q_R \rceil_{n-R} \end{array}\right).$$

□

A demonstração do teorema, que é construtiva, nos ensina que devemos construir, inicialmente, uma tabela $n \times (r+1)$, referente a $\lfloor a \rfloor_n$. Uma vez identificado o R tal que $2 \nmid \beta^R(a_0)$, podemos construir, a partir da próxima linha, uma tabela $(n-R) \times (n-R)$ para ser preenchida conforme $\lceil q_R \rceil_{n-R}$, e com isso fica determinado o bloco O, e, por conseguinte, $[a]_n$.

Evidentemente, nesse processo, podemos lançar mão das propriedades estudadas anteriormente. Nesse contexto, é importante mencionar que os itens (i) e (ii) da proposição 5.5 podem ser estendidos à matriz $[a]_n$, o que pode ser provado de maneira idêntica ao que fizemos para $\lfloor a \rfloor_n$. No mais, todas as demais propriedades vistas até aqui permanecem válidas para a matriz do dividendo inteiro.

Exemplo 5.10. *Construiremos* $[416]_8$. *A título de ilustração,o faremos exibindo os detalhes de cada passo:*

1. *Inicialmente construímos* $\lfloor 416 \rfloor_8$:

$$\lfloor 416 \rfloor_8 = \left[\begin{array}{ccc} 2 & 0 & 8 \\ 1 & 0 & 4 \\ 0 & 5 & 2 \\ 0 & 2 & 6 \\ 0 & 1 & 3 \\ \hline 0 & 0 & 6 \\ 0 & 0 & 3 \\ 0 & 0 & 1 \end{array}\right]$$

2. *Identificada a primeira linha ímpar, no caso, a* $q_5 = 13$, *passamos a construir sua matriz complementar:*

$$\lceil 13 \rceil_{8-5} \lceil 13 \rceil_3 = \begin{bmatrix} 5 & 0 & 0 \\ 2 & 5 & 0 \\ 6 & 2 & 5 \end{bmatrix}$$

Finalmente, formamos $[328]_8$ *justapondo os dois blocos matriciais a partir da última linha e completando com zeros os espaços vazios:*

$$[328]_8 = \left[\begin{array}{ccc|ccc} 2 & 0 & 8 & 0 & 0 & 0 \\ 1 & 0 & 4 & 0 & 0 & 0 \\ 0 & 5 & 2 & 0 & 0 & 0 \\ 0 & 2 & 6 & 0 & 0 & 0 \\ 0 & 1 & 3 & 0 & 0 & 0 \\ \hline 0 & 0 & 6 & 5 & 0 & 0 \\ 0 & 0 & 3 & 2 & 5 & 0 \\ 0 & 0 & 1 & 2 & 5 & 0 \end{array}\right]$$

□

Naturalmente, se nosso interesse for tão somente o cálculo de q, como se espera, os detalhes de notação podem ser dispensados para agilizar o processo. É o que faremos a seguir:

Exemplo 5.11. *Vamos calcular* $\dfrac{600}{2^{10}}$*:*

Seguindo os passos acima com as devidas abreviações[4]*, e usando uma grade para facilitar a localização dos termos, teremos:*

[4] Apesar de não fazer parte da matriz, alocaremos o dividendo numa linha superior na tabela para tornar visualmente mais cômodo o processo

6	0	0							
3	0	0							
1	5	0							
.	7	5							
.	3	7	5						
.	1	8	7	5					
.	.	9	3	7	5				
.	.	4	6	8	7	5			
.	.	2	3	4	3	7	5		
.	.	1	1	7	1	8	7	5	
0	0	0	5	8	5	9	3	7	5

Tomando então a última linha, temos $\frac{600}{2^{10}} = 0,5859375$ □

5.7 Dividendos Reais Quaisquer

5.7.1 Forma Produto de um Quociente

Seja $a \in \mathbb{R}$ uma dízima exata e $q = \frac{a}{2^n}$ com $n \in \mathbb{N}^*$. Pela proposição 4.1, existem $m \in \mathbb{N}$ e $\hat{a} \in \mathbb{Z}$ tais que $a = \frac{\hat{a}}{10^m}$. Se, além disso, m é o menor inteiro tal que $\hat{a} \in \mathbb{Z}$, então

$$m = N(a) = \text{número de algarismos fracionários de } a$$

Nestas condições, podemos escrever $q = \frac{\hat{a}}{2^n} \cdot 10^{-m}$, ou ainda $q = \hat{q} \cdot 10^{-m}$, pondo $q = \frac{\hat{a}}{2^n}$ $(*)$
Segue então da proposição 5.1 que a linha $q_n(\hat{a})$ da matriz $[\hat{a}]_n$ é tal que $\hat{q} = q_n(\hat{a})$, e daí, supondo $\hat{q} = \sum_{i=-s}^{r} b_i 10^i$ temos, de $(*)$ que

$$q = q_n(\hat{a})10^{-m} = \sum_{i=-s}^{r} b_i 10^{i-m} = \sum_{i=-(s+m)}^{r-m} b_i 10^i.$$

Por outro lado, se tomarmos $a \in \mathbb{Z}$ e considerarmos que toda expressão decimal inteira é também uma dízima finita (Corolário 4.1), podemos ainda escrever $a = \frac{\hat{a}}{10^m}$, bastando para isto que consideremos $m \leq 0$. Isto pode ser útil nos casos em que a é múltiplo de 10, conforme ilustraremos a seguir. Antes, porém, formalizaremos o que discutimos:

Definição 5.9 (Forma produto)**.** Seja a uma dízima finita e $n \in \mathbb{N}^*$ tais que $q = \frac{a}{2^n}$. Damos o nome de forma produto de q à expressão que $q = \hat{q} \cdot 10^m$, em que $\hat{q} = \frac{\hat{a}}{2^n}$ e m é o menor número inteiro tal que $\hat{a} \in \mathbb{Z}$.

De acordo com a Definição, temos, por exemplo, $\frac{8}{2^5} \cdot 10^{-2}$, $\frac{3}{2^9} \cdot 10^2$ e $\frac{5}{2^{12}} \cdot 10^0$ são as formas produto dos quocientes $\frac{0,08}{2^5}$, $\frac{300}{2^9}$ e $\frac{5}{2^{12}}$, respectivamente. Note, ainda, que a forma como definimos m nos dá informações sobre o dividendo escrito na forma usual:

- $m < 0$ indica que o dividendo a possui $|m|$ dígitos não inteiros;
- $m > 0$ indica que o dividendo original possui $|m|$ zeros na extrema direita de sua parte inteira;
- $m = 0$ indica que o dividendo original já é inteiro e não múltiplo de 10.

É fácil ver que $\hat{q}$ se transforma em q após a operação de aumentar em $|m|$ unidades o número de seus algarismos fracionários, ou de diminuir em $|m|$ esse número, conforme seja m, respectivamente, negativo ou positivo[5].

Exemplo 5.12. *Para* $q = \frac{0,008}{2^9}$, *temos* $q = \frac{8}{2^9} \cdot 10^{-3}$. *Construindo* $[8]_9$*:*

8						
4						
2						
1						
.	5					
.	2	5				
.	1	7	5			
.	.	6	7	5		
.	.	3	1	2	5	
0	0	1	5	6	2	5

Logo, $q = \hat{q} \cdot 10^{-3} = 0,000015625$ □

[5]Trata-se da regra do "deslocamento da vírgula"no produto ou divisão por potências de 10.

Exemplo 5.13. *Para* $q = \dfrac{6000}{2^9}$, *temos* $q = \dfrac{6}{2^9} \cdot 10^3 = \dfrac{3}{2^8} \cdot 10^3$. *e daí, a matriz* $[3]_8$ *é:*

3									
1	5								
.	7	5							
.	3	7	5						
.	1	8	7	5					
.	.	9	3	7	5				
.	.	4	6	8	7	5			
.	.	2	3	4	3	7	5		
.	.	1	1	7	1	8	7	5	
0	0	0	5	8	5	9	3	7	5

Então, $q = 0,005859375 \cdot 10^3 = 5,859375$ □

5.7.2 Matriz Inteira Associada a Dízimas Infinitas

Seja $a \in \mathbb{R}$ uma dízima infinita, e $q = \dfrac{a}{2^n}$ com $n \in \mathbb{N}^*$. Supondo $a = \lfloor a \rfloor, a_{-1}a_{-2}a_{-3}\cdots a_{-s}\cdots$, temos, pela Proposição 4.3 que sua s-aproximação ótima é dada por

$$A_s(a) = \lfloor a \rfloor, a_{-1}a_{-2}a_{-3}\cdots a_{-s}$$

Por outro lado, k aplicações sucessivas do Teorema 4.5 nos garantem que o $k-$iterado

$$q'_k = \left\lfloor \frac{a}{2^k} \right\rfloor, \beta^k(a_{-1})\beta^k(a_{-2})\cdots\beta^k(a_{-s})$$

é a $s-$aproximação ótima de q_k. Em particular,

$$A_s(q) = A_s(q_n) = \left\lfloor \frac{a}{2^n} \right\rfloor, \beta^n(a_{-1})\beta^n(a_{-2})\cdots\beta^n(a_{-s})$$

é a s-aproximação ótima de q. Então, pelo Teorema 5.2 devemos ter:

$$q = \left\lfloor \frac{a}{2^n} \right\rfloor, \beta^n(a_{-1})\beta^n(a_{-2})\cdots\beta^n(a_{-s})\beta^n(a_{-s-1})\cdots = A_s(q_n) + \sum_{j=1}^{\infty} \beta^n(a_{-s-j})10^{-s-j}$$

Dito de outra forma, para determinarmos q com s algarismos exatos visíveis antes das reticências, é suficiente iterarmos a s-aproximação ótima $A_s(a)$ de a obtendo a sequência de aproximações ótimas com s algarismos fracionários $A_s(q_1), A_s(q_2), \cdots, A_s(q_n)$.

Note agora que $A_s(a)$ é uma dízima exata, e daí, existe $\gamma \in \mathbb{Z}$ tal que

$$A_s(a) = \frac{\gamma}{10^s}$$

Agora, como queremos que a iteração $(A_s(q_i))_{1\leq i\leq n}$ só tenha algarismos exatos, estamos interessados apenas na parte inteira de cada $A_s(q_k)$. Segue que $A_s(q_n) = \left\lfloor \frac{\gamma}{2^n} \right\rfloor \cdot 10^{-s}$, e daí, $A_s(q)$ será a dízima cujos algarismos fracionários são dados pela sequência dos s últimos termos da última linha da matriz $\lfloor \hat{a} \rfloor_n$, e os algarismos inteiros pela sequência dos termos restantes.

Exemplo 5.14. *Vamos calcular $q = \frac{a}{2^6}$ com 5 algarismos fracionários expostos, sendo $a = 1,11111\cdots$.*

Para isso, tomemos a 5-aproximação ótima de a, $A_5(a) = 1,11111$. Usando-a, temos que a 5-aproximação ótima de q é dada por $A_5(q)$ tal que

$$A_5(q) = \left\lfloor \frac{111111}{2^6} \right\rfloor 10^{-5}$$

Construindo $\lfloor 111111 \rfloor_6$, temos:

$$\lfloor 111111 \rfloor_6 = \begin{bmatrix} 0 & 5 & 5 & 5 & 5 & 5 \\ 0 & 2 & 7 & 7 & 7 & 7 \\ 0 & 1 & 3 & 8 & 8 & 8 \\ 0 & 0 & 6 & 9 & 4 & 4 \\ 0 & 0 & 3 & 4 & 7 & 2 \\ 0 & 0 & 1 & 7 & 3 & 6 \end{bmatrix}$$

Então, $A_5(q) = 0,01736$, e daí, $q = 0,01736\cdots$. □

6 APLICAÇÕES

Encerramos nossa exposição apresentando algumas aplicações elementares de nosso trabalho. Para tanto, nos serviremos de tudo quanto tratamos nas páginas anteriores bem como de algumas interpretações adicionais eventualmente necessárias que serão apresentadas a seu tempo.

6.1 Sobre o Uso do Presente Trabalho na Escola Básica

Sendo este um trabalho que se propõe a oferecer um meio alternativo de se determinar quocientes de divisores do tipo 2^n, pouco além das aplicações da própria divisão por dois usual podemos ir. Ao nosso ver, no entanto, isto é o suficiente; de fato, a divisão por 2 assume, em nossos tempos fortemente marcados pela tecnologia, uma importância ímpar: como já dissemos, provém dos restos possíveis da divisão por 2 o sistema binário e, deste, a linguagem utilizada pelos computadores e dispositivos eletrônicos em geral. Nessas condições, decodificar a linguagem do computador em linguagem comum e vice-versa ou, equivalentemente, converter expressões binárias em expressões decimais e estas naquelas constitui relevante matéria de estudo que pode ser tratada já na escola básica. De fato, a menos de um tratamento adequado à maturidade (cronológica e cognitiva) dos alunos aos quais se propuser a atividade, o estudo que aqui temos desenvolvido pode ser trabalhado em qualquer curso de matemática em nível básico e mesmo em cursos superiores de Teoria dos Números, a título de ilustração das propriedades aritméticas das representações binária e decimal, por exemplo. Por outro lado, a abordagem que optamos dar no decorrer do texto, utilizando a linguagem algébrica das matrizes, sequências, somas e séries, bem como os rudimentos dos conceitos de limite e convergência, se usados na atividade voltada a uma clientela mais experiente, pode fornecer uma boa oportunidade de ilustrar as aplicações e integração de tais conceitos, assim como fomentar o hábito da observação e sistematização de regularidades, o que constitui uma das competências elencadas pelos Parâmetros Curriculares Nacionais de matemática em nível médio: segundo esse documento, é competência a ser desenvolvida pelo aluno durante a educação básica

> "(...) estabelecer relações, identificar regularidades, invariantes e transformações (...) em situações semelhantes para estabelecer regras, algoritmos e propriedades" (BRA-

SIL: [7], p.113).

Nesse contexto, sugerimos que as atividades que visem a aplicação do estudo que desenvolvemos se pautem inicialmente na experimentação, seguida da formalização, e finalmente nas aplicações complementares. Este capítulo objetiva fornecer alguns subsídios adicionais que servem ao propósito de ilustrar situações outras da divisão por 2 nas quais a aplicação do método que aqui desenvolvemos pode fornecer maior dinâmica ao processo.

6.2 Representação Binária de um Inteiro Dado na Base Decimal

Segundo Bianchini e Paccola [3] , o sistema posicional de numeração de base 2 foi imaginado inicialmente por Leibnitz, matemático alemão que lançou os alicerces desse sistema ao proceder a busca por "uma base que fosse a mais simples possível, que usasse menos algarismos, e na qual os cálculos fossem mais fáceis de serem efetuados"(idem, p.50).

Evidentemente, a pretensão inicial de substituir o sistema decimal pelo binário não seguiu adiante, por razões cuja discussão não nos compete; entretanto, a numeração de base dois assume capital importância nos dias atuais, já que a maioria dos equipamentos de computação trabalha com valores numéricos em representação binária, conforme destaca Arenales e Darezzo ([1], p.2). Desse modo, o computador "[converte] para o sistema binário, automaticamente, o que lhe fornecemos no sistema decimal" (Giovanni e Parente: [12], p.29).

Esse processo de mudança de base, que internamente é feito pelo computador é baseado no Teorema 2.1 e consiste em

> fazer sucessivas divisões [euclidianas] por 2. As divisões serão feitas com o número [base 10] e com cada um dos quocientes encontrados (...). Os restos das divisões, escritos na ordem inversa em que aparecem (...) nos dão a representação do número [dado] na base dois (Bianchini e Paccola: [3], p.57).

A seguir, queremos abordar o processo de representação na base 2 de um inteiro como aplicação do que discutimos no capítulo precedente. Nesse contexto, é a matriz inteira de um dividendo a ferramenta adequada para atacarmos tal problema, conforme mostraremos a seguir:

Proposição 6.1 (Representação binária)**.** *Sejam $a = a_n a_{n-1} \cdots a_1 a_0$ um inteiro escrito na base 10, e*

$$\lfloor a \rfloor_k = \left(\beta^i(a_j)\right)_{k\times(n+1)}$$

a matriz inteira de a tal que sua $k-$ésima linha é dada por $q_k = \begin{pmatrix} 0 & 0 & \cdots & 1 \end{pmatrix}$. *Se* $a = (r_k r_{k-1} \cdots r_1 r_0)_2$ *é a representação binária de* a, *então*

$$r_k = \begin{cases} \overline{a_0} & , \text{se } k = 0 \\ \\ \overline{\beta^k(a_0)} & , \text{se } k > 0 \end{cases}$$

Demonstração. A existência e finitude da sequência de dígitos binários $r_0, r_1, \cdots r_k$, bem como o fato de que $a = (r_k r_{k-1} \cdots r_1 r_0)_2$ são fatos garantidos pelo Teorema 2.1.

Além disso, pelo Algoritmo de Euclides, existem inteiros $q_1, \cdots, q_{k+1}$ univocamente determinados tais que

$$a = 2q_1 + r_0$$

e

$$q_k = 2q_{k+1} + r_k, \quad se \quad k \geq 1.$$

Nessas condições, temos então:

$$\overline{a} = \overline{2q_1 + r_0} = \overline{0 + r_0} = r_0 \tag{6.1}$$

e

$$\overline{q_k} = \overline{2q_{k+1} + r_k} = \overline{0 + r_k} = r_k \tag{6.2}$$

Mas sendo $a = a_n a_{n-1} \cdots a_1 a_0$ a Proposição 2.2 e (6.1) nos garante que $\overline{a} = \overline{a_0} \Rightarrow r_0 = \overline{a_0}$.

e pelo Corolário 5.2 e por (6.2), temos

$$q_k = \beta^k(a_n)\beta^k(a_{n-1}) \cdots \beta^k(a_0) \text{ , e daí, } \overline{q_k} = \overline{\beta^k(a_0)} \Rightarrow r_k = \overline{\beta^k(a_0)}$$

□

Exemplo 6.1. *Usaremos a Proposição 6.1 para expressar os inteiros* $a = 150$ *e* $b = 64$ *na base binária. Para tanto, iremos construir a Matriz inteira de cada dividendo com tantas linhas quantas forem necessárias para que suas últimas linhas sejam* $(0 \ 0 \ 1)$ *e* $(0 \ 1)$, *respectivamente.*

Nestas condições, para $a = 150$, *temos* $\left\lfloor \frac{a}{2^7} \right\rfloor = 1$ *(pois* $2^7 < 150 < 2^8$*), e daí, temos:*

$$\lfloor 150 \rfloor_7 = \begin{bmatrix} . & 7 & 5 \\ . & 3 & 7 \\ . & 1 & 8 \\ . & . & 9 \\ . & . & 4 \\ . & . & 2 \\ 0 & 0 & 1 \end{bmatrix}$$

e pondo $150 = (r_7 r_6, \cdots r_0)_2$, *a proposição nos dá* $r_0 = \overline{0} = 0$, *e*

$$150 = (\overline{1}\ \overline{2}\ \overline{4}\ \overline{9}\ \overline{8}\ \overline{7}\ \overline{5}\ 0)_2 = (10010110)_2$$

Analogamente, para $b = 64$, *temos* $\left\lfloor \frac{64}{2^6} \right\rfloor = 1$, *e daí,*

$$\lfloor 64 \rfloor_6 = \begin{bmatrix} 3 & 2 \\ 1 & 6 \\ . & 8 \\ . & 4 \\ . & 2 \\ . & 1 \end{bmatrix}$$

donde $64 = (r_6 r_5 r_4 r_3 r_2 r_1 r_0)_2 = (\overline{1}\ \overline{2}\ \overline{4}\ \overline{8}\ \overline{6}\ \overline{2}\ \overline{4})_2 = (1000000)_2$ □

Uma interessante aplicação do resultado anterior, apontada por Hefez ([14], p. 49), mostra que todo número inteiro se escreve de maneira única como soma de potências de base 2. De fato, o Teorema 2.1 nos garante que se $a = (r_n r_{n-1} \cdots r_1 r_0)_2 \in \mathbb{Z}$ e $r_i \in \{0,1\}$ para todo $i \in \{0, \cdots, n\}$, então $a = \sum_{i=0}^{n} r_i 2^i$, e daí, desprezando as parcelas tais que $r_k = 0$, temos então

$$a = \sum_{i \in A} 2^i, \quad \text{com} \quad A = \{k : r_k \neq 0\}. \tag{6.3}$$

O que prova, pois, o resultado a seguir:

Proposição 6.2. *: A todo número inteiro corresponde uma, e apenas uma, soma de potências de base 2.*

Exemplo 6.2. *Escreveremos 1387 como soma de potências de base 2. Para isso, construiremos* $\lfloor 1387 \rfloor_k$ *com* $k = 10$, *já que* $\left\lfloor \frac{1387}{2^{10}} \right\rfloor = 1$*:*

$$\lfloor 1387 \rfloor_{10} = \begin{bmatrix} . & 6 & 9 & 3 \\ . & 3 & 4 & 6 \\ . & 1 & 7 & 3 \\ . & . & 8 & 6 \\ . & . & 4 & 3 \\ . & . & 2 & 1 \\ . & . & 1 & 0 \\ . & . & . & 5 \\ . & . & . & 2 \\ . & . & . & 1 \end{bmatrix}$$

Temos então, $1387 = (10101101011)_2 = 2^{10} + 2^8 + 2^6 + 2^5 + 2^3 + 2^1 + 2^0$ □

6.3 Representação Decimal de Expressões Binárias Finitas

Uma vez tendo sido abordada a conversão base decimal-base binária de números inteiros, é natural que o estudante desse tema indague quanto à representação de um número real qualquer na base 2, tendo em vista as importantes aplicações de tal base na tecnologia atual.

Para além do ponto de vista técnico, não é difícil constatar-se que a representação binária de um número real não goza da mesma notoriedade que a forma binária de um inteiro nas salas de aula da educação básica, talvez pela falta de familiaridade dos professores com o tema, sua ausência nos conteúdos programáticos oficiais, ou mesmo por preferência do ensino de outros temas mais tradicionais do currículo.

Aqui pretendemos amenizar as dificuldades de ordem técnica relacionadas a esse tema; para isso, utilizaremos os conceitos tratados nos capítulos precedentes focando no caso específico das representações binárias finitas, uma vez que para as infinitas pouco podemos fazer além do que já é feito tradicionalmente. Para tanto, o primeiro passo que daremos consiste em definir o nosso objeto de estudo:

Definição 6.1 (Expressão Binária Finita)**.** Seja o número real definido pela série

$$a = \lfloor a \rfloor + \sum_{i=1}^{-\infty} a_i 2^i, \quad a_i \in \{0,1\} \text{ para todo } i \in \mathbb{Z}$$

Diremos que a possui uma *Representação Binária Finita* quando existe um $k \in \mathbb{Z}$ tal que $a_i = 0$ para todo $i < k$. Nesse caso escrevemos

$$a = (\lfloor a \rfloor, a_{-1}a_{-2}\cdots a_k)_2 \tag{6.4}$$

e diremos que (6.4) é a *Expressão Binária Finita* de a.

De maneira análoga ao que fizemos anteriormente no estudo da expansão decimal, estabeleceremos, na proposição a seguir, uma condição necessária e suficiente para a finitude de uma expansão binária:

Proposição 6.3. *Um número real q admite representação binária em expansão finita se, e somente se, existem $a \in \mathbb{Z}$ e $n \in \mathbb{N}^*$ tais que*

$$q = \frac{a}{2^n}$$

Demonstração. A menos da base, é idêntica à demonstração da Proposição 4.1, e não oferece nenhuma dificuldade adicional, de modo que optaremos por omití-la. □

Decorre dessa proposição que todas e apenas as expressões decimais que possuem representação binária finita são quocientes de divisor 2^n, e daí, suas partes não inteiras são linhas da matriz complementar $\lceil a \rceil_n$ de algum dividendo inteiro a. No exemplo a seguir, ilustraremos o método para reconhecimento das dízimas decimais que dão origem a expressões binárias finitas:

Exemplo 6.3. *Possuem expressão binária finita:*

$a = 2,125$, *pois* $(\ 1 \quad 2 \quad 5\ ) = q_5$ *em* $\lceil 1 \rceil_n$; *e*

$b = 50,1875$, *pois* $(\ 1 \quad 8 \quad 7 \quad 5\ ) = q_4$ *em* $\lceil 3 \rceil_n$,

e não possuem representação finita na base 2:

$c = 5,885$, $d = 0,0075$, e $e = 0,10875$;

os dois primeiros casos por razões facilmente identificáveis, já que a terminação decimal de quocientes de divisor 2^n só pode ser do tipo 125, 625, 875 ou 375, se considerarmos apenas os 3 últimos dígitos (ver proposição 5.2 (4)). O reconhecimento da finitude do terceiro na base 2, por outro lado, pode requerer um esforço adicional, se não soubermos se existe alguma matriz $\lceil a \rceil_n$ tal que $q_5(a) = (\ 1\ \ 0\ \ 8\ \ 7\ \ 5\ )$. Para dirimir essa dúvida, basta que suponhamos que existe um $a \in \mathbb{Z}$ tal que isso aconteça, e, usando as propriedades da construção da matriz complementar chegaremos à confirmação do que supomos ou a uma contradição:

$$\lceil a \rceil_5 = \begin{bmatrix} 5 & & & & \\ 7 & 5 & & & \\ 8 & 7 & 5 & & \\ \Delta_{41} & 3 & 7 & 5 & \\ 1 & 0 & 8 & 7 & 5 \end{bmatrix}$$

Perceba que conhecemos todos os termos da matriz, com exceção de Δ_{41}. Entretanto, sabemos que $\Delta_{41} = \left\langle \overline{\beta^3(a_0)}, 8 \right\rangle \in \{4,9\}$. Porém, verificando os possíveis valores, temos:

Se $\Delta_{41} = 4$, então $1 = \left\langle \overline{\beta^4(a_0)}, 4 \right\rangle \in \{2,7\}$ (absurdo); e

Se $\Delta_{41} = 9$, então $1 = \left\langle \overline{\beta^4(a_0)}, 9 \right\rangle \in \{4,9\}$ (absurdo).

Logo, não existe $a \in \mathbb{Z}$ tal que $\lceil a \rceil_n$ possua a quinta linha igual a $(\ 1\ \ 0\ \ 8\ \ 7\ \ 5\ )$, e daí o número dado não possui representação binária finita. □

Finalizando este tópico, trataremos agora da conversão à base dez de uma expressão binária $q \in \mathbb{R}$ finita. É claro que é suficiente tratarmos do caso $0 < q < 1$. De fato, para $q \geq 1$ temos

$$q = (\lfloor q \rfloor, a_{-1} \cdots a_{-n})_2 = (\lfloor q \rfloor)_2 + (0, a_{-1}a_{-2}a_{-3} \cdots a_{-n})_2$$

daí, podemos converter em separado as partes inteira e não-inteira de q, desde que as somemos ao fim. Como a conversão da parte inteira é uma soma trivial de potências de base 2, nos deteremos na conversão da parte fracionária.

A seguir apresentamos o algoritmo que nos fornecerá isto:

Proposição 6.4. *Seja $q = (0, a_{-1}a_{-2}a_{-3} \cdots a_{-n})_2 \in \mathbb{R}$ com $a_{-n} = 1$ uma expressão binária finita.*

Se $J = \{n_1 < n_2 < \cdots < n_k = n\}$ é o conjunto dos índices $i \in \{0, \cdots, n\}$ tais que $a_{-i} \neq 0$, então a representação decimal de q é dada pela expressão decimal do quociente

$$a = \frac{\sum_{j=1}^{k} 2^{n-n_j}}{2^n}$$

Demonstração. Por hipótese, temos:

$$q = (0, a_{-1}a_{-2}a_{-3}\cdots a_{-n})_2 = \sum_{i=1}^{n} \frac{a_i}{2^i} = \sum_{i \in I} \frac{1}{2^i} = \frac{1}{2^{n_1}} + \frac{1}{2^{n_2}} + \cdots \frac{1}{2^n}$$

Como $n = max\ I$, seque que $n - n_i \geq 0$ para todo $i \in \{1, \cdots, k\}$, e daí, usando (6.5), podemos escrever:

$$q = \frac{2^{n-n_1}}{2^n} + \frac{2^{n-n_2}}{2^n} + \cdots + \frac{2^{n-n}}{2^n} = \frac{\sum_{j=1}^{k} 2^{n-n_j}}{2^n}$$

□

Exemplo 6.4. *Escrevamos $q = (11,0110101)_2$ na base decimal.*

Temos

$$(\lfloor q \rfloor)_2 = (11)_2 = 2 + 1 = 3$$

Por outro lado,

$$q - \lfloor q \rfloor = (0,0110101)_2$$

cujas ordens não nulas possuem índices -2, -3, -5, e -7. Logo, pela proposição, a forma decimal de q será dada pelo quociente

$$q = \frac{2^5 + 2^4 + 2^2 + 1}{2^7} = \frac{32 + 16 + 4 + 1}{2^7} = \frac{53}{2^7}$$

construindo $[53]_7$*, temos, então:*

5	3							
2	6	5						
1	3	2	5					
.	6	6	2	5				
.	3	3	1	2	5			
.	1	6	5	6	2	5		
.	.	8	2	8	1	2	51	
0	0	4	1	4	0	6	2	5

Portanto, $(11,0110101)_2 = 3,4140625$ □

Exemplo 6.5 (Potências de 2 com expoente negativo)**.** *Potências do tipo* $2^n, n \in \mathbb{Z}^-$ *podem ser vistas como casos particulares de expressões binárias finitas em que* $\#J = 1$*. De fato, temos:*

$$2^{-1} = (0,1)_2,\ 2^{-2} = (0,01)_2, \cdots, 2^{-n} = (0, \underbrace{0\cdots01}_{n-dígitos})_2$$

Nestas condições, calcular 2^{-5}*, por exemplo, é o mesmo que determinar a expressão decimal do número* $(0,00001)_2$*, o que equivale, por sua vez, a calcular o quociente* $q = \frac{1}{2^5}$*, o que conseguimos determinando a 5.ª linha de* $[1]_5$*, a saber,* $0,03125$ □

6.4 Representação Binária de Quocientes do tipo $q = \frac{a}{2^n},\ a \in \mathbb{Z}, n \in \mathbb{N}^*$

Segundo [1], o procedimento usual que se adota para mudança da base 10 para a base binária de um número real $0 < |q| < 1$ é chamado de método das "multiplicações sucessivas"e consiste, como o nome sugere, em multiplicar q seguidas vezes por 2 e, em cada passo, separar o dígito da ordem 0, formando uma sequência de algarismos que representará o número dado na base binária:

> "O procedimento [para a conversão base 10- base 2] é constituído dos seguintes passos:
>
> (a) Multiplicamos o número fracionário por 2;
> (b) Do resultado do passo (a), a parte inteira é o primeiro dígito binário;
> (c) Do resultado do passo (b), a parte fracionária é novamente multiplicada por 2;
> (d) O processo continua até que a parte fracionária seja nula" (Arenales e Darezzo: [1], p. 4).

Não é difícil se concluir que se trata de um procedimento simples, mas relativamente trabalhoso. Além disso, a mecânica do processo não é intuitiva: o ato de dobrar o número e tomar sua parte inteira seguidamente não deixa claro o que de fato ocorre.

Não obstante, vemos também aqui uma boa possibilidade de aplicação das técnicas que temos apresentado. Novamente restringiremos nossa exposição ao caso em que q pode ser representado com expansão finita na base 2. Nesse caso, conforme a Proposição 6.3, q admite a representação na forma do quociente

$$q = \frac{a}{2^n} \tag{6.5}$$

para algum $a \in \mathbb{Z}$ e $n \in \mathbb{N}^*$.

Nosso trabalho, então, se resume a determinar o dividendo a e o expoente n do divisor em (6.5). De fato, pelo Teorema 2.1 e por 6.3, existem números naturais $n_1, n_2, \cdots, n_k$ tais que

$$a = \sum_{i=1}^{k} 2^{n_i}$$

Sem perda de generalidade, podemos supor q irredutível, e daí, teremos a ímpar e para algum índice i deve ocorrer $n_i = 0$. Seja $i = k$ esse índice. Então podemos escrever

$$a = 2^{n_1} + 2^{n_2} + 2^{n_3} + \cdots + 2^{n_{k-1}} + 1 \tag{6.6}$$

e substituindo (6.6) em (6.5), teremos

$$q = \frac{2^{n_1}}{2^n} + \frac{2^{n_2}}{2^n} + \cdots + \frac{2^{n_{k-1}}}{2^n} + \frac{1}{2^n} = \frac{1}{2^{2^n - n_1}} + \frac{1}{2^{2^n - n_2}} + \cdots + \frac{1}{2^{2^n - n_{k-1}}} + \frac{1}{2^n} \tag{6.7}$$

que é a forma polinomial binária de q.

Resta-nos agora determinar a e n e, com esses dados, escrevermos (6.7). Para determinarmos n, usemos o Teorema 5.2, que nos garante que a forma decimal de cada parcela de (6.7) possui $n - n_i$ dígitos não inteiros. Além disso, note que (6.7) representa a soma $\sum_{i=1}^{k} q_{n-n_i}$ das linhas de ordem $n - n_1,\ n - n_2,\ \cdots,\ n - n_{k-1},\ n$ da matriz $\lceil 1 \rceil_n$. Usando isso, uma simples soma pode nos revelar que

$$N(q) = N\left(\sum_{i=1}^{k} q_{n-n_i}\right) = max\{n - n_i : i \in \{1, 2, \cdots, n\}\} = n$$

o que nos diz que a matriz complementar de a possui n colunas e n linhas (Teorema 5.2) e $[a]_n$ possui última linha $q_n = q$. Assim, para determinar o dividendo a devemos reconstituir $[a]_n$ a partir de sua última linha, o que exige que calculemos $\Delta_{(i-1)j}$ a partir de cada Δ_{ij}. Para isto, podemos usar o Corolário 3.1, ou então a técnica de *tentativa e verificação* que propomos a seguir:

1. Calculamos módulo 10 o dobro de Δ_{ij}, isto é, calculamos o resto de $2\Delta_{ij}$ na divisão por 10, que denotaremos por $2 \overset{(10)}{\odot} \Delta_{ij}$.

2. Verificamos se o valor encontrado satisfaz $\left\langle \overline{\Delta_{(i-1)j}}, \Delta_{(i-1)(j+1)} \right\rangle = \Delta_{i(j+1)}$. Caso afirmativo,

temos $\Delta_{(i-1)j} = 2 \overset{(10)}{\odot} \Delta_{ij}$. Do contrário, $\Delta_{(i-1)j} = 2 \overset{(10)}{\odot} \Delta_{ij} + 1$

De fato,

$$\Delta_{ij} = \left\langle \overline{\Delta_{(i-1)(j-1)}}, \Delta_{(i-1)j} \right\rangle \in \left\{ \frac{\Delta_{(i-1)j}}{2},\ \frac{\Delta_{(i-1)j}}{2} + 5,\ \frac{\Delta_{(i-1)j} - 1}{2},\ \frac{\Delta_{(i-1)j} - 1}{2} + 5 \right\}$$

$$\Rightarrow\ \Delta_{(i-1)j} \in \left\{ 2\Delta_{ij},\ 2\Delta_{ij} - 10,\ 2\Delta_{ij} + 1,\ (2\Delta_{ij} - 10) + 1 \right\}$$

o que equivale a

$$\Delta_{(i-1)j} \in \left\{ 2 \overset{(10)}{\odot} \Delta_{ij},\ 2 \overset{(10)}{\odot} \Delta_{ij} + 1 \right\}.$$

Uma vez obtido o valor de a, (6.7) nos ensina que devemos escrever a como soma de potências de 2, o que fazemos construindo a matriz

$$\begin{bmatrix} \overline{a_0} \\ \\ \overline{\beta(a_0)} \\ \\ \overline{\beta^2(a_0)} \\ \\ \vdots \\ \\ \overline{\beta^n(a_0)} \end{bmatrix} = \overline{A}$$

Conforme provamos na proposição 6.1. Note, entretanto, que essa matriz já foi obtida no processo de reconstrução de $[a]_n$, bastando agora que reescrevamos seus termos módulo 2. Na verdade, é totalmente dispensável a construção de $\lfloor a \rfloor_n$ por completo, uma vez que só precisaremos de $\overline{A}$. Isto suaviza sensivelmente o processo e nos devolve a na base 2 de imediato.

Ilustraremos o processo detalhadamente no exemplo a seguir:

Exemplo 6.6. *Converteremos a dízima $q = 0,05078125$ para o sistema binário. Para isso, devemos:*

1- Determinar as dimensões de $\lceil a \rceil_n$ e sua linha final q_n:

$$n = N(q) = 8 \text{ e } q_n = \begin{pmatrix} 0 & 5 & 0 & 7 & 8 & 1 & 2 & 5 \end{pmatrix}$$

2- Construir $\lceil a \rceil_n$*:*

0	5	0	7	8	1	2	5

3-Determinar os termos Δ_{ii}, $\Delta_{i(i-1)}$ *e* $\Delta_{i(i-2)}$ *que já conhecemos:*

5							
2	5						
6	2	5					
	1	2	5				
		6	2	5			
			1	2	5		
				6	2	5	
0	5	0	7	8	1	2	5

4-Calcular os termos que faltam por teste e verificação: Se $\Delta_{(i-1)j}$ *é o dígito procurado e* Δ_{ij} *é o dígito que está imediatamente abaixo na matriz, fazemos*

$$x = 2 \overset{(10)}{\odot} \Delta_{ij} \tag{6.8}$$

e depois verificamos se ocorre

$$\left\langle \overline{x}, \Delta_{(i-1)(j+1)} \right\rangle = \Delta_{i(j+1)}. \tag{6.9}$$

Se a igualdade 6.9 é verdadeira, então $x = \Delta_{(i-1)j}$; caso contrário, $\Delta_{(i-1)j} = x+1$.

Usando isto para determinar os elementos da penúltima linha, temos:

$x = 2 \overset{(10)}{\odot} 7 = 4 \Rightarrow \left\langle \overline{4}, 6 \right\rangle = 3 \neq 8 \Rightarrow \Delta_{74} = 5$

$x = 2 \overset{(10)}{\odot} 0 = 0 \Rightarrow \left\langle \overline{0}, 5 \right\rangle = 2 \neq 7 \Rightarrow \Delta_{73} = 0+1 = 1$

$x = 2 \overset{(10)}{\odot} 5 = 0 \Rightarrow \left\langle \overline{0}, 1 \right\rangle = 0 \Rightarrow \Delta_{72} = 0$

$x = 2 \overset{(10)}{\odot} 0 = 0 \Rightarrow \left\langle \overline{0}, 0 \right\rangle = 0 \neq 5 \Rightarrow \Delta_{71} = 0+1 = 1$:

5							
2	5						
6	2	5					
	1	2	5				
		6	2	5			
			1	2	5		
1	0	1	5	6	2	5	
0	5	0	7	8	1	2	5

De modo análogo determinamos os demais termos da matriz complementar:

5							
2	5						
6	2	5					
8	1	2	5				
4	0	6	2	5			
2	0	3	1	2	5		
1	0	1	5	6	2	5	
0	5	0	7	8	1	2	5

5-Construir a matriz coluna $\overline{A}$, para obter a: Basta decidir o valor binário de cada célula: 0 ou 1, o que se pode fazer facilmente resolvendo as equações em $\overline{\beta^i(a_0)}$ dadas por:

$$\left\langle \overline{\beta^i(a_0)}, \Delta_{i1} \right\rangle = \Delta_{(i+1)1} \tag{6.10}$$

e lembrando que $\Delta_{11} = \langle \overline{a_0}, 0 \rangle$ e $\beta^8(a_0) = \lfloor q \rfloor = 0$. Usando isto, temos:

$$\langle \overline{a_0}, 0 \rangle = 5 \;\Rightarrow\; \overline{a_0} = 1$$

$$\left\langle \overline{\beta^1(a_0)}, 5 \right\rangle = 2 \;\Rightarrow\; \overline{\beta^1(a_0)} = 0$$

$$\left\langle \overline{\beta^2(a_0)}, 2 \right\rangle = 6 \;\Rightarrow\; \overline{\beta^2(a_0)} = 1$$

$$\left\langle \overline{\beta^3(a_0)}, 6 \right\rangle = 8 \;\Rightarrow\; \overline{\beta^3(a_0)} = 1$$

$$\left\langle \overline{\beta^4(a_0)}, 8 \right\rangle = 4 \;\Rightarrow\; \overline{\beta^4(a_0)} = 0$$

$$\left\langle \overline{\beta^5(a_0)}, 4 \right\rangle = 2 \;\Rightarrow\; \overline{\beta^5(a_0)} = 0$$

$$\left\langle \overline{\beta^6(a_0)}, 2 \right\rangle = 1 \Rightarrow \overline{\beta^6(a_0)} = 0$$

$$\left\langle \overline{\beta^7(a_0)}, 1 \right\rangle = 0 \Rightarrow \overline{\beta^7(a_0)} = 0$$

Logo, temos

$$\overline{A} = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

e então,

$$a = \left(\overline{\beta^8(a_0)}\ \overline{\beta^7(a_0)}\ \overline{\beta^6(a_0)}\ \overline{\beta^5(a_0)}\ \overline{\beta^4(a_0)}\ \overline{\beta^3(a_0)}\ \overline{\beta^2(a_0)}\ \overline{\beta^1(a_0)}\ \overline{a_0}\right)_2 = (000001101)_2 =$$

$$= (1101)_2$$

o que nos dá $a = 2^3 + 2^2 + 1$.

6-Escrever a soma binária conforme 6.7:

$$a = \frac{1}{2^{8-3}} + \frac{1}{2^{8-2}} + \frac{1}{2^8} = \frac{1}{2^5} + \frac{1}{2^6} + \frac{1}{2^8} = (0,00001101)_2. \qquad \square$$

Na verdade, uma vez de posse da expressão binária de a, podemos operar diretamente na base 2 se fizermos a conversão do divisor, o que é algo simples e que torna os cálculos mais diretos e intuitivos. No exemplo anterior, poderíamos fazer $2^8 = (10^8)_2$ e então,

$$\frac{a}{2^8} = \left(\frac{1101}{10^8}\right)_2 = (0,00001101)_2.$$

Exemplo 6.7. *Escrevamos $q = 7,8359375$ no sistema binário:*

Inicialmente, separamos as partes inteira e não inteira:

$\lfloor q \rfloor = 7 = 2^2 + 2 + 1 = (111)_2$.

Para $q - \lfloor q \rfloor$, construímos a matriz conforme o tutorial anterior. Por praticidade, escreveremos uma coluna adicional à esquerda da matriz para representar $\overline{A}$, e uma linha extra acima, para representar $\overline{a_0}$ e a_{-1}:

1	0						
1	5						
0	7	5					
1	3	7	5				
0	6	8	7	5			
1	3	4	3	7	5		
1	6	7	1	8	7	5	
0	8	3	5	9	3	7	5

Logo, $q - \lfloor q \rfloor = \left(\dfrac{1101011}{10^7} \right)_2 = (0, 1101011)_2$,

e daí,

$q = (111, 1101011)_2$. □

6.5 Aplicações com a Forma Produto

Encerraremos nossa exposição apresentando duas singelas aplicações do algoritmo do par binário que podem ser confortavelmente usadas em qualquer etapa do ensino básico, e que decorrem da *forma produto* (Definição 5.9). De fato, para obtê-las, não precisaremos dispor de nenhuma teoria adicional, mas tão-somente da reescrita adequada do quociente em questão.

Seja, pois, $q = \dfrac{a}{2^n} \cdot 10^m$. Analisaremos separadamente os casos $m \neq n$ e $m = n$:

1) Se $m \neq n$, reescrevendo

$$q = \frac{a}{2^n \cdot 10^{-m}}$$

obtemos quocientes com novos divisores não contemplados até aqui, mas inteiramente calculáveis pelos métodos que propomos.

Exemplo 6.8. *Calculemos a forma decimal de* $q = \dfrac{3}{2,56}$*:*

Sabemos que $256 = 2^8$, *e daí, temos* $2,56 = 2^8 \cdot 10^{-2}$. *Logo, podemos reescrever*

$$q = \frac{3}{2^8 \cdot 10^{-2}} = \frac{3}{2^8} \cdot 10^2$$

e daí, precisamos construir a matriz $[3]_8$. *É o que faremos:*

3								
1	5							
.	7	5						
.	3	7	5					
.	1	8	7	5				
.	.	9	3	7	5			
.	.	4	6	8	7	5		
.	.	2	3	4	3	7	5	
0	0	1	1	7	1	8	7	5

Temos então $q = 0,01171875 \cdot 10^2 = 1,1171875$. □

Exemplo 6.9. *Para* $q = \dfrac{18000}{0,0032}$, *temos*

$$q = \frac{18 \cdot 10^3}{2^5 \cdot 10^{-4}} = \frac{18}{2^5} \cdot 10^7$$

Calculando $\dfrac{18}{2^5}$, *temos:*

1	8				
.	9				
.	4	5			
.	2	2	5		
.	1	1	2	5	
0	0	5	6	2	5

e então, $q = 0,05625 \cdot 10^7 = 562500$. □

Exemplo 6.10. *Para* $q = \dfrac{0,7}{1600}$, *temos*

$$q = \frac{7 \cdot 10^{-1}}{2^4 \cdot 10^2} = \frac{7}{2^4} \cdot 10^{-3}$$

e daí temos:

$$[7]_4 = \begin{pmatrix} 3 & 5 & & & \\ 1 & 7 & 5 & & \\ 0 & 8 & 7 & 5 & \\ 0 & 4 & 3 & 7 & 5 \end{pmatrix}$$

o que nos dá $q = 0,4375 \cdot 10^{-3} = 0,0004375$. □

2) Se $m = n$, podemos escrever

$$q = \frac{a}{2^n} \cdot 10^n = a \cdot \frac{10^n}{2^n} = a \cdot \left(\frac{10}{2}\right)^n = a \cdot 5^n,$$

e obtemos uma identidade que nos permite aplicar a divisão por 2^n e, consequentemente, do Algoritmo do par binário para o cálculo de produtos do tipo $a \cdot 5^n$:

Proposição 6.5 (Multiplicação por Potências de Base 5)**.** *:*

Se $k \in \mathbb{N}^*$, $I \subset \mathbb{Z}$ *e* $a = \sum_{i \in I} a_i 10^i$, *então* $a \cdot 5^k = \sum_{i \in I} \beta^k(a_i) 10^i$

Em particular, se $n = 1$, a identidade

$$a \cdot 5 = \frac{a}{2} \cdot 10 \tag{6.11}$$

nos retorna o produto por 5 por meio da divisão por 2. Por outro lado, se $a = 1$ temos

$$5^n = \frac{1}{2^n} \cdot 10^n$$

e o teorema 5.2 nos diz que $\frac{1}{2^n}$ possui n algarismos fracionários, e daí, o produto pelo fator 10^n nos diz que 5^n será o número cujos algarismos são a $n-$ésima linha da matriz $\lceil 1 \rfloor_n$, cuja determinação não oferece maiores dificuldades.

Exemplo 6.11 (Multiplicação por 5)**.** *Vamos calcular alguns produtos de fator 5:*

a) $5 \cdot 147 = \frac{147}{2} \cdot 10 = \langle \overline{0}, 1 \rangle \langle \overline{1}, 4 \rangle \langle \overline{4}, 7 \rangle \langle \overline{7}, 0 \rangle = 0735.$

b) $0,095 \cdot 5 = \frac{95 \cdot 10^{-3}}{2} \cdot 10 = \frac{95}{2} \cdot 10^{-2} = \langle \overline{0}, 9 \rangle \langle \overline{9}, 5 \rangle, \langle \overline{5}, 0 \rangle \cdot 10^{-2} = 0,475.$

c) $0,099 \cdot 0,05 = 99 \cdot 10^{-3} \cdot 5 \cdot 10^{-2} = 99 \cdot 5 \cdot 10^{-5} = \langle \overline{0}, 9 \rangle \langle \overline{9}, 9 \rangle, \langle \overline{9}, 0 \rangle \cdot 10^{-4} = 495 \cdot 10^{-4} =$
$= 0,00495.$ □

Exemplo 6.12 (Potências de 5)**.** *Vamos determinar as potências* $5^3, 5^5$, *e* 5^7. *Por* 6.12, as conseguiremos determinando a 3.ª, a 5.ª e a 7.ª linhas de $\lceil 1 \rceil_7$:

$$\lceil 1 \rceil_7 = \begin{pmatrix} 5 & & & & & & \\ 2 & 5 & & & & & \\ 1 & 2 & 5 & & & & \\ 0 & 6 & 2 & 5 & & & \\ 0 & 3 & 1 & 2 & 5 & & \\ 0 & 1 & 5 & 6 & 2 & 5 & \\ 0 & 0 & 7 & 8 & 1 & 2 & 5 \end{pmatrix}$$

Temos então $5^3 = q_3 = 125$, $5^5 = q_5 = 3125$ e $5^7 = q_7 = 78125$ □

Exemplo 6.13 (Produto por potências de 5)**.** *Calculemos* $p = 57 \cdot 5^9$*:*

Pela proposição 6.5, $p = q_9 \cdot 10^9$*, o que nos induz a determinar a 9.ª linha de* $[57]_9$*:*

5	7									
2	8	5								
1	4	2	5							
.	7	1	2	5						
.	3	5	6	2	5					
.	1	7	8	1	2	5				
.	.	8	9	2	6	2	5			
.	.	4	4	5	3	1	2	5		
.	.	2	2	2	6	5	6	2	5	
0	0	1	1	1	3	2	8	1	2	5

Logo, $p = 111328125$ □

Exemplo 6.14. *Calcular* $0,25^3$:

Temos $0,25^3 = (25 \cdot 10^{-2})^3 = (5^2 \cdot 10^{-2})^3 = 5^6 \cdot 10^{-6} = \frac{1}{2^6} \cdot 10^6 \cdot 10^{-6} = \frac{1}{2^6} = q_6$

Agora, consultando a matriz que construímos no exemplo 6.12, temos $q_6 = 0,015625$. □

7 PROPOSTA DE SEQUÊNCIA DIDÁTICA: JOGO DOS CARTÕES NUMERADOS

7.1 Descrição e Regras

O Jogo dos cartões numerados é uma popular atividade matemático-recreativa da linha das "matemágicas", segmento de jogos matemáticos que se prestam à utilização de propriedades aritméticas dos números inteiros para gerar o efeito da adivinhação ou previsão do futuro.

Como seu nome sugere, este jogo consiste numa coleção de cartões, em geral 6, cada um com 32 números inteiros escolhidos entre o 1 e o 63, inclusive, distribuídos de forma aparentemente aleatória em cada cartão, em ordem crescente, de modo que cada número aparece em pelo menos um dos cartões.

Participam dele dois jogadores, um um dos quais ocupará a função de "mágico"e o outro, a função de voluntário da "plateia". A este último, será entregue o baralho e caberá escolher um número qualquer de um dos cartões. Em seguida, é solicitado a memorizar o número escolhido e mantê-lo em segredo. Os cartões são mais uma vez embaralhados e entregues ao mágico. Feito isso, o mágico os tomará nas mãos e os mostrará um por um ao voluntário, que será convidado a indicar os cartões que possuem o número que escolheu.

O voluntário, então, faz isso, e ao fim da última carta mostrada pelo mágico, este, como num "passe de mágica", revelará à plateia o número escolhido por aquele, para surpresa de todos.

7.2 O Segredo

Há diversas referências disponíveis, sobretudo na internet, que se prestam a explicar o funcionamento da suposta mágica dos cartões. Dentre estas, destacamos Menezes ([22]) que o faz para o

caso particular do jogo para 5 cartões. Aqui o faremos para a forma mais habitual de apresentação do jogo, a de seis cartas, que permite a utilização dos inteiros no intervalo de 1 a 64. Para tanto, considere o quadro 7.2, na qual são exibidas o conjunto de cartas para tal apresentação.

Atentemo-nos agora ao primeiro número de cada cartão. Perceba que em todos eles essa posição é ocupada por uma potência de 2; a saber, 1, 2 ,4, 8, 16, 32. Para facilitar a referência, nomearemos os cartões de acordo com esse primeiro número: assim, a carta 2^2 ou 4 será a carta cujo primeiro número é o 4, por exemplo.

Conhecido isto, o truque é bem simples: quando o voluntário for solicitado a indicar em quais das cartas o número escolhido comparece, o mágico deve atentar rapidamente para o valor desse primeiro número em cada cartela, com o fim de os somar à medida que as cartas escolhidas foram sendo reveladas. A menos de erro de atenção do voluntário ou de cálculo do mágico, o número secreto será o resultado dessa soma.

Quadro 2: Cartões para o jogo com seis cartas

carta 2^0				**carta** 2^1				**carta** 2^2			
1	**3**	**5**	**7**	**2**	**3**	**6**	**7**	**4**	**5**	**6**	**7**
9	**11**	**13**	**15**	**10**	**11**	**14**	**15**	**12**	**13**	**14**	**15**
17	**19**	**21**	**23**	**18**	**19**	**22**	**23**	**20**	**21**	**22**	**23**
25	**27**	**29**	**31**	**26**	**27**	**30**	**31**	**28**	**29**	**30**	**31**
33	**35**	**37**	**39**	**34**	**35**	**38**	**39**	**36**	**37**	**38**	**39**
41	**43**	**45**	**47**	**42**	**43**	**46**	**47**	**44**	**45**	**46**	**47**
49	**51**	**53**	**55**	**50**	**51**	**54**	**55**	**52**	**53**	**54**	**55**
57	**59**	**61**	**63**	**58**	**59**	**62**	**63**	**60**	**61**	**62**	**63**

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

Fonte: Autor, 2013

Exemplo 7.1. *Suponha que o voluntário escolha um número que esteja nos cartões* 2^0, 2^1 *e* 2^4. *O mágico, nesse caso, deve realizar mentalmente a soma: 16+2+1=19* □

É claro que tanto mais convincente será a mágica quanto maior for a destreza do mágico em realizar cálculos com as potências de 2 referente às cartas.

7.3 Análise do Jogo

O segredo do funcionamento do jogo reside na forma criteriosa com que os números são distribuídos entre as cartelas. Com efeito, considerando a Proposição 6.2, sabemos que todo número inteiro pode ser escrito de maneira única como uma soma de potências de base 2, a qual, por sua vez, se associa uma forma binária inteira.

Nessas condições, perceba inicialmente que se considerarmos as potências 2^0, 2^1, 2^2, 2^3, 2^4 e 2^5, então o menor inteiro positivo que pode ser representado a partir da soma de tais parcelas é $2^0 = 1$, enquanto que o maior inteiro é dado por 1+2+4+8+16+32=63.

Tendo isto em vista, a ideia é a de alocarmos em cada carta 2^n todos, e apenas os números inteiros que possuem a parcela 2^n em sua forma binária. Desse modo, quando o voluntário nos indica as cartas em que constam o número que ele escolheu, ele estará, na verdade, nos retornando a representação binária do número escolhido. Daí, uma soma trivial nos revela o resultado.

Exemplo 7.2. *: No caso do exemplo 7.1, quando o voluntário nos retorna a informação de que o número escolhido encontra-se nos cartões* 2^0, 2^1 *e* 2^4, *estará revelando que o número escolhido possui a forma binária em que as ordens 0, 1, e 4 são não-nulas, do que segue que o número escolhido será dado por* $(10011)_2 = 2^4 + 2 + 1 = 16 + 2 + 1 = 19$ □

7.4 Construção dos Cartões

Uma vez tratado o funcionamento do Sistema Binário e explorada a técnica de conversão que apresentamos no capítulo 6, a confecção de um conjunto de cartões pelo aluno pode se constituir numa atividade de assimilação de conteúdo muito enriquecedora. De fato, uma vez tendo aprendido a escrever na forma binária um inteiro dado no sistema decimal, a construção de um baralho de seis cartas exigirá do aluno que este converta corretamente os números inteiros no intervalo de 1 a 63.

Aqui sugerimos que se organize um quadro cujas linhas sejam as formas binárias dos inteiros de 1 a 63, e cujas colunas sejam os algarismos binários de cada ordem. Nessas condições, a bijetividade da função que associa um inteiro a à sua representação binária (Teorema 2.1) nos garante que as linhas de tal quadro são distintas entre si, acontecendo o mesmo com suas colunas.

Uma vez feito isto, os cartões do jogo se referirão a cada uma das ordens binárias (colunas) do número inteiro a (linhas), e daí, cada cartão 2^i deverá conter os números cujas linhas correspondentes apresentem o digito 1 na coluna relativa i.

Nos quadros 7.4, 7.4 e 7.4 apresentamos o quadro correspondente a um conjunto de 6 cartas. Para ilustrar o processo, considere o exemplo a seguir:

Exemplo 7.3. *: Suponha que queiramos construir o cartão* 2^4*. Observemos, então, a coluna correspondente a* 2^4 *nos quadros 7.4, 7.4 e 7.4. Nelas, as linhas que possuem o digito 1 são, em ordem crescente, as linhas de 16 a 31, e as linhas de 48 a 63. Isto significa que o cartão* 2^4 *deverá conter todos os inteiros de 16 a 31, e de 48 a 63, inclusive.* □

Quadro 3: Codificação Binária dos inteiros de 1 a 21 para confecção dos cartões

a	a_5	a_4	a_3	a_2	a_1	a_0
1	**0**	**0**	**0**	**0**	**0**	**1**
2	**0**	**0**	**0**	**0**	**1**	**0**
3	**0**	**0**	**0**	**0**	**1**	**1**
4	**0**	**0**	**0**	**1**	**0**	**0**
5	**0**	**0**	**0**	**1**	**0**	**1**
6	**0**	**0**	**0**	**1**	**1**	**0**
7	**0**	**0**	**0**	**1**	**1**	**1**
8	**0**	**0**	**1**	**0**	**0**	**0**
9	**0**	**0**	**1**	**0**	**0**	**1**
10	**0**	**0**	**1**	**0**	**1**	**0**
11	**0**	**0**	**1**	**0**	**1**	**1**
12	**0**	**0**	**1**	**1**	**0**	**0**
13	**0**	**0**	**1**	**1**	**0**	**1**
14	**0**	**0**	**1**	**1**	**1**	**0**
15	**0**	**0**	**1**	**1**	**1**	**1**
16	**0**	**1**	**0**	**0**	**0**	**0**
17	**0**	**1**	**0**	**0**	**0**	**1**
18	**0**	**1**	**0**	**0**	**1**	**0**
19	**0**	**1**	**0**	**0**	**1**	**1**
20	**0**	**1**	**0**	**1**	**0**	**0**
21	**0**	**1**	**0**	**1**	**0**	**1**

Fonte: Autor, 2013

Quadro 4: Codificação Binária dos inteiros de 22 a 42 para confecção dos cartões

a	a_5	a_4	a_3	a_2	a_1	a_0
22	**0**	**1**	**0**	**1**	**1**	**0**
23	**0**	**1**	**0**	**1**	**1**	**1**
24	**0**	**1**	**1**	**0**	**0**	**0**
25	**0**	**1**	**1**	**0**	**0**	**1**
26	**0**	**1**	**1**	**0**	**1**	**0**
27	**0**	**1**	**1**	**0**	**1**	**1**
28	**0**	**1**	**1**	**1**	**0**	**0**
29	**0**	**1**	**1**	**1**	**0**	**1**
30	**0**	**1**	**1**	**1**	**1**	**0**
31	**0**	**1**	**1**	**1**	**1**	**1**
32	**1**	**0**	**0**	**0**	**0**	**0**
33	**1**	**0**	**0**	**0**	**0**	**1**
34	**1**	**0**	**0**	**0**	**1**	**0**
35	**1**	**0**	**0**	**0**	**1**	**1**
36	**1**	**0**	**0**	**1**	**0**	**0**
37	**1**	**0**	**0**	**1**	**0**	**1**
38	**1**	**0**	**0**	**1**	**1**	**0**
39	**1**	**0**	**0**	**1**	**1**	**1**
40	**1**	**0**	**1**	**0**	**0**	**0**
41	**1**	**0**	**1**	**0**	**0**	**1**
42	**1**	**0**	**1**	**0**	**1**	**0**

Fonte: Autor, 2013

Quadro 5: Codificação Binária dos inteiros de 43 a 63 para confecção dos cartões

a	a_5	a_4	a_3	a_2	a_1	a_0
43	**1**	**0**	**1**	**0**	**1**	**1**
44	**1**	**0**	**1**	**1**	**0**	**0**
45	**1**	**0**	**1**	**1**	**0**	**1**
46	**1**	**0**	**1**	**1**	**1**	**0**
47	**1**	**0**	**1**	**1**	**1**	**1**
48	**1**	**1**	**0**	**0**	**0**	**0**
49	**1**	**1**	**0**	**0**	**0**	**1**
50	**1**	**1**	**0**	**0**	**1**	**0**
51	**1**	**1**	**0**	**0**	**1**	**1**
52	**1**	**1**	**0**	**1**	**0**	**0**
53	**1**	**1**	**0**	**1**	**0**	**1**
54	**1**	**1**	**0**	**1**	**1**	**0**
55	**1**	**1**	**0**	**1**	**1**	**1**
56	**1**	**1**	**1**	**0**	**0**	**0**
57	**1**	**1**	**1**	**0**	**0**	**1**
58	**1**	**1**	**1**	**0**	**1**	**0**
59	**1**	**1**	**1**	**0**	**1**	**1**
60	**1**	**1**	**1**	**1**	**0**	**0**
61	**1**	**1**	**1**	**1**	**0**	**1**
62	**1**	**1**	**1**	**1**	**1**	**0**
63	**1**	**1**	**1**	**1**	**1**	**1**

Fonte: Autor, 2013

7.5 Sequência didática

A seguir apresentamos uma sugestão de sequência didática utilizando o Jogo dos cartões numerados:

Objetivo

Introduzir o Sistema de Numeração Binário no universo $\mathbb{Z}$.

Público-alvo

Alunos do Ensino Fundamental, Ensino Médio ou Médio Profissionalizante voltado para a área das ciências da informação e afins.

Metodologia e Tempo Pedagógico

1. Apresentação do Jogo dos cartões numerados e exposição do seu funcionamento (1 h/a);
2. Apresentação do Sistema binário de numeração e da decomposição de um inteiro como soma de potências de base 2 (2 h/a);
3. Abordagem tradicional da conversão entre os sistemas Binário e decimal (2 h/a);
4. Introdução do Algoritmo do Par binário no contexto da iteração de quocientes e sua aplicação na conversão de números inteiros da forma decimal para a binária (2 h/a);
5. Atividade de fixação de aprendizagem e avaliação: Confecção dos cartões do jogo (2 h/a);
6. Levantamento de questões complementares (2 h/a).

Para a etapa de conclusão de trabalhos, convém levantar questões que instiguem o estudante a refletir sobre as consequências na alteração de algumas características do jogo, tais como o uso de um intervalo maior de inteiros, o que tornaria o efeito do truque ainda mais surpreendente, embora aumente a quantidade de cartas, e daí, a complexidade dos cálculos mentais envolvidos, o porquê da utilização da base binária ao invés de outra qualquer, bem como a possibilidade de repetir o truque em tais condições, dentre outros questionamentos do gênero cuja resposta, em geral, pode exigir uma maior compreensão do sistema de representação númerico, e daí, suscitar o desejo de pesquisa complementar no estudante.

Além das etapas prescritas acima, a depender da maturidade da turma, tempo disponível para tanto e objetivos específicos do curso, constituem interessantes desdobramentos da proposta a abordagem dos seguintes temas suplementares:

(a) Sistema binário em $\mathbb{R}$ e aplicação do Algoritmo do par binário na conversão entre as bases 10 e 2 nesse universo;

(b) Operações fundamentais no sistema binário: Tábuas de operação em $\mathbb{Z}_2$;

(c) Conversão entre linguagem de máquina e linguagem humana: Neste tema, pode ser particularmente interessante mencionar a *Tabela de Códigos ASCII*[1] que consiste numa tábua de conversão de caracteres e comandos codificados entre as bases decimal e binária, e

> "é usada pela maior parte da indústria de computadores para a troca de informações [entre homem e máquina]. Cada caractere é representado por um código de 8 bits[2]" (Cruz: [8]).

Avaliação

Sugerimos que seja feita de duas formas distintas e complementares: a primeira, contínua e subjetiva, no decorrer do processo, englobando aspectos como participação e trabalho em grupo, e objetiva e focal, ao final do processo, contemplando o conteúdo de início proposto.

[1] sigla da língua inglesa para *American Standard Code for Information Interchange*, que em português significa "Código Padrão Americano para o Intercâmbio de Informação"

[2] *bit: Binary digit*: Termo utilizado na computação para representar os algarismos do sistema binário: 0, que representa o circuito aberto, e 1, que representa o circuito fechado.

CONSIDERAÇÕES FINAIS

No presente trabalho apresentamos o algoritmo do par binário, teorema de nossa autoria que possibilita o cálculo da forma decimal do quociente numa divisão euclidiana por 2 de dividendos inteiros a partir da definição da função par binário, que se presta à associação direta de cada algarismo do dividendo ao seu respectivo de mesma ordem no quociente.

Demonstramos a validade de tal algoritmo no universo $\mathbb{Z}$ partindo de sua forma mais elementar, para o divisor 2, e, a partir daí, recorrendo à análise real, indução finita e à notação matricial, procedemos à generalização do algoritmo do par binário a dividendos em $\mathbb{R}$, num primeiro momento, e a divisores do tipo $2^n,\ n \in \mathbb{N}^*$, em seguida. Para tanto, definimos a função par binário composto e estabelecemos a conexão com a álgebra matricial, com o que tornou-se possível a determinação de cada algarismo do quociente $a/2^n$ a partir da iterada aplicação da função par binário em cada algarismo do dividendo, tomados a partir da maior para a menor ordem. Nessa fase foi possível detectar diversas regularidades interessantes relativas à terminação decimal dos quocientes iterados a partir de dividendos decimais de expansão finita, o que contribuiu significativamente para a aceleração do processo.

Como consequência direta dos resultados tratados no decorrer do texto, foi possível detectar diversas possibilidades de aplicações, das quais destacamos a conversão de números reais entre as bases decimal e binária, o cálculo de potências de 5 com expoente natural e o produto por tais potências, e obtivemos, como corolário do teorema do par binário em $\mathbb{Z}$, o algoritmo tradicional da multiplicação por 2.

Finalmente, como produto final de nosso trabalho, propusemos uma sequência didática baseada no conhecido jogo "matemágica dos cartões numerados", na qual é introduzido o sistema binário de numeração e a teoria desenvolvida nos capítulos precedentes é aplicada como facilitadora do processo de ensino de tal conteúdo.

Por ocasião da conclusão deste trabalho, percebemos que o estudo do tema proposto não se encontra definitivamente encerrado. Conjecturas tais como a possibilidade de generalização da função par binário a outros divisores, do teorema principal a outras bases de numeração, e da existência de uma regra geral para o cálculo da terminação decimal de quocientes de dízimas finitas com qualquer número de algarismos fracionários, dentre outras, surgiram naturalmente no nosso estudo e mostraram-se como pistas para um futuro prosseguimento para tal pesquisa.

Referências Bibliográficas

[1] ARENALES, Selma e DAREZZO, Artur. *Cálculo Numérico:* Aprendizagem com o apoio de Software São Paulo: Thompson, 2011.

[2] ÁVILA, Geraldo Severo de Souza. *Análise Matemática para Licenciatura.* 3.ª ed. rev. amp. São Paulo: Edgard Blücher, 2011.

[3] BIANCHINI, E. & PACCOLA, H. *Sistemas de Numeração ao Longo da História.* 2.ª ed. São Paulo: Moderna, 1997.

[4] BRASIL, Secretaria de Educação Fundamental. *Parâmetros Curriculares Nacionais do Ensino Fundamental.* Matemática. Brasília: Ministério da Educação: 1998.

[5] BRASIL, Secretaria de Educação Fundamental. *Parâmetros Curriculares Nacionais do Ensino Fundamental.* Matemática: Ensino de primeira à quarta série. Brasília: MEC/SEF: 1997.

[6] BRASIL, Secretaria de Educação Média e tecnológica. *Parâmetros Curriculares Nacionais do Ensino Médio:* Linguagens, códigos e suas tecnologias. Brasília: Ministério da Educação: 2000.

[7] BRASIL, Secretaria de Educação Média e tecnológica. *PCN+ Ensino Médio:* Orientações Educacionais complementares aos Parâmetros Curriculares Nacionais. Linguagens, códigos e suas tecnologias. Brasília: Ministério da Educação: 2002.

[8] CRUZ, A. J. O. *Tabela ASCII*. Disponível em <http://equipe.nce.ufrj.br/adriano/c/apostila/ tabascii.htm>. Acesso em 21 de Abril de 2013.

[9] DOMINGUES, Hygino. *Fundamentos de Aritmética*. São Paulo:Atual, 1991.

[10] DOMINGUEZ, H. E IEZZI, G. *Álgebra Moderna.* 4.ª ed. ref. São Paulo: Atual, 2003.

[11] EVES, Howard. *Introdução à História da Matemática*. Tradução de Hygino H. Domingues. Campinas: Editora da UNICAMP, 2008.

[12] GIOVANNI, José Ruy e PARENTE, E. A. de Medeiros. *Matemática:* 1.º grau. São Paulo: FTD, 1988.

[13] HEFEZ, Abramo. *Curso de Álgebra* . 3.ª ed. Rio de Janeiro: IMPA, 2002. Coleção Matemática Universitária.

[14] HEFEZ, Abramo. *Elementos de Aritmética.* Rio de Janeiro: IMPA, 2002. Coleção Textos Universitários.

[15] JAKUBOVIC, José. *Par ou ímpar.* 4.ª edição. São Paulo: Scipione, 1995. Coleção Vivendo a Matemática.

[16] LIMA, E.L. et al. *A matemática do Ensino Médio volume 1*. 9.ª ed. Rio de Janeiro, SBM: 2006. Coleção do Professor de Matemática

[17] LIMA, E. L. *Análise Real Volume 1:* Funções de Uma Variável. 11.ª ed. Rio de Janeiro: IMPA, 2011. Coleção Matemática Universitária.

[18] LIMA, E. L. Base Decimal ou Duodecimal. *Revista do Professor de Matemática* n.º 12. Rio de Janeiro: SBM, 1987.

[19] LIMA, E. L. *Curso de Análise Volume 1.* 13.ª ed. Rio de Janeiro: IMPA, 2011. Coleção Projeto Euclides.

[20] LIMA, E.L. et al. *Meu Professor de Matemática e Outras Histórias.* Rio de Janeiro, SBM: 1991. Coleção do Professor de Matemática

[21] LUNA, J.E.L. *Programa de qualificação do Ensino de Matemática em Nível Médio: uma proposta para a Escola Francisco Pereira da Costa*. Monografia. Garanhuns, (Não publicado): 2007.

[22] MENEZES, S. V. *Matemágica binária*. Disponível em <http:// colegiosantamarcelina.com.br/Theorema/binaria.pdf>. Acesso em 24 de Abril de 2013.

[23] MOREIRA, Carlos Gustavo Moreira et al. *Teoria dos Números: um passeio com primos e outros números familiares pelo mundo inteiro.* 2.ª ed. Rio de Janeiro: IMPA, 2011. Coleção Projeto Euclides.

[24] MORGADO, A. C. et al. *Progressões e Matemática Financeira.* 4.ª ed. Rio de Janeiro, SBM: 2001. Coleção do Professor de Matemática.

[25] MUNIZ NETO, Antônio Caminha. *Tópicos de Matemática Elementar Volume 5: Teoria dos números*. Rio de Janeiro: SBM, 2012. Coleção do Professor de Matemática.

[26] PERNAMBUCO, Secretaria de Educação. *Base Curricular Comum para as Redes Públicas de Ensino de Pernambuco.* Matemática. Recife: SE, 2008.

[27] SANTOS, José Plínio de Oliveira. *Introdução à Teoria dos Números* . 2.ª ed. Rio de Janeiro: IMPA, 2000. Coleção Matemática universitária.

[28] TÁBOAS, Carmem M. G. & RIBEIRO, Hermano de Souza. Sobre Critérios de Divisibilidade. *Revista do Professor de Matemática*. Rio de Janeiro: SBM, 2012.

[29] ANGELA e et al. *Fundamentos de Álgebra.* Belo Horizonte: Editora UFMG, 2009.