UNIVERSIDADE FEDERAL DE CAMPINA GRANDE
Programa de Pós-Graduação em Matemática
Mestrado Profissional - PROFMAT/CCT/UFCG

Um Estudo Sobre Aplicação do Algoritmo de Euclides

Alecio Soares Silva

Trabalho de Conclusão de Curso

Orientador: Prof. Dr. Bráulio Maia Junior

Campina Grande - PB
Agosto/2014

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA CENTRAL DA UFCG.

S586e Silva, Alecio Soares.

Um Estudo Sobre Aplicação do Algoritmo de Euclides /
Alecio Soares Silva.
Campina Grande, 2014.
60f.:il.color.
Trabalho de Conclusão de Curso - Universidade Federal
de Campina Grande, Centro de Ciências e Tecnologia.
Orientação: Prof. Dr. Bráulio Maia Junior.
Referências.
1. Algoritmo de Euclides 2. MDC 3. Reações Químicas
I.Um Estudo Sobre Aplicação do Algoritmo de Euclides.

CDU-510.5(043)

UNIVERSIDADE FEDERAL DE CAMPINA GRANDE
Programa de Pós-Graduação em Matemática
Mestrado Profissional - PROFMAT/CCT/UFCG

Um Estudo Sobre Aplicação do Algoritmo de Euclides

por

Alecio Soares Silva †

Trabalho de Conclusão de Curso apresentado ao Corpo Docente do Programa de Pós-Graduação em Matemática - CCT - UFCG, na modalidade Mestrado Profissional, como requisito parcial para obtenção do título de Mestre.

†Bolsista CAPES

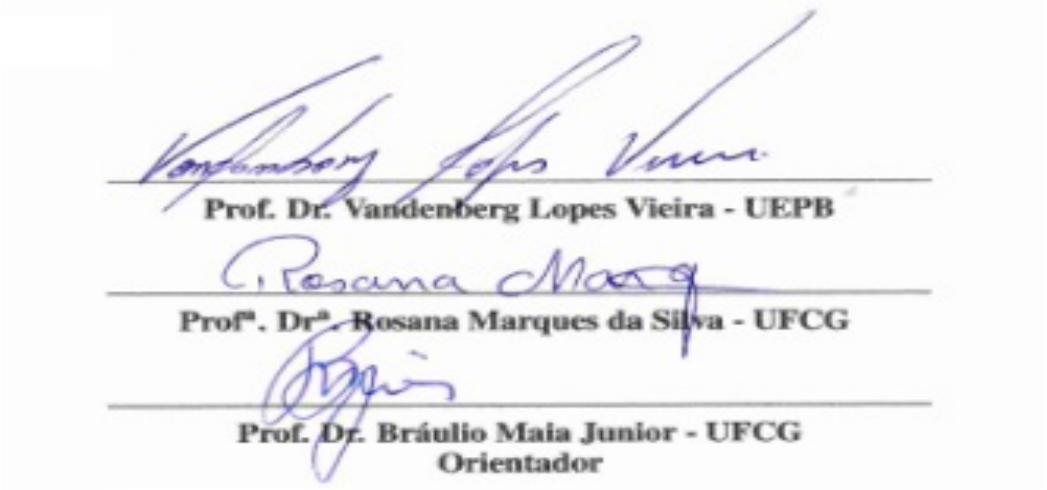
Um Estudo Sobre Aplicação do Algoritmo de Euclides

por

Alecio Soares Silva

Trabalho de Conclusão de Curso apresentado ao Corpo Docente do Programa de Pós-Graduação em Matemática-CCT-UFCG, Modalidade Mestrado Profissional, como requisito parcial para obtenção do título de Mestre.

Aprovado por:



Universidade Federal de Campina Grande
Centro de Ciências e Tecnologia
Unidade Acadêmica de Matemática
Curso de Mestrado Profissional em Matemática em Rede Nacional

Agosto/2014

Dedicatória

A meu querido írmão Almicio *(in memorian)*, por tudo que ele pôde me proporcionar durante o tempo que esteve ao meu lado, tanto amor, carinho, atenção, respeito e imensa dedicação.

Agradecimentos

Primeiramente a Deus, pela sua divina misericórdia e por tudo de tão maravilhoso quanto nos tem dado.

À minha família, pai , mãe, irmãos, tias pelo companheirismo, apoio e admiração que transcendem nossos laços sanguíneos.

Prof. Dr. Bráulio Maia Junior, meu orientador, pela sua sabedoria, paciência, pelo modo respeitoso e dedicado de orientar.

Ao Professor Urânio, por toda sua sabedoria, sua disposição, pela incomensurável contribuição dada na produção deste trabalho.

Aos Professores Vandenberg Lopes e Rosana Marques por terem aceitado participar da Banca Examinadora, assim como por toda contribuição por eles dada.

A todos meus amigos do Mestrado turma 2012, Flávio, Fernando, Carlos André, Marcos, Michele, Vandenberg, Damião, Jorge Porto, Jorge Luiz, Edson, Emerson, João, pelos momentos de troca, pela grande ajuda em momentos difíceis, por todos os momentos que pudemos compartilhar, risos e tanto companheirismo.

A meus amigos Ailton, Francisco, Angélica, Maria, Rosimere, Rostand, Dona Maria pelo carinho, Força, apoio e toda ajuda que puderam dispor.

À Escola Estadual Walnyza Borborema Cunha Lima pelo apoio e pela liberação parcial de minha carga horária semanal para que eu pudesse me dedicar ao PROFMAT.

Por fim, agradeço à Sociedade Brasileira da Matemática - SBM pelo oferecimento deste Curso em Rede Nacional e à CAPES pela concessão da bolsa.

Resumo

Neste trabalho consideramos o uso de algoritmo de Euclides com o intuito de aplicá-lo de uma forma interdisciplinar. Para atingir este objetivo construimos o conjunto dos números naturais, com base nos quatro axiomas de Peano e o conjunto dos inteiros por uma relação de equivalência específica. Além disto, fizemos um estudo de algumas propriedades aritméticas dos números inteiros, bem como do magnífico algoritmo de Euclides. Em seguida utilizamos este algoritmo como uma ferramenta para calcular o maximo divisor comum (MDC) de números inteiros e a partir do MDC estudamos a resolução de equações lineares diofantinas, as quais foram empregadas para fazer o balanceamento de Reações Quimicas.

Palavras-Chave: Algoritmo de Euclides. MDC. Reações Químicas.

Abstract

In this work we consider the use of the Euclid's algorithm in order to apply it in an interdisciplinary way. To achieve this we constructed the set of the natural numbers based on the four Peano axioms and the set of integers by a specific equivalence relation. Moreover, we have studied some arithmetic properties of integers, as well as the magnificent Euclidean algorithm. We then use this algorithm as a tool to calculate the Greatest Common Divisor (GCD) of integers and from this study the resolution of Diophantine linear equations, which were employed to do the balance of Chemical Reactions.

Keywords: Euclidean Algorithm. GCD. Chemical Reaction.

Sumário

Capítulo 1

Introdução

O objetivo principal deste Trabalho de Conclusão de Curso é contribuir para uma melhor compreensão do processo de ensino-aprendizagem de algumas aplicações do Algoritmo de Euclides. Nesse sentido fizemos uma aplicação para encontrar Máximo Divisor Comum, usando o resultado estudado como uma ferramenta para resolver Equações Diofantinas Lineares e tais equações como mecanismo para balancear equações químicas.

Sendo assim, buscamos atingir os objetivos de apresentar uma proposta de estudo, mediante uma construção desde o conjunto dos números naturais, conjunto dos números inteiros até uma aplicação do conteúdo na disciplina de Química, buscando encontrar uma contextualização na disciplina de Química, pois assim como pode ser visto nas Orientações Curriculares para o Ensino Médio [2], página 37, "Um primeiro passo, que pode ser produtivo e conduzir posteriormente à interdisciplinaridade sistêmica, é a abordagem simultânea de um mesmo assunto por diferentes disciplinas". Desta maneira, articulando os conteúdos de forma que os alunos possam perceber a utilidade do Algoritmo de Euclides, bem como facilitar o processo de balanceamento de equações químicas.

Justifica-se esta proposta de trabalho lembrando de uma pergunta, muito frequente, durante a aula de matemática. Quando um aluno diz:

"Professor, para que serve o conteúdo da aula de hoje?"

É indiscutível que tal pergunta não pode deixar de ser respondida de maneira convincente, pois, caso contrário, para que se ensina o conteúdo em discussão? Com certeza, uma aplicação de um conteúdo em uma situação cotidiana ou em outra área do conhecimento serve para motivar o aluno no que se refere a perceber o sentido do que se está aprendendo, todavia não esquecendo que o ensino de matemática tem como base a formação do pensamento. Desta maneira, os procedimentos metodológicos que nortearam este trabalho têm como caminho a pesquisa bibliográfica, tendo como base várias obras sobre *Aritmética e Álgebra* [6, 5, 10, 9], como também o uso de algumas obras sobre o ensino de química, [4, 12],

direcionadas ao ensino médio ou superior.

Em vista deste caminho, sugerimos uma proposta para o ensino-aprendizagem de um estudo sobre números inteiros, partindo da ideia de que o aprendizado se dá de maneira mais eficaz, quando o aluno consegue perceber o sentido e a importância dos conceitos matemáticos envolvidos em situações concretas.

1.1 Objetivos

Este Trabalho tem por objetivo geral contribuir com o processo de ensino aprendizagem de aplicações do Algortitmo da Divisão de Euclides, dentre as quais cálculo do *MDC* e resoluções de Equações Diofantinas Lineares, aplicando estas equações como ferramenta no processo de balanceamento de equações químicas.

E como objetivos específicos:

- Construir de maneira formal o conjunto dos números naturais;
- Construir de maneira formal o conjunto dos números inteiros;
- Estudar propriedades aritméticas relativas aos números inteiros;
- Calcular o M.D.C de números inteiros usando o Algoritmo de Euclides;
- Propor maneiras de encontrar soluções de Equações Diofantinas Lineares;
- Mostrar uma aplicação do conteúdo no processo de balanceamento de equações químicas.

1.2 Metodologia

Na elaboração deste trabalho, realizamos uma pesquisa de caráter bibliográfico, buscando elementos para sua fundamentação. Atentamos para que fosse feita uma aplicação do conteúdo contextualizando em outra área do conhecimento para denotar sua relevância.

1.3 Público Alvo

Partindo do pressuposto de que o conteúdo de conjuntos numéricos é tratado no Ensino Médio, 1º ano, este Trabalho é direcionado a Professores de Matemática e Química da educação básica e alunos do ensino médio, para que possam consultar durante suas pesquisas diárias, já que nele sugerimos uma abordagem conveniente para o balanceamento de

equações químicas, usando Equações Diofantinas Lineares como aplicação do Algoritmo Euclidiano da Divisão.

Capítulo 2

Um Pouco de História da Matemática

2.1 Egito e Mesopotâmia

Ao falarmos da matemática ensinada na escola básica, nos remetemos, fundamentalmente, a quatro áreas sobre as quais sempre se ouve falar: a aritmética, a álgebra, a geometria e a trigonometria. Neste trabalho faremos um estudo sobre o Algoritmo de Euclides, usando-o como ferramenta no cálculo do Máximo Divisor Comumm e nas soluções Equações Diofantinas Lineares. A fim de melhor compreendermos a temática, exploraremos momentos históricos que descrevem o desenvolvimento da notação algébrica, bem como alguns momentos da história de Euclides e Diofanto. Mais detalhes podem ser consultados em Boyer [1], Eves [3] e Pitombeira [13].

Sabemos que os textos matemáticos mais antigos, dentre os que conhecemos atualmente, tais como, o Papiro de Rhind ver Fig. 2.1 e o Osso de Ishango, ver Fig. 2.2, entre outros, remetem ao povo Mesopotâmico.

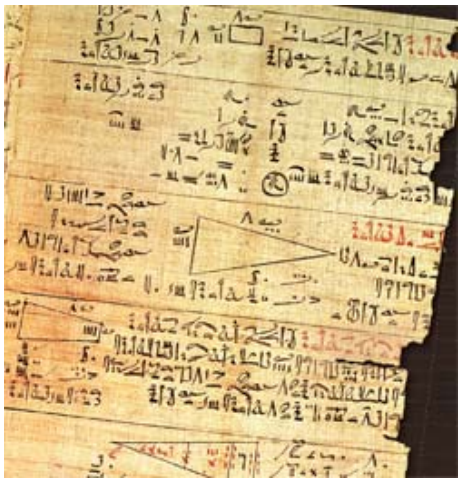


Figura 2.1: Papiro de Rhind. Foto: Egyptian/Getty Images [15].

Tais textos geralmente eram gravados em tabletes de argila e papiros ou em tábuas. Os seus conteúdos nos trazem uma grande variedade de problemas algébricos escritos e resolvidos em linguagem coloquial. Tais resoluções eram apenas uma sequência de procedimentos, verificando casos particulares destes problemas, onde eram usados exemplos e o que importava era o procedimento aplicado.

Figura 2.2: Osso de Ishango exposto no Real Instituto Belga de Ciências Naturais [16].

Existiam vários problemas semelhantes, isto é, um problema de cada tipo era resolvido para vários conjuntos de dados, os quais eram resolvidos aplicando-se o mesmo processo até que se pudesse compreender o algoritmo. Mas, em momento algum era feita uma verificação de que os resultados alcançados valiam para problemas semelhantes. Percebia-se a generalidade pelo número de exemplos feitos.

Nessa época, portanto, os componentes de um problema eram expostos de maneira retórica, ou seja, todo problema e o procedimento ou algoritmo para sua resolução era feito por textos em prosa. Assim, dizemos que a notação algébrica esteve no período da notação retórica. A transição do período retórico para um novo período de notação algébrica ocorreu após as contribuições feitas por vários matemáticos, dentre eles Euclides e Diofanto.

Nos problemas mesopotâmicos e egípcios, eram realizados cálculos com medidas de comprimentos, áreas e volumes. Logo, estas práticas exerceram certa influência sobre a geometria grega. Na qual os problemas geométricos eram transformados em problemas numéricos. Era esccolhida uma unidade de medida para converter um comprimento, uma área ou um volume em um número e realizar o cálculo. Certamente, os primeiros matemáticos gregos, tratavam a geometria de forma semelhante aos antigos egípicios e mesopotâmicos baseados em cálculos de medidas, porém, não existem fontes confiavéis sobre a relação entre a Matemática mesopotâmica e egípcia com a Matemática grega.

2.2 Euclides e os Elementos

Euclides foi um matemático que teve sua carreira na cidade grega de Alexandria, embora não possamos afirmar com precisão a cidade de seu nascimento, muito menos a época em que viveu. Segundo alguns historiadores, Euclides foi um dos grandes professores da famosa escola de matemática de Alexandria, conhecida segundo Boyer [1], página 74, como "Museu". Ele é autor de algumas publicações sobre matemática, música astronomia e tantas outras áreas do conhecimento, dentre as quais, a geometria com destaque para *Os Elementos*, uma coleção formada por treze livros, que datam aproximadamente do ano 300a.C., trazem resultados, organizados sistematicamente, muitos atribuídos a outros matemáticos, alguns anteriores a Euclides.

Ao contrário do que muitos pensam, Os Elementos não tratam apenas de geometria. Em suas 465 proposições figuram textos sobre teoria dos números e álgebra elementar. Os treze volumes desta publicação estão divididos da seguinte maneira:

- Livros I-VI Geometria plana;
- Livros VII-IX Aritmética;
- Livros XI-XIII Geometria espacial.

A grande inovação feita por Euclides, nos Elementos, é a adoção do método axiomático-dedutivo, no qual, partindo de alguns conceitos primitivos, aceitos como triviais ou intuitivos, demonstram-se consequências chamadas de teoremas ou proposições.

No início do livro VII, Euclides expõe o processo conhecido hoje, como Algoritmo Euclidiano da divisão, bem como o processo para encontrar o Máximo Divisor Comum de dois ou mais números inteiros. Tais procedimentos servem de base para outros procedimentos como o procedimento usado para resolver uma Equação Diofantina Linear.

2.3 Diofanto e a Arithmética

Sobre o matemático Diofanto também não podemos afirmar com precisão a cidade de seu nascimento. Sabemos apenas que a sua atuação se deu na cidade grega de Alexandria e por tal fato, ficou conhecido como Diofanto de Alexandria. Também não podemos afirmar nada sobre a época em que viveu, todavia alguns historiadores o situam nos meados do século III, o que parece ser bastante razoável, já que por um lado Diofanto cita em sua obra Hipsicles (240 - 170 a.C.) um geômetra e astrônomo da cidade de Alexandria, certamente tendo vivido após 150 a.C. Por outro lado, Diofanto é citado pelo também geômetra e astrônomo Teon, que viveu na cidade de Alexandria. Logo, Diofanto deve ter vivido antes de 365 d.C.

Diofanto de Alexandria por muitos é considerado pai da álgebra, tal designação se dá pela grande contribuição dada por ele no período de transição da álgebra retórica para álgebra sincopada explicitada em sua obra. Transição que levou a notação algébrica para um novo estágio cujas representações são usadas atualmente pela álgebra moderna.

Sua obra é composta por três publicações:

1-**Arithmética;**

3-**Uma obra sobre números poligonais;**

2-**Porismas.**

Dentre estas obras a Arithmética é a principal. Este tratado é uma coleção de treze livros dos quais os seis primeiros se preservaram, sobrevivendo ao tumulto da idade das trevas (400-1000 d.C.), período histórico caracterizado pela estagnação cultural européia após a queda do império romano.

A coleção com os treze volumes de sua obra esteve durante quase toda era clássica (VI - IV a. C.), desde sua publicação, na biblioteca de Alexandria, cidade que durante muitos séculos foi considerada a capital intelectual do mundo civilizado. Porém, esteve sob ameaça de ataques estrangeiros, como o primeiro deles que ocorreu em 47 a.C.. quando Júlio César, Imperador Romano, tentou derrubar a rainha do Egito, nesse período, Cleópatra, e acabou incendiando a biblioteca de Alexandria, queimando centenas de milhares de obras, dentre elas algumas da coleção dos treze livros da Arithmética.

O segundo ataque ocorreu em dois momentos: um no ano de 389, quando o imperador Teodósio ordenou que Teófilo destruísse todos os símbolos pagãos. Infelizmente, após o ataque anterior feito por Júlio Cesar, Cleópatra reconstruiu a biblioteca, no templo de Serápis, divindade egípcia pagã, sendo então a biblioteca jogada no meio da destruição. O outro momento foi no ano de 642 quando o califa Omar invadiu com os muçulmanos e dominou Alexandria, ordenando que todos os livros que fossem contra o *Alcorão*, livro sagrado para os muçulmanos, fossem destruídos. Restando após estes brutos ataques apenas seis volumes da Arithmética de Diofanto.

A obra Arithmética não é uma exposição sobre as operações algébricas ou sobre as funções algébricas. É, na verdade, uma coleção de aproximadamente cento e cinquenta problemas, dos quais alguns são problemas já conhecidos na época e outros são problemas novos criados por Diofanto. Todos eles foram expostos, como forma de exemplos e estudados em termos numéricos específicos, são problemas envolvendo vários números, expressando, sempre que possível, todos em termos de apenas um.

Muitos dos problemas tratados na Arithmética conduzem à equações do 1^o e 2^o graus,

a uma ou mais de uma incógnita, determinadas ou não; outros referem-se à equações cúbicas, mas para estas equações, Diofanto escolhe adequadamente os dados para que seja fácil obter a solução. Mas há também problemas algébricos que ele resolve com recurso da geometria.

Na obra Arithmética também não é feita uma distinção entre problemas determinados e indeterminados e, nestes indeterminados, mesmo quando as equações possuíam infinitas soluções, aparecia apenas uma solução particular. O caráter desta obra de Diofanto é mais para teoria dos números do que para própria álgebra, pois Arithmética é, na verdade, uma abordagem analítica à teoria algébrica dos números. Mesmo assim, sua produção representa um momento de evolução da álgebra no que se refere à notação, um momento de transição entre a álgebra retórica dos babilônicos e a notação moderna essencialmente simbólica das funções, equações, etc. usadas atualmente.

O único detalhe sobre a vida de Diofanto que restou foi uma inscrição em prosa que pode ser encontrada em Boyer [1], página 130, que dizem ter sido gravado na lápide de seu túmulo. Nessa referênciia, tal inscrição foi traduzida em:

"Deus lhe concedeu ser um menino pela sexta parte de sua vida, e somando uma duodécima parte a isso cobriu-les a face de penugem. Ele acendeu a lâmpada nupcial após uma sétima parte, e cinco anos após seu casamento, concedeu-lhe um filho. Ai! Infeliz criança tardia; depois de chegar a metade da vida de seu pai, o destino frio o levou. Depois de se consolar de sua dor durante quatro anos com a ciência dos números ele terminou sua vida".

O desafio é calcular a idade de Diofanto. Em Boyer [1], página 130, encontramos a seguinte afirmação: "Este enigma é historicamente exato, pois Diofanto viveu oitenta e quatro anos". Tal problema pode ser resolvido com simplicidade usando a notação algébrica moderna:

$$\frac{x}{6}+\frac{x}{12}+\frac{x}{7}+5+\frac{x}{2}+4=x\Rightarrow x=84.$$

Mas este tipo de problema não interessava a Diofanto, já que este deu pouca atenção às equações do primeiro grau. Este matemático é mais conhecido por uma classe especial de equações que leva seu nome *Equações Diofantinas*.

2.4 O Último Teorema de Fermat

Diofanto estudou apenas alguns casos particulares de algumas das Equações Diofantinas, usando como universo os números racionais positivos. A mais famosa de todas estas equações é a conhecida como *O Último Teorema de Fermat*, por conta de notas feitas em uma das edições da Arithmética, que fora traduzida para o latim por Bachet, em 1621, um

brilhante linguístico, poeta estudioso dos clássicos e que também era fascinado por problemas matemáticos, assim como podemos ver em Singh [14]. Alguns historiadores apontam que esta obra foi impressa e republicada de maneira descuidada em 1670, por um dos filhos de Fermat, após sua morte. Mas, mesmo assim, seu valor histórico é bastante alto, pois esta foi uma contribuição significativa para a segunda era de ouro da matemática.

Estas anotações, feitas nas margens das páginas do livro Arithmética, foram feitas por Pierre de Fermat, Fig. 2.3, um jurista Francês, servidor público nomeado conselheiro do parlamento de Toulouse. Nascido em 1601 filho de um rico mercador de peles, tinha por hobby formular problemas matemáticos, dos quais quase nunca apresentava as soluções, para desafiar matemáticos profissionais de sua época os resolvessem.

Figura 2.3: Pierre de Fermat. [14]

Mesmo Fermat não sendo matemático de ofício, publicou vários trabalhos sobre matemática, além de alguns não publicados, como em 1629, quando descreveu as suas ideias num trabalho não publicado intitulado *Introdução aos lugares geométricos planos e sólidos*, que circulou na sociedade francesa apenas na forma de manuscrito e é considerado por alguns historiadores como a invenção da geometria analítica. A tradução da obra Arithmética feita por Bachet, tinha largas margens e uma anotação feita em uma destas margens carregou o nome por bastante tempo de *O Último Teorema de Fermat*. Podemos encontrar esta inscrição em Singh [14], página 80, onde lê-se:

É impossível para um cubo ser escrito como a soma de dois cubos ou uma quarta potência ser escrita como a soma de dois números elevados a quatro, ou em geral, para qualquer número que seja elevado a uma potência maior que dois ser escrito como a soma de duas potências semelhantes.

Esta anotação foi feita no livro dois da Arithmética, em uma seção onde Diofanto havia feito várias observações sobre o Teorema de Pitágoras e os trios pitagóricos, trios de números que satisfazem ao Teorema de Pitágoras. Fermat fez esta anotação na margem desta página.

O problema pode ser reformulado como "não existem soluções com números inteiros não nulos para equação $x^n + y^n = z^n$, na qual n seja qualquer número inteiro maior que

dois". Note que excluindo o valor zero como possibilidade para x, y ou z estamos excluindo soluções triviais como $x = y = z = 0$, $x = 0$, com $y = z$ e $y = 0$ com $x = z$, já que tal problema sem estas restrições se tornaria bastante simples. Sendo assim, com o passar dos anos esta equação diofantina se tornou um problema que, com certeza, é um dos maiores problemas de matemática de todos os tempos, tornando-se pesadelo para muitos matemáticos que tentaram resolvê-lo.

Para um olhar mais rigoroso, o Último Teorema de Fermat era, na verdade, somente uma conjectura, já que Fermat apenas sugere em uma nota feita ainda na margem da página do livro, onde fizera a anotação anterior dizendo que possui uma demonstração, mas não explicita se quer como abordar tal problema.

Alguns historiadores, assim como Boyer [1] ou Eves [3], duvidam se Fermat realmente tinha uma demonstração para tal conjectura e, além disso, discute-se também se, caso Fermat tivesse realmente uma demonstração estaria esta correta já que este problema foi solucionado anos depois.

A tarefa de resolver esta equação diofantina seduzia os matemáticos profissionais e também matemáticos amadores. Talvez por sua simplicidade no enunciado pudesse ser entendida de maneira simples. Mesmo assim, apenas cem anos depois, alguém conseguiria dar um primeiro passo na tentativa de resolvê-lo. Foi o Matemático Suíço Leonard Euler, Fig. 2.4, nascido na cidade da Basiléia e filho de um pastor protestante, que após passar um tempo trabalhando para os Czares na antiga Prússia, tormou-se professor na Academia de Berlin convidado pelo rei da Prússia, conhecido como Frederico, o Grande, título devido ao sucesso militar que transformara a Prússia em uma potência europeia.

Figura 2.4: Leonard Euler. [14]

As publicações de trabalhos de Euler se deram em todas as áreas da matemática. Mesmo sendo cego de um olho e depois de algum tempo perdendo visão do outro olho o que não se tornou um obstáculo para ele. Alguns historiadores afirmam que a maior produção dos trabalhos de Euler se deu após ele ter perdido a visão dos dois olhos o que era justificado pela memória fenomenal que possuía.

Euler estudando anotações feitas na edição da Arithmética resolveu atacar o problema

usando uma ideia onde Fermat mostrava que não existem soluções para equações do tipo $x^n + y^n = z^n$, no caso $n = 4$, então ele usou tal demonstração como ponto de partida podendo provar que a o raciocínio de Fermat vale também para o caso $n = 3$, precisando para conseguir tal prova incorporar o conceito bizarro para época, de número imaginário sugerido pelo matemático italiano Rafaello Bombeli criador da unidade imaginária $i = \sqrt{-1}$.

Os casos da resolução provados por Euler fizeram com que a solução para o problema parecesse não estar tão distante, pois os casos em que $n = 8, 12, 16, 20, ...$ são casos que podem ser escritos sem problema algum como uma potência de expoente 4, bem como os casos em que $n = 6, 9, 12, 15, ...$ também podem ser escritos como potências de expoente 3. Resumindo o problema em provar de que vale para qualquer número primo maior que 3. O problema se tornava a cada dia mais famoso e sua solução parecia estar muito próxima e, ao mesmo tempo, muito distante. Foram oferecidos vários prêmios para quem conseguisse o demonstrar. Sendo assim, muitos matemáticos, como o americano Ken Ribet, que mostrou que o teorema de Fermat era um resultado da Conjectura de Taniyama-Shimura, provando que cada curva elíptica se relacionava com uma forma modular, tentaram resolvê-lo, como podemos ver em Singh [14].

Mas somente na década de 90, como pode ser visto em Singh [14], o Matemático britânico e professor da Universidade de Princeton, Andrew Wiles, Fig. 2.5, depois de vários anos de estudos e uma tentativa frustrada em 1993, na qual havia cometido um erro na sua demonstração, conseguiu resolver este problema.

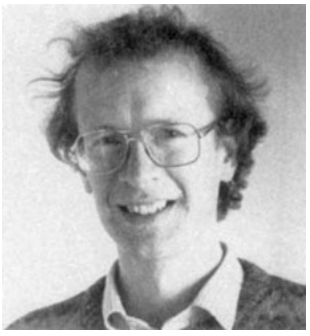


Figura 2.5: Professor Andrew Wiles. [14]

A demonstração para tal teorema que passou a ser chamado de Teorema de Fermat-Wiles, foi feita em dois trabalhos produzidos por Wiles e Richard Taylor, nos quais utilizaram argumento semelhante ao usado por Wiles na sua palestra em 1993, mas esta nova abordagem foi feita de maneira mais simples, e foi desta forma que foi resolvida a mais famosa Equação Diofantina de todos os tempos.

Capítulo 3

O Conjunto $\mathbb{N}$ dos Números Naturais

Neste capítulo faremos a construção do conjunto dos números naturais baseados nos quatro axiomas de *Peano*. Sabemos que alguns autores consideram que o número zero não pertence a $\mathbb{N}$, porém por uma questão de conveniência outros preferem considerar que o número zero pertence a esse conjunto. Neste trabalho faremos a construção de tal conjunto aceitando que o zero está incluído nele, assim como pode ser visto em Ferreira [5]. Definiremos também, as operações de adição, multiplicação, a relação de ordem e algumas propriedades de $\mathbb{N}$. Contudo o leitor interessado pode consultar uma construção dos naturais, na qual o número zero não está incluído, em Lima [9].

3.1 Número Natural

Número natural é o resultado da operação de comparação entre uma grandeza e a unidade de medida. É fato que quando esta grandeza é discreta dizemos que a comparação é uma contagem e que o resultado desta é um número natural. Assim, portanto, fica claro que a principal função dos números naturais está relacionada com o modelo de contagem. Sabemos que junto ao desenvolvimento da civilização houve também o desenvolvimento da necessidade de contar objetos. Porém estas contagens sofreram grandes mudanças na forma que eram executadas. Segundo Lima [9], na página 34, "As tribos, mais rudimentares contam apenas um, dois, muitos". Contudo a necessidade criada pelos avanços sociais levaram o homem a desenvolver um instrumento extraordinário para contar, conhecido como o conjunto dos números naturais.

A partir de agora representaremos por $\mathbb{N}$ o conjunto cujos elementos são números naturais. Em $\mathbb{N}$ temos que a principal ideia é a de sucessor, entenderemos que sucessor é aquele que aparece logo após. Lima [9], página 35, e Ferreira [5], página 15, citam que o matemático Italiano Giuseppe Peano sintetizou de forma concisa e precisa uma maneira de

descrever tal conjunto baseado basicamente em quatro axiomas, os quais ficaram conhecidos como Axiomas de Peano. Estes axiomas são as regras básicas para construção de $\mathbb{N}$. Usaremos a notação A_1, A_2, A_3, A_4 para identificá-los, e os elencaremos em seguida:

A_1 – *Todo número natural tem um único sucessor;*
A_2 – *Números naturais diferentes possuem sucessores diferentes;*
A_3 – *Existe um único número natural, chamado de "zero" e representado pelo símbolo 0, que não é sucessor de nenhum outro;*
A_4 – *Seja X um conjunto de números naturais (isto é, $X \subset \mathbb{N}$). Se $0 \in X$ e se além disso, o sucessor de todo elemento de X ainda pertencer a X, então temos que $X = \mathbb{N}$.*

Até os dias atuais afirmamos que tudo que se sabe sobre os números naturais pode ser demonstrado como conseqüência destes quatro axiomas. Baseando-nos, no sistema de numeração decimal com auxílio dos dez símbolos $0,1,2,3,4,5,6,7,8,9$, podemos representar qualquer número natural. Assim como qualquer outro objeto os números naturais possuem nomes: Como vimos aquele que não é sucessor de nenhum outro chama-se "zero", seu sucessor chama-se "um" e é representado pelo símbolo 1, o sucessor de um chama-se "dois" e é representado pelo símbolo 2, o sucessor do dois chama-se "três" e é representado pelo símbolo 3 e assim sucessivamente, até que os nomes dos números se tornam bastante complicados.

Assim, segue que o conjunto dos números naturais é:

$$\mathbb{N} = \{0,1,2,3,4,5,6,7,8,9,10...\}.$$

Precisamos ainda ter clareza de que tal conjunto a princípio é vazio de significado, pois cada um dos números é elemento abstrato dessa sequência.

Usaremos a notação $s(n)$, para reprensentar o sucessor do número natural n. Este "s" foi escolhido apenas por ser a primeira letra da palavra sucessor.

3.2 O Quarto Axioma de Peano (Axioma da Indução)

Dos quatro axiomas citados um deles precisa de atenção especial. O quarto axioma é também conhecido como axioma A_4 da indução. E este é a base para um dos métodos mais eficientes de demonstrações matemáticas que envolvem o conjunto dos números naturais. A prova por indução é uma forma poderosa de demonstração para uma propriedade matemática que vale no conjunto dos números naturais, porque esta técnica permite provar que uma declaração é válida para um número infinito de casos, demonstrando apenas um único caso. De forma grosseira o Axioma da Indução baseia-se em provar que a declaração vale para o

número 0, depois para o número 1, depois para o número 2 e assim por diante para todos os números naturais. Resumidamente é necessário provar que se $n \in \mathbb{N}$ e a declaração vale para n, então a declaração vale também para o sucessor de n. Podemos enunciar o *Axioma da Indução* em forma de propriedade da seguinte maneira:

Consideremos $n, s(n) \in \mathbb{N}$ e $P(n)$ uma propriedade mátemática válida para n.
Suponhamos que:
$P(0)$ é válida;
Para todo $n \in \mathbb{N}$, a validez de $P(n)$ implica a validez de $P(s(n))$.

Então podemos afirmar que $P(n)$ é válida para qualquer número natural. Percebemos que se chamarmos de X o conjunto cujos elementos são os números naturais n para os quais $P(n)$ é válida, temos que:
(i) Afirma que $0 \in X$ e (ii) afirma que, se $n \in X$, então $s(n) \in X$. Logo pelo axioma da indução, podemos concluir que $X = \mathbb{N}$.

O axioma da indução basicamente é uma forma de dizer que qualquer número natural n pode ser alcançado a partir do número 0 apenas tomando várias vezes os sucessores até chegar a n.

Singh [14], página 219, faz uma analogia para o princípio da indução matemática que diz que outra maneira de pensar na prova por indução é imaginar o número infinito de casos como uma fila infinita de dominós. E que para provar cada um dos casos é preciso derrubar todos os dominós desta fila. É claro que derrubar um por vez levaria uma quantidade infinita de tempo e esforço, mas a prova por indução permite que os matemáticos derrubem todos os dominós derrubando apenas o primeiro, já que cada dominó derrubará seu sucessor na fila.

Daí verificamos que o axioma da indução está presente sempre que dizemos "tal proposição" vale para $n = 0$, $n = 1$, $n = 2$, $n = 3$ e assim por diante.

3.3 Adição e Multiplicação de Números Naturais

Podemos definir a adição e a multiplicação de números naturais usando recorrência, assim como Lima [9].

Definição 3.1 *Dados $m, n \in \mathbb{N}$, a adição entre m e n, pode ser denotada por $m+n$ e se define por recorrência, a partir dos seguintes dados:*
(i) $m+0 = m$;
(ii) $m+s(n) = s(m+n)$.

O item (ii) da definição 3.1, nos permite conhecer $m+n$ para quaisquer $m, n \in \mathbb{N}$. Assim, temos ainda que sendo $m \in \mathbb{N}$ um número arbitrário, então:

$$m+s(s(n)) = s(m+s(n)) = s(s(m+n)) \quad \text{e assim por diante.}$$

Podemos validar este processo usando o axioma A_4, da seguinte forma:
Consideremos o conjunto

$$S = \{n \in \mathbb{N}, \text{ tal que}, m+n, \text{está bem definida}\}.$$

Segue que $0 \in S$, pois tomando um natural arbitrário m, temos pela definição, $m = m+0$. Temos ainda que $1 \in S$, pois como m é um número natural arbitrário, pelo primeiro axioma de Peano, o sucessor de m também será um número natural, isto é, o número $m+1 \in \mathbb{N}$, logo a soma $m+1$ está bem definida em $\mathbb{N}$. Desta forma temos, ainda pelo primeiro axioma de Peano, que $s(0) \in S$ e se $k \in S$ temos que $s(k) \in S$, e $m+s(k) = s(m+k)$, logo por A_4 temos que $S = \mathbb{N}$. Ou seja, para m arbitrário a soma $m+n$ está bem definida para quaisquer $m, n \in \mathbb{N}$.

Podemos definir a multiplicação de dois números naturais de maneira análoga a definição dada para adição. Fixando arbitrariamente um número natural k, a multiplicação por k associa a todo número natural n o produto denotado por $n \cdot k$.

Definição 3.2 *Dados $k, n \in \mathbb{N}$. A multiplicação entre k e n pode ser denotada por $k \cdot n$, e se define por recorrência, a partir dos seguintes dados:*
(i) $1 \cdot k = k$;
(ii) $(n+1) \cdot k = k \cdot n + k$.

O produto $n \cdot k$ pode ser também escrito como nk e lê-se "n vezes k". A definição acima diz, portanto, que uma vez k é igual a k e que $(n+1)$ vezes k é igual a n vezes k mais (uma vez) k. Assim, por definição, $2 \cdot k = k+k$, $3 \cdot k = k+k+k$, $4 \cdot k = k+k+k+k$, etc.

Para provar as propriedades básicas da adição e da multiplicação de números naturais podemos usar a indução. Entre elas, destacam-se as seguintes, válidas para quaisquer números $k, n, p \in \mathbb{N}$:

- **Associatividade:** $k+(n+p) = (k+n)+p$ e $k \cdot (n \cdot p) = (k \cdot n) \cdot p$;
- **Comutatividade:** $k+n = n+k$ e $k \cdot n = n \cdot k$;
- **Lei do Cancelamento:** $k+n = k+p \Rightarrow n = p$ e $k \cdot n = k \cdot p \Rightarrow n = p$;
- **Distributividade:** $k(n+p) = k \cdot n + k \cdot p$.

3.4 A Ordem dos Números Naturais

Definida a adição de números naturais podemos introduzir uma relação de ordem neste conjunto.

Definição 3.3 *Dados os números naturais m,n diremos que m é menor do que n, e escreveremos $m < n$, para representar que existe $p \in \mathbb{N}$, com $p \neq 0$, tal que $n = m + p$.*

Neste caso, diz-se também que n é maior do que m e escreve-se $n > m$. A notação $m \leqslant n$ significa que $m < n$ ou $m = n$. Por definição, tem-se portanto $m \leqslant m + p$ para quaisquer $m, p \in \mathbb{N}$. Em particular, $m < m + 1$. Segue-se também da definição que $0 < n$ para todo número natural $n \neq 0$.

Com efeito, pelo Axioma A_3, o número zero não é sucessor de nenhum número natural, o fato de n ser diferente de 0, implica que o número n é sucessor de algum número natural m, ou seja, $n = m + 1$, logo $n > 1 > 0$. Assim, o 0 é o menor dos números naturais.

Apresentaremos a seguir, as propriedades básicas da relação de ordem.

Proposição 3.1 *Se m,n e p são números naturais, então são verdadeiras as seguintes sentenças:*

i) **(Transitividade)** Se $m < n$ e $n < p$, então $m < p$;
ii) **(Tricotomia)** Quaisquer das afirmações $m < n$, $m = n$ e $n < m$, exclui as outras duas;
iii) **(Monotonicidade)** Se $m < n$, então $m + p < n + p$ e $mp < np$;
iv) Não existem números naturais entre n e $n + 1$.

Demonstração. *i*) Se $m < n$, $n < p$ então pela Definição 3.3, existem $k, r \in \mathbb{N}$ tais que, $n = m + k$, $p = n + r$, logo $p = (m + k) + r = m + (k + r)$, portanto $m < p$.

ii) Se tivéssemos $m < n$ e $m = n$, então seria $m = m + p$, cancelando m em ambos os lados da igualdade, concluiríamos que $0 = p$, um absurdo, pois, pela Definição 3.3 $p \neq 0$. Portanto $m < n$ (e analogamente, $n < m$) é incompatível com $m = n$. Do mesmo modo, se tivéssemos $m < n$ e $n < m$, então teríamos $n = m + p$ e $m = n + k$, do que resultaria $n = n + k + p$, logo $n + 1 = n + k + p + 1$ e, cancelando n em ambos os lados da igualdade, concluiríamos que $1 = k + p + 1$, um absurdo.

iii) Usando a Definição 3.3, $m < n \Rightarrow n = m + k \Rightarrow n + p = (m + k) + p \Rightarrow m + p < n + p$. Analogamente: $m < n \Rightarrow n = m + k \Rightarrow np = mp + kp \Rightarrow np > mp$.

iv) Se fosse possível ter $n < p < n + 1$, teríamos então $p = n + k$ e $n + 1 = p + r$, logo $n + 1 = n + k + r$. Cancelado n, obteríamos $1 = k + r$. Por definição, isto significaria $k < 1$, mas, dessa forma, obtemos $k = 0$ e assim, $p = n$ contrarindo o fato de $n < p$. □

Proposição 3.2 *Dados $a, b, c \in \mathbb{N}$, valem as seguintes propriedades:*

i) Na adição vale a lei do cancelamento, com respeito a relação "menor que". Isto é,

$$a < b \Leftrightarrow a + c < b + c;$$

ii) Na adição vale a lei do cancelamento, em relação à igualdade, $a = b$ é equivalente a

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

iii) Na multiplicação vale a lei do cancelamento, com respeito à igualdade, assim temos que,

$$a = b \Rightarrow ac = bc;$$

iv) Na multiplicação vale a lei do cancelamento, com respeito à relação menor do que,

$$a < b \Leftrightarrow ac < bc.$$

Demonstração. *i*) Suponhamos que $a < b$. Logo, existe $d \in \mathbb{N}$, tal que $b = a + d$. Somando c a ambos os lados da igualdade $b = a + d$, obtemos $b + c = (a + d) + c$; Pela propriedade comutativa da adição, $b + c = c + (a + d)$ e pela propriedade associativa da adição, temos, $b + c = (a + c) + d$, donde segue que $a + c < b + c$.

Reciprocamente, suponhamos que $a + c < b + c$. A tricotomia, nos dá três possibilidades:

(a) $a = b$. Isto acarretaria $a + c = b + c$, portanto, falso;

(b) $b < a$. Isto acarretaria, pela primeira parte da demonstração, que $b + c < a + c$; também é falso;

(c) $a < b$. Esta é a única possibilidade que resta.

ii) A implicação, $a = b \Rightarrow a + c = b + c$, é consequência da definição da adição. Suponhamos agora que $a + c = b + c$. Assim restam três possibilidades:

(a) $a < b$. A Proposição 3.1, nos diz que $a + c < b + c$, o que é um absurdo;

(b) $b < a$. Pelo mesmo argumento acima, $b + c < a + c$, o que é também um absurdo;

(c) $a = b$. Esta é a única alternativa válida.

iii) A implicação, $a = b \Rightarrow ac = bc$, decorre imediatamente da definição de multiplicação. Suponhamos agora que $ac = bc$. Temos três possibilidades:

(a) $b < a$. Pelo mesmo argumento acima, $bc < ac$, o que é um absurdo;

(b) $a < b$. Pela Proposição anterior, segue que $ac < bc$, o que é um absurdo;

(c) $a = b$. Está é a única alternativa válida.

iv) Suponhamos que $a < b$. Logo, existe $d \in \mathbb{N}$ tal que $b = a + d$. Multiplicando por c ambos os lados dessa última igualdade, pelas propriedades comutativa e distributiva da multiplicação, decorre que, $bc = cb = c(a + d) = ca + cd = ac + cd$. O que mostra que $ac < bc$, pois, $cd \in \mathbb{N}$.

Reciprocamente, suponhamos que $ac < bc$. Devemos mostrar que $a < b$, para isso, usaremos a tricotomia, gerando três possibilidades:

$a = b$ o que acarreta $ac = bc$, mas pela hipótese isto é falso. Uma outra possibilidade é $b < a$, novamente isto não é possível, pois $b < a$ implica que $bc < ac$, contrariando a hipótese. Por último $a < b$, e esta é a única possibilidade válida. □

3.5 Boa Ordenação

Tomando um subconjunto $A \subset \mathbb{N}$, diz-se que o número natural a é o *menor* (ou *primeiro*) elemento do conjunto A quando $a \in A$ e, além disso, $a \leqslant x$, para todos os elementos $x \in A$. Por exemplo, 0 é o menor elemento de $\mathbb{N}$. Dado $n \in \mathbb{N}$, definimos

$$I_n = \{p \in \mathbb{N} : \quad p \leqslant n\}.$$

Desse modo,

- $I_0 = \{0\}$.
- $I_1 = \{0,1\}$.
- $I_2 = \{0,1,2\}$.

Considerando as propriedades da relação de ordem $m < n$, para os números naturais, diremos que existe uma propriedade de suma importância que é válida para a ordem entre os números naturais, mas sem equivalente para outros conjuntos numéricos. Assim como Lima [9] e Hefez [6], chamaremos esta propriedade de Princípio da Boa Ordenação ou Princípio da Boa Ordem.

Teorema 3.3 *(Princípio da Boa Ordenação) Todo subconjunto não-vazio $A \subset \mathbb{N}$ possui um menor elemento.*

Demonstração. Admitindo que $0 \notin A$, pois caso $0 \in A$ certamente seria 0 o menor elemento de A, assim $I_n \neq \varnothing$, já que $0 \notin A$, logo $0 \in I_n$. Temos que o menor elemento de A deve ser um número da forma $n+1$ para algum $n \in \mathbb{N}$, desta forma, $I_n \subset \mathbb{N} - A = \{x \in \mathbb{N}, \text{ tal que, } x \notin A\}$.

Consideremos o conjunto:

$$X = \{n \in \mathbb{N} : \quad I_n \subset \mathbb{N} - A\}.$$

Podemos observar que $I_n = \{0,1,...,n\} \subset \mathbb{N} - A$ significa que nenhum elemento de I_n pertence a A. Consequentemente, todos os elementos de A são maiores que n. Como $A \neq \varnothing$, então $X \neq \mathbb{N}$, de modo que, não podemos aplicar o quarto axioma de Peano ao conjunto X, ou seja, existe algum $n \in X$ tal que $n+1 \notin X$. Assim todos os elementos de A são maiores que n, mas nem todos maiores que $n+1$. Daí $n+1$ é o menor elemento de A. □

Capítulo 4

O conjunto $\mathbb{Z}$ dos números inteiros

Ao falarmos do conjunto dos números naturais, incluímos o número zero como o primeiro deles, mesmo levando em consideração que a descoberta do zero se deu algum tempo depois do surgimento dos outros números naturais, ocorrendo pela necessidade de notar a não existência de unidades em uma ordem posicional. Neste capítulo construiremos o conjunto $\mathbb{Z}$ dos números inteiros, tomando como ponto de partida o conjunto $\mathbb{N}$ dos números naturais, segundo Ferreira [5], Monteiro [10], para isto usaremos uma relação de equivalência. Mais detalhes consultar as referências supra citadas.

4.1 Relação de equivalência

Relação de equivalência é um importante tipo de relação sobre um conjunto, não vazio, que permite particionar o conjunto em classes de equivalência, surgindo daí um novo conjunto chamado de conjunto quociente.

Obs. 4.1 *Usaremos a notação aRb para informar que o elemento a está relacionado com o elemento b pela relação R.*

Definição 4.1 *Dizemos que uma relação R sobre um conjunto A, não vazio, é uma relação de equivalência quando ocorrem as seguintes condições:*
i) A relação R é reflexiva, isto é, se $a \in A$, então aRa;
ii) A relação R é simétrica, isto é, dados $a, b \in A$, se aRb então bRa;
iii) A relação R é transitiva, isto é, dados $a, b, c \in A$, se aRb e bRc, então aRc.

Definição 4.2 *Considere uma relação de equivalência R num conjunto A, não vazio, e $a \in A$, fixado arbitrariamente. Chamaremos o conjunto*

$$[a] = \{x \in A : xRa\}$$

de ***classe de equivalência*** *de a pela relação R.*

Definição 4.3 *Seja X um conjunto não vazio. Uma partição de X é qualquer família de subconjuntos X_i, com $i \in \mathbb{N}$, não vazios de X, com as seguintes propriedades:*

i) $X_i \cap X_j \neq \varnothing$ ou $X_i = X_j$, com $i \neq j$
ii) $X_1 \cup X_2 \cup X_3 \cup \ldots \cup X_n = X$.

Temos como consequência da definição de relação R de equivalência sobre um conjunto A, que suas classes de equivalências formam uma partição de A como mostraremos em seguida.

Proposição 4.1 *Sejam R uma relação de equivalência sobre um conjunto A e a, b elementos quaisquer de A, então:*
i) $[a] \neq \varnothing$;
ii) Dados $a, b \in A$, *então* $[a] = [b]$ *ou* $[a] \cap [b] = \varnothing$.

Demonstração. *i*) Como $a \in A$ segue pela reflexividade que aRa; Daí pela Definição 4.2, temos que $a \in [a]$.

ii) Suponhamos que exista $x \in [a] \cap [b]$. Desta forma, por definição xRa e xRb. Daí temos pela simetria que aRx, e pela transitividade aRb. Vamos mostrar que $[a] = [b]$, seja $y \in [a]$, então, segue que yRa. Por outro lado como aRb pela transitividade, yRb, implicando em $y \in [b]$, isto é, $[a] \subset [b]$. Dado $z \in [b]$, temos zRb e como bRa segue, pela transitividade que zRa, assim $z \in [a]$, então $[b] \subset [a]$. Portanto, concluímos que $[a] = [b]$. □

Definição 4.4 *Seja R uma relação de equivalência num conjunto A. O conjunto das classes de equivalências de A pela relação R é chamado de conjunto quociente, o qual denotaremos por A/R.*

Exemplo 1 $\mathbb{Z}_2 = \{[0], [1]\}$, *onde* $[0]$ *é a classe que representa os números pares e* $[1]$ *é a classe que representa os números ímpares.*

4.2 A construção de $\mathbb{Z}$

Sejam $\mathbb{N}$ o conjunto dos números naturais e $P = \mathbb{N} \times \mathbb{N}$ o produto cartesiano de $\mathbb{N}$ com ele mesmo. Desta forma, P é o conjunto de todos os pares ordenados (a, b) tais que $a, b \in \mathbb{N}$, ou seja, $P = \{(a, b) : \quad a, b \in \mathbb{N}\}$.

Considere R a seguinte relação no conjunto P:

$$(a,b)R(c,d) \Leftrightarrow a + d = b + c, \quad \forall \quad (a,b),(c,d) \in P.$$

Mostraremos que a relação R é uma relação de equivalência sobre P:
i) R é reflexiva, pois dado $(a,b) \in P$, temos que $(a,b)R(a,b)$, já que $a+b=b+a$.

ii) R é simétrica, pois se $(a,b)R(c,d)$, então $a+d=b+c$, como a adição de números naturais goza da propriedade comutativa, temos que $d+a=c+b$ implicando em $c+b=a+d$, ou seja, $(c,d)R(a,b)$.

iii) A relação R é transitiva, pois se $(a,b)R(c,d)$ então $a+d=b+c$ e que $(c,d)R(e,f)$, ou seja, $c+f=d=e$. Desta forma segue que:

$$a+d+f=c+b+f=b+c+f=b+d+e.$$

Logo, $a+f+d=b+e+d$. Daí, $a+f=e+b$ e assim $(a,b)R(e,f)$.

Concluímos com isso que a relação R do conjunto P é uma relação de equivalência.

Obs. 4.2 *Um elemento do conjunto* $\mathbb{N}\times\mathbb{N}$ *é denotado por* (a,b)*, e este elemento como uma classe de equivalência será denotado por* $[a,b]$*. Portanto,*

$$[a,b]=\{(p,q)\in P : (p,q)R(a,b)\}.$$

Ao conjunto quociente P/R daremos o nome de conjunto dos números inteiros e usaremos o símbolo $\mathbb{Z}$ como notação para este conjunto. Ou seja, $\mathbb{Z}=P/R$.

Os elementos $[0,0],[1,0]\in P/R$, são classes de quivalências especiais. Chamaremos $[0,0]$ de "zero" e o representaremos por "0" e $[1,0]$ de "um ou unidade" e o representaremos por "1". O número 0 é o menor dos números naturais segundo o terceiro axioma de Peano.

Observemos que com esta relação de equivalência existem infinitos pares ordenados que representam a mesma classe de equivalência. Podemos esboçar um diagrama Fig. 4.1, que mostra essa situação, em que partindo dos números inteiros obtemos os pares que representam as respectivas classes.

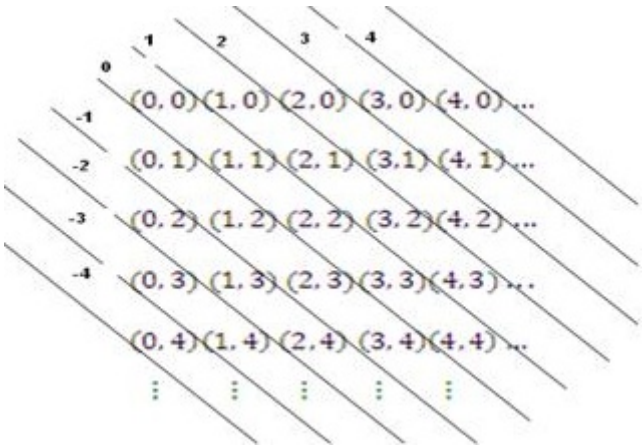


Figura 4.1: Classes de equivalência de $\mathbb{Z}$.

Temos, por exemplo, em $\mathbb{Z}$ que os pares ordenados $(1,2)$, $(3,4)$, $(11,12)$ estão relacionados, já que $(1,2)R(3,4)$, pois $1+4=2+3$ e $(3,4)R(11,12)$. Logo representam a mesma classe de equivalência.

Percebemos que os pares $(0,0)$, $(1,1)$, $(2,2)$,...,(a,a) com $a \in \mathbb{N}$, representam a classe $[0,0]$. Os pares do tipo (a,b) em que $a,b \in \mathbb{N}$, com $a > b$, representam classes de números positivos, bem como os pares (a,b) em que $a,b \in \mathbb{N}$, com $a < b$, representam classes de números negativos. Desta forma, temos por exemplo, $1 = [1,0]$, $-1 = [0,1]$, $0 = [0,0]$, $2 = [2,0]$, $-2 = [0,2]$,...

Os símbolos $\mathbb{Z}^*$, $\mathbb{Z}_+$, $\mathbb{Z}_-$, $\mathbb{Z}_+^*$ e $\mathbb{Z}_-^*$, significam, respectivamente, conjunto dos números inteiros não nulos, conjunto dos números inteiros não negativos, conjunto dos números inteiros não positivos, conjunto dos números inteiros positivos e conjunto dos números inteiros negativos.

4.3 Adição em $\mathbb{Z}$

Definição 4.5 *Definiremos a adição em $\mathbb{Z}$ da seguinte forma:*

$$\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$$

$$([a,b],[c,d]) \to [a,b]+[c,d] = [a+c,b+d].$$

Proposição 4.2 *A adição está bem definida em $\mathbb{Z}$.*

Demonstração. Devemos mostrar que esta operação está bem definida em $\mathbb{Z}$, para tal mostraremos que a soma não depende do representante escolhido, ou seja, se $[a,b] = [a',b']$ e $[c,d] = [c',d']$, então $[a,b]+[c,d] = [a',b']+[c',d']$.

Como $[a,b] = [a',b']$ e $[c,d] = [c',d']$, então $(a,b)R(a',b')$ e $(c,d)R(c',d')$. Daí $a+b' = a'+b$ e $c+d' = c'+d$ somando membro a membro as duas igualdades teremos $a+b'+c+d' = b+a'+d+c'$. Pelas propriedades comutativa e associativa da adição no conjunto dos números naturais, temos $(a+c)+(b'+d') = (b+d)+(a'+c')$, e dessa forma, $[a+c,b+d]R[a'+c',b'+d']$ e portanto, pela Proposição 4.1, segue que $(a+c,b+d) = (a'+b',c'+d')$, consequentemente,

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

□

4.4 Propriedades da adição em $\mathbb{Z}$

Proposição 4.3 *Dados $x=[a,b], y=[c,d]$ e $z=[e,f]$ elementos de $\mathbb{Z}$, então temos que:*
i) A adição é associativa em $\mathbb{Z}$, isto é, $(x+y)+z=x+(y+z)$;
ii) A adição é comutativa em $\mathbb{Z}$, isto é, $x+y=y+x$;
iii) Existência de um elemento neutro, $x+0=0+x=x$;
iv) Existência de um elemento simétrico $x+(-x)=(-x)+x=0$.

Demonstração. *i)* $(x+y)+z=([a,b]+[c,d])+[e,f]$, pela definição da adição em $\mathbb{Z}$ temos,

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

usando a associatividade da adição em $\mathbb{N}$ temos:

$$[a+(c+e),b+(d+f)]=[a,b]+[c+e,d+f]=[a,b]+([c,d]+[e,f])=x+(y+z).$$

ii) $x+y=[a,b]+[c,d]=[a+c,b+d]=[c+a,d+b]$, usamos a comutatividade de $\mathbb{N}$.

iii) $x+0=[a,b]+[0,0]=[a+0,\,b+0]=[a,b]$.

iv) Como $x+y=0$, segue que, $[a,b]+[c,d]=[0,0]$, ou seja, $[a+c,b+d]=[0,0]$, implicando em $a+c=b+d$, isto é, $d=a, c=b$. Logo $y=[b,a]$. □

Obs. 4.3 *Chamamos atenção, que é fácil ver que o elemento neutro é único, assim como o simétrico de cada elemento.*

4.5 Subtração em $\mathbb{Z}$

Por conta da existência e da unicidade do elemento simétrico de um número inteiro, podemos definir a operação de subtração em $\mathbb{Z}$, denotada pelo símbolo (-) e definida da seguinte maneira.

Definição 4.6 *Dados os números inteiros x e y, a subtração $x-y$ é definida da seguinte forma:*

$$(x-y)=x+(-y).$$

Assim a subtração $x-y$ nada mais é que a soma de x com o oposto de y.
Temos as seguintes ropriedades básicas:

Proposição 4.4 *Se x,y,z, são números inteiros, então valem as seguintes propiedades:*
i) $(-1)x=-x$;

ii) $x-y=z \Leftrightarrow y+z=x$;
iii) $x(y-z)=xy-xz$;
iv) $-(-x)=x$.

Demonstração. *i*) Notemos que $0=0x=(1+(-1))x=x+(-1)x$, logo pela unicidade do elemento simétrico $(-1x)=-x$.

ii) Inicialmente mostraremos que $x-y=z \Rightarrow y+z=z$. Somando y em ambos os lados da igualdade $x-y=z$ temos, $x=y+z$.

Reciprocamente, $y+z=x \Rightarrow x-y=z$. Somando $-y$ em ambos os lados da igualdade $y+z=x$ temos, $x-y=z$.

iii) $x(y-z)=x[y+(-z)]=xy+x(-z)=xy+(-xz)=xy-xz$.

iv) Como $(-x)=(-1)\cdot(x)$, temos então que: $-(-x)=-(-1)\cdot(x)=(-1)\cdot(-x)=x$. □

4.6 Multiplicação em $\mathbb{Z}$

Definição 4.7 *Definiremos a multiplicação em $\mathbb{Z}$ da seguinte forma:*

$$\mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}$$

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

Proposição 4.5 *A multiplicação está bem definida em $\mathbb{Z}$.*

Demonstração. Devemos mostrar que o produto está bem definido em $\mathbb{Z}$. Para tal suponhamos que, $[a,b]=[a',b']$ e $[c,d]=[c',d']$, desta forma segue que, $(a,b)R(a',b')$ e $(c,d)R(c',d')$, logo, $a+b'=b+a'$ e $c+d'=d+c'$. Daí, pela distributividade da multiplicação em $\mathbb{N}$:

$$ac+b'c=bc+a'c \quad \text{e} \quad ad+b'd=bd+c'd.$$

Somamndo as duas igualdades membro a membro, temos:

$$ac+b'c+bd+a'd=bc+a'c+ad+b'd.$$

Pela comutatividade em $\mathbb{N}$:

$$ac+bd+a'd+b'c=ad+bc+a'c=bd, \quad \text{ou seja,} \quad (ac+bd,ad+bc)R(a'c+b'd,a'd+b'c).$$

Daí, $[a,b]\cdot[c,d]=[a',b']\cdot[c,d]$.

A prova de que $[c,d]\cdot[a,b]=[c',d']\cdot[a,b]$ se faz de maneira análoga. □

4.7 Propriedades da multiplicação em $\mathbb{Z}$

Proposição 4.6 *Dados $x=[a,b], y=[c,d]$ e $z=[e,f]$ elementos de $\mathbb{Z}$, então temos que:*
i) $(x\cdot y)\cdot z = x\cdot(y\cdot z)$*;*
ii) $x\cdot y = y\cdot x$*;*
iii) $1\cdot x = x\cdot 1$*;*
iv) $x\cdot(y+z) = x\cdot y + x\cdot z$*;*
v) Se $x\cdot y = 0$*, então* $x=0$ *ou* $y=0$*.*

Demonstração. *i)* $(x\cdot y)\cdot z = ([a,b]\cdot[c,d])\cdot[e,f]$, pela definição da multiplicação em $\mathbb{Z}$, temos $([ac+bd, ad+bc])\cdot[e,f] = [(ac+bd)e+(ad+bc)f, (ac+bd)f+(ad+bd)e]$, pela distributividade dos naturais segue que

$$\begin{aligned} &= [(ace+bde+adf+bcf, acf+bdf+ade+bce)] \\ &= [a(ce+df)+b(de+cf), a(de+cf)+b(ce+df)] \\ &= [a,b]\cdot[ce+df, de+cf] \\ &= [a,b]\cdot([c,d]\cdot[e,f]) = x\cdot(y\cdot z). \end{aligned}$$

ii) $x\cdot y = [a,b]\cdot[c,d] = [ad+bc, ac+bd] = [bc+da, ac+bd] = [c,d]\cdot[a,b] = y\cdot x$.

iii) $x\cdot 1 = [a,b]\cdot[1,0] = [a\cdot 1+b\cdot 0, a\cdot 0+b\cdot 1] = [a,b] = x$.

iv) $x(y+z) = [a,b]\cdot([c,d]+[e,f]) = [a,b]\cdot[c+e, d+f]$. Pela definição de multiplicação segue que, $[(ac+ae)+(bc+be), (ad+bc)+(af+be)]$. Daí, concluímos que:

$$[ac+bd, ad+bc]+[ae+bf, af+be] = [a,b]\cdot[c,d]+[a,b]\cdot[e,f] = x\cdot y + x\cdot z.$$

v) Suponhamos que $[a,b]\neq 0$, isto é, $a\neq b$. Logo $a>b$ ou $b>a$. Sem perda de generalidade, podemos supor que $a>b$, então existe $n\in\mathbb{N}$, $n\neq 0$ tal que $a=b+n$. Por outro lado, como $x\cdot y=0$, então $[a,b]\cdot[c,d]=0$. Daí $ac+bd=ad+bc$. Agora substituindo $a=b+n$ obtemos

$$(b+n)c+bd = (b+n)d+bc$$

pela lei do cancelamento em $\mathbb{N}$ temos que $nc=nd$, como $n\neq 0$ segue que $c=d$, ou seja, $y=[c,d]=[0,0]=0$. □

4.8 Ordem em $\mathbb{Z}$

Assim como no conjunto dos números naturais, a ordem se preserva no conjunto dos números inteiros. Dizemos que x é positivo se $0\leqslant x$, e que x é negativo se $x\leqslant 0$. Valendo assim as relações:

Proposição 4.7 *Dados os números inteiros x, y e z, então valem as seguintes propriedades:*
i) $x \leqslant x$;
ii) Se $y \leqslant x$ *e* $x \leqslant y$, *então* $x = y$;
iii) Se $y \leqslant x$ *e* $x \leqslant z$, *então* $y \leqslant z$;
iv) Se $y \leqslant x$, *então* $y + z \leqslant x + z$;
v) Se $0 \leqslant x$ *e* $0 \leqslant y$, *então* $0 \leqslant x + y$ *e* $0 \leqslant xy$;
vi) $x + z < x + y$ *se, e somente se,* $x < y$;
vii) $y \leqslant x \Leftrightarrow -x \leqslant -y$;
viii) Se $x < y$ *e* $0 < z$, *então* $zx < zy$;
ix) Se $x < y$ *e* $z < 0$, *então* $zy < zx$.

Por considerarmos que foge ao objetivo desse trabalho, não iremos demonstrar essas propriedades, o leitor interessado pode consultar Hefez [6].

Capítulo 5

Divisibilidade em $\mathbb{Z}$

Neste capítulo definiremos algumas propriedades aritméticas do conjunto dos números inteiros, afim de termos ferramentas suficientes para abordar o Algoritmo de Euclides e o aplicarmos para calcular o *Máximo Divisor Comum* de números inteiros.

5.1 Multiplicidade e Divisibilidade em $\mathbb{Z}$

Iniciaremos esta seção definindo múltiplos, divisores e mostraremos o algoritmo de Euclides além de definirmos máximo divisor comum, segundo Hefez [6].

Definição 5.1 *Dado um número inteiro m, os múltiplos de m são os números inteiros:*

$$0, \pm m, \pm 2m, \pm 3m, ...$$

Definidos assim podemos perceber facilmente que vale a seguinte propriedade:

Proposição 5.1 *Se a, b são números inteiros tais que ambos são múltiplos de $m \in \mathbb{Z}$, então $a+b$ e $a \cdot b$ são múltiplos de m.*

Demonstração. De fato, suponhamos que $a = qm$ e $b = km$, com $q, k \in \mathbb{Z}$, daí segue que: $a+b = qm+km = (q+k)m$ e $a \cdot b = qm \cdot km = (qkm)m$. □

Definição 5.2 *Dados $a, b \in \mathbb{Z}$, dizemos que a divide b e escrevemos $a|b$, quando existir $c \in \mathbb{Z}$, tal que $b = ac$. Ao número c daremos o nome de quociente de a e b.*

Proposição 5.2 *Dados $a, b, c \in \mathbb{Z}$. As seguintes afirmações são verdadeiras:*
i) $1|a$ *e* $a|a$*;*
ii) $a|0$*;*
iii) Se $a|b$ e $b|c$ então $a|c$;
iv) Se $a|b$ e $b|a$, com $a \cdot b > 0$ então $a = b$;

v) Suponhamos que $a \neq 0$ e $c \neq 0$ e que $a|b$ e $c|d$, então $ac|bd$;
vi) Dados $a,b,c \in \mathbb{Z}$, com $a \neq 0$, se $a|(b+c)$, então $a|b$ implicando em $a|c$;
vii) Se $a,b,c,x,y \in \mathbb{Z}$, com $a \neq 0$, tais que $a|b$ e $a|c$, então $a|(xb \pm yc)$.

Demonstração. *i*) $a = a \cdot 1$. O que justifica os dois casos.

ii) $0 = a \cdot 0$.

iii) Como $a|b$ e $b|c$, existem $m,n \in \mathbb{Z}$ tais que $a \cdot m = b$ e $b \cdot n = c$. Substituindo o valor de b em $b \cdot n = c$ temos, $c = (a \cdot m) \cdot n = a(mn) \Rightarrow a|c$.

iv) Sabemos que se $a|b$, então existe $c \in \mathbb{Z}$, tal que $a \cdot c = b$ e que $b|a$ então existe $d \in \mathbb{Z}$,tal que $b \cdot d = a$. Se $a = 0$ então $b = 0$, pois por hipótese $a|b$ e $b|a$. Caso $a \neq 0$, temos que $c > 0$ e $d > 0$. Como $ac = b$ e $bd = a$, podemos substituir o valor de b da primeira igualdade na segunda e teremos $(ac)d = a$, ou seja, $a(cd) = a$. Assim $c = d = 1$. Logo $a = b$.

v) Como $a|b$ e $c|d$ é fato que existem $e, f \in \mathbb{Z}$, tais que $ae = b$ e $cf = d$. Multiplicando as duas igualdades temos que $(ae)(cf) = bd$, logo $(ac)(ef) = bd$. Portanto $ac|bd$.

vi) Como $a|(b+c)$, é fato que existe d tal que $ad = b + c$. Como $a|b$, é fato que existe e tal que $ae = b$. Substituindo o valor de b da segunda igualdade na primeira temos que $ae + c = ad$. Portanto $c = ad - ae \Rightarrow c = a(d-e)$. Isto é, $a|c$. De maneira análoga temos que $a|(b+c)$, isto é, existe d tal que $ad = b+c$. Como $a|c$, é fato que existe f tal que $af = c$. Substituindo o valor de c da segunda igualdade na primeira temos que $af + b = ad$. Portanto $b = ad - af \Rightarrow b = a(d-f)$. Isto é $a|b$.

vii) Como $a|b$ e $a|c$ é fato que existem e e $f \in \mathbb{Z}$, tais que $ae = b$ e $af = c$. Assim, segue que $xb \pm yc = x(ae) \pm y(af) = a(ex \pm yf)$. O que conclui a prova. □

5.2 Algoritmo da Divisão

A divisão de dois números inteiros pode ser realizada, mesmo quando um destes números não é múltiplo do outro, para isso apresentaremos e demonstraremos o conhecido **Algoritmo de Euclides** fazendo algumas aplicações deste importante resultado. Restringiremos o Algoritmo de Euclides para o caso em que $m \in \mathbb{Z}_+^*$, pois sem perda de generalidade podemos supor que se $n \in \mathbb{Z}_+^*$ e $m \in \mathbb{Z}_-^*$ o resultado da divisão de n por m equivale ao resultado da divisão de $-n$ por $-m$.

Teorema 5.3 *(Algoritmo de Euclides restrito ao caso m inteiro e positivo) Dados $m \in \mathbb{Z}_+^*$ e $n \in \mathbb{Z}$. Existem dois únicos inteiros q e r tais que $n = mq + r$, com $0 \leqslant r < m$.*

Demonstração. Inicialmente mostraremos a existência de q e r. Em seguida mostraremos suas unicidades. Temos que n é um múltiplo de m ou n está situado entre dois múltiplos qm

e $(q+1)m$ de m, para algum $q \in \mathbb{Z}$. Se n é múltiplo de m, digamos, $n = mk$, trivialmente temos $q = k$ e $r = 0$. Caso n não seja múltiplo de m, é fato que teremos, $qm < n < (q+1)m$. Nesta desigualdade podemos subtrair qm de todos os membros, tendo assim, $0 < n - qm < m$. Tomemos $n - qm = r$ implicando em $n = mq + r$, daí $0 < r < m$. Segue que, quando $r = 0$, n é múltiplo de m.

Para provar a unicidade de q e r, suponhamos que existam outros inteiros r' e q' tais que $n = mq' + r'$, com $0 \leqslant r' < n$. Desta forma temos que $n = mq + r = mq' + r'$, ou seja, $(r - r') = (q - q')m$, percebemos assim que $(r - r')$ é múltiplo de m e como $-m < r - r' < m$, o único valor possível é $r - r' = 0$, mas assim temos $r = r'$. Desta forma, $q = q'$. □

Obs. 5.1 *Chamamos n de dividendo, m de divisor, q de quociente e r de resto.*

Exemplo 2 *O quociente e o resto da divisão de 17 por 5, usando o Algortmo de Euclildes é obtido fazendo.*

$$17 - 5 = 12, 17 - 2 \cdot 5 = 7, 17 - 3 \cdot 5 = 2 < 5$$

Portanto o quociente desta divisão é 3 e o resto é 2.

Exemplo 3 *O quociente e o resto da divisão de -54 por 8, usando o Algortmo de Euclildes é obtido fazendo.*

$$-54 + 8 = -46, -54 + 2 \cdot 8 = -38, -54 + 3 \cdot 8 = -30, ..., -54 + 6 \cdot 8 = -6, -54 + 7 \cdot 8 = 2$$

Portanto o quociente desta divisão é -7 e o resto é 2.

5.3 Máximo Divisor Comum

Aplicaremos o Algoritmo da divisão para determinar o *Máximo Divisor Comum* de números inteiros.

Definição 5.3 *Dados $a, b \in \mathbb{Z}$, não ambos nulos, dizemos que $d \in \mathbb{Z}_+^*$ é divisor comum de a e b se $d|a$ e $d|b$.*

Definição 5.4 *Dados $a, b \in \mathbb{Z}$, não ambos nulos, dizemos que $d \in \mathbb{Z}_+^*$, é Máximo Divisor Comum de a e b, quando d cumpre duas condições.*

(i) $d|a$ e $d|b$;

(ii) Se $e \in \mathbb{Z}$, tal que $e|a$ e $e|b$, então $e|d$, ou seja, d é o maior divisor comum de a e b.

Obs. 5.2 *Esta definição vale também, para uma quantidade finita de números inteiros.*

Obs. 5.3 *Denotaremos, o Máximo Divisor Comum de dois números a e b, simplesmente por* $mdc(a,b)$.

Proposição 5.4 *Dados* $a,b \in \mathbb{Z}$ *e* $d = mdc(a,b)$. *As seguintes afirmações são verdadeiras:*
(i) Se $a = b = 0$, *então* $d = 0$;
(ii) Se $a = 0$ *e* $b \neq 0$, *então* $d = |b|$, *já que* $d \in \mathbb{Z}_+^*$;
(iii) Se $d = mdc(a,b)$, *então* $d = mdc(-a,b) = mdc(a,-b) = mdc(-a,-b)$.

Demonstração. i) e ii) são triviais; iii) Dados $a,b \in \mathbb{Z}$, não ambos nulos. Temos que o maior divisor de a é $|a|$. Daí temos que o maior divisor de $-a$ é $|a|$. Dessa forma, $mdc(a,b) = mdc(-a,b)$ e analogamente $mdc(a,-b) = mdc(-a,-b) = mdc(a,b)$. □

Lema 5.5 ***(Lema de Euclides)*** *Dados* $a,b,q,r \in \mathbb{Z}$ *tais que,* $a = bq + r$, *então* $d = mdc(a,b)$ *se, e somente se,* $d = mdc(b,r)$.

Demonstração. Suponhamos que $d = mdc(a,b)$ desta forma, temos, por definição que $d > 0$, $d|a$ e $d|b$. Daí $d|(a-bq)$, isto é, $d|r$. Agora seja $d' \in \mathbb{Z}_+^*$ tal que $d'|b$ e $d'|r$. Assim $d'|(bq+r)$, ou seja, $d'|a$, logo $d'|d$, pois $d = mdc(a,b)$.

Reciprocamente, suponhamos que $d = mdc(b,r)$. Daí $d|b$ e $d|r$, então $d|(bq+r)$, ou seja, $d|a$. Seja $f \in \mathbb{Z}$ tal que $f|a$ e $f|b$, então $f|(a-bq)$, isto é, $f|r$. Logo $f|d'$, pois $d' = mdc(b,r)$. Donde concluímos que $mdc(a,b) = mdc(b,r)$ □

Teorema 5.6 *Dados* $a,b \in \mathbb{Z}$, *Existe um inteiro positivo d, que é máximo divisor comum de a e b.*

Demonstração. Considere $a,b \in \mathbb{Z}$. Notemos que caso, $a|b$ ou $a = 1$, temos $mdc(a,b) = |a|$, assim podemos supor que $1 < a < b$ e que a não divide b, logo pelo Algoritmo de Euclides existem q_1, r_1, tais que:

$$b = aq_1 + r_1, \quad \text{com} \quad 0 < r_1 < a.$$

Daí surgem duas possibilidades:

$$r_1|a.$$

Assim:

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

Ou então:

$$r_1 \quad \text{não divide} \quad a.$$

Aplicando o Algoritmo de Euclides em a e r_1, desta maneira existem inteiros q_2 e r_2, tais que:

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

O que também nos dá duas possibilidades:

$$r_2 | r_1.$$

Assim:

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

Ou então:

$$r_2 \quad \text{não divide} \quad r_1.$$

Aplicando novamente o Algortimo de Euclides. Portanto existem inteiros q_3 e r_3, tais que:

$$r_1 = r_2 q_3 + r_3, \quad 0 < r_3 < r_2 < r_1 < a.$$

Mas, este procedimento não é infinito, já que pelo Princípio da Boa Ordenação a sequência $a > r_1 > r_2 > r_3 ...$ possui um menor elemento. Portanto, para algum n teremos que $r_n | r_{n-1}$, pois em algum momento teremos que o resto é igual a zero, implicando em

$$mdc(a, b) = r_n.$$

Ou seja, mostramos a existência do $mdc(a, b)$.

Vamos mostrar a unicidade. Para tal, suponhamos que $mdc(a, b) = d$ e $mdc(a, b) = d'$. Notemos que tanto d, quanto d' são divisores comuns de a e b, assim $d | d'$ e $d' | d$, e como d e d' são ambos positivos segue que $d = d'$. Provando assim a unicidade de $mdc(a, b)$. □

Proposição 5.7 ***(Identidade de Bezout).*** *O máximo divisor comum de dois inteiros a e b, não nulos simultaneamente, se escreve como combinação linear de a e b, ou seja, existem inteiros x e y tais que* $mdc(a, b) = ax + by$.

Demonstração. Aplicando Proposição 5.4 (iii), sem perda de generalidade, podemos supor que $a > 0$ e $b > 0$. Tomemos o conjunto

$$A = \{ax + by; \quad x, y \in \mathbb{Z}\},$$

notamos facilmente que existem elementos estritamente positivos em A, já que $a \in A$, basta tomar $x = 1$ e $y = 0$ e $b \in A$ tomemos $x = 0$ e $y = 1$. Seja d o menor dos elementos positivos de A. Mostraremos que d é o máximo divisor comum entre a e b. É fato que $d > 0$. Como

$d \in A$, então existem $x_0, y_0 \in \mathbb{Z}$, de maneira que $d = ax_0 + by_0$. Aplicando o algoritmo da divisão aos números a e d segue que:

$$a = dk + r \quad 0 \leqslant r < a.$$

Das duas últimas igualdades tiramos $a = (ax_0 + by_0)k + r$. Ou ainda podemos concluir que $r = a(1 - kx_0) + b(-y_0)k$. Portanto $r \in A$. Sendo r positivo e levando em conta a escolha do d a conclusão é que $r = 0$. Daí ficamos com $a = dk$, o que mostra que $d|a$. A prova que $d|b$ é análoga. Para finalizar temos que se $d'|a$ e $d'|b$, então, pelo fato de $d = ax_0 + by_0$, $d'|d$. □

Para outra demonstração da Identidade de Bezout usando o Princípio da Casa dos Pombos (PCP), o leitor pode consultar Lima [9] ou o **Apêndice C**.

Proposição 5.8 *Sejam os números inteiros a, b, c, d, d' com d e d' positivos. Se $d = mdc(a,b)$ e $d' = mdc(a,b,c)$, então $d' = mdc(mdc(a,b),c) = mdc(d,c)$.*

Demonstração. Seja $d' = mdc(a,b,c)$ e $d'' = mdc(d,c)$, com $d = mdc(a,b)$. Queremos mostrar que $d'|d''$ e $d''|d'$. Daí, como d' e d'' são positivos por definição, então $d' = d''$

De $d' = mdc(a,b,c)$ segue por definição, que $d'|a$ e $d'|b$, e como $d = mdc(a,b)$ então $d'|d$, pelo fato de $d'|c$ segue que $d'|d''$, pois $d'' = mdc(d,c)$.

Por outro lado, $d'' = mdc(d,c)$ por definição, $d''|d$ e $d''|c$. Agora como $d = mdc(a,b)$, por definição $d|a$ e $d|b$, daí segue que $d''|a$ e $d''|b$, mas $d''|c$ logo $d''|d'$, pois $d' = mdc(a,b,c)$. Donde concluímos que $d'' = d'$. □

Capítulo 6

Equações Diofantinas

Neste capítulo definiremos as equações diofantinas lineares, mostraremos a condição para que existam soluções de uma equação diofantina linear e mostraremos como resolver equações deste tipo fazendo uma aplicação do *mdc*, que por sua vez é uma aplicãção do Algoritmo de Euclides, assim como pode ser visto em Hefez [6] e Hygino [7].

6.1 Equações Diofantinas Lineares

Uma equação diofantina linear é uma equação polinomial de primeiro grau em um dado número de variáveis cujos coeficientes são números inteiros e suas soluções são números inteiros.

Exemplo 4 *3x+7y=4, com $x, y \in \mathbb{Z}$: Uma Equação Diofantina Linear em duas variáveis.*

6.2 Equações Diofantinas Lineares com Uma Incógnita

Uma Equação Diofantina Linear com Uma Incógnita é uma equação polinomial do primeiro grau com uma indeterminda. Se existe solução inteira para este tipo de Equação Diofantina Linear, tal solução é única. Assim, para $ax = b$, segue que, caso exista um valor inteiro de x tal que esta sentença seja verdadeira, ele é único.

Proposição 6.1 *A equação $ax = b$, possui solução inteira se, e somente se, $a|b$.*

Demonstração. Suponhamos que $a|b$. Logo existe $k \in \mathbb{Z}$, tal que $ak = b$. Consequentemente, k é solução inteira da equação $ax = b$.

Suponhamos que equação $ax = b$ possui solução inteira, digamos $m \in \mathbb{Z}$, daí, $am = b$, logo $a|b$.

Mostraremos que se a equação $ax = b$ possui solução ela é única. De fato, suponhamos que x e x' sejam as soluções da equação. Logo $ax = b = ax'$, daí $ax = ax'$, podemos notar que $a \neq 0$, pois ax é um polinômio do primeiro grau, logo pela lei do cancelamento em $\mathbb{Z}$ temos que $x = x'$. □

6.3 Equações Diofantinas Lineares com Duas Variáveis

Uma Equação Diofantina Linear com duas variáveis é uma equação do tipo:

$$ax + by = c,$$

na qual $a, b, c \in \mathbb{Z}$, não sendo a e b nulos simultaneamente. Diremos que uma das soluções de uma equação deste tipo é um par $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$, tais que $ax_0 + by_0 = c$.

Definição 6.1 *Chamaremos de x_0 e y_0 uma solução particular da equação $ax + by = c$, esta solução particular é um par de números inteiros que torna a sentença $ax_0 + by_0 = c$ verdadeira.*

Proposição 6.2 *Dada uma equação diofantina linear $ax + by = c$, tal equação possui solução se, e somente se, $d|c$, com $d = mdc(a, b)$.*

Demonstração. Suponhamos que a equação $ax + by = c$ possua solução do tipo (x_0, y_0). Vamos mostrar que $d|c$. Seja $d = mdc(a, b)$, desta forma sabemos que, $d|a$ e $d|b$. Logo pela Proposição 5.2, $d|(ax_0 + by_0)$, ou seja, $d|c$. Reciprocamente, suponhamos que $d|c$. Logo existe $k \in \mathbb{Z}$, tal que $c = dk$ e como $d = mdc(a, b)$ então, pela Identidade de Bezout, existem os inteiros x_0, y_0, tais que $ax_0 + by_0 = d$. Logo, $k(ax_0 + by_0) = kd = c$ implicando em $akx_0 + bky_0 = c$, implicando, desta forma, que (kx_0, ky_0) é solução da equação $ax + by = c$. □

Podemos perceber que se em uma Equação Diofantina Linear, $mdc(a, b)$ divide c, a equação $ax + by = c$ é equivalente a $a_i x + b_i y = c_i$, com $a_i = \frac{a}{d}, b_i = \frac{b}{d}, c_i = \frac{c}{d}$, em que $mdc(a_i, b_i) = 1$. Desta forma, encontrar solução para a equação $ax + by = c$ é equivalente a encontrar solução para $a_i x + b_i y = c_i$.

Teorema 6.3 *Se a Equação Diofantina Linear $ax + by = c$, possui uma solução do tipo $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$, então possui infinitas soluções do tipo $(x = x_0 + \frac{b}{d}t, y = y_0 - \frac{a}{d}t) \in \mathbb{Z} \times \mathbb{Z}$ e $t \in \mathbb{Z}$, para cada valor arbitrário do parâmetro t, com $d = mdc(a, b)$.*

Demonstração. Sejam (x_0, y_0) uma solução particular e (x_k, y_k) uma solução qualquer da equação $ax + by = c$. Segue que $ax_0 + by_0 = c = ax_k + by_k$. Assim, $ax_0 + by_0 = ax_k + by_k$.

Subtraindo ax_0 de ambos os lados temos, $by_0 = ax_k + by_k - ax_0$. Subtraindo by_k de ambos os lados da igualdade temos que

$$a(x_k - x_0) = b(y_0 - y_k).$$

Como $d|a$ e $d|b$, existem $p,q \in \mathbb{Z}$, tais que $a = pd$ e $b = qd$, com $mdc(p,q) = 1$. Isto nos diz que, $p(x_k - x_0) = q(y_0 - y_k)$. Percebemos então que $p|q(y_0 - y_k)$, como $mdc(p,q) = 1$ segue que $p|(y_0 - y_k)$, pois p e q são primos entre si, logo existe $t \in \mathbb{Z}$, tal que $(y_0 - y_k) = pt$. Notemos que $(y_0 - y_k) = pt \Rightarrow y_k = y_0 - pt$, mas $p = \frac{a}{d}$, logo,

$$y_k = y_0 - \frac{a}{d}t.$$

Agora observemos que $(y_0 - y_k) = pt$ implica em, $q(y_0 - y_k) = qpt = p(x_k - x_0)$, cancelando o fator p nos dois últimos membros da igualdade temos, $qt = (x_k - x_0) \Rightarrow x_k = x_0 + qt$, mas $q = \frac{b}{d}$, logo,

$$x_k = x_0 + \frac{b}{d}t.$$

□

Exemplo 5 *Estudar a equação diofantina* $2x + 4y = 7$.

Solução: Como $mdc(2,4) = 2$ e 2 não divide 7. Assim a equação $2x + 4y = 7$ não admite solução inteira.

Exemplo 6 *Analisar se existem soluções inteiras da equação* $12x + 5y = 7$.

Solução: Notemos que $mdc(12,5) = 1$ e 1 divide 7. Para escrevermos 1 como combinação linear de 12 e 5 podemos proceder da seguinte forma:
$1 = 5 - 2 \cdot 2 = 5 - 2(12 - 5 \cdot 2) = 5 - 2 \cdot 12 + 4 \cdot 5 = (-2) \cdot 12 + 5 \cdot 5$. Multiplicando a igualdade $(-2) \cdot 12 + 5 \cdot 5 = 1$ por 7 teremos:
$7[(-2) \cdot 12 + 5 \cdot 5] = 7 \cdot (-14) \cdot 12 + 35 \cdot 5 = 7$.

Concluímos então que $(-14, 35)$ é uma solução particular da equação $12x + 5y = 7$. Desta forma as soluções destas equações são dadas por: $x = -14 + 5t$, $y = 35 - 12t$, com $t \in \mathbb{Z}$.

6.4 Equações Diofantinas Lineares com Três Variáveis

Nesta seção trataremos de Equações Diofantinas Lineares com três variáveis, ou seja, trataremos das equações do tipo $ax + by + cz = n$ onde $a,b,c \in \mathbb{Z}$, tais que a,b,c não são ambos nulos. Inicialmente mostraremos que $ax + by + cz = n$, possui solução inteira quando $mdc(a,b,c)|n$.

Proposição 6.4 *A equação diofantina linear $ax+by+cz=n$, possui solução se, e somente se, $d|n$, com $d=mdc(a,b,c)$.*

Demonstração. Suponhamos que (x_0,y_0,z_0) seja solução, isto é, $ax_0+by_0+cz_0=n$. Sendo $d=mdc(a,b,c)$ então por definição $d|a$, $d|b$ e $d|c$. Logo $d|ax_0+by_0+cz_0=n$.

Reciprocamente, se $d|n$ com $d=mdc(a,b,c)$. Pela identidade de Bezout, existem inteiros r,s,t tais que $ar+bs+ct=d$. Agora como $d|n$, existe inteiro q tal que $n=dq$. Daí, $arq+bsq+czq=n$. Logo (rq,sq,tq) é uma solução da equação $ax_0+by_0+cz_0=n$. □

Teorema 6.5 *Se a Equação Diofantina Linear $ax+by+cz=n$, possui solução, então ela possui infinitas soluções inteiras do tipo $x=x_0+\frac{b}{d}s$, $y=y_0-\frac{a}{d}s$, $z=z_0-t$, com $s,t\in\mathbb{Z}$, $d=mdc(a,b)$, $q=ax+by$, (x_0,y_0) solução da equação $ax+by=q_0+ct_0$, (q_0,z_0) solução da equação $q+cz=n$.*

Demonstração. Chamaremos $ax+by$ de q. Assim $ax+by+cz=n$ equivale a $q+cz=n$. É fato que $q+cz=n$ possui solução (q_0,z_0) pois, $mdc(1,c)=1$. A solução geral desta equação será,

$$(q_0+ct,\ z_0-t),\quad \text{com}\quad t\in\mathbb{Z}.$$

Logo temos,

$$q=q_0+ct\quad \text{e}\quad q=ax+by.$$

Então $ax+by=q_0+ct$. Escolhendo $t\in\mathbb{Z}$, digamos t_0 tal que $d|q_0+ct_0$. Daí a equação $ax+by=q_0+ct_0$ possui solução, digamos (x_0,y_0). E portanto possui solução geral do tipo $(x_0+\frac{b}{d}s, y_0-\frac{a}{d}s)$, com $s\in\mathbb{Z}$. Concluímos então que a solução geral da Equação Diofantina Linear $ax+by+cz=n$ será:

$$x=x_0+\frac{b}{d}s,\quad y=y_0-\frac{a}{d}s,\quad z=z_0-t,$$

com $s,t,\in\mathbb{Z}$; $q=ax+by$; (q_0,z_0) soluções particulares da equação $q+cz=n$; t_0 escolhido de modo que $d|q_0+ct_0$ e (x_0,y_0) solução particular de $ax+by=q_o+ct_0$. □

Exemplo 7 *Resolver a equação diofantina linear $x+10y+25z=99$.*

Solução: Chamaremos $10y+5z$, de $5p$, com $p\in\mathbb{Z}$, assim $x+5p=99$ como $mdc(1,5)=1$ temos que $1\cdot 6+5(-1)=1$. Multiplicando ambos os lados da igualdade por 99 teremos, $1\cdot 594+5(-99)=99$. Portanto a solução geral da equação $x+5p=99$ será,

$$x=594+5t_1, p=-99-t_1\quad \text{com}\quad t_1\in\mathbb{Z}.$$

Temos a seguinte igualdade $10y+5z=5p$, dividindo ambos os lados desta igualdade por 5, $2y+z=p$. Pela Identidade de Bezout, temos que $2(1)+1(-1)=1$, multiplicando por p ambos os lados da igualdade, $2(p)+1(-p)=p$, daí vemos que $y=p+t$ e $z=-p-2t$), com $t\in\mathbb{Z}$. Substituindo o valor de $p=-99-t_1$ nestas igualdades, $y=-99-t_1+t$ e $z=-(-99-t_1)-2t=99+t_1-2t$. Concluímos então que a solução geral da equação $x+10y+25z=99$ será,

$$x=594+5t_1,\ y=-99-t_1+t,\ z=99+t_1-2t \quad \text{com} \quad t,t_1\in\mathbb{Z}.$$

Capítulo 7

Congruências

Neste capítulo faremos um estudo sobre uma aritmética com restos da divisão Euclidiana por um número fixado. Definiremos equações de congruências e mostraremos como resolver Equações Diofantinas Lineares usando congruências segundo a notação de Hefez [6].

7.1 Congruência Módulo m

Definição 7.1 *Dados $m, a, b \in \mathbb{Z}$. Diremos que a e b são **congruentes** módulo m. Quando o resto das divisões Euclidianas de a e b por m forem os mesmos.*

Denotaremos que a é congruente a b módulo m da seguinte forma:

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

A verificação de que dois números são ou não congruentes módulo m pode ser feita usando a seguinte proposição.

Proposição 7.1 *Considere $a, b \in \mathbb{Z}$. Temos $a \equiv b$ (mod m) se, e somente se, $m|b-a$.*

Demonstração. Suponhamos que $a \equiv b \pmod{m}$. Por deinição $a = qm + r$ e $b = q_1 + r$, com $0 \leqslant r < m$ e $q, q_1 \in \mathbb{Z}$. Daí, $b - a = (q_1 - q)m$, ou seja, $m|(b-a)$.

Reciprocamente, suponhamos que $m|(b-a)$. Logo existe $q \in \mathbb{Z}$ tal que $b - a = mq$. Daí $b = a + mq(*)$. Sejam r e q_1 o resto e o quociente da divisão euclidiana de b por m, isto é, $b = mq_1 + r(**)$ com $0 \leqslant r < m$. De $(*)$ e $(**)$ temos que $a + mq = mq_1 + r$ então $a = m(q_1 - q) + r$, com $0 \leqslant r < m$. Portanto r também é o resto da divisão euclidiana de a por m. □

Proposição 7.2 *$a \equiv b$ (mod 1), para quaisquer $a, b \in \mathbb{Z}$.*

Demonstração. $x = 1 \cdot x + 0$ para todo $x \in \mathbb{Z}$, ou seja, todo número inteiro quando dividido por 1 deixa resto zero. □

Daqui em diante a congruência módulo m admitirá apenas valores de m maiores que 1, pois pela Proposição 7.2, o caso $m = 1$ é trivial. A próxima proposição afirma que a relação de congruência módulo m é reflexiva, simétrica e transitiva, portanto uma relação de equivalência em $\mathbb{Z}$.

Proposição 7.3 *Dados $m, a, b \in \mathbb{N}$ tais que $m > 1$. São verdadeiras as sentenças:*
i) $a \equiv a$ (mod m);
ii) Se $a \equiv b$ (mod m), então $b \equiv a$ (mod m);
iii) Se $a \equiv b$ (mod m) e $b \equiv c$ (mod m), então $a \equiv c$ (mod m).

Demonstração. *i*) É trivial já que $m|a-a$.

ii) Notemos que se $m|a-b$, então $m|-(-b+a)$, ou seja, $m|b-a$, assim $b \equiv a \pmod{m}$.

iii) Como $m|b-a$ e $m|c-b$, é fato que, $m|(c-b)+(b-a)$, isto é, $m|c-a$ e desta forma, $a \equiv c \pmod{m}$. □

7.2 Compatibilidade com a Adição e a Multiplicação

A relação de congruência é compatível com a adição.

Proposição 7.4 *Dados os números inteiros a, b, c, d, m, com $m > 1$. Se $a \equiv b$ (mod m) e $c \equiv d$ (mod m), então $a + c \equiv b + d$ (mod m).*

Demonstração. Como $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$. Segue que, $m|a-b$ e $m|c-d$. Basta observar que $m|(a-b)+(c-d)$, isto é, $m|(a+c)-(b+d)$, logo $a+c \equiv b+d \pmod{m}$. □
A relação de congruência módulo m também é compatível com a operação de multiplicação.

Proposição 7.5 *Dados os números inteiros a, b, c, d, m, com $m > 1$.*

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

Demonstração. Mostraremos que $m|(bd-ac)$. Notemos que $bd = d(b-a)+a(d-c)$. Como por hipótese $m|(b-a)$ e $m|(d-c)$, temos que $m|d(b-a)+a(d-c)$, portanto podemos concluir que $d|(bd-ac)$. □

7.3 Classes de Congruências

Definição 7.2 *Dados os números inteiros a, b, m, com $m > 1$. seja a relação $\sim$ definida em $\mathbb{Z}$ como:*

$$a \sim b \Leftrightarrow a \equiv b\,(mod\, m).$$

A Proposição 7.3, nos garante que $\sim$ é uma relação de equivalência em $\mathbb{Z}$.

Definição 7.3 *Dados os inteiros a e m, com $m > 1$. A classe de congruência de a módulo m, será denotada $[a]$.*

$$\begin{aligned} [a] &= \{x \in \mathbb{Z};\quad x \equiv a\,(mod\, m)\}; \\ [a] &= \{x \in \mathbb{Z}; x = a + mq, \text{com } q \in \mathbb{Z}\}; \\ [a] &= \{\ldots, -2m + a, -m + a, a, m + a, 2m + a, \ldots\}. \end{aligned}$$

Assim, fixando um inteiro a, pelo Algoritmo da Divisão Euclidana, existe um único inteiro r, tal que $0 \leqslant r < m$. Logo temos $a \equiv r \pmod{m}$. O conjunto quociente $\mathbb{Z}/_m$, será denotado daqui em diante simplesmente por $\mathbb{Z}_m$.

7.4 Sistema Completo de Resíduos

Podemos perceber que se $x \in \mathbb{Z}$, x será congruente módulo m ao seu resto na divisão euclidiana de x por m, isto é, x será congruente módulo m a um dos números da sequência $\{0, 1, 2, 3, \ldots, m-1\}$. Além disso nenhum par destes números são congruentes módulo m.

O conjunto quociente $\mathbb{Z}_m$, com $m > 1$, terá os seguintes elementos ou classes de congruência módulo m:

$$\begin{aligned} [1] &= \{x \in \mathbb{Z}; x \equiv 1\,(\mathrm{mod}\, m)\} \\ [2] &= \{x \in \mathbb{Z}; x \equiv 2\,(\mathrm{mod}\, m)\} \\ [3] &= \{x \in \mathbb{Z}; x \equiv 3\,(\mathrm{mod}\, m)\} \\ [4] &= \{x \in \mathbb{Z}; x \equiv 4\,(\mathrm{mod}\, m)\} \\ &\vdots \\ [m-1] &= \{x \in \mathbb{Z}; x \equiv m-1\,(\mathrm{mod}\, m)\} \end{aligned}$$

Desta forma diremos que um Sistema Completo de Resíduos módulo m será o conjunto

$$[y] = \{x \in \mathbb{Z}; x \equiv y\,(\mathrm{mod}\, m)\}$$

Definição 7.4 *Dado um conjunto de inteiros* $\{a_0, a_1, a_2, a_3, ..., a_{m-1}\}$*, diremos que tal conjunto é um Sistema Completo de Resíduos (SCR), se, e somente se,* $a_r \equiv r (mod\, m)$.

Exemplo 8 *O conjunto* $F = \{0,1,2,3,4\}$ *é um Sistema Completo de Resíduos módulo 5, pois, os restos possíveis na divisão por cinco são 0, 1, 2, 3 e 4.*

Definiremos as operações de adição e multiplicação em $\mathbb{Z}_m$ da seguinte forma:

Definição 7.5 *Dados* $[a], [b] \in \mathbb{Z}_m$*, temos,* $[a] + [b] = [a+b]$

Para que a adição esteja bem definida precisamos mostrar que não importa quais sejam os representantes a e b das classes $[a]$ e $[b]$ escolhidas, o resultado de $[a]+[b]$ será a classe de equivalência $[a+b]$. Isto ocorre pela Proposição 7.4, se $a \equiv a'$ (mod m) e $b \equiv b'$ (mod m), então $(a+b) \equiv (a'+b')$ (mod m).

7.5 Propriedades da Adição em $\mathbb{Z}_m$

Usaremos as notações x, y, z para representar as classes $[x], [y], [z] \in \mathbb{Z}_m$ respectivamente. Para as quais valem as seguintes propriedades:
i) Associatividade $(x+y)+z = x+(y+z)$;
ii) Comutatividade $x+y = y+x$;
iii) Existência de um elemento neutro $x+0 = 0+x = x$;
iv) Existência de um elemento simétrico $x+(-x) = (-x)+x = 0$.

Definição 7.6 *Dados* $[a], [b] \in \mathbb{Z}_m$*, temos,* $[a] \cdot [b] = [a \cdot b]$

De modo análogo do comentário da adição , usando o que a Proposição 7.5, mostra-se que a multiplicação está bem definida.

7.6 Propriedades da Multiplição em $\mathbb{Z}_m$

Para quaisquer $x, y, z \in \mathbb{Z}_m$ valem as seguintes propriedades:
i) Associatividade $(x \cdot y) \cdot z = x \cdot (y \cdot z)$;
ii) Comutatividade $x \cdot y = y \cdot x$;
iii) Existência de um elemento neutro $x \cdot 1 = 1 \cdot x = x$;
iv) Distributividade $x \cdot (y+z) = x \cdot y + x \cdot z$.

Um conjunto que possui as operações de adição e multiplicação definidas como acima e gozando destas propriedades pode ser chamado de *anel*, assim $\mathbb{Z}_m$ é um anel das classes residuais módulo m.

7.7 Tabelas de Adição e Multiplicação em $\mathbb{Z}_m$

Considerandoo conjunto $\mathbb{Z}_m$ do conjunto $\mathbb{Z}$, para facilitar o cálculo de operações, podemos construir tabelas de adição e multiplicação. Como podem ser visto na Fig. 7.1 e Fig. 7.2.

Exemplo 9 *Tabelas de adição e multiplicação em* $\mathbb{Z}_6$.

+	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

x	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1]

Figura 7.1: Tabelas de adição e multiplicação módulos 6.

Exemplo 10 *Tabelas de adição e multiplicação* $\mathbb{Z}_5$.

+	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]

x	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]

Figura 7.2: Tabelas de adição e multiplicação módulos 5.

Na tabela de multiplicação módulo 6, Fig. 7.1, notemos que os únicos elementos que possuem inverso multiplicativo são, $[1]\cdot[1]=[1]$ e $[5]\cdot[5]=[1]$, ou seja, existem apenas dois inversos multiplicativos. Mas na tabela de multiplicação módulo 5, Fig. 7.2, temos que cada elemento possui um inverso multiplicativo

$$[1]\cdot[1]=[1], \quad [2]\cdot[3]=[1], \quad [3]\cdot[2]=[1] \quad \text{e} \quad [4]\cdot[4]=[1].$$

7.8 Congruências Lineares

Nesta seção faremos um estudo sobre congruências do tipo $ax \equiv c \pmod{b}$, com o objetivo de resolver uma Equação Diofantina Linear do tipo $ax+by=c$, usando este tipo de congruência.

Teorema 7.6 *Dados $a, c \in \mathbb{Z}$, e $b, m \in \mathbb{N}$, com $m > 1$ tais que b não divide a. A congruência linear $ax \equiv c$ (mod b), possui solução inteira se, e somente se $d|c$, com $d = mdc(a,b)$, além disso a solução geral desta congruência é $x = x_0 + \frac{b}{d}t$, com $t \in \mathbb{Z}$ e x_0 uma solução particular de $ax \equiv c$ (mod b).*

Demonstração. Pela definição de congruência temos que $ax \equiv c \bmod b$, se $b|ax - c$, ou seja, existe $y \in \mathbb{Z}$, tal que $ax - c = by$. Desta forma, teremos $ax - by = c$ e pela Proposição 6.2, segue que existem soluções para tal equação se, e somente se $d|c$, com $d = mdc(a,b)$ sendo tais soluções: $\{x = x_0 + \frac{b}{d}t \ , y = t_0 - \frac{a}{d}t\}$, com $t \in \mathbb{Z}$. □

Proposição 7.7 *Dados $a, m \in \mathbb{Z}$, com $m > 1$. Então existe $b \in \mathbb{Z}$ com $ab \equiv 1$ (mod m) se, e somente se, $mdc(a,m) = 1$.*

Demonstração. $ab \equiv 1 \pmod{m}$, admite solução na variváel b se, e somente se, existem $b, k \in \mathbb{Z}$, tais que $ab - 1 = mk$, assim $ab - mk = 1$ que admite solução se, e somente se, $d = mdc(a,m)|1$. desse modo temos $d = 1$. Reciprocamente $mdc(a,m) = 1$ implica que existem $b, k \in \mathbb{Z}$, tais que $ab - mk = 1$, daí $ab - 1 = mk$, ou seja, $m|(ab-1)$, isto é, $ab \equiv 1 \pmod{m}$. □

7.9 Resolvendo Equações Diofantinas Lineares Utilizando Congruências Lineares

Para resolvermos uma Equação Diofantina Linear do tipo $ax + by = c$ podemos escrevê-la como uma congruência do tipo $ax \equiv c \pmod{b}$. Portanto, resolver a equação $ax + by = c$ equivale a resolver a congruência $ax \equiv c \pmod{b}$, ou seja, encontrar a classe de equivalência $[x]$ tal que $a \cdot x \equiv c \pmod{b}$.

Exemplo 11 *Vamos resolver a Equação Diofantina Linear $5x + 7y = 50$.*

Solução: Usando o módulo 5, teremos $7 \cdot y \equiv 50 \pmod{5}$, como $7 \equiv 2 \pmod{5}$ e $50 \equiv 0 \pmod{5}$ segue que, $2 \cdot y \equiv 0 \pmod{5}$. Percebemos desta forma que, $5|(2y - 0)$, portanto, $5|y$, ou seja, existe $t \in \mathbb{Z}$, tal que $y = 5t$. Substituindo na equação $5x + 7y = 50$, temos $5x + 7(5t) = 50$, isto é, $5x + 35t = 50$. Isolando o x chegamos na seguinte solução $x = 10 - 7t$. Logo a solução geral dessa equação será $x = 10 - 7t, y = 5t$, com $t \in \mathbb{Z}$.

Caso seja mais conveniente, podemos, sem perda de generalidade, usar o módulo 7, desta forma, $5 \cdot x \equiv 50 \pmod{7}$, como $5 \equiv 5 \pmod{7}$ e $50 \equiv 1 \pmod{7}$ temos, $5 \cdot x \equiv 1 \pmod{7}$. Percebemos que a classe $[x]$ é elemento inverso da classe $[5]$. Desta forma,

$x \equiv 3 \pmod 7$. Concluímos então que $7|x-3$, ou seja, existe t inteiro, tal que $x-3=7t$ implicando em $x=7t+3$. Substituindo em $5x+7y=50$, temos $5(7t+3)+7y=50$, logo isolando o y chegamos em $y=5-5t$. Logo a solução geral dessa equação será $x=7t+3, y=5-5t$, com $t \in \mathbb{Z}$.

Exemplo 12 *Resolver a Equação Diofantina Linear* $12x+5y=7$.

Solução: Usando o módulo 5, temos que $12 \cdot x \equiv 7 \pmod 5$. Isto é, $2 \cdot x \equiv 2 \pmod 5$. Percebemos usando a tabela de multiplicação módulo 5 Fig. 7.2, que a classe que devemos multiplicar pela classe [2] para obter a classe [2] é a classe $[1]$, assim, $x \equiv 1 \pmod 5$. Desta maneira, teremos que, $5|(x-1)$ o que nos diz que existe $t \in \mathbb{Z}$, tal que $5t=x-1$, implicando em $x=5t+1$. Substituindo o valor de x em $12x+5y=7$ segue $12(5t+1)+5y=7$, portanto $y=-1+12t$. Logo a solução geral dessa equação será $x=5t+1, y=-1+12t$, com $t \in \mathbb{Z}$.

Capítulo 8

Aplicação

8.1 Usando Equações Diofantinas Lineares Como Ferramenta no Balanceamento de Equações Químicas

Uma equação química é uma forma simbólica de representar abreviadamente uma reação ou um fenômeno químico, por exemplo, na reação de decomposição da amônia, na qual ocorre a formação de dioxido de nitrogênio e a liberação de água.

$$NH_4NO_3 \rightarrow N_2O + H_2O$$

Nesta representação, as substâncias que aparecem no primeiro membro (antes da seta) são chamadas de reagentes e as substâncias que aparecem no segundo membro (depois da seta) são chamadas de produtos, Feltre [4].

A estequiometria é o ramo da química que estuda as quantidades envolvidas de cada substância em uma equação química. Em cálculos estequiométricos calculamos as quantidades mensuráveis de reagentes e de produtos envolvidos em uma reação química. Tais cálculos estequiométricos baseiam-se em três leis que definem as reações químicas, como pode ser visto em Peruzzo [12].

A primeira delas, é a lei de conservação das massas, proposta pelo Francês Antoine Laurent Lavoisier,[1] a qual afirma que a soma das massas de todos os reagentes de uma equação química é igual à soma das massas de todos os produtos.

A segunda, é a lei das proporções definidas, que diz que as massas dos produtos de uma reação química se relacionam de forma proporcional com as massas dos reagentes desta mesma reação. Assim caso tenhamos 10 gramas de uma substância A reagindo com 12

[1] Um químico que fora eleito, aos 25 anos, membro da Academia Real de Ciências da França e que viveu até os 51 anos de idade quando fora guilhotinado em praça pública. Acusado por peculato durante a Revolução Francesa

gramas de uma substância B para formar 22 gramas de uma substância C, então 5 gramas da substância A reagem com 6 gramas da substância B para formar 11 gramas da substância C.

A terceira, é a lei da proporção atômica, que afirma que os coeficientes estequiométricos são proporcionais a quantidade de átomos em cada molécula tanto nos reagentes quanto nos produtos de uma reação química. Assim, por exemplo, são necessárias três moléculas de uma substância que possui dois átomos de um elemento químico, para formar duas moléculas de uma substância que possui dois átomos do mesmo elemento, como por exemplo, três moléculas do gás oxigênio (O_2) reagindo para formar duas moléculas do gás ozônio (O_3).

As quantidades de moléculas de cada substância envolvida em uma equação química são representadas por um número chamado de coeficiente estequiométrico ou simplesmente coeficiente. Dizemos que uma equação química está balanceada quando a quantidade total de átomos de cada elemento em seus primeiro e segundo membros é igual, contudo precisamos que os coeficientes estequiométricos sejam os menores números inteiros positivos possíveis.

Para balancear uma equação química podemos utilizar o método chamado de método algébrico, que consiste em representar as equações químicas por um conjunto de equações, onde as variáveis são os coeficientes estequiométricos.

Exemplo 13 *Balancear a seguinte equação química:*

$$NH_4NO_3 \rightarrow N_2O + H_2O.$$

Solução: Podemos chamar os coeficientes estequiométricos de x, y, e z. Assim teremos:

$$xNH_4NO_3 \rightarrow yN_2O + zH_2O.$$

Usando o método algébrico e baseando-nos na lei da proporção atômica, devemos igualar a quantidade de átomos de cada elemento. Assim, $2x = 2y$, balanceando os átomos de nitrogênio, $4x = 2z$, balanceando os átomos de hidrogênio e $3x = y + z$, balanceando os átomos de oxigênio. Resolvendo este sistema de equações, que é possível e indeterminado, temos $2x - z = 0$, ou seja, balancear esta equação química equivale a encontrar as menores soluções inteiras positivas da equação diofantina $2x - z = 0$. E tal equação possui solução já que $mdc(2,-1) = mdc(2,1) = 1$ e $1|0$, portanto, uma solução é $x = 1$ e $z = 2$, de modo que $y = 1$. E a equação balanceada é:

$$NH_4NO_3 \rightarrow N_2O + 2H_2O.$$

Exemplo 14 *Balancear a equação que representa a reação de combustão que está relacionada à queima do álcool.*

$$C_2H_6O + O_2 \rightarrow CO_2 + H_2O.$$

Solução: Inicialmente chamemos os coeficientes de x, y, z, w respectivamente. Assim:

$$xC_2H_6O + yO_2 \rightarrow zCO_2 + wH_2O.$$

Usando o método algébrico, temos,

- $2x = z$ (balanceando o carbono);
- $6x = 2w$ (balanceando o hidrogênio);
- $x + 2y = 2z + w$ (balanceando o oxigênio).

Encontramos um sistema de equações possível e indeterminado, resolvendo este sistema temos como solução a equação diofantina linear $6x - 2y = 0$, o que é equivalente a equação $3x - y = 0$. Esta equação possui solução, pois $mdc(3,-1) = mdc(3,1) = 1$ e, além disso, $1|0$. Portanto balancear a equação química equivale a encontrar os menores números inteiros positivos que são as soluções da equação diofantina $3x - y = 0$. Tais números inteiros são $x = 1$ e $y = 3$, daí $z = 2$ e $w = 3$. Logo a equação balanceada é:

$$C_2H_6O + 3O_2 \rightarrow 2CO_2 + 3H_2O.$$

Capítulo 9

Considerações Finais

Atualmente o ensino de matemática em escolas da educação báscia tem sido caracterizado como "bicho papão" pelos alunos, pois muitas vezes não é estabelecida uma relação entre o conhecimento trabalhado em sala de aula e a realidade vivida por eles, tornando o conhecimento matemático meramente abstrato e, portanto, dificilmente alcançável.

Pensando nesse tipo de situação, foi buscado neste trabalho uma proposta de estudo que teve como foco aplicar o Algoritmo de Euclides como ferramenta no cálculo do Máximo Divisor Comum, e aplicamos o MDC na resolução de Equações Diofantinas Lineares. Mostramos uma aplicação destas equações no balanceamento de equações químicas. Para que o conteúdo trabalhado pudesse ser visto pelos alunos como uma ferramenta útil na resolução de problemas, em outra área do conhecimento, como sugerem as Orientações Curriculares para o Ensino Médio [2], página 7, quando propõe que a organização curricular deve ocorrer com "integração e articulação dos conhecimentos em processo permanente de interdisciplinaridade e contextualização". Sendo assim buscamos fazer com que o conhecimento matemático pudesse ser encarado pelos alunos como algo que tem sentido, pois eles conseguem, com essa relação contextualização perceber seu significado.

Para fundamentar nosso trabalho fizemos uma abordagem histórica. Logo depois trabalhamos a construção do conjunto dos números naturais baseados nos quatro axiomas de *Peano*. Em seguida, usando uma relação de equivalência construímos o conjunto dos números inteiros. Fizemos, também, a abordagem de algumas propriedades aritméticas relativas a números inteiros, dentre as quais o conhecido **Algoritmo de Euclides**, calculamos Máximo Divisor Comum como uma aplicação do Algoritmo Euclidiano, chegando a um importante resultado usado como base nas resoluções de Equações Diofantinas Lineares. Daí sugerimos caminhos para resolução de Equações Diofantinas Lineares com duas variáveis. Por fim, foi feita uma aplicação do conteúdo na disciplina de Química visando, simplificar o processo de balanceamento de uma equação química.

Desta maneira, chegamos a conclusão de que o Algoritmo de Euclides tanto pode servir como ferramenta para o cálculo do Máximo Divisor Comum de números inteiros, como também tem consequências teóricas muito importantes que podem ser exploradas de muitas formas, tais como, buscando alcançar uma contextualização em outra área do conhecimento que ajude a dar sentido no porquê estudar este conteúdo, e assim motive os alunos.

Finalizamos dizendo que este trabalho pode ser utilizado por professores de Matemática e Química do Ensino básico, com a intenção de atingir seus objetivos, mesmo sabendo que as relações interdisciplinares e contextuais entre o conteúdo estudado e outras áreas do conhecimento, ainda podem ser abordadas de outras maneiras, usando outros procedimentos. Desejamos, também, que surjam novas propostas de abordagens para tal tema, e que trabalhos posteriores nos completem e nos superem. Buscamos com este Trabalho de Conclusão de Curso dar uma pequena contribuição para melhorar a qualidade da educação básica, no que se refere à direção de interdisciplinaridade, tornando o ensino de matemática um processo significativo.

Referências Bibliográficas

[1] BOYER, Carl Benjamim; *História da matemática*, Tradução: Elza F. Gomide. Edgar Blucher. Editora da Universidade de São Paulo, São Paulo, 1974.

[2] BRASIL; MEC, SEB; *Orientações Curriculares para o Ensino Médio*, Ciências da natureza, Matemática e suas Tecnologias, Brasilia: MEC. SEB, 2008.

[3] EVES, Howard; *Introdução a história da matemática* . Tradução: Hygino H. Domingues: Editora UNICAMP, Campinas-SP, 2004.

[4] FELTRE, Ricardo; *Química/Ricardo Feltre. Volume 1*, 6ª Ed. Editora Moderna, São Paulo, 2004.

[5] FERREIRA, Jamil; *A construção dos números/Jamil Ferreira.*. 3ª Ed. SBM, Rio de Janeiro, 2013.

[6] HEFEZ, Abramo; *Elementos de Aritmética.* . SBM, Rio de Janeiro, 2011.

[7] DOMINGUES, Hygino Hugueros; *Álgebra Moderna* . Volume único/ Hygino Domingues, Gelson Iezzi - 4ªEd. Reform. Atual, São Paulo 2003.

[8] IFRAH, Georges; *Os números: História de uma grande invenção/ Geroges Ifrah*, Tradução: Stella Maria de Freitas Senra, 3ª Ed. Editora Globo, São Paulo, 1989.

[9] LIMA, Elon Lages;*A Matemática do Ensino Médio*, volume 1. SBM, Rio de Janeiro, 2006.

[10] JACY MONTEIRO, Luis Henrique; *Elementos de álgebra*. IMPA. Livros técnicos e científicos editora S.A, Rio de Janeiro, 1969.

[11] OLIVEIRA, Krerley Irraciel Martins;*Iniciação a matemática: um cursos com problemas e soluções/ Krerley Irraciel Martins Oliveira, Adán Corcho Fernández*-2ª Edição. SBM, Rio de Janeiro, 2010.

[12] PERUZZO, Francisco Miragaia; *Química na abordagem do cotidiano* . 4ª edição. Editora Moderna, Sao Paulo, 2006.

[13] PITOMBEIRA, João Bosco e ROQUE, Tatiana Martins; *Tópicos de História da Matemática.* SBM, Rio de Janeiro, 2013.

[14] SINGH, Simon; *O Último Teorema de Fermat: a história que confundiu as maiores mentes do mundo durante 358 anos.* Tradução: Jorge Luiz Calife. 13ª edição. Record, Rio de Janeiro, 2008.

Páginas da internet consultadas

[15] Revista Escola; <http://revistaescola.abril.com.br/matematica/fundamentos/geometria-origem-figuras-geometricas-450656.shtml> Acesso em 1 de Agosto de 2014.

[16] Wikipédia; <http://pt.wikipedia.org/wiki/Osso_de_Ishango> Acesso em 1 de Agosto de 2014.

Apêndice A

Solução para o Problema do Epitáfio de Diofanto

No Capítulo 2 falamos sobre o problema escrito na lápide do túmulo de Diofanto, que diz que:

"Deus lhe concedeu ser um menino pela sexta parte de sua vida, e somando uma duodécima parte a isso cobriu-les a face de penugem. Ele acendeu a lâmpada nupcial após uma sétima parte, e cinco anos após seu casamento, concedeu-lhe um filho. Ai! Infeliz criança tardia; depois de chegar a metade da vida de seu pai, o destino frio o levou. Depois de se consolar de sua dor durante quatro anos com a ciência dos números ele terminou sua vida".

Solução: Seja x a quantidade de anos que Diofanto viveu, temos pelo enunciado do problema temos:

$$\frac{x}{6}+\frac{x}{12}+\frac{x}{7}+5+\frac{x}{2}+4=x.$$

Tirando o mínimo múltiplo comum dos denominadores:

$$\frac{14x}{84}+\frac{7x}{84}+\frac{12x}{84}+\frac{420}{84}+\frac{42x}{84}+\frac{336}{84}=x.$$

Escrevendo como uma fração de denominador comum:

$$\frac{14x+7x+12x+420+42x+336}{84}=x.$$

Multiplicando ambos os lados da igualdade por 84:

$$14x+7x+12x+420+42x+336=84x.$$

Somando:

$$75x+756=84x.$$

Subtraindo $75x$ de ambos os lados da igualdade:

$$84x-75x=756 \Rightarrow 9x=756.$$

Daí segue que $x=84$, Ou seja, Diofanto viveu por 84 anos.

Apêndice B

O número Zero

Ao falarmos de números naturais incluímos o zero como o primeiro deles, mesmo tendo levado em consideração que a descoberta do número zero aconteceu algum tempo depois da invenção dos outros números naturais e se deu por conta da necessidade de notar a não existência de algarismos em uma ordem posicional. Alguns historiadores remetem a invenção do zero aos hindus, porém em alguns documentos babilônicos podemos encontrar evidências de que os babilônicos tinham o cuidado de deixar uma das ordens de seu sistema de numeração em branco para representar que naquela ordem não havia uma quantidade número a ser representado, Ifrah [8].

É natural que se associemos a história dos números à necessidade de contagem, mas este tipo de relação não passa segurança alguma pela imprecisão nas fontes das civilizações muito antigas. Os primeiros registros escritos foram encontrados na região da Baixa Mesopotâmia sobre uma forma de escrita chamada cuneiforme, que se baseava em prensar uma cunha sobre tabletes de argila e depois cozinhá-los, tal escrita deve ter sido motivada para ajudar a organizar socialmente o povo Babilônio.

Os registros eram usados quase sempre para representar operações administrativas e neles existia um complexo sistema de controle. Em tal sistema os números não representavam relações diretas com quantidades eles, na verdade, dependiam do que estava sendo contado. Acredita-se que o povo Babilônio agrupava os objetos contados em grupos de 10, 60, 600 ou 3600.

O sistema de numeração Mesopotâmico era um sistema posicional. Por exemplo, o símbolo em forma de cunha servia para 1, 60 e 3600 seu valor dependia da posição na qual o símbolo aparecia. Temos em nosso sistema de numeração, um exemplo bastante semelhante, no qual o símbolo 1 também serve para representar os números 10 e 100. O sistema sexagesimal posicional, usado no período babilônio, surgiu da padronização deste sistema numérico, antes do final do terceiro milênio.

Neste sistema eram usados 60 símbolos que podiam ser combinados para representar qualquer número. Ainda que o conceito de zero não estivesse plenamente desenvolvido, era representado em muitas das tábuas babilônicas apenas como um espaço entre grupos de símbolos quando uma potência particular de 60 não era necessária.

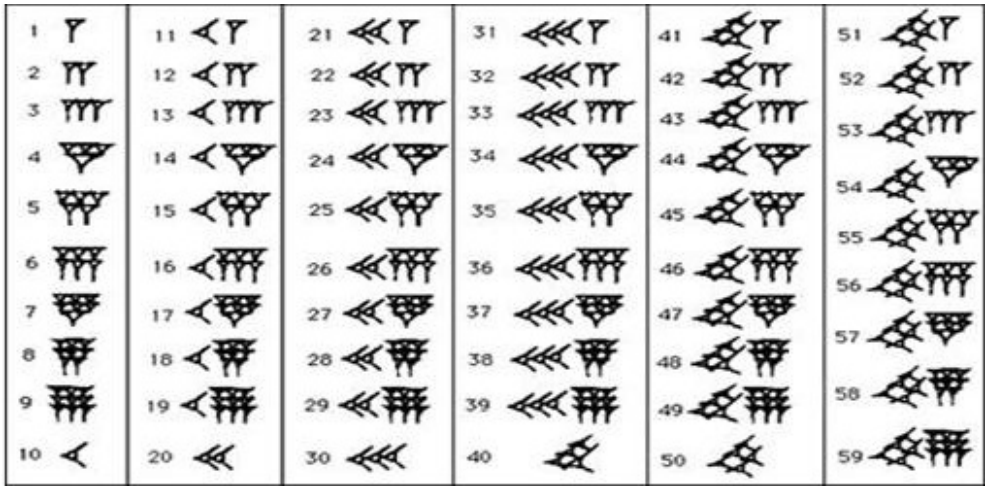


Figura B.1: Símbolos do sistema de numeração sexagesimal Babilônico. [8].

Nas tábuas babilônicas produzidas nos últimos três séculos a.C. usava-se um símbolo para indicar a ausência de uma potência, mas isto só ocorria no interior de um grupo numérico nunca no final. Os gregos usaram o sistema sexagesimal babilônico para desenvolver suas tabelas astronômicas. As tabelas de Ptolomeu no Almagesto [1], incluem o símbolo 0 para indicar a ausência de uma ordem posicional.

Acredita-se que o primeiro a usar um símbolo para representar o zero em um sistema de valor relativo foi o povo maia. Dentre os povos pré-colombianos foi a cultura que mais influenciou as outras, influência essa, que pode ser comparada com a influência da cultura grega sobre outros povos europeus. Alguns historiadores creditam ao povo maia muitas invenções, como por exemplo, a de um calendário bem mais preciso até que o nosso própio calendário gregoriano. Na matemática, os maias são apontados como criadores do sistema posicional e inventores do número zero.

No manuscrito conhecido como **Codex de Dresden** eles revelam a existência de um sistema de numeração de base vinte, no qual figurava um símbolo equivalente ao nosso **zero** e a posição de cada símbolo determina seu valor.

Os maias usavam um conjunto de dezenove símbolos para representar os primeiros dezenove números e os combinavam como na Fig. B.2, para representar números maiores.

[1] Um tratado de astronomia escrito no século II pelo astrônomo Claudio Ptolomeu astrônomo e matemático que viveu na cidade de Alexandria (150 d.C.)

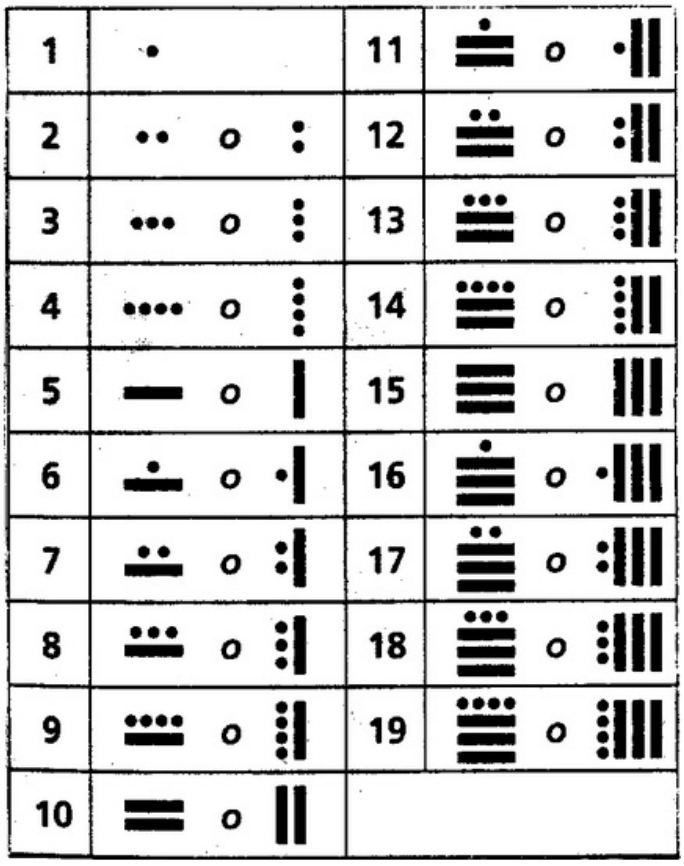


Figura B.2: Símbolos do sistema de numeração maia. [8].

Escreviam uma nova coluna vertical sobre a ordem das unidades, tal coluna representava as vitenas do número, assim $42 = (2 \cdot 20 + 2)$ era representado como segue na Fig.B.3:

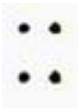


Figura B.3: Número 42 no sistema de numeração maia. [8].

Curiosamente, a próxima ordem não representava uma ordem vinte vezes maior que a ordem anterior, para os sábios maias a próxima ordem equivalia aos múltiplos de 360, criando uma irregularidade no sistema de numeração maia, mas as ordens seguintes voltavam a ser vinte vezes maiores que as ordens anteriores.

A ideia de sistema posicional surge, pelo fato de que cada símbolo precisa estar em sua posição para representar de forma única o número desejado. Para garantir essa fixação na posição os maias iventaram o zero. Que era representado por símbolos que pareciam conchas, como pode ser visto na Fig.B.4.

Figura B.4: Diferentess formas de representar o zero pelos maias. [8].

O símbolo maia do zero era usado para indicar a ausência de quaisquer unidades das várias ordens. Tal sistema foi muito mais usado na produção de calendários ou para registrar o tempo do que com o objetivo de realizar algum tipo de operação matemática. Infelizmente tais invenções não chegaram ao ocidente, que teve que esperar até a idade média para que os árabes trouxessem esse conceito aprendidos com os sábios da Índia.

Apêndice C

Outra Demonstração para a Identidade de Bezout

Comecemos esta seção falando sobre o princípio da casa dos pombos (PCP), como pode ser visto em Oliveira [11]. Tal princípio será uma ferramenta de grande utilidade na demonstração da Identidade de Bezout. O (PCP), nos diz que se tivermos um número de pombos maior que o número de casas alguma dessas casas receberá mais de um pombo.

Proposição C.1 *Se tivermos N casas e $N+1$ pombos, pelo menos uma casa receberá mais de um pombo.*

Demonstração. O número médio de pombos em cada casa neste caso será, $\frac{N+1}{N}$. Como $\frac{N+1}{N} > 1$ segue que alguma casa receberá um número de pombos maior que 1. □

Proposição C.2 *O máximo divisor comum de inteiros a e b, não nulos simultaneamente, se escreve como combinação linear de a e b,ou seja, $mdc(a,b) = ax+by$ para alguns inteiros x e y.*

Demonstração. Caso $mdc(a,b) = 1$, temos $ax+by = 1$, caso contrário podemos tomar $\alpha = \frac{a}{d}$ e $\beta = \frac{b}{d}$, tais que $\alpha x+\beta y = 1$, ou seja, $\frac{a}{d}x+\frac{b}{d}y = 1$.

Daí podemos supor sem perda de generalidade que $ax+by = 1$. Considerando então a sequência $\{a, 2a, 3a, ..., ba\}$ podemos concluir que algum dos termos desta sequência deixa resto 1, quando dividido por b, ou seja, $b|ax-1$. Suponhamos por absurdo que nenhum desses termos deixasse resto 1 ao ser dividido por b, teríamos b números deixando $b-1$ restos diferentes quando divididos por b, nesta sequência.

Assim, digamos que ma e na com $b > m > n \geq 1$, devem segundo o (PCP) deixar o mesmo resto quando divididos por b. Como $mdc(a,b) = 1$, segue que $b|m-n$, mas $b > m$

implica que $b > m - n$ o que é um absurdo. Portanto realmente existe um termo da sequência $\{a, 2a, 3a, ..., ba\}$, que deixa resto 1, quando dividido por b. Chamando este termo de ax temos $b|ax - 1$, isto é, $ax - 1 = by$. □