Universidade Federal de Goiás
Instituto de Matemática e Estatística
Programa de Mestrado Profissional em
Matemática em Rede Nacional

Aplicações de Equações Diofantinas e um Passeio pelo Último Teorema de Fermat

Lucinda Freese Alves

Jataí
2017

sistema de bibliotecas ufg

PRPG
PRÓ-REITORIA DE PÓS-GRADUAÇÃO

UFG

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO PARA DISPONIBILIZAR VERSÕES ELETRÔNICAS DE TESES E DISSERTAÇÕES NA BIBLIOTECA DIGITAL DA UFG

Na qualidade de titular dos direitos de autor, autorizo a Universidade Federal de Goiás (UFG) a disponibilizar, gratuitamente, por meio da Biblioteca Digital de Teses e Dissertações (BDTD/UFG), regulamentada pela Resolução CEPEC nº 832/2007, sem ressarcimento dos direitos autorais, de acordo com a Lei nº 9610/98, o documento conforme permissões assinaladas abaixo, para fins de leitura, impressão e/ou *download*, a título de divulgação da produção científica brasileira, a partir desta data.

1. Identificação do material bibliográfico: **[x] Dissertação** **[ ] Tese**

2. Identificação da Tese ou Dissertação:

Nome completo do autor: Lucinda Freese Alves

Título do trabalho: Aplicações de Equações Diofantinas e um Passeio pelo Último Teorema de Fermat

3. Informações de acesso ao documento:

Concorda com a liberação total do documento [x] SIM [ ] NÃO[1]

Havendo concordância com a disponibilização eletrônica, torna-se imprescindível o envio do(s) arquivo(s) em formato digital PDF da tese ou dissertação.

Assinatura do(a) autor(a)[2]

Ciente e de acordo:

Assinatura do(a) orientador(a)[2]

Data: 20 / 12 / 2017

[1] Neste caso o documento será embargado por até um ano a partir da data de defesa. A extensão deste prazo suscita justificativa junto à coordenação do curso. Os dados do documento não serão disponibilizados durante o período de embargo.
Casos de embargo:
- Solicitação de registro de patente;
- Submissão de artigo em revista científica;
- Publicação como capítulo de livro;
- Publicação da dissertação/tese em livro.

[2] A assinatura deve ser escaneada.

Lucinda Freese Alves

Aplicações de Equações Diofantinas e um Passeio pelo Último Teorema de Fermat

Trabalho de Conclusão de Curso apresentado ao Instituto de Matemática e Estatística da Universidade Federal de Goiás, como parte dos requisitos para obtenção do grau de Mestre em Matemática.

Área de Concentração: Matemática do Ensino Básico

Orientador: Prof. Dr. Wender José de Souza

Jataí

2017

Ficha de identificação da obra elaborada pelo autor, através do
Programa de Geração Automática do Sistema de Bibliotecas da UFG.

Alves, Lucinda Freese
Aplicações de Equações Diofantinas e um Passeio pelo Último Teorema de Fermat [manuscrito] / Lucinda Freese Alves. - 2017.
LXIV, 64 f.: il.

Orientador: Prof. Dr. Wender José de Souza.
Dissertação (Mestrado) - Universidade Federal de Goiás, Unidade Acadêmica Especial de Ciências Exatas e Tecnológicas, Jataí, PROFMAT- Programa de Pós-graduação em Matemática em Rede Nacional - Sociedade Brasileira de Matemática (RJ), Jataí, 2017.
Bibliografia. Apêndice.
Inclui tabelas, lista de figuras, lista de tabelas.

1. Equações Diofantinas. 2. Teorema de Pitágoras. 3. Equações Fermatianas. I. de Souza, Wender José, orient. II. Título.

CDU 511

Universidade Federal de Goiás-UFG REGIONAL JATAÍ
Mestrado profissional em Matemática em Rede Nacional - PROFMAT/UFG
Regional Jataí – Caixa Postal 03 – CEP: 75,804-020 – Jataí-GO.
Fones: (64) 3606-8213 **www.jatai.ufg.br/matematica**

Ata da reunião da Banca Examinadora da Defesa de Trabalho de Conclusão de Curso da aluna Lucinda Freese Alves – Aos vinte dias do mês de dezembro do ano de dois mil e dezessete (20/12/2017), às 14:00 horas, reuniram-se os componentes da Banca Examinadora, Prof. Dr. Wender José de Souza - Orientador, Prof. Gecirlei Francisco da Silva e Profa. Dra. Kamila da Silva Andrade, sob a presidência do primeiro, e em sessão pública realizada na Sala 08 da Pós Graduação da Universidade Federal de Goiás - Regional Jataí, procederem a avaliação da defesa intitulada: **"Aplicações de Equações Diofantinas e um passeio pelo Último Teorema de Fermat",** em nível de Mestrado, área de concentração Matemática do Ensino Básico, do Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT da Universidade Federal de Goiás, polo Jataí. A sessão foi aberta pelo Presidente da Banca, Prof. Dr. Wender José de Souza , que fez a apresentação formal dos membros da banca. A seguir, a palavra foi concedida ao autor da Dissertação que, em 40 minutos, procedeu a apresentação de seu trabalho. Terminada a apresentação, cada membro da banca arguiu o examinando, tendo-se adotado o sistema de diálogo sequencial. Terminada a fase de arguição, procedeu-se a avaliação da defesa. Tendo em vista o que consta na Resolução nº. 1403/2016 do Conselho de Ensino, Pesquisa, Extensão e Cultura (CEPEC), que regulamenta os Programas de Pós-Graduação da UFG e procedidas as correções recomendadas, o trabalho de conclusão foi **APROVADA** por unanimidade, considerando-se integralmente cumprido este requisito para fins de obtenção do título de **MESTRE EM MATEMÁTICA**, na área de concentração Matemática do Ensino Básico pela Universidade Federal de Goiás. A conclusão do curso dar-se-á quando da entrega na Secretaria da Coordenação de Matemática da Regional Jataí da versão definitiva do trabalho, com as devidas correções supervisionadas e aprovadas pelo orientador. Cumpridas as formalidades de pauta, às 15:30 horas a presidência da mesa encerrou a sessão e para constar, eu, José Alfredo Cespi de Oliveira, Secretário da Coordenação Geral de Pós-Graduação da Regional Jataí - UFG, lavrei a presente ata que, depois de lida e aprovada, é assinada pelos membros da Banca Examinadora em quatro vias de igual teor.

Wender José de Souza

Prof. Dr. Wender José de Souza
Departamento de Matemática-UFG/Reg. Jataí
Presidente da Banca

Profa. Dra. Kamila da Silva Andrade
UFG- Goiânia
Membro externo

Gecirlei Francisco da Silva

Prof. Dr. Gecirlei Franscisco da Silva
Profmat (Pólo Jataí)-UFG
Membro interno

Lucinda Freese Alves graduou-se em Licenciatura em Matemática pela Universidade Estadual de Goiás - Câmpus Jataí em 2005, atualmente é professora efetiva de matemática no Colégio Estadual José Dutra de Oliveira - Perolândia Goiás.

Dedico este trabalho à minha família pelo apoio, amor e compreensão, durante o período de realização deste projeto.

Agradecimentos

Agradeço à Deus pelo dom da vida. Aos meus familiares pelo apoio incondicional durante a realização deste trabalho. Ao meu orientador Prof. Dr. Wender José de Souza pelas orientações ministradas. A todos os professores envolvidos no mestrado PROFMAT. A todos os amigos do mestrado, pelo apoio e incentivo oferecido.

Resumo

O presente trabalho tem como objetivo auxiliar estudantes, professores e apaixonados pela matemática, a melhor compreender, interpretar e resolver problemas que possam ser solucionados através das Equações Diofantinas. Desta forma, apresentamos alguns conceitos básicos sobre Equações Diofantinas bem como algumas aplicações práticas. Discutimos ainda, o Último Teorema de Fermat para os casos de n=2, n=3 e n=4, visando despertar o interesse no aluno pela teoria dos números.

Palavras-chave Equações Diofantinas, Teorema de Pitágoras, Equações Fermatianas.

Abstract

The present work aims to help students, teachers and lovers of mathematics, to better understand, interpret and solve problems that can be solved through Diophantine Equations. In this way, we present some basic concepts about Diophantine Equations as well as some practical applications.We also discuss Fermat's Last Theorem for the cases n = 2, n = 3, and n = 4, aiming to arouse interest, on the students, in Number Theory.

Keywords Diophantine Equations, Pythagorean Theorem, Fermatian Equations.

Lista de ilustrações

Lista de tabelas

Sumário

Introdução

Este trabalho propõe auxiliar estudantes, professores e apaixonados na matemática, a melhor compreender, interpretar e resolver problemas que possam ser solucionados através das Equações Diofantinas. Apresentamos ainda, alguns conceitos básicos sobre Equações Diofantinas, lineares e não lineares, bem como algumas aplicações práticas. Passamos ainda para as Equações Diofantinas quadráticas, como o Teorema de Pitágoras e as Equações Fermatianas, com $n = 3$ e biquadráticas.

De acordo com os Parâmetros Curriculares Nacionais (PCN's), a resolução de problemas é o ponto de partida da atividade matemática, que deixa de ser uma simples reprodução de procedimentos e acúmulo de informações e ganha significado. Por isso, é conveniente a relação da aplicação das Equações Diofantinas como método para a resolução de problemas.

Por fim, apresentamos um dos problemas mais intrigantes na matemática de Pierre de Fermat $(1601 - 1665)$, às margens do livro de Aritmética de Diofante, como segue abaixo suas palavras, segundo Simon SINGH [5]:

"É impossível resolver um cubo em (soma de) dois cubos, uma potência quarta em duas de potências de quatro, ou em geral, qualquer potência de maior que segunda em duas potências do mesmo tipo. Encontrei uma prova notável deste fato, mas a margem é muito pequena para contê-la".

Em síntese, Fermat afirmou:

Não existe qualquer solução de três números inteiros x, y, z satisfazendo a Equação Diofantina $x^n + y^n = z^n$, para $n > 2$.

Foram 350 anos de um mistério que desafiou as mentes mais brilhantes e determinadas da matemática para se chegar a uma prova definitiva, conhecida como o "Monte Everest"da Teoria dos Números e demonstrado por Andrew Wiles em 1995.

Importante ressaltar que a introdução à resolução de problemas dessa natureza são abordados no Ensino Fundamental e Médio, mas serão melhor trabalhadas no Ensino Superior.

Objetivos do Trabalho

Objetivos Gerais

- Compreender o uso das Equações Diofantinas na resolução de problemas do dia a dia;
- Despertar o interesse pelas Equações Diofantinas e Fermáticas.

Objetivos Específicos

- Mostrar um pouco da história das Equações Diofantinas e do Último Teorema de Fermat;
- Ampliar os conhecimentos na resolução de problemas com o uso da álgebra, ou seja, Equações Diofantinas;
- Resolver situações do dia a dia, tendo como alternativa o uso das Equações Diofantinas.

Organização e Estrutura do Trabalho

Diofanto de Alexandria, em seu livro Arithmética, introduziu o uso de símbolos na resolução de equações. A mais famosa é a equação $x^n + y^n = z^n$ e que desafiou por mais de trezentos e cinquenta anos, matemáticos renomados, depois que Fermat afirmou que as equações desse tipo, não possuem soluções com valores inteiros e positivos de x, y e z, quando $n \geq 2$. Nesse sentido, o presente trabalho está delineado como segue:

No Capítulo 1, apresentamos o enunciado e a demonstração de divisão nos inteiros, máximo divisor comum, números primos e algoritmo de Euclides, que serviram para compreensão das demonstrações na resolução das Equações Diofantinas.

No Capípulo 2, discorremos sobre aplicações das Equações Diofantinas. São situações do dia a dia que podem ser resolvidas através da análise Diofantina, mas também com estratégias de resolução como tentativa e erro, método pictórico e conceitos da Teoria dos Números.

No Capítulo 3, discorremos sobre as aplicações práticas das Equações Diofantinas que possuem solução no conjunto dos números inteiros e no Capítulo 4, abordamos sobre o Teorema de Pitágoras e apresentando duas de algumas de suas provas. É aqui que discutimos os casos em que $n = 3$ e $n = 4$, que são chamadas de equações Fermatianas.

Por fim, nossas considerações finais a respeito desta dissertação.

1 Tópicos da Teoria dos Números

Para o estudo das Equações Diofantinas, necessário se faz a utilização de alguns tópicos da Teoria dos Números e é neste capítulo que discorremos o conteúdo, tendo como fonte de pesquisa, os livros: Fundamentos da Aritmética, de Higino H. Domingues [2] e Aritmética de Abramo Hefez [4]. A fundamentação teórica nos permite compreender os métodos algébricos que nos fornecem todas as soluções inteiras para as Equações Diofantinas.

Trataremos aqui dos tópicos de divisibilidade, máximo divisor comum, números primos e algoritmo de Euclides, pois é neles que todo esse trabalho relaciona-se.

1.1 Divisão nos Inteiros

O conjunto dos números inteiros é representado pela letra $\mathbb{Z}$ e dado por:

$$\mathbb{Z} = \{..., -2, -1, 0, 1, 2, 3, ...\}.$$

e por se tratar de um conjunto que possui muitas propriedades, iremos aqui apenas referenciar às que serão úteis ao desenvolvimento deste trabalho.

Definição 1. *Dados a e b, inteiros, diremos que a divide b e denotaremos por, $a|b$, quando existir um $k \in \mathbb{Z}$ tal que $b = ka$. A negação dessa sentença é denotada por $a \nmid b$.*

Podemos concluir da definição que a é um divisor de b, consequentemente, b é divisível por a, ou ainda, que b é múltiplo de a. Será a um divisor positivo de b, se $a|b$ e $a > 0$.

Exemplo 1. $4|20$, pois existe um inteiro $k = 5$, tal que $20 = 4.5$.

Exemplo 2. $5 \nmid 16$, pois não existe um inteiro k que satisfaça $16 = 5.k$.

Proposição 1. *Dados a, b e c inteiros, tais que $a|b$ e $b|c$, então $a|c$.*

Demonstração. Sejam a, b e c inteiros tais que $a|b$ e $b|c$, logo existem k_1 e k_2 tal que $b = ak_1$ e $c = bk_2$. Logo, $c = (ak_1)k_2 = a(k_1k_2)$ e, portanto, $a|c$. □

Exemplo 3. Como $2|4$ e $4|12$, então $2|12$. De fato, $4 = 2.2$ e $4.3 = 12 \Longrightarrow 2.2.3 = 12$, logo $2|12$.

Proposição 2. *Dados a, b e c inteiros, tais que $a|b$ e $a|c$, então $a|(mb+nc)$, para quaisquer $m, n \in \mathbb{Z}$.*

Demonstração. Sejam a, b e c inteiros tais que $a|b$ e $a|c$, então existem inteiros k_1 e k_2 tais que $b = ak_1$ e $c = ak_2$. Multiplicando ambas as equações respectivamente por m e n obtemos

$$mb = mak_1 \tag{1.1}$$

e

$$nc = nak_2. \tag{1.2}$$

Somando as equações (1.1) e (1.2) lado a lado, temos que: $mb + nc = mak_1 + nak_2 = a(mk_1 + nk_2)$. Portanto, $a|(mb + nc)$. □

Exemplo 4. Como $5|20$ e $5|15$, então $5|(5.20 + (-6).15) = 10$.

Teorema 1. (Algoritmo da Divisão em $\mathbb{Z}$) Dados a e b números inteiros sendo um b inteiro positivo, existe um único par de inteiros q e r que satisfazem $a = q.b + r$, com $0 \leq r < b$.

Demonstração. Dado b, um número inteiro positivo e não nulo. Se $a \in \mathbb{Z}$, então ou a é múltiplo de b ou a está situado entre dois múltiplos consecutivos de b, isto é, $qb \leq a < (q + 1)b$.

Vamos adicionar $-qb$ em todos os termos da desigualdade obtemos:

$$qb - qb \leq a - qb < qb + b - qb, 0 \leq a - qb < b \tag{1.3}$$

Assim, fazendo $r = a - qb$, podemos escrever também $a = qb + r$, em que $0 \leq r < b$.

Vamos supor que existam inteiros q_1, q_2, r_1, r_2 , onde $q_1 \neq q_2$ e $r_1 \neq r_2$ e que satisfaçam às igualdades:

$$a = q_1 b + r_1, \quad \text{com} \quad 0 \leq r_1 < b \tag{1.4}$$

e

$$a = q_2 b + r_2, \quad \text{com} \quad 0 \leq r_2 < b. \tag{1.5}$$

Suponha, sem perda de generalidade que $r_2 > r_1$ se $b > r_1$ e $b > r_2$, fazendo $b > r_2 - r_1$ e comparando (1.4) e (1.5) temos que: $a = bq_1 + r_1 = bq_2 + r_2$. Isolando, $r_2 - r_1$, obtemos: $b(q_2 - q_1) = r_2 - r_1$. Chamando de $t = (q_2 - q_1)$, segue que $r_2 - r_1 = tb$, com $t \in \mathbb{Z}$ e daí $b|(r_2 - r_1)$.

Portanto, $b \leq (r_2 - r_1)$,só se $r_2 > r_1$ o que é um absurdo, pois contradiz o fato de $b > r_2 - r_1$. Logo, $r_2 = r_1$.

Concluímos que $(q_2 - q_1)\, b = 0$. Sendo $b \neq 0$, temos que $(q_2 - q_1) = 0 \Longrightarrow q_2 = q_1$.

Na equação $a = q.b + r$, com $0 \leq r < b$, os inteiros, q e r são chamados, respectivamente, de quociente e resto da divisão de a por b. Vale lembrar que b somente é divisor de a se $r = 0$. Neste caso, temos que $a = bq$ e o quociente q na divisão exata de a por b pode ser indicado também por $\frac{a}{b}$ ou a/b. □

Exemplo 5. Numa divisão de 396 por $b > 0$, o quociente é 13 e o resto é r. Determine os possíveis valores para b e r.

Resolução: Sabemos que na divisão de a por b tem que $a = q.b + r$, $0 \leq r < b$. Então, podemos escrever:

$$396 = 13b + r, \quad \text{com} \quad 0 \leq r < b. \tag{1.6}$$

Ou seja,

$$r = 396 - 13b, \quad \text{com} \quad 0 \leq r < b. \tag{1.7}$$

Da inequação (1.7) obtemos:

$$0 \leq 396 - 13b < b. \tag{1.8}$$

Desmembrando a inequação (1.8) temos:

$$0 \leq 396 - 13b \quad \text{e} \quad 396 - 13b < b, \tag{1.9}$$

De (1.9) temos:

$$13b \leq 396 \quad \text{e} \quad 14b > 396.$$

Logo, isolando b concluímos que: $28,29 < b \leq 30,46$.

Portanto, como estamos procurando apenas valores inteiros para b e r, os possíveis valores são:

$$b = 29 \text{ e } r = 19 \text{ ou } b = 30 \text{ e } r = 6.$$

Exemplo 6. Dados $a = 53$ e $b = 7$. Verifique se a é múltiplo de b ou, caso não seja, determine os múltiplos consecutivos em que a se situa entre eles.

Resolução: Sabemos que na divisão de a por b, temos que $a = qb + r$, então podemos escrever:

$$53 = 7q + r, \quad \text{com} \quad q \in \mathbb{Z}. \tag{1.10}$$

Para que a seja múltiplo de b, é necessário ter resto zero. Assim, vamos encontrar o valor de q em (1.10):

$$7q = 53 \tag{1.11}$$

$$q = 7,57. \tag{1.12}$$

Como não existe $q \in \mathbb{Z}$ que satisfaça (1.11), concluímos que 53 não é múltiplo de 7.

No entanto, podemos perceber que q se situa entre 7 e 8, desta forma, temos que $49 = 7.7 < q < 7.8 = 56$. Portanto, os múltiplos consecutivos de $b = 7$ procurados são 49 e 56.

Proposição 3. *Dado $a \in \mathbb{Z}$ temos que:*
1)$1|a, a|a$ *e* $a|0$
2)$0|a \iff a = 0$.

Demonstração. 1)$1|a$ pois $a.1 = a$; $a|a$ pois $1.a = a$ e $a|0$ pois $0 = 0.a$

2)Vamos supor que $0|a$; logo existe $k \in \mathbb{Z}$ tal que pela propriedade distributiva da multiplicação, $a = k.0$ ou seja, $a.0 = a(0 + 0) = a.0 = a.0$. Somando $-(a.0)$ a ambos membros da igualdade, temos que:

$$0 = -(a.0) + a.0 = -(a.0) + (a.0 + a.0)$$
$$0 = (-(a.0) + a.0) + a.0 = 0 + a.0$$
$$0 = a.0$$

que restou provada a propriedade. □

1.2 Máximo Divisor Comum

O máximo divisor comum de dois números inteiros, é o maior número inteiro que divide esses dois números. Exemplo disso, é o número inteiro 4 que divide o número 16 e também divide 20, que é o maior inteiro positivo com essa propriedade. Logo, 4 é o máximo divisor comum de 16 e de 20, podendo ser representado assim: $mdc(16, 20) = 4$ ou $(16, 20) = 4$, o que nos leva a seguinte definição.

Definição 2. *O máximo divisor comum de dois inteiros a e b, com a e b diferentes de zero, é o maior inteiro que divide a e b. Assim, temos que, o $mdc(a, b)$ é o inteiro positivo d que satisfaz às seguintes propriedades:*

1)d é um divisor comum de a e b e,

2)d é divisível por todo divisor comum de a e b, que é o mesmo que dizer: se c é um divisor comum de a e b, então $c|d$.

Exemplo 7. Dados $a = 18$ e $b = 56$. Determine o $mdc(18; 56)$.

Denotamos o conjunto dos divisores de $a = 18$ por $D_{(18)}$ e o conjunto dos divisores de $b = 56$ por $D_{(56)}$, sendo:

$$D_{(18)} = \{\pm1; \pm2; \pm3; \pm6; \pm9; \pm18\} \text{ e } D_{(56)} = \{\pm1; \pm2; \pm4; \pm7; \pm8; \pm14; \pm28; \pm56\}.$$

Já vimos que o mdc é o maior inteiro que divide 18 e 56, para encontrar o máximo divisor comum entre estes números, basta determinar $D_{(18)} \cap D_{(56)}$ e tomar o maior número em módulo desse conjunto. Logo, $D_{(18;54)} = D_{(18)} \cap D_{(56)} = \{\pm1; \pm2\}$, que tem máximo igual a 2, que é o $mdc(18; 56)$.

Definição 3. *Dados a e b dois inteiros não nulos. Dizemos que a e b são primos entre si se, e somente se, $mdc(a; b) = 1$.*

Exemplo 8. Os inteiros $3, 7, 9$ e 11 são primos entre si. Temos que: $mdc(3; 7) = 1$ e $mdc(9; 11) = 1$. Logo, 3 e 7, 9 e 11 são primos entre si.

Teorema 2. Dados $a, b \in \mathbb{Z}$, ambos não nulos, e seja $t = mdc(a, b)$. Então, existem $x_1, y_1 \in \mathbb{Z}$ tais que: $ax_1 + by_1 = t$, ou seja, t é uma combinação linear de a e b.

Demonstração. Seja o conjunto:

$$S = \{ax + by, \quad / \quad x, y \in \mathbb{Z}, ax + by > 0\}.$$

Consideremos primeiro a não nulo. Fazendo-se $y = 0$ e $x = 1$, se $a > 0, x = -1$, se $a < 0$, temos que $ax + by = a(\pm 1) + b.0 = |a| > 0$ o que nos mostra que S não é vazio. Agora se $a = 0$, então $ax + by = 0.x + b(\pm 1) = |b|$. 0 que mostra que S é também não vazio.

Usando o princípio da indução, existe um $t \in S$ minimal. Se $t \in S$ temos $t > 0$ e existem $x_1, y_1 \in \mathbb{Z}$ tais que;

$$t = ax_1 + by_1. \tag{1.13}$$

Assim podemos afirmar que t é o $mdc(a, b)$. Vamos escrever a divisão de a por t com resto: $\exists\ q, r \in \mathbb{Z}$ tais que:

$$a = qt + r \text{ e } 0 \leq r \leq t - 1.$$

Logo, $r = a - q.t$, substituindo (1.13), temos $r = a - q(ax_1 + by_1) = a(1 - qx_1) + b(-qy_1)$. Se fosse $r > 0$ poderíamos concluir que $r \in S$, o que é um absurdo pois $r < t$ e t é o elemento minimal de S. Logo $r = 0$ e $a = qt$ o que significa que t divide a. Analogamente, podemos mostrar que $t|b$. Portanto t é o divisor comum de a e b. Concluímos então que $t = mdc(a, b)$. □

Portanto, as combinações lineares de a e b, são exatamente os múltiplos do $mdc(a, b)$. Chamemos $L = \{ax + by/x, y \in \mathbb{Z}\}$ e $S = \{tz/z \in \mathbb{Z}\}$. Pelo teorema acima, sabemos que existem $x_1, y_1 \in \mathbb{Z}$ tais que $t = ax_1 + by_1$. Para todo $z \in \mathbb{Z}$, segue $tz = (ax_1z) + (by_1z) \in L$ Logo, $S \subseteq L$. Como $t|(ax + by)$ para qualquer $ax + by \in L$, temos que $L \subseteq S$. Então $L = S$, ou seja:

$$\{ax + by/x, y \in \mathbb{Z}\} = \{tz/z \in \mathbb{Z}\}.$$

1.3 Números Primos

Nesta seção, apresentar uma definição de que, quando encontrarmos o $mdc(a, b) = 1$ esses dois números $a, b \in \mathbb{Z}$ são chamados de números relativamente primos, ou primos entre si.

Proposição 4. *Dados $a, b \in \mathbb{Z}$, não nulos, são relativamente primos entre si, se e somente se existirem $x_1, y_1 \in \mathbb{Z}$ tais que: $ax_1 + by_1 = 1$.*

Demonstração. Se $mdc(a,b) = t$ e se $t = 1$, então existem $x_1, y_1 \in \mathbb{Z}$ com $ax_1 + by_1 = 1$ pelo teorema 2. Seja $ax + by = 1$ com $x, y \in \mathbb{Z}$. Se $t|a$ e $t|b$, podemos concluir que $t|1$. Portanto, $t = 1$, ou seja, $mdc(a,b) = 1$. □

Desta caracterização dos números primos entre si, surgem algumas consequências:

Proposição 5. *Dados $a, b \in \mathbb{Z}$, não nulos, e $t = mdc(a,b)$. Então,*

$$mdc\left(\frac{a}{t}, \frac{b}{t}\right) = 1, \text{ sendo } \frac{a}{t}, \frac{b}{t} \in \mathbb{Z}.$$

Demonstração. Se $ax + by = t$ para certos $x, y \in \mathbb{Z}$, dividindo-se todos os membros da equação por t, obtemos:

$$\frac{ax}{t} + \frac{by}{t} = \frac{t}{t} \Longrightarrow \frac{a}{t}x + \frac{b}{t}y = 1.$$

Pela proposição 4, concluímos a afirmação. □

Proposição 6. *Dados $a, b, c \in \mathbb{Z}$, tais que $a|c$ e $b|c$. Se $mdc(a,b) = 1$ então $ab|c$.*

Demonstração. Suponhamos que $a|b$ e $b|c$, então existem r e s inteiros, tais que

$$ar = c = bs. \tag{1.14}$$

Além disso, como $mdc(a,b) = 1$ existem x e y tais que:

$$ax + by = 1. \tag{1.15}$$

Multiplicando a equação (1.15) por c obtemos:

$$c = c.(ax + by)$$

$$c = cax + cby. \tag{1.16}$$

Substituindo os valores da equação (1.14) no lado direito da equação (1.16), temos que:

$$c = (bs)ax + (ar)by \text{ ou seja,}$$
$$c = ab(sx + ry), \text{ com } sx + ry \in \mathbb{Z}. \text{ Portanto } ab|c.$$

□

Proposição 7. *(Lema de Euclides) Dados $a, b, c \in \mathbb{Z}$ tais que $mdc(a,b) = 1$ e $a|bc$. Então $a|c$.*

Demonstração. Suponhamos que $a|bc$, então existe $r \in \mathbb{Z}$, tal que:

$$ar = bc. \tag{1.17}$$

Além disso, como $mdc(a,b) = 1$, existem x e y inteiros, tais que:

$$ax + by = 1. \tag{1.18}$$

Multiplicando a equação (1.18) por c, obtemos:

$$c = c(ax + by)$$

$$c = cax + cby. \tag{1.19}$$

Substituindo o valor da equação (1.17) na equação (1.19), temos que:

$$c = cax + ary, \text{ ou seja,}$$
$$c = a(cx + ry) \text{ com } cx + ry \in \mathbb{Z}. \text{ Portanto, } a|c.$$

□

1.4 Algoritmo de Euclides

A seguir, apresentamos um método efetivo para calcular o *mdc*, máximo divisor comum, entre dois números, pois se estes forem muito altos, pode-se tornar muito cansativo e pouco prático o cálculo através dos divisores e a verificação da intersecção desses conjuntos. O método é chamado de Algoritmo de Euclides, que constitui a aplicação de sucessivas divisões. Esse algoritmo é uma importante ferramenta da Teoria dos Números.

Sejam a e b, não nulos, com $a > 0$. Aplicando a divisão Euclidiana de b por a, temos:

$$b = aq_1 + r_1, 0 \leq r_1 < a.$$

Procedendo a divisão euclidiana de a por r_1, temos:

$$a = r_1q_2 + r_2, 0 \leq r_2 < r_1.$$

Em seguida, faz a divisão euclidiana sucessivamente:

$$r_1 = r_2q_3 + r_3, 0 \leq r_3 < r_2$$
$$\vdots$$
$$r_j = r_{(j+1)}q_{(j+2)} + r_{(j+2)}, 0 \leq r_{(j+2)} < r_{(j+1)}.$$

Essa sucessão (r_j) é estritamente decrescente de inteiros positivos ou nulos, após P etapas, $r_P = 0$, tem se:

$$r_{(P-3)} = r_{(P-2)}q_{(P-1)} + r_{(P-1)}, 0 \leq r_{(P-1)} < r_{(P-2)}$$
$$r_{(P-2)} = r_{(P-1)}q_P + 0, 0 \leq r_P < r_{(P-1)}$$
$$r_{(P-1)} = r_P.q_{(P+1)}.$$

Esse é o procedimento de cálculo do *mdc*, chamado de Algoritmo de Euclides: o último resto, não nulo, encontrado no algoritmo de Euclides, é o máximo divisor comum de a e b, pois só podemos efetuar a divisão euclidiana enquanto $r_j \neq 0$ e nesse caso, temos que $r_1 > r_2 > ... > r_j > 0$.

Pelo princípio da Boa Ordenação, é impossível termos uma sequência infinita:

$$r_1 > r_2 > ... > r_j > .... > 0,$$

logo, a um certo ponto teremos $r_j = 0$.

Seja n, o maior índice para o qual $r_n \neq 0$, portanto $r_{(n+1)} = 0$. Vamos provar o seguinte:

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

Então:

$$\begin{gathered} mdc(a,b) = mdc(a, b - aq_1) = mdc(a, r_1) \\ mdc(a, r_1) = mdc(r_1, a - r_1q_2) = mdc(r_1, r_2) \\ mdc(r_1, r_2) = mdc(r_1 - r_2q_3, r_2) = mdc(r_3, r_2) = mdc(r_2, r_3) \\ \vdots \\ mdc(r_{(n-1)}) = mdc(r_{(n-1)} - r_nq_{(n+1)}, r_n) = mdc(r_{(n+1)}, r_n) = mdc(0, r_n) = r_n. \end{gathered}$$

Daí segue o resultado. Na prática, assim sintetizamos:

Vamos efetuar a divisão $b = aq_1 + r_1$ e colocamos os números envolvidos no diagrama abaixo:

	q_1	
b	a	
r_1		

Transportamos o r_1 e continuamos efetuando a divisão: $a = r_1q_2 + r_2$, conforme diagrama abaixo:

	q_1	q_2	
b	a	r_1	
r_1	r_2		

Novamente, transportamos r_2 e prosseguindo, enquanto for possível (até que para algum $n \geq 2, r_n | r_{(n-1)}$, ou seja, $r_{(n+1)} = 0$), teremos:

	q_1	q_2	q_3	...	$q_{(n-1)}$	q_n	$q_{(n+1)}$
b	a	r_1	r_2	...	$r_{(n-2)}$	$r_{(n-1)}$	$r_n = mdc(a, b)$
r_1	r_2	r_3	r_4	...	r_n	0	

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

Segundo exemplo de Abramo Hefez [4], vamos calcular o *mdc* de 372 e 162, utilizando o Algoritmo de Euclides:

	2	3	2	1	2
372	162	48	18	12	6
48	18	12	6		

Observamos que o Algoritmo de Euclides nos fornece a seguinte informação:

$$\begin{aligned} 6 &= 18 - 1.12 \\ 12 &= 48 - 2.18 \\ 18 &= 162 - 3.48 \\ 48 &= 372 - 2.162 \end{aligned}$$

Donde se segue que:

$$\begin{aligned} 6 = 18 - 1.12 = 18 - 1.(48 - 2.18) = 3.18 - 48 = \\ 3.(162 - 3.48) - 48 = 3.162 - 10.48 = \\ 3.162 - 10(372 - 2.162) = 23.162 - 10.372. \end{aligned}$$

Temos, então, que:

$$(372, 162) = 6 = 23.162 + (-10).372.$$

Conseguimos então, através do uso do Algoritmo de Euclides de trás para frente, escrever $6 = (372, 162)$ como múltiplo de 162 mais um múltiplo de 372.

Em geral, seguindo o procedimento detalhado no exemplo acima, vê-se que o Algoritmo de Euclides também fornece um meio de escrever o *mdc* de dois números como soma de múltiplos dos números em questão. E sempre que utilizarmos o Algoritmo de Euclides para expressar (a, b) na forma $ma + nb$, com $m, n \in \mathbb{Z}$, o denominaremos de Algoritmo de Euclides Estendido.

2 Equações Diofantinas Lineares

Neste capítulo definimos e apresentamos as Equações Diofantinas com duas e três incógnitas, verificando sua solubilidade particular e de forma geral. Muitos são os problemas de aritmética, que em suas resoluções em números inteiros, recaem em equação deste tipo, objeto deste trabalho. O presente capítulo fundamenta-se nas obras de Hefez [4], Domingues [2], de Landau [1] e [8].

Em homenagem à Diofanto de Alexandria (aprox. 300 d.C), tais equações são chamadas de Equações Diofantinas Lineares.

Uma relação de n incógnitas $x_1, x_2, x_3, ..., x_n$ da forma:

$$f(x_1, x_2, ..., x_n) = 0,$$

onde f é uma função polinomial com coeficientes inteiros e $x_1, ..., x_n$ assumem valores inteiros é denominada uma Equação Diofantina.

Uma Equação Diofantina é linear se ela tiver a forma :

$$a_1x_1 + a_2x_2 + ... + a_nx_n = c.$$

2.1 Equações Diofantinas com Duas Incógnitas

Iniciamos estudando as Equações Diofantinas lineares, com duas incógnitas, da forma:

$$ax + by = c, \tag{2.1}$$

onde $a, b \in \mathbb{Z}$ e suponhamos a e b não simultaneamente nulos. Uma solução para a equação acima é um par $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ para qual a igualdade :

$$ax_0 + by_0 = c \text{ é verdadeira.}$$

A seguir, mostramos as condições em que (2.1) admite soluções.

Proposição 8. *Uma Equação Diofantina $ax + by = c$, em que $a, b, c \in \mathbb{Z}$, com a e b não-nulos, admite solução se, e somente se, $d|c$, onde $d = mdc(a, b)$.*

Demonstração. Se $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ é solução da equação (2.1), então vale a igualdade

$$ax_0 + by_0 = c.$$

Se $d = mdc(a, b)$ então $d|a$ e $d|b$, logo $d|\,(ax_0 + by_0)$ ou seja, $d|c$. Reciprocamente, se $d|c$ então $c = sd$ para algum $s \in \mathbb{Z}$. Como $d = mdc(a, b)$ então segue do teorema 2 que existem $x_0, y_0 \in \mathbb{Z}$ tais que $d = ax_0 + by_0$. Mas por hipótese, que $d|c$ ou seja, $c = sd$, para

algum $s \in \mathbb{Z}$. Assim, $c = ds = (ax_0 + by_0)s = ax_0s + by_0s$ o que mostra que (x_0s, y_0s) é uma solução da equação dada. □

Se (x_0, y_0) é uma solução particular da equação $ax + by = c$ e (x', y') uma solução qualquer desta equação, então temos que:

$$ax' + by' = c = ax_0 + by_0 \tag{2.2}$$

podemos concluir que,

$$a\,(x' - x_0) = b\,(y' - y_0)\,. \tag{2.3}$$

Suponhamos que $d = mdc(a, b)$, então existem inteiros t e u tais que $a = dt$ e $b = du$, com $mdc(t, u) = 1$, assim substituindo em (2.3), temos:

$$t\,(x' - x_0) = u\,(y' - y_0)\,. \tag{2.4}$$

Da equação (2.4), temos que $t|u\,(y' - y_0)$. Como $mdc(t, u) = s$ segue que $(y' - y_0) = ts$, para algum $s \in \mathbb{Z}$, onde:

$$y' = y_0 + ts. \tag{2.5}$$

Portanto, obtemos: $y' = y_0 + \left(\frac{a}{d}\right) s$.

Substituindo, agora o valor de y' dado pela equação (2.5) na equação (2.4), segue que:

$$t(x' - x_0) = u(y' - y_0) = sut$$

ou seja:

$$x' = x_0 + us = x_0 + \left(\frac{b}{d}\right) s.$$

Então, estes cálculos, nos permite enunciar a seguinte proposição:

Proposição 9. *Seja (x_0, y_0) uma solução particular da equação diofantina $ax + by = c$ em que $a \neq 0$ e $b \neq 0$. Então qualquer solução dessa equação é dada pelo par de inteiros:*

$$S = \left\{ \left(x_0 + \left(\frac{b}{d}\right) u, y_0 - \left(\frac{a}{d}\right) u \right) / u \in \mathbb{Z} \right\}$$

onde $d = mdc(a, b)$.

Corolário 1. *Se $d = mdc(a, b) = 1$ e $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ é uma solução particular da Equação Diofantina linear $ax + by = c$ então todas as soluções dessa equação são dadas por*

$$S = \{(x_0 + bu, y_0 - au)/u \in \mathbb{Z}\}\,.$$

Exemplo 9. Dada a equação

$$54x + 21y = 906,$$

encontre sua solução geral.

Solução: Vamos encontrar o $mdc(54, 21)$, usando o algoritmo de Euclides para o cálculo de mdc, temos a Tabela 1:

	2	1	1	3
54	21	12	9	3
12	9	3	0	

Tabela 1: $mdc(54, 21)$.

A tabela acima foi construída da seguinte maneira, o que servirá para as demais construções com as devidas adequações:

- Construímos uma tabela com três linhas e cinco colunas. Na primeira linha, serão dispostos os quocientes, na segunda linha dividendos e divisores e na terceira, os restos;
- Inicialmente vamos dividir 54 por 21 e obtivemos 2 de quociente e 12 de resto;
- Daí transportamos o resto 12 para a linha do meio e efetuamos a divisão, de 21 por 12, obtendo 1 de quociente e 9 de resto;
- Transportamos 9 para a linha do meio e efetuamos a divisão de 12 por 9, obtendo 1 de quociente e resto 3;
- Transportando o 3 para a linha do meio, efetuamos a divisão de 9 por 3, obtendo 3 de quociente e 0 de resto, finalizando a divisão.

Portanto, o $mdc(54, 21)$ é 3. Como $3|906$, a equação tem solução. Dividimos tudo por 3 daí obtemos uma equação simplificada: $18x + 7y = 302$, com $mdc(18, 7) = 1$. Se (x_0, y_0) for solução da equação $18x + 7y = 1$, então o par $(302x_0, 302y_0)$ é solução de $18x + 7y = 302$.

Usando o algoritmo de Euclides para o cálculo de mdc, temos a Tabela 2:

	2	1	1	3
18	7	4	3	1
4	3	1	0	

Tabela 2: $mdc(18, 4)$.

Logo,

$$4 = 18 - 7.2,$$
$$3 = 7 - 4.1,$$
$$1 = 4 - 3.1.$$

Daí, $1 = 4 - 3.1 = 4 - (7 - 4.1) = 4.2 - 7 = (18 - 7.2).2 - 7 = 18.2 + 7.(-5)$. Portanto, $(x_0, y_0) = (2, -5)$. Assim, $(302x_0, 302y_0) = (604, -1510)$ é uma solução particular da equação. Consequentemente, sua solução geral é expressa da seguinte forma:

$$x = 604 + 7u, y = -1510 - 18u, \text{ com } u \in \mathbb{Z}.$$

Exemplo 10. Dada a equação $5x - 2y = 2$, encontre sua solução geral.

Solução: Vamos primeiro encontrar o $mdc(5, 2)$. Temos então que $mdc(5, 2) = 1$. Notemos que se (x_0, y_0) é solução de $5x - 2y = 1$, então o par $(2x_0, 2y_0)$ é solução de $5x - 2y = 2$.

Usando o algoritmo de Euclides para o cálculo do mdc, obtemos a Tabela 3:

	2	2
5	2	1
1	0	

Tabela 3: $mdc(5, 2)$.

Assim, temos que:

$$1 = 5.1 - 2.2.$$

Portanto, $(x_0, y_0) = (1, 2)$. Assim, $(2x_0, 2y_0) = (2, 4)$ é uma solução particular da equação. Consequentemente, sua solução geral é:

$$\{x = 2 - 2t, y = 4 - 5t\}, \text{ com } t \in \mathbb{Z}.$$

2.2 Equações Diofantinas com Três Incógnitas

Consideremos uma equação $a_1x + a_2y + a_3z = b$, onde os $a_i (i = 1, 2, 3)$ são não nulos.

Serve aqui a mesma argumentação utilizada para provar a proposição 8, que garante que essa equação tem solução se, e somente se, $d = mdc(a_1, a_2, a_3)$ divide b.

É possível calcular o mdc de uma quantidade finita de números, então, primeiro analisaremos $mdc(a_1, a_2) = d_1$ e, a partir deste, $mdc(d_1, a_3) = d$.

Seja $d_1 = mdc(a_1, a_2)$ então existem k_1, $k_2 \in \mathbb{Z}$, para os quais $a_1k_1 + a_2k_2 = d_1$. E como $d = mdc(d_1, a_3)$, então existem k, $z_0 \in \mathbb{Z}$ de maneira que $d = d_1k + a_3z_0$. Logo,

$$d = (a_1k_1 + a_2k_2)k + a_3z_0 = a_1(k_1k) + a_2(k_2k) + a_3z_0. \tag{2.6}$$

Fazendo $k_1k = x_0$ e $k_2k = y_0$, substituindo em (2.6) obteremos:

$$a_1x_0 + a_2y_0 + a_3z_0 = d. \tag{2.7}$$

Portanto, se $a_1x + a_2y = b$, admite solução e como $b = dq$, para algum $q \in \mathbb{Z}$, multiplicando (2.7) por q, temos:

$$a_1(x_0q) + a_2(y_0q) + a_3(z_0q) = dq = b.$$

que nos resta demonstrado que (x_0q, y_0q, z_0q) é uma das suas soluções particulares.

Exemplo 11. Encontre uma das soluções particulares da equação $120x + 84y + 144z = 60$.

Verifiquemos a solubilidade, a partir do cálculo do $mdc(120, 84, 144)$: $D(120) = \{1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 20, 24, 30, 40, 60, 120\}$; $D(84) = \{1, 2, 3, 4, 6, 7, 12, 14, 21, 28, 42, 84\}$; *e* $D(144) = \{1, 2, 3, 4, 6, 8, 12, 18, 24, 36, 48, 72, 144\}$.

Portanto, $mdc(120, 84, 144) = 12$ e $12|60$, então a equação possui solução.

Dividindo toda equação por 12, temos sua forma equivalente: $10x + 7y + 12z = 5$ cujo $mdc(10, 7, 12) = 1$ e $1|5$. Assim, calculemos o $mdc(10, 7)$ usando o algoritmo de Euclides temos a Tabela 4:

0	1	2	3
10	7	3	1
3	1	0	

Tabela 4: $mdc(10, 7)$.

$$10 = 7.1 + 3 \Longrightarrow 3 = 10 + 7.(-1)$$
$$7 = 3.2 + 1 \Longrightarrow 1 = 7 + 3.(-2)$$
$$3 = 1.3 + 0.$$

Daí:

$$1 = 7 + 3(-2) = 7 + (10 - 7).(-2) = 7.3 + 10.(-2). \tag{2.8}$$

Passamos agora ao cálculo do $mdc(1, 12)$ usando o algoritmo de Euclides conforme Tabela 5:

	12	1
12	1	1
1	0	

Tabela 5: $mdc(12, 1)$.

$$12 = 1.11 + 1 \Longrightarrow 1 = 1(-11) + 12.$$

E como $1 = 10.(-2) + 7.3$, segue que

$$1 = (10.(-2) + 7.3).(-11) + 12$$
$$1 = 10.22 + 7.(-33) + 12.$$

Portanto, temos a solução particular da Equação Diofantina:

$$5 = 10.(110) + 7.(-165) + 12.5.$$

Logo, a terna, $(110, -165, 5)$ é a solução procurada.

Exemplo 12. Encontre todas as soluções inteiras da equação $120x + 84y + 144z = 60$.

Verificado a solubilidade da equação no exemplo anterior, passemos a encontrar a solução geral.

Tomamos $k = 10x + 7y$, então teremos $k + 12z = 5$, que também possui solução pois $mdc(12, 1) = 1$ e $1|5$. Podemos escrever $mdc(1, 12) = 1$ como combinação linear de 1 e 12:

$$1 = 1.(-11 + 12).$$

Multiplicando ambos os lados por 5 teremos:

$$5 = 1.(-55) + 12.5.$$

Assim, $(-55, 5)$ é uma solução particular de $k + 12z = 5$ e segue da proposição 9 que a solução geral é dada por:

$$S_1 = \{(-55 + 12u_1, 5 - u_1), \text{ com } u_1 \in \mathbb{Z}\}.$$

Verifiquemos agora, que $10x + 7y = k = -55 + 12u_1$. Importante verificar que $mdc(10, 7) = 1$ e $1|(-55 + 12u_1)$, isto é, u pode assumir qualquer valor inteiro pois:

$$1| - 55 \text{ e}$$
$$1|12.$$

No exemplo 10, obtivemos (2.8): $1 = 10(-2) + 7.3$, então vamos multiplicar ambos os lados por $(-55 + 12u_1)$, que resulta em:

$$(-55 + 12u_1).1 = 10(-2).(-55 + 12u_1) + 7.7.(-55 + 12u_1), \text{ ou seja,}$$
$$(-55 + 12u_1) = 10(110 - 24u_1) + 7.(-165 + 36u_1).$$

Portanto, temos que a solução geral procurada é:

$$S_2 = \{(110 - 24u_1 + 7u_2, -165 + 36u_1 - 10u_2) \text{ com } u_1 \text{ e } u_2 \in \mathbb{Z}\}.$$

Que resulta na solução geral da equação $10x + 7y + 12z = 5$ é da forma:

$$S_2 = \{(110 - 24u_1 + 7u_2, -165 + 36u_1 - 10u_2, 5 - u_1) \text{ com } u_1 \text{ e } u_2 \in \mathbb{Z}\}.$$

3 Aplicações Práticas das Equações Diofantinas

Neste capítulo, exibimos várias aplicações das Equações Diofantinas utilizadas no dia a dia. Estas equações, nos levam à diversas soluções inteiras que podem resolvê-las. Verificamos que aplicando-se restrições à uma solução geral, de forma parametrizada, podemos obter uma ou mais soluções que atendam ao que se deseja.

Vejamos alguns exemplos, onde as estratégias de resolução podem divergir da tentativa e erro, método pictórico, abordagem utilizando conceitos da Teoria dos Números e da Análise Diofantina:

Exemplo 13. Priscila recebeu $R\$50,00$ para comprar dois tipos de lanches para um piquenique com suas amigas. Depois de pesquisar, conseguiu o preço de $R\$4,00$ por misto quente e $R\$6,00$ por cachorro quente. De quantas maneiras Priscila pode comprar a sua parte do lanche para o piquenique?

Inicialmente precisamos entender que a solução envolve números inteiros, pois Priscila não pode comprar fração do misto quente, nem do cachorro quente, o problema é, portanto, caso típico de uma Equação Diofantina. Chamemos de x a quantidade de misto quente e de y a quantidade de cachorro quente. Então, temos que:

$$4x + 6y = 50 \tag{3.1}$$

e dividindo (3.1) por 2, obtemos uma equação equivalente dada por:

$$2x + 3y = 25. \tag{3.2}$$

Utilizando o Algoritmo de Euclides podemos encontrar o $mdc(2,3)$ e uma solução particular de (3.2), vejamos:

	1	2
3	2	1
1	0	

Tabela 6: $mdc(3,2)$.

A Tabela 6, nos fornece que $mdc\ 1 = 3 - 1.2$.

$$mdc(3,2) = 1 \quad e \quad 1 = 1.3 - 1.2. \tag{3.3}$$

Note que, se(x_0, y_0) for solução da equação $2x+3y = 1$, então o par $(25x_0, 25y_0)$ é solução da equação (3.2). Desta forma, observando a equação (3.3), temos que que $(x_0, y_0) = (-1, 1)$

é uma solução da equação $2x+3y=1$, consequentemente $(x,y)=(-25,25)$ é uma solução da equação (3.1).

Segue agora do corolário 1 que a solução geral é expressa da seguinte forma:

$$\begin{cases} x &= -25+3t \\ y &= 25-2t. \end{cases} \tag{3.4}$$

Como $x>0$ e $y>0$ temos que $-25+3t>0$ e $25-2t>0$.

Resolvendo cada uma delas temos que:

$$-25+3t>0 \Longrightarrow 3t>25 \Longrightarrow t>\frac{25}{3}.$$
$$25-2t>0 \Longrightarrow -2t>-25 \Longrightarrow t<\frac{25}{2}.$$

Portanto, os valores inteiros de t que se encontram no intervalo são: $9, 10, 11$ e 12.

Logo, substituindo os valores inteiros de t no sistema (3.4), as soluções possíveis são:

- Quando $t=9$, temos que $x=2$ mistos quente e $y=7$ cachorros quente;
- Quando $t=10$, temos que $x=5$ mistos quente e $y=5$ cachorros quente;
- Quando $t=11$, temos que $x=8$ mistos quente e $y=3$ cachorros quente;
- Quando $t=12$, temos que $x=11$ mistos quente e $y=1$cachorros quente.

Concluindo, essas são todas as possibilidades de adquirir mistos quente e cachorros quente com $R\$50,00$, que Priscila teria.

Outra alternativa, provavelmente utilizada por alunos do Ensino Fundamental e Médio, seria através de tentativa e erro, encontrando uma solução particular $x=2$ e $y=7$, pois de (3.2), temos: $2(2)+3(7)=25$ cujo par ordenado $(2,7)$ torna verdadeira a igualdade. Esse par seria a solução particular. Parametrizando, podemos encontrar uma solução geral. Então, seja um inteiro t. Observando os coeficientes de x e y (2 e 3, respectivamente), o par ordenado $(2,7)$ e o $mdc(2,3)=1$, podemos escrever:

$$\begin{cases} x &= 2+3t \\ y &= 7-2t. \end{cases} \tag{3.5}$$

Como $x>0$ e $y>0$ temos que $2+3t>0$ e $7-2t>0$.

Resolvendo cada uma delas temos que:

$$2+3t>0 \Longrightarrow 3t>-2 \Longrightarrow t>\frac{-2}{3}.$$
$$7-2t>0 \Longrightarrow -2t>-7 \Longrightarrow t<\frac{7}{2}.$$

Portanto, os valores inteiros de t que se encontram no intervalo são: $0, 1, 2$ e 3.

Logo, substituindo os valores inteiros de t no sistema (3.5), as soluções possíveis são:

- Quando $t = 0$, temos que $x = 2$ e $y = 7$;
- Quando $t = 1$, temos que $x = 5$ e $y = 5$;
- Quando $t = 2$, temos que $x = 8$ e $y = 3$;
- Quando $t = 3$, temos que $x = 11$ e $y = 1$.

Então, como x representa a quantidade de mistos quente e y a quantidade de cachorros quente, Priscila poderia comprar com os $R\$50,00$:

- 2 mistos quente e 7 cachorros quente ou,
- 5 mistos quente e 5 cachorros quente ou,
- 8 mistos quente e 3 cachorros quente ou,
- 11 mistos quente e 1 cachorro quente.

Enfim, conclui-se que as duas maneiras de resolução levaria ao acerto.

Exemplo 14. Júlia e Mariana resolveram chupar picolés. Chegando na sorveteria, tinham duas opções de compra: de frutas, que custava R$ 2,00 cada e ao leite, R$ 4,00 cada. Várias eram as opções para os pedidos. Pergunta-se:

a) Se Júlia e Mariana, juntas dispõe de R$ 12,00, qual o máximo de picolés que poderão comprar?

b) E o mínimo de picolés que poderão comprar?

c) Qual é o número de opções que Júlia e Mariana dispõe para fazer a compra?

Trata-se de uma situação do cotidiano. Logo, o aluno ao tentar resolver, irá realizar tentativas, verificando possibilidade de acerto. No item (a), o aluno deverá perceber que comprando os picolés de frutas, conseguirá comprar o número máximo, tendo em vista que é o que tem menor preço. Assim, realizará a operação $\frac{12}{2} = 6$ picolés de frutas. No item (b), de modo similar, deverá o aluno realizar a operação $\frac{12}{4} = 3$ picolés ao leite, pois trata-se do mais caro, portanto, será o número mínimo. Por fim, no item (c), o aluno deverá organizar uma Tabela 7, conforme abaixo, com o auxílio de cálculos:

x(de frutas)	0	2	4	6
y (ao leite)	3	2	1	0

Tabela 7: Quantidades de picolés.

Outra maneira de resolução seria através da construção da Equação Diofantina que representa a situação.

Chamemos x a quantidade de picolés de frutas e y a quantidade de picolés ao leite. Então temos que:

$$2x + 4y = 12 \tag{3.6}$$

e dividindo (3.6) por 2, obtemos uma equação equivalente dada por:

$$x + 2y = 6. \tag{3.7}$$

Como o $mdc(1, 2) = 1$ e $1|6$, logo é possível termos soluções inteiras.

Uma solução possível, através de uma abordagem de tentativa e erro, seria: $x = 2$ e $y = 2$, pois substituindo em (3.7), temos: $1(2) + 2(2) = 6$, logo o par ordenado $(2, 2)$ torna verdadeira a igualdade.Trata-se de uma solução particular da equação.

Parametrizando, podemos encontrar uma solução geral. Então, seja um inteiro t. Observando os coeficientes de x e y (1 e 2, respectivamente), o par ordenado $(2, 2)$ e o $mdc(1, 2) = 1$, podemos escrever:

$$\begin{cases} x &= 2 + 2t \\ y &= 2 - t. \end{cases} \tag{3.8}$$

Como $x \geq 0$, e $y \geq 0$ temos que $2 + 2t \geq 0$ e $2 - t \geq 0$.

Resolvendo cada uma delas temos que:

$$2 + 2t \geq 0 \Longrightarrow 2t \geq -2 \Longrightarrow t \geq -1 \text{ e,}$$
$$2 - t \geq 0 \Longrightarrow -t \geq -2 \Longrightarrow t \leq 2.$$

Portanto, os valores inteiros de t que se encontram no intervalo são: $-1, 0, 1$ e 2.

Logo, as soluções possíveis quando substituímos no sistema (3.8) são:

- Quando $t = -1$, temos que $x = 0$ e $y = 3$;
- Quando $t = 0$, temos que $x = 2$ e $y = 2$;
- Quando $t = 1$, temos que $x = 4$ e $y = 1$;
- Quando $t = 2$, temos que $x = 6$ e $y = 0$.

Então Júlia e Mariana poderiam comprar com os R$ 12, 00:

- 0 picolés de frutas e 3 picolés ao leite ou,
- 2 picolés de frutas e 2 picolés ao leite ou,
- 4 picolés de frutas e 1 picolé ao leite ou,
- 6 picolés de frutas e 0 picolés ao leite.

Exemplo 15. O cinema do centro de São Paulo, cobra o ingresso no valor de R$ 24, 00 por adulto e R$ 12, 00 por criança, em todas as sessões. O gerente do cinema (com lotação para 100 pessoas) sabe que há prejuízo se a renda por cada sessão for inferior a R$ 480, 00. Pergunta-se:

(a) Qual é o menor número de pessoas que podem assistir a uma sessão de maneira que a bilheteria não tenha prejuízo?

Resposta: O aluno deverá perceber que, para não ter prejuízo, o valor de R$ 480, 00 deverá ser dividido pelo valor do ingresso mais caro, ou seja, $\frac{480}{24} = 20$ adultos.

(b) Qual é o maior número de pessoas que podem assistir a uma sessão de maneira que a bilheteria não tenha prejuízo, nem lucro?

Resposta: O aluno deverá dividir o valor de R$ 480, 00 pelo ingresso mais barato, ou seja, $\frac{480}{12} = 40$ crianças.

(c) Se uma determinada sessão tiver vendido 5 entradas para crianças e 28 para adultos, haverá lucro ou prejuízo? Explique.

Resposta: O aluno deverá realizar os cálculos do número de ingressos de criança vezes seu preço, mais, número de ingressos de pessoa adulta vezes seu preço, ou seja: $5.12 + 28.24 = 732$, concluindo que houve lucro nesta sessão.

(d) Ajude o gerente a organizar uma tabela de acordo com a quantidade de ingressos adquiridos de adulto e criança, para que seja feito um controle sobre o lucro ou prejuízo de determinada sessão.

Resposta: Ao iniciar a construção da tabela, o aluno deverá perceber que já tem através dos itens (a) e (b), o número máximo de adultos e crianças para que não tenha valor inferior a R$ 480, 00, como seguem as Tabelas 8:

x	20	19	18	17	16	15	14	13	12	11	10
y	2	4	6	8	10	12	14	16	18	20	22

x	9	8	7	6	5	4	3	2	1	0
y	24	26	28	30	32	34	36	38	40	42

Tabela 8: Quantidade de ingressos para que se tenha lucro.

Na tabela referência, x representa a quantidade de ingressos para adultos e y, quantidade de ingressos para crianças.

Com certeza, a solução acima irá causar um desconforto no aluno, pois demandará de uma interpretação, organização de dados e cálculos. Por isso da importância de ajudá-lo na construção de uma equação que torne possível a construção da tabela acima. Vejamos:

Chamemos x a quantidade de ingressos para adultos e y a quantidade de ingressos para crianças. Então temos que:

$$24x + 12y = 480 \tag{3.9}$$

e dividindo (3.9) por 12, temos:

$$2x + y = 40. \tag{3.10}$$

Como o $mdc(2, 1) = 1$ e $1|40$, logo é possível termos soluções inteiras.

Uma solução possível, através de uma abordagem de tentativa e erro, seria: $x = 10$ e $y = 20$, pois substituindo em (3.10), temos: $2(10) + 1(20) = 40$ cujo par ordenado $(10, 20)$ torna verdadeira a igualdade.Trata-se de uma solução particular da equação.

Parametrizando, podemos encontrar uma solução geral. Então, seja um inteiro t. Observando os coeficientes de x e y (2 e 1, respectivamente), o par ordenado $(10, 20)$ e o $mdc(2, 1) = 1$, podemos escrever:

$$\begin{cases} x &= 10 + t \\ y &= 20 - 2t. \end{cases} \tag{3.11}$$

Como $x \geq 0$, e $y \geq 0$ temos que $10 + 1t \geq 0$ e $20 - 2t \geq 0$.
Resolvendo cada uma delas temos que:

$$10 + 1t \geq 0 \Longrightarrow 1t \geq -10 \Longrightarrow t \geq -10$$
$$20 - 2t \geq 0 \Longrightarrow -2t \geq -20 \Longrightarrow t \leq 10.$$

Logo, os valores inteiros de t que se encontram no intervalo são: $, -10, -9, ..., 8, 9$ e 10. Substituindo t no sistema (3.11) encontramos os valores de x e y que são dados por:

- Quando $t = -10$, temos que $x = 0$ e $y = 40$;
- Quando $t = -9$, temos que $x = 1$ e $y = 38$;
- Quando $t = -8$, temos que $x = 2$ e $y = 36$;
- Quando $t = -7$, temos que $x = 3$ e $y = 34$;
- Quando $t = -6$, temos que $x = 4$ e $y = 32$;
- Quando $t = -5$, temos que $x = 5$ e $y = 30$;
- Quando $t = -4$, temos que $x = 6$ e $y = 28$;
- Quando $t = -3$, temos que $x = 7$ e $y = 26$;
- Quando $t = -2$, temos que $x = 8$ e $y = 24$;
- Quando $t = -1$, temos que $x = 9$ e $y = 22$;
- Quando $t = 0$, temos que $x = 10$ e $y = 20$;
- Quando $t = 1$, temos que $x = 11$ e $y = 18$;
- Quando $t = 2$, temos que $x = 12$ e $y = 16$;
- Quando $t = 3$, temos que $x = 13$ e $y = 14$;
- Quando $t = 4$, temos que $x = 14$ e $y = 12$;

- Quando $t = 5$, temos que $x = 15$ e $y = 10$;
- Quando $t = 6$, temos que $x = 16$ e $y = 8$;
- Quando $t = 7$, temos que $x = 17$ e $y = 6$;
- Quando $t = 8$, temos que $x = 18$ e $y = 4$;
- Quando $t = 9$, temos que $x = 19$ e $y = 2$;
- Quando $t = 10$, temos que $x = 20$ e $y = 0$.

Então os alunos terão que perceber que os valores encontrados acima, garantem apenas que não haverá prejuízo, necessitando para haver lucros, que o número de pessoas seja maior, por isso a tabela foi construída com número de pessoas superior ao mínimo.

Exemplo 16. Fernando tem dois baldes: um com capacidade para comportar 5 litros, e outro que comporta 3 litros. Ele não possui outros recipientes e os baldes não possuem marcações de volume. Pergunta-se:

(a) Fernando precisa retirar exatamente sete litros de água de uma caixa, com esses baldes. Como fazer isto?

Aqui o aluno poderá ir por tentativa e erro, utilizando-se inclusive de um registro pictórico, ilustrado pela Figura 1, proceder com a seguinte dinâmica:

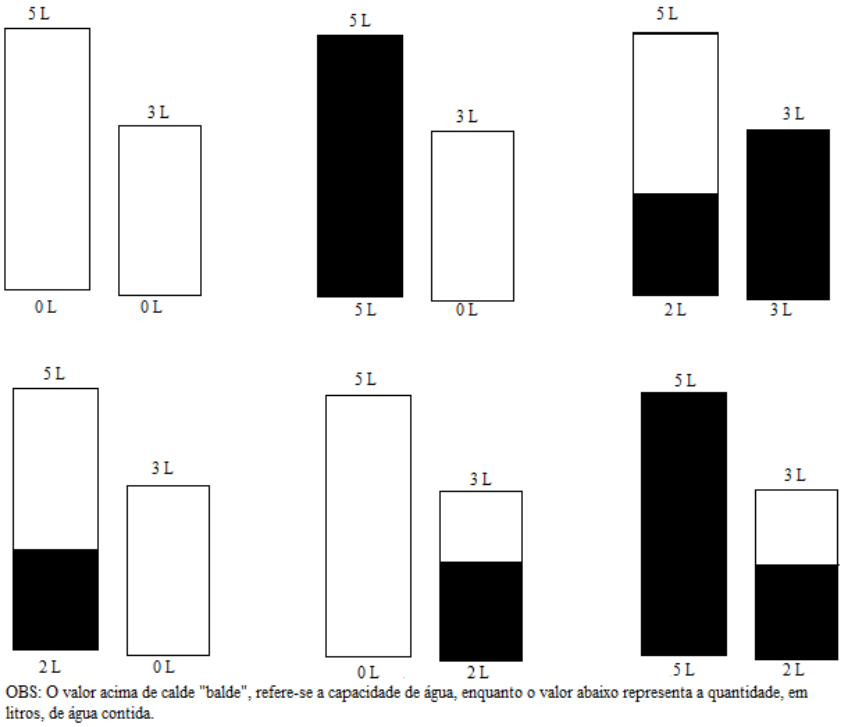


Figura 1: Balde com 7 litros [Fonte [12] - Adaptado]

- Encher o balde de 5 litros e despejar a água, até onde for possível, no balde de 3 litros, enchendo-o. Agora, restaram 2 litros no balde de 5 litros.
- Retornar a água do balde de 3 litros na caixa e colocar nele os 2 litros que estavam no balde de 5 litros. Agora, encher o balde de 5 litros de novo.
- Pronto! No balde de 3 litros estão, agora, 2 litros de água, enquanto o balde de 5 litros está cheio, totalizando 7 litros!

Temos aqui uma equação diofantina $3x + 5y = 7$, que representa a situação, é uma proposta de estratégia de Wielewki [6] onde contabiliza-se $+1$ toda vez que o balde é preenchido completamente com água e -1 para o operação de esvaziar integralmente, sendo xo número de vezes que o balde de $3l$ foi preenchido completamente com água e y o número de vezes que o balde de $5l$ foi preenchido completamente com água, logo $x = -1$ e $y = +2$, uma solução particular da equação.

(b) Com os mesmos baldes, diga como fazer para retirar exatamente 1 litro de água da mesma caixa.

O aluno deverá, por tentativa e erro, com uso de um registro pictórico, ilustrado pela Figura 2, seguir o procedimento:

- Encher o balde de 3 litros até o fim e despejar a água no balde de 5 litros;
- Encher o balde de 3 litros de novo e despejar toda a água que puder no balde de 5 litros;
- Agora, temos 1 litro de água no balde de 3 litros.

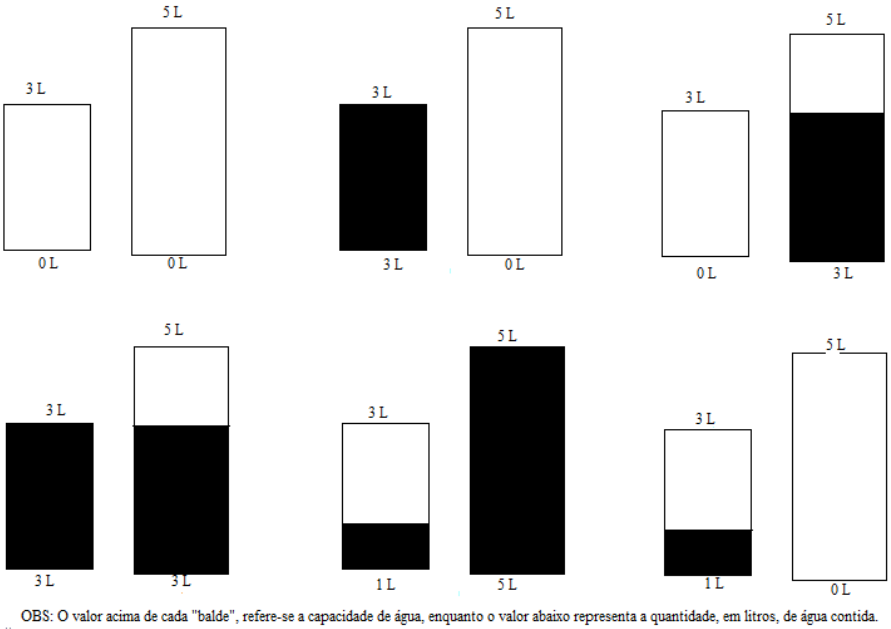


Figura 2: Balde com 1 litro. [Fonte [12] - Adaptado]

A equação diofantina $3x+5y = 1$, que representa a situação acima, é uma proposta de estratégia de Wielewki [6] onde contabiliza-se $+1$ toda vez que o balde é preenchido completamente com água e -1 para o operação de esvaziar integralmente, sendo x o número de vezes que o balde de $3l$ foi preenchido completamente com água e y o número de vezes que o balde de $5l$ foi preenchido completamente com água, logo $x = +2$ e $y = -1$, uma solução particular da equação.

Exemplo 17. Uma aluna, Paola, fã de música, reserva num certo mês R$ 120, 00 para a compra de CDs e DVDs. Um CD custa R$ 10, 00 e um DVD custa R$ 15, 00. Quais são as várias possibilidades de aquisição deste dois bens, gastando-se exatamente R$ 120, 00? ([7] Adaptado).

Chamemos de x e y, respectivamente as quantidades de CDs e DVDs possíveis que Paola poderá adquirir. Assim podemos escrever a Equação Diofantina linear $10x + 15y = 120$, que é necessária à resolução. Pois, se Paola optar por compra apenas CDs, o cálculo será:$\frac{120}{10} = 12$ CDs. Se optar com comprar apenas DVDs, $\frac{120}{15} = 8$ DVDs. Vejamos, resolvendo a equação diofantina:

$$10x + 15y = 120 \tag{3.12}$$

e dividindo (3.12) por 5, obtemos uma equação equivalente dada por:

$$2x + 3y = 24. \tag{3.13}$$

Utilizando o Algoritmo de Euclides podemos encontrar o $mdc(2, 3)$ e uma solução particular de (3.13), vejamos:

	1	2
3	2	1
1	0	

Tabela 9: $mdc(3, 2)$.

A Tabela 9, nos fornece que $mdc\ 1 = 3 - 1.2$.

$$mdc(3, 2) = 1 \quad e \quad 1 = 1.3 - 1.2. \tag{3.14}$$

Note que, se(x_0, y_0) for solução da equação $2x + 3y = 1$, então o par $(24x_0, 24y_0)$ é solução da equação (3.13). Desta forma, observando a equação (3.14), temos que que $(x_0, y_0) = (-1, 1)$ é uma solução da equação $2x + 3y = 1$, consequentemente $(x, y) = (-24, 24)$ é uma solução da equação (3.12).

Segue agora do corolário 1 que a solução geral é expressa da seguinte forma:

$$\begin{cases} x &= -24 + 3t \\ y &= 24 - 2t. \end{cases} \tag{3.15}$$

Como $x \geq 0$ e $y \geq 0$ temos que $-24 + 3t \geq 0$ e $24 - 2t \geq 0$.

Resolvendo cada uma delas temos que:

$$-24 + 3t \geq 0 \Longrightarrow 3t \geq 24 \Longrightarrow t \geq \frac{24}{3} \Longrightarrow t \geq 8.$$
$$24 - 2t \geq 0 \Longrightarrow -2t \geq -24 \Longrightarrow t \leq \frac{24}{2} \Longrightarrow t \leq 12.$$

Portanto, os valores inteiros de t que se encontram no intervalo são: $8, 9, 10, 11$ e 12.

Logo, substituindo os valores inteiros de t no sistema (3.15), as soluções possíveis são:

- Quando $t = 8$, temos que $x = 0$ CDs e $y = 8$ DVDs;
- Quando $t = 9$, temos que $x = 3$ CDs e $y = 6$ DVDs;
- Quando $t = 10$, temos que $x = 6$ CDs e $y = 4$ DVDs;
- Quando $t = 11$, temos que $x = 9$ CDs e $y = 2$ DVDs;
- Quando $t = 12$, temos que $x = 12$ CDs e $y = 0$DVDs.

Concluindo, essas são todas as possibilidades de adquirir CDs e DVDs com $R\$120,00$, que Paola teria.

Outra alternativa, provavelmente utilizada por alunos do Ensino Fundamental e Médio, seria através de tentativa e erro, encontrando uma solução particular $x = 6$ e $y = 4$, pois substituindo em(3.13), temos: $2(6) + 3(4) = 24$ cujo par ordenado $(6, 4)$ torna verdadeira a igualdade. Trata-se de uma solução particular da equação. Parametrizando, podemos encontrar uma solução geral. Então, seja um inteiro t. Observando os coeficientes de x e y (2 e 3, respectivamente), o par ordenado $(6, 4)$ e o $mdc(2, 3) = 1$, podemos escrever:

$$\begin{cases} x &= 6 + 3t \\ y &= 4 - 2t \end{cases} \tag{3.16}$$

Como $x \geq 0$ e $y \geq 0$ temos que: $6 + 3t \geq 0$ e $4 - 2t \geq 0$.

Resolvendo cada uma delas, obtemos:

$$6 + 3t \geq 0 \Longrightarrow 3t \geq -6 \Longrightarrow t \geq -2$$
$$4 - 2t \geq 0 \Longrightarrow -2t \geq -4 \Longrightarrow t \leq 2.$$

Portanto, os valores inteiros de t que se encontra no intervalo são: $-2, -1, 0, 1$ e 2.

Logo, as soluções possíveis para aquisição dos CDs e DVDs, substituindo t no sistema (3.16) são:

- Quando $t = -2$, temos que $x = 0$ e $y = 8$;
- Quando $t = -1$, temos que $x = 3$ e $y = 6$;

- Quando $t = 0$, temos que $x = 6$ e $y = 4$;
- Quando $t = 1$, temos que $x = 9$ e $y = 2$;
- Quando $t = 2$, temos que $x = 12$ e $y = 0$.

Enfim, conclui-se que as duas maneiras de resolução levaria ao acerto.

Exemplo 18. ([3] - adaptado) Em um evento do famoso Bráulio Bessa, que visava arrecadar fundos em prol dos idosos do Recanto da Terceira Idade, que ocorreu no Centro Cultural Benedito, em 2017 no município de Jataí-GO, foram vendidos R$ $720,00$ em ingressos. O valor do ingresso para homens custava R$ $15,00$ e para mulheres custava R$ $8,00$. Quantos homens e quantas mulheres participaram do evento? Descreva todas as possibilidades.

Solução: Chamemos de h o número de homens e m, o número de mulheres que participaram do evento. Como o ingresso do homem tem um custo de R$ $15,00$, da mulher um custo de R$ $8,00$ e o total arrecadado foi de R$ $720,00$, temos a Equação Diofantina $15h + 8m = 720$. Devemos verificar então se tem solubilidade tal equação. Calculando o $mdc(15, 8) = 1$ e $1|720$, então possui solução. Vamos encontrar então uma solução particular para a equação diofantina $15h + 8m = 720$, utilizando o recurso do algoritmo de Euclides obtemos a Tabela 10:

	1	1	7
15	8	7	1
7	1	0	

Tabela 10: $mdc(15, 8)$.

$$15 = 8.1 + 7 \Longrightarrow 7 = 15 + 8(-1). \tag{3.17}$$

$$8 = 7.1 + 1 \Longrightarrow 1 = 8 + 7(-1). \tag{3.18}$$

$$7 = 7.1 + 0. \tag{3.19}$$

Assim, substituindo (3.17) em (3.18) temos que:

$$1 = 8 + (15 + 8(-1))(-1) = 8 + 15(-1) + 8(1) = 15(-1) + 8(2).$$

$$1 = 15(-1) + 8(2). \tag{3.20}$$

Multiplicando por 720 (3.20), obtemos:

$$720 = 15(-720) + 8(1440).$$

Portanto, encontramos uma solução da equação, mas não do problema pois o número de homens não pode ser um valor negativo tal como encontramos,-720. Consequentemente precisamos encontrar uma solução geral para equação e limitar o intervalo de valores que sejam válidos para o problema.

Assim, escrevemos as equações paramétricas, utilizando os coeficientes da Equação Diofantina e o par ordenado $(-720, 1440)$:

$$h = -720 + 8u \text{ e } m = 1440 - 15u.$$

Como $x \geq 0$ e $y \geq 0$ temos que: $-720 + 8u \geq 0$ e $1440 - 15u \geq 0$.

Resolvendo cada uma delas, obtemos:

$$-720 + 8u \geq 0 \Longrightarrow 8u \geq 720 \Longrightarrow t \geq 90, \text{ e}$$
$$1440 - 15u > 0 \Longrightarrow -15u \geq -1440 \Longrightarrow t \leq 96.$$

Portanto, os valores inteiros de u que se encontram no intervalo são: $90, 91, 92, 93, 94, 95$ e 96.

Logo, as soluções possíveis para quantidade de homens e mulheres que participaram do evento, substituindo u nas equações paramétricas, seguem na Tabela 11:

u	h = -720 + 8u	m = 1440 -15u
90	0	90
91	8	75
92	16	60
93	24	45
94	32	30
95	40	15
96	48	0

Tabela 11: Soluções das eq. paramétricas.

Para encontrar todas as soluções da equação dada, basta substituir os valores obtidos na fórmula a seguir:

$$h = h_0 + \left(\frac{b}{d}\right) u \Longrightarrow h = -720 + \left(\frac{8}{1}\right) u,$$
$$m = m_0 - \left(\frac{a}{d}\right) u \Longrightarrow m = 1440 - \left(\frac{15}{1}\right) u,$$

sendo (h_0, m_0) o par ordenado resultante do cálculo do Algoritmo de Euclides, (a, b), os coeficientes da Equação Diofantina e d $mdc(15, 8)$.

Portanto, as soluções para a equação $15h + 8m = 720$ são dadas por:

$$S = \{(-720 + 8u, 1440 - 15u), / u \in \mathbb{Z}\}.$$

4 Sobre Equações Diofantinas não Lineares

Neste capítulo tratamos das equações Fermatianas, cujos expoentes sejam $2, 3$ ou 4. Fermat jamais publicou seus trabalhos, a não ser pelas cartas que enviava aos amigos da época, porém atualmente o conteúdo produzido por ele está incluído em todos os textos da Teoria dos Números.

4.1 Equações Diofantinas Quadráticas

Toda equação algébrica cujo expoente maior é igual a dois e as soluções estão contidas no conjunto dos números inteiros, são ditas quadráticas. Iremos assim tratar especificadamente do Teorema de Pitágoras, partindo da observação das ternas Pitagóricas e ternas Pitagóricas primitivas.

Definição 4. *Uma terna Pitagórica é uma terna de números naturais (x, y, z) tais que:*

$$x^2 + y^2 = z^2.$$

Além disso, dizemos que a terna (x, y, z) é primitiva se $mdc(x, y, z) = 1$

Proposição 10. *Seja (x, y, z) uma terna Pitagórica primitiva, então os termos x, y e z são dois a dois primos entre si.*

Demonstração. Se $d = mdc(x, y) > 1$, então existe um número primo tal que $p|d$, daí $p|x$ e $p|y$. Logo $p|x^2 + y^2 = z^2$ e, portanto $p|z$. Mas é uma contradição tendo em vista que (x, y, z) é uma terna primitiva, o $mdc(x, y, z) = 1$ então $p \leq 1$ mas p é primo logo p não pode ser um. Portanto, $d = 1$. O mesmo procedimento pode ser usado para demonstrar com os pares (y, z) e (x, z). □

Proposição 11. *Seja (x, y, z) uma terna Pitagórica qualquer, com $d = mdc(x, y, z)$ e sejam: $x_1 = \frac{x}{d}, y_1 = \frac{y}{d}$ e $z_1 = \frac{z}{d}$. Então, (x_1, y_1, z_1) forma uma terna Pitagórica primitiva.*

Demonstração. Dados $mdc(x_1, y_1, z_1) = 1$ e sendo válido $(x, y, z) = (dx_1, dy_1, dz_1)$ temos que:

$$x_1^2 + y_1^2 = z_1^2.$$

ou seja, substituindo os valores de x_1 e y_1, obtemos:

$$\left(\frac{x}{d}\right)^2 + \left(\frac{y}{d}\right)^2 = \frac{x^2 + y^2}{d^2} = \left(\frac{z}{d}\right)^2 = z_1^2.$$

Portanto (x_1, y_1, z_1) é uma terna Pitagórica primitiva. □

Enfim, podemos concluir que é possível determinar qualquer terna Pitagórica não primitiva de uma terna primitiva. Basta que multipliquemos os seus elementos por um inteiro positivo maior do que 1. Portanto, todas as soluções da equação $x^2 + y^2 = z^2$, resultam de (x_1, y_1, z_1) onde $mdc(x_1, y_1, z_1) = 1$.

Exemplo 19. Dada a terna primitiva $(3, 4, 5)$ e $mdc(3, 4, 5) = 1$. Como gerar outras ternas?

Multiplicando por um inteiro positivo k, podemos gerar infinitas: $(3k, 4k, 5k)$ fazendo $k = 2$, temos $(6, 8, 10)$; $k = 3$, temos: $(9, 12, 15)$; $k = 4$ obtemos: $(12, 15, 20)$ e assim sucessivamente. As ternas listadas são ditas não primitivas porque são obtidas multiplicando $(3, 4, 5)$ por um número inteiro maior que 1, enquanto $(3, 4, 5)$ é chamado terna Pitagórica primitiva, pois não é obtida a partir de uma multiplicação por uma constante inteira maior ou igual a dois.

Segundo Pitágoras, ainda temos as chamadas ternas Pitagóricas clássicas de primeiro tipo, em que um dos catetos e a hipotenusa são inteiros consecutivos, isto é $(a, b, b + 1)$, senão vejamos:

$$a^2 + b^2 = (b + 1)^2 \Longrightarrow a^2 = (b + 1)^2 - b^2 = 2b + 1$$

logo, a é um número ímpar, isto é, existe $k \in \mathbb{Z}$ / $a = 2k+1 \Longrightarrow 2b+1 = a^2 = (2k+1)^2 = 4k^2 + 4k + 1$.

Daí, segue que $2b = 4(2k^2) + 2(2k)$, portanto $b = 2k^2 + 2k$. Por fim, $c = b + 1 = (2k^2 + 2k) + 1 = 2k^2 + 2k + 1$.

Platão observou as ternas Pitagóricas de segundo tipo, isto é, ternas da forma $(a, b, b+2)$. Conforme argumento anterior, temos:

$$a^2 + b^2 = (b + 2)^2 \Longrightarrow a^2 = (b + 2)^2 - b^2 = 2(2b + 2), \tag{4.1}$$

logo a^2 é par e consequentemente a é par, então existe $t \in \mathbb{Z}$ tal que $a = 2t$. Desta forma, substituindo $a = 2t$ em (4.1) temos:

$$\begin{aligned}(2t)^2 = 2(2b + 2) &\Longrightarrow 4t^2 = 2(2b + 2)\\ &\Longrightarrow t^2 = \frac{2(2b + 2)}{4}\\ &\Longrightarrow t^2 = b + 1\end{aligned}$$

Como nos interessa apenas as ternas Pitagóricas primitivas então b não pode ser par, pois a é par, assim da equação $b = t^2 - 1$, concluímos que t não pode ser ímpar, logo existe $k \in \mathbb{Z}$ tal que:

$$t = 2k \Longrightarrow b = t^2 - 1 = (2k)^2 - 1 = 4k^2 - 1$$

e

$$c = (b + 2) = (4k^2 - 1) + 2 = 4k^2 + 1$$

logo, obtemos a terna pitagórica dada por $(4k, 4k^2 - 1, 4k^2 + 1)$, com $k \in \mathbb{N}$.

A tabela a seguir mostra algumas ternas de obtidas a partir das equações de Pitágoras e Platão:

(k)	$(2k + 1, 2k^2 + 2k, 2k^2 + 2k + 1)$	$(4k, 4k^2 - 1, 4k^2 + 1)$
1	$(3, 4, 5)$	$(4, 3, 5)$
2	(5,12,13)	(8,15,17)
3	(7,24,25)	(12,35,37)
4	(9,40,41)	(16,63,65)
5	(11,60,61)	(20,99,101)
6	(13,84,85)	(24,143,145)

Tabela 12: Ternas Pitagóricas

4.1.1 A Base do Teorema de Pitágoras

Pitágoras, figura envolvida na lenda e na mitologia, era muito influente. Desenvolveu a ideia lógica numérica, deixando números de serem apenas para contar e calcular, passando a serem apreciados por suas próprias características.

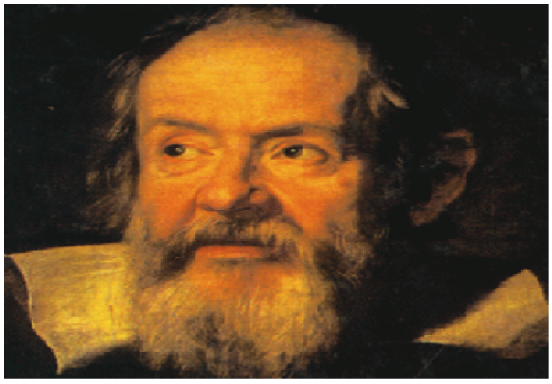


Figura 3: Pitágoras. [Fonte: [9]]

Pitágoras, no século VI a.C., reuniu muitos discípulos, criando uma sociedade secreta regida por rituais e procedimentos. Egípcios e babilônicos realizaram cálculos segundo uma receita, que sempre produziam resposta certa, sem preocuparem-se em questionar, examinar, o por que davam certo. Isso intrigava Pitágoras, que acreditava, que se entendesse a relação entre os números, poderia descobrir os segredos espirituais do universo, tornando-o próximo aos deuses. Nesse sentido, uma Irmandade Pitagórica caminhava.

Afirmava Pitágoras que a perfeição numérica dependia do número de divisores positivos distintos do próprio número. Assim 12 tem como divisores $1, 2, 3, 4, 5, 6$, é chamado de "excessivo"pois a soma de seus divisores é maior do que ele : 16. Já o número 10 tem divisores $1, 2, 5$ e somam 8, por isso, é chamado de " deficiente" e no caso do 6 que tem como divisores $1, 2, 3$ é dito "perfeito" tendo em vista que somados os divisores produzem ele mesmo.

Notou Pitágoras que os números estavam ocultos em tudo, da harmonia musical até as órbitas dos planetas, concluindo que tudo é número, inspirando muitas revoluções na ciência e a mais importante é a que leva o seu nome : o Teorema de Pitágoras.

O Teorema leva o nome de Pitágoras, não em razão de que ele fez a descoberta, pois chineses e babilônicos mil anos antes, já o utilizavam, no entanto foi ele quem realizou a demonstração universal.

Apresentamos adiante, o enunciado do Teorema de Pitágoras e em seguida duas demonstrações distintas do mesmo.

Teorema 3 (Pitágoras)**.** Seja um triângulo retângulo ABC, o quadrado da hiponetusa é igual à soma dos quadrados dos catetos, ou seja, $a^2 = b^2 + c^2$. com $a, b, c \in \mathbb{Z}$

Demonstração. 1)Dado um triângulo retângulo ABC, traça-se uma reta que irá sair do vértice A (o vértice que possui o ângulo reto) de maneira perpendicular em direção ao lado a e diremos que o ponto de encontro dessa reta com esse lado será D, então obteremos a Figura 4:

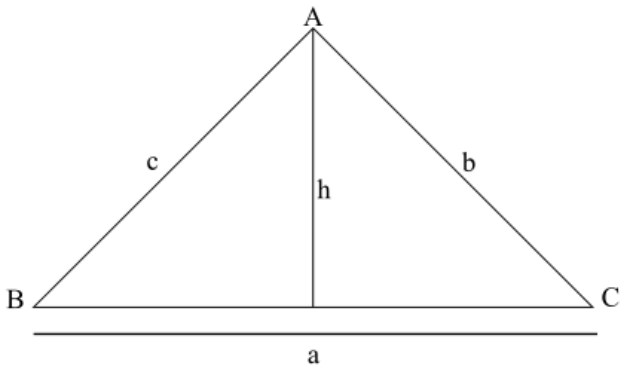


Figura 4: Triângulo Retângulo ABC.

Notemos que essa reta que acabamos de construir nada mais é do que a própria altura do nosso triângulo. Vamos dizer então que essa altura mede h. Percebemos que, depois que traçamos essa reta (altura), o lado a ficou dividido em dois pedaços. Diremos que esses pedaços medem m e n, então nossa figura ficará da seguinte maneira agora, veja Figura 5:

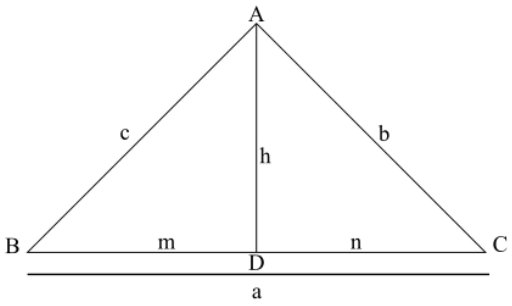


Figura 5: Triângulo com $a = m + n$.

Agora iremos dizer que os vértices B e C possuem os ângulos medindo x e y respectivamente , então teremos a Figura 6, vejamos:

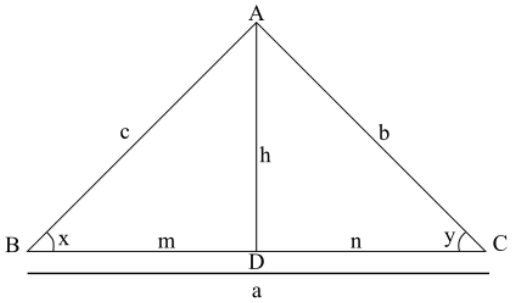


Figura 6: Triângulo com ângulos x e y.

Se observarmos bem, veremos que $x + y = 90$ olhando o triângulo ABC pois o ângulo A mede 90, então podemos, ainda preencher os dois triângulos menores ABD e ADC pelos ângulos que faltam, que no caso serão x e y. Vejamos como ficará a nova Figura 7:

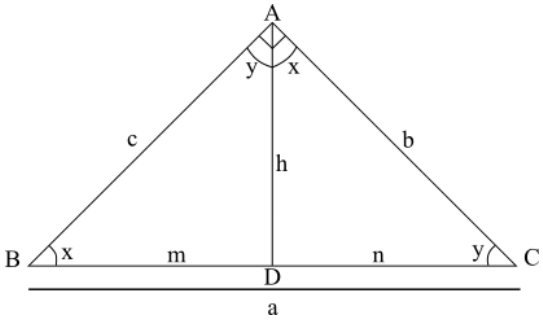


Figura 7: Triângulo com $\hat{A} = x + y$.

Essa é a figura que estávamos querendo encontrar desde o início, pois será com ela que iremos tirar as deduções necessárias para demonstrarmos o Teorema de Pitágoras. Essa figura nos permite deduzir que os triângulos ABC, ABD e ADC são semelhantes entre si e isso nos permite fazer algumas relações matemáticas com seus lados.

Para melhor entendimento, separemos esses três triângulos, veja Figura 8:

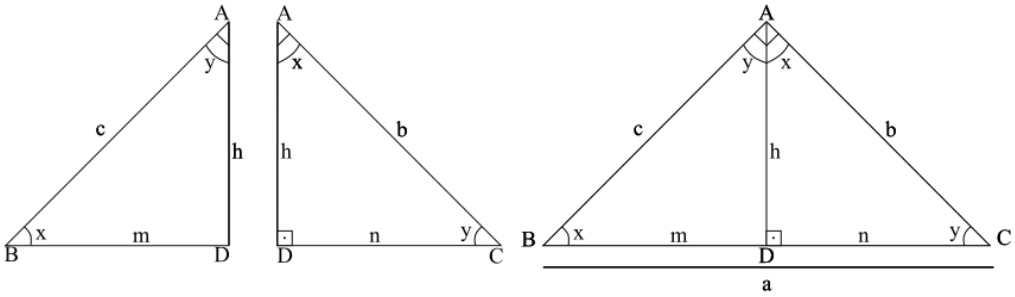


Figura 8: Triângulos ADC, ABD e ABC.

Agora faremos nossas observações, analisando apenas os triângulos ABC e ABD temos:

$$\frac{\overline{AB}}{\overline{BD}} = \frac{\overline{BC}}{\overline{AB}}$$
$$\frac{c}{m} = \frac{a}{c}$$
$$c^2 = a.m. \tag{4.2}$$

Analisando somente para os triângulos ABC e ADC temos:

$$\frac{\overline{AC}}{\overline{CD}} = \frac{\overline{BC}}{\overline{AC}}$$
$$\frac{b}{n} = \frac{a}{b}$$
$$b^2 = a.n. \tag{4.3}$$

Vimos que $b^2 = a.n$ e $c^2 = a.m$, então vamos somar (4.2) e (4.3), vejamos:

$$b^2 + c^2 = a.n + a.m.$$

Logo,

$$b^2 + c^2 = a.(m + n). \tag{4.4}$$

Sabemos que,

$$m + n = a \tag{4.5}$$

Logo, substituindo (4.5) em (4.4) obtemos:

$$b^2 + c^2 = a.(m + n)$$
$$b^2 + c^2 = a.a$$
$$b^2 + c^2 = a^2 \text{ ou seja, } a^2 = b^2 + c^2,$$

que restou provado o Teorema de Pitágoras. □

Vejamos a seguir mais uma demonstração.

Demonstração. 2) Considere um triângulo retângulo cujos lados medem, numa unidade u, a e b, catetos e a hipotenusa mede c, conforme Figura 9:

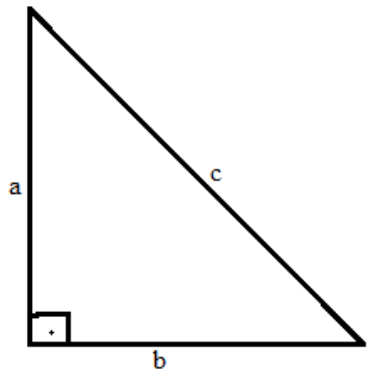


Figura 9: Triângulo retângulo de lados a, b e c.

Primeiro constroem-se dois quadrados iguais de lados $a + b$, vejamos Figura 10:

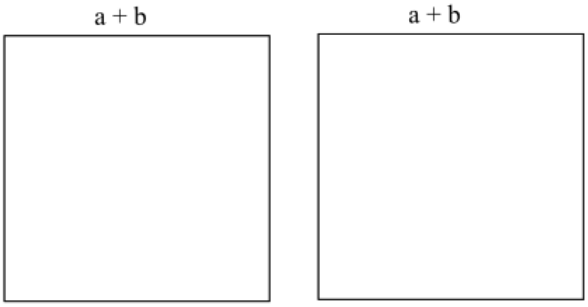


Figura 10: Quadrados de lados $a + b$.

Em sequência, num dos quadrados constroem-se 4 triângulos e no outro, dois quadrados e 4 triângulos, conforme Figuras 11.

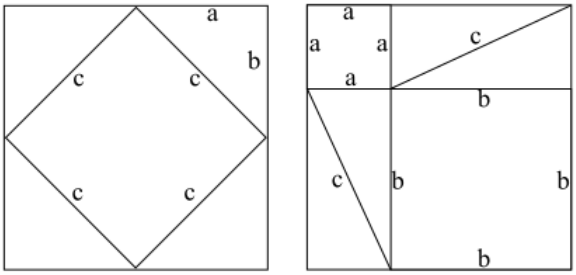


Figura 11: Quadrado com 4 triângulos.

Ora, mas em cada figura, o quadrado inicial tem de lado $a + b$. Um dos quadrados foi dividido em 4 triângulos e um quadrado com medida de lado igual a c cuja medida é da hipotenusa do triângulo considerado inicialmente. O outro quadrado foi também dividido em 4 triângulos iguais aos do quadrado anterior.

Portanto, se temos dois quadrados iniciais geometricamente iguais e ambos contêm 4 triângulos geometricamente iguais ao triângulo retângulo considerado inicialmente, então o que resta num quadrado tem que ser igual ao que resta no outro. Assim, vamos comparar as áreas dos quadrados que restam, conforme Figura 12:

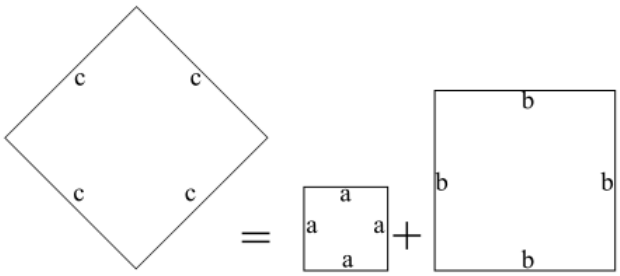


Figura 12: Representação geométrica do Triângulo de Pitágoras.

Disto concluímos que $c^2 = a^2 + b^2$ que se trata do Teorema de Pitágoras.

O Teorema de Pitágoras permite a descoberta de combinações de três números inteiros que satisfazem-no e são ditos termos de Pitágoras. Vejamos se para $a = 5, b = 4$ e $c = 3$ é verdadeira a relação de Pitágoras:

$$\begin{aligned} b^2 + c^2 &= a^2 \\ 3^2 + 4^2 &= 5^2 \\ 9 + 16 &= 25 \\ 25 &= 25. \end{aligned}$$

e geometricamente temos a Figura 13:

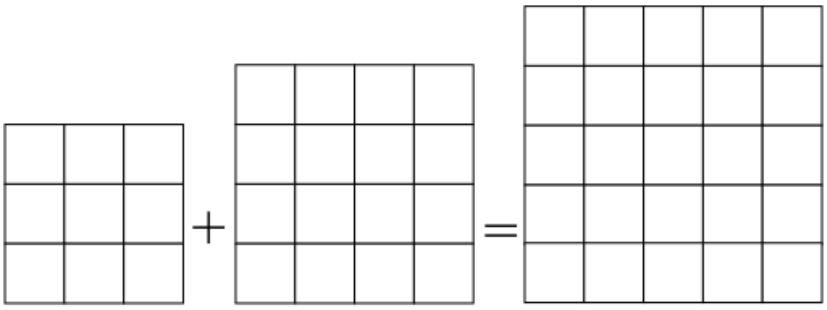


Figura 13: Representação geométrica do Teorema de Pitágoras.

Mas os Pitagóricos ficavam intrigados com essa descoberta e queriam mais trios, perceberam que os mesmos se tornam raros a medida, que os números aumentavam e encontrá-los era cada vez mais difícil. □

4.2 Equação Fermatiana Para n=3

Gerações de matemáticos tentavam encontrar números não nulos que satisfizessem a mesma equação, mas com a potência 3.

A lógica estava em re-arrumar 2 cubos, feitos de tijolinhos sem furos, para formar um terceiro cubo, maior! E o mais próximo de que alguém já chegou de um arranjo perfeito foi aquele em que falta um tijolo, conforme Figura 14:

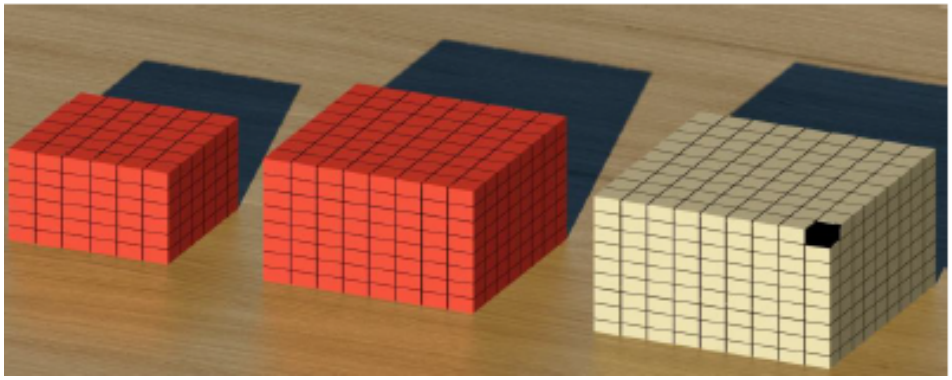


Figura 14: Representação de cubos de lados $6, 8, 9$. [Fonte: [13]]

Vejamos que a Figura 14, tem $x = 6$, $y = 8$ e $z = 9$, que numericamente calculando temos:

$$6^3 + 8^3 = 9^3, \tag{4.6}$$

onde faltará um tijolo para tornar verdadeira a igualdade (4.6).

E, se a potência for mudada de terceira (cubo), para qualquer número maior que 2, não iremos encontrar números inteiros que satisfaçam a equação:

$$x^n + y^n = z^n \text{ para } n > 2.$$

Fermat foi quem alterou ainda mais essa equação e afirmava o tempo todo que não podia existir três números inteiros, todos não nulos, que satisfizessem a equação que ficou conhecida como Fermatiana. Mas acreditava que poderiam prová-la.

Fermat intrigou a muitos matemáticos mas os motivou também a muitas descobertas. Se correspondiam por cartas, não se deixava aparecer, desafiava o mundo dos matemáticos. A fama do Teorema $x^n + y^n = z^n$ para $n > 2$ se deve unicamente ao fato do grau de dificuldade em demonstrá-lo, apesar de não ter deixado tais registros.

Fermat, através de suas cartas a alguns matemáticos, entre eles Mersenne $(1588-1648)$, Digby $(1603-1665)$ e Carcavi $(1603-1684)$ propôs para que demonstrassem que um cubo não pode ser igual à soma de dois cubos diferentes de zero.

Leonhard Euler $(1707-1783)$ foi o primeiro a apresentar uma prova, tendo em vista que utilizou o método da descida infinita, criado por Fermat, e esta apareceu em seu livro de Álgebra, publicado em São Petersburgo em 1770. No entanto, um estudo crítico dessa prova constatou-se que não foi apresentado um passo importante, sobre as propriedades da divisibilidade de números inteiros da forma a^2+3b^2. Em 1760, em seu artigo Euler, já havia provado rigorosamente que se um primo ímpar p divide a^2+3b^2, onde a e b são inteiros não nulos e primos entre si, então existem inteiros u e v tais que $p=u^2+3v^2$. Euler não estabeleceu plenamente os passos que são exigidos da prova.

Legendre$(1808-1830)$, em seu livro reproduziu a prova de Euler, sem completar os detalhes. Já em 1875, Pepin publicou um artigo sobre números na forma $a+b\sqrt{-c}$, apontando os argumentos que não tinham sido suficientemente justificados por Euler, referentes aos números na forma a^2+cb^2, especialmente para $c=1,2,3,4,7$. Schumacher (1894), Landau $(1877-1938)$, Holden $(1960-1925)$, Bergmann $(1915-2002)$ deram importantes contribuições à prova de Euler. Em 1972, Legendre considerou a prova de Euler não era perfeita e em 1977, Edwards também discutiu essa prova em seu livro.

Vejamos a demonstração da Equação Fermatiana Cúbica.

Teorema 4. Não existe uma solução de inteiros não nulos para a equação:

$$x^3+y^3+z^3=0. \tag{4.7}$$

Demonstração. Assuma que x, y e z são números inteiros não nulos, primos entre si dois a dois, tais que $x^3+y^3+z^3=0$. Então eles devem ser distintos (porque 2 não é cubo), e exatamente um destes inteiros é par, digamos que x e y são ímpares e z é par.

Entre todas as soluções com as propriedades acima escolhemos uma para que $|z|$ seja a menor escolha possível.

Devemos encontrar inteiros p, m e n, primos entre si dois a dois, satisfazendo a equação $p^3+m^3+n^3=0$, onde n é par e $|z|>|n|$. Isto irá gerar uma contradição pois teremos uma sequência infinita descendente de inteiros positivos.

Considerando que x e y são ímpares, $(x+y)$ e $(x-y)$ são pares, então existem inteiros a e b tais que $(x+y)=2a$ e $(x-y)=2b$. Portanto, $x=(a+b)$ e $y=(a-b)$, consequentemente a e b são não nulos com $mdc(a,b)=1$ e de paridades diferentes. Segue da equação $x^3+y^3+z^3=0$ que:

$$-z^3=x^3+y^3=(a+b)^3+(a-b)^3=2a(a^2+3b^2). \tag{4.8}$$

Tendo em vista que (a^2+3b^2) é ímpar, pois a e b tem paridades diferentes e z é par, portanto 8 divide z^3 e assim 8 divide $2a$. Portanto, a é par e b é ímpar.

Sendo a par e b ímpar, então $\text{mdc}(2a, a^2+3b^2) = 1$ ou 3. De fato, seja q um primo e qk um fator comum dos termos acima, isto é, $2a = qkc$ e $(a^2+3b^2) = qkd$. Como (a^2+3b^2) é ímpar, logo $q \mp 2$ e qk dividem a e assim qk divide $3b^2$. Como $\text{mdc}(a,b) = 1$ e q divide a então q não divide b e como divide $3b^2$, concluímos que $k = 1$ e $q = 3$.

Vamos agora considerar dois casos: $\text{mdc}(2a, a^2+3b^2) = 3$ e $\text{mdc}(2a, a^2+3b^2) = 1$.

Caso 1: O $mdc(2a, a^2+3b^2) = 3$

Vamos escrever $a = 3c$. Como $8|2a$ segue que $4|a$, c é par e 3 não divide b, visto que $mdc(a,b) = 1$. Logo:

$$-z^3 = 2a\left(a^2+3b^2\right) = 2\,(3c)\left[(3c)^2+3b^2\right] = 18c\left(3c^2+b^2\right) \tag{4.9}$$

Consideremos que $mdc\,(18c, 3c^2+b^2) = 1$. De fato, como c é par e b é ímpar, teremos que $3c^2+b^2$ é ímpar, 3 não divide b e $\text{mdc}(b,c) = 1$. Pela fatoração única de inteiros, temos que 18c e $(3c^2+b^2)$ são cubos, ou seja:

$$18c = r^3 \text{ e } 3c^2+b^2 = s^3,$$

onde s é ímpar e divide r.

Se s é ímpar e $s^3 = (b^2+3c^2)$ com $mdc(b,c) = 1$, então s também será da forma $s = (u^2+3v^2)$ com $u, v \in \mathbb{Z}$, assim:

$$b = u(u^2-9v^2) \text{ e } c = 3v(u^2-v^2).$$

Assim teremos que u é ímpar e v é par (em razão de que b é ímpar), $v \neq 0$, e $mdc(u,v) = 1$. Portanto, $2v, (u+v), (u-v)$ são relativamente primos dois a dois, segue a equação:

$$r^3 = 18c = 18[3v(u^2-v^2)] = 54v(u+v)(u-v). \tag{4.10}$$

Daí, partindo da equação (4.10), podemos escrever:

$$\left(\frac{r}{3}\right)^3 = 2v(u+v)(u-v). \tag{4.11}$$

Concluímos, então, que todos são cubos, ou seja:

$$\begin{aligned} 2v &= -n^3, \\ u+v &= p^3, \\ u-v &= -m^3, \end{aligned}$$

a terna (n,p,m) são todos distintos de zero, relativamente primos entre si, dois a dois, e satisfazem a (4.7):

$$x^3+y^3+z^3 = 0$$

$$n^3 + p^3 + m^3 = 0$$
$$(u+v) - (u-v) - 2v = 0,$$

onde n é par e $|z| > |n|$, o que contradiz a escolha inicial, solução da equação (4.7) para o qual o $|z|$ é a menor escolha possível.

Caso 2: O $mdc(2a, a^2 + 3b^2) = 1$

Da equação (4.8), temos que $(2a)$ e $(a^2 + 3b^2)$ são cubos:

$$2a = r^3 \tag{4.12}$$

e

$$a^2 + 3b^2 = s^3, \tag{4.13}$$

onde s é ímpar e não é múltiplo de 3. Sendo s ímpar, válida a equação (4.13) com $mdc(a, b) = 1$, então podemos escrever $s = (u^2 + 3v^2)$ com $u, v \in \mathbb{Z}$ e,

$$a = u(u^2 - 9v^2) \tag{4.14}$$

e

$$b = 3v(u^2 - v^2). \tag{4.15}$$

Temos então que v é ímpar, u é par (porque b é ímpar), u é não nulo, 3 não divide u, pois 3 não divide a e $mdc(u, v) = 1$. Portanto, $2u, (u + 3v), (u - 3v)$ são relativamente primos e da equação (4.12), temos que:

$$r^3 = 2.u(u^2 - 9v^2) = 2u(u - 3v_)(u + 3v). \tag{4.16}$$

Segue então que todos os termos de r^3, (4.16), são cubos:

$$2u = -n^3, \tag{4.17}$$

$$u - 3v = p^3, \tag{4.18}$$

e

$$u + 3v = m^3, \tag{4.19}$$

como 3 não divide u, temos que a terna (p, m, n) todos são distintos de zero, relativamente primos entre si dois a dois e satisfazem a equação (4.7), pois:

$$p^3 + m^3 + n^3 = (u - 3v) + (u + 3v) - 2u = 0, \tag{4.20}$$

onde n é par e $|z| > |n|$, o que contradiz a escolha inicial da terna (x, y, z) como solução da equação (4.7) para qual $|z|$ é a menor escolha possível. □

4.3 Equação Fermatiana Biquadrática

Apresentamos o caso para $n = 4$, onde Fermat estudou o seguinte problema: A área de um triângulo Pitagórico de lados (a, b, c) satisfazendo a equação

$$a^2 + b^2 = c^2 \tag{4.21}$$

pode ser o quadrado de um número inteiro?

Sabemos que a área de um triângulo satisfazendo (4.21) é dada por: $A = \frac{1}{2}a.b$. Para atender o que foi pedido, queremos escrever: $a.b = 2d^2$, onde $d \in \mathbb{Z}$.

Exemplo 20. Vamos verificar se é válido para o triângulo pitagórico de lados $(3, 4, 5)$:

$$5^2 = 4^2 + 3^2 \Longrightarrow A = \frac{1}{2}.3.4 \Longrightarrow a.b = 2d^2$$
$$25 = 16 + 9 \Longrightarrow A = 6 \Longrightarrow 5.4 = 2d^2.$$
$$25 = 25 \Longrightarrow A = 6 \Longrightarrow \sqrt{10} = d.$$

Portanto, concluímos que é falso para este caso.

Fermat foi levado a estudar a equação do tipo $x^4 + y^4 = z^2$ e concluiu o seguinte resultado:

Proposição 12. *As equações do tipo $x^4 + y^4 = z^2$ não possuem solução no conjunto dos números inteiros não nulos.*

Demonstração. Visto que a afirmação é falsa, então temos (x, y, z) uma terna de inteiros positivos com x o menor possível tais que:

$$x^4 + y^4 = z^2. \tag{4.22}$$

Então, $mdc(x, y) = 1$, porque se um primo divide x e y simultaneamente, então p^4 divide z^2, e portanto p^2 divide z. Desta forma, fazendo $x = px_1, y = py_1$ e $z = pz_1$ e substituindo em (4.22), obtemos:

$$(px_1)^4 - (py_1)^4 = (p^2z_1)^2 \text{ logo,}$$
$$p^4x_1^4 - p^4y_1^4 = p^4z_1^2.$$

Dividindo tudo por p^4, temos:

$$x_1^4 - y_1^4 = z_1^2,$$

com $0 < x_1 < x$, o que contradiz a hipótese para escolha inicial de x. Assim temos que:

$$z^2 = x^4 - y^4$$
$$z^2 = (x^2 + y^2).(x^2 - y^2),$$

podendo o $mdc((x^2+y^2).(x^2-y^2))$ igual a 1 ou 2, pois $mdc(x,y)=1$

Assim devemos analisar os dois casos: 1) mdc $(x^2+y^2).(x^2-y^2)=1$ e 2)mdc $(x^2+y^2).(x^2-y^2)=2$.

Caso 1: Como o produto de $(x^2+y^2).(x^2-y^2)$ é um quadrado, então (x^2+y^2) e (x^2-y^2) são quadrados, ou seja, existem inteiros positivos s, t com mdc$(s,t)=1$, tais que:

$$x^2+y^2=s^2 \tag{4.23}$$

e

$$x^2-y^2=t^2. \tag{4.24}$$

Daí segue que s e t devem ser ambos ímpares, visto que somando as equações (4.23) e (4.24), obtemos: $2x^2=s^2+t^2$, então s e t tem a mesma paridade e não podem ser ambos pares pois o $mdc(s,t)=1$. Assim, existem inteiros positivos u, v tais que:

$$u=1/2(s+t) \tag{4.25}$$

e

$$v=1/2(s-t), \tag{4.26}$$

segue que $mdc(u,v)=1$ porque s e t são ambos ímpares. Multiplicando as equações (4.25) e (4.26), logo temos que:

$$u.v=\frac{1}{4}(s^2-t^2)=\frac{1}{2}y^2 \text{ e}$$
$$u.v=\frac{1}{2}y^2,$$

assim $y^2=2uv$ e, como $mdc(u,v)=1$ então existem inteiros positivos l,m tais que:

$$u=2l^2 \text{ ou } u=l^2 \text{ e}$$
$$v=m^2 \text{ ou } v=2m^2$$

Faremos a primeira alternativa, pois a outra, de maneira análoga, também se resolve. Deste modo, u é par e o $mdc(u,v,x)=1$, logo:

$$u^2+v^2=\frac{1}{4}(s+t)^2+\frac{1}{4}(s-t)^2=\frac{(s^2+t^2)}{2}=\frac{(2x^2)}{2}=x^2.$$

Como $x^2=u^2+v^2$, existem inteiros positivos a,b com $0<b<a$ com $mcd(a,b)=1$ onde $u=2l^2$ e $v=m^2$ tais que:

$$u=2ab,$$
$$v=a^2-b^2 \text{ e}$$
$$x=a^2+b^2.$$

Assim, $u = 2l^2 = 2ab \Longrightarrow l^2 = ab$ e com, $mdc(a, b) = 1$, existem inteiros positivos c e d como $mdc(c, d) = 1$ tais que:

$$a = c^2 \text{ e}$$
$$b = d^2,$$

logo, $m^2 = v = a^2 - b^2 = c^4 - d^4$. Como $0 < c < a < x$ e sendo (c, d, m) uma terna de números inteiros positivos, ela seria uma solução da equação $x^4 + y^4 = z^2$ com $0 < c < x$, o que contradiz a hipótese para escolha inicial de x, como sendo o menor possível.

Caso 2: $mdc(x^2 + y^2, x^2 - y^2) = 2$ e temos x e y, ambos ímpares e z par.

Sendo $x^4 - y^4 = z^2$ temos que $z^2 + (y^2)^2 = (x^2)^2$ que existem inteiros positivos a, b com $0 < b < a$, e $mdc(a, b) = 1$, tais que:

$$z = 2ab,$$
$$y^2 = a^2 - b^2, \text{ e}$$
$$x^2 = a^2 + b^2.$$

Agora, $(xy)^2 = x^2y^2 = (a^2 + b^2).(a^2 - b^2) = a^4 - b^4$, o que contradiz novamente a hipótese para escolha inicial de x como sendo o menor possível que satisfaz a equação. □

Conhecido como Método da Descida Infinita, que fora inventado por Fermat, o argumento acima pode ser formulado da seguinte maneira: Se tivermos (x_0, y_0, z_0) como uma solução em inteiros positivos da equação $x^2 - y^2 = z^2$ então obteríamos uma outra solução em inteiros positivos (x_1, y_1, z_1) com a propriedade $x_1 < x_0, x_2 < x_1$ e assim por diante, por isso intitulada sequência decrescente infinita de inteiros positivos:

$$x_0 > x_1 > x_2 > ...$$

o que não é possível.

A seguir, apresentaremos uma Equação Diofantina, mais conhecida como Declaração de Fermat.

Proposição 13. *As equações do tipo $x^4 + y^4 = z^4$ não possuem solução no conjunto dos números inteiros não nulos.*

Demonstração. Primeiramente suponhamos que, se houver uma solução x, y, z, existe uma solução primitiva, ou seja, uma terna com $mdc(x, y, z) = 1$. Isso significa que os três números são relativamente primos.

Em segundo lugar, substituímos $x^4 + y^4 = z^4$ com $x^4 + y^4 = z^2$, pois se o último não tiver soluções inteiras, o mesmo vale para o primeiro devido a $x^4 + y^4 = (z^2)^2$.

Então, temos é provar que $x^4 + y^4 = z^2$ não possui soluções inteiras. Suponha, por contradição, que, para alguns x, y, z, com $mdc(x, y, z) = 1, x^4 + y^4 = z^2$. Então, é claro, $(x^2)^2 + (y^2)^2 = z^2$ de modo que x^2, y^2, z é um triplo pitagórico que podemos assumir

primitivo. Por isso (se necessário realizar a troca de x e y), existem p, q, de paridades opostas , com $q \neq 0 \neq p$:

$$x^2 = 2pq, \tag{4.27}$$

$$y^2 = p^2 - q^2 \tag{4.28}$$

e

$$z = p^2 + q^2. \tag{4.29}$$

Segue-se que existem soluções positivas, mutuamente primos, b de paridade oposta, de modo que $b \neq 0 \neq a$ e

$$q = 2ab, \tag{4.30}$$

$$y = a^2 - b^2 \tag{4.31}$$

e

$$p = a^2 + b^2. \tag{4.32}$$

Substituindo p e q (equações (4.30) e (4.32)) em (4.27), obtemos:

$$x^2 = 2pq = 4ab(a^2 + b^2).$$

Vamos mostrar que todos os três a, b, $a^2 + b^2$ são quadrados.

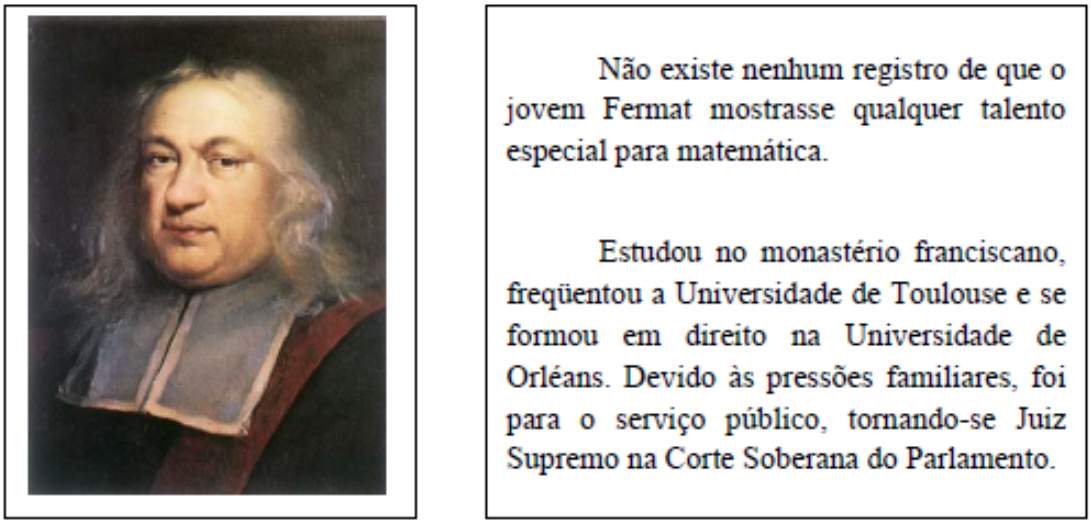
Sendo, $ab(a^2 + b^2) = \left(\frac{x}{2}\right)^2$ o quadrado de um inteiro. Se um primo s divide ab, uma vez que são mutuamente primos, s então divide exatamente um deles: a ou b. Então, é claro, s não pode dividir $a^2 + b^2$, portanto, $mdc(ab, a^2 + b^2) = 1$. Assim a, b e $a^2 + b^2$ são quadrados desde que $mdc(a, b) = 1$.

Façamos $a = x^2, b = y^2, a^2 + b^2 = z^2$. Então $x^4 + y^4 = z^2$, o que contradiz a proposição 12. Serve assim, como ponto de partida para a descida infinita. □

Apêndice

Pierre de Fermat: o criador de enigmas e a evolução da Teoria dos Números.

Em 20 de agosto de 1601, na cidade de Beaumont-de-Lomagne no sudoeste da França, nasce Pierre de Fermat [5]. De família rica pela exploração de peles, Fermat recebeu uma educação privilegiada no Monastério Franciscano de Grandselve, frequentou a Universidade de Toulouse e se formou em direito na Universidade de Orléans.



Não existe nenhum registro de que o jovem Fermat mostrasse qualquer talento especial para matemática.

Estudou no monastério franciscano, freqüentou a Universidade de Toulouse e se formou em direito na Universidade de Orléans. Devido às pressões familiares, foi para o serviço público, tornando-se Juiz Supremo na Corte Soberana do Parlamento.

Figura 15: Fermat [Fonte: [10]]

Fermat teve uma ascensão rápida como funcionário público na cidade francesa Toulouse, sendo nomeado Conselheiro do Parlamento e Conselheiro na Câmara dos Requerimentos. Os requerimentos dos cidadãos primeiro teriam que convencer Fermat da sua relevância, para depois ser apresentado ao Rei.

Aos 51 anos, Fermat é acometido de uma doença que se alastrava por toda a Europa, além do que ele precisava sobreviver aos riscos de entrega e tramas tendo em visto que o Cardeal Richeliieu era ministro da França; necessário não chamar as atenções para si pois o Cardeal era maquiavélico.

Fermat era eficiente, não tinha ambições políticas, cumpria suas obrigações de modo que não chamasse a atenção. De temperamento pacato e evitando chamar as atenções para si, adotou a estratégia de ficar a maior parte do seu tempo recolhido em casa, focando toda a sua energia que lhe sobrava à matemática e à literatura clássica.

Era corriqueiro Fermat desafiar a outros matemáticos com problemas intrigantes e que por vezes deixou seus contemporâneos mergulhados na tentativa de dar as soluções

cabíveis aos problemas propostos.

Um grande amigo de Fermat, Maren Marsenne $(1588 - 1648)$ era o contato com os matemáticos, servindo como centro de distribuição de informações. Certa vez, Marsenne escreveu-lhe indagando sobre o número muito grande 100.895.598.169 era primo ou não e sem hesitar respondeu que por se tratar do produto de 112.303 e 898.432, e que cada um desses fatores era primo, então o número 100.895.598.169 era primo também . Mersenne encoraja Fermat a dar publicidade aos seus trabalhos e demonstrações. Porém para ele nada significativa o reconhecimento público, o que gostava mesmo era de criar novos teoremas sem ser perturbado.

A influência de Fermat na matemática foi limitada pelo desinteresse em publicar suas descobertas, pois se comunicava com outros matemáticos através de correspondências, sem fornecer a demonstração, desafiando os amigos que possuíam interesse pelo a matemática. As cartas eram repletas de ideias e descobertas mas não continham a solução, com duplo sentido de assim serem, desafiar seus amigos e prosseguir diretamente para a próxima conquista.

Contribuiu Fermat, com Teoria da Probabilidade, em conjunto com Blaise Pascal, enquanto trocavam cartas. Determinaram as regras essenciais da probabilidade, mas seu interesse maior era na Teoria dos Números e em jogos com números, que ele criava e desafiava matemáticos. Também esteve envolvido na fundação de outra área matemática, o calculo infinitesimal, que revolucionou a ciência , compreendendo melhor a conceito de velocidade e sua relação com a aceleração. Foi dele também o estudo dos eixos perpendiculares e base das coordenadas cartesianas, cujo estudo é atribuido à René Descartes.

Fermat era obcecado em entender as propriedades e as relações entre os números, garantido assim suas maiores realizações na Teoria dos Números, ampliando um conhecimento deixado por Pitágoras.

Acreditava-se que a ideia de demonstração na matemática se espalhou rapidamente pelo mundo civilizado depois morte de Pitágoras. Alexandre, o Grande, depois de conquistar a Grécia, a Ásia menor e o Egito em $332.a.C$, resolveu construir uma capital que seria a cidade mais importante do mundo: Alexandria. Porém somente depois de sua morte, com ascensão de Ptolomeu I ao trono do Egito, é que a capital recebe a primeira universidade do mundo. Muitos matemáticos e outros intelectuais foram atraídos para lá pois a Biblioteca de Alexandria continha cerca de 600 mil livros, os melhores e os mais famosos professores.

Euclides foi o primeiro diretor do departamento matemático, ele acreditava na busca da verdade matemática pura e não buscava aplicações de seu trabalho, tal como Pitágoras. Escreveu "Os elementos" em 13 volumes e explorava em sua obra uma arma lógica, conhecida como "redução ao absurdo" ou " prova da contradição". A ideia de provar que um teorema é verdadeiro, presumindo primeiro que a tese seja falsa. Explorando as consequências lógicas do teorema ser falso, obtêm-se uma contradição de algum fato que

sabemos ser verdade, e portanto concluímos que o teorema original não pode ser falso, ou seja, o teorema deve ser verdadeiro.

O livro Apologia do matemático, de G.H Hardy, assim descreve a redução ao absurdo: "Redução ao absurdo, que Euclides tanto amava, é uma das melhores armas do matemático. É um desafio muito maior que qualquer jogo de xadrez. O jogador de xadrez pode oferecer um sacrifício de cem peões ou de uma peça mais importante, mas o matemático oferece o jogo inteiro".

Diofanto de Alexandria, o último herói da tradição matemática, apenas deve ter vivido em torno de 250 antes de nossa era. Na obra intitulado "Aritmética", dos treze volumes formavam, somente seis sobreviveram e inspiraram outros matemáticos da renascença, incluindo Fermat. Os demais, foram perdidos numa série de acontecimentos trágicos que levaram a matemática de volta para a era Babilônica.

Figura 16: Livro Aritmética[Fonte: [11]]

Fermat não adquiriu o interesse pela a matemática sob a influência de algum tutor, mais o contato com uma cópia de Aritmética. Encontrava ali a teoria dos números como era no tempo de Diofante e todo o conhecimento dos números obtidos por gênios como Euclides e Pitágoras, sobre a teoria dos números, Fermat estava fascinado.

No livro II da Aritmética, Fermat encontrou uma série de observações, problemas e soluções relacionados ao Teorema de Pitágoras e as ternos pitagóricos. Fermat estava convencido que Euclides conhecia infinitas ternas Pitágoricas, denominadas de primeiro e segundo tipo.

No decorrer do tempo, grandes matemáticos aventuram-se a solucionar o UTF, percorrendo caminhos tortuosos com temor de que o mesmo os levasse à direção errada. Leonhard

Euler $(1707 - 1783)$, um dos mais importantes matemáticos do século XVIII foi quem fez o primeiro avanço em direção, para o caso $n = 3$.

A matemática na época de Fermat era como cálculo que só tinha a desafiar e elucidar enigmas. Porém no século XVIII os matemáticos eram tratados como solucionares profissionais de problemas. Isaac Newton mesmo, queira aplicar a matemática ao mundo físico, nas órbitas dos planetas às trajetórias das balas de canhão. E foi logo depois que Newton morreu, que Euler publicou o seu trabalho que apresentava uma matemática elegante e moderadora, um problema relacionado a rastreamento de navios.

Euler se tornou uma celebridade matemático capaz de resolver qualquer problema que lhe fosse apresentado . No tocante ao Teorema de Fermat, recebeu um empurrão quando descobriu uma pista oculta nas anotações de Fermat, que escreve disfarçadamente uma prova para o caso $n = 4$, em outra parte do livro Aritmética de Diofante, usando claramente uma prova contradição conhecida como "método de descida infinita".

Considerações Finais

Neste trabalho, fizemos uma abordagem dos métodos que nos possibilitam resolver uma Equação Diofantina, encontrando infinitas soluções.

Inicialmente, apresentamos alguns estudos sobre algumas propriedades aritméticas relativas aos números inteiros, sendo: Divisibilidade, Números Primos, Máximo Divisor Comum e Algoritmo de Euclides, com a finalidade de garantir caminhos para a resolução de Equações Diofantinas com duas variáveis, três variáveis, n variáveis, as quadráticas e o Último Teorema de Fermat para $n = 3$ e $n = 4$.

Ao concluir este, esperamos que tenhamos contribuído para que os alunos da Segunda Etapa do Ensino Fundamental, Ensino Médio e possíveis leitores interessados neste conteúdo, possam valer-se dos ensinamentos deste para entender situações do dia-a-dia e que se relacionam com as Equações Diofantinas.

Referências

[1] LANDAU, Edmund.Teoria elementar dos números, Coleção Clássicos da Matemática. 25

[2] DOMINGUES, Higino. Fundamentos de Aritmética, 1ª Edição. São Paulo: Atual Editora Ltda - 1991. 16, 25

[3] SOUZA, Romario S. Equações Diofantinas, Quadráticas e Aplicações, Dissertação (Mestrado Profissional em Matemática), Universidade Estadual Paulista "Júlio de Mesquita Filho", Rio Claro, SP - 2017. 41

[4] HEFEZ, Abramo. Aritmética, Coleção PROFMAT, 1ª edição. Rio de Janeiro, 2014. 16, 23, 25

[5] SINGH, Simon. O Último Teorema de Fermat, Tradução de Jorge Luis Calife, 20ª edução, Editora Record, 2012. 14, 59

[6] AVERBACH, Schein, 2000, páginas 117-118 apud WIELEWSKI, 2005, página 252. 38, 39

[7] STIGLITIZ JE, Walsh CE. Introdução à Microeconomia, 3.ed.Rio de Janeiro: Editora Campus, 2003. 39

[8] CAMPOS, G.D.M. Equações Diofantinas Lineares. Dissertação(Mestrado Profissional em Matemática). Universidade Federal de Mato Grosso, Cuiabá - MT, 2013. 25

[9] www.astropt.org/2014/08/27/demonstracao-do-teorema-pitagoras/. 11, 45

[10] https://pt.wikipedia.org/wiki/Pierre-de-Fermat. 11, 59

[11] http://www.educ.fc.ul.pt/docentes/opombo/seminario/fermat/imagem/Livro-fermat1.jpg. 11, 61

[12] WIELEWSKI, Gladys Denise. Aspectos do pensamento matemático na resolução de problemas: uma representação contextualizada na obra de Krutestskii,2005.407f. Tese(Doutorado em Educação Matemática). Pontifícia Universidade Católica de São Paulo. 11, 37, 38

[13] http://www2.unirio.br/unirio/ccet/profmat/tcc/TCCSALVADOR01.10.2014 VERSAOFINAL.pdf 11, 51