Charles James Leite Martins

Algoritmo da Divisão de Euclides: uma nova proposta de ensino de matemática na educação básica

Dissertação apresentada como parte dos requisitos para obtenção do título de Mestre em Matemática, junto ao Programa de Pós-Graduação em Matemática em Rede Nacional, do Instituto de Biociências, Letras e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", Câmpus de São José do Rio Preto.

Orientador: Prof. Dr. Edson Donizete de Carvalho

São José do Rio Preto

2015

Martins, Charles James Leite.
Algoritmo da divisão de Euclides : uma nova proposta de ensino de matemática na educação básica / Charles James Leite Martins. -- São José do Rio Preto, 2015
74 f. : tabs.

Orientador: Edson Donizete de Carvalho
Dissertação (mestrado profissional) – Universidade Estadual Paulista "Júlio de Mesquita Filho", Instituto de Biociências, Letras e Ciências Exatas

1. Matemática - Estudo e ensino. 2. Aritmética - Estudo e ensino. 3. Algoritmos. 4. Matemática - Metodologia. I. Carvalho, Edson Donizete de. II. Universidade Estadual Paulista "Júlio de Mesquita Filho". Instituto de Biociências, Letras e Ciências Exatas. III. Título.
CDU – 511(07)

Ficha catalográfica elaborada pela Biblioteca do IBILCE
UNESP - Câmpus de São José do Rio Preto

Charles James Leite Martins

Algoritmo da Divisão de Euclides: uma nova proposta de ensino de matemática na educação básica

Dissertação apresentada como parte dos requisitos para obtenção do título de Mestre em Matemática, junto ao Programa de Pós-Graduação em Matemática em Rede Nacional, do Instituto de Biociências, Letras e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", Câmpus de São José do Rio Preto.

Banca Examinadora

Prof. Dr. Edson Donizete de Carvalho
UNESP - Ilha Solteira/SP
Orientador

Prof. Dr. Inocêncio Fernandes Balieiro Filho
UNESP - Ilha Solteira/SP

Profa.. Dra.Elen Viviani Pereira Spreafico
Universidade Federal do Mato Grosso do Sul - Campo Grande/MS

São José do Rio Preto

2015

AGRADECIMENTOS

Primeiramente agradeço a Deus, aos meus pais Wilson (in memorian) e Ivani que muito me incentivaram nos meus estudos, a minha esposa Cristiane pelo estímulo e paciência nestes anos de estudo e a CAPES pelo apoio financeiro.

Agradeço imensamente ao meu professor e orientador Prof. Dr. Edson Donizete de Carvalho, pela dedicação, orientações e conselhos, e também a todos os professores do Profmat da Unesp de Ilha Solteira, pelos ensinamentos e em especial ao meu professor Ernandes Rocha de Oliveira pelas aulas de Latex.

RESUMO

O presente trabalho tem o objetivo de propor ao professor de Matemática uma nova maneira de abordar alguns conteúdos na Educação Básica e tratá-los como consequência do Algoritmo da Divisão de Euclides, bem como propormos uma reflexão sobre a postura de sua docência em relação a esse tópico e também em relação a bagagem matemática para o exercício da docência. Por fim, propomos alguns conteúdos estudados em qualquer curso de Aritmética, alguns resultados importantes e exercícios de aplicação.

Palavras-chave: Algoritmo da Divisão de Euclides, Conjunto dos Inteiros, Aritmética Modular.

ABSTRACT

This paper aims to propose to the mathematics of teacher a new way to approach some content in Basic Education and treat them as a consequence of Euclid Division Algorithm and propose a reflection on the position of his teaching regarding this topic and also in relation to mathematics luggage to the exercise of teaching . Finally , proposed some content studied in any course of Arithmetic, some important results and practical exercises.

Keywords: *Euclidean Algorithm, Integer Sets, Modular Arithmetic.*

Sumário

Capítulo 1

INTRODUÇÃO

Pretendemos com este trabalho propor uma nova maneira de abordar alguns tópicos da Educacão Básica, como consequência do Algoritmo de Euclides. Sabemos que este material não será ensinado com o grau de profundidade no qual estamos expondo.

Na Educação Básica, no Ensino Fundamental, aplicamos o Algoritmo de Euclides quando lidamos com os números naturais e com os números inteiros. Muitas vezes, o aluno nem seguer consegue diferenciar entre os números naturais e os inteiros. Talvez porque a noção de conjuntos não tenha sido abordada de forma clara. Então precisamos saber como caracterizar $\mathbb{N}$ e $\mathbb{Z}$ como conjuntos. Não apenas isto, mas os professores também precisam entender como se deu o processo de construção de $\mathbb{N}$ de forma axiomática.

Porém, temos como meta despertar no docente da Educacão Básica reflexões a respeito de como ele ensina este tópico. Mostrar a aplicação da divisão Euclidiana em outros tópicos da Matemática da Educação Básica. Além disto, uma reflexão com respeito à sua bagagem matemática para o exercício da docência e também estimular uma reflexão com respeito à sua formação em Matemática com o intuito de promover uma formação que contribua para sua prática docente.

Neste último caso, dentro da concepção do Programa de Pós Graduação - PROFMAT, pretendemos com esta dissertação auxiliar o professor no ensino deste tópico que por vezes passa de forma despercebida por parte dos alunos pela forma que é abordado, sem despertar o interesse pelo seu real alcance.

De acordo com os Parâmetros Curriculares Nacionais de Matemática do Ensino Fun-

damental dos 3º e 4º ciclos (dos 6º ao 9º anos), o estudo da Matemática deve partir do conhecimento prévio dos alunos e utilizar a Resolução de Problemas como ponto de partida da atividade matemática.

Ainda de acordo com esse documento, o aluno deve ser protagonista do processo ensino-aprendizagem e o professor deve partir da Resolução de Problemas e utilizar recursos como História da Matemática, utilização de Jogos e uso de Tecnologias da Comunicação e Informação em suas aulas.

Dentro do processo ensino-aprendizagem o professor tem as funções de organizar, facilitar, mediar, incentivar e avaliar a aprendizagem.

Os conteúdos matemáticos, de acordo como os PCNs, são organizados em quatro blocos:

1º) Números e Operações: neste bloco são trabalhados os conteúdos de Aritmética e Álgebra.

2º)Espaço e Forma: são trabalhados neste bloco os conceitos de geometria.

3º)Grandezas e Medidas: são estudados grandezas envolvidas na matemática e ciências tais como: comprimento, massa, tempo, capacidade, temperatura, velocidade, energia elétrica, densidade demográfica e outras.

4º) Tratamento de informação: são trabalhados dados estatísticos, análise de gráficos e tabelas, bem como o Estudo da probabilidade e problemas de contagem.

Mas de acordo com o trabalho que estamos propondo, vamos nos aprofundar mais no eixo de números e operações.

Neste trabalho também abordaremos uma ferramenta muito importante em algumas demonstrações matemáticas, que é o Princípio da Indução Finita, no qual deixaremos bem claro quando a mesma é válida.

No decorrer deste nosso Trabalho vamos efetuar a resolução de alguns problemas em determinados capítulos e que poderão ser retomados posteriormente, mas utilizando outras ferramentas na sua resolução, dando ao leitor deste trabalho várias ferramentas para resolver problemas.

Capítulo 2

Construção Axiomática dos Números Naturais

Com o desenvolvimento da humanidade houve por parte do homem a necessidade de desenvolver a noção de número de forma mais sofisticada, dentre elas propor novas técnicas de contagem e como registrá-las. Foi uma evolução lenta e demandou um tempo considerável. Apenas no final do século XIX, quando boa parte dos fundamentos da Matemática foram questionados e revistos, é que a noção de número passou a ser baseada na teoria de conjuntos como a conhecemos nos dias de hoje.

Em particular, um modelo abstrato para contagem é dado pelos números naturais e que denotamos por $\mathbb{N}$, o qual trata-se do primeiro conjunto que temos contato na escola.

2.0.1 Axiomas de Peano e o Princípio da Indução Finita

Na forma que conhecemos nos dias de hoje, o conjunto dos números naturais $\mathbb{N}$, o rigor matemático empregado no seu tratamento se deu apenas no ínicio de século XX de forma axiomática e foi proposto pelo matemático italiano Giuseppe Peano através de quatro axiomas que se tornaram conhecidos por Axiomas de Peano, que descrevemos a seguir:

1) Todo número natural tem um único sucessor.

2) Números naturais diferentes, têm sucessores diferentes.

3) Existe um único número natural, que é o um (1) e ele não é sucessor de algum outro natural.

4) Sendo X um conjunto de números ($X \subset \mathbb{N}$), se $1 \in X$ e se para todo elemento $x \in X$ implicar que o seu sucessor, $x + 1 \in X$. Então, $X = \mathbb{N}$.

O Axioma 4 é conhecido também por Axioma de Indução, e aparece na demonstração de problemas que recaiam em indução ou recorrência. Pode ser reformulado da seguinte forma:

Princípio da Indução Finita: Consideremos a propriedade relativa ao número natural n.

Suponhamos que:

(i) $P(1)$ é válida.

(ii) $\forall n \in \mathbb{N}$ a validez de $P(n)$ implica na validez de $P(n+1)$, onde $n+1$ é o sucessor de n.

Uma consequência direta dos Axiomas de Peano, é de que por meio dele percebemos que o processo de construção do Conjunto dos Números Naturais está intimamente ligado ao conceito de sucessor de um número.

Tal conceito também está associado à propriedade de ordem dos números naturais que ensinamos na escola, que denominamos como números ordinais, ou seja, em $\mathbb{N}$ segue uma ordem: o número um (1) é o primeiro, o número dois (2) é segundo, o número três (3) é o terceiro e assim por diante.

2.1 Aplicações do Princípio da Indução Finita

O Princípio da Indução Finita é um eficiente método que auxilia na demonstração de diversos problemas matemáticos.

No sentido de ilustrar sua importância, nesta seção discutiremos a formalização matemática de um jogo muito famoso, conhecido como "Torre de Hanói".

2.1.1 A Torre de Hanói

No jogo da Torre de Hanói há três hastes. Na primeira haste há uma certa quantidade de discos inseridos com tamanhos diferentes, dispostos de tal forma que os discos maiores estão na posição mais baixa e os menores na posição mais altas. A regra do jogo consiste em mover todos os discos para a última haste, de tal maneira, que nenhum disco maior fique sobre um disco menor. Logo, torna-se óbvio que a haste central será um intermediário para encontrarmos a solução do problema em questão. O interessante neste jogo não é apenas completá-lo, mas conseguir finalizá-lo realizando o menor número de movimentos possíveis. No intuito de poder calcular este número de movimentos, chamaremos de $T(n)$ a quantidade mínima de movimentos necessários para movermos todos os discos da primeira haste para a última. Chamamos a atenção que o problema estará resolvido de forma completa somente quando este valor for calculado. A primeira meta a ser realizada é de mover a maior peça para a última haste, mas para conseguirmos teremos antes movido $n-1$ peças anteriores para a haste central, para isto teremos realizado $T(n-1)$ movimentos.

A próxima etapa a ser feita é de mover a peça n para a última haste, realizando mais um movimento e, por fim, movemos as $n-1$ peças da haste central para a última haste realizando mais $T(n-1)$ movimentos, desta forma, temos:

$$T(n) = T(n-1) + 1 + T(n-1) = 2T(n-1) + 1. \tag{2.1}$$

Assim, para calcularmos a quantidade de movimentos mínimos para determinada quantidade de discos basta saber a movimentação mínima, caso tivéssemos um disco a menos, como:

$$T(1) = 1,\ \ T(2) = 3,\ \ T(3) = 7,\ \ T(4) = 15,\ \ T(5) = 31,\ \ T(6) = 63, \ldots \tag{2.2}$$

Observamos antes que para os valores de $n = 1, 2, 3, 4, 5$ e 6 da Expressão dada em (2.1) obedece como lei de formação $T(n) = 2^n - 1$.

Uma consequência da forma em que está sendo atacado o problema é que precisamos realizar diversas vezes o mesmo procedimento para encontrarmos o resultado desejado,

trata-se de uma *fórmula de recorrência*. Em outras palavras, para saber a quantidade de movimentos $T(a)$ devemos saber anteriormente a quantidade de movimentos $T(a-1)$. Para saber a quantidade de movimentos de $T(a-1)$ devemos saber a quantidade de movimentos anteriores $T(a-2)$. Assim, realizando esse procedimento de forma sucessiva teremos de saber anteriormente as quantidades de movimentos $T(a-3), \ldots, T(1)$.

O que mostra ser um trabalho árduo quando realizado de forma manual. Claro que se analisarmos esse procedimento do ponto de vista computacional não chega a ser tão ruim. Basta executar um algoritmo simples em alguma plataforma computacional.

Porém, como o nosso enfoque é para o Ensino Médio seria interessante simplificar ainda mais os cálculos e encontrar a resposta deste problema de forma mais rápida do que a obtido até o presente momento. Para isso, utilizaremos o Princípio de Indução Finita que funcionará como um método para encontrarmos uma fórmula fechada para $T(n)$ e que seja válida para todo $n \in \mathbb{N}$.

Neste sentido, consideremos como P a propriedade dada por $T(n) = 2^n - 1$. Note que para $n = 1$ a propriedade T é válida já que $T(1) = 2^1 - 1 = 1$, o que mostra que a parte (i) da Propriedade de Indução é satisfeita.

Para provar a parte (ii) da Propriedade de Indução, assumamos válido para n a propriedade válida $T(n) = 2^n - 1$. Agora, verificamos o caso $n + 1$. Antes observe pela Equação 2.1 que podemos escrever $T(n+1) = 2T(n) + 1$. Mas, pela hipótese de indução, temos que $T(n) = 2^n - 1$. Logo, $T(n+1) = 2(2^n - 1) + 1 = 2^{n+1} - 2 + 1 = 2^{n+1} - 1$.

Portanto, $\forall n \in \mathbb{N}$ temos que para $T(n)$ válido implica que $T(n+1)$ também é válido. Sabe-se que $T(1) = 1$ e $2^1 - 1 = 1$, logo, a primeira condição foi satisfeita, para a segunda condição, considera-se $T(n) = 2^n - 1$ e deseja-se mostrar que $T(n+1) = 2^{n+1} - 1$.

Note que por meio do Princípio da Indução Finita obtemos uma fómula fechada para $T(n)$ para um número n de movimentos quaisquer do jogo.

$$T(n+1) = 2(2^n - 1) + 1 = 2^{n+1} - 2 + 1 = 2^{n+1} - 1.$$

Desta forma, está provado que a fórmula é verdadeira para qualquer $n \in \mathbb{N}$.

Agora vamos resolver a recorrência abaixo e determinar de outro modo a Fórmula

Fechada para $T(n)$ para um número n de movimentos quaisquer do jogo.

Demonstração. Agora vamos resolver a a recorrência $T(n) = 2T(n-1) + 1, T(1) = 1$

Solução da equação homogênea $T(n) = 2T(n-1) \rightarrow T(n) = 2^{n-1}$

Fazendo a susbstituição $T(n) = 2^{n-1}y_n$, temos:

$2^n y_{n+1} = 2^n y_n + 1 \rightarrow y_{n+1} = y_n + 2^{-n}$, então:

$$y_2 = y_1 + 2^{-1}$$

$$y_3 = y_2 + 2^{-2}$$

$$y_4 = y_3 + 2^{-3}$$

$$\vdots$$

$$y_n = y_{n-11} + 2^{-(n-1)}$$

Somando

$$y_n = y_1 + 2^{-1} + 2^{-2} + ... + 2^{-(n-1)}$$

$$y_n = y_1 + 1 - 2^{-(n-1)}.$$

Então:

$T(n) = 2^{(n-1)}(y_1 + 1 - 2^{-(n-1)}) \rightarrow T(n) = (1 + y_1).2^{n-1} - 1$

Mas, $T(1) = 1 \rightarrow T(n) = 2^{n-1}y_n \rightarrow y_1 = 1$.Logo:

$T(n) = 2.2^{n-1} - 1 \rightarrow T(n) = 2^n - 1.$ □

Observação 2.1.1. *De acordo com o Prof. Dr. Edson Donizete de Carvalho, meu professor e orientador no PROFMAT, um típico erro recorrente que se observa por parte dos alunos quando são cursadas as disciplinas de Teoria dos Números e Aritmética, tanto em nível de graduação quanto de pós-graduação (PROFMAT), é o uso inadequado do*

Princípio da Indução Finita, olhando o método apenas de forma mecânica, raciocinando da seguinte forma: desde que a propriedade seja válida para $n = 1$, então basta supor a propriedade válida para n e de alguma forma manipular a expressão para seja válida para $n+1$. Porém, o problema é de que muitas vezes tenta-se utilizar o método para valores de n assumindo valores seja em $\mathbb{Q}, \mathbb{R}$ ou em outros conjuntos. Ou seja, não ficou claro que esta propriedade $P(n)$ do Princípio da Indução Finita é uma maneira equivalente de enunciar o quarto axioma de Peano. É claro que em nível de Educação Básica/Ensino Médio, o professor não irá ensinar com este grau de formalismo. Porém, precisa estar claro que se trata de uma propriedade intríseca do Conjunto dos Números Naturais. Ou melhor, ao dizer que a propriedade é válida para todo $n \in \mathbb{N}$, estamos no fundo estabelecendo uma função $P : \mathbb{N} \to P(\mathbb{N})$, onde $P(\mathbb{N})$ é a imagem que essa função assume para cada valor no domínio em $\mathbb{N}$. Caso o domínio da propriedade P esteja definida em qualquer conjunto numérico diferente de $\mathbb{N}$ então esse método não pode ser aplicado. Necessita-se procurar outros métodos para resolver problemas desta natureza.

2.1.2 Números de Fermat

No exemplo da Torre de Hanói, verificamos que para os primeiros valores de $n \in \{1, 2, 3, 4, 5, 6\}$ que a propriedade T era dada por $T(n) = 2^n - 1$. Por meio do Princípio da Indução Finita conseguimos estabelecer a fórmula fechada para T. Porém, o método também é interessante para uma situação em que conhecemos para um número finito de valores de n e desejamos observar se a propriedade é válida para qualquer valor de n e também é útil para provar quando a propriedade não é válida para todo n em $\mathbb{N}$. Caso não conseguíssemos realizar a prova por Indução Finita, seríamos levados a desconfiar da validade da propriedade para qualquer valor de $n \in \mathbb{N}$ e assim procuraríamos o valor finito em que a propriedade não é satisfeita. Uma típica situação que podemos considerar para ilustrar essa observação são os *números de Fermat*.

Pierre de Fermat (1601-1665) observou que a expressão dada por $F_n = 2^{2^n} + 1$ fornecia números primos desde que $n = 0, 1, 2, 3$ e $n = 4$. Verificou que $F_0 = 2^{2^0} + 1 = 3$, $F_1 = 2^{2^1} + 1 = 5$, $F_2 = 2^{2^2} + 1 = 17$, $F_3 = 2^{2^3} + 1 = 257$, $F_4 = 2^{2^4} + 1 = 65537$,

O que levou Fermat a conjecturar que a expressão $F_n = 2^{2^n} + 1$ fornecia apenas números

primos em uma carta enviada a Mersenne. Caso esta conjectura fosse válida, teríamos uma fórmula geral para gerar números primos. Algo não obtido até os dias de hoje. Recentemente, os últimos maiores primos inteiros positivos encontrados foram obtidos por meio de sofisticados métodos computacionais, dada a complexidade de cálculos envolvidos. Coube a Euler (1707-1783), alguns anos após a conjectura de Fermat ser proposta, mostrar que, em particular, para valor próximo ao natural dado por $n = 5$ a propriedade de F_n ser um número primo era falsa. Mostrou que $F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 4294967297$.

Mas como Fermat cometeu um erro destes?

É bastante provável que a tentativa de prova fosse do tipo que delineou noutra área da sua obra teórica sobre números, o Método da Descida Infinita, e que simplesmente acreditasse que os métodos utilizados para inteiros positivos até 4 funcionasse para outros maiores.

Capítulo 3

Adição e Multiplicação nos Conjuntos dos Números Naturais e dos Inteiros

Neste capítulo vamos discutir as operações de adição e multiplicação em $\mathbb{N}$, já familiar aos professores, nas quais se estabelece que para quaisquer $a, b \in \mathbb{N}$ associa-se de maneira única um único elemento em $\mathbb{N}$ denotado por $a + b$ e um único elemento em $\mathbb{N}$ denotado por $a.b$ que chamamos de soma e produto, respectivamente.

3.1 Propriedades aritméticas da soma e do produto

As próximas propriedades que enunciaremos a seguir são bem familiares ao docente na Educação Básica, e como veremos estão bem definidas, estabelecendo a existência de elemento neutro para a operação de adição, as leis de distributividade da multiplicação em relação à adição, as leis do cancelamento, comutatividade e associativas. Por meio delas, obteremos diversas novas propriedades no conjunto dos números naturais e todas elas também são válidas para o conjunto dos números inteiros. Neste trabalho, optamos por assumir essas propriedades válidas em $\mathbb{N}$, de forma axiomática.

Propriedade 3.1.1. *A adição e a multiplicação são bem definidas, pois operando com dois números naturais temos como resultado sempre um número natural; em outras pala-*

vras dizemos que o Conjunto dos Números Naturais ($\mathbb{N}$) *é fechado em relação às operações de adição e multiplicação:*

$\forall a, b \in \mathbb{N}$, *se* $a = c$ *e* $b = d$ *então* $a + b = c + d$ *e* $a.c = b.d$.

Propriedade 3.1.2. $a + b = b + a$ *e* $a.b = b.a$, $\forall a, b \in \mathbb{N}$.

Propriedade 3.1.3. $(a + b) + c = a + (b + c)$ *e* $(a.b).c = a.(b.c)$, $\forall a, b, c \in \mathbb{N}$.

Propriedade 3.1.4. $a + 0 = a$ *e* $a.1 = a$, $\forall a \in \mathbb{N}$.

Propriedade 3.1.5. $a(b + c) = a.b + a.c$, $\forall a, b, c \in \mathbb{N}$.

Propriedade 3.1.6. *Dados* $\forall a, b \in \mathbb{N}$, *se* $a.b = 0$, *então* $a = 0$ *ou* $b = 0$.

Propriedade 3.1.7. *Dados* $a, b \in \mathbb{N}$, *temos que apenas uma destas possibilidades é verificada:*

(i) $a = b$;

(ii) $a < b$;

(iii) $a > b$.

Estas sete propriedades constituem os pilares da aritmética em $\mathbb{N}$. Note que a propriedade (3.1.1) garante que podemos somar e multiplicar ambos os lados de uma igualdade por um mesmo número. A propriedade (3.1.2) garante que a adição e a multiplicação em $\mathbb{N}$ são operações comutativas. Enquanto, que a propriedade (3.1.3) assegura que a soma e o produto são associativas em $\mathbb{N}$. Já a propriedade (3.1.4) estabelece a existência de um elemento neutro tanto para a soma quanto para o produto. A propriedade (3.1.5) garante a distributividade da multiplicação em relação à adição. A propriedade (3.1.6) é conhecida como integridade assegura que caso o produto de números em $\mathbb{N}$ seja nulo, então ao menos um destes números é nulo. A propriedade (3.1.7) conhecida como Tricotomia estabelece uma relação de ordem em $\mathbb{N}$, ou seja, assegura que podemos comparar dois elementos em $\mathbb{N}$. A primeira possibilidade é a igualdade entre a e b. A segunda possibilidade é a qual em que dizemos que a *é menor do que* b e denotamos por $a < b$. Já a terceira possibilidade é aquela em que dizemos que a *é maior do que* b e denotamos por

$a > b$. Embora não seja foco desta Dissertação, convém observar que a relação de ordem é uma propriedade intrínseca do conjunto dos números reais ($\mathbb{R}$) e de seus subconjuntos, em particular, $\mathbb{N}$.

A partir destas sete propriedades assumidas de forma axiomática, demonstraremos várias propriedades aritméticas com relação à adição e à multiplicação, válidas em $\mathbb{N}$.

Proposição 3.1.1. $a.0 = 0 \ \ \forall a \in \mathbb{N}$.

Demonstração. :

Repare que $\forall a \in \mathbb{N}$, pela propriedade (3.1.5) que refere-se a distributividade da multiplicação em relação à adição, obtemos que $a.0 = a(0 + 0) = a.0 + a.0$. Caso, $a.0 \neq 0$, teríamos que $a.0 \in \mathbb{N}^*$. Assim, concluímos como consequência da igualdade acima que $a.0 > a.0$, o que contradiz a propriedade da tricotomia.Logo, a.0=0. □

Proposição 3.1.2. $\forall a, b, c \in \mathbb{N}, a < b$ *e* $b < c$. *Então,* $a < c$.

Demonstração. :

Seja $a, b \in \mathbb{N}$ tal que $a < b$ e $b < c$. Então, pela pela parte (ii) da Propriedade da Tricotomia, temos que existem d e f em $\mathbb{N}$ não simultaneamente nulos tais que $b = a + d$ e $c = b + f$. Assim, como consequência da propriedade associativa, segue-se que

$$c = b + f = (a + d) + f = a + (d + f),$$

Como $d + f$ é um natural não nulo, implica que $a < c$. □

A proposição acima estabelece que a "relação menor do que"é transitiva.

Proposição 3.1.3. $\forall a, b, c \in \mathbb{N}, a < b$ *, se, e somente se,* $a + c < b + c$.

Demonstração. Seja $a, b \in \mathbb{N}$ tal que $a < c$. Então, existe d em $\mathbb{N}$ não nulo tal que $b = a+d$. Somando c a ambos lados da igualdade que é garantida pela Propriedade (3.1.1). Em seguida, aplicando as propriedades associativa e comutativa da adição, obtemos:

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

O que implica que $a + c < b + c$.

Reciprocamente, suponhamos que $a + c < b + c$. Agora, dados $a, b \in \mathbb{N}$, pela Propriedade da Tricotomia temos três possibilidades para a e b. A primeira possibilidade é que $a = b$. Ao somarmos c aos dois lados da igualdade, obtemos $a + c = b + c$, contrariando a nossa hipótese.

A segunda possibilidade seria $b < a$, e caso utilizássemos a primeira parte da demonstração, concluiríamos que $b + c < a + c$, o que também contraria a hipótese.

Logo, resta como possibilidade que: $a < b$. □

A proposição anterior estabelece que a adição é compatível e cancelativa em relação à desigualdade "menor do que"

Proposição 3.1.4. $\forall a, b, c \in \mathbb{N}$ *com* c *não nulo, temos que* $a < b$ *, se e somente se,* $a.c < b.c$.

Demonstração. :

Seja $a, b \in \mathbb{N}$ tal que $a < b$. Então, existe d em $\mathbb{N}$ não nulo tal que $b = a + d$. Multiplicando c a ambos lados da igualdade que é garantida pela Propriedade (3.1.1). Em seguida, aplicando as propriedades comutativa e associativa da adição, obtemos:

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

O que implica que $a.c < b.c$. Já que pela integridade, temos que $c.d \in \mathbb{N}$ é não nulo.

Reciprocamente, suponhamos que $a.c < b.c$. Agora, dado $a, b \in \mathbb{N}$. Pela Propriedade da Tricotomia, temos três possibilidades para a e b. A primeira possibilidade é que $a = b$. Ao multiplicarmos c dos dois lados da igualdade, obtemos $a.c = b.c$ contrariando a nossa hipótese.

A segunda possibilidade seria $b < a$, e caso utilizemos a primeira parte da demonstração, concluiremos que $b.c < a.c$, o que também contraria a hipótese.

Logo, sobrou como possibilidade que $a < b$. □

A proposição anterior estabelece que a multiplicação é compatível e cancelativa em relação a desigualdade "menor do que".

Proposição 3.1.5. $\forall a, b, c \in \mathbb{N}$ *temos que* $a = b$*, se, e somente se,* $a + c = b + c$.

Demonstração. :

Seja $a, b \in \mathbb{N}$ tal que $a = b$. Como $c = c$ da Propriedade (3.1.1), segue-se da Proposição (3.1.1) que $a + c = b + c$.

Reciprocramente, suponhamos que $a + c = b + c$. Pela Propriedade da Tricotomia, temos três possibidades para a e b. A primeira possibilidade seria $a < b$, pela Proposição 3.1.3, concluiremos que $a + c < b + c$, o que contraria a hipótese.

A segunda possibilidade seria $b < a$, pela Proposição 3.1.3, concluiremos que $b + c < a + c$, o que também contraria a hipótese.

Logo, sobrou como possibilidade que $a = b$. □

A proposição anterior estabelece que a adição é cancelativa em relação à igualdade.

Proposição 3.1.6. $\forall a, b, c \in \mathbb{N}$ *com* c *não nulo, temos que* $a = b$*, se, e somente se:* $a.c = b.c$.

Demonstração. :

Seja $a, b \in \mathbb{N}$ tal que $a = b$. Como $c = c$ da Propriedade (3.1.1), segue-se da Proposição (3.1.1), que $a.c = b.c$.

Reciprocamente, suponhamos que $a.c = b.c$. Pela Propriedade da Tricotomia, temos três possibidades para a e b. A primeira possibilidade seria $a < b$, e segue que $a.c < b.c$, o que contraria a hipótese.

A segunda possibilidade seria $b < a$, daí $b.c < a.c$, o que também contraria a hipótese.

Logo, sobrou como possibilidade que $a = b$. □

A proposição anterior estabelece que a multiplicação é cancelativa em relação à igualdade.

A relação $<$ (menor do que) não é uma relação de ordem, de fato não é reflexiva e nem antissimétrica.

A subtração em $\mathbb{N}$, ao contrário da adição, não é tão natural ao aluno na escola, nos primeiros anos da Educação Básica. Como veremos a seguir, esta operação não está definida para dois elementos quaisquer em $\mathbb{N}$.

Neste sentido, sejam a e b dois números naturais, e definimos o número b menos a, denotado por $b - a$, como sendo o número c; equivalentemente, $c = b - a$. Assim, o número

natural c é o resultado da subtração a e de b. Satisfazendo a condição de que $a < b$ ou $a = b$. Na primeira situação, temos que existe $c \in \mathbb{N}$ tal que $b = a + c$. Definimos o número c como sendo $b - a$ e denotamos c por $b - a$, equivalentemente, $c = b - a$. Quanto à segunda possiblidade, temos que existe $0 \in \mathbb{N}$ tal que $b = a + 0$. Definimos o número 0 como sendo $b - a$ e denotamos 0 por $b - a$, equivalentemente, $0 = b - a$.

3.2 As Estruturas Algébricas nos Conjuntos dos Números Naturais e dos Inteiros

O enfoque central deste trabalho é o de discutirmos aritmética em $\mathbb{N}$. Porém, com o intuito de discutirmos algumas limitações em termos de propriedades aritméticas no conjunto dos naturais ($\mathbb{N}$), compararemos com o conjunto dos números inteiros ($\mathbb{Z}$).

Apenas chamamos a atenção de que o conjunto dos números naturais pode ser obtido a partir de $\mathbb{N}$. Para uma maior compreensão do que mencionamos, definiremos a seguir o que vem a ser uma relação de equivalência.

Dado um conjunto X não vazio, uma relação de equivalência em um conjunto X é uma relação que denotamos por $\sim$ e que satisfaz às propriedades a seguir:

1. $\forall a \in X; a \sim a$ (Reflexiva).

2. $\forall a, b \in X; a \sim b$. Então, $b \sim a$ (Simetria).

3. $\forall a, b, c \in X; a \sim b$ e $b \sim c$. Então, $a \sim c$ (Transitiva).

O subconjunto dos elementos $x \in X$ tais que $x \sim a$, onde $a \in X$ é chamado de classe de equivalência e é denotado por:

$$[a] = \{x \in X; x \sim a\}.$$

Um importante fato é que uma relação de equivalência particiona o conjunto X em classes de equivalência, isto é, podemos obter o conjunto X como sendo a união destas classes de equivalência onde a interseção destas classes de equivalência é vazia.

Richard Dedekind (1831-1916) mostrou que a relação definida pelos pares ordenados (x, y) e (n, m) de números naturais são equivalentes segundo a relação dada por $x + m = y + n$ o que equivale a afirmar que:

$$x - y = n - m. \tag{3.1}$$

Porém, nem sempre a igualdade faz sentido no conjuntos dos números naturais. Por exemplo, para o par $(2, 7)$ em $\mathbb{N} \times \mathbb{N}$ dada por $2 - 7 = -5 \notin \mathbb{N}$.

Para melhor compreensão antes de mostrarmos que isto, de fato, é uma relação de equivalência.

Sabemos que em $\mathbb{N}$ é válido a propriedade comutativa, isto é, $x + y = y + x$. Mas, esta é a relação que estabelece que (x, y) é equivalente a (x, y), logo, a propriedade reflexiva é verificada.

Se $x + m = y + n$, então pela comutatividade válida em $\mathbb{N}$, temos que $y + n = x + m$. Em outras palavras, se (x, y) é equivalente a (n, m), então (n, m) é equivalente a (x, y). Isto é, vale a propriedade simétrica.

Finalmente, suponhamos que (x, y) seja equivalente a (n, m) e que (n, m) seja por sua vez equivalente a (s, t). Então: $x + m = y + n$ e $n + t = m + s$.

Assim, $(x + t) + m = x + (t + m)$
$= x + (m + t)$
$= (x + m) + t$
$= (y + n) + t$
$= y + (n + t)$
$= y + (m + s)$
$= y + (s + m)$
$= (y + s) + m.$

Agora, desde que $(x + t) + m = (y + s) + m$, pela propriedade de adição em $\mathbb{N}$, temos que $x + t = y + s$, ou seja, (x, y) é equivalente a (s, t). Logo, pela propriedade transitiva, isto está provado.

O conjunto dos inteiros $\mathbb{Z}$ assim definido é formado pelas classes de equivalências de pares ordenados de números naturais. Representamos a classe que contém (a, b) por $a - b$.

Definimos a adição e a multiplicação da seguinte forma:

$$[(a,b)] + [(c,d)] = [(a+c, b+d)];$$

$$[(a,b).(c,d)] = [(ac+bd, ad+bc)],$$

onde $[(a,b)]$ denota a classe de equivalência que contém (a,b).

Aprendemos na escola que o conjunto do naturais $\mathbb{N}$ é um subconjunto do conjunto dos inteiros $\mathbb{Z}$. A questão natural que aparece via essa abordagem é como é escrito $\mathbb{N}$ por meio dessa relação de equivalência. Para melhor ilustrar estes conceitos, temos por exemplo que a classe que representa o número inteiro 3 é dada por:

$$[3,0] = \{\ldots, (-1,-4), (0,-3), (3,0), (4,1), (5,2), \ldots\},$$

já que:

$$3 = \ldots = 3-0 = 4-1 = 5-2 = \ldots. \tag{3.2}$$

O número natural $n \in \mathbb{N}$ pode ser visto como o representante da classe $[(n,0)]$. Similarmente, podemos listar todos os números inteiros na seguinte forma:

$$\ldots [(0,3)], [(0,2)], [(0,1)], [(0,0)], [(1,0)], [(2,0)], [(3,0)]. \ldots$$

Novamente, convém chamarmos a atenção de que o professor no Educação Básica/Ensino Médio não ensina que o conjunto $\mathbb{Z}$ seja obtido como uma relação de $\mathbb{N} \times \mathbb{N}$. Porém, há a necessidade de que esteja claro que o número inteiro n é na verdade uma classe de equivalência. Como regra, consideremos o representante em $\mathbb{Z} \times \mathbb{Z}$ dado por $(n,0)$.

Apenas como exemplo, fica claro que o número 3 representa a classe de de equivalência como dada pela Expressão 3.2. Os elementos desta classe preservam a propriedade de que a diferença entre eles seja igual a 3.

3.2.1 Grupos

Vimos que as operações de adição e multiplicação estão bem definidas em $\mathbb{N}$, isto é, dados $a, b \in \mathbb{N}$, tem-se que $a+b$ e $a.b \in \mathbb{N}$. Porém, a subtração de dois números

$a, b \in \mathbb{N}$ é apenas estabelecida quando $a \leq b$. Na seção anterior, vimos que o conjunto $\mathbb{Z}$ é obtido via relação de equivalência a partir de $\mathbb{N}$. Como vimos agora há pouco, segundo a relação de equivalência em $\mathbb{N}$, o número inteiro $3 = (-1, -4) = (0, -3) = (3, 0)$. Isto é, $3 = -1 - (-4) = 0 - (-3) = 3 - 0$. Porém, para que a expressão faça sentido, temos que $-1 - (-4) = -1 + 4 = 0 - (-3)$, ou melhor, precisamos ter $-(-4) = 4$ e $-(-3) = 3$. Comumente, na escola diz-se ao aluno a regra de que "menos vezes menos é mais". Aqui obviamente surge algum incômodo ao aluno, mas por quê? Certamente, começa a sensação que a Matemática é chata e tem um conjunto de regras sem sentido. O que leva o aluno a decorar e começar a odiar a Matemática.

Neste sentido de esclarecer e discutir as primeiras diferenças entre $\mathbb{N}$ e $\mathbb{Z}$ segundo as operações de adição e multiplicação definidas até o presente momento, definiremos o conceito de grupo.

Seja G um conjunto não vazio, uma **operação binária** $*$ sobre um conjunto $G \neq \emptyset$ é uma aplicação fechada em G, ou seja, a cada par de elementos de $(a, b) \in G \times G$ corresponde um único elemento em G.

$$* : G \times G \to G$$

$$(a, b) \mapsto c = a * b \in G.$$

Caso a operação binária definida sobre G satisfaça:

- a propriedade de que $a * b = b * a$, $\forall a, b \in G$, então dizemos que a operação binária $*$ é **comutativa**,
- a propriedade de que $(a * b) * c = a * (b * c)$, $\forall a, b, c \in G$, então dizemos que a operação binária $*$ é **associativa**.

Em particular, caso tomemos $G = \mathbb{N}$ ou $\mathbb{Z}$ e a operação binária dada pela adição $+$, temos que $\mathbb{N}$ tanto $\mathbb{Z}$ quanto a operação $+$ e . multiplicativa é comutativa e associativa.

Na Definição 3.2.1 veremos quando um conjunto G não vazio munido de uma operação binária é um grupo.

Definição 3.2.1. *Um conjunto $G \neq \emptyset$ com uma operação binária $*$ definida sobre G é um **grupo**, cuja notação é dada por $(G, *)$, se as seguintes propriedades são verificadas:*

(i) *A operação $*$ é associativa em G;*

(ii) *A existência de um elemento neutro para a operação em G, isto é, $g * e = e * g = g$, para todo $g \in G$;*

(iii) *A existência de um elemento inverso para cada elemento em G, isto é, $\forall g \in G$ existe um elemento $g' \in G$ tal que $g * g' = e = g' * g$.*

Desde que a operação binária $*$ definida no grupo G seja comutativa, diremos que o grupo G é **abeliano** (ou comutativo). Continuamos a nossa comparação entre $\mathbb{N}$ e $\mathbb{Z}$, primeiro com relação à operação de adição. Note que caso $\mathbb{N}$ fosse um grupo segundo a operação de adição, as propriedades (i),(ii) e (iii) deveriam ser verificadas. Quanto à propriedade (i) já vimos que é verificada. Já quanto à propriedade (ii), temos que 0 é o elemento neutro para a soma em $\mathbb{N}$. Parece ser um grupo, mas quando verificamos a propriedade (iii), notamos que os elementos não nulos em $\mathbb{N}$ da forma x não possuem inversos aditivos em $\mathbb{N}$. Apenas para ilustrar, ao tomarmos $2 \in \mathbb{N}$, qual é o valor de $x \in \mathbb{N}$ tal que $2 + x = 0$? Certamente, se perguntarmos a um aluno no Ensino Fundamental, o mesmo dirá $x = -2$. Mas, $-2 \notin \mathbb{N}$.

Porém, caso consideremos os inteiros $\mathbb{Z}$, segundo a operação aditiva, verifica-se facilmente que $\mathbb{Z}$ é um grupo.

Dado x um inteiro positivo não nulo. Logo, o oposto aditivo é dado por $-x$, já que $x + (-x) = 0$. Caso y seja um inteiro negativo, logo, $-y$ é o seu oposto aditivo, já que $y + (-y) = 0$. Por exemplo, o oposto aditivo de 4 em $\mathbb{Z}$ é -4, já que $4 + (-4) = 0$. O oposto aditivo de -4 em $\mathbb{Z}$ é $-(-4)$, que acabamos denotando por 4, já que $-4 + 4 = 0$. Agora analisemos se $\mathbb{N}$ e $\mathbb{Z}$ são grupos segundo a operação multiplicativa. Repare que tanto $\mathbb{N}$ quanto $\mathbb{Z}$ satisfazem às propriedades (i) e (ii).

Nos dois casos o elemento neutro com relação a multiplicação é 1. Com relação à propriedade (iii), note que nos dois casos o número 0 não tem inverso.

Logo, poderíamos especular se os conjuntos $\mathbb{N}^* = \{x \in \mathbb{N}; x \neq 0\}$ e $\mathbb{Z}^* = \{x \in \mathbb{Z}; x \neq 0\}$ satisfazem à propriedade (iii). Para isto, se x for um número inteiro não nulo, deve haver um elemento x^{-1}, o inverso em $\mathbb{Z}^*$ tal que para $x.x^{-1} = 1$, mas isso significa que $x^{-1} = \frac{1}{x} \in \mathbb{Z}^*$.

No sentido de fornecer uma maior compreensão do problema, caso tomássemos $x = 4$, teríamos que $\frac{1}{x} = \frac{1}{4} \in \mathbb{Z}^*$, já que $4.\frac{1}{4} = 1$.

A mesma situação se repete para o conjunto $\mathbb{N}^*$ segundo a operação multiplicativa.

Nesta mesma seção vimos que o conjunto dos $\mathbb{N}$ segundo a operação aditiva satisfaz às duas primeiras propriedades (i) e (ii) de um grupo. No entanto, a propriedade (iii) não é satisfeita. Porém, vimos que o conjunto dos inteiros ($\mathbb{Z}$), obtido como uma classe de equivalência a partir da relação de equivalência em $\mathbb{N}$ constitui um grupo segundo a operação de adição.

Nesta mesma vertente, poderíamos especular se não poderíamos obter um conjunto que contenha os inteiros postivos $\mathbb{Z}^*$ e satisfaça à condição de ser um grupo multiplicativo.

Logo, pensaríamos no Conjunto dos Números Racionais $\mathbb{Q} = \{\frac{m}{n}; m, n \in \mathbb{Z}$, onde $n \neq 0\}$, que aprendemos na escola e onde sabemos que as operações de adição e multiplicação estão bem definidas, isto é, dados $a, b \in \mathbb{Q}$, temos que $a + b$ e $a.b \in \mathbb{Q}$.

Verifica-se facilmente que $\mathbb{Q}$ é um grupo segundo a operação de adição; e que caso consideremos o conjunto dos racionais não nulos $\mathbb{Q}^*$, este é um grupo segundo a operação multiplicativa (e, como vimos na escola, contém $\mathbb{Z}$), continuando a comparação que realizamos entre $\mathbb{N}$ e $\mathbb{Z}$.

Chamamos atenção que os números racionais também podem ser formados e definidos como classes de equivalências a partir de $\mathbb{Z} \times \mathbb{Z}^*$, como pares ordenados do tipo (m, n), onde m e n são inteiros, porém, com a restrição de que $n \neq 0$. Sem muita dificuldade, mostra-se que na relação definida por $(m_1, n_1) \simeq (m_2, n_2)$, se, e somente se: $m_1 n_2 = m_2 n_1$, define-se uma relação de equivalência.

Exemplo 3.2.1. *Note que* $(1, 2) \simeq (2, 4)$*, já que* $1.4 = 2.2$*. Na linguagem da Educação Básica denotamos os elementos* $(1, 2)$ *e* $(2, 4)$ *por* $\frac{1}{2}$ *e* $\frac{2}{4}$*, respectivamente.*

Comumente, imagina-se que $\frac{2}{4}$ seja igual a $\frac{1}{2}$, porque podemos "cortar em cima e em baixo por 2". Note que a relação $1.4 = 2.2$ é verificada, pois caso apliquemos a Proposição 3.1.6 obtemos $1.2 = 1.2$. Por este motivo é que se denota na Educação Básica $\frac{2}{4} = \frac{1}{2}$, pois estão na mesma classe de equivalência. Na verdade todos os pares de $\mathbb{Z} \times \mathbb{Z}^*$ dados por:

$$\{\ldots, -\frac{3}{6}, -\frac{2}{4}, -\frac{1}{2}, \frac{1}{2}, \frac{2}{4}, \frac{3}{6}, \ldots\}$$

estão na mesma classe de equivalência de $\frac{1}{2}$.

Ao denotarmos por $\frac{1}{2}$ estamos escrevendo o representante da classe acima.

Finalmente, chamamos a atenção de que nos cursos de Análise Matemática os números reais também são construídos via números racionais por meio de completamentos, segundo as sequências de Cauchy ou cortes de Dedekind.

3.3 Divisibilidade

Na seção anterior, vimos que tanto o conjunto dos inteiros $\mathbb{Z}$ quanto o conjunto dos inteiros não nulos $\mathbb{Z}^*$ não tem uma estrutura de grupo multiplicativo. Vimos que para que o inteiro x não nulo pudesse admitir um inverso multiplicativo, obrigatoriamente, precisaria ter-se que $x^{-1} = \frac{1}{x} \in \mathbb{Z}$, ou melhor, como dizemos na escola que x divide 1. Na escola aprendemos que em $\mathbb{Z}$ apenas para $x = 1$ ou $x = -1$, verifica-se tal condição.

Esta seção é dedicada à divisiblidade em $\mathbb{N}$ e em $\mathbb{Z}$. Caso continuássemos a fazer a mesma especulação como fizemos anteriormente, poderíamos nos indagar se esta é uma operação fechada em $\mathbb{N}$ como acontece quanto à adição e à multiplicação. Antes, no entanto, faremos uma exposição mais formal da definição de divisibilidade em $\mathbb{N}$.

Definição 3.3.1. *Dados a e $b \in \mathbb{N}$ com a restrição de que $a \leq b$. Dizemos que a divide b, se, e somente se, existe $k \in \mathbb{N}$ tal que: $b = a.k$. Também é comum afirmarmos neste caso que a é divisor de b ou ainda que b é múltiplo de a. A notação comum para denotar isso é $a|b$.*

Exemplo 3.3.1.

(1) $5|20$, já que existe $4 \in \mathbb{N}$ tal que $20 = 5.4$.

(2) $7|14$, já que existe $2 \in \mathbb{N}$ tal que $14 = 7.2$

(3) $4|12$, já que existe $3 \in \mathbb{N}$ tal que $12 = 4.3$

(4) $2 \nmid 9$, pois não existe $k \in \mathbb{N}$ tal que $9 = 2.k$

(5) $3 \nmid 8$, pois não existe $k \in \mathbb{N}$ tal que $8 = 3.k$

Exemplo 3.3.2. *Para todo n natural e $n \geq 1$, temos que $8 \mid 3^{2n} - 1$.*

Demonstração. Para efetuar a demonstração do exemplo acima vamos utilizar o Princípio da Indução Finita.

Primeiramente vamos mostrar que a sentença acima é válida para $n = 1$. Temos que $3^{2.1} - 1 = 9 - 1 = 8$ e $8 \mid 8$, logo a sentença é válida para $n = 1$.

Agora vamos supor que a sentença acima seja válida para n e devemos demonstrar que também seja válida para $n + 1$.

Para facilitar a segunda parte da demonstração, vamos reescrever a sentença acima.

$3^{2n} - 1 = 8k$, com $k \in \mathbb{N}$, multiplicando ambos os membros da expressão acima, por 3^2, temos:

$3^2.3^{2n} - 1.3^2 = 8.k.3^2 \Longrightarrow 3^{2n+2} - 1 = 72k + 8 \Longrightarrow 3^{2(n+1)} - 1 = 8.(9k + 1)$, fazendo $t = 9k + 1$, temos:

$3^{2(n+1)} - 1 = 8.t$, com $t \in \mathbb{N}$, ou seja, $8 \mid 3^{2n} - 1$.

Logo, a sentença é válida para $n + 1$.

Portanto, a sentença $8 \mid 3^{2n} - 1$ é válida para todo número natural n e $n \geq 1$. □

Notemos que a divisibilidade não está definida em $\mathbb{N}$ para quaisquer dois pares de elementos de $\mathbb{N}$, como pode ser verificado pelo itens (4) e (5) do exemplo citado. O mesmo vale também em $\mathbb{Z}$.

Embora, não seja possível aqui realizar uma discussão em termos de grupos com relação à divisibidade, seja em $\mathbb{N}$ quanto em $\mathbb{Z}$, mesmo assim, temos importantes propriedades aritméticas que podem ser observadas como listaremos na sequência.

Propriedade 3.3.1. *$a|a, \forall a \in \mathbb{N}$.(Reflexiva)*

Demonstração. De fato, pois existe $1 \in \mathbb{N}$ tal que $a = 1.a$ □

Propriedade 3.3.2. *Dados $a, b \in \mathbb{N}$ tal que $a|b$ e $b|a$, então $a = b$. (Antissimétrica)*

Demonstração. De fato, se $b = a.k_1$ e $a = b.k_2$, então $b = b(k_1.k_2)$.

Analisaremos as situações em $b = 0$ e $b \neq 0$. Para caso $b = 0$, como $a = b.k_1$, então $a = 0$. Por outro lado, se $b \neq 0$, concluímos que $k_1.k_2 = 1$, ou seja, que $k_1 = k_2 = 1$. Portanto, $a = b$. □

Propriedade 3.3.3. *Dados a, b e $c \in \mathbb{N}$ tal que se $a|b$ e $b|c$, então $a|c$. (Transitiva)*

Demonstração. Se $a|b$ e $b|c$, então existem $k_1, k_2 \in \mathbb{N}$ tal que $b = a.k_1$ e $c = b.k_2$. Logo, c pode ser reescrito na forma $c = a.(k_1k_2)$, o que mostra que $a|c$. □

Propriedade 3.3.4. *Se $a|b$ e $c \neq 0$, então $a.c|b.c$.*

Demonstração. De fato, se $a|b$, então existe $k \in \mathbb{N}$ tal que $b = a.k$. Logo, temos que $b.c = (a.c).k$. Portanto,$a.c|b.c$. □

Propriedade 3.3.5. *Se $a.c|b.c$ e $c \neq 0$, então $a|b$.*

Demonstração. Por hipótese, temos que $b.c = k.a.c$ para algum $k \in \mathbb{N}$, como $c \neq 0$, podemos dividir ambos os lados da igualdade acima por c, resultando na igualdade $b = k.a$. Portanto, $a|b$. □

Propriedade 3.3.6. *Se $a|b$ e $a|c$, então $a|(b + c)$.*

Demonstração. Por hipótese, temos que $b = a.k_1$ e $c = a.k_2$, para algum $k_1, k_2 \in \mathbb{N}$. Somando as duas equações acima, temos: $b + c = a.(k_1 + k_2)$. Portanto, $a|(b + c)$. □

Capítulo 4

Algoritmo da Divisão Euclidiana

No capítulo 3, definimos formalmente a divisibilidade tanto entre dois números naturais quanto entre dois números inteiros. A partir desta definição apresentamos diversas propriedades aritméticas que são ensinadas na Educação Básica.

Neste capítulo, o foco central é para os casos em que não seja satisfeita a divisibilidade entre números naturais ou entre números inteiros. Graças a estes casos, veremos ao longo desta dissertação diversas propriedades aritméticas e aplicações em diferentes áreas da Matemática, obtidas seja como consequência direta ou como consequência indireta do Algoritmo da Divisão de Euclides.

4.1 Algoritmo da Divisão de Euclides

Na Educação Básica, nos livros didáticos é comumente feita a afirmação de que na divisão entre dois números inteiros positivos, há duas possibilidades:

(i) A divisão é exata, ou seja, temos resto zero.

(ii) A divisão não é exata, temos um resto diferente de zero e necessariamente menor do que o divisor.

Estas duas possibilidades são consequências diretas do Algoritmo da Divisão Euclidiana que é citado no livro VII, proposições 1 e 2 dos Elementos.

Antes de apresentarmos o Algoritmo da Divisão de Euclides, enunciaremos o Princípio da Boa Ordem.

O Princípio da Boa Ordem

Todo Subconjunto não vazio dos Números Naturais possui um menor elemento.

Isto pode ser reescrito da seguinte forma:

Dado um conjunto $\mathbf{B} \subset \mathbb{N}$ não vazio, dizemos que b é o menor elemento de $\mathbf{B}$ se atender às seguintes propriedades listadas a seguir.

(i) $b \in \mathbf{B}$

(ii) $\forall x \in \mathbf{B}$, $b \leq x$

Convém observar que o menor elemento de $\mathbf{B}$ é único, e caso tenhamos b e x como menores elementos de $\mathbf{B}$, temos $b \leq x$ e $x \leq b$, ou seja, $b = x$.

Exemplo 4.1.1. *Sejam $a, b, n \in \mathbb{N}$ tal que $b > a$ e considere o conjunto S formado pelos elementos $b - an' \geq 0$ tal que $0 \leq n' \leq n$. Note que $S \neq \phi$, se $n = 0$, então $b \in S$ é único elemento de S. Assim, b é o menor elemento de S.*

Porém, se $n \neq 0$, então todo elemento da forma $b - an' \geq 0$ tal que $0 \leq n' \leq n$ pertence a S.

Repare que neste caso o Princípio da Boa Ordem garante que o conjunto

$$S = \{b, b - a, b - 2a, b - na, \ldots, b - an''\} \tag{4.1}$$

não tem infinitos elementos e que S tem um menor elemento na forma $b - an''$.

Teorema 4.1.1. *Sejam dois inteiros positivos a e b. Então, existem inteiros positivos q e r obtidos de forma única tais que:*

$$b = aq + r, \tag{4.2}$$

onde $0 \leq r < a$.

Demonstração. (Adaptação de COUTINHO, 2011, p.22-23)

Mostraremos de forma construtiva que existem elementos q e r com as propriedades requeridas pelo teorema. Sem perda de generalidade, vamos assumir que $b > a$ e consideremos o conjunto S como dado no Exemplo (4.1.1). Vimos no Exemplo (4.1.1) que S é diferente de vazio e tem ao menos o elemento $b \in S$. No conjunto S o último elemento satisfaz à condição de que o elemento $b - na < b$ e deve ser positivo, além de ter um menor elemento $b - an$" o qual denotaremos por $r = b - qa$, onde $q = n$". Mostraremos que $r < a$.

Caso $a|b$, então $r = 0$, e assim, para este caso, a prova está completa. Caso a não divida b, então $r \neq a$. Note que para completarmos a prova, basta mostrar que não pode ocorrer o caso $r > a$. Deste modo, supondo que $r > a$, logo existe $c \in \mathbb{N}$ tal que $r = c + a$, então $r = c + a = b - qa$, o que implica em que $c = b - (q + 1)a$. Mas note que $c \in \mathbb{N}$; logo, pela construção do conjunto S, temos que $c \in S$. Mas isto contradiz com o fato de r ser elemento mínimo de S, uma vez que $c < r$. Portanto, temos que $b = aq + r$ com $r < a$, o que mostra a existência de q e r.

Agora mostraremos a unicidade de q e r. Assim, sejam:

$b = aq + r$ e $0 \leq r < a$

e

$b = aq' + r'$ e $0 \leq r' < a$.

Vamos supor inicialmente, sem perda de generalidade, que $r \geq r'$. Subtraindo a primeira equação da segunda, obtemos:

$$r - r' = (b - aq) - (b - aq') = b - aq - b + aq' = aq' - aq = a(q' - q).$$

Lembrando que todas as vezes que efetuamos uma divisão o resto deve ser menor do que o divisor, então r e r' são menores que a. Supondo $r \geq r'$, devemos ter $0 \leq r - r' < a$. Comparando $r - r' = a(q' - q)$, teremos $0 \leq a(q' - q) < a$ e lembrando que a é um número inteiro, podemos dividir toda inequação por a, resultando em $0 \leq q' - q < 1$.

Concluindo, como $q' - q$ é número inteiro, as desigualdades acima são válidas para $q' - q = 0$, o que nos leva a concluir que $q = q'$ e por consequência $r = r'$, o que prova a unicidade.

Portanto, concluímos que o quocientes q e o resto r existem e são únicos. □

Observação 4.1.1. *A demonstração do Teorema (4.1.1), fornece um rico algoritmo para se encontrar o resto r e o quociente q da Divisão Euclidiana de um número natural b por um outro número a, o que pode ser utilizado pelo professor em sala de aula, dada a sua simplicidade, e acima de tudo, porque torna mais claro o entendimento do aluno em relação à divisão.*

Exemplo 4.1.2. *Encontre o quociente q e o resto r da divisão de 31 por 7.*

$$31 - 7.1 = 24 > 7, \;\; 31 - 7.2 = 17 > 7, \;\; 31 - 7.3 = 10 > 7, \;\; 31 - 7.4 = 3 < 7.$$

Portanto, $q = 4$ e $r = 3$.

Exemplo 4.1.3. *Encontre o quociente q e o resto r da divisão de 53 por 11.*

$$53 - 11.1 = 42 > 11, \;\; 53 - 11.2 = 31 > 11, \;\; 53 - 11.3 = 20 > 11, \;\; 53 - 11.4 = 9 < 11.$$

Portanto, $q = 4$ e $r = 9$.

4.2 Aplicações

Iniciaremos esta seção mostrando que um importante resultado da Análise Matemática, que é a Propriedade Arquimediana, pode ser obtido por meio do Teorema da Divisão Euclidiana. Por fim, mostraremos importantes resultados aritméticos, maneiras de particionar o conjunto dos inteiros através do resto da divisão por um inteiro diferente de 1 e estabelecer em que condições podemos escrever um número como sendo uma soma de quadrados.

A Propriedade Arquimediana aparece na Definição 4, Livro V nos *Elementos*, sem prova. Antes de enunciá-la consideraremos o Lema 4.2.1.

Lema 4.2.1. *Sejam a e b números naturais satisfazendo a condição de que $1 < a \leq b$, então existe um número natural n tal que*

$$na \leq b < (n+1)a.$$

Demonstração. Como consequência da Divisão Euclidiana, temos que dados a e b quaisquer, sabemos que podemos determinar de maneira única q e $r \in \mathbb{N}$, tais que $b = aq + r$ satisfazendo a condição de que $r < a$. Assim, tomando $n = q$, obtemos $b = na + r$, o que implica que $na \leq b$. De forma trivial, temos que $b < (n+1)a$. O que prova o enunciado da lema. □

Propriedade 4.2.1. *(Propriedade Arquimediana)*

Sejam $a, b \in \mathbb{N}^*$ quaisquer, sempre existe $m \in \mathbb{N}$ tal que $ma > b$.

Demonstração. Consideraremos inicialmente, o caso, em que $a > b$. Tomando $m = 1$, já obtemos o desejado. Agora, analisemos a situação em que $a \leq b$. Neste caso, basta considerarmos $m = n + 1$ e usar a segunda parte da desigualdade da propriedade anterior do Lema 4.2.1. □

A fim de estabelecer importantes propriedades aritméticas a seguir, vamos enunciar a Proposição 4.2.2 que é obtida como consequência do Teorema da Divisão Euclidiana.

Proposição 4.2.2. *Para um dado um número natural fixo $m \geq 2$ qualquer, sempre é possível escrever todo número natural n de forma única por $n = mq + r$, onde $q, r \in \mathbb{N}$ e $r < m$.*

A prova é uma consequência direta da aplicação do Teorema da Divisão Euclidiana.

Exemplo 4.2.1. *Todo número natural n pode ser escrito de maneira única na forma $2k$ ou $2k + 1$, onde $k \in \mathbb{N}$.*

Demonstração. Para isto, basta tomar $m = 2$ e aplicar a Proposição 4.2.2. □

Uma consequência natural do Exemplo 4.2.1 é que o conjunto dos números inteiros pode ser particionado em dois conjuntos disjuntos: um conjunto dos inteiros da forma $2k$, chamados de números pares e outro conjunto dos inteiros da forma $2k + 1$, chamados de números ímpares.

A mesma consideração pode ser obtida pelo próximo Exemplo.

Exemplo 4.2.2. *Todo número natural n pode ser escrito na forma $4k, 4k + 1, 4k + 2$ ou $4k + 3$, onde $k \in \mathbb{N}$. Neste caso, os números naturais se dividem em quatro conjuntos*

distintos, os da forma $4k$ *que em comum tem resto* 0 *na divisão euclidiana por* 4*, os da forma* $4k+1$ *que em comum tem resto* 1*, os da forma* $4k+2$ *que em comum tem resto* 2 *e os da forma* $4k+3$ *que em comum tem resto* 3*.*

No capítulo 8 abordaremos a parte da Aritmética Modular, na qual faremos uso da forma sistemática da Proposição 4.2.1. Nos próximos exemplos veremos que através da Proposição 4.2.2 são obtidas várias propriedades aritméticas.

Exemplo 4.2.3. *Todo quadrado de número natural quando dividido por* 5 *nunca deixa resto* 2 *ou* 3*.*

Demonstração. Todo número natural pode ser escrito na forma $5k$, $5k+1$, $5k+2$, $5k+3$ ou $5k+4$.

Agora vamos elevar ao quadrado todos os números acima.

$(5k)^2 = 25k^2 = 5.5k^2$, deixa resto 0 na divisão por 5.

$(5k+1)^2 = 25k^2 + 10k + 1 = 5.(5k^2 + 2k) + 1$, deixa resto 1 na divisão por 5.

$(5k+2)^2 = 25k^2 + 20k + 4 = 5.(5k^2 + 4k) + 4$, deixa resto 4 na divisão por 5.

$(5k+3)^2 = 25k^2 + 30k + 9 = 5.(5k^2 + 6k + 1) + 4$, deixa resto 4 na divisão por 5.

$(5k+4)^2 = 25k^2 + 40k + 16 = 5.(5k^2 + 8k + 3) + 1$, deixa resto 1 na divisão por 5.

Portanto, todo quadrado de um número natural quando dividido por 5 nunca deixa resto 2 ou 3. □

Com o intuito de obter mais propriedades aritméticas é que consideraremos a próxima Proposição.

Proposição 4.2.3. *Nenhum número natural da forma* $4n+3$ *pode ser escrito como o quadrado ou a soma de dois quadrados.*

Demonstração. Todo número natural pode ser escrito da forma $4n$, $4n+1$,$4n+2$ ou $4n+3$, com $n \in \mathbb{N}$.

Elevando esses números ao quadrado, obtemos:

$(4n)^2 = 16n^2 = 4.4n^2$, que é da forma $4n$.

$(4n+1)^2 = 16n^2 + 8n + 1 = 4.(4n^2 + 2n) + 1$, que é da forma $4n+1$.

$(4n+2)^2 = 16n^2 + 16n + 4 = 4.(4n^2 + 4n + 1)$, que é da forma $4n$.

$(4n+3)^2 = 16n^2 + 24n + 9 = 4.(4n^2 + 6n + 2) + 1$, que é da forma $4n + 1$. Assim, conseguimos mostrar que um número ao quadrado é da forma $4n$ ou $4n + 1$ e nunca da forma $4n + 3$.

Agora, se somarmos dois números ao quadrado, podemos ter:

$4n_1 + 4n_2 = 4.(n_1 + n_2)$ que é da forma $4n$.

$4n_1 + 1 + 4n_2 = 4.(n_1 + n_2) + 1$ que é da forma $4n + 1$.

$4n_1 + 4n_2 + 1 = 4.(n_1 + n_2) + 1$ que é da forma $4n + 1$.

$4n_1 + 1 + 4n_2 + 1 = 4.(n_1 + n_2) + 2$ que é da forma $4n + 2$.

Portanto, a soma de dois quadrados de dois naturais é da forma $4n, 4n + 1$ ou $4n + 2$ e nunca da forma $4n + 3$. □

Note que o inteiro primo 5 é da forma $4n + 1$ e pode ser escrito da forma $5 = 1^2 + 2^2$. Poderíamos indagar se isso acontece com os outros inteiros primos que são soma de quadrados. O próximo Corolário, responde essa questão.

Corolário 4.2.4. *Todo inteiro primo p que é soma de dois quadrados é igual a* 2 *ou da forma* $4n + 1$.

Demonstração. Note que $2 = 1^2 + 1^2$. Pela demonstração da Proposição 4.2.3, vimos que todo inteiro positivo que é a soma de dois quadrados é da forma $4n, 4n + 1$ ou $4n + 2$. Logo, se p é um inteiro primo só pode ser da forma $4n + 1$. □

De uma maneira mais geral, obtemos o próximo Corolário.

Corolário 4.2.5. *Todo inteiro positivo ímpar que é escrito como soma de dois quadrados é da forma* $4n + 1$.

Demonstração. Novamente, pela demonstração da Proposição 4.2.3, vimos que todo inteiro positivo que é a soma de dois quadrados é da forma $4n, 4n + 1$ ou $4n + 2$. Logo, o inteiro primo só pode ser da forma $4n + 1$. □

Exemplo 4.2.4. *Nenhum número a da forma* $11\ldots1$ *(n dígitos iguais a* 1, $n>1$*) é o quadrado ou soma de dois quadrados.*

Demonstração. Caso 1: Se $a = 11$, então a pode ser reescrito na forma: $11 = 4.2 + 3$ que é da forma $4n + 3$; logo não é um quadrado e nem a soma de dois quadrados.

Caso 2: Se a= 111, então a pode ser reescrito na forma:$a = 111 = 100 + 11 = 4(4.25 + 2) + 3$, que é também da forma $4n + 3$, isto é, da forma, $4n + 3$

Caso 3: Se a= 1111, então a pode ser reescrito na forma: $a = 1111 = 1000 + 111 = 4(250) + 4.(25 + 2) + 3$, que também é da forma $4n + 3$.

Como necessitamos de uma prova geral.Vamos supor $a = 11\ldots1$ ($n - 1$ dígitos 1) e que a é da forma $4n + 3$, para $n > 1$,que será nossa Hipótese de Indução e teremos de mostrar que a mesma é válida para n dígitos.

Primeiramente, temos que provar que a sentença acima é válida para $n = 2$, mas não é necessário, pois já fizemos a demonstração acima (Caso 1).

Sabemos que $a = 11\ldots1$ pode ser reescrito da seguinte forma:

$a = 11\ldots1$(n dígitos 1)= $4.(250\ldots0)$(n-2 dígitos 0)+$11\ldots1$(n-1 dígitos 1)(Hipótese de Indução)= $4.(250\ldots0) + 4n^{'} + 3 = 4n + 3$

Portanto, provamos que $11\ldots1$ para $n > 1$ é da forma $4n + 3$ que não é um quadrado e nem a soma de dois quadrados. □

Através da próxima proposição, obteremos mais propriedades aritméticas.

Proposição 4.2.6. *Nenhum número inteiro positivo ao quadrado é da forma* $6n + 2$ *ou da forma* $6n + 5$.

Demonstração. Todo número inteiro positivo pode ser escrito nas formas $6n, 6n + 1, 6n + 2, 6n + 3, 6n + 4$ ou $6n + 5$, com $n \in \mathbb{N}$.

Elevando esses números ao quadrado, obtemos:

$(6n)^2 = 36n^2 = 6.6n^2$, que é da forma $6n$.

$(6n + 1)^2 = 36n^2 + 12n + 1 = 6.(6n^2 + 2n) + 1$, que é da forma $6n + 1$.

$(6n + 2)^2 = 36n^2 + 24n + 4 = 6.(6n^2 + 3n) + 4$, que é da forma $6n + 4$.

$(6n + 3)^2 = 36n^2 + 36n + 9 = 6.(6n^2 + 6n + 1) + 3$, que é da forma $6n + 3$. $(6n + 4)^2 = 36n^2 + 48n + 16 = 6.(6n^2 + 8n + 2) + 4$, que é da forma $6n + 4$. $(6n + 5)^2 = 36n^2 + 60n + 25 = 6.(6n^2 + 10n + 3) + 1$, que é da forma $6n + 1$.

Assim, conseguimos mostrar que um número ao quadrado é da forma $6n, 6n+1, 6n+3, 6n+4$ e nunca da forma $6n+2$ e $6n+5$. □

Capítulo 5

Sistemas de Numeração

Neste capítulo, nos dedicaremos aos sistemas de numeração posicionais umas das aplicações mais importantes do Teorema da Divisão de Euclides. Daremos maior ênfase ao sistema posicional decimal, mas também estudaremos o sistema posicional de base 2.

O sistema posicional decimal é o mais conhecido e difundido em todo mundo, pois tal sistema serve para representar os números naturais. Neste sistema utilizamos a base 10 como referência e dependendo da posição que o algarismo ocupa é atribuído um peso, este que é uma potência de 10.

No último século com o advento dos computadores eletrônicos, o sistema binário tem recebido uma especial atenção, já que as unidades de informação, os "bits"assumem os valores lógicos que são rotulados como 0 e 1.

5.1 Teorema Geral da Enumeração

No sentido de ilustrar que o sistema posicional de numeração é uma consequência do Teorema da Divisão Euclidiana, apresentaremos o teorema geral da enumeração.

Teorema 5.1.1. *(Teorema Geral da Enumeração) Sejam a e b dois números naturais quaisquer, com $b > 1$, então existem números naturais $c_0, c_1, c_2, \ldots, c_n$ menores do que b, determinados de maneira única, tais que $a = c_0 + c_1.b + c_2.b^2 + \cdots + c_n.b^n$.*

Demonstração. (Adaptação de HEFEZ, 2011, p.44-45)

Faremos tal demonstração, utilizando a Segunda forma do Princípio da Indução Finita sobre a.

Considerando $a = 0$, ou $a = 1$, devemos ter $n = 0$ ou $c_0 = a$.

Agora, vamos considerar que o resultado obtido tem validade para qualquer número natural menor do que a, devemos demonstrá-lo para a. Utilizando a Divisão Euclidiana e sabendo da unicidade de q e r, temos:

$a = bq + r$, com $r < b$.

Admitindo que $q < a$ e utilizando a hipótese de indução, sabemos que existem números naturais n' e $d_0, d_1, d_2, \ldots, d_n$, com $d_j < b$, para $\forall j$, de modo que:

$$q = d_0 + d_1 b + \ldots + d_{n'} b^{n'}.$$

Utilizando as duas igualdades acima, obtemos:

$a = bq + r = b(d_0 + d_1 b + \ldots + d_{n'} b^{n'}) + r$.

Logo, de acordo com o que foi concluído acima, colocamos $c_0 = r$,$n = n' + 1$ e $c_j = d_{j-1}$ para $j = 1, 2, \ldots, n$.

Agora, para provarmos a unicidade, vamos supor que existam dois polinômios distintos que representem a, e mostraremos que eles são iguais.

$a = c_0 + c_1.b + c_2 b^2 + \ldots + c_n.b^n$

e

$a = g_0 + g_1.b + g_2 b^2 + \ldots + g_n.b^n$.

Como as duas expressões representam a, temos:

$a - a = c_0 + c_1.b + c_2 b^2 + \ldots + c_n.b^n - (g_0 + g_1 b + g_2 b^2 + \ldots + g_n.b^n) = 0$.

Utilizando a igualdade de polinômios temos que:

$c_0 = g_0; c_1 = g_1; c_2 = g_2, \ldots, c_n = g_n$. Portanto, os polinômios são idênticos, o que mostra a unicidade do polinômio: $a = c_0 + c_1.b + c_2.b^2 + \cdots + c_n.b^n$. □

A expressão $c_0 + c_1.b + c_2 b^2 + \cdots + c_n.b^n$ chama-se expansão relativa à base b, recebendo o nome expansão decimal se $b = 10$ e expansão binária se $b = 2$.

A expansão relativa à base b nos dá um método para representar os números naturais. Tal sistema utiliza b, e símbolos que representam seus algarismos são: 0,1, 2, ..., b_{n-2}, b_{n-1}.

5.2 Sistema Decimal

O sistema decimal posicional, já pelo nome sugere que trabalharemos com os algarismos $0, 1, 2, 3, 4, 5, 6, 7, 8$ e 9. Lembrando que aqui já incluímos o 0, que representa a ausência de algarismos e serve para guardar a posicão, pois como já vimos acima estamos trabalhando com sistemas posicionais.

Voltando ao Sistema de Numeração Posicional Decimal, que o próprio nome vem do número de símbolos que utilizamos para formar os números.Temos que com esse sistema conseguimos representar qualquer número que desejarmos, utilizando os dez símbolos citados acima, acompanhados de seus pesos que são potências de 10.

Agora, vamos relembrar como funcionam os pesos que são atribuídos a cada posição que o algarismo ocupa. O último algarismo da direita (algarismo das unidades) tem peso 1, pois $1 = 10^0$; o algarismo seguinte, mantendo a mesma ordem anterior, ou seja, da direita para à esquerda, tem peso 10, pois $10^1 = 10$ que é algarismo das dezenas, o próximo algarismo (algarismo das centenas) tem peso $100 = 10^2$; o algarismo seguinte (algarismo das unidades de milhar) tem peso 1000, pois $1000 = 10^3$ e continuamos o processo até que todos os algarismos do número tenham seus pesos atribuídos. Outro conceito importante que devemos relembrar é o conceito de ordem, tomando os algarismos de um número qualquer de n algarismos. O primeiro algarismo da direita para esquerda (algarismo das unidades) é da 1^a ordem, o próximo algarismo sempre da direita para esquerda (algarismo das dezenas) é da 2^a ordem, o próximo (algarismo das centenas) é da 3^a ordem, o outro algarismo (algarismo das unidades de milhar) é da 4^a ordem e assim por diante.

No Sistema Posicional Decimal também temos o conceito de classes, ou seja, as 1^a, 2^a e 3^a ordens formam a classe das unidades simples. As 4^a, 5^a e 6^a ordens formam a classe dos milhares. As 7^a, 8^a e 9^a ordens formam a classe do milhões. As 10^a,11^a e 12^a ordens formam a classe dos bilhões, e assim em diante, a cada três ordens há uma nova classe, até a n-ésima posição.

Agora que vimos todos os conceitos envolvidos na representação dos números na base 10, veremos alguns exemplos e relações nesta base.

Exemplo 5.2.1. *O número 275164, na base* 10 *tem a seguinte representação:*

$2.10^5 + 7.10^4 + 5.10^3 + 1.10^2 + 6.10^1 + 4.10^0 = 2.10^5 + 7.10^4 + 5.10^3 + 1.10^2 + 6.10 + 4.1.$

Então, em relação ao exemplo acima, o algarismo 4 *é da* 1^a *ordem, o* 6 *da* 2^a *ordem, o* 1 *da* 3^a *ordem, o* 5 *da* 4^a *ordem, o* 7 *da* 5^a *ordem e o* 2 *da* 6^a *ordem.*

5.2.1 Aplicações

Nesta subseção veremos algumas aplicações decorrentes do Teorema Geral da Enumeração do sistema de numeração decimal. A primeira se refere aos algarismos das unidades de um quadrado perfeito.

Exemplo 5.2.2. *Na base* 10*, o algarismo das unidades de um quadrado perfeito só pode ser* 0,1,4,5,6 *ou* 9.

Demonstração. Primeiramente, vamos escrever o número n, na base 10, na forma $n = b_0 + 10.b_1 + 100.b_2 + \ldots + 10^n.b_n$. Porém, para facilitar a resolução, reescreveremos n na forma $n = b_0 + 10.(b_1 + 10.b_2 + \ldots + 10^{n-1}.b_n) = b_0 + 10k = 10k + b_0$ com $k \in \mathbb{N}$. Elevando n ao quadrado, obtemos:

$n^2 = 100k^2 + 20k + b_0^2$. Notamos que o primeiro termo e o segundo termo da identidade acima são múltiplos de 10; portanto, o algarismo das unidades de um quadrado perfeito só depende de b_0^2. O algarismo das unidades de um número na base 10, só pode ser $0, 1, 2, 3, 4, 5, 6, 7, 8$ ou 9.

Analisaremos cada situação:

Para o caso $b_0 = 0$, obtemos $b_0^2 = 0$, logo o algarismos das unidades é 0.

No caso de $b_0 = 1$, obtemos $b_0^2 = 1$, logo o algarismos das unidades é 1.

No caso $b_0 = 2$, obtemos $b_0^2 = 4$, logo o algarismos das unidades é 4.

No caso $b_0 = 3$, obtemos $b_0^2 = 9$, logo o algarismos das unidades é 9.

No caso $b_0 = 4$, obtemos $b_0^2 = 16$, logo o algarismos das unidades é 6.

No caso $b_0 = 5$, obtemos $b_0^2 = 25$, logo o algarismos das unidades é 5.

No caso $b_0 = 6$, obtemos $b_0^2 = 36$, logo o algarismos das unidades é 6.

No caso $b_0 = 7$, obtemos $b_0^2 = 49$, logo o algarismos das unidades é 9.

No caso, $b_0 = 8$, obtemos $b_0^2 = 64$, logo o algarismos das unidades é 4.

Finalmente, para o caso $b_0 = 9$, obtemos $b_0^2 = 81$, logo o algarismos das unidades é 1.

Portanto, na base 10, o algarismo das unidades de um quadrado perfeito é 0,1,4,5,6 ou 9. □

Embora o enfoque desta dissertação seja aritmética em $\mathbb{N}$ e em $\mathbb{Z}$ com destaque nas aplicações decorrentes da aplicação do Algoritmo de Euclides, não deixaremos de discutir o sistema de numeração de um número real e de um número racional e sua relação com o Teorema da Divisão de Euclides.

Todo número real a no sistema numeração decimal é expresso da seguinte forma:

$$a = a_0 + \sum_{n=1}^{+\infty} a_n 10^{-n}, \tag{5.1}$$

onde $a_0 \in \mathbb{Z}$ e os a_n assumem valores entre 0 e 9.

Note que dado um número racional da forma $a = \frac{m}{n}$, temos que em função da Equação (5.1), o número a possui representação finita no sistema de numeração finita posicional de base 10 se, e somente se, existe um $k \in \mathbb{N}$ tal que $10^k a \in \mathbb{N}$. O que nos leva a concluir que $\frac{m}{n}$ tem representação finita no sistema posicional de base 10 caso $n|10^k m$, ou melhor, $\frac{10^k m}{n} \in \mathbb{N}$. Mas, se $n|10^k m$ e desde que m e n não tenham fatores primos em comum, concluímos que $n|10^k$. O que nos leva a concluir que n não tem fatores primos que não sejam fatores de 10^k.

Porém, são os mesmos fatores primos de 10, ou seja, 2 e 5.

Reciprocamente, caso n não tenha os fatores primos que não sejam 2 e 5 da fatoração de 10, então $n|10$ para um n suficientemente grande . Então, $n|10^k m$, e assim $\frac{10^k m}{n} \in \mathbb{N}$. Portanto, a possui representação finita no sistema de numeração posicional de base 10.

Assim, podemos reescrever via a proposição a seguir:

Proposição 5.2.1. *Todo número racional tem representação finita no sistema de numeração posicional de base* 10 *se, e somente se, o denominador n não possui fatores primos que não sejam fatores de* 2 *e* 5*.*

Observação 5.2.1. *Note que a proposição acima é uma consequência direta da Teorema da Divisão Euclidiana, ou seja, dado* $a = \frac{m}{n}$ *com m e n sem fatores primos em comum,*

então o a terá representação finita caso o resto da divisão de n por 10 *tiver resto zero. O número a terá representação infinita caso o resto da divisão de n por* 10 *tenha resto diferente de zero.*

5.3 Sistemas de numeração com bases diferentes de 10 e de 2

Neste seção, apresentaremos uma Proposição no contexto de sistemas de bases diferente de 10 análoga à Proposição 5.2.1 para a base 10 e por meio de alguns exemplos mostraremos como podemos converter uma número escrito em uma base para outra base.

Neste sentido, consideremos os próximos exemplos a seguir.

Exemplo 5.3.1. *Escreva o número* 5231 *que está na base* 6 *nas bases* 4 *e* 9.

Resolução:

Primeiramente, vamos escrever o número $(5231)_6$ na base 10.

$$(5234)_6 = 5.6^3+2.6^2+3.6^1+4.6^0 = 5.216+2.36+3.6+4.1 = 1080+72+18+4 = (1174)_{10}.$$

Agora, vamos escrever $(1174)_{10}$ na base 4.

$1174 = 293.4 + 2$; $293 = 73.4 + 1$; $73 = 18.4 + 1$; $18 = 4.4 + 2$; $4 = 1.4 + 0$

Logo, temos $(102112)_4$.

Finalmente, vamos escrever $(1174)_{10}$ na base 9. $1174 = 130.9 + 4$; $130 = 14.9 + 4$; $14 = 1.9 + 5$. Logo, temos $(1544)_9$.

Exemplo 5.3.2. *Um número na base* 10 *escreve-se 59; encontre em que base esse número é escrito na forma* 73.

Resolução:

Chamaremos de b a base desconhecida e vamos converter o número 73 da base b para a base 10.

Montamos a seguinte equação $7.b^1 + 3.b^0 = 59$, temos que $7.b + 3.1 = 59$, logo, $7b + 3 = 59$, e concluindo a resolução da equação, $b = 8$. Portanto, a base procurada é 8.

Exemplo 5.3.3. *O número* 270 *está escrito na base* 10*, determine em que base ele será escrito* 534*.*

Resolução:

Inicialmente, vamos chamar a base desconhecida de b e vamos montar uma equação com os dados do problema.

$270 = (534)_b \Longrightarrow 270 = 5.b^2 + 3.b^1 + 4.b^0$, podemos reescrever a equação

$5b^2 + 3b - 266 = 0$

Sabendo que $a = 5$, $b = 3$ e $c = -266$. Então,

$x = \dfrac{-b \pm \sqrt{b^2 - 4.a.c}}{2.a}$, temos:

$x = \dfrac{-3 \pm \sqrt{3^2 - 4.5.(-266)}}{2.5}$, fazendo os cálculos

$x = \dfrac{-3 \pm \sqrt{5359}}{10}$; logo, temos $x_1 = 7$ e $x_2 = -\dfrac{38}{5}$.

Analisando estas respostas, sabemos que $x_2 = -\dfrac{38}{5}$ não é válida, pois toda base é um número natural.

Portanto, a base procurada é 7.

5.3.1 Aplicações

Uma aplicação de um sistema posicional antigo de base diferente de 2 e de 10 é o sistema posicional sexagenal, que foi muito utilizado pelos babilônios no século $XVII$ a.C.. Tal sistema é muito utilizado quanto estudamos ângulos, pois temos como submúltiplos do grau o minuto (1/60) e o segundo (1/3600). Também estudamos esse sistema quando estudamos unidades de tempo, pois a hora tem como submúltiplos também o minuto e segundo.

De forma análoga, no caso do sistema de numeração decimal, todo número real a no sistema de numeração γ é expresso da seguinte forma:

$$a = a_0 + \sum_{n=1}^{+\infty} a_n \gamma^{-n}, \tag{5.2}$$

onde $a_0 \in \mathbb{Z}$ e os a_n assumem valores entre 0 e $\gamma - 1$.

Note que dado um número racional da forma $a = \frac{m}{n}$, temos que em função da Equação (5.2) o número a possui representação finita no sistema de numeração finita posicional de base γ se, e somente se, existe um $k \in \mathbb{N}$ tal que $\gamma^k a \in \mathbb{N}$. O que nos leva a concluir que $\frac{m}{n}$ tem representação finita no sistema posicional de base γ caso $n|\gamma^k m$, ou melhor, $\frac{\gamma^k m}{n} \in \mathbb{N}$. Mas, se $n|\gamma^k m$ e desde que m e n não tenham fatores primos em comum, concluímos que $n|\gamma^k$. O que nos leva a estabelecer que n não tem fatores primos que não sejam fatores de γ^k.

Porém, são os mesmos fatores primos de γ.

Reciprocamente, caso n não tenha os fatores primos com γ, então $n|\gamma$ para um n suficientemente grande . Então, $n|\gamma^k m$, e assim $\frac{\gamma^k m}{n} \in \mathbb{N}$. Portanto, a possui representação finita no sistema de numeração posicional de base γ.

Assim, podemos estabelecer a proposição a seguir:

Proposição 5.3.1. *Todo número racional da forma $\frac{m}{n}$ tem representação finita no sistema de numeração posicional de base γ se, e somente se, o denominador n não possui fatores primos com γ.*

Observação 5.3.1. *Note que a proposição acima é uma consequência direta da Teorema da Divisão Euclidiana, ou seja, dado $a = \frac{m}{n}$ com m e n sem fatores primos em comum, então o número a terá representação finita caso o resto da divisão de n por γ tenha resto zero e terá representação infinita caso o resto da divisão de n por γ tenha resto diferente de zero.*

5.4 Sistema de base binária e aplicações

Nesta seção, mostraremos algumas outras aplicações de um sistema de base binária distinta daquela envolvendo valores lógicos e dos "bits"de informação.

Aplicação 1 (Fonte: CARVALHO, E. D. - Arquivo pessoal.)

Representaremos subconjuntos por meio de "códigos" para isso utilizaremos a *representação binária* de números inteiros. Para uma melhor compreensão, considere o conjunto ordenado $A = \{a, b, c\}$ e seus respectivos subconjuntos:

$$\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}, \{a, b, c\}.$$

Seja um subconjunto B qualquer, ao analisarmos seus elementos um a um, escreveremos 1, se o elemento está em B e 0, se não está em B. Por exemplo, para o subconjunto $\{a, c\}$ escrevemos 101, pois os elementos a e c estão, mas não o b. Desta forma, todo subconjunto é "codificado" por uma cadeia de 3 dígitos consistindo de 0's e 1's. Especificando qualquer cadeia, podemos obter o subconjunto ao qual corresponde. Assim, a cadeia 001 está associada ao subconjunto $\{c\}$.

Tais cadeias de 0's e 1's nos remetem à *representação binária*. A forma binária de inteiros não-negativos até 7 é a seguinte:

$$0 = 0_2, \qquad 1 = 1_2, \qquad 2 = 10_2, \qquad 3 = 11_2, \qquad 4 = 100_2, \qquad 5 = 101_2,$$

$$6 = 110_2, \qquad 7 = 111_2.$$

Estas formas binárias dos inteiros $0, 1, \cdots, 7$ parecem ser "códigos" para os subconjuntos. A diferença é que a forma binária de um inteiro sempre começa com 1 e os primeiros quatro inteiros têm formas binárias mais curtas do que três, enquanto todos os códigos dos subconjuntos em questão consistem de exatamente três dígitos. Resolvemos isto acrescentando 0 no início de cada forma binária, fazendo que todas possuam o mesmo comprimento. Desta forma, obtemos a seguinte correspondência:

Tabela 5.1: Aplicação 1

Número inteiro	Forma binária	Código	Subconjunto
0	0	000	$\emptyset$
1	1	001	$\{c\}$
2	10	010	$\{b\}$
3	11	011	$\{b, c\}$
4	100	100	$\{a\}$
5	101	101	$\{a, c\}$
6	110	110	$\{a, b\}$
7	111	111	$\{a, b, c\}$

Fonte: CARVALHO, E. D. - Arquivo pessoal.

Portanto, os subconjuntos de $\{a, b, c\}$ correspondem aos números $0, 1, \cdots, 7$.

Exemplo 5.4.1. *Imagine a lista dos subconjuntos de um conjunto com* 10 *elementos e perguntamos qual é o subconjunto número* 233 *dessa lista. Para responder a esta pergunta, convertemos* 233 *à notação binária, resultando o número* 11101001_2 *ou* 0011101001_2*, acrescentado dois zeros no início. Então, se* $a_1, a_2, \cdots, a_{10}$ *são os elementos do nosso conjunto, então o subconjunto* 233 *de um conjunto de* 10 *elementos consiste dos elementos* a_{10}, a_7, a_5, a_4 *e* a_3.

Aplicação 2: Adivinhando o número pensado (CARVALHO, E. D. - Arquivo pessoal.)

Considere a seguinte brincadeira entre dois amigos A e B, onde A diz a B: "Pense um número (entre 1 e 31), escolha na tabela abaixo e diga em que colunas aparece o número que você pensou, que eu o adivinharei".

Note que uma maneira de A adivinhar é memorizar todos os números da tabela. Esta estratégica não é viável, caso a tabela seja grande.

A pessoa B pensa no número 15. Olhando a tabela observamos que o número 15 está presente nas colunas A_0, A_1, A_2, A_3. Surpreendendo B, a pessoa A "advinha"o número pensado por B. O que está por trás do jogo?

Está na maneira de construir a tabela.

Tabela 5.2: Aplicação 2

A_0	A_1	A_2	A_3	A_4
1	2	4	8	16
3	3	5	9	17
5	6	6	10	18
7	7	7	11	19
9	10	12	12	20
11	11	13	13	21
13	14	14	14	22
15	15	15	15	23
17	18	20	24	24
19	19	21	25	25
21	22	22	26	26
23	23	23	27	27
25	26	28	28	28
27	27	29	29	29
29	30	30	30	30
31	31	31	31	31

Fonte: CARVALHO, E. D. - Arquivo pessoal.

A construção está relacionada com a maneira de escrever os números inteiros (de 1 a 31) na base binária:

$1 = 1 \cdot 2^0$

$2 = 0 \cdot 2^0 + 1 \cdot 2^1$,

$3 = 1 \cdot 2^0 + 1 \cdot 2^1$,

$4 = 0 \cdot 2^0 + 0 \cdot 2^0 + 1 \cdot 2^2,$

$5 = 1 \cdot 2^0 + 0 \cdot 2^1 + 1 \cdot 2^2,$

$6 = 0 \cdot 2^0 + 1 \cdot 2^1 + 1 \cdot 2^2,$

$7 = 1 \cdot 2^0 + 1 \cdot 2^1 + 1 \cdot 2^2,$

$8 = 0 \cdot 2^0 + 0 \cdot 2^1 + 0 \cdot 2^2 + 1 \cdot 2^3,$

$9 = 1 \cdot 2^0 + 0 \cdot 2^1 + 0 \cdot 2^2 + 1 \cdot 2^3,$

$10 = 0 \cdot 2^0 + 1 \cdot 2^1 + 0 \cdot 2^2 + 1 \cdot 2^3,$

$11 = 1 \cdot 2^0 + 1 \cdot 2^1 + 0 \cdot 2^2 + 1 \cdot 2^3,$

$12 = 0 \cdot 2^0 + 0 \cdot 2^1 + 1 \cdot 2^2 + 1 \cdot 2^3,$

$13 = 1 \cdot 2^0 + 0 \cdot 2^1 + 1 \cdot 2^2 + 1 \cdot 2^3,$

$14 = 0 \cdot 2^0 + 1 \cdot 2^1 + 1 \cdot 2^2 + 1 \cdot 2^3,$

$15 = 1 \cdot 2^0 + 1 \cdot 2^1 + 1 \cdot 2^2 + 1 \cdot 2^3,$

$16 = 0 \cdot 2^0 + 0 \cdot 2^1 + 0 \cdot 2^2 + 0 \cdot 2^3 + 1 \cdot 2^4,$

$17 = 1 \cdot 2^0 + 0 \cdot 2^1 + 0 \cdot 2^2 + 0 \cdot 2^3 + 1 \cdot 2^4,$

$18 = 0 \cdot 2^0 + 1 \cdot 2^1 + 0 \cdot 2^2 + 0 \cdot 2^3 + 1 \cdot 2^4,$

$19 = 1 \cdot 2^0 + 1 \cdot 2^1 + 0 \cdot 2^2 + 0 \cdot 2^3 + 1 \cdot 2^4,$

$20 = 0 \cdot 2^0 + 0 \cdot 2^1 + 1 \cdot 2^2 + 0 \cdot 2^3 + 1 \cdot 2^4,$

$21 = 1 \cdot 2^0 + 0 \cdot 2^1 + 1 \cdot 2^2 + 0 \cdot 2^3 + 1 \cdot 2^4,$

$22 = 0 \cdot 2^0 + 1 \cdot 2^1 + 1 \cdot 2^2 + 0 \cdot 2^3 + 1 \cdot 2^4,$

$23 = 1 \cdot 2^0 + 1 \cdot 2^1 + 1 \cdot 2^2 + 0 \cdot 2^3 + 1 \cdot 2^4,$

$24 = 0 \cdot 2^0 + 0 \cdot 2^1 + 0 \cdot 2^2 + 1 \cdot 2^3 + 1 \cdot 2^4,$

$25 = 1 \cdot 2^0 + 0 \cdot 2^1 + 0 \cdot 2^2 + 1 \cdot 2^3 + 1 \cdot 2^4,$

$26 = 0 \cdot 2^0 + 1 \cdot 2^1 + 0 \cdot 2^2 + 1 \cdot 2^3 + 1 \cdot 2^4,$

$27 = 1 \cdot 2^0 + 1 \cdot 2^1 + 0 \cdot 2^2 + 1 \cdot 2^3 + 1 \cdot 2^4,$

$28 = 0 \cdot 2^0 + 0 \cdot 2^1 + 1 \cdot 2^2 + 1 \cdot 2^3 + 1 \cdot 2^4,$

$29 = 1 \cdot 2^0 + 0 \cdot 2^1 + 1 \cdot 2^2 + 1 \cdot 2^3 + 1 \cdot 2^4,$

$30 = 0 \cdot 2^0 + 1 \cdot 2^1 + 1 \cdot 2^2 + 1 \cdot 2^3 + 1 \cdot 2^4,$

$31 = 1 \cdot 2^0 + 1 \cdot 2^1 + 1 \cdot 2^2 + 1 \cdot 2^3 + 1 \cdot 2^4.$

Capítulo 6

Algoritmo de Euclides e o Máximo Divisor Comum

Neste capítulo, abordaremos o Algoritmo de Euclides, como consequência, obteremos um método geral para se determinar o máximo divisor comum entre dois números quaisquer. Este algoritmo, embora muito antigo, é muito eficiente do ponto de vista computacional e em quase nada foi aperfeiçoado nesses dois mil anos de sua existência.

6.1 O Máximo Divisor Comum

Inicialmente, anunciaremos o conceito de máximo divisor comum.

Dados dois números inteiros positivos a e b, dizemos que d é o máximo divisor entre a e b, caso d seja o maior inteiro que é divisor simultaneamente de a e b. As notações utilizadas são $mdc(a, b)$ ou (a, b).

Se $mdc(a, b) = 1$, dizemos que a e b são números primos entre si.

A seguir descreveremos alguns enunciados equivalentes sobre o máximo divisor comum que aparecem nos livros didáticos da Educação Básica.

Primeiramente, são encontrados todos os divisores do primeiro número e depois são encontrados os divisores do segundo. No primeiro caso, podemos montar um conjunto com todos os divisores do primeiro número e do segundo obtemos outro conjunto com os divisores do segundo número. O maior inteiro que estiver contido nos dois conjuntos

(Interseção) é o tão procurado Máximo Divisor Comum de a e de b.

Outro método para encontrar o máximo divisor comum entre dois números inteiros a e b é dado pela decomposição dos dois números inteiros positivos em fatores primos, em seguida separamos os fatores que se repetem com menor expoente e finalmente multiplicamos estes fatores ente si obtendo o Máximo Divisor Comum entre os dois números.

Percebemos que os dois métodos descritos acima são eficazes para números pequenos, mas quando os números envolvidos são grandes esses métodos citados são muito demorados. Trataremos, ainda, neste capítulo, que o máximo divisor comum entre dois números naturais sempre existe e é único, valendo ressaltar que $mdc(a, b) = mdc(b, a)$.

Inicialmente, abordaremos a existência do máximo divisor comum de alguns casos particulares dados pelas proposições a seguir.

Sem muita dificuldade, provam-se as propriedades dadas a seguir.

Proposição 6.1.1. *Para qualquer inteiro positivo a, tem-se que $mdc(0, a) = a$.*

Proposição 6.1.2. *Para qualquer inteiro positivo a, tem-se que $mdc(1, a) = 1$.*

Proposição 6.1.3. *Para qualquer inteiro positivo a, tem-se que $mdc(a, a) = a$.*

As Propriedades (6.1.1),(6.1.2) e (6.1.3) descrevem os casos mais particulares ao se determinar o máximo divisor comum.

Na próxima seção, apresentaremos um método para determinar o máximo divisor comum entre dois números inteiros positivos quaisquer.

6.2 Algoritmo de Euclides

O objetivo desta seção é o de mostrar que para quaisquer dois inteiros existe o máximo divisor comum entre eles. Chamamos a atenção que mostraremos apenas para os inteiros positivos, mas a prova geral para dois inteiros quaisquer é análoga à que iremos tratar nesta dissertação.

Neste sentido, dados a e b dois inteiros positivos quaisquer, consideremos os itens (i) e (ii):

(i) O caso em que $a \mid b$ ou $b \mid a$.

(ii) O caso em que a não divide b e que b não divide a.

O caso (i) nos conduz às Proposições (6.2.1) e (6.2.2).

Proposição 6.2.1. *Dados dois números inteiros positivos a e b, se $a \mid b$, então $mdc(a, b) = a$.*

Demonstração. Pela hipótese, temos $a \mid b$, ou seja , temos um inteiro positivo k tal que $b = a.k$, o que nos leva a concluir que $mdc(a, b) = a$. □

Proposição 6.2.2. *Dados dois números inteiros positivos a e b, se $b \mid a$, então $mdc(a, b) = b$.*

Demonstração. Análoga, a demonstração da Proposição 6.2.1. □

Para darmos resposta ao item (ii), de qual é o máximo de divisor comum entre a e b, forneceremos um método geral que determina o máximo divisor comum entre quaisquer inteiros positivos.

Este procedimento geral é dado pelo Algoritmo de Euclides. Para que possamos demonstrá-lo, estabelecemos os Lemas (6.2.3) e (6.2.4).

Lema 6.2.3. *Sendo a, b inteiros positivos com $a < na < b$. Se existe $mdc(a, b - na)$, então $mdc(a, b)$ existe e $mdc(a, b) = mdc(a, b - na)$.*

Demonstração. Sendo $d = mdc(a, b - na)$. Por definição, do máximo divisor comum temos que $d \mid a$ e $d \mid b - na$, então $d \mid b - na + na$. Logo, d é divisor comum de a e b. Portanto, provamos a existência. Agora, vamos provar a unicidade, vamos supor que c seja um divisor comum de a e $b - na$, temos que $c \mid d$, pois d é o máximo divisor comum, e com isso concluímos $d = mdc(a, b)$. □

Exemplo 6.2.1. *Todo número racional escrito na forma $\dfrac{5n+1}{10n+3}$ é irredutível.*

Primeiro, observamos que afirmar que a fração $\dfrac{5n+1}{10n+3}$ é irredutível equivale a mostrar que $mdc(5n + 1, 10n + 3) = 1$.

Repare que:

$$mdc(5n+1, 10n+3-2.(5n+1)) = mdc(5n+1, 1) = 1. \tag{6.1}$$

Pelo Lema 6.2.3, temos que

$$mdc(5n+1, 10n+3) = mdc(5n+1, 10n+3-2.(5n+1)). \tag{6.2}$$

Como consequência dos Equações (6.1) e (6.2), obtemos $mdc(5n+1, 10n+3) = 1$. Portanto, a fração $\dfrac{5n+1}{10n+3}$ é irredutível.

Lema 6.2.4. *Sendo a, b inteiros positivos com $a < na < b$. Se existe $mdc(a, b+na)$, então existe $mdc(a, b)$ e $mdc(a, b) = mdc(a, b+na)$.*

Demonstração: É feita de forma análoga à demostração do Lema (6.2.3).

Exemplo 6.2.2. *Todo número racional escrito na forma $\dfrac{n+1}{3n+4}$ é irredutível.*

Para verificarmos a afirmação do Exemplo (6.2.2), usaremos uma argumentação análoga àquela utilizada na verificação de que $\dfrac{5n+1}{10n+3}$ é irredutível .

Repare que

$$mdc(n+1, 3n+4-3.(n+1)) = mdc(n+1, 1) = 1. \tag{6.3}$$

Pelo Lema 6.2.3, temos que

$$mdc(n+1, 3n+4) = mdc(n+1, 3n+4-3.(n+1)). \tag{6.4}$$

Como consequência dos Equações (6.3) e (6.4), temos que $mdc(n+1, 3n+4) = 1$.

Assim, o $mdc(n+1, 3n+4) = 1$.

Portanto, $\dfrac{n+1}{3n+4}$ é irredutível.

Teorema 6.2.5. *(Algoritmo de Euclides) Quaisquer dois números inteiros positivos admitem máximo divisor comum.*

Demonstração. (Adaptado de HEFEZ, 2011, p.56)

Dados dois inteiros positivos a e b. Sem perda de generalidade, suporemos que $a < b$.

Se tivermos $a = 1$, $a = b$ ou $a|b$, sabemos que $mdc(a, b) = a$. Agora, vamos supor que $1 < a < b$ e que $a \nmid b$. Utilizando a divisão euclidiana, obtemos:

$b = aq_1 + r_1$, com $r_1 < a$.

Agora, temos duas possibilidades:

(i) Se $r_1 \mid a$, de acordo com o Lema de Euclides

$$mdc(a, b) = mdc(a, b - aq_1) = r_1$$

e finalizamos o algoritmo.

(ii) Se $r_1 \nmid a$ Agora devemos efetuar a divisão a por r_1, obtendo:

$a = r_1q_2 + r_2$, com $r_2 < r_1$.

Agora, novamente, temos duas possibilidades:

(a) Se $r_2 \mid r_1$, novamente pelo Lema de Euclides, obtemos:

$$r_2 = mdc(a, b) = mdc(a, b - q_1a) = mdc(a, r_1) = (r_1, a - q_2.r_1) = (r_1, r_2) = r_2$$

(b) Se $r_2 \nmid r_1$ agora devemos recomeçar o processo e dividir r_2 por r_1 , e agora obtendo:

$r_1 = r_2q_3 + r_3$, com $r_3 < r_2$.

O processo acima é finito, caso não fosse, contraria o Princípio da Boa Ordenação, pois teríamos a sequência de números inteiros positivos $a > r_1 > r_2 > r_3 \ldots$ que não tem um menor elemento. Se neste processo o $r_n \mid r_{n-1}$, temos que $mdc(a, b) = r_n$. □

Exemplo 6.2.3. *Encontre o* $mdc(14, 63)$ *utilizando o Algoritmo de Euclides.*

Resolução

Aplicando o Algoritmo de Euclides, temos:

$mdc(14, 63) = mdc(14, 63 - 4.14) = mdc(14, 7) = 7$.

Portanto, o $mdc(14, 63) = 7$.

Exemplo 6.2.4. *Tenho 4,2 metros de fita branca e 2,4 metros de fita vermelha para fazer enfeites. Desejo cortar as fitas de tal modo que obtenha pedaços com a mesma medida, no maior comprimento possível e que ambas as fitas sejam utilizadas integralmente. Qual é o comprimento de cada pedaço de fita?*

Resolução Primeiramente vamos transformar 4,2m e 2,4m em centímetros. Logo, temos que 4,2m=420cm e 2,4m=240cm. Podemos resolver tal problema calculando o $mdc(420, 240)$, utilizando o Algoritmo de Euclides, temos:

$mdc(240, 420) = mdc(240, 420-1.240) = mdc(240, 180) = mdc(180, 240) = mdc(180, 240-1.180) = mdc(180, 60) = 60$

Portanto, cada pedaço de fita tem 60 centímetros de comprimento.

6.3 Propriedades do Máximo Divisor Comum

Dados números inteiros quaisquer a e b, denotaremos por $I(a, b)$ como sendo o subconjunto de $\mathbb{Z}$ definido por $I(a, b) = \{xa+yb; x, y \in \mathbb{Z}\}$,. Como vale a propriedade comutativa com relação à operação de adição quanto a multiplicativa em $\mathbb{Z}$, $I(a, b)$ pode ser reescrito também na forma $I(a, b) = \{ax + by; x, y \in \mathbb{Z}\}$. Por meio de uma argumentação análoga, temos que $I(a, b) = I(b, a)$.

Exemplo 6.3.1. *Dados os números inteiros* 3 *e* 6. *Temos que* $I(3, 6) = \{3x + 6y; x, y \in \mathbb{Z}\}$.

Note que $18 \in I(3, 6)$*, já que existem inteiros* 2 *e* 3 *tal que* $18 = 3.2 + 6.2$.

Por outro lado, 1 *não pertence ao subconjunto* $I(3, 6)$ *de* $\mathbb{Z}$. *Caso* $1 \in I(3, 6)$*, então existiria ao menos pares de inteiros* (x, y) *tais que* $1 = 3x + 6y$. *Tal igualdade pode ser reescrita na forma* $3.\frac{1}{3} = 3(x+2y)$. *Sem perda de generalidade, analisaremos essa equação sobre* $\mathbb{R}$*, onde sabemos que vale a Lei do Cancelamento Multiplicativo.*

A equação acima é equivalente à equação dada por

$$\frac{1}{3} = x + 2y.$$

Já discutimos nos primeiros capítulos desta dissertação que o produto de números

inteiros e a soma de dois números inteiros também é um número inteiro. Por outro lado, sabemos $\frac{1}{3} \notin \mathbb{Z}$. *O que garante que* $1 \notin I(3,6)$.

Para analisarmos se existem x, y inteiros satisfazendo a condição de que para inteiros fixos a e b inteiros que satisfazem a condição de que $ax + by \in I(a,b)$, serão utilizadas as soluções de uma equação diofantina, e no próximo capítulo forneceremos ferramentas para dar tal resposta.

A partir de um subconjunto $I(a,b)$ qualquer de $\mathbb{Z}$, consideraremos um novo subconjunto dado por $I(a,b) \cap \mathbb{N}$. Pelo Princípio da Boa Ordem, desde que esse subconjunto de $\mathbb{N}$ seja não vazio, garante-se que exista um elemento mínimo em $I(a,b) \cap \mathbb{N}$.

Neste sentido, mostraremos essa relação entre esses subconjuntos $I(a,b)$ de $\mathbb{N}$ com o máximo divisor entre a e b por meio das próximas proposições.

Proposição 6.3.1. *Se* d *é o mínimo do conjunto* $I(a,b) \cap \mathbb{N}$, *então* $d = mdc(a,b)$.

Demonstração. Vamos supor que $\exists c \in \mathbb{Z}$ tal que c divide a e b. Como consequência das propriedades de divisibilidade, conclui-se facilmente que c divide todos os elementos de $I(a,b)$. Em particular, temos que $c \mid d$.

Agora, suponnhamos que exista $x \in I(a,b)$, tal que $d \nmid x$. Utilizando o Algoritmo da Divisão de Euclides, temos:

$x = d.q. + r$, com $0 < r < d$.

Sabendo que $x, d \in I(a,b)$, $\exists u, v, m, n \in \mathbb{Z}$, tal que $x = ua+vb$ e $d = ma+nb$, podemos reescrever $ua + vb = dq + r = (ma + nb)q + r = maq + nbq + r$, partindo de $ua + vb = maq + nbq + r$ e isolando r temos $r = ua - maq + vb - nbq \Longrightarrow r = (u - mq)a + (v - nq)b$ e que $\in \mathbb{Z}$.

Logo, encontramos um número natural $x \in I(a,b)$ que é menor do que d o que contraria a hipótese inicial.

Portanto, d divide todos os elementos de $I(a,b)$ e, em particular, $d \mid a$ e $d \mid b$. □

Proposição 6.3.2. $I(a,b) \cap \mathbb{N} = \{ld; l \in \mathbb{N}\}$.

Demonstração. Na demonstração da Proposição (6.3.1), já havíamos provado que se d divide todos elementos de $I(a,b)$, ou seja, $x \in I(a,b)$, então, $d \mid x$, assim $x = k.d$ para algum $k \in \mathbb{Z}$, o que equivale a afirmar que $x \in I(a,b)$.

Portanto, $I(a,b) \subset \{ld; l \in \mathbb{Z}\}$.

Reciprocamente, sabendo que $ld = l(ma+nb)$, temos que $lma+lnb = (lm)a+(ln)b \in I(a,b)$, ou seja, $\{ld; l \in \mathbb{Z}\} \subset I(a,b)$.

Portanto, $I(a,b) = \{ld; l \in \mathbb{Z}\}$. □

Exemplo 6.3.2. *Considere o conjunto $I(3,6)$ do Exemplo (6.3.1). Então:*

(i) *Sem muita dificuldade prova-se que $3 = min\ I(3,6) \cap \mathbb{N}$ e que $3 = mdc(3,6)$. O que está de acordo com a Proposição (6.3.1) já que o $min\ I(3,6) = mdc(3,6)$.*

(ii) *Pela Proposição (6.3.2) temos que $I(3,6) \cap \mathbb{N} = \{3.l\, l \in \mathbb{N}\}$.*

Através da Propriedade (6.3.1) apresentaremos importantes resultados que podem auxiliar no cálculo do máximo divisor entre dois números inteiros.

Propriedade 6.3.1. *Para quaisquer inteiros positivos a, b e n, temos:*

(i) $mdc(na, nb) = n.mdc(a,b)$.

(ii) $mdc(\frac{a}{(a,b)}, \frac{b}{(a,b)}) = 1$.

Demonstração. Pela Proposição (6.3.2) temos que $I(na,nb) = \{nx | x \in I(a,b)\} = nI(a,b)$. Assim, o $min\ nI(a,b) = min\ I(na,nb)$, ou seja, $mdc(na,nb) = n\ mdc(a,b)$, o que mostra o item (i).

Para provar o item (ii) basta utilizar o resultado do item (i). Seja $d = mdc(a,b)$, então $d.\ mdc(\frac{a}{d}, \frac{b}{d}) = (d\frac{a}{d}, d\frac{b}{d}) = mdc(a,b) = d$.

Portanto, concluímos que $(\frac{a}{d}, \frac{b}{d}) = 1$. □

Exemplo 6.3.3.

(i) Consideremos $3 = mdc(15,9)$. Como consequência do item (i) da Propriedade (6.3.1), temos que $mdc(45,27) = mdc(3.15, 3.3) = 3.mdc(15,3) = 3.3 = 9$.

(ii) Como consequência do item (ii) da Propriedade (6.3.1), temos $1 = mdc(5,3) = mdc(\frac{45}{9}, \frac{27}{9})$.

Capítulo 7

Equações Diofantinas Lineares

Neste capítulo, temos como foco a resolução de equações diofantinas lineares do tipo $ax+by=c$ e $ax-by=c$ com a,b e $c \in \mathbb{Z}$. Os possíveis valores das incógnitas x e y estarão definidos no conjunto dos números inteiros. As Equações Diofantinas recebem tal nome pois representam uma homenagem ao matemático Diofanto, matemático grego, considerado o maior algebrista grego. Diofanto escreveu vários livros sendo o mais importante "Aritmética", no qual introduz uma notação simbólica para o quadrado, cubo e assim em diante.

7.1 Método para se obter soluções de uma equação diofantina

No capítulo 6, fixamos $a, b \in \mathbb{Z}$, em seguida definimos o conjunto $I(a,b)$. Para ilustrar e discutir a importância da forma que definimos esse conjunto, consideremos o Exemplo (6.3.1). Em particular, para os casos em que $c = 18$ e 1, observamos de forma especial para esses elementos que $c \in I(3,6)$ equivaleria a analisar se uma particular solução de uma equação diofantina seria verificada.

Observação 7.1.1. *A partir do Exemplo (6.3.1), também pode ser verificado que:*

(i) $18 \in I(3,6)$ *e que* $3 = mdc(3,6)$ *divide* 18 *em* $\mathbb{Z}$*;*

(ii) $1 \notin I(3,6)$ *e que* $3 = mdc(3,6)$ *não divide* 1 *em* $\mathbb{Z}$*;*

A partir de agora focaremos nas condições gerais para a existência de solução em uma Equação Diofantina. Tais condições estão intimamente ligadas ao máximo divisor comum dos coeficientes a e b. Para discutirmos a existência de soluções inteiras de uma Equação Diofantina vejamos dois Teoremas importantes.

Teorema 7.1.1. *Sejam $a, b \in \mathbb{Z}$. A equação diofantina $ax + by = c$ tem solução inteira se, e somente se, $mdc(a, b) = d$ e $d \mid c$.*

Demonstração. De acordo com o Teorema acima teremos duas partes a demonstrar:

(i) De acordo com a hipótese, temos que a equação diofantina tem solução, e podemos considerá-la como sendo x_0 e y_0. Como $ax_0 + by_0 = c$ e $mdc(a, b) = d$, temos que:

$d \mid a$, então $a = d.q_1, q_1 \in \mathbb{Z}$ e $d \mid b$, então $b = d.q_2, q_2 \in \mathbb{Z}$. E, agora, utilizando a equação acima, temos:

$ax_0 + by_0 = c \Rightarrow d.q_1x_0 + d.q_2y_0 = c \Rightarrow d(.q_1x_0 + q_2y_0) = c \Rightarrow d \mid c$. O que conclui a primeira parte da demonstração.

(ii) Reciprocamente, temos por hipótese, agora, que $mdc(a, b) = d$ e que $d \mid c$. Sabendo que $d \mid c$ temos que $c = d.q, q \in \mathbb{Z}$.

Como $mdc(a, b) = d$, temos que $d = ax_0 + by_0$ e multiplicando os dois membros da equação por q, temos:

$d.q = qax_0 + qby_0$, organizando a equação, temos:

$aqx_0 + bqy_0 = d.q$, como $d.q = c$, $qx_0 = x$ e $qy_0 = y$. Assim:

$ax + by = c$. □

Teorema 7.1.2. *Sejam x_0,y_0 solução da Equação Diofantina $ax + by = c$, então todas as soluções inteiras são da forma: $x = x_0 + b.t$ e $y = y_0 - a.t$, onde $t \in \mathbb{Z}$.*

Demonstração. De fato, considerando $d = mdc(a, b) = 1$, caso contrário, vamos dividir os dois membros da equação por d, pois de acordo com as propriedades do máximo divisor comum temos que, $mdc(\frac{a}{d}, \frac{b}{d}) = 1$.

Por hipótese, temos que x_0,y_0 são solução da equação diofantina. Temos que $ax+by = c$ e $ax_0 + by_0 = c$, e igualando ambas as equações, pois ambas são iguais a c, temos:

$ax + by = ax_0 + by_0 \Longrightarrow ax - ax_0 = by_0 - by \Longrightarrow a(x - x_0) = b(y_0 - y)$.

Como $mdc(a, b) = 1$ temos duas situações $a \nmid b$ e $b \nmid a$.

(i) Nesta primeira parte, sabemos que $a \nmid b$ e $a \mid b(y_0 - y)$, então temos que $a \mid y_0 - y$, escrevendo de outro modo temos $y_0 - y = a.t$, o que implica $y = y_0 - a.t$,$t \in \mathbb{Z}$.

(ii) A segunda parte é semelhante à primeira, pois $b \nmid a$ e $b \mid a(x - x_0)$, escrevendo de outro modo, temos $x - x_0 = b.t'$, $t' \in \mathbb{Z}$, que reescrito fica $x = x_0 + b.t'$.

Substituindo $x - x_0 = b.t'$ e $y_0 - y = a.t$ na equação $a(x - x_0) = b(y_0 - y)$, temos:

$a.b.t' = b.at. \Longrightarrow t' = t$.

Logo, as soluções inteiras de uma Equação Diofantina são $x = x_0 + b.t$ e $y = y_0 - a.t$, onde $t \in \mathbb{Z}$. O que conclui a demonstração. □

Agora que concluímos as demonstrações dos dois teoremas importantes, vamos resolver alguns exemplos de equações diofantinas em $\mathbb{Z}$ e em $\mathbb{N}$.

7.2 Aplicações

Exemplo 7.2.1. *Encontre todas as soluções inteiras da Equação Diofantina* $12x + 15y = 120$.

Resolução:

Incialmente, repare que na equação acima para percebermos que todos os seus coeficientes são divisíveis por 3, o que nos dá uma nova equação equivalente à primeira.

$4x + 5y = 40$. Agora vamos verificar se essa tem solução em $\mathbb{Z}$, $mdc(4, 5) = 1$ e $1 \mid 40$, logo a equação possui solução inteira.

Agora utilizando o Algoritmo da Divisão de Euclides, vamos calcular o $mdc(4, 5) = 1$:

Escrevendo o Algoritmo da Divisão de Euclides, temos que:

$5 = 4.1 + 1$ que pode ser reescrito, como: $5.1 + 4.(-1) = 1$, multiplicando a equação acima por 40, temos:

$4.(-40) + 5.(40) = 40$ que é equivalente a equação inicial.

Logo, a solução da equação é $x_0 = -40$ e $y_0 = 40$ e como as todas suas soluções inteiras são da forma $x = x_0 + b.t$ e $y = y_0 - a.t$ e neste caso são $x = -40 + 5.t$ e $y = 40 - 4.t$, com $t \in \mathbb{Z}$

Exemplo 7.2.2. *Encontre todas as soluções inteiras da equação diofantina* $18x + 14y = 60$.

Resolução:

Primeiramente, simplificamos a equação $18x + 14y = 60$ por 2.

Agora obtemos $9x + 7y = 30$ e sabendo que $mdc(9, 7) = 1$ e que $1 \mid 30$, sabemos que a equação tem solução inteira.

Utilizando o Algoritmo da Divisão de Euclides, podemos escrever:

$9 = 7.1 + 2$ e $7 = 2.3 + 1$, reescrevendo a primeira sentença, temos:

$9.1 + 7.(-1) = 2$. Agora, multiplicamos os dois membros da equação por 15 e obtemos $9.15 + 7.(-15) = 30$.

Percebemos que $x_0 = 15$ e $y_0 = -15$.

Portanto, todas as soluções inteiras são da forma $x = 15 + 7.t$ e $y = -15 - 9.t$, com $t \in \mathbb{Z}$.

Exemplo 7.2.3. *Encontre todas as soluções naturais da equação diofantina* $14x + 6y = 168$.

Resolução:

Primeiramente, simplicamos os dois membros da equação por 2, e daí obtemos $7x + 3y = 80$.

Agora, vamos obter o $mdc(7, 3) = 1$ e com isso percebemos que a equação acima tem solução em $\mathbb{Z}$, pois $1 \mid 84$.

Utilizando o Algoritmo da Divisão de Euclides para escrever o $mdc(7, 3) = 1$ em função de 7 e 3, temos que:

$7 = 3.2 + 1$, então $7.1 + 3.(-2) = 1$, multiplicando ambos os membros dessa equação por 84, temos:

$7.84 + 3.(-168) = 84$, agora sabemos que a solução particular $x_0 = 84$ e $y_0 = -168$, logo todas as soluções inteiras são da forma $x = x_0 + b.t$ e $y = y_0 - a.t$ com $t \in \mathbb{Z}$, o que

nos dá $x = 84 + 3t$ e $y = -168 - 7t$, com $t \in \mathbb{Z}$.

Mas de acordo com o enunciado do exercício, precisamos encontrar todas as soluções naturais, o que nos leva a utilizar um artifício interessante, ou seja, todas nossas soluções têm que $\in \mathbb{N} \bigcup \{0\}$, logo:

$84 + 3.t \geqslant 0 \Longrightarrow t \geqslant -28$

e

$-168 + 7.t \geqslant 0 \Longrightarrow t \leqslant -22$

Logo, nossos possíveis valores para t são -22,-23,-24,-25,-26 ,-27 e -28.

Para t = -22, temos:

$x = 84 + 3.(-22)$, o que resulta em $x = 18$ e

$y = -168 - 7.(-22)$ o que resulta em $y = -14$.

Para t = -23, temos:

$x = 84 + 3.(-23)$, o que resulta em $x = 15$ e

$y = -168 - 7.(-23)$ o que resulta em $y = -7$.

Para t = -24, temos:

$x = 84 + 3.(-24)$, o que resulta em $x = 12$ e

$y = -168 - 7.(-24)$ o que resulta em $y = 0$.

Para t = -25, temos:

$x = 84 + 3.(-25)$, o que resulta em $x = 9$ e

$y = -168 - 7.(-25)$ o que resulta em $y = 7$.

Para t = -26, temos:

$x = 84 + 3.(-26)$, o que resulta em $x = 6$ e

$y = -168 - 7.(-26)$ o que resulta em $y = 14$.

Para t = -27, temos:

$x = 84 + 3.(-27)$, o que resulta em $x = 3$ e

$y = -168 - 7.(-27)$ o que resulta em $y = 21$.

Para t = -28, temos:

$x = 84 + 3.(-28)$, o que resulta em $x = 0$ e

$y = -168 - 7.(-28)$ o que resulta em $y = 28$.

Portanto, temos os seguintes pares de números que podem ser considerados as soluções naturais da equação: 12 e 0, 9 e 7,6 e 14, 3 e 21,0 e 28.

Exemplo 7.2.4. *Em um evento, os ingressos para homens são vendidos por 28 reais cada e por 24 reais os ingressos para mulheres. Quantos ingressos para homens e quantos ingressos para mulheres podem ser comprados por uma pessoa que dispõe de 420 reais?*

Resolução:

Incialmente, definiremos como sendo x a quantidade de homens e y como sendo a quantidade de mulheres e logo teremos a equação:

$28x + 24y = 420$, agora podemos dividir ambos os membros desta equação por 4 e obtemos a equação equivalente $7x + 6y = 105$ com $mdc(7, 6) = 1$ e $1 \mid 105$. Agora, precisamos escrever o $mdc(7, 6) = 1$ como combinação linear de 7 e 6, e utilizando o Algoritmo da Divisão de Euclides, temos:

$7 = 6.1 + 1 \Longrightarrow 7.1 + 6.(-1) = 1$ e em seguida, multiplicando ambos os membros da equação por 105, temos: $7.(105) + 6.(-105) = 105$

Logo, as soluções inteiras são $x = 105 - 6.t$ e $y = -105 + 7.t$ com $t \in \mathbb{Z}$. Mas de acordo com o enunciado só nos servem as quantidades inteiras não negativas.

$105 - 6.t \geq 0 \Longrightarrow t \leq \frac{35}{2}$

$-105 + 7.t \geq 0 \Longrightarrow t \geq 15.$

Os números inteiros que satisfazem às duas desigualdades são 15,16 e 17.

Para t = 15, temos:

$x = 105 - 6.(15)$, o que resulta em $x = 15$ e

$y = -105 + 7.(15)$ o que resulta em $y = 0$.

Para t = 16, temos:

$x = 105 - 6.(16)$, o que resulta em $x = 9$ e

$y = -105 + 7.(16)$ o que resulta em $y = 7$.

Para t = 17, temos:

$x = 105 - 6.(17)$, o que resulta em $x = 3$ e

$y = -105 + 7.(17)$ o que resulta em $y = 14$.

Portanto, com 420 reais pode-se comprar 15 ingressos para homens e 0 ingresso para

mulheres, 9 ingressos para homens e 7 ingressos para mulheres ou 3 ingressos para homens e 14 para mulheres.

Exemplo 7.2.5. *Se uma pessoa subir em um escada de dois em dois degraus sobra um degrau e se a mesma pessoa utilizando a mesma escada subir de três em três degraus, sobram 2 degraus. Quantos degraus possui a escada sabendo que esse número está entre 55 e 59?*

Resolução:

Inicialmente, vamos chamar o número de degraus da escada de N. No primeiro caso, temos que:

$N = 2x + 1$, onde x é o número de passos que a pessoa deu para subir a primeira vez. E, no segundo caso, temos que $N = 3y + 2$. Como se trata da mesma escada podemos ter:

$2x+1 = 3y+2$, fazendo as operações necessárias, obtemos a seguinte equação diofantina $2x - 3y = 1$.

Sabemos que $mdc(2, 3) = 1$ e que $1 \mid 1$, logo a equação tem solução.

Vamos Utilizar o Algoritmo da Divisão de Euclides para escrever $mdc(3, 2) = 1$ como combinação linear de 2 e 3, temos:

$3 = 2.1+1 \Longrightarrow 3.1+2.(-1) = 1$ reescrevendo tal sentença, temos: $2.(-1)-3.(-1) = 1$, logo as soluções são $x = -1 + 3t$ e $y = -1 + 2t$, com $t \in \mathbb{Z}$.

Para $t = 5$, temos $x = 14$, $y = 9$ e $N = 29$.

Para $t = 9$, temos $x = 26$, $y = 17$ e $N = 53$.

Para $t = 10$, temos $x = 29$,$y = 19$ e $N = 59$.

Para $t = 11$, temos $x = 32$, $y = 21$ e $N = 63$

Portanto, a escada tem 59 degraus.

Capítulo 8

Aritmética Modular

Nosso propósito neste capítulo é apresentar as congruências, bem como suas propriedades e prová-las e propor algumas aplicações para deixar claro o objetivo principal de estudar congruências que é facilitar a resolução de exercícios que tem como objetivo trabalhar com o resto de determinada divisão. Outro aspecto, importante a ser lembrado, é que a congruência módulo m está intimamente ligada ao Algoritmo da Divisão de Euclides.

Durante este capítulo vamos resolver exercícios propostos em capítulos anteriores e utilizando outro modo de resolução para que possamos convencer o leitor desta dissertação da utilidade do estudo das congruências.

8.1 Congruências Módulo m.

Nesta seção deste capítulo, vamos apresentar algumas propriedades importantes das congruências, que são muito úteis na resolução de problemas, bem como demonstrá-las.

Dados $a, b, m \in \mathbb{Z}$, temos que,a é congruente a b módulo m, se a e b deixam o mesmo resto, quando divididos por m, isto é, $m \mid (a - b)$. Denotamos por $a \equiv \ b \ mod \ m$.

Exemplo 8.1.1.

(i) $4 \equiv 1 \ mod \ 3$, pois 1 e 4 deixam o mesmo resto na divisão por 3.

(ii) $5 \equiv 15 \ mod \ 10$, pois 5 e 15 deixam o mesmo resto na divisão por 10.

(iii) $3 \equiv 10 \ mod \ 7$, pois 3 e 10 deixam o mesmo resto na divisão por 7.

Propriedade 8.1.1. *$a \equiv a \ mod \ m$ (Propriedade Reflexiva).*

Demonstração. De acordo com a definição de congruência, temos que $m \mid (a - a)$ e $m \mid 0$. □

Propriedade 8.1.2. *Se $a \equiv b \ mod \ m$, então $b \equiv a \ mod \ m$ (Propriedade Comutativa).*

Demonstração. Pela hipótese temos que $m \mid (a - b)$. Sabendo que o oposto de $(a - b)$ também é divisível por m, temos que $m \mid -(a - b) = (b - a) \Longrightarrow b \equiv a \ mod \ m$. □

Propriedade 8.1.3. *Se $a \equiv b \ mod \ m$ e $b \equiv c \ mod \ m$, então $a \equiv c \ mod \ m$ (Propriedade Transitiva)*

Demonstração. Pela hipótese temos que $m \mid (a-b)$ e $m \mid (b-c)$. Podemos somar as duas e a soma continua sendo divisível por m, temos que $m \mid (a - b) + (b - c) = a - c \Longrightarrow a \equiv c \ mod \ m$. □

Propriedade 8.1.4. *Se $a \equiv b \ mod \ m$ e $c \equiv d \ mod \ m$, então $a + c \equiv b + d \ mod \ m$.*

Demonstração. Pela hipótese temos que $m \mid (a-b)$ e $m \mid (c-d)$, podemos somar as duas expressões e a soma continua sendo divisível por m, temos que $m \mid (a - b) + (c - d)$ e reagrupando os termos temos $m \mid (a + c) - (b + d) \Longrightarrow a + c \equiv b + d \ mod \ m$. □

Propriedade 8.1.5. *Se $a \equiv b \ mod \ m$ e $c \equiv d \ mod \ m$ então, $a - c \equiv b - d \ mod \ m$.*

Demonstração. Pela hipótese temos que $m \mid (a-b)$ e $m \mid (c-d)$, podemos subtrair as duas expressões e a diferença continua sendo divisível por m, temos que $m \mid (a - b) - (c - d)$ e reagrupando os termos temos $m \mid (a - c) - (b - d) \Longrightarrow a - c \equiv b - d \ mod \ m$. □

Propriedade 8.1.6. *Se $a \equiv b \ mod \ m$ e $c \equiv d \ mod \ m$ então, $a.c \equiv b.d \ mod \ m$.*

Demonstração. Da hipótese, temos que $m \mid (a - b)$ e $m \mid (c - d)$. Podemos multiplicar o lado direito da primeira expressão por c, pois $c \in \mathbb{Z}$ e a expressão continua verdadeira. Podemos fazer o mesmo multiplicando o lado direito da segunda expressão por b, pois $b \in \mathbb{Z}$ e a expressão também continua verdadeira, ou seja, $m \mid (a - b).c$ e $m \mid (c - d).b$. Como $m \mid (a-b).c$ e $m \mid (c-d).b$, então $m \mid (a-b).c+(c-d).b$, efetuando as operações, temos $m \mid (ac - bd)$ então $a.c \equiv b.d \ mod \ m$. □

Propriedade 8.1.7. *Se $a \equiv b \ mod \ m$, então $a^n \equiv b^n \ mod \ m$, para $\forall n \in \mathbb{N}$.*

Demonstração. Da hipótese, temos que $m \mid (a-b)$, e se multiplicarmos a segunda parte da expressão por um polinômio de grau $n-1$ a hipótese continua valendo, então $m \mid (a-b)(a^{n-1}+a^{n-2}b+a^{n-3}b^{2+}\cdots+a.b^{n-2}+b^{n-1}) = a^n - b^n$, e fazendo as operações temos $m \mid (a^n - b^n) \Longrightarrow a^n \equiv b^n \ mod \ m$. □

8.2 Aplicações

Nesta seção de nosso trabalho vamos resolver alguns exemplos que foram propostos nos capítulos anteriores, mas agora utilizaremos a congruência para mostrar que essa ferramenta facilita muito as resoluções de tais exemplos e inúmeros outros.

Exemplo 8.2.1. *Nenhum número natural da forma $4n+3$ pode ser escrito como o quadrado ou a soma de dois quadrados.*

Demonstração. Todo número natural quando é dividido por quatro pode ter quatro restos possíveis que são: 0,1,2 e 3.Portanto, estes números são da forma $4k$, $4k+1$, $4k+2$ e $4k+3$. Utilizando a notação de congruência estes números podem ser escritos assim:

$4k \equiv 0 \ mod \ 4$, $4k+1 \equiv 1 \ mod \ 4$, $4k+2 \equiv 2 \ mod \ 4$ e $4k+3 \equiv 3 \ mod \ 4$.

Agora resolveremos a primeira parte do exemplo. Elevando ao quadrado todas as congruências acima, temos:

$(4k)^2$=$0^2 \equiv 0 \ mod \ 4$

$(4k+1)^2$=$1^2 \equiv 1 \ mod \ 4$

$(4k+2)^2$=$2^2 = 4 \equiv 0 \ mod \ 4$ e

$(4k+3)^2$=$3^2 = 9 \equiv 1 \ mod \ 4$.

Portanto, todo quadrado de um número natural pode ser escrito na forma $4k$ ou $4k+1$ e nunca na forma $4k+3$.

Agora, para resolver a segunda parte do exemplo podemos tomar como base que todo quadrado de um número natural pode ser escrito utilizando a notação de congruência na forma $4k \equiv 0 \ mod \ 4$ e $4k+1 \equiv 1 \ mod \ 4$.

Lembrando que teremos que analisar três casos:

[i] Se tivermos dois números $4m \equiv 0\ mod\ 4$ e $4n \equiv 0\ mod\ 4$ e efetuarmos a adição de $4m + 4n$, teremos:

$4m + 4n \equiv 0 + 0\ mod\ 4 \Longrightarrow 4m + 4n \equiv 0\ mod\ 4$

[ii] Se tivermos dois números $4m \equiv 0\ mod\ 4$ e $4n + 1 \equiv 1\ mod\ 4$ e efetuarmos a adição de $4m + 4n + 1$, teremos: $4(m + n) + 1 \equiv 0 + 1\ mod\ 4 \Longrightarrow 4(m + n) + 1 \equiv 1\ mod\ 4$

[iii] Se tivermos dois números $4m + 1 \equiv 0\ mod\ 4$ e $4n + 1 \equiv 1\ mod\ 4$ e efetuarmos adição de $4m + 4n + 1$, teremos: $4m + 1 + 4n + 1 \equiv 1 + 1\ mod\ 4 \Longrightarrow 4(m + n) + 2 \equiv 2\ mod\ 4$.

Portanto, a soma de dois quadrados só pode ser da forma $4k$, $4k + 1$ ou $4k + 2$. □

Exemplo 8.2.2. *Na base* 10*, o algarismo das unidades de um quadrado perfeito só pode ser* 0,1,4,5,6 *ou* 9*.*

Demonstração. Primeiramente, vamos escrever o número n, na base 10, na forma $n = b_0 + 10.b_1 + 100.b_2 + \ldots + 10^n.b_n$. Porém, para facilitar a resolução, reescreveremos n na forma $n = b_0 + 10.(b_1 + 10.b_2 + \ldots + 10^{n-1}.b_n) = b_0 + 10k = 10k + b_0$ com $k \in \mathbb{N}$.

Elevando n ao quadrado, obtemos:

$n^2 = (10k + b_0)^2 = 100k^2 + 20k + b_0^2 = 10.(10k^2 + 2k) + b_0^2$. Percebemos que o primeiro e o segundo termos da última expressão são múltiplos de 10, logo, não pertencem às unidades, então o algarismo das unidades só depende de b_0, portanto trabalharemos com potências de b_0^2.

Vejamos:

para $b_0 = 0$, temos $b_0^2 = 0^2 = 0 \Longrightarrow 0 \equiv 0\ mod\ 10$.

para $b_0 = 1$, temos $b_0^2 = 1^2 = 1 \Longrightarrow 1 \equiv 1\ mod\ 10$.

para $b_0 = 2$, temos $b_0^2 = 2^2 = 4 \Longrightarrow 4 \equiv 4\ mod\ 10$.

para $b_0 = 3$, temos $b_0^2 = 3^2 = 9 \Longrightarrow 9 \equiv 9\ mod\ 10$.

para $b_0 = 4$, temos $b_0^2 = 4^2 = 16 \Longrightarrow 16 \equiv 6\ mod\ 10$.

para $b_0 = 5$, temos $b_0^2 = 5^2 = 25 \Longrightarrow 25 \equiv 5\ mod\ 10$.

para $b_0 = 6$, temos $b_0^2 = 6^2 = 36 \Longrightarrow 36 \equiv 6\ mod\ 10$.

para $b_0 = 7$, temos $b_0^2 = 7^2 = 49 \Longrightarrow 49 \equiv 9\ mod\ 10$.

para $b_0 = 8$, temos $b_0^2 = 8^2 = 64 \Longrightarrow 64 \equiv 4\ mod\ 10$.

para $b_0 = 9$, temos $b_0^2 = 9^2 = 81 \Longrightarrow 81 \equiv 1 \ mod \ 10$.

Portanto, todo quadrado perfeito tem como algarismo das unidades 0,1,4, 5,6 ou 9. □

Exemplo 8.2.3. *Qual é o algarismo das unidades da potência* 3^{82}*?*

Resolução:

Primeiramente, vamos escrever as primeiras potências de 3 e analisá-las.

$3^1 = 3 \equiv 3 \ mod \ 10$, o algarismo das unidades é 3.

$3^2 = 9 \equiv 9 \ mod \ 10$, o algarismo das unidades é 9.

$3^3 = 27 \equiv 7 \ mod \ 10$, o algarismo das unidades é 7.

$3^4 = 81 \equiv 1 \ mod \ 10$, o algarismo das unidades é 1.

$3^5 = 243 \equiv 3 \ mod \ 10$, o algarismo das unidades é 3.

$3^6 = 729 \equiv 9 \ mod \ 10$, o algarismo das unidades é 9.

Percebemos que as potências de 3 seguem um ciclo de 4 em 4, com restos respectivamente 3,9,7 e 1.

Agora sabendo que:

$3^4 = 81 \equiv 1 \ mod \ 10$, e aplicando a *Propriedade* 8.1.7. das congruências temos $3^{4.20} \equiv 1^{20} \ mod \ 10 \Longrightarrow 3^{80} \equiv 1 \ mod \ 10$.

e sabendo também que $3^2 = 9 \equiv 9 \ mod \ 10$ e aplicando a *Propriedade* 8.1.6, temos:

$3^{80}.3^2 \equiv 1.9 \ mod \ 10 \Longrightarrow 3^{82} \equiv 9 \ mod \ 10$.

Portanto, o algarismo das unidades de 3^{82} é 9.

Exemplo 8.2.4. *Todo quadrado perfeito é congruente, módulo 8, a um dos números 0,1 ou 4.*

Demonstração. Primeiramente, temos que observar que todo número $n \in \mathbb{N}$ é da forma: 8k+r, onde $k \in \mathbb{N}$ e $r \in \{0, 1, 2, 3, 4, 5, 6, 7\}$.

Temos:

$n^2 = (8k + 0)^2 = 8.8k^2 \Longrightarrow n^2 \equiv 0 \ mod \ 8$.

$n^2 = (8k + 1)^2 = 8.8k^2 + 2.8k + 1 \Longrightarrow n^2 \equiv 1 \ mod \ 8$.

$n^2 = (8k + 2)^2 = 8.8k^2 + 4.8k + 4 \Longrightarrow n^2 \equiv 4 \ mod \ 8$.

$n^2 = (8k + 3)^2 = 8.8k^2 + 6.8k + 9 \Longrightarrow n^2 \equiv 9 \ mod \ 8 \Longrightarrow n^2 \equiv 1 \ mod \ 8$.

$n^2 = (8k + 4)^2 = 8.8k^2 + 8.8k + 16 \Longrightarrow n^2 \equiv 16 \ mod \ 8 \Longrightarrow n^2 \equiv 0 \ mod \ 8$.

$n^2 = (8k+5)^2 = 8.8k^2 + 10.8k + 25 \Longrightarrow n^2 \equiv 25 \ mod \ 8 \Longrightarrow n^2 \equiv 1 \ mod \ 8.$

$n^2 = (8k+6)^2 = 8.8k^2 + 12.8k + 36 \Longrightarrow n^2 \equiv 36 \ mod \ 8 \Longrightarrow n^2 \equiv 4 \ mod \ 8.$

$n^2 = (8k+7)^2 = 8.8k^2 + 14.8k + 49 \Longrightarrow n^2 \equiv 49 \ mod \ 8 \Longrightarrow n^2 \equiv 1 \ mod \ 8.$

Portanto, todo quadrado perfeito é congruente, módulo 8, a 0, 1 ou 4, ou seja, qualquer quadrado perfeito ao ser dividido por 8 deixa resto 0, 1 ou 4. □

Exemplo 8.2.5. *Encontre o resto da divisão de* 2^{201} *por* 11.

Resolução:

Neste exercício vamos usar congruência módulo 11, pois o enunciado faz referência à divisão por 11.

$2^1 = 2$ e $2 \equiv 2 \ mod \ 11$

$2^2 = 4$ e $4 \equiv 4 \ mod \ 11$

$2^3 = 8$ e $8 \equiv 8 \ mod \ 11$

$2^4 = 16$ e $16 \equiv 5 \ mod \ 11$

$2^5 = 32$ e $32 \equiv -1 \ mod \ 11$

A congruência $2^5 \equiv -1 \ mod \ 11$ nos dá um resultado muito interessante, bastando agora aplicar a *Propriedade* 8.1.7. e teremos:

$2^5 \equiv -1 \ mod \ 11 \Longrightarrow (2)^{5.40} \equiv (-1)^{40} \ mod \ 11 \Longrightarrow 2^{200} \equiv 1 \ mod \ 11.$

Agora, utilizando as congruências $2 \equiv 2 \ mod \ 11$ e $2^{200} \equiv 1 \ mod \ 11$, e aplicando a *Propriedade* 8.1.6, temos:

$2^{200}.2 \equiv 1.2 \ mod \ 11 \Longrightarrow 2^{201} \equiv 2 \ mod \ 11.$

Portanto, o resto da divisão de 2^{201} por 11 é 2.

Capítulo 9

Considerações

Durante a realização deste trabalho tivemos a convicção da relevância dos conteúdos trabalhados em Aritmética, e em especial o Algoritmo da Divisão de Euclides, para a formação do docente de Matemática.

Esperamos que o presente trabalho auxilie o professor de Matemática a utilizar tais conteúdos e conceitos abordados, não com a mesma complexidade empregada aqui, mas de tal modo que seus alunos consigam compreender.

Acreditamos que a abordagem feita estimule o docente a estudar e pesquisar os conceitos desenvolvidos e outros mais que tenha interesse em conhecer.

Por fim, supomos que tal trabalho ajude os professores de Matemática em sala de aula para que esses se sintam seguros em relação aos conceitos aqui vistos. Incentivando-os a lançar um novo olhar sobre o tratamento de alguns conceitos matemáticos abordados e discutidos.

Referências Bibliográficas

AABOE, A. *Episódios da história antiga da matemática*. 3.ed. Rio de Janeiro: SBM, 2013.

BOYER, C. B. *História da matemática*. 2.ed. São Paulo: Edgard Blücher, 1996.

BRASIL. Ministério da Educação e Cultura(MEC). Secretaria de Educação Fundamental. *Parâmetros Curriculares Nacionais:* matemática. (3º e 4º ciclos do ensino fundamental). Brasília, 1998.

COUTINHO, S. C. *Números inteiros e criptografia RSA*. 2.ed. Rio de Janeiro: IMPA, 2011.

HEFEZ, A. *Elementos de aritmética*. 2.ed. Rio de Janeiro: SBM, 2011.

IEZZI, G.; DOMINGUES, H. H. *Álgebra moderna*. 4.ed. São Paulo: Atual, 2003.

LIMA, E. L. et al. *A matemática do ensino médio* 9.ed. Rio de Janeiro: SBM, 2006. v.1

MUNIZ NETO, A. C. *Tópicos de matemática elementar:* teoria dos números. Rio de Janeiro: SBM, 2012.v.5

OLIVEIRA, K. I. M.; FERNÁNDEZ, A. J. C. *Iniciação à matemática:* um curso com problemas e soluções. 2.ed. Rio de Janeiro: SBM, 2012.

ROQUE, T.; CARVALHO, J. B. P . *Tópicos de história da matemática*. Rio de Janeiro: SBM, 2012.

SANTOS, J. P. O. *Introdução à teoria dos números*. 3.ed. Rio de Janeiro: IMPA, 2005.