unesp UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
CAMPUS DE GUARATINGUETÁ

LUCAS AZEVEDO DOS SANTOS

EQUAÇÕES DIOFANTINAS LINEARES: UM APLICATIVO PARA A RESOLUÇÃO

Guaratinguetá – SP
2016

LUCAS AZEVEDO DOS SANTOS

EQUAÇÕES DIOFANTINAS LINEARES: UM APLICATIVO PARA A RESOLUÇÃO

Trabalho de Graduação apresentado ao Conselho de Curso de Graduação em Licenciatura em Matemática da Faculdade de Engenharia do Campus de Guaratinguetá, Universidade Estadual Paulista, como parte dos requisitos para obtenção do diploma de Graduação em Licenciatura em Matemática.

Orientadora: Profª Drª Ana Paula Marins Chiaradia

Guaratinguetá – SP
2016

S237e

Santos, Lucas Azevedo dos

Equações diofantinas lineares: um aplicativo para a resolução / Lucas Azevedo dos Santos. – Guaratinguetá, 2016.

65 f : il.

Bibliografia: f. 63-65

Trabalho de Graduação em Licenciatura em Matemática – Universidade Estadual Paulista, Faculdade de Engenharia de Guaratinguetá, 2016.

Orientadora: Profa. Dra. Ana Paula Marins Chiaradia

1. Equações lineares 2. Androides 3. Algoritmos I. Título

CDU517.983 (043)

unesp UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
CAMPUS DE GUARATINGUETÁ

LUCAS AZEVEDO DOS SANTOS

ESTE TRABALHO DE GRADUAÇÃO FOI JULGADO ADEQUADO COMO PARTE DO REQUISITO PARA A OBTENÇÃO DO DIPLOMA DE **"GRADUADO EM LICENCIATURA EM MATEMÁTICA"**

APROVADO EM SUA FORMA FINAL PELO CONSELHO DE CURSO DE GRADUAÇÃO EM LICENCIATURA EM MATEMÁTICA

Profª. Drª. Vivian Martins Gomes
Coordenadora

BANCA EXAMINADORA:

Profª. Drª. Ana Paula Marins Chiaradia
Orientadora/UNESP-FEG

Prof. Dr. José Federico Vizcaino Gonzalez
UNESP-FEG

Profª. Drª. Elisangela Pavanelo Rodrigues Dos Santos
UNESP-FEG

Novembro 2016

DADOS CURRICULARES

LUCAS AZEVEDO DOS SANTOS

NASCIMENTO	02.01.1991 – Guaratinguetá/SP
FILIAÇÃO	Antonio Carlos Azevedo dos Santos Margarida de Souza Azevedo
2011/2016	Formação acadêmica: Licenciatura em Matemática Faculdade de Engenharia de Guaratinguetá Campus de Guaratinguetá Universidade Estadual Paulista "Júlio Mesquita Filho" - UNESP
2015	Intercâmbio Universitário (Study Abroad Year) Programa Ciência Sem Fronteira Bolsista CAPES QUT – Queenland University of Technology Brisbane - Austrália

Dedico este trabalho, em especial, à minha mãe Margarida, que esteve ao meu lado em todos os momentos, e que com muita fé fez com que eu me formasse matemático.

AGRADECIMENTOS

Em primeiro lugar, agradeço meus pais, Margarida e Toninho, que sempre me deram força para superar todos os desafios da minha vida, e sempre estiveram do meu lado apoiando todas as escolhas que fiz.

A minha irmã Eliana e sua família, que fizeram com que a palavra “lar” tivesse seu mais verdadeiro significado, me dando apoio e ajudando em tudo que é possível.

A minha irmã Ana Rosa e sua família, que sempre me deram força e motivação e que sempre estão ao meu lado em todos os momentos necessários.

A toda minha família no geral, que sempre acreditou em mim e me fez acreditar que eu consigo alcançar qualquer objetivo que eu almeje.

A todos os professores do curso de Graduação em Matemática, em especial a minha orientadora Ana Paula Marins Chiaradia, que gentilmente disponibilizou tempo, atenção, dedicação e paciência e me guiou para completar esse trabalho.

Aos funcionários da FEG em geral, sempre dispostos a ajudar e contribuir para que tenhamos um ensino de qualidade.

Agradeço imensamente a Deus por ter todas essas pessoas ao meu lado me apoiando. Agradeço todos os caminhos que Deus abriu e fechou, que fizeram que eu me tornasse quem eu sou hoje, e toda a força e determinação para que eu não desistisse.

Por fim, a todos vocês, o meu muito obrigado.

“A vida é uma peça de teatro que não permite ensaios. Por isso, cante, chore, dance, ria e viva intensamente, antes que a cortina se feche e a peça termine sem aplausos. ”

Charlie Chaplin

RESUMO

Uma equação diofantina é uma equação polinomial com a restrição que seus coeficientes devem ser números inteiros. Tais equações são comumente utilizadas em resolução problemas, e atualmente, em várias áreas da computação. Partindo dessa premissa, o presente trabalho tem como objetivo a implementação de um algoritmo computacional de resolução das equações diofantinas. Para tal, é feita uma revisão da história da teoria dos números, destacando os principais matemáticos que contribuíram para esse estudo, da Grécia antiga até a modernidade. Também é feita uma revisão da teoria dos números, onde são vistos conceitos matemáticos usados para a resolução das equações diofantinas. Após a explanação do método de resolução de equações diofantinas e alguns exemplos da sua aplicação em resolução de problemas, é feita uma revisão sobre programas computacionais que para resolução da equação, e então será implementado, para a platafroma *Android*, um programa de resolução dessas equações. As principais funções desse programa são analisadas e mostradas. Conclui-se com o presente trabalho a importância da base teórica e histórica para o melhor entendimento das equações diofantinas, assim como a sua importância no mundo de hoje em dia. Esse trabalho é focado na resolução de equações diofantinas lineares de duas variáveis.

PALAVRAS-CHAVE: Equação diofantina linear. *Android*. Algoritmo. Java. Teoria dos números. Diofanto.

ABSTRACT

A Diophantine equation is a polynomial equation with the restriction which each of its coefficients must be integers. These equations are mostly found in everyday issues, and nowadays, in several areas of computer science. Taking this as a premise, this work aims at the implementation of technics for solving Diophantine equations in a computer program. To accomplish this goal, a revision in the history of the theory of the numbers is made, highlighting the main mathematicians who contributed for this theory, from the ancient Greece until modernity. A revision of the theory of the numbers itself is also made, where key concepts for resolving Diophantine equations are studied. After explaining the method for solving Diophantine equations, a revision in already existing programs which make this resolution is made, and then, a program for the *Android* platform is implemented. The main features of this program are analysed and exposed. The conclusion of this work is the importance of the theoretical and historical basis for a better understanding in solving Diophantine equations, as well as its importance in the world nowadays. The focus of this work are linear Diophantine equations with two variables.

KEYWORDS: Linear Diophantine Equation. Android. Algorithm. Java. Number theory. Diophantus.

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1 INTRODUÇÃO

Equações diofantinas recebem esse nome graças a Diofanto de Alexandria, um dos maiores matemáticos da Antiguidade. Chamado por alguns de ‘O pai da aritmética’, o seu mais famoso trabalho foi a série de livros chamada ‘Arithmetica’, coleção de problemas algébricos que influenciaram fortemente o desenvolvimento da teoria dos números.

Pela definição, equação diofantina é qualquer equação polinomial em que os coeficientes do polinômio em questão sejam números inteiros. O que faz uma equação ‘diofantica’ é o fato de suas soluções estarem restritas ao conjunto dos números inteiros. Exemplos de equações diofantinas:

- Equações lineares de duas variáveis, $ax + by = c$;
- A equação quadrática de três variáveis, $x^2 + y^2 = z^2$

O objetivo do presente trabalho é implementar, em linguagem computacional, um aplicativo que calcule as soluções inteiras de equações diofantinas lineares com duas variáveis e que mostre todas as soluções inteiras positivas. Esse trabalho baseia-se na justificativa de que o tema escolhido é de grande aplicação na atualidade. Com o advento da tecnologia, essa tem se tornado parte fundamental do nosso dia-a-dia. E a Matemática é a alma da tecnologia, sendo toda a sua estrutura regida por leis e teoremas matemáticos. Com esse trabalho, tenta-se explorar um pouco dessa matemática que existe por trás desse universo tão gigante, demonstrando como um simples programa contém tantos conceitos da teoria dos números.

Para alcançar tal objetivo, após essa introdução, é apresentado, no Capítulo 2, um referencial bibliográfico, com acertos de trabalhos de outros autores que também estudaram teoria dos números e suas aplicações na computação.

No Capítulo 3, uma breve explanação sobre a história da teoria dos números é realizada. Nesse capítulo é apresentada um pouco da história de Diofanto e de outros matemáticos que deram continuidade em seu estudo sobre esta teoria.

Em seguida, no Capítulo 4, será abordado o referencial teórico utilizado como base para o estudo e implementação computacional das equações diofantinas. Alguns dos principais teoremas desta teoria são abordados, assim como, máximo divisor comum, números primos e divisão euclidiana.

No Capítulo 5 apresenta-se as técnicas de resolução das equações diofantinas. É apresentado o método pelo qual pode-se resolver equações lineares de duas variáveis e também exemplo de resolução de equações. Apresenta-se também uma breve explicação do método de resolver equações diofantinas com três variáveis.

O Capítulo 6 apresenta como se deu a implementação em linguagem computacional das técnicas apresentadas no capítulo anterior. Usando a linguagem de programação JAVA® para a plataforma *Android*, um programa para resolver equações diofantinas de duas variáveis é apresentado e suas principais funções são explicadas.

No Capítulo 7 faz-se uma breve revisão de programas já existentes usados para calcular equações diofantinas. São pesquisados alguns programas de plataformas diferentes os quais tem como função a mesma do aplicativo do presente trabalho. São apresentadas capturas de telas e uma breve explicação de cada um. Finalmente, no Capítulo 8, apresenta-se o programa desenvolvido no presente trabalho. Capturas de tela do programa criado são apresentadas, mostrando suas principais funções e como dá-se a parte de interação com o usuário. E o por fim, a conclusão deste trabalho é apresentada.

2 REVISÃO DA LITERATURA

Vários estudos sobre algoritmos computacionais para a resolução de equações diofantinas podem ser encontrados na literatura. Diverge-se muito a escolha de linguagem computacional usada para a implementação dos algoritmos, como PASCAL®, MAPLE®, Linguagem C++®. Porém nenhum deles, em JAVA®.

Hanta (2001) utiliza três métodos distintos para a resolução das equações. São apresentados três desses, os quais: algoritmo euclidiano, modificações elementares de uma matriz e método para coeficientes indefinidos. Ao final, uma pequena comparação dos métodos é feita, concluindo que o método que foi escolhido para ser explanado no presente trabalho é de fato o que maior gasto computacional.

Yesilyurt (2012) utiliza também o método de resolução pelo algoritmo de Euclides. Faz uma explanação sobre teoria dos números e a aplicação da mesma nas equações diofantinas. Nesse trabalho abrange também o tema de congruências lineares. Ele utiliza desse método para encontrar resolução para a equação dada. Apresenta também uma sólida base teórica e sua aplicação no tema estudado.

Campos (2013) apresenta em seu trabalho toda a teoria numérica que envolve a resolução das equações diofantinas, e em seguida, apresenta métodos para o cálculo de equações lineares com duas, três e quatro variáveis. Ao final de seu trabalho, apresenta um capítulo dedicado a resolução de problemas que se utilizam de equações diofantinas. Essa parte teórica é também apresentada por Hanta (2001) e Yesilyurt (2012), porém Campos a apresenta com mais detalhes.

Ferreira e Domingues (2013), primeiramente, apresentaram uma base teórica sobre equações diofantinas e sobre a linguagem de programação PASCAL®, e em seguida apresentam a resolução das equações diofantinas por outro método, o método de tentativa-erro, ou seja, de ir testando conjuntos de números inteiros em um dado intervalo, até que algum conjunto seja resolução da equação dada. Esse método de resolução apresenta complexibilidade de grau 2, ou seja, uma equação com intervalo de teste de x, será necessário que se calcule até x^2 processos para achar uma solução. Para um programa pequeno, esse grau de complexibilidade não é notado pelo usuário, porém tende a causar mais demora quando se aplica esse método para programas que realizam mais cálculos.

Bispo (2013) e Freitas (2015) explicam mais a fundo o lado prático das equações estudadas. Ambos, além de apresentar uma base teórica bem completa para a resolução das equações diofantinas não-lineares e lineares, exploram vários problemas que usam equações lineares que podem ser encontrados em situações cotidianas, como problemas financeiros e de distribuição de produtos, problemas estes que são muito comuns para empresas e negócios. Bispo também nos dá exemplos de gráficos das equações diofantinas plotados no programa *Winplot*®. Freitas também usa o *Winplot*® para mostrar gráficos de equações, e usa o programa *Maple*® para a resolução das mesmas.

Podem-se citar alguns trabalhos sobre o uso das equações diofantinas na Educação Básica como o de Pommer (2008), o qual disserta sobre a aplicação das equações diofantinas no ensino básico como forma de articular conteúdos e competências. Por meio de apresentação de jogos para as turmas de alunos de matemática do ensino básico, o autor estimula os alunos a criarem um pensamento crítico, fazendo com que a situação-problema apresentada servisse como base para a evolução desse pensamento crítico. Os alunos primeiramente pensam numa resolução de tentativa-erro, e aos poucos vão adquirindo os conhecimentos necessários para a resolução das equações de forma algébrica.

Pommer e Pommer (2012) discutem a relevância da utilização de situações-problema envolvendo tópicos da teoria elementar dos números na educação básica, enfatizando aspectos da origem e desenvolvimento histórico-epistemológico das Equações Diofantinas Lineares.

Savóis e Freitas (2014) fazem uma análise sobre o conceito de máximo divisor comum generalizado, para que possam usar os racionais como conjunto numérico dos coeficientes das equações diofantinas. De forma, expandem a abrangência de problemas solucionados por estas equações. Apresentam alguns problemas práticos e suas soluções considerando os números racionais como coeficientes das equações diofantinas.

3 HISTÓRIA DA TEORIA DOS NÚMEROS

Durante a maior parte da história, a teoria dos números foi sempre considera uma área cuja aplicações no mundo real quase inexistem. “Se algum dia houve um ramo da matemática considerado como vivendo nas alturas inebriantes das torres de marfim foi a teoria dos números”(Stewart, 2014, p. 88). Porém, após quase 2500 anos como exercício puramente intelectual, surgiu uma área na qual a teoria dos números é amplamente aplicada, a computação. Os problemas e situações levantadas pelos computadores atuais remetem quase que totalmente a esta teoria.

Nesse contexto, será feita uma breve história sobre o estudo da teoria dos números, passando pelo seu início na Grécia antiga, onde fora apresentada por Euclides “disfarçada” de geometria e desenvolvida por Diofanto, até os tempos atuais, com o impulso inicial dado por Fermat no século XVII, e desenvolvida mais profundamente por Euler e Gauss.

3.1 DIOFANTO DE ALEXANDRIA

Diofanto de Alexandria, Figura 1, foi o último grande matemático da Escola de Alexandria, nome dado ao período de proliferação do saber naquela cidade, como a filosofia, a arte, a ciência e a religião. Um dos mais importantes matemáticos da Grécia antiga, Diofanto exerceu papel na Aritmética semelhante a Euclides (360-295 a.C.) da Geometria e Ptolomeu (85 – 165 a.C.) na Astronomia.

Diofanto estudou na Universidade de Alexandria. Naquela época, Alexandria era um grande centro econômico e cultural. Juntamente com a concentração de riqueza dos nobres que lá viviam, Alexandria se tornou um local propício para o cultivo do saber. A biblioteca de Alexandria possuía mais de 7000 manuscritos, o que atraia muitos pensadores para aquela região.

Pouco se sabe sobre sua vida pessoal. Até mesmo o período em que ele viveu é ainda questionado pelos historiadores. Documentos antigos citam várias passagens do matemático, o que nos permite demarcar um limite temporal de quase cinco séculos onde ele pode ter vivido. Como cita Bashmakova (1972), não sabemos quando ele viveu e nem sobre seus ancestrais, os quais trabalharam na mesma área. Seu trabalho nos lembra uma chama viva no

meio de uma escuridão impenetrável. Estudos mostram que a data mais provável para o nascimento de Diofanto está entre os anos de 200 e 214 a.C.

Figura 1: Diofanto de Alexandria

Fonte: http://diophantus.weebly.com/uploads/2/6/9/8/26986989/1347997_orig.jpg. Acesso em 29 ago. 2016

O que se sabe de sua vida deve-se a documentos e citações de outros autores. Um famoso enigma, escrito em sua tumba e publicado em uma antologia grega de livros nos dá uma pista sobre algumas informações da vida de Diofanto. Eis o enigma:

> Aqui jaz Diofanto, contemple a maravilha.
> Por meio da arte algébrica, a pedra mostra sua idade:
> Deus deu à ele um sexto de sua vida na infância,
> Um duodécimo como adolescente enquanto cresciam bigodes;
> E ainda um sétimo antes de iniciar o casamento;
> Em cinco anos chegou um vigoroso filho.
> Ah! Querida criança do mestre e sábio,
> Depois de alcançar metade da idade que viveu seu pai, o destino frio o levou.
> Após consolar-se por quatro anos com a ciência dos números,
> ele terminou sua vida.(MADEIRA, 2011)

Resolvendo esse enigma, a equação que representa o problema será:

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

consegue-se concluir que Diofanto morreu aos 84 anos de idade.

Sua maior contribuição para a história é uma coleção de 13 livros chamada ‘Aritmética’ onde são encontrados diversos problemas de álgebra. Dos 13 volumes, apenas seis sobreviveram ao tempo. Recentemente foram descobertos mais quatro desses livros, porém escritos em Árabe.

Os problemas matemáticos encontrados nessa sua série de livros focam mais na resolução de equações especificas com engenhosos artifícios algébricos do que encontrar um método geral para a resolução dessas. “Possivelmente, a Aritmética, assim como os Elementos de Euclides, foi uma compilação e sistematização dos conhecimentos da época.”(Mol, 2013, p.58).

> Diofanto é frequentemente chamado o pai da álgebra, mas talvez seja muito mais adequado tratá-lo como precursor da moderna teoria dos números, cujo ponto de partida seria o trabalho de Fermat no século XVII. O matemático persa al-Khwarizmi (780-850) partilha o título de “pai da álgebra” pelo seu próprio livro intitulado Álgebra, que continha uma solução sistemática de equações lineares e quadráticas. Al-Khwarizmi introduziu os numerais hindu-arábicos e os conceitos de Álgebra na matemática europeia. As palavras algoritmo e álgebra decorrem do seu nome e al-jbr (é uma palavra árabe que significa operação matemática usada para resolver equações quadráticas), respectivamente. (Freitas, p.23, 2015)

Outra grande contribuição dessa obra foi a notação empregada. Diofanto foi o primeiro matemático que se tem registro a usar notação algébrica em seus problemas. Ele abandona a álgebra puramente retórica e passa a empregar abreviações, símbolos e notações. Os símbolos utilizados por Diofanto diferem dos símbolos usados atualmente, principalmente por serem escritos em grego. Mas foi a partir de sua obra que posteriormente foi desenvolvida a notação que conhecemos hoje em dia.

Como exemplo, Diofanto utilizava como símbolo para uma variável a letra S. O Quadro 1 mostra algumas potencias dessa variável, a qual hoje em dia usa-se normalmente ‘x’.

Quadro 1 - Potencias da variável x na escrita de Diofanto

x	S
x^2	Δ^{γ}
x^3	K^{γ}
x^4	$\Delta^{\gamma}\Delta$
x^5	$\Delta \boldsymbol{K}^{\boldsymbol{\gamma}}$
x^6	$\boldsymbol{K}^{\boldsymbol{\gamma}}\boldsymbol{K}$

Fonte: MOL, R. S. Introdução à História da Matemática. Belo Horizonte: CAED-UFMG, 2013, p. 58

Outro exemplo apresentado por Mol (2013) é a adição e subtração. A adição era representada pela justaposição dos símbolos (o que hoje é comum para a multiplicação). Já para a subtração, era usado o símbolo ↀ.

O sistema de numeração empregado era o alfabético ou jônio, em que cada letra grega representava um número. Sabendo disso e sabendo que a variável independente era representada por Ṁ, podemos escrever polinômios de uma variável de uma maneira tão concisa quanto atualmente. Assim, o polinômio $x^4 + 2x^3 - 3x^2 + 4x - 5$ era escrito, naquela época, da seguinte maneira:

$$\Delta^{\gamma}\Delta\boldsymbol{\alpha}\boldsymbol{K}^{\gamma}\boldsymbol{\beta}\Uparrow\Delta^{\gamma}\boldsymbol{\gamma}\boldsymbol{S}\boldsymbol{\delta}\Uparrow\dot{\mathrm{M}}\boldsymbol{\varepsilon}$$

Lembrando que os números eram colocados após as variáveis.

3.2 EUCLIDES

Euclides de Alexandria viveu aproximadamente entre 360 e 295 a.C.. Apesar de Euclides ser um dos mais aclamados matemáticos de todos os tempos, pouco se sabe sobre sua vida, devido à falta de documentos que a detalhem. Diz-se que teria sido educado em Atenas e frequentado a academia de Platão. Convidado por Ptolomeu I para ser professor da recém-formada academia de Alexandria.

Numa época de disputas entre generais gregos por territórios, Ptolomeu I, governante da região da Grécia, onde atualmente se encontra o Egito, pode voltar sua atenção a parte intelectual de seu governo. Criou a famosa escola de Alexandria, e convidou Euclides para ser um de seus professores.

Euclides possui pelo menos dez trabalhos, dos quais cinco chegaram completos até os dias atuais. Porém o trabalho que o dá o título de autor matemático mais famoso da Grécia antiga, senão de todos os tempos são Os Elementos (300 a.C.), uma coletânea de treze livros que reúnem todos os conhecimentos matemáticos da época até então.

Os primeiros seis livros dessa coletânea tratam de problemas de geometria plana, área que hoje é chamada de geometria euclidiana. Nesses livros, Euclides apresenta postulados utilizados até os dias de hoje, necessários para os estudos dos livros seguintes; apresenta também propriedades sobre triângulos, retas paralelas, circunferências e formas de construção dessas figuras.

Figura 2 - Euclides de Alexandria

Fonte: http://ecalculo.if.usp.br/ferramentas/pif/historia/imagens/Euclid_2.jpg. Acesso em 19/09/2016

Os livros VII, VIII e IX são os que tratam da teoria dos números. Para os gregos, números eram apenas os números inteiros e positivos. O livro VII se inicia com a definição de várias propriedades dos números, como o que são números primos, compostos, pares e ímpares, etc. No que se refere aos números primos, pode ser encontrada, por exemplo, a seguinte propriedade, que será demonstrada nesse trabalho: “Todo número pode ser expresso como produto de primos”. No livro VII também é apresentado o famoso algoritmo de Euclides, que será apresentado posteriormente no presente trabalho.

O livro VIII, considerado por Boyer (1996) o menos interessante entre os 13 livros, trata principalmente de proporções continuas (progressões geométricas), tratando também de propriedades simples de quadrados e cubos.

Finalmente, o livro IX, último sobre teoria dos números, apresenta alguns teoremas de muita importância. É nesse livro que se encontra uma proposição equivalente ao Teorema Fundamental da Aritmética, explanado no capítulo que segue. É nele também que Euclides prova a existência de infinitos números primos, “considerada universalmente pelos matemáticos como modelo de elegância universal ” (Eves, 2004, p. 175).

O livro X, considerado por estudiosos o mais admirável e o mais temido antes do advento da álgebra moderna, trata de problemas de incomensurabilidade, ou seja, problemas usando números que não podem ser medidos, os racionais. Os três últimos livros têm como tema a geometria espacial, com o estudo de sólidos e suas propriedades. Como pode-se perceber, diferente do que se é dito de maneira equivocada, os Elementos não tratam apenas da geometria plana, e sim de toda a matemática estudada até então na época.

Segundo Boyre (1996), certamente um dos grandes feitos dos matemáticos gregos, presente na obra de Euclides, foi o sistema postulacional, o qual apresenta as definições matemáticas em forma de postulados. Para que se demonstre uma afirmação, é necessário que esta seja consequência de outra afirmação previamente estabelecida, e essa de outra, e assim por diante. Percebe-se que essa cadeia não pode correr de modo infinito. Dá-se o nome de postulado ou axioma às definições iniciais que servem de base para essas afirmações.

3.3 PIERRE DE FERMAT

Outro nome que também teve papel importantíssimo na evolução do estudo da teoria dos números foi Pierre de Fermat (1601-1665). Advogado e político francês, Fermat nunca atuou como matemático profissionalmente, o que fez com que não publicasse obras. Porém, seus estudos e sua genialidade os fez um dos precursores da teoria dos números moderna, e até mesmo da geometria analítica e cálculo diferencial. Fermat deu continuidade aos trabalhos de Diofanto na área de teoria dos números.

Figura 3 - Pierre de Fermat

Fonte: http://mimosa.pntic.mec.es/jgomez53/matema/conocer/fermat.jpg acesso em 19/09/2016.

Fermat nasceu em Beaumont de Lomagne em 17 de agosto de 1601. Filho de um comerciante de couro, seu pai foi capaz de lhe oferecer ótimas condições de ensino desde a

infância. Seguiu na carreia de direito, sendo Juiz Supremo na Corte Criminal Soberano do Parlamento de Toulouse. Em seu tempo vago, sua atividade preferida era a Matemática, atividade que lhe rendeu o título de maior matemático francês do Século XVII. Faleceu em 1665, em Castres.

Fermat estudou diversos assuntos da Matemática, desde geometria analítica a análise infinitesimal, mas tudo indica que seu assunto preferido era a teoria dos números. Fermat possuía talento extraordinário para essa área, o que o tornou o fundador da teoria moderna dos números. O fato de ele não ter como área principal de atuação a Matemática fez com que ele publicasse quase nenhuma obra, sendo praticamente todos seus estudos retirados de anotações e manuscritos encontrados após sua morte.

Um fato muito interessante é que Fermat, em posse da tradução latina de Aritmética, de Diofanto, fez anotações que se tornaram celebres, como a conjectura a seguir. Ela foi escrita na margem de uma das páginas da obra de Diofanto, se tornando importantíssima para o estudo da teoria dos números. Essa conjectura é conhecida como o Último Teorema de Fermat:

"Para $n > 2$, não existem números inteiros positivos x, y e z satisfazendo a identidade

$$x^n + y^n = z^n$$"

Fermat escreveu também na margem do seu exemplar de Aritmética que tinha uma prova magnifica para tal teorema. Porém, ele não a deu, pois, segundo palavras do próprio Fermat escritas juntamente com o teorema, "essa margem é demasiadamente pequena para tal". Muitos matemáticos tentaram provar tal teorema, porém em vão. Somente em 1995 uma prova definitiva foi encontrada, usando fatos sobre curvas elípticas. Porém, tais métodos são muito sofisticados, levando-se a crer que não era possível Fermat ter tal prova naquela época.

Não é somente o grande teorema de Fermat que permaneceu sem prova. Outro teorema bastante famoso dele, chamado de Pequeno Teorema de Fermat, somente foi provado um século depois por Leonhard Euler. Tal teorema é o seguinte: *"Se p é primo e a é um número não divisível por p, o número* $a^{p-1} - 1$ *é divisivel por p".*

A prova desse teorema fez o uso de indução, artificio que era bem conhecido por parte de Fermat. Aliás, indução matemática é muitas vezes chamada também de indução de Fermat, para ser diferenciada da indução científica.

Fermat também presumiu que todos os números na forma $F_n = 2^{2^n} + 1$ fossem todos primos, o que foi provado errado por Euler mais tarde.

3.4 LEONHARD EULER

Leonhard Euler (1707 - 1783), matemático suíço, foi considerado o maior matemático do século XVIII. Euler estudou na Universidade de Basel, onde desde cedo fora considerado um gênio devido à sua aptidão matemática. Foi considerado o matemático mais produtivo de seu tempo, e um estudioso em que seu nome aparece em várias áreas do conhecimento.

Figura 4 - Leonhard Euler

Fonte: http://www.ega-math.narod.ru/Bell/IMG/Euler1.jpg. Acesso em 19/09/2016.

Nascido na cidade de Basel, Euler pretendia seguir carreira na teologia, até perceber que seu verdadeiro talento era na área dos números. Seu pai o ensinou, e vendo seu exímio dom para a Matemática, conseguiu com que ele estudasse com Jean Bernoulli na Universidade de Basel. Com 20 anos, Euler foi indicado à um posto na Academia de Ciências Imperial, em São Petersburgo, na Rússia. Em pouco tempo, Euler se tornou o cabeça da seção de matemática na instituição.

Euler é dos matemáticos que possuem mais trabalhos publicados na história, superando 800 se contabilizados com os publicados após sua morte. E ele não é somente

reconhecido no ramo da Matemática. Além de seus trabalhos nas áreas da álgebra, geometria, teoria dos números e tantos outros campos da Matemática, Euler tem também publicações no ramo da Astronomia, Botânica, Química, Teologia, Medicina, entre outros.

O que nos chama atenção é que sua produtividade não decresceu mesmo quando, durante o período em que atuou em São Petersburgo, ficou cego. Ele já era cego de um olho desde sua juventude, e mesmo com a cegueira total, devido a sua memória fenomenal e seu poder de concentração incomum, continuou a publicar trabalhos, com ajuda de um assistente.

Dentre suas maiores contribuições para a Matemática está a implementação da notação que é usada até nos dias atuais, tais quais: $f(x)$ para funções; e para base dos logaritmos naturais; Σ para somatório; i para a unidade imaginaria, $\sqrt{-1}$; entre tantos outros.

Na área de teoria dos números Euler não teve desempenho diferente. Como dito anteriormente, Euler demonstrou o Pequeno Teorema de Fermat e contribuiu para a demonstração do Último Teorema de Fermat, provando que para $n = 3$, não existe soluções inteiras para a equação $x^n + y^n = z^n$. Euler mostrou também que a dedução de Fermat, que dizia que $F_n = 2^{2^n} + 1$ é primo para todo n, estava errada para $n = 5$, ou seja, provou que o número 4.294.967.297 não era primo, algo fascinante para a época.

3.5 CARL FRIEDRICH GAUSS

Carl Friedrich Gauss (1777-1855), outro nome importantíssimo na matemática, possui papel fortíssimo no estudo da teoria dos números. Desde a infância, Gauss demostrava fortíssima aptidão matemática. Aos 22 anos de idade, já defendia sua tese de doutorado, a qual forneceu uma demonstração ao Teorema Fundamental da Álgebra.

Figura 5 - Carl Friedrich Gauss

Fonte: http://cdn2.rare-earth-magnets.com/images/content/johann_carl_friedrich_gauss.jpg. Acesso em 19/09/2016.

Nascido em Brunswick, na Alemanha, teve um pai que não lhe estimulava nos estudos, porém uma mãe que, mesmo numa época onde mulheres tinham a opinião desgastada, lhe deu estímulo para que estudasse.

Gauss foi uma criança prodígio. Conta Mol (2013) que, na infância, durante uma aula, o professor, para ocupar os alunos, pediu-lhes que somassem todos os números de 1 a 100. Em poucos minutos, Gauss tinha a resposta, e para a ira do professor, fora o único aluno que acertou-a. Acredita-se que Gauss usou para isso a soma de termos de uma progressão aritmética.

Aos 18 anos ingressou na faculdade na dúvida se cursaria Matemática ou Filosofia, mas se rendeu a Matemática. Um de seus feitos como aluno foi a descoberta de como traçar, com régua e compasso, um polígono regular de 17 lados (até então só se sabia traçar polígonos regulares cujos lados são números primos de lados 3 e 5). Nessa idade também já dominava várias línguas, como o Latim, o Inglês, o Francês e o Dinamarquês.

Aos 20 anos escreveu sua tese de doutorado, a qual dava a primeira demonstração satisfatória do Teorema Fundamental da Álgebra. Ao longo de sua vida, deu ainda mais três demonstrações desse teorema.

Gauss era conhecido por seus amigos por vários títulos, como Príncipe dos matemáticos, Titã, entre outros, graças a sua inteligência fora do comum. Gauss possui trabalhos de grande relevância não só na Matemática, mas também na Astronomia, Ótica, Eletricidade, entre muitos outros campos.

Na obra *Disquisitiones Arithmeticae*, a qual Gauss começou a trabalhar em 1801, ele trata da teoria dos números mais profundamente. Até então, a teoria dos números era um emaranhado de resultados isolados.

Nessa obra, ele reúne trabalhos de seus antecessores e desenvolveu novas teorias, dando uma cara nova ao assunto. Dividida em sete seções, Gauss trata nas quatro primeiras seções de uma reformulação da teoria dos números do século XIII. As seções seguintes tratam da resolução de equações específicas. Tais demonstrações serviram de base para estudos mais sofisticados nos séculos que seguiram. Essa obra é considerada o marco inicial da teoria moderna dos números.

3.6 MATEMÁTICA NO FUTURO

É impossível descobrir o que nos aguarda no estudo da Matemática para o futuro. Como já pode-se ver quando se estuda os matemáticos antigos, não existe uma linha contínua que se segue. Assuntos que estão em alta podem, de repente, se tornarem obsoletos, assim como assuntos esquecidos podem voltar à tona com resultados inimagináveis. Tem-se como maior prova dessa imprevisibilidade a criação de calculadoras e computadores, que no começo do século parecia algo inacreditável e impossível, e hoje faz parte do dia-a-dia da população, e fez com que cálculos matemáticos pudessem ser feitos em velocidades que antes não podiam nem ser imaginadas.

O mais impressionante da teoria dos números, como cita Stewart (p. 88, 2014) é o fato de, mesmo estando lidando com números simples como os inteiros, as perguntas que cercam são inúmeras, sendo que teoremas formulados séculos atrás ainda seguem sem resposta. Somente o tempo guarda a resposta dessas perguntas.

4 FUNDAMENTOS DA TEORIA DOS NÚMEROS

Atualmente, o estudo da teoria dos números está muito mais avançado que na Antiguidade como foi visto no capítulo anterior. As técnicas, fórmulas e notações matemáticas utilizadas antigamente foram, com o tempo, sendo aprimoradas e aperfeiçoadas por matemáticos e estudiosos modernos. A teoria dos números, atualmente, é a base de vários ramos da ciência, principalmente da computação.

Com o advento da tecnologia e sua constante evolução, cálculos que antigamente demorariam dias para serem feitos, hoje em dia são realizados em questão de segundos. Essa revolução tecnológica deve-se, em grande parte, ao maior entendimento matemático que se vem adquirindo durante os séculos.

Nesse capítulo, são abordados alguns desses conceitos básicos da teoria dos números que serão imprescindíveis para o entendimento de equações diofantinas e sua aplicação computacional, que podem ser encontrados em Domingues e Iezzi (2003), Milies e Coelho (2003), Domingues (2009) e Vidigal et. al. (2009).

4.1 DIVISIBILIDADE EM Z

Definição 4.1.1 Dados $a, b \in \mathbb{Z}$ e $b \neq 0$, diz-se que a divide b se, e somente se, $b = ac$, para qualquer $c \in \mathbb{Z}$. Quando isso acontece, pode-se também dizer que b é múltiplo de a ou que a é dividor de b. Quando um número a divide b, será usada a notação $a|b$, ou seja, a divide b. Caso contrário (a não divide b) será usado $a \nmid b$.

No caso da equação $b = ac$, o elemento c é chamado de quociente de b por a e pode também ser representado como $c = b/a$.

A partir dessa definição, pode-se destacar algumas propriedades imediatas:

P1: **Reflexiva**: $a|a$, para todo $a \in \mathbb{Z}$.

P2: $1|a$, para todo $a \in \mathbb{Z}$.

P3: $a|0$, para todo $a \in \mathbb{Z}$.

De acordo com essas propriedades, apresentam-se as seguintes proposições, considerando $a, b, c, d \in \mathbb{Z}$:

Proposição 4.1.1: Se $a|b \; e \; b|a \, , então \; a = \pm b$.

Prova: Sejam considerados $m, n \in \mathbb{Z}$. Como $a|b$, tem-se que $b = am$. Também, como $b|a$, tem-se que $a = bn$. Substituindo as equações, tem-se que $a = (am)\, n = a(mn)$, o que implica que $mn = 1$. A única solução possível dentro dos inteiros é $m = n = 1$ ou $m = n = -1$. Assim, conclui-se que $a = \pm b$. ♦

Proposição 4.1.2 (Transitiva): Se $a|b$ e $b|c, então \; a|c$, para todo $a, b, c \in \mathbb{Z}$.

Prova: Sejam considerados $m, n \in \mathbb{Z}$. Sabe-se que $b = an$ e $c = bm$. Por substituição, tem-se que $c = (am)n = a(mn)$. Como $mn \in \mathbb{Z}$, conclui-se que $a|c$. ♦

Proposição 4.1.3: Para todo $a, b, c \in \mathbb{Z}$. Se $a|b$ e $a|c$, então $a|(bx + cy)$, para todo $x, y \in \mathbb{Z}$

Prova: Sejam $m, n \in \mathbb{Z}$. Como $a|b$, então $b = am$. Da mesma forma, como $a|c, c = an$. Substituindo, tem-se que $bx + cy = (am)x + (an)y = a(mx) + a(ny) = a(mx + ny)$. Como $bx + cy = a(mx + ny)$, conclui-se que $a|\,(bx + cy)$. ♦

Corolário 4.1.1: Para todo $a, b \in \mathbb{Z}$. Se $a|b$, então $a|(bx)$, para todo $x \in \mathbb{Z}$.

Prova: Seja considerado $m \in \mathbb{Z}$. Como $a|b$, tem-se que $b = am$. Substituindo, tem-se que $bx = (am)x = a(mx)$. Como $bx = a(mx)$, conclui-se que $a|bx$. ♦

Proposição 4.1.4: Se $a = (b + c) \; e \; d|c$, então $d|a$ se, e somente se, $d|b$.

Prova: Sejam $m, n, p \in \mathbb{Z}$. Como $d|c, \; c = dp$.

($\Rightarrow$) Como $d|a, a = dm$. Substituindo na equação, tem-se que $dm = b + dp$. Logo, $b = dm - dp = d(m - p)$. Sabendo que $m - p \in d|b$, conclui-se que $d|b$.

($\Leftarrow$) Analogamente a prova acima, como $d|b, \; b = dn.b$. Substituindo na equação, tem-se que $a = dn + dp$. Logo, $a = d(n + p)$. Sabendo que $n + p \in \mathbb{Z}$, conclui-se que $d|a$. ♦

Proposição 4.1.5: Se $a|b$, com $a, b \neq 0$, então $|b| \geq |a|$.

Prova: Sejam considerados $n \in \mathbb{Z}$. Como $a|b$, tem-se que $b = an$. Daí, $|b| = |an|$, ou seja, $|b| = |a||n|$. Como n não pode ser 0, $|n| > 0$, o que implica em $|b| \geq |a|$.♦

4.2 NÚMEROS PRIMOS

Definição 4.2.1: Um número $p \in \mathbb{Z}$ é dito primo se, se somente se,

$$p \neq 0 \; e \; p \neq \pm 1;$$

Os únicos divisores de p são ± 1 e o próprio p.

Se um número não é primo, esse número é dito composto. De acordo com a definição, 0 e 1 não são primos nem compostos.

Teorema 4.2.1 (Teorema Fundamental da Aritmética): Para todo $a \in \mathbb{Z}, a \neq 0 \; e \; a \neq \pm 1$, existe um único conjunto de primos $p_1, p_2, p_3, \dots, p_r \in \mathbb{Z}$, com $r > 0$ tal que $a = \pm p_1 p_2 \dots p_r$.

Prova: Prova-se esse teorema por indução. Seja $P(n)$ a afirmativa: n é um número primo ou n pode ser escrito como um produto de números primos. Então, tem-se:

$P(2)$ é verdadeira, pois 2 é primo;

Suponha-se que a afirmativa é verdadeira para todo m, em que $2 \leq m \leq k$. Então é necessário provar que a afirmativa também é verdadeira para $P(k+1)$.

Se $k+1$ é primo, a afirmativa é verdadeira. Se $k+1$ é composto, então $k+1$ pode ser escrito da forma $k+1 = ab$, com $2 \leq a \leq k$ e $2 \leq b \leq k$.

Portanto, pela hipótese, $P(a) \; e \; P(b)$ são verdadeiras, logo a e b são números primos. Para demonstrar a unicidade dessa decomposição, considera-se o conjunto S:

$$S = \{n \in N : n > 2 \; e \; n \; tem \; duas \; decomposições \; distintas \; em \; fatores \; primos\}.$$

Como foi dito anteriormente, a decomposição em fatores primos é única, logo $S = \emptyset$. Mas supõe-se que, por absurdo, $S \neq \emptyset$. Considera-se também $m \in S$ o menor elemento do conjunto. Logo:

$$m = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s \tag{4.1}$$

São duas fatorações distintas de m em números primos. Reordenando esses números, caso necessário, tem-se:

$$p_1 < p_2 < \cdots < p_r \;\; e \;\; q_1 < q_1 < \cdots < q_s \tag{4.2}$$

Percebe-se que, necessariamente, $p_1 \neq q_1$. Percebe-se isso pois, caso contrário, haveriam duas decomposições diferentes do número $\frac{m}{p_1}$, que é menor que m, o que contrariaria a hipótese de que m é o menor elemento do grupo. Assim, pode-se assumir que $p_1 < q_1$.

Define-se agora um novo elemento m', tal que:

$$m' = m - (p_1 q_2 q_3 \dots q_s) \tag{4.3}$$

Substituindo a Eq. (4.1) na Eq. (4.3):

$$m' = (p_1 p_2 \dots p_r) - (p_1 q_2 \dots q_s) = p_1(p_2 \dots p_r - q_2 \dots q_s) \tag{4.4}$$

e

$$m' = (q_1 q_2 \dots q_s) - (p_1 q_2 \dots q_s) = (q_1 - p_1)(q_2 \dots q_s) \tag{4.5}$$

Como nota-se, $m' < m$. Se $p_2 \dots p_r - q_2 \dots q_s = 0$, por consequência, teria-se que $p_1 = q_1$, o que já foi mostrado ser impossível. Logo, $m' > 2$, pois $p_1 | m'$. Assim, m' tem decomposição única em fatores primos.

Como $p_1 < q_2 \leq \cdots \leq q_s$, necessariamente o fator primo p_1 deve estar presente na decomposição de $(q_1 - p_1)$. Mas isso quer dizer que $q_1 - p_1 = cp_1$, para $c \in \mathbb{Z}$. Portanto, $q_1 = cp_1 + p_1 = c(p_1 + 1)$, o que contraria o fato de q_1 ser primo. Prova-se assim, por absurdo, que $S = \emptyset$ e, por conseguinte, que a fatoração em primos é única (Vidigal et. al. 2009).

Quando o mesmo primo aparece várias vezes na fatoração, escreve-se a potência desse primo ao invés de repeti-lo.

4.3 MÁXIMO DIVISOR COMUM

Definição 4.3.1: Sejam $a, b, c \in \mathbb{Z}$. Máximo Divisor Comum de a e b, também representado por $MDC(a, b)$ é um número $d \in \mathbb{Z}$, tal que:

i) $d \geq 0$;

ii) $d|a \ e \ d|b$;

iii) $Se \ c|a \ e \ c|b, então \ c|d$.

Ou seja, $MDC(a, b)$ é o maior número positivo entre os divisores comuns de $a \ e \ b, a, b \in \mathbb{Z}$ e é único.

A partir dessa definição, pode-se destacar algumas propriedades imediatas:

P1: $MDC(a,b) = MDC(|a|,|b|)$;

P2: $MDC(a,b) = MDC(b,a)$.

P3: Se $a \neq 0$, então $MDC(0,a) = MDC(a,0) = |a|$.

Proposição 4.3.1: Se $a|b$, então $MDC(a,b) = |a|$;

Prova: Pela definição: i) Obviamente, $|a| > 0$. ii) $|a| \mid a$, pois é sabido que $a = |a| \pm 1$. iii) Se $c|a$ e $c|b$, então $c| |a|$.

Proposição 4.3.2: Sejam $a, b \in \mathbb{Z}$, com $b \neq 0$. Se $a = bq + r$, então $MDC(a,b) = MDC(b,r)$.

Prova: Como $d = MDC(a,b)$, logicamente, $d|a$ *e* $d|b$. Daí tem-se que $d|(bq)$. Pela proposição 4.1.3, tem-se que $d|(a - bq)$. Como $r = a - bq$, tem-se $d|r$. Por outro lado, se u for um inteiro tal que $u|r$ *e* $u|b$, então $u|a$ $(pois\, a = bq + r)$. Portanto, como d é máximo divisor comum de a e b, conclui-se que $u \leq d$, ou seja, d satisfaz a definição do máximo divisor comum de b e r.

Definição 4.3.2: Sejam $a, b \in \mathbb{Z}$. Se $MDC(a,b) = 1$, diz-se que a e b são $primos\ entre\ si$.

Proposição 4.3.3: Se $a|bc$ e $mdc(a,b) = 1$, então $a|c$.

Prova: Como $mdc(a,b) = 1$, decorre que $MDC(ac,bc) = c$. Como, por hipótese, $a|bc$, e, logicamente, $a|ac$, conclui-se que $a|MDC(ac,bc)$. Ou seja, $a|c$.

Proposição 4.3.4: Sejam a,b e $p \in \mathbb{Z}$. Se $p|ab$ e p é primo, então $p|a$ ou $p|b$.

Prova: Suponha que p não divide a. Logo, tem-se que $MDc(p,a) = 1$. Portanto, pela proposição 4.3.3, tem-se que $p|b$. O inverso é análogo.

Proposição 4.3.5: Sejam $a, b \in \mathbb{Z}$, com $MDC(a,b) = d$. Então, $MDC\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Prova: Seja suposto que $MDC\left(\frac{a}{d}, \frac{b}{d}\right) = k$. Então, tem-se que $\frac{a}{d} = km$ e $\frac{b}{d} = kn, m, n \in \mathbb{Z}$. Daí tem-se que $a = dkm$ e $b = dkn$. Portanto, $(dk)|a$ e $(dk)|b$. Como d é o máximo divisor comum de a e b, tem-se que $dk \leq d, k \leq 1$. Como $k \in \mathbb{Z}$, k só pode ser igual a 1, pois se $k > 1, d$ não seria mais $MDC(a,b)$. Logo, $k = MDC\left(\frac{a}{d} = \frac{b}{d}\right) = 1$. ♦

Também é possível também calcular o máximo divisor comum de mais de dois números inteiros. Nesse caso, é dito que $d = MDC(a_1, a_2, a_3, \dots, a_n)$.

Proposição 4.3.6: Sejam $a_1, a_2, a_3, \dots, a_n \in \mathbb{Z}$ sendo não todos iguais a 0. Então, $MDC(a_1, a_2, a_3, \dots, a_{n-1}, a_n) = MDC(a_1, a_2, a_3, \dots, MDC(a_{n-1,}\, a_n))$.

Prova: Seja $d = MDC(a_1, a_2, a_3, \dots, a_{n-1}, a_n)$. Para achar o valor de d é necessário achar o máximo múltiplo comum de n inteiros. Porém, pode-se chamar $MDC(a_{n-1,}\, a_n) = d_1$. Sabe-se que d_1 será ou igual ou maior a d, pois não faria sentido ser menor. Logo, é possível diminuir o número de cálculos para $n - 1$. Segue fazendo isso até que sobrem apenas dois inteiros.

4.4 ALGORITMO DA DIVISÃO DE EUCLIDES

Como visto no Capítulo 2, Euclides foi um importante matemático da Grécia antiga. Seu mais importante legado para os dias atuais foi a obra "Os Elementos", de onde surge toda a base da atualmente chamada Geometria Euclidiana. No livro VII, Euclides trata do método para achar o MDC de dois números inteiros. Esse método é extremamente rápido para mostrar qual o MDC de dois inteiros.

Lema 4.4.1 (Divisão de Euclides): Sejam $a, b \in \mathbb{Z},\ b > 0$. Existem $q, r \in \mathbb{Z}$ tal que:

$$a = bq + r$$

em que $0 \leq r < b$. Além disso, são únicos os inteiros q e r satisfazendo essas condições. Os inteiros a, b, q, r são chamados, nessa ordem, de $dividendo, divisor, quociente\ e\ rest$.

Prova (existência): Seja $b \in \mathbb{Z}$. Para todo $a \in \mathbb{Z}$,, tem-se que ou a é múltiplo de b ou a está compreendido entre dois multiplos de b. Ou seja:

$$bq \leq a \leq b(q + 1) \tag{4.6}$$

Para $q \in \mathbb{Z}$. Somando $-(bq)$ em cada termo da Eq. (4.6), tem-se:

$$0 \leq a - bq < b \tag{4.7}$$

Chama-se o termo $a - bq$ de r. Assim, conclui-se que $a - bq = r$, ou seja:

$$a = bq - r, 0 \leq r < b \tag{4.8}$$

Prova (unicidade): Sejam $q_1, q_2, r_1, r_2 \in \mathbb{Z}, q_1 \neq q_2,\ r_1 \neq r_2$, e sejam as igualdades $a = bq_1 + r_1$, com $0 \leq r_1 < b$, e $a = bq_2 + r_2$, com $0 \leq r_2 < b$. Como já foi visto, $b > r_1$ e $b > r_2$. Logicamente, então $b > r_1 - r_2$ (i). Também se tem que $a = bq_1 + r_1 = bq_2 + r_2$, o que implica em $b(q_2 - q_1) = r_1 - r_2$. Fazendo $(q_2 - q_1) = k$, tem-se que $bk = r_1 - r_2$, ou seja, $b|(r_1 - r_2)$. Portanto, para que isso seja possível, $b < r_1 - r_2$, o que é absurdo, pois difere do que foi provado em (i). Logo, $q_1 = q_2$ *e* $r_1 = r_2$.

Para calcular o MDC de dois inteiros pelo algoritmo de Euclides usa-se a técnica de divisões sucessivas. Na primeira divisão, divide-se os dois inteiros a *e* b. Em seguida, divide-se o divisor da divisão anterior, no nosso caso b, pelo resto da equação anterior, no nosso caso, r, e assim sucessivamente, até que seja encontrado resto 0. O $MDC(a, b)$ será o último resto não nulo nesse processo. Exemplifica-se o método a seguir:

$$a = bq_1 + r_1$$

$$b = r_1 q_2 + r_2$$

$$r_1 = r_2 q_3 + r_3$$

...

$$r_{n-2} = r_{n-1} q_n + r_n$$

$$r_{n-1} = r_n q_{n+1} + 0$$

Nesse caso, tem-se que $MDC(a, b) = r_n$.

Teorema 4.4.2 (Relação de Bézout): Sejam $a, b \in \mathbb{Z}$, ambos não nulos, e seja $d = MDC(a, b)$. Nessas condições, existem $m, n \in \mathbb{Z}$ tais que $am + bn = d$.

Prova: Considerando $S = \{ax + by \,|x, y \in \mathbb{Z}\}$. Sabe-se que $S \neq \emptyset$ pois $a.a + b.b = a^2 + b^2 \in S$ e também se nota que $a^2 + b^2 > 0$, logo S possui elementos estritamente positivos. Sendo d o menor desses inteiros, prova-se a seguir que $d = MDC(a, b)$. Como $d \in S$, então existem $x_0, y_0 \in \mathbb{Z}$, tais que

$$ax_0 + by_0 = d \tag{4.9}$$

Aplicando o algoritmo das divisões sucessivas em a e d:

$$a = dq + r \tag{4.10}$$

E, em seguida substituindo a Eq. (4.9) na Eq. (4.10):

$$a = (ax_0 + by_0)q + r \tag{4.11}$$

Após manipulações na Eq. (4.11), tem-se:

$$r = a(1 - qx_0) + b\big(q(-y_0)\big), \tag{4.12}$$

Logo, conclui-se que, $r \in S$. Como $0 \leq r < d$, conclui-se que r é positivo. Porém, como d é o menor dos elementos do conjunto pela hipótese, tem-se somente que $r = 0$. Então, $a = dq$ e $d|a$. Analogamente, se prova que $d|b$.

5 RESOLUÇÃO DE EQUAÇÕES DIOFANTINAS

Segundo Domingues (2009), são consideradas equações diofantinas todas as equações polinomiais, em várias incógnitas, com coeficientes inteiros, sempre que se trata de procurar suas possíveis soluções também entre os inteiros. De modo geral, é uma equação do tipo:

$$f(x_1, x_2, \ldots, x_n) = 0,$$

em que f é uma função n-variável com $n \geq 2$ e coeficientes inteiros. Nesse trabalho são estudadas as Equações Diofantinas lineares que são equações do tipo:

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = b,$$

sendo $a_1, a_2, \ldots, a_n$ e b números inteiros, cujas soluções são inteiros $x_1, x_2, \ldots, x_n$.

Problemas envolvendo equações diofantinas são muito comuns no dia-a-dia, como do tipo "quantos pães de R$5,00 e sucos de R$8,00 poderei comprar com R$60,00".

A partir desse problema, algumas questões nos vêm à cabeça de imediato:

- Quais as condições para que existam soluções inteiras?
- Caso existam, quantas são as soluções inteiras? E soluções inteiras estritamente positivas?
- Como calcular essas soluções?

As soluções das perguntas em questão são exploradas nesse capítulo. Apesar do termo Equação Diofantina abranger equações com qualquer número de incógnitas, aqui é apresentado um estudo com equações lineares de duas incógnitas, como no exemplo acima.

O primeiro passo é certificar-se da existência ou não de soluções inteiras para a equação diofantina dada. A seguir é enunciado o Teorema que permite verificar a existência de soluções inteiras. Toda a teoria apresentada aqui pode ser encontrada em em Domingues e Iezzi (2003), Milies e Coelho (2003), Domingues (2009) e Vidigal et. al. (2009).

5.1 CONDIÇÃO DE EXISTÊNCIA E SOLUÇÃO GERAL

A condição necessária e suficiente para determinar se uma equação linear tenha solução inteira é dada pelo teorema a seguir.

Teorema 5.1.1 Uma equação diofantina linear do tipo $ax + by = c$, em que $a, b \in \mathbb{Z}$,, $a \neq 0$ ou $b \neq 0$, admite solução se, e somente se, $d = MDC(a, b)|c$.

Prova:

($\Rightarrow$) Seja (x_0, y_0) uma solução inteira para a equação acima. Logo, vale a igualdade:

$$ax_0 + by_0 = c \tag{5.1}$$

Como $d|a$ e $d|b$, temos que $d|c$ (Proposição 4.1.3).

($\Leftarrow$) Pelo Teorema 4.4.2, sendo $d = MDC(a, b)$, é garantido que $d = ax_0 + by_0$ para algum $x_0, y_0 \in \mathbb{Z}$. Mas da hipótese, $d|c$. Segue que $c = dt, t \in \mathbb{Z}$. Portanto,

$$c = dt = (ax_0 + by_0)t = ax_0\, t + by_0\, t \tag{5.2}$$

Como $x_0\, t, y_0\, t \in \mathbb{Z}$, o par $(x_0 t, y_0 t)$ é solução inteira da equação. ♦

Exemplo 5.1.1: A equação $24a + 54b = 7$ não admite solução inteira, pois $MD\ (24{,}54) = 6$ e $6 \nmid 7$.

Já a equação $14a + 49b = 21$ admite solução inteira, pois $MDC(14{,}49) = 7$ e $7|21$.

5.2 RESOLUÇÃO PARA EQUAÇÕES COM DUAS VARIÁVEIS

Satisfeita a condição de existência de soluções inteiras para equação diofantina dada, apresentada no Teorema 5.1.1, pode-se iniciar os cálculos das soluções. Para encontrar a solução geral, primeiramente é necessário calcular uma solução particular. Para tal, usa-se o algoritmo de divisões sucessivas de Euclides para calcular o $MDC(a, b)$. Generalizando esse algoritmo, tem-se que, no caso de uma equação do tipo $ax + by = c$:

$$\begin{gathered} a = bq_1 + r_1 \\ b = r_1 q_2 + r_2 \\ r_1 = r_2\, q_3 + r_3 \\ . \\ . \\ . \\ r_{n-3} = r_{n-2}\, q_{n-1} + r_{n-1} \end{gathered} \tag{5.2}$$

$$r_{n-2} = r_{n-1}\, q_n + r_n$$

$$r_{n-1} = r_n q_{n-1} + 0.$$

Portanto, o $MDC(a,b) = r_n = d$.

Primeiramente, deve-se escrever $MDC(a,b)$ como combinação linear de a e b, isto é, $ar + bs = d$. Para achar os valores de r e s, deve-se fazer o seguinte:

É possível expressar $d = r_n$ como uma combinação linear de r_{n-2} e r_{n-1}, no caso:

$$r_n = r_{n-2} - r_{n-1}\, q_n \tag{5.3}$$

Substituindo sucessivamente os restos das equações anteriores a Eq. (5.3) encontradas no processo (5.2), tem-se:

$$r_n = r_{n-2} - (r_{n-3} - r_{n-2}\, q_{n-1})q_n$$

$$= r_{n-2}(1 + q_{n-1}\, q_n)q_n\, r_{n-3} \tag{5.4}$$

Agora, a Eq. (5.4) está em termos de r_{n-3} e r_{n-2}. Continuando a escrever $MDC(a,b)$ como combinação linear dos restos das divisões sucessivas até o topo do processo (5.2), será encontrada uma combinação linear de a e $b, ar + bs = d$.

Finalmente, para achar a solução trivial desejada da equação da $ax + by = c$, basta multiplicar ambos os lados da equação por $\frac{c}{r_n}$, obtendo:

$$ar\frac{c}{r_n} + bs\frac{c}{r_n} = d\frac{c}{r_n} \tag{5.5}$$

Sabendo que $d = r_n$, tem-se:

$$ar\frac{c}{r_n} + bs\frac{c}{r_n} = c \tag{5.6}$$

Então, conclui-se que a solução particular é dada por:

$$(x_0, y_0) = \left(r\frac{c}{r_n}, s\frac{c}{r_n}\right) \tag{5.7}$$

Teorema 5.2.1 Seja (x_0, y_0) uma solução inteira para a equação diofantina $ax + by = c$. Então, essa equação admite infinitas soluções inteiras da forma:

$$x = x_0 + \frac{b}{d}t \tag{5.8}$$

$$y = y_0 - \frac{a}{d}t \tag{5.9}$$

em que $d = MDC(a,b)$ e com $t \in \mathbb{Z}$.

Prova: Suponha-se que (x, y) seja uma solução qualquer da equação. Então:

$$\mathrm{ax} + \mathrm{by} = \mathrm{ax}_0 + \mathrm{by}_0 = \mathrm{c}, \tag{5.10}$$

em que pode-se concluir que

$$a(x - x_0) = b(y_0 - y) \ . \tag{5.11}$$

Dividindo ambos os lados da Eq. (5.11) por d, e chamando $\frac{a}{d} = r \ e \ \frac{b}{d} = s$, tem-se:

$$r(x - x_0) = s(y_0 - y) \tag{5.12}$$

Portanto, $r|[s(y_0 - y)]$. Pela proposição 4.3.3 vê-se que $MDC(r, s) = 1$. Logo, $r|(y_0 - y)$ e daí, $y_0 - y = rt$, e conclui-se que $y = y_0 - rt = \ y_0 - \frac{a}{d}t$.

Analogamente, é possível obter $x = x_0 + \frac{b}{d}t$.

Para encontrar os valores de *x* e *y* estritamente positivos, basta aplicar a condição $x > 0$ e $y > 0$. Das Eqs. (5.8) e (5.9), tem-se:

$$x_0 + \frac{b}{d}t > 0, \ y_0 - \frac{a}{d}t > 0 \tag{5.13}$$

Daí, basta isolar *t* em ambas inequações, e teremos a condição:

$$\frac{y_o d}{a} > t > -\frac{x_0 d}{b} \tag{5.14}$$

Cabe observar que a mudança no sinal de *a* ou *b* mudará a desigualdade.

Corolário 5.2.1 Numa equação diofantina do tipo $ax + by = c$, se $a, b \in \mathbb{Z}$ são primos entre si, essa equação sempre terá solução.

Prova: Como $a, b \in \mathbb{Z}$ são primos entre si, tem-se que $MDC(a, b) = 1$. Pelo Teorema 5.1.1, qualquer equação diofantina somente admite solução nos inteiros caso $MDC(a, b)|c$. Como $1|c$, esta equação tem solução.

Exemplo 5.2.1 Encontre uma solução para a equação $32x + 9y = 7$

Primeiramente, checa-se se a equação tem solução inteira. Como $MDC(32{,}9) = 1$, afima-se que a equação tem solução inteira, pelo Corolário 5.2.1.

Fazendo o uso do algoritmo de Euclides, tem-se:

$$32 = 9 \cdot 3 + 5 \tag{i}$$

$$9 = 5 \cdot 1 + 4 \tag{ii}$$

$$5 = 4 \cdot 1 + 1 \quad \text{(iii)}$$

$$4 = 1 \cdot 4 + 0 \quad \text{(iv)}$$

O próximo passo será escrever as equações (i), (ii) e (iii) em função dos restos das divisões euclidianas.

$$\begin{aligned} 1 &= 5 - 4 \cdot 1 \\ &= 5 - (9 - 5 \cdot 1) \cdot 1 \\ &= 5 - 9 \cdot 1 + 5 \cdot 1 \\ &= 5 \cdot 2 - 9 \cdot 1 \\ &= (32 - 9 \cdot 3) \cdot 2 - 9 \cdot 1 \\ &= 32 \cdot 2 - 9 \cdot 6 - 9 \cdot 1 \\ &= 32 \cdot 2 - 9 \cdot 7 \end{aligned}$$

Encontra-se uma combinação linear para 32 e 9, tal que:

$$32 \cdot 2 + 9 \cdot (-7) = 1$$

Então, obtém-se $r = 2$ e $s = -7$. Agora, multiplica-se ambos os lados por c/r_n, ou seja, 7, o que resulta em:

$$32 \cdot 14 + 9 \cdot (-49) = 7$$

Portanto a solução trivial é $(14, -49)$. Assim, foram encontrados os valores triviais da nossa equação. As soluções gerais serão:

$$x = 14 + 9t$$

$$y = -49 - 32t, \ \ t \in \mathbb{Z}.$$

Para encontrar os valores estritamente positivos de x e y, basta dar a condição a ambos:

$$x > 0 \Leftrightarrow 14 + 9t > 0 \Leftrightarrow t > (-14)/9 \Leftrightarrow t > -1$$

$$y > 0 \Leftrightarrow -49 - 32t > 0 \Leftrightarrow t < (-49)/32 \Leftrightarrow t < -1$$

Percebe-se assim que não existem soluções inteiras para que x e y sejam ambos positivos.

5.3 EQUAÇÕES DE TRÊS VARIÁVEIS

Agora, considere a equação diofantina com três variáveis inteiras:

$$a_1x + a_2y + a_3z = b.$$

A mesma argumentação utilizada no Teorema 5.1.1 é aplicada, ou seja, essa equação somente terá solução inteira se $MDC(a, b, c) \mid d$.

Seja $MDC(a_1, a_2) = d_1$. Então existem $k_1, k_2 \in \mathbb{Z}$ tais que:

$$a_1k_1 + a_2\, k_2 = d_1 \tag{5.15}$$

Pelo Teorema 4.3.2, tem-se então que $d = MDC(d_1, a_3)$. Da mesma forma, existem $k, z_0 \in \mathbb{Z}$ tais que:

$$d_1k + a_3z_0 = d \tag{5.16}$$

Substituindo a Eq. (5.13) na Eq. (5.14) tem-se:

$$d = (a_1k_1 + a_2k_2\,)k + a_3z_0 = \; a_1k_1k + a_2k_2k + a_3z_0 \tag{5.17}$$

Fazendo $k_1k = x_0$ e $k_2k = y_0$, tem-se finalmente:

$$a_1x_0 + a_2y_0 + a_3z_0 = d \tag{5.18}$$

Como $a_1x_0 + a_2y_0 + a_3z_0 = d$ admite solução, temos que $b = dq, q \in \mathbb{Z}$. Então:

$$a_1x_0\, q + a_2y_0\, q + a_3z_0\, q = dq = b \tag{5.19}$$

O que nos dá que (x_0q, y_0q, z_0q) é uma solução da equação.

Exemplo 4.3.1: Encontre a solução da equação diofantina $4x + 8y + 5z = 7$.

Primeiro, encontramos $MDC(4{,}8) = 4$. Então:

$$4(x + 2y) + 5z = 7 \tag{5.20}$$

Agora, diz-se que $x + 2y = w$. Substituindo em (5.20):

$$4w + 5z = 7 \tag{5.21}$$

Agora tem-se uma equação com duas variáveis, o que já é conhecido como calcular. Utilizando o algoritmo de Euclides:

$$5 = 4 \cdot 1 + 1$$

$$4 = 1 \cdot 4 + 0$$

Substituindo os restos:

$$1 = 5 \cdot 1 - 4 * 1$$

Multiplicando a equação por 7, tem-se as soluções triviais $w_0 = -7, z_0 = 7$. As soluções gerais são:

$$w = -7 + 5t$$

$$z = 7 - 4t, t \in \mathbb{Z}$$

Porém, não interessa o valor de w, e sim de x e y. Então, volta-se a expressar a solução em termos de x e y:

$$x + 2y = -7 + 5t \tag{5.22}$$

Como $MDC(1,2) | (-7 + 5t)$, para qualquer $t \in \mathbb{Z}$, essa equação tem solução inteira.

Tem-se como solução trivial

$$x_0 = -7 + 5t$$

$$y_0 = 0$$

Logo, as soluções gerais da equação dada são:

$$x = -7 + 5t + 2u$$

$$y = -u$$

$$z = 7 - 4t, \qquad t, u \in \mathbb{Z}$$

Equações com 4 ou mais variáveis seguem o mesmo princípio.

5.4 APLICAÇÕES DE EQUAÇÕES DIOFANTINAS DE DUAS VARIÁVEIS

5.4.1 Situações-Problema

No início desse capítulo, foi apresentado o seguinte problema: “quantos pães de R$5,00 e sucos de R$8,00 poderei comprar com RS60,00?”. Esse é um exemplo de aplicação de equações diofantinas no dia-a-dia. Para resolvê-lo, primeiramente escreve-se esse problema na forma algébrica: $5x + 8y = 60$, sendo x o número de pães e y o número de sucos. Usando os métodos de resolução apresentados, tem-se como um dos valores que satisfazem essa equação é $x = -180$ e $y = 120$. Porém, vê-se que esse valor é absurdo, pois não existe como comprar uma quantidade negativa de pães. Basta então achar os valores de *t*

em que x e y serão positivos, como visto na Definição (5.2.1). Assim, encontram-se $x = 4$ e $y = 5$, valores que satisfazem o problema.

Segue um a lista de diversos tipos de situações problemas que podem ser encontrados no dia-a-dia.

Problema 1 (Problema de Mahaviracarya, matemático hinhu (Domingues e Iezzi, p. 52, 2003)): Uma certa quantidade de maçãs é dividida em 37 montes de igual número. Após serem retiradas 17 frutas, as restantes são acondicionadas em 79 caixas, cada uma com a mesma quantidade. Quantas maçãs foram colocadas em cada caixa? Quantas maçãs tinha cada monte?

Problema 2: Deseja-se sacar R$ 1000,00 em notas de R$ 20,00 e R$ 50,00. Apresente um método para encontrar formas distintas de efetuar esse saque?

Problema 3: Uma loja de conveniência trabalha com diversas marcas de café. Num determinado mês, um comprador desta loja adquiriu 2 tipos de café – tipo A (normal) e tipo B (descafeinado). Sabendo-se que ele gastou exatamente R$ 58,00, quais são as diversas maneiras que ele pode adquirir os pacotes do tipo A e do tipo B? O preço do pacote da marca A é R$ 2,00 e do pacote da marca B, R$ 3,00 (POMMER, 2008, p.61).

Problema 4: Uma aluna, Bianca, fã de música, reserva num certo mês R$ 70,00 para a compra de CDs ou DVDs. Um CD custa R$ 12,00 e um DVD R$ 16,00. Quais são as possibilidades de compra destes dois bens gastando-se exatamente R$ 70,00 (POMMER, 2008, p.63).

Problema 5: Quantas quadras de basquete e quantas quadras de vôlei são necessárias para que 80 alunos joguem simultaneamente?

Problema 6: O valor da Entrada de um cinema é R$8,00 e da meia R$5,00. Qual é o menor número de pessoas que pode assistir a uma sessão de maneira que a bilheteria seja de R$500,00?

5.4.2 Aplicações na Matemática

Problemas simples de Matemática podem ser resolvidos por equações diofantinas, como a lista a seguir.

Problema 1 (Problema do Matemático L. Euler (Domingues e Iezzi, p. 52, 2003)). Decomponha o número 100 em duas parcelas positivas tais que uma é múltiplo de 7 e a outra de 11.

Problema 2: Ache todos os números inteiros estritamente positivos com a seguinte propriedade: dão resto 6 quando divididos por 11 e resto 3 quando divididos por 7.

Problema 3: Determine duas frações positivas que tenham 13 e 17 como denominadores e cuja soma seja igual a $\frac{305}{221}$.

Problema 4: Encontre todos os valores positivos de x e y que sejam soluções da equação indeterminada 7x+19y=1921 de modo que a soma x+y seja a menor possível.

Problema 5: Dê uma interpretação geométrica, em termos de coordenadas cartesianas, para o fato de que a equação diofantinas linear em duas incógnitas, quando admite uma solução, admite infinitas.

5.4.3 Aplicação em Química

Além de problemas do cotidiano, várias outras áreas da ciência e da sociedade utilizam equações diofantinas para resolver os seus problemas. Tem-se como exemplo o balanceamento de equações químicas. Em reações químicas, a quantidade de moléculas presentes nos reagentes deve ser igual a quantidade de moléculas presentes nos produtos. Uma maneira de calcular essas quantidades é usando equações diofantinas. Como exemplo, temos a seguinte equação química, estudada por Silva et al. (2016):

$$NH_4NO_3 \rightarrow N_2O + H_2O \tag{5.23}$$

Aqui, as substancias presentes do lado esquerdo da seta são as chamadas reagentes, e as do lado direito, produtos. Percebe-se que existe quatro moléculas de hidrogênio (*H*) do lado esquerdo, e duas do lado direito. Vê-se que a equação está desbalanceada. Para achar os valores para o balanceamento, chamamos de *x, y* e *z* os coeficientes:

$$xNH_4NO_3 \rightarrow yN_2O + zH_2O \tag{5.24}$$

Realizando os cálculos necessários, é possível resolver essa equação calculando a resolução da equação diofantina $2x - z = 0$. Usando o método de resolução visto

anteriormente, conclui-se que uma das respostas para essa equação é $x = 1, y = 1$ e $z = 2$. A equação balanceada será:

$$NH_4NO_3 \rightarrow N_2O + 2H_2O \tag{5.25}$$

6 DESENVOLVIMENTO COMPUTACIONAL

Neste trabalho, foi implementado o algoritmo estudado na plataforma *Android*, pela facilidade de manipulação e a grande fração do mercado atual que essa plataforma abrange.

"O *Android* ... consiste em uma nova plataforma de desenvolvimento para aplicativos móveis, baseada em um sistema operacional Linux, com ... um ambiente de desenvolvimento bastante poderoso, ousado e flexível. " (LECHETA, 2015, p. 20).

Em um programa *Android*, as linguagens de programação que são utilizadas são XML e JAVA. XML é usado para a criação do layout do aplicativo, usando para isso diversos *widgets*[1], como botões, caixas de texto, barras de seleção, etc. Já a linguagem JAVA é usada para fazer a parte "de trás" do aplicativo, ou seja, as funções que rodam quando se clica em um dos *widgets* mencionados anteriormente, assim como o link entre esses *widgets* e as funções. O ambiente de desenvolvimento utilizado foi o *Android Studio*.

Para efeito do nosso trabalho, são apresentadas as funções feitas em JAVA, as quais são usadas para resolver equações diofantinas de duas variáveis.

6.1 MÁXIMO DIVISOR COMUM

Para iniciar os cálculos das equações diofantinas na forma $ax + by = c$, é necessário, como dito no Teorema 5.1.1, que o $MDC(a,b) = d$ divida c. Logo, o primeiro passo da implementação é criar uma função que verifique o MDC dos coeficientes dados.

Segue o código da função que recebe dois coeficientes inteiros como argumentos.

```
private int gcd(int x, int y) {
    if (y == 0)
        return Math.abs(x);
    return GCD(y, x % y);
}
```

[1] Um widget é um componente de interface gráfica que visa facilitar o acesso a certa função ou programa.

A função calcula o MDC dos inteiros x e y por recorrência. Caso o valor de y seja 0, ou seja, quando o resto das divisões sucessivas resulta em 0, a função retorna o valor de x, que é o último resto não nulo das divisões. Caso y não seja nulo, a função retorna ela mesma, porém agora os coeficientes são y no lugar de x e o resto da divisão de x por y no lugar de y. A função é declarada privada pois ela é usada somente na classe que é declarada e serve apenas para testar se é possível encontrar soluções inteiras para a equação dada.

As funções que segue se encontram dentro da classe Diophantine, cujas variáveis são as seguintes:

```
public class Diophantine {

    private int a;
    private int b;
    private int c;
    private int gcd;
    private int r;
    private int s;
    private List<Integer> posList;
    private Context context;
...
```

6.2 ALGORITMO EUCLIDIANO

A próxima função calcula a combinação linear entre os termos $a\ e\ b$ da equação diofantina e $MDC(a,b)$. Essa função recebe dois coeficientes inteiros, $a\ e\ b$, e não retorna nenhum valor. Ela muda os valores dos objetos da classe.

```
public void extended_gcd(int a, int b) {
    int s = 0;  // s and t are the factors, where tx + sy = d (d is GCD(a,b))
    int old_s = 1;

    int t = 1;
    int old_t = 0;

    int r = Math.abs(b); //this is the remainder
    int old_r = Math.abs(a);

    while (r != 0) {
        int q = old_r / r;

        int temp = old_r;
        old_r = r;
        r = temp - q * r;

        temp = old_s;
        old_s = s;
        s = temp - q * s;

        temp = old_t;
        old_t = t;
        t = temp - q * t;
```

```
    }

    int signa = a > 0 ? 1 : -1;
    int signb = b > 0 ? 1 : -1;
    this.r = old_s * signa;
    this.s = old_t * signb;
    this.gcd = Math.abs(old_r);
}
```

Primeiramente, são declaradas seis variáveis inteiras. São elas: *s, old_s, t, old_t, r, old_r*. As variáveis *s* e *t* são as variáveis da combinação linear $sa + tb = MDC(a, b)$. As variáveis *old_s* e *old_t* são usadas para guardar os valores de *s* e *t* do passo anterior, respectivamente. É necessário saber o valor anterior de *s* e *t* para realizar esse algoritmo. A variável *r* é o resto das divisões, e da mesma forma que antes, *old_r* guarda o resto da divisão anterior.

Enquanto o valor de *r* for diferente de 0 (pois se for 0, chega-se no final das divisões), o programa procede o seguinte:

Define uma variável *q*, a qual é o quociente da divisão. Cria uma variável temporária chamada de *temp*, que irá guardar o valor de *old_r*, ou seja, do resto da divisão anterior (ou no primeiro passo, o valor de *a*). Atribui o valor de *r* a *old_r*. Em seguida, atribui o valor obtido na divisão para *r*. Tem-se que *a=bq+r*. Logo, *r=a-bq*. No caso da função, como o valor de *a* está atribuída a *temp* e o valor *b* atribuído a *old_r*, tem-se que o valor do resto atual, ou seja, de *r* será *temp-q*old_r*.

Analogamente, se repetem os passos para *t* e *s*.

Ao final do *loop*, tem-se que *r=0*, o que quer dizer que o resto anterior, ou seja, *old_r* resulta no MDC(a,b). Tem-se assim a combinação linear desejada se forem analisados os parâmetros *old_s* e *old_t*.

Ao final da função, um ajuste de sinal é feito, caso os coeficientes digitados sejam negativos.

6.3 SOLUÇÕES INTEIRAS ESTRITAMENTE POSITIVAS

Outra funcionalidade do aplicativo é a possibilidade de determinar o intervalo para o qual as soluções da equação dada são positivas. Ou seja, tendo as soluções gerais:

$$x = x_0 + \frac{b}{d}\,t$$

$$y = y_0 - \frac{a}{d}\,t$$

Deseja-se saber qual o intervalo de *t* para o qual os valores de *x* e *y* são ambos positivos. Para isso, a seguinte função é escrita. A função retorna uma lista com os valores de *t* os quais permitem soluções positivas.

```
private List<Integer> PositiveOnly() {

    double tx = (-this.r * this.c * 1.0) / (b * 1.0);
    double ty = (this.s * this.c * 1.0) / (a * 1.0);

    int signa = a > 0 ? 1 : -1;
    int signb = b > 0 ? 1 : -1;

    List<Integer> list = new ArrayList();

    if (signa == 1) {
        if (signb == 1) {
            for (int i = (int) Math.ceil(tx + 0.1); i < ty; i++) {
                list.add(i);
            }
        } else {
            for (int i = (int) Math.min(tx, ty) - 1; i > -10000; i--) {
                list.add(i);
            }
        }
    } else {
        if (signb == 1) {
            for (int i = (int) Math.ceil(Math.max(tx, ty)); i < 10000; i++) {
                list.add(i);
            }
        } else {
            for (int i = (int) Math.ceil(ty + 0.1); i < tx; i++) {
                list.add(i);
            }
        }
    }
    return list;
}
```

Isolando t nas soluções gerais de *x* e *y*, tem-se que $t > \frac{-x_0 d}{b}$ e $t < \frac{y_0 d}{a}$. Serão usadas essas desigualdades no código. Logo, duas variáveis são declaradas, *tx* e *ty*, as quais calculam, respectivamente, esses valores de *t*.

Em seguida, são declarados dois inteiros, *signa* e *signb*. Eles irão guardar o sinal dos coeficientes *a* e *b*, respectivamente. Também é declarada uma lista de inteiros, *List<Integer>list*, que armazenará os valores do intervalo que se deseja encontrar.

Na próxima parte, pode ser visto alguns *ifs* e *elses*. Eles irão checar se o sinal dos coeficientes *a* e *b* são positivos ou negativos, usando para isso os inteiros *signa* e *signb*. Dependendo dos sinais, o aplicativo retornará uma lista diferente.

Caso o sinal de *a* seja positivo, tem-se que o maior valor de *t* que se pode encontrar será o valor de *ty*. Caso o sinal de *b* também seja positivo, o menor valor de *t* será o valor de *tx*. Assim, calcula-se esse intervalo, e os valores encontrados são armazenados na lista anteriormente declarada. Mas caso o valor de *a* seja positivo, porém *b* seja negativo, os valores de *t*, que são procurados, serão menores que o menor valor entre *tx* e *ty*. Assim, o programa escolherá, por meio da função *Math.min( )* o menor valor entre *tx* e *ty*, e o intervalo desejado de *t* será desse valor até -∞.

Agora, caso o sinal de *a* seja negativo, *ty* se torna o menor valor possível para *t* naquele caso. Sendo o sinal de *b* positivo, tem-se que o intervalo de *t* que é procurado será o intervalo entre o maior entre os inteiros *tx* e *ty*, calculado pela função *Math.max ( )*, e +∞. Caso sejam ambos *a* e *b* negativos, o intervalo será entre *ty* e *tx*, o oposto do caso quando ambos eram positivos. Assim, tem-se uma lista com os valores de *t* os quais satisfazem o sistema acima, lista a qual será o retorno da função.

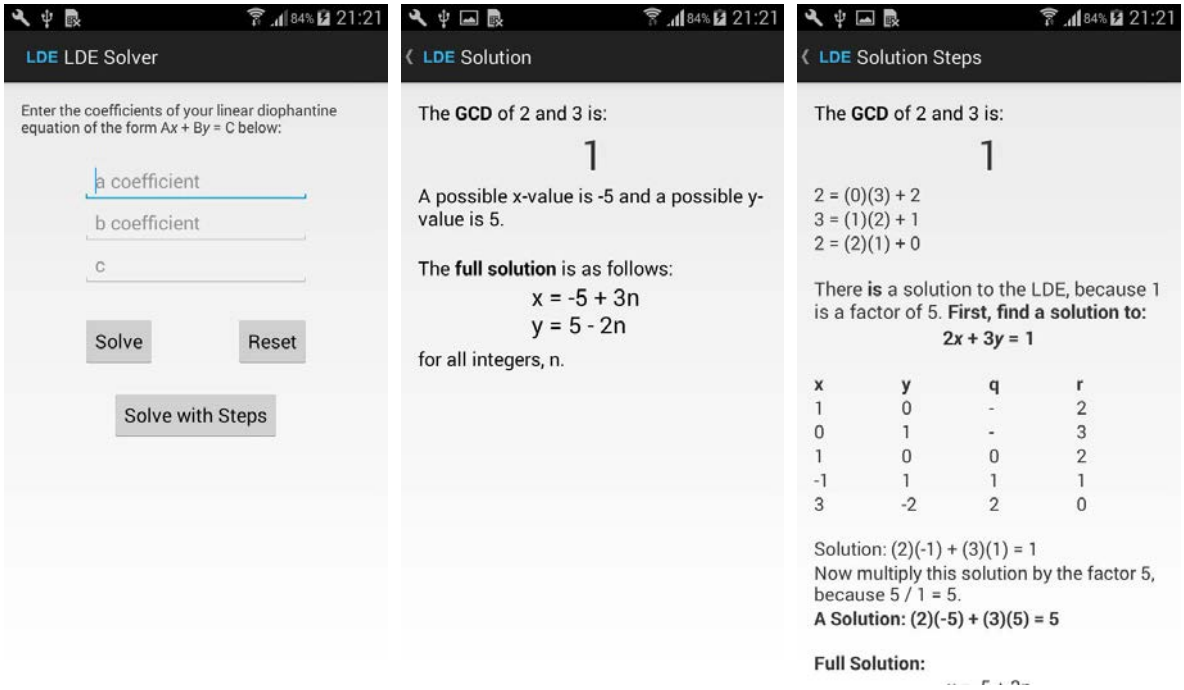
7 APLICATIVOS ENVOLVENDO CÁLCULO DE EQUAÇÕES DIOFANTINAS

Nesse capítulo, são apresentados alguns aplicativos gratuitos que realizam a função de calcular as possíveis soluções inteiras de uma equação diofantina dada. Os aplicativos analisados são da plataforma *Android*, os quais podem ser obtidos através da loja virtual *PlayStore*. Também foi analisado um aplicativo para navegador de Internet.

7.1 APLICATIVO: LINEAR DIOPHANTINE EQUATIONS

Este aplicativo com desenvolvido por Stephen Marcok. A versão analisada foi a versão 1.0 e está disponível para a plataforma *Android*.

Figura 6 - Telas do aplicativo Linear Diophantine Equations



Fonte: autoria própria

O aplicativo utiliza uma tela de entrada simples, com três campos para digitar os coeficientes a, b e c. Apresenta também três botões: *Solve* resolve a equação de forma sucinta; *Reset* apaga os valores já digitados nos campos; e *Solve with Steps* resolve a equação com mais detalhes do processo.

Ao apertar o botão *Solve*, o aplicativo apresenta o valor do *MDC* dos coeficientes digitados, valores iniciais de *x* e *y* e a solução geral. Já quando é apertado o botão *Solve with Steps* mais informações são mostradas. Mostra o processo de encontrar o MDC pelas sucessivas divisões euclidianas, visto no Lema (4.4.1); também é mostrado o processo de encontrar uma combinação linear para o MDC, visto no Teorema (4.4.2). Em seguida apresenta a solução geral. Pode ser visto, na Figura 6, respectivamente, a tela de início, a tela caso seja pressionado o botão *Solve* e a tela quando é pressionado o botão *Solve with Steps*.

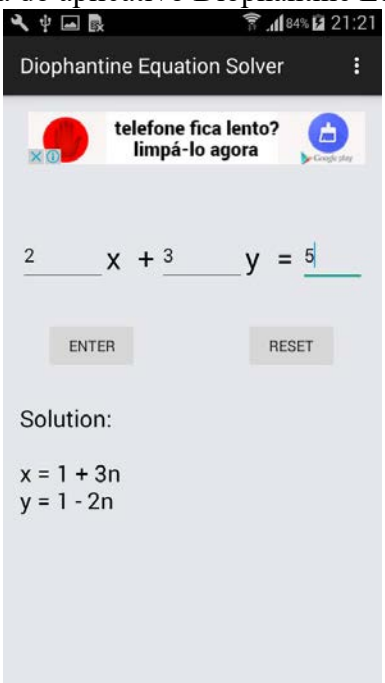
Caso um dos botões sejam apertados sem antes terem sido digitados os coeficientes da equação, um alerta aparece ao usuário dizendo que é necessário digitar os três inteiros.

Um problema encontrado no aplicativo é quando o usuário insere valores negativos para o coeficiente *a*. Na tela seguinte, na solução geral, aparecem dois sinais de negativo, sendo o correto apenas um.

7.2 APLICATIVO: DIOPHANTINE EQUATION SOLVER

Este aplicativo com desenvolvido por Mathlogic. A versão analisada foi a versão 1.1 e está disponível para a plataforma *Android*.

Figura 6 - Tela do aplicativo Diophantine Equation Solver



Fonte: autoria própria

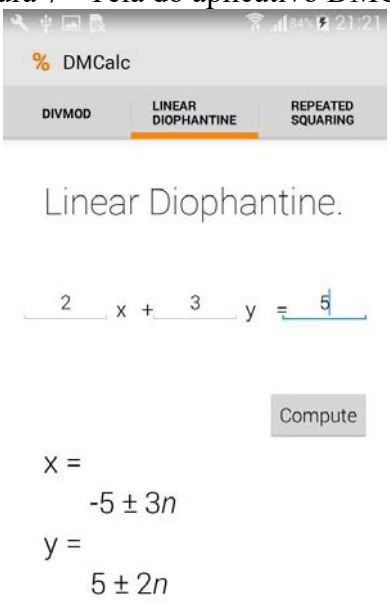
O aplicativo utiliza uma tela muito semelhante a criada nesse trabalho, que será apresentada no próximo capítulo. São encontrados três campos para serem digitados os valores dos coeficientes *a,b* e *c*. São também encontrados dois botões, um com o escrito *Enter* e outro *Reset*. Ao clicar no botão *Enter* após digitar os valores desejados, aparece, na mesma tela, a solução geral da equação, como é visto na Figura 7. O aplicativo é bem simples e não possui muitos detalhes sobre como foi feito o processo de resolução. Caso seja digitado uma equação sem solução, apenas a frase *No solutions* (Sem soluções) é mostrada.

Um problema encontrado foi quando o coeficiente *c* tem mais do que dois algarismos. O aplicativo não fornece solução correta.

7.3 APLICATIVO DMCALC

Este aplicativo com desenvolvido por Victor Szeto. A versão analisada foi a versão 1.0.2 e está disponível para a plataforma *Android*.

Figura 7 - Tela do aplicativo DMCalc



Fonte: autoria própria

Esse aplicativo possui mais funções da estudada nesse trabalho. Ao abrir o aplicativo, é possível escolher entre o cálculo de divisão Euclidiana, cálculo de equação diofantina ou cálculo de congruências lineares.

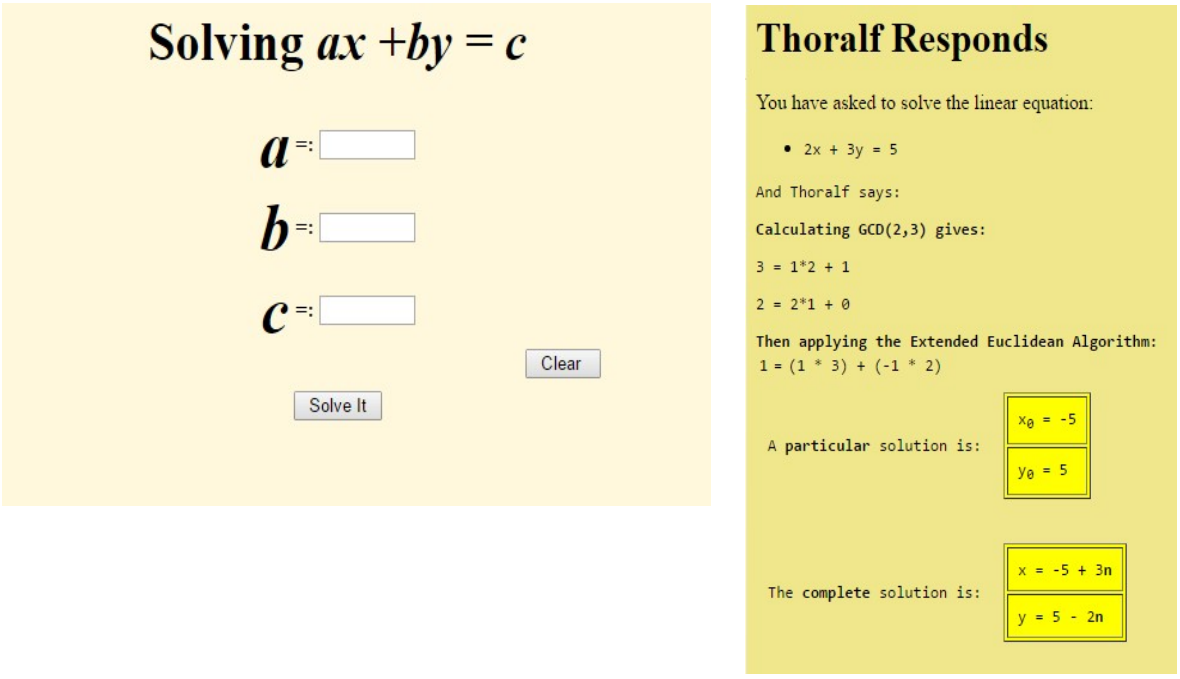
Na seção referente a equações diofantinas, a tela é bem simples, como é visto na Figura 8. Apresenta os campos para entrada dos coeficientes, e um botão *Compute*. Ao serem digitados os coeficientes desejados e pressionar o botão, na mesma tela aparece o resultado geral da equação. Novamente, não são fornecidos muitos detalhes sobre como foi alcançado esse resultado.

Um problema encontrado foi o de digitar equações que não possuem soluções inteiras. O aplicativo para de funcionar e fecha, algo que não pode acontecer com aplicativos desse gênero.

7.4 APLICATIVO LINEAR DIOPHANTINE EQUATIONS BROWSER

Este aplicativo com desenvolvido por Stanley N. Burris. O aplicativo está disponível para qualquer navegador de Internet, e pode ser acessado pelo endereço https://www.math.uwaterloo.ca/~snburris/htdocs/linear.html.

Figura 8 - Telas do aplicativo Linear Diophantine Equations (Internet)



Fonte: autoria própria

Nesse aplicativo, temos novamente três campos para serem digitados os coeficientes da equação diofantina. Tem também dois botões, *Solve it* e *Clear*. Ao preencher os campos com os coeficientes e clicar em *Solve it* , uma tela com o título *Thoralf Responds* é mostrada.

Nessa tela, é mostrada a equação que foi digitada, o cálculo do MDC, a aplicação do Teorema 4.2.2, e as soluções triviais e gerais da equação, como pode ser vista na Figura 9.

8 APLICATIVO DESENVOLVIDO

Nesse capítulo, são apresentadas imagens do aplicativo desenvolvido. O modelo de celular utilizado foi o *Nexus 5*, da LG, e as capturas de tela são referentes a versão 1.0 do aplicativo, disponível em https://play.google.com/store/apps/details?id=com.lucasazevedo.android.calcdiofantina&hl=en.

A tela principal do aplicativo é a apresentada na Figura 10a.

Figura 9 - Telas iniciais

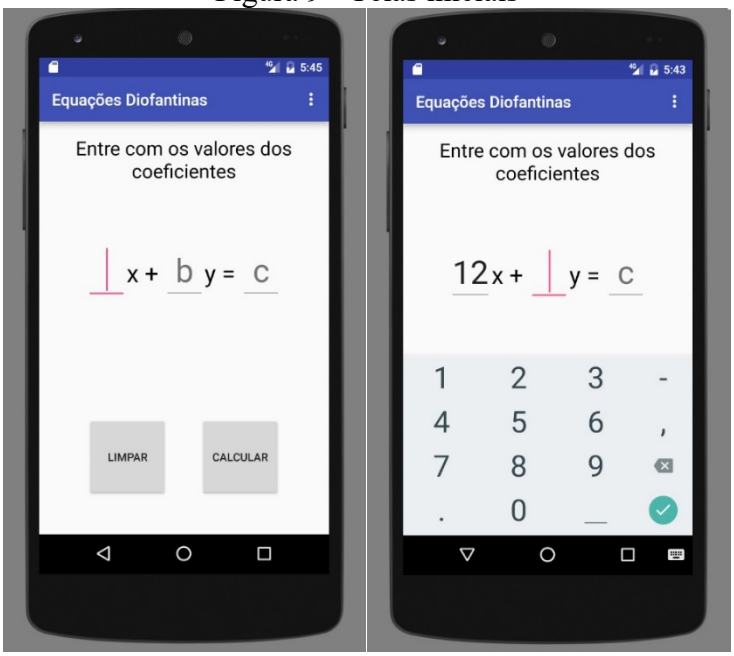


Figura 10a – Tela Inicial Figura 10b – Teclado numérico

Fonte: autoria própria

Existem três campos para digitar texto. Nesses campos, o usuário digita os valores dos coeficientes da equação diofantina desejada. Encontra-se também dois botões na parte inferior da tela. O botão *Limpar* limpa todos os dados escritos pelo usuário. O botão *Calcular* efetua o cálculo da equação digitada, como é visto na Figura 10a. Ao clicar em um dos campos de entrada de texto, um teclado numérico aparece ao usuário, permitindo a digitação, como pode ser visto na Figura 10b.

Caso o usuário pressione o botão calcular sem que tenha preenchido algum dos campos, uma mensagem aparece, alertando-o do equívoco, como pode ser visto na Figura 11.

No caso dessa figura, a mensagem alerta o usuário a preencher o campo com o valor do coeficiente *a*, ou seja, o primeiro campo.

Figura 10 - Mensagem de Alerta

Fonte: autoria própria

Existe também um botão na parte superior direita o qual abre um menu com duas opções. São essas opções: *INFO*, que ao ser clicada, uma tela com informações sobre Diofanto e sobre equações diofantinas é mostrada, como pode ser visto na Figura 12a; e *Créditos*, que mostra informações sobre o desenvolvimento do aplicativo, como pode ser visto na Figura 12b. Essas informações foram retiradas do presente trabalho.

Figura 11 - Telas de Informações

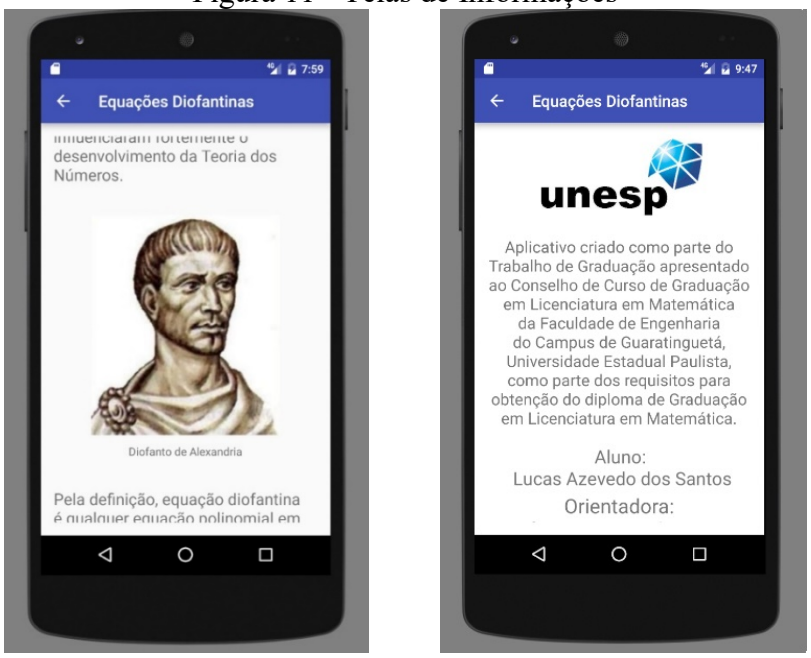


Figura 12a – Informações sobre Diofanto Figura 12b - Créditos

Fonte: autoria própria

Voltando à tela inicial, ao digitar os valores para os parâmetros e pressionar o botão *Calcular*, o aplicativo irá conferir se é possível ou não encontrar soluções inteiras. Caso não seja possível, uma nova tela mostrará a equação digitada, o MDC dos parâmetros a e b digitados, e uma mensagem que não existem soluções inteiras, como pode ser visto na Figura 13a.

No caso de existirem soluções inteiras para a equação digitada, uma nova tela é mostrada. Na Figura 13b mostra-se a tela quando existem soluções inteiras. No caso apresentado, a equação que permite resolução nos inteiros é $12x + 15y = 6$. Da mesma forma da anterior, será mostrada a equação digitada e o *MDC* dos parâmetros a e b, porém agora com a mensagem de que é possível calcular as soluções inteiras para essa equação, como mostra a Figura 13b.

Figura 12 - Telas de Soluções Não Existentes ou Existentes

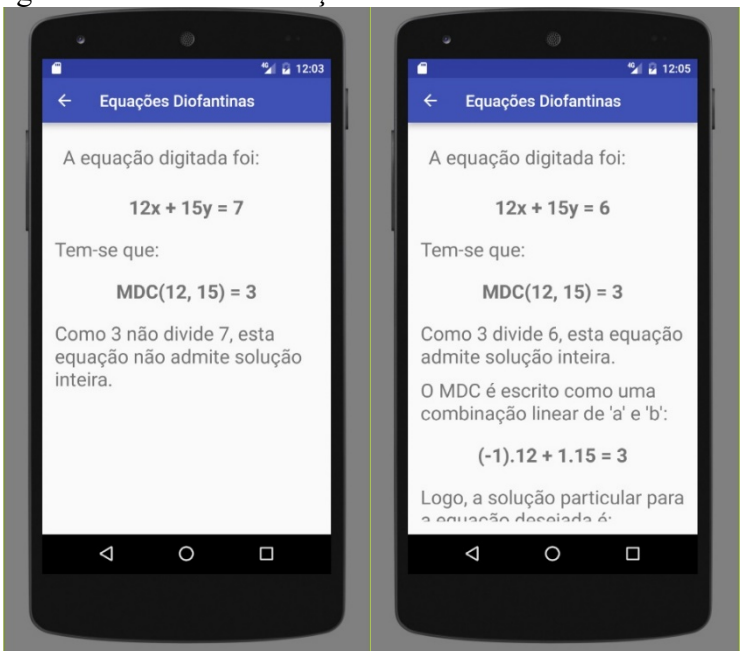


Figura 13a – Soluções não existentes Figura 13b – Soluções existentes

Fonte: autoria própria

A seguir, mostra-se como o MDC encontrado pode ser escrito como uma combinação linear dos parâmetros *a* e *b*. Então, encontra-se uma solução particular para a equação digitada, como mostra a Figura 14a. Nesse caso, uma solução para a equação dada será $x_0 = -2,\ y_0 = 2$. E finalmente, o aplicativo mostra a solução geral para a equação dada, que nesse caso $x = -2 + 5t$ e $y = 2 - 4t$.

Também calcula o intervalo de *t* em que *x* e *y* são estritamente positivos. Caso não existam valores para *t* que satisfaçam essa condição, uma mensagem como a que pode ser vista na Figura 14b é apresentada.

Figura 13 - Telas de Soluções Existentes

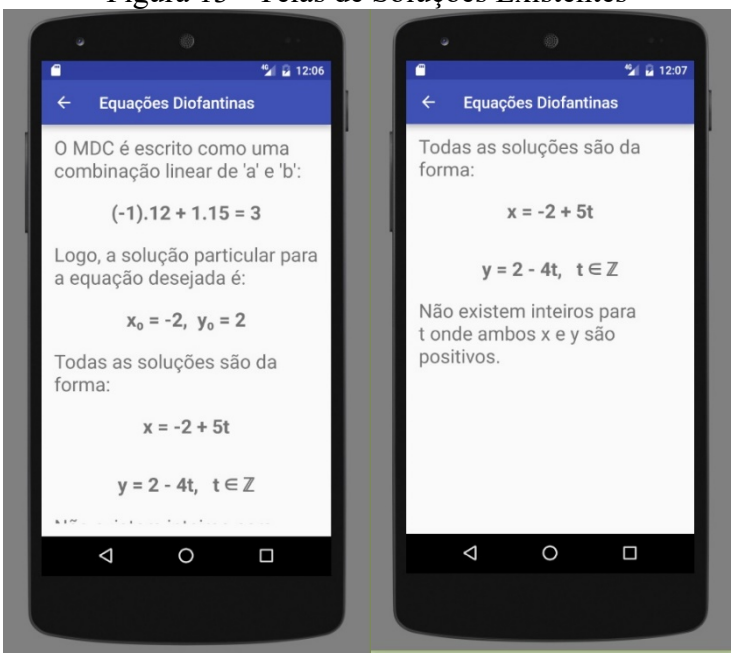
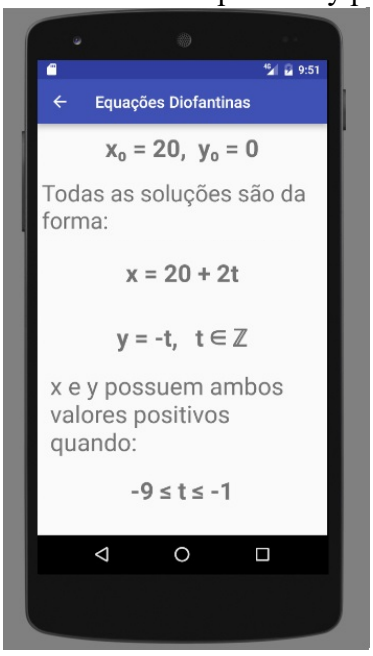


Figura 14a – Combinação Linear e Solução Figura 14b – Soluções Gerais e valores de t

Fonte: autoria própria

No caso da equação apresentar valores estritamente positivos de x e y para algum t, a tela apresentada na Figura 15 será vista. Nesse caso, a equação digitada foi $x + 2y = 20$.

Figura 14 - Valores de t para x e y positivos



Fonte: autoria própria

9 CONCLUSÃO

Nesse trabalho foi apresentado como se dá a resolução de equações diofantinas lineares de duas variáveis e sua implementação em linguagem computacional JAVA. Para essa implementação ocorrer, foi imprescindível uma revisão dos conceitos matemáticos da teoria dos números. Nessa revisão, foram tratados assuntos como divisibilidade dos números inteiros, máximo divisor comum e algoritmo de Euclides. Tais conceitos, muitas vezes vistos como apenas matemática teórica, provam-se, por meio desse trabalho, aplicáveis em situações problemas por meio das equações diofantinas. Alguns exemplos estudados foram aplicações em problemas do cotidiano, balanceamento de equações químicas e computação.

Conclui-se também a importância dos estudos dos matemáticos antigos para a atual teoria dos números. Diofanto, que dá o nome das equações diofantinas, teve papel muito importante como precursor dessa teoria. Seus trabalhos, juntamente com o de Euclides, outro grande matemático da Grécia antiga, serviram de base para que matemáticos modernos, como Fermat, Euler e Gauss aprimorassem os conceitos e iniciassem definitivamente a teoria dos números. A teoria dos números foi por muito tempo vista como a área da matemática com menos aplicações em situações cotidianas, mas com o avanço da tecnologia e o advento da computação, hoje em dia, mais do que nunca, essa área tem um papel muito importante na sociedade. Toda a base da computação na atualidade dá-se a partir da teoria dos números.

Ao se desenvolver o aplicativo de resolução das equações diofantinas, percebe-se a fraca disponibilidade de aplicativos com a mesma função no mercado. Dos aplicativos analisados, a grande maioria possui telas de apresentação sem muitas informações, com propagandas que atrapalham a experiência do usuário ou com erros de formatação. Espera-se que com a criação desse aplicativo, estudantes ou curiosos que procurem aplicativos que resolvam tais equações possam se sentir satisfeitos com o criado por esse trabalho.

Espera-se também que estudantes que desejem saber mais sobre equações diofantinas, sua história, sua base e aplicações possam utilizar do presente trabalho para aprofundarem seus conhecimentos. Em trabalhos futuros, pretende-se aplicar os conceitos vistos no presente trabalho para a implementação de um algoritmo computacional de resolução de equações diofantinas com 3 ou mais variáveis. Pretende-se também, em um futuro estudo, utilizar o aplicativo desenvolvido em salas de aula da educação básica, procurando meios de interligar o ensino de conteúdos matemáticos com tecnologia.

REFERÊNCIAS BIBLIOGRÁFICAS

BISPO, D., S**. Equações diofantinas lineares e suas aplicações**. 2013. 76 f. Trabalho de Graduação (Graduação em Matemática) – Universidade Estadual do Sudoeste da Bahia – Campous de Vitória da Consquita, Vitória da Conquista, 2013.

BOYER, C. B. **História da matemática**. São Paulo: Edgard Blucher, 1996.

BURRIS, S. **Solver linear diphantine equations**. Disponível em <https://www.math.uwaterloo.ca/~snburris/htdocs/linear.html>. Acessado em 30 de agosto de 2016.

CAMPOS, G. D. M. **Equações diofantinas lineares**. 2013. 71 f. Dissertação (Mestrado Profissional em Matemática) – Instituto de Ciências Exatas e da Terra, Universidade Federal do Mato Grosso, Cuiabá, 2013.

DOMINGUES, H. H. **Fundamentos de aritmética**. Florianópolis: Editora da UFSC. 2009.

DOMINGUES, H. H. Iezzi, G. **Álgebra moderna**. 4ª ed. reform. São Paulo: Editora Atual. 2003.

EVES, H. **Introdução à história da matemática**. Campinas: Editora da Unicamp, 2004.

FERREIRA, H. B. O. DOMINGOS, J. S. Equações diofantinas lineares: Fundamentação Matemática e um Algoritmo de Resolução. ForScience: **Revista Científica Do Ifmg**, Formiga, v. 1, n. 1, p. 22-32, jul./dez. 2013.

FREITAS, C. W. A. **Equações diofantinas**. 2015. 201 f. Dissertação (Mestrado em Matemática) – Departamento de Matemática, Universidade Federal do Ceará, Fortaleza, 2015.

HANTA, V. **Solution of Simple Diophantine Equations by Means of Matlab**.

LECHETA, R. R., **Google Android:** Aprenda a criar aplicações para dispositivos móveis com o Android SDK. Santa Catarina: Novatec, 4ª ed. 2015.

MADEIRA, D. **Problema de lógica**: Epitáfio de Diofanto. Sorocaba, 2011. Disponível em < http://dan-scientia.blogspot.com.br/2011/07/problema-de-logica-epitafio-de-diofanto.html>. Acesso em: 15 ago. 2016.

MILIES, C. P.; COELHO, S. P. **Números:** uma introdução à matemática. 3ª Ed. 1 reimpr. São Paulo: Editora da Universidade de São Paulo, 2003.

MOL, R. S. **Introdução à história da matemática**. Belo Horizonte: CAED-UFMG, 2013.

POMMER, W. M. **Equações diofantinas lineares**: Um Desafio Motivador para alunos do ensino médio. 2008. 155f. Dissertação de Mestrado Acadêmico em Educação

Matemática, PUC/SP.

POMMER, W. M. POMMER, C. P. C. R. **Equações diofantinas lineares**: um viés históricoepistemológico como recurso para introduzir diferentes estratégias de resolução de problemas. REnCiMa, v. 3, n. 1, p. 28-43, jan/jul 2012.

SAVÓIS, J. N. FREITAS, D. Método para resolver equações diofantinas com coeficientes no conjunto dos números racionais. **Revista do centro de ciências naturais e exatas –** UFSM. Santa Maria, v. 37 Ed. Especial PROFMAT, p. 47 – 57. 2015.

SILVA, A. S. MORAIS, C. R. B. SILVA, A. R da, BARROS, W. B. Aplicando equações diofantinas lineares num contexto interdisciplinar: um diálogo entre a matemática e a química. In: CONGRESSO NACIONAL DE PESQUISA E ENSINO EM CIÊNCIAS, 1., 2016, Campina Grande. **Anais...** Campina Grande.

STEWART, I. **Em busca do infinito:** uma história da matemática dos primeiros números à teoria do caos. Rio de Janeiro: Zahar, 2014.

VIDIGAL, A.; AVRITZER, D; SOARES, E.F; BUENO, H.P; FERREIRA, M. C.C; FARIA, M. C. **Fundamentos de álgebra**. Editora UFMG. 1ª edição atualizada. 2009.

YESILYURT, D. **Solving linear diophantine equations and linear congruential equations**. 2012. 37 f. Trabalho de Graduação (Graduação em Matemática) Linnaeus University, Kalmar, 2012.

BIBLIOGRAFIA CONSULTADA

DUTENHEFNER, F., CADAR, L. **Encontros de Aritmética**. Rio de Janeiro: IMPA/OBMEP. 2015.

FIORENTINI, D. MIGUEL, A. MIORIM, M. A. **Contribuição para um repensar:** a Educação Algébrica elementar. Campinas: PRO-POSIÇÕES, v. 4, n.1 (10), 1993.

HEFEZ, A. **Iniciação a aritmética**. Rio de Janeiro: IMPA/OBMEP, 2005.

HELLENISTIC **Mathematics Diophantus**. 2010. Disponível em http://www.storyofmathematics.com/hellenistic_diophantus.html. Acesso em: 03 ago. 2016.

LASATER, J. **Diophantus, Father of Algebra**. Disponível em http://www.math.wichita.edu/history/men/diophantus.html. Acesso em: 08 ago. 2016.

TORRES, R. **A Escola de Alexandria**. 2010. Disponível em <http://reflexoesentremundos.blogspot.com.br/2010/05/escola-de-alexandria.html>. Acesso em: 15 ago. 2016.