Universidade Federal do Triângulo Mineiro - UFTM

Mestrado Profissional em Matemática em Rede Nacional - PROFMAT

PROFMAT

Dissertação de Mestrado

Um breve estudo sobre Equações Diofantinas

Uberaba - Minas Gerais

Dezembro de 2019

Um breve estudo sobre Equações Diofantinas

Érika Brinck Gonçalves

Dissertação de Mestrado apresentada à Comissão Acadêmica Institucional do PROFMAT-UFTM como requisito parcial para obtenção do título de Mestre em Matemática.

Orientador: Prof. Dr. Rafael Peixoto.

Uberaba - Minas Gerais

Dezembro de 2019

Catalogação na fonte: Biblioteca da Universidade Federal do Triângulo Mineiro

Gonçalves, Érika Brinck
G625b Um breve estudo sobre equações diofantinas / Érika Brinck Gonçalves. -- 2020.
88 f. : il.

Dissertação (Mestrado Profissional em Matemática em Rede Nacional) -- Universidade Federal do Triângulo Mineiro, Uberaba, MG, 2020
Orientador: Prof. Dr. Rafael Peixoto

1. Equações diofantinas. 2. Soma de quadrados. 3. Fermat, Último teorema de. I. Peixoto, Rafael. II. Universidade Federal do Triângulo Mineiro. III. Título.

CDU 511.5

ÉRIKA BRINCK GONÇALVES

UM BREVE ESTUDO SOBRE EQUAÇÕES DIOFANTINAS

Dissertação de Mestrado apresentada à Comissão Acadêmica Institucional do PROFMAT-UFTM como requisito parcial para obtenção do título de Mestre em Matemática.

14 de Fevereiro de 2020.

Banca Examinadora

Prof. Dr. Rafael Peixoto
Orientador
Universidade Federal do Triângulo Mineiro – UFTM

Leonardo de Amorim e Silva
Prof. Dr. Leonardo de Amorim e Silva
Universidade Federal do Triângulo Mineiro – UFTM

Prof. Dr. José Ricardo Gonçalves Manzan
Instituto Federal do Triângulo Mineiro – IFTM - Uberaba

Dedico este trabalho a minha família, que sempre esteve ao meu lado, me incentivando e dando força nos momentos mais difíceis.

Agradecimentos

Agradeço primeiramente à Deus, pela vida, saúde e oportunidades.

À minha família, por serem minha base e meu apoio, meus pais, Claudio e Ione, e minha irmã Kárita, luz da minha vida, amor puro e exemplo de força.

Ao meu namorado, Giovanni, pelo grande incentivo, me fazendo sentir capaz nos momentos em que pudesse pensar em desistir.

Ao meu orientador, Prof. Dr. Rafael Peixoto, pela paciência, apoio e auxílio, e por compartilhar seus conhecimentos.

Aos meus colegas Paloma, Olívia, Paula, Carlos e Guilherme, por serem apoio, alívio e carinho em meio às turbulências e dificuldades do curso e a todos os demais, colegas e professores, que de alguma forma contribuíram para que eu pudesse vencer esta etapa.

"A felicidade não se resume na ausência de problemas, mas sim na sua capacidade de lidar com eles." Albert Einstein

Resumo

Este trabalho trata-se de um breve estudo e pesquisa sobre algumas Equações Diofantinas. Estas equações são conhecidas por tal nome em homenagem à Diofanto de Alexandria, conhecido por suas contribuições em Álgebra e Teoria dos Números e pelo seu principal trabalho, o livro Aritmética. As Equações Diofantinas, tratam-se de equações polinomiais que permitem a duas ou mais variáveis assumirem apenas valores inteiros e podem apresentar várias formas diferentes, e, portanto, em sua maioria devem ser analisadas de forma individual, para verificar se possuem ou não solução. Buscamos apresentar algumas Equações Diofantinas, entre elas algumas famosas e conhecidas na história da Matemática, como o Último Teorema de Fermat. Buscamos também apresentar possíveis abordagens de Equações Diofantinas na Educação Básica através de uma sequência didática.

Palavras-chave: Equações Diofantinas; Soma de quadrados; Último Teorema de Fermat.

Abstract

This paper is a brief study and research on some Diophantine Equations. These equations are known by such a name in honor of the Diophantus of Alexandria, known for his contributions to Algebra and Number Theory and for his principal work, the book Arithmetic. Diophantine equations are polynomial equations that allow two or more variables to assume only integer values and can come in many different forms, and therefore most of them must be analyzed individually to determine whether or not they have a solution. We seek to present some Diophantine Equations, including some famous and well-known in the history of mathematics, such as Fermat's Last Theorem. We also seek to present possible approaches to Diophantine Equations in Basic Education through a didactic sequence.

Keywords: Diophantine Equations; Sum of squares; Fermat's Last Theorem.

Sumário

Lista de Figuras

INTRODUÇÃO

As Equações Diofantinas, nome dado em homenagem a Diofanto de Alexandria, tratam-se de equações polinomiais que permitem a duas ou mais variáveis assumirem apenas valores inteiros.

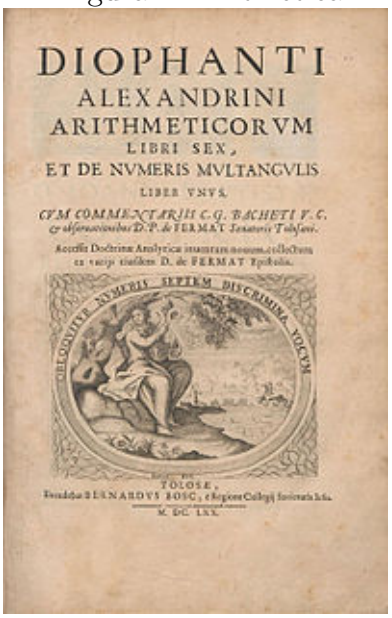
De acordo com (O'CONNOR; ROBERTSON, 1999) pouco se sabe sobre a vida de Diofanto de Alexandria, matemático grego, mas considerando seus escritos e algumas citações de seu nome, acredita-se que tenha vivido entre 200 a 284.

> Os maiores detalhes que temos da vida de Diofanto (e estes podem ser totalmente fictícios) vêm da Antologia Grega, compilada por Metrodorus por volta de 500 dC. Esta coleção de quebra-cabeças contém um sobre Diofanto que diz: "... sua infância durou $\frac{1}{6}$ de sua vida; casou-se depois de mais $\frac{1}{7}$; sua barba cresceu depois de $\frac{1}{12}$, e seu filho nasceu 5 anos depois; o filho viveu a metade da idade do pai e o pai morreu quatro anos depois do filho."(tradução nossa) ((O'CONNOR; ROBERTSON, 1999))

Com estas informações, e considerando x como a idade de morte de Diofanto, podemos escrever e resolver a equação $\frac{1}{6}x + \frac{1}{7}x + \frac{1}{12}x + 5 + \frac{x}{2} + 4 = x$ concluindo assim que ele se casou aos 26 anos e teve um filho que morreu aos 42 anos de idade, quatro anos antes do próprio Diofanto morrer aos 84 anos.

Diofanto é conhecido principalmente por suas contribuições na Álgebra e na Teoria dos Números. Seu principal trabalho, e mais conhecido é o livro Aritmética, que se trata de uma coleção de 130 problemas que fornecem soluções numéricas de equações determinadas e equações indeterminadas.

Figura 1: Aritmética



O trabalho de Diofanto trata a solução de muitos problemas relativos a equações lineares e quadráticas, mas considera apenas soluções racionais positivas para esses problemas. Equações que levariam a soluções que são raízes quadradas negativas ou irracionais, Diofanto considerava inúteis. No entanto, o fato de ele estar sempre satisfeito com uma solução racional e não exigir um número inteiro indica sofisticação na matemática trabalhada por ele na época.

Diofanto analisou três tipos de equações quadráticas $ax^2 + bx = c$, $ax^2 = bx + c$ e $ax^2 + c = bx$. A razão pela qual houve três casos para Diofanto, enquanto hoje temos apenas um caso, é que ele não tinha noção de zero e evitou coeficientes negativos considerando os números dados a, b, c sempre positivos em cada um dos três casos.

Existem, no entanto, muitos outros tipos de problemas considerados por Diofanto. Ele resolveu problemas como pares de equações quadráticas simultâneas. No Livro III, Diofanto resolve problemas de encontrar valores que fazem duas expressões lineares serem quadrados simultaneamente, dentre outros problemas.

Diofanto também parecia saber que cada número pode ser escrito como a soma de quatro quadrados. Se, de fato, ele soubesse esse resultado, seria realmente notável, pois Fermat, que declarou o resultado, não forneceu uma prova disso e não foi resolvido por muitos anos.

As Equações Diofantinas podem apresentar várias formas diferentes, com número de incógnitas diferentes, e portanto em sua maioria devem ser analisadas de forma indi-

vidual, quanto ao fato de possuírem ou não solução, e o número de soluções possíveis, quando possíveis. As Equações Diofantinas podem também ser classificadas em Lineares e Não Lineares.

As Equações Diofantinas Lineares tratam-se da soma de monômios de grau zero ou um, resultando em um número inteiro. Veremos que é possível analisar algumas condições para verificar quando uma equação deste tipo possui ou não soluções inteiras e até mesmo expressarmos uma solução geral. Estudaremos os casos de Equações Diofantinas Lineares com duas, três e n incógnitas.

Já as Equações Diofantinas Não Lineares tratam-se da soma de monômios de grau maior que um, por exemplo, quando um número inteiro é soma de quadrados, ou cubos, e devem ser analisadas caso a caso.

Trataremos então de Equações Diofantinas Não Lineares trabalhando com a soma de quadrados, o Último Teorema de Fermat e encontraremos todas as soluções da equação $p^3 + q^2 = z^3$ quando p é um número primo e $q > 1$.

Assim, buscamos pesquisar e analisar algumas Equações Diofantinas, com o intuito de destacar a importância e a grande contribuição de tais teorias e problemas para a Matemática e suas aplicações no mundo atual, dando ênfase principalmente às grandes contribuições de alguns matemáticos que participaram de maneira significativa no desenvolvimento e estudo deste tipo de equação.

Com base no trabalho já desenvolvido por alguns matemáticos, buscamos resolver e analisar de maneira detalhada alguns problemas envolvendo Equações Diofantinas, destacando alguns resultados importantes.

Baseado no que é indicado nos documentos que orientam a Educação Básica, destacamos também algumas possibilidades para se trabalhar Equações Diofantinas em sala de aula.

No atual cenário educacional, busca-se mais que o simples acúmulo de conteúdos, mas que o aluno também atue significativamente, e saiba raciocinar, relacionar e construir através dos conhecimentos prévios adquiridos. Os conteúdos estudados não devem ser um fim, e sim um meio para o desenvolvimento pessoal e social.

A Base Nacional Curricular Comum (BRASIL, 2018) traz como algumas das competências gerais da Educação básica:

1. Valorizar e utilizar os conhecimentos historicamente construídos sobre o mundo físico, social, cultural e digital para entender e explicar a realidade, continuar aprendendo e colaborar para a construção de uma sociedade justa, democrática e inclusiva.

2. Exercitar a curiosidade intelectual e recorrer à abordagem própria das ciências, incluindo a investigação, a reflexão, a análise crítica, a imaginação e a criatividade, para investigar causas, elaborar e testar hipóteses, formular e resolver problemas e criar soluções (inclusive tecnológicas) com base nos conhecimentos das diferentes áreas.

Assim, após estudo de diversas Equações Diofantinas, enxergamos grandes possibilidades de se trabalhar tal assunto como uma ferramenta interessante para ensino na Educação Básica, podendo ser trabalhada tanto nos anos finais do Ensino Fundamental, quanto no Ensino Médio, com as devidas adaptações.

As Equações Diofantinas podem integrar e viabilizar o estudo de equações de primeiro e segundo grau, estudo de sistemas de equações, o Teorema de Pitágoras, dentre outras várias possibilidades.

Assim, após o estudo mais aprofundado dos problemas envolvendo Equações Diofantinas, foi produzida uma Sequência Didática a ser trabalhada na Educação Básica, como uma das possibilidades existentes de se abordar o tema e contribuir de maneira significativa na aprendizagem.

1 EQUAÇÕES DIOFANTINAS LINEARES

Para o estudo das Equações Diofantinas Lineares nos baseamos inicialmente no que é apresentado por Abramo Hefez no livro Aritmética da Coleção PROFMAT, onde trata de aplicações do máximo divisor comum, introduzindo o método utilizado para resolver equações com duas incógnitas, fornecendo uma solução geral através de uma solução particular.

Para o estudo deste tipo de equação nos casos com três e n incógnitas, utilizamos um método para redução do número de incógnitas, conforme apresentado por Romario Sidrone de Souza em sua tese de mestrado, "Equações diofantinas lineares, quadráticas e aplicações". Através da redução do número de incógnitas é possível chegarmos a resolução de uma equação com apenas duas incógnitas.

Uma Equação Diofantina Linear é uma equação entre somas de monômios de grau zero ou um. Ou seja,

$$a_1x_1 + a_2x_2 + ... + a_nx_n = c \tag{1.1}$$

com $a_1, a_2, ..., a_n, x_1, x_2, ..., x_n, c \in \mathbb{Z}$.

1.1 Equações Diofantinas Lineares com duas incógnitas

As Equações Diofantinas Lineares com duas incógnitas são do tipo

$$ax + by = c \tag{1.2}$$

com soluções inteiras, e $a, b, c, x, y \in \mathbb{Z}$.

Nem sempre este tipo de equação possui solução, mas é possível determinarmos quando possui, e encontrá-las, como vamos mostrar, baseado em (HEFEZ, 2016).

Proposição 1.1. *Sejam $a, b \in \mathbb{Z} \setminus \{0\}$ e $c \in \mathbb{Z}$. A equação $ax + by = c$ admite solução em números inteiros se, e somente se, $mdc(a, b)|c$.*

Demonstração. Sejam $a, b \in \mathbb{Z}$. De acordo com as propriedades de Máximo Divisor Comum definimos o conjunto

$$I(a, b) = \{na + mb; n, m \in \mathbb{Z}\}$$

e se $d = min\ I(a, b) \cap \mathbb{N}$, então $d = mdc(a, b)$ e $mdc(a, b)\mathbb{Z} = \{l.d; l \in \mathbb{Z}\}$.

Assim temos que

$$I(a, b) = \{na + mb; n, m \in \mathbb{Z}\} = mdc(a, b)\mathbb{Z}$$

.

É claro que a equação $ax + by = c$ possui solução se, e somente se, $c \in I(a, b)$, o que é equivalente a $c \in mdc(a, b)\mathbb{Z}$, que, por sua vez, é equivalente a $mdc(a, b)|c$.

Portanto, temos que uma Equação Diofantina Linear com duas incógnitas possui solução se, e somente se o Máximo Divisor Comum entre a, b divide c. □

É imediato verificar que a equação $ax + by = c$ é equivalente à equação $a_1x + b_1y = c_1$, onde

$$a_1 = \frac{a}{mdc(a, b)}, b_1 = \frac{b}{mdc(a, b)} \text{ e } c_1 = \frac{c}{mdc(a, b)}$$

Note que $mdc(a_1, b_1) = 1$ e, portanto, podemos nos restringir às equações do tipo $aX + bY = c$, com $mdc(a, b) = 1$, que sempre têm soluções.

Podemos também determinar as soluções de uma equação deste tipo a partir de uma solução particular x_0, y_0, como mostraremos a seguir.

Proposição 1.2. *Seja x_0, y_0 uma solução da equação $ax + by = c$, onde $mdc(a, b) = 1$. Então, as soluções x, y em $\mathbb{Z}$ da equação são $x = x_0 + tb, y = y_0 - ta$ com $t \in \mathbb{Z}$:*

Demonstração. Seja x, y uma solução de $ax + by = c$, com $c \in \mathbb{Z}$, logo,

$$ax_0 + by_0 = ax + by = c$$

.

Consequentemente,

$$a(x - x_0) = b(y_0 - y) \tag{1.3}$$

Como $mdc(a, b) = 1$, segue-se que $b|(x - x_0)$. Logo, $x - x_0 = tb, t \in \mathbb{Z}$.

Substituindo a expressão de $x - x_0$ acima em (1.3), segue-se que

$$a(x - x_0) = b(y_0 - y)$$

$$atb = b(y_0 - y)$$

$$y_0 - y = ta$$

o que prova que as soluções são do tipo $x = x_0 + tb, y = y_0 - ta; t \in \mathbb{Z}$.

Por outro lado, x, y, como no enunciado, é solução, pois

$$ax + by = a(x_0 + tb) + b(y_0 - ta) = ax_0 + by_0 = c$$

□

Então, pela Proposição 1.2 temos que a equação diofantina $ax + by = c$, com $mdc(a, b) = 1$, admite infinitas soluções em $\mathbb{Z}$.

Veremos agora um método que permite encontrar uma solução particular para uma equação do tipo $ax + by = c$, quando $mdc(a, b) = 1$.

Usando o algoritmo euclidiano estendido, é possível determinar $n, m \in \mathbb{Z}$ tais que

$$na + mb = mdc(a, b) = 1$$

Multiplicando ambos os membros da igualdade acima por c, obtemos

$$c = cna + cmb$$

Logo, $x_0 = cn$ e $y_0 = cm$ é uma solução particular da equação.

Exemplo 1.3. Encontre as soluções da equação $24x + 14y = 18$.

A equação tem solução, pois $mdc(24, 14)|18$. Dividindo ambos os membros da equação por $2 = mdc(24, 14)$, obtemos a equação equivalente $12x + 7y = 9$.

Vamos, em seguida, achar uma solução particular x_0, y_0 desta última equação.

Pelo algoritmo euclidiano, temos

$12 = 7 \cdot 1 + 5$

$7 = 5 \cdot 1 + 2$

$5 = 2 \cdot 2 + 1$

Substituindo as equações acima umas nas outras, obtemos

$$1 = 12 \cdot (3) - 7 \cdot (5)$$

portanto, multiplicando os dois lados da igualdade por 9, temos

$$9 = 12 \cdot (27) + 7 \cdot (-45)$$

Logo, $x_0 = 27$ e $y_0 = -45$ é solução particular da equação e, consequentemente,as soluções são $x = 27 + 7t, y = -45 - 12t; t \in \mathbb{Z}$.

O problema seguinte apareceu no Exame Nacional de Desempenho Acadêmico [ENADE] de 2014 e mostra uma aplicação prática de uma Equação Diofantina de duas variáveis.

Exemplo 1.4. Considere que os ingressos de um cinema custam $R\$9,00$ para estudantes e $R\$15,00$ para o público geral, e que, em certo dia, durante determinado período, a arrecadação nas bilheterias desse cinema foi de $R\$246,00$. Quantas e quais são as possíveis soluções?

Estamos procurando então as possíveis soluções para a equação

$$9x + 15y = 246$$

Esta equação possui solução, pois $mdc(9, 15)|246$. Dividindo ambos os lados da equação por $3 = mdc(9, 15)$, obtemos a equação equivalente $3x + 5y = 82$

Vamos então encontrar a solução particular da última equação. Pelo algoritmo euclidiano temos:

$5 = 3 \cdot 1 + 2$

$3 = 2 \cdot 1 + 1$

Assim substituindo as equações acima umas nas outras obtemos

$$1 = 3 \cdot (2) + 5 \cdot (-1)$$

Portanto, multiplicando os dois lados da equação por 82, temos

$$3 \cdot (164) + 5 \cdot (-82) = 82$$

Logo, $x_0 = 164$ e $y_0 = -82$ é uma solução particular da equação, e portanto as soluções são $x = 164 + 5t$ e $y = -82 - 3t$.

Porém, temos que as soluções não podem ser negativas, pois se tratam de número de pessoas. Assim devemos ter

$$x = 164 + 5t \geq 0$$

$$5t \geq -164$$

$$t \geq -32,8 \Rightarrow t \geq -32$$

e

$$y = -82 - 3t \geq 0$$

$$-82 \geq 3t$$

$$-27,33... \geq t \Rightarrow t \leq -28$$

Ou seja, $-32 \leq t \leq -28$, portanto temos 5 pares de soluções possíveis:

$$t = -32 \Rightarrow x = 4, y = 14$$

$$t = -31 \Rightarrow x = 9, y = 11$$

$$t = -30 \Rightarrow x = 14, y = 8$$

$$t = -29 \Rightarrow x = 19, y = 5$$

$$t = -28 \Rightarrow x = 24, y = 2$$

1.2 Equações Diofantinas Lineares com três incógnitas

As Equações Diofantinas Lineares com três incógnitas são do tipo

$$a_1x + a_2y + a_3z = c \tag{1.4}$$

com soluções inteiras, e $a_1, a_2, a_3, c, x, y, z \in \mathbb{Z}$.

Para resolvermos equações do tipo (1.4) vamos proceder de forma parecida com o que foi realizado com as equações do tipo (1.2), como explicitado por (SOUZA, 2017).

Definição 1.5. Sejam a_1, a_2 e a_3 inteiros e $d = mdc(a_1, a_2, a_3)$. O número d é dado por $d = mdc(d_1, a_3)$, onde $d_1 = mdc(a_1, a_2)$.

Se $d_1 = mdc(a_1, a_2)$, com $d_1 \in \mathbb{Z}$, então existem $k_1, k_2 \in \mathbb{Z}$ para os quais $a_1k_1 + a_2k_2 = d_1$. Como $d = mdc(d_1, a_3)$, então existem $k, z_0 \in \mathbb{Z}$ tal que $d_1k + a_3z_0 = d$.

Assim,

$$d = (a_1k_1 + a_2k_2)k + a_3z_0$$

$$d = a_1(k_1k) + a_2(k_2k) + a_3z_0$$

Tomando $k_1k = x_0$ e $k_2k = y_0$, teremos

$$d = a_1x_0 + a_2y_0 + a_3z_0. \tag{1.5}$$

Daí, se $d|c$, existe um número inteiro q, tal que $c = dq$. Agora, multiplicando a equação (1.5) por q, obtemos

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

Logo, $(x_0q,\ y_0q,\ z_0q)$ é uma das soluções particulares da equação (1.4).

Proposição 1.6. *A equação $a_1x + a_2y + a_3z = c$ em que $a_1 \neq 0$, $a_2 \neq 0$, $a_3 \neq 0$ e $c \in \mathbb{Z}$ admite solução, se e somente se, $mdc(a_1, a_2, a_3) = d$ divide c.*

Nosso objetivo, a partir de agora, é encontrar uma solução geral da equação (1.4).

Para se obter a solução geral como desejado, devemos inicialmente reduzir essa equação para duas variáveis, pois a Equação Diofantina Linear com Duas incógnitas já

sabemos como encontrar as soluções. Considerando, $a_1x + a_2y = k$, temos

$$k + a_3z = c \tag{1.6}$$

e evidentemente a equação (1.6) possui solução, pois $d_1 = mdc(1, a_3) = 1$ e $1|c$.

Dessa forma, de acordo com o que vimos com equações de duas variáveis, a solução geral da equação (1.6) é dada por $k = k_0 + \frac{a_3}{d_1}t_1$ e $z = z_0 - \frac{1}{d_1}t_1,\ t_1 \in \mathbb{Z}$.

Como $d_1 = mdc(1, a_3) = 1$, segue que, $k = k_0 + a_3t_1$ e $z = z_0 - t_1$. Vejamos agora que $a_1x + a_2y = k = k_0 + a_3t_1$, sendo assim, devemos escolher um valor conveniente para t_1, que satisfaça $d_2 = mdc(a_1, a_2)|(k_0 + a_3t_1)$.

Assim temos que a equação $a_1x + a_2y = k$, pelo que sabemos de equações com duas variáveis, terá como solução $x = x_0 + \frac{a_2}{d_2}t_2$ e $y = y_0 - \frac{a_1}{d_2}t_2,\ t_2 \in \mathbb{Z}$.

Assim, podemos concluir que o conjunto solução da equação $a_1x + a_2y + a_3z = c$ é

$$S = \left\{ \left(x_0 + \frac{a_2}{d_2}t_2, y_0 - \frac{a_1}{d_2}t_2, z_0 - t_1 \right),\ \text{com } t_1, t_2 \in \mathbb{Z},\ e\ mdc(a_1, a_2)|(k_0 + a_3t_1) \right\}$$

Exemplo 1.7. Encontre as soluções da equação $8x + 12y + 6z = 2$.

Nesta equação temos $a_1 = 8, a_2 = 12$ e $a_3 = 6$. Temos que $mdc(8, 12, 6) = 2$ e $2|2$. Portanto, a equação dada admite solução.

A equação $8x + 12y + 6z = 2$ equivale a equação $4x + 6y + 3z = 1$ Como $d_1 = mdc(4, 6) = 2$, então existem $k_1, k_2 \in \mathbb{Z}$ tal que

$$4 \cdot k_1 + 6 \cdot k_2 = 2 \tag{1.7}$$

Através do algoritmo euclidiano obtemos

$$6 = 4 \cdot 1 + 2$$

$$4 = 2 \cdot 2$$

Substituindo uma equação na outra chegamos que

$$4 \cdot (-1) + 6 \cdot (1) = 2 \tag{1.8}$$

, portanto $k_1 = -1$ e $k_2 = 1$

Como $d = mdc(2, 3) = 1$, então existem $k, z_0 \in \mathbb{Z}$ tal que

$$2 \cdot k + 3 \cdot z_0 = 1 \tag{1.9}$$

Novamente, através do algoritmo euclidiano

$$3 = 2 \cdot 1 + 1$$

Então $2 \cdot (-1) + 3 \cdot (1) = 1$, portanto $k = -1$ e $z_0 = 1$

Substituindo (1.7) em (1.9), obtemos

$$(4 \cdot k_1 + 6 \cdot k_2)k + 3 \cdot z_0 = 2$$

$$4(k_1 k) + 6(k_2 k) + 3z_0 = 2$$

Assim obtemos uma solução particular

$x_0 = k_1 k = (-1) \cdot (-1) = 1$,

$y_0 = k_2 k = 1 \cdot (-1) = -1$ e

$z_0 = 1$

Para encontrar a solução geral, inicialmente vamos considerar a equação $4x + 6y = k$, e assim obtemos uma nova equação com apenas duas incógnitas:

$$k + 3z = 1 \tag{1.10}$$

Pelo algoritmo euclidiano temos $3 = 2 \cdot 1 + 1 \Rightarrow 1 \cdot (-2) + 3 \cdot 1 = 1$, o que nos dá $k_0 = -2, z_0 = 1$, portanto a solução geral é dada por $k = -2 + 3t_1$ e $z = 1 - t_1$.

Sendo assim, devemos escolher um valor conveniente para t_1, tal que $mdc(4, 6) = 2|(-2 + 3t_1)$. Observemos que $2|2$ e $2 \nmid 3$, então $t_1 = 2 \cdot l, l \in \mathbb{Z}$.

Note que $k = -2 + 3t_1 = -2 + 3 \cdot 2l = 2(-1 + 3l)$.

Pela equação (1.8), temos que $4 \cdot (-1) + 6 \cdot 1 = 2$, multiplicando os dois lados por $-1 + 3l$ temos

$$4 \cdot (-1) \cdot (-1 + 3l) + 6 \cdot (-1 + 3l) = 2 \cdot (-1 + 3l)$$

$$4 \cdot (1 - 3l) + 6 \cdot (-1 + 3l) = -2 + 3t_1 = k$$

Logo, temos $x_0 = 1 - 3l$ e $y_0 = -1 + 3l, l \in \mathbb{Z}$ e a solução geral então é dada por

$$\begin{aligned} x &= 1 - 3l + 6t_2 \\ y &= -1 + 3l - 4t_2 \qquad , l, t_1, t_2 \in \mathbb{Z}, t_1 = 2l \\ z &= 1 - t_1 \end{aligned}$$

Exemplo 1.8. O senhor José deseja pagar uma conta no supermercado no valor de $R\$237,00$, usando tickets no valor de $R\$3,00$, $R\$5,00$ e $R\$7,00$. Quantos tickets de cada valor João deverá usar?

Para resolver este problema, devemos encontrar ternas de inteiros (x, y, z) que sejam soluções da equação

$$3x + 5y + 7z = 237 \tag{1.11}$$

Como $d = 1$ e $1|237$, a equação (1.11) tem solução. Temos $a_1 = 3, a_2 = 5$ e $a_3 = 7$. Como $d_1 = mdc(3, 5) = 1$, então existem $k_1, k_2 \in \mathbb{Z}$ tal que

$$3 \cdot k_1 + 5 \cdot k_2 = 1 \tag{1.12}$$

Através do algoritmo euclidiano obtemos

$$5 = 3 \cdot 1 + 2$$

$$3 = 2 \cdot 1 + 1$$

Substituindo uma equação na outra chegamos que

$$3 \cdot (2) + 5 \cdot (-1) = 1 \tag{1.13}$$

portanto $k_1 = 2$ e $k_2 = -1$

Como $d = mdc(1, 7) = 1$, então existem $k, z_0 \in \mathbb{Z}$ tal que

$$1 \cdot k + 7 \cdot z_0 = 1 \tag{1.14}$$

Novamente, através do algoritmo euclidiano

$$7 = 6 \cdot 1 + 1$$

Então $1 \cdot (-6) + 7 \cdot (1) = 1$, portanto $k = -6$ e $z_0 = 1$

Substituindo (1.13) em (1.14), obtemos

$$(3 \cdot k_1 + 5 \cdot k_2)k + 7 \cdot z_0 = 1$$

$$3(k_1 k)237 + 5(k_2 k)237 + 7z_0 237 = 237$$

Assim obtemos uma solução particular

$x_0 = 237k_1 k = 237 \cdot (2) \cdot (-6) = -2844$,

$y_0 = 237k_2 k = 237 \cdot (-1) \cdot (-6) = 1422$ e

$z_0 = 237$

Para encontrar a solução geral, inicialmente vamos considerar a equação $3x + 5y = k$, e assim obtemos uma nova equação com apenas duas incógnitas:

$$k + 7z = 237 \tag{1.15}$$

Pelo algoritmo euclidiano temos $7 = 6 \cdot 1 + 1 \Rightarrow 1 \cdot (-6) + 7 \cdot 1 = 1 \Rightarrow 1 \cdot (-1422) + 7 \cdot 237 = 237$, o que nos dá $k_0 = -1422, z_0 = 237$, portanto a solução geral é dada por $k = -1422 + 7t_1$ e $z = 237 - t_1, t_1 \in \mathbb{Z}$.

Sendo assim, devemos escolher um valor conveniente para t_1, tal que $mdc(3, 5) = 1 | (-1422 + 7t_1)$, então t_1 pode assumir qualquer valor inteiro.

Pela equação (1.13), temos que $3 \cdot (2) + 5 \cdot (-1) = 1$, multiplicando os dois lados por $-1422 + 7t_1$ temos

$$3 \cdot (2) \cdot (-1422 + 7t_1) + 5 \cdot (-1) \cdot (-1422 + 7t_1) = (-1422 + 7t_1)$$

Logo, temos $x_0 = -2844 + 14t_1$ e $y_0 = 1422 - 7t_1, t_1 \in \mathbb{Z}$ e a solução geral então é dada por

$$\begin{aligned} x &= -2844 + 14t_1 + 5t_2 \\ y &= 1422 - 7t_1 - 3t_2 \qquad\quad , t_1, t_2 \in \mathbb{Z} \\ z &= 237 - t_1 \end{aligned}$$

Como estamos lidando com quantidade de tickets, temos que $x, y, z \geq 0$, daí se

$$z \geq 0 \Rightarrow 237 - t_1 \geq 0 \Rightarrow t_1 \leq 237$$

Além disso, temos que $z \leq 33$, pois caso contrário x ou y teriam que assumir valores negativos. Então

$$z \leq 33 \Rightarrow 237 - t_1 \leq 33 \Rightarrow t_1 \geq 204$$

Temos então 33 possíveis valores para z, sendo $204 \leq z \leq 237$. Como uma das possibilidades, vamos considerar $t_1 = 204$.

Temos então:

$$x \geq 0 \Rightarrow -2844 + 14 \cdot 204 + 5t_2 \geq 0 \Rightarrow t_2 \geq -2,4$$

$$y \geq 0 \Rightarrow 1422 - 7 \cdot 204 - 3t_2 \geq 0 \Rightarrow t_2 \leq -2$$

Então, quando tomamos $t_1 = 204$, $-2,4 \leq t_2 \leq -2$, temos então $t_2 = -2$, o que nos dá

$$x = 2$$

$$y = 0$$

$$z = 33$$

uma das soluções.

Variando t_1 e t_2 de acordo com as condições, obtemos 284 soluções possíveis, as quais são enumeradas abaixo:

- $t_1 = 204$

$x = 2; y = 0; z = 33$

- $t_1 = 205$

$x = 1; y = 2; z = 32$

- $t_1 = 206$

$x = 0; y = 4; z = 31$ $x = 5; y = 1; z = 31$

- $t_1 = 207$

$x = 4; y = 3; z = 30$ $x = 9; y = 0; z = 30$

- $t_1 = 208$

$x = 3; y = 5; z = 29$ $x = 8; y = 2; z = 29$

- $t_1 = 209$

$x = 2; y = 7; z = 28$ $x = 12; y = 1; z = 28$

$x = 7; y = 4; z = 28$

- $t_1 = 210$

$x = 1; y = 9; z = 27$ $x = 11; y = 3; z = 27$

$x = 6; y = 6; z = 27$ $x = 16; y = 0; z = 27$

- $t_1 = 211$

$x = 0; y = 11; z = 26$ $x = 10; y = 5; z = 26$

$x = 5; y = 8; z = 26$ $x = 15; y = 2; z = 26$

- $t_1 = 212$

$x = 4; y = 10; z = 25$ $x = 14; y = 4; z = 25$

$x = 9; y = 7; z = 25$ $x = 19; y = 1; z = 25$

- $t_1 = 213$

$x = 3; y = 12; z = 24$ $x = 18; y = 3; z = 24$

$x = 8; y = 9; z = 24$ $x = 23; y = 0; z = 24$

$x = 13; y = 6; z = 24$

- $t_1 = 214$

$x = 2; y = 14; z = 23$ $x = 17; y = 5; z = 23$

$x = 7; y = 11; z = 23$ $x = 22; y = 2; z = 23$

$x = 12; y = 8; z = 23$

- $t_1 = 215$

$x = 1; y = 16; z = 22$ $x = 16; y = 7; z = 22$

$x = 6; y = 13; z = 22$ $x = 21; y = 4; z = 22$

$x = 11; y = 10; z = 22$ $x = 26; y = 1; z = 22$

- $t_1 = 216$

$x = 0; y = 18; z = 21$ $x = 15; y = 9; z = 21$

$x = 5; y = 15; z = 21$ $x = 20; y = 6; z = 21$

$x = 10; y = 12; z = 21$ $x = 25; y = 3; z = 21$

$$x = 30; y = 0; z = 21$$

- $t_1 = 217$

$$x = 4; y = 17; z = 20 \qquad x = 19; y = 8; z = 20$$

$$x = 9; y = 14; z = 20 \qquad x = 24; y = 5; z = 20$$

$$x = 14; y = 11; z = 20 \qquad x = 29; y = 2; z = 20$$

- $t_1 = 218$

$$x = 3; y = 19; z = 19 \qquad x = 23; y = 7; z = 19$$

$$x = 8; y = 16; z = 19 \qquad x = 28; y = 4; z = 19$$

$$x = 13; y = 13; z = 19 \qquad x = 33; y = 1; z = 19$$

$$x = 18; y = 10; z = 19$$

- $t_1 = 219$

$$x = 2; y = 21; z = 18 \qquad x = 22; y = 9; z = 18$$

$$x = 7; y = 18; z = 18 \qquad x = 27; y = 6; z = 18$$

$$x = 12; y = 15; z = 18 \qquad x = 32; y = 3; z = 18$$

$$x = 17; y = 12; z = 18 \qquad x = 37; y = 0; z = 18$$

- $t_1 = 220$

$$x = 1; y = 23; z = 17 \qquad x = 11; y = 17; z = 17$$

$$x = 6; y = 20; z = 17 \qquad x = 16; y = 14; z = 17$$

$x = 21; y = 11; z = 17$ $x = 31; y = 5; z = 17$

$x = 26; y = 8; z = 17$ $x = 36; y = 2; z = 17$

- $t_1 = 221$

$x = 0; y = 25; z = 16$ $x = 25; y = 10; z = 16$

$x = 5; y = 22; z = 16$ $x = 30; y = 7; z = 16$

$x = 10; y = 19; z = 16$ $x = 35; y = 4; z = 16$

$x = 15; y = 16; z = 16$

$x = 20; y = 13; z = 16$ $x = 40; y = 1; z = 16$

- $t_1 = 222$

$x = 4; y = 24; z = 15$ $x = 29; y = 9; z = 15$

$x = 9; y = 21; z = 15$ $x = 34; y = 6; z = 15$

$x = 14; y = 18; z = 15$ $x = 39; y = 3; z = 15$

$x = 19; y = 15; z = 15$

$x = 24; y = 12; z = 15$ $x = 44; y = 0; z = 15$

- $t_1 = 223$

$x = 3; y = 26; z = 14$ $x = 18; y = 17; z = 14$

$x = 8; y = 23; z = 14$ $x = 23; y = 14; z = 14$

$x = 13; y = 20; z = 14$ $x = 28; y = 11; z = 14$

$x = 33; y = 8; z = 14$ $x = 43; y = 2; z = 14$

$x = 38; y = 5; z = 14$

- $t_1 = 224$

$x = 2; y = 28; z = 13$ $x = 27; y = 13; z = 13$

$x = 7; y = 25; z = 13$ $x = 32; y = 10; z = 13$

$x = 12; y = 22; z = 13$ $x = 37; y = 7; z = 13$

$x = 17; y = 19; z = 13$ $x = 42; y = 4; z = 13$

$x = 22; y = 16; z = 13$ $x = 47; y = 1; z = 13$

- $t_1 = 225$

$x = 1; y = 30; z = 12$ $x = 26; y = 15; z = 12$

$x = 6; y = 27; z = 12$ $x = 31; y = 12; z = 12$

$x = 11; y = 24; z = 12$ $x = 36; y = 9; z = 12$

$x = 16; y = 21; z = 12$ $x = 41; y = 6; z = 12$

$x = 21; y = 18; z = 12$ $x = 46; y = 3; z = 12$

- $t_1 = 226$

$x = 0; y = 32; z = 11$ $x = 15; y = 23; z = 11$

$x = 5; y = 29; z = 11$ $x = 20; y = 20; z = 11$

$x = 10; y = 26; z = 11$ $x = 25; y = 17; z = 11$

$x = 30; y = 14; z = 11$

$x = 35; y = 11; z = 11$

$x = 40; y = 8; z = 11$

$x = 45; y = 5; z = 11$

$x = 50; y = 2; z = 11$

- $t_1 = 227$

$x = 4; y = 31; z = 10$

$x = 9; y = 28; z = 10$

$x = 14; y = 25; z = 10$

$x = 19; y = 22; z = 10$

$x = 24; y = 19; z = 10$

$x = 29; y = 16; z = 10$

$x = 34; y = 13; z = 10$

$x = 39; y = 10; z = 10$

$x = 44; y = 7; z = 10$

$x = 49; y = 4; z = 10$

$x = 54; y = 1; z = 10$

- $t_1 = 228$

$x = 3; y = 33; z = 9$

$x = 8; y = 30; z = 9$

$x = 13; y = 27; z = 9$

$x = 18; y = 24; z = 9$

$x = 23; y = 21; z = 9$

$x = 28; y = 18; z = 9$

$x = 33; y = 15; z = 9$

$x = 38; y = 12; z = 9$

$x = 43; y = 9; z = 9$

$x = 48; y = 6; z = 9$

$x = 53; y = 3; z = 9$

$x = 58; y = 0; z = 9$

- $t_1 = 229$

$x = 2; y = 35; z = 8$

$x = 7; y = 32; z = 8$

$x = 12; y = 29; z = 8$

$x = 17; y = 26; z = 8$

$x = 22; y = 23; z = 8$

$x = 27; y = 20; z = 8$

$x = 32; y = 17; z = 8$

$x = 37; y = 14; z = 8$

$x = 42; y = 11; z = 8$

$x = 47; y = 8; z = 8$

$x = 52; y = 5; z = 8$

$x = 57; y = 2; z = 8$

- $t_1 = 230$

$x = 1; y = 37; z = 7$

$x = 6; y = 34; z = 7$

$x = 11; y = 31; z = 7$

$x = 16; y = 28; z = 7$

$x = 21; y = 25; z = 7$

$x = 26; y = 22; z = 7$

$x = 31; y = 19; z = 7$

$x = 36; y = 16; z = 7$

$x = 41; y = 13; z = 7$

$x = 46; y = 10; z = 7$

$x = 51; y = 7; z = 7$

$x = 56; y = 4; z = 7$

$x = 61; y = 1; z = 7$

- $t_1 = 231$

$x = 0; y = 39; z = 6$

$x = 5; y = 36; z = 6$

$x = 10; y = 33; z = 6$

$x = 15; y = 30; z = 6$

$x = 20; y = 27; z = 6$

$x = 25; y = 24; z = 6$

$x = 30; y = 21; z = 6$

$x = 35; y = 18; z = 6$

$x = 40; y = 15; z = 6$

$x = 45; y = 12; z = 6$

$x = 4; y = 38; z = 5$

$x = 9; y = 35; z = 5$

$x = 14; y = 32; z = 5$

$x = 19; y = 29; z = 5$

$x = 24; y = 26; z = 5$

$x = 29; y = 23; z = 5$

$x = 34; y = 20; z = 5$

$x = 50; y = 9; z = 6$

$x = 55; y = 6; z = 6$

$x = 60; y = 3; z = 6$

$x = 65; y = 0; z = 6$

$x = 39; y = 17; z = 5$

$x = 44; y = 14; z = 5$

$x = 49; y = 11; z = 5$

$x = 54; y = 8; z = 5$

$x = 59; y = 5; z = 5$

$x = 64; y = 2; z = 5$

- $t_1 = 233$

$x = 3; y = 40; z = 4$

$x = 8; y = 37; z = 4$

$x = 13; y = 34; z = 4$

$x = 18; y = 31; z = 4$

$x = 23; y = 28; z = 4$

$x = 28; y = 25; z = 4$

$x = 33; y = 22; z = 4$

$x = 38; y = 19; z = 4$

$x = 43; y = 16; z = 4$

$x = 48; y = 13; z = 4$

$x = 53; y = 10; z = 4$

$x = 58; y = 7; z = 4$

$x = 63; y = 4; z = 4$ $x = 68; y = 1; z = 4$

- $t_1 = 234$

$x = 2; y = 42; z = 3$ $x = 42; y = 18; z = 3$

$x = 7; y = 39; z = 3$ $x = 47; y = 15; z = 3$

$x = 12; y = 36; z = 3$ $x = 52; y = 12; z = 3$

$x = 17; y = 33; z = 3$ $x = 57; y = 9; z = 3$

$x = 22; y = 30; z = 3$ $x = 62; y = 6; z = 3$

$x = 27; y = 27; z = 3$ $x = 67; y = 3; z = 3$

$x = 32; y = 24; z = 3$ $x = 72; y = 0; z = 3$

$x = 37; y = 21; z = 3$

- $t_1 = 235$

$x = 1; y = 44; z = 2$ $x = 36; y = 23; z = 2$

$x = 6; y = 41; z = 2$ $x = 41; y = 20; z = 2$

$x = 11; y = 38; z = 2$ $x = 46; y = 17; z = 2$

$x = 16; y = 35; z = 2$ $x = 51; y = 14; z = 2$

$x = 21; y = 32; z = 2$ $x = 56; y = 11; z = 2$

$x = 26; y = 29; z = 2$ $x = 61; y = 8; z = 2$

$x = 31; y = 26; z = 2$ $x = 66; y = 5; z = 2$

$$x = 71; y = 2; z = 2$$

- $t_1 = 236$

$$x = 0; y = 46; z = 1 \qquad x = 40; y = 22; z = 1$$

$$x = 5; y = 43; z = 1 \qquad x = 45; y = 19; z = 1$$

$$x = 10; y = 40; z = 1 \qquad x = 50; y = 16; z = 1$$

$$x = 15; y = 37; z = 1 \qquad x = 55; y = 13; z = 1$$

$$x = 20; y = 34; z = 1 \qquad x = 60; y = 10; z = 1$$

$$x = 25; y = 31; z = 1 \qquad x = 65; y = 7; z = 1$$

$$x = 30; y = 28; z = 1 \qquad x = 70; y = 4; z = 1$$

$$x = 35; y = 25; z = 1 \qquad x = 75; y = 1; z = 1$$

- $t_1 = 237$

$$x = 79; y = 0; z = 0 \qquad x = 44; y = 21; z = 0$$

$$x = 74; y = 3; z = 0 \qquad x = 39; y = 24; z = 0$$

$$x = 69; y = 6; z = 0 \qquad x = 34; y = 27; z = 0$$

$$x = 64; y = 9; z = 0 \qquad x = 29; y = 30; z = 0$$

$$x = 59; y = 12; z = 0 \qquad x = 24; y = 33; z = 0$$

$$x = 54; y = 15; z = 0 \qquad x = 19; y = 36; z = 0$$

$$x = 49; y = 18; z = 0 \qquad x = 14; y = 39; z = 0$$

$$x = 9; y = 42; z = 0 \qquad\qquad x = 4; y = 45; z = 0$$

1.3 Equações Diofantinas Lineares com n incógnitas

As equações do tipo

$$a_1x_1 + a_2x_2 + ... + a_nx_n = c \tag{1.16}$$

com $a_i \in \mathbb{Z}$ e $i = 1, 2, ..., n \in \mathbb{N}$ são as chamadas Equações Diofantinas Lineares com n incógnitas, e a partir do que estudamos com relação a estes tipos de equações com duas e três incógnitas podemos chegar as soluções procuradas neste caso.

Ainda baseados no que é feito por (SOUZA, 2017), de forma análoga ao que foi mostrado na Proposição 1.1, podemos garantir que a equação (1.16) admite solução inteira se, e somente se, $d = mdc(a_1, a_2, ..., a_n) \in \mathbb{Z}$ e $d|c$.

De acordo com o que vimos na solução de equações com três incógnitas, podemos de forma análoga, reduzir uma equação com mais de duas incógnitas em uma que tenha duas incógnitas, resolvendo assim nosso problema inicial, a solução da equação (1.16).

2 EQUAÇÕES DIOFANTINAS NÃO LINEARES

São chamadas de Equações Diofantinas Não Lineares a soma de monômios de grau maior que um. No livro "Teoria dos números: um passeio com primos e outros números familiares pelo mundo inteiro" de (MARTINEZ et al., 2011), são encontrados alguns exemplos os quais são analisados a seguir.

2.1 Triplas ou Ternas Pitagóricas

As triplas ou Ternas Pitagóricas são assim chamadas por serem possíveis comprimentos dos lados de um triângulo retângulo de acordo com o Teorema de Pitágoras, onde a e b são catetos e c é a hipotenusa.

Tratam-se de números inteiros que satisfazem a equação:

$$a^2 + b^2 = c^2 \tag{2.1}$$

Vamos então encontrar tais ternas de acordo com o que é apresentado em (MARTINEZ et al., 2011). Dados três números inteiros, primos dois a dois (a, b, c) que satisfaçam a equação acima, chamamo-os de Tripla Pitagórica Primitiva. Para encontrarmos tais triplas, consideremos sem perda de generalidade, a ímpar, pois a e b não podem ser pares ao mesmo tempo (primos entre si).

Temos que quadrados perfeitos são congruentes a 0 ou 1 módulo 4, pois:

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

e

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

Daí, se b também é ímpar, temos:

$$a^2+b^2 = c^2 \Rightarrow (4k^2+4k+1)+(4t^2+4t+1) = c^2 \Rightarrow 4(k^2+k+t^2+t)+2 = c^2 \equiv 2 \mod 4$$

O que nos dá uma contradição com a afirmação acima. Assim temos a ímpar, b par e c ímpar. Por outro lado:

$$a^2 + b^2 = c^2 \Rightarrow b^2 = c^2 - a^2 \Rightarrow b^2 = (c-a)(c+a) \tag{2.2}$$

$mdc(a,c) = 1 \Rightarrow mdc(c, c+a) = 1$ e $c+a$ é par. Então $mdc(2c, c+a) = 2$, logo $2 = mdc(2c, c+a) = mdc(2c \cdot (c+a), c+a) = mdc(c-a, c+a)$.

Logo, $\frac{c+a}{2}$ e $\frac{c-a}{2}$ são coprimos e por (2.2) seu produto é um quadrado perfeito:

$$\left(\frac{c+a}{2}\right)\left(\frac{c-a}{2}\right) = \frac{(c+a)(c-a)}{4} = \left(\frac{b}{2}\right)^2$$

Pelo Teorema Fundamental da Aritmética cada um destes fatores deve ser o quadrado de um número natural. Digamos então:

$\left(\frac{c+a}{2}\right) = m^2$ e $\left(\frac{c-a}{2}\right) = n^2$, $(m,n) = 1$

Portanto,

$$b^2 = (c-a)(c+a) = 2n^2.2m^2 = 4m^2n^2 \Rightarrow b = 2mn$$

$$\left(\frac{c+a}{2}\right) = m^2 \Rightarrow c = 2m^2 - a$$

$$\left(\frac{c-a}{2}\right) = n^2 \Rightarrow c = 2n^2 + a$$

Daí temos

$$2m^2 - a = 2n^2 + a \Rightarrow 2m^2 - 2n^2 = 2a \Rightarrow a = m^2 - n^2$$

Substituindo a:

$$c = 2m^2 - (m^2 - n^2) \Rightarrow c = m^2 + n^2$$

com $mdc(m, n) = 1$ e $m + n$ ímpar, o que garante (a, b, c) coprimos

Exemplo 2.1. Vamos encontrar todas as triplas pitagóricas de inteiros positivos (a, b, c) tais que a^2, b^2 e c^2 estão em progressão aritmética.

Demonstração. Uma Progressão Aritmética é uma sequência numérica em que cada termo, a partir do segundo, é igual à soma do termo anterior com uma constante. Então, pela definição, a subtração de dois termos sequentes resulta na mesma constante, o que nos dá:

$$b^2 - a^2 = c^2 - b^2 \Rightarrow a^2 + c^2 = 2b^2 \tag{2.3}$$

Vamos considerar a, b, c primos entre si. Observe que a e c têm paridade igual, pois a soma resulta em um número par, mas como são primos entre si, logo os dois são ímpares e, portanto, exitem r e s tais que $c = r + s$ e $a = r - s$. Substituindo:

$$2b^2 = a^2+c^2 = (r-s)^2+(r+s)^2 = r^2-2rs+s^2+r^2+2rs+s^2 = 2(r^2+s^2) \Rightarrow r^2+s^2 = b^2$$

Logo, (r, s, b) é uma tripla pitagórica, que é primitiva, portanto existem m e n tais que $r = m^2 - n^2$, $s = 2mn$ e $b = m^2 + n^2$.

Então $a = m^2 - n^2 - 2mn$, $b = m^2 + n^2$ e $c = m^2 - n^2 + 2mn$. □

As soluções inteiras primitivas da equação $x^2 + y^2 = z^2$ formam uma bijeção com as soluções racionais da equação $x^2 + y^2 = 1$. Pois,

$$\frac{x^2}{z^2} + \frac{y^2}{z^2} = \frac{z^2}{z^2} \Rightarrow \frac{x^2}{z^2} + \frac{y^2}{z^2} = 1$$

Então

$$(x, y, z) \longmapsto \left(\frac{x}{z}, \frac{y}{z}\right)$$

Já as soluções da equação $x^2 + y^2 = 1$ podem ser obtidas através do seguinte método geométrico:

Teorema 2.2. *Os pontos racionais (x, y) da circunferência de equação $x^2 + y^2 = 1$ são todos os pontos da forma $(x, y) = (1, 0)$ e $(x, y) = \left(\frac{t^2-1}{t^2+1}, \frac{2t}{t^2+1}\right)$, com $t \in \mathbb{Q}$.*

Demonstração. Considere a reta passando pelos pontos $(1, 0)$ e $(0, t)$ com $t \in \mathbb{Q}$:

$$\begin{vmatrix} x & y & 1 \\ 1 & 0 & 1 \\ 0 & t & 1 \end{vmatrix} = 0$$

$$\Rightarrow 0 + 0 + t - (0 + y + xt) = 0$$
$$\Rightarrow t - y - xt = 0$$
$$\Rightarrow y = -t(x - 1)$$

Esta reta intercepta a circunferência $x^2 + y^2 = 1$ em:

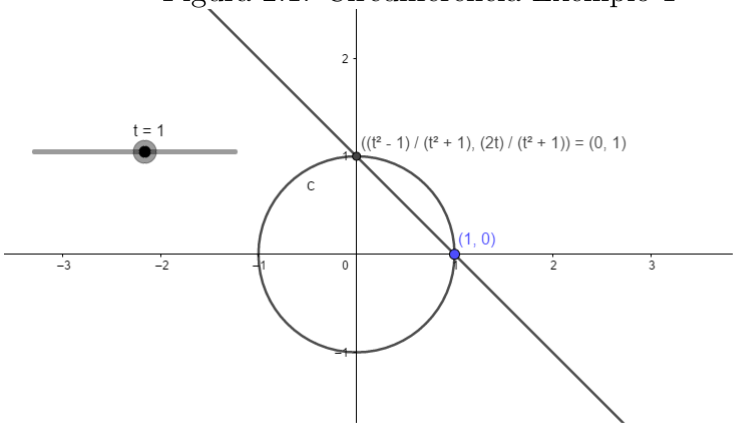
$$x^2 + [t(1 - x)]^2 = 1$$
$$t^2 = \frac{1 - x^2}{(1 - x)^2}$$
$$\frac{(1 - x)(1 + x)}{(1 - x)^2} = t^2$$
$$1 + x = t^2 - t^2x$$
$$x(1 + t^2) = t^2 - 1$$
$$x = \frac{t^2 - 1}{t^2 + 1}$$

Substituindo x em y na equação $x^2 + y^2 = 1$:

$$\left(\frac{t^2 - 1}{t^2 + 1}\right)^2 + y^2 = 1$$
$$y^2 = 1 - \left(\frac{t^4 - 2t^2 + 1}{t^4 + 2t^2 + 1}\right)$$
$$y^2 = \frac{t^4 + 2t^2 + 1 - t^4 + 2t^2 - 1}{t^4 + 2t^2 + 1}$$
$$y^2 = \frac{4t^2}{(t^2 + 1)^2}$$

$$y = \pm\frac{2t}{t^2+1}$$

Figura 2.1: Circunferência Exemplo 1



Observe que $(0,t) \longmapsto \left(\frac{t^2-1}{t^2+1}, \frac{2t}{t^2+1}\right)$ estabelece uma bijeção entre os pontos racionais do eixo y e os pontos racionais P da circunferência, menos o ponto $(1,0)$. Reciprocamente, dado um ponto racional $P \neq (1,0)$ da circunferência, temos que a reta que une P a $(1,0)$ admite uma equação com coeficientes racionais, logo intercepta o eixo y em um ponto $(0,t)$ com $t \in \mathbb{Q}$. Isto completa a demonstração. □

Agora substituindo $t = \frac{m}{n}$ com $m, n \in \mathbb{Z}$ e $mdc(m,n) = 1$, obtemos as soluções racionais $\left(\frac{m^2-n^2}{m^2+n^2}, \frac{2mn}{m^2+n^2}\right)$, que correspondem às ternas pitagóricas $(m^2-n^2, 2mn, m^2+n^2)$.

2.2 Soma de Quadrados

Um resultado de Legendre fornece um critério para determinar quando uma equação do tipo

$$ax^2 + by^2 + cz^2 = 0 \tag{2.4}$$

possui solução não nula e que dá uma generalização natural das triplas pitagóricas, encontrada em (MARTINEZ et al., 2011), como segue.

Teorema 2.3. *(Teorema de Legendre) Sejam a, b, c inteiros livres de quadrados, primos entre si, dois a dois, e não todos do mesmo sinal. A equação (2.4) tem solução $(x, y, z) \neq$*

$(0,0,0)$ *com* x, y *e* z *inteiros se, e somente se,* $-bc$ *é quadrado módulo* a*,* $-ac$ *é quadrado módulo* b *e* $-ab$ *é quadrado módulo* c*.*

Demonstração. Pela simetria da equação (2.4) temos que $-bc$ é quadrado módulo a:

$$ax^2 + by^2 + cz^2 = 0 \Rightarrow bc + \frac{c^2z^2}{y^2} = \frac{-cx^2.a}{y^2} \Rightarrow -bc \equiv \frac{c^2z^2}{y^2} \mod a$$

Seja x, y e z primos dois a dois, pois seja $d = mdc(x, y)$, então $d^2|(cz^2)$, mas c é livre de quadrados, portanto, $d|z$. Agora como $by^2 + cz^2 \equiv 0 \mod a$ segue que $b^2y^2 \equiv -bcz^2 \mod a$.

Note que z deve ser primo com a, pois se p é primo tal que $p|a$ e $p|z$, teremos que $p|by^2$, mas $mdc(a, b) = 1$, segue que $p|y$ o que contradiz o fato de y e z serem primos entre si. Assim, z é invertível módulo a ($\exists\ z^{-1} = r \in \mathbb{Z}\ e\ z \cdot r \equiv 1 \mod a$), e logo, necessariamente,

$$(byz^{-1})^2 \equiv -bc \mod a$$

Agora supondo, sem perda de generalidade, que $a < 0$, $b < 0$ e $c > 0$. Por hipótese, existe $u \in \mathbb{Z}$ tal que $u^2 = -bc \mod a$.

$b \cdot b^{-1} = 1 \mod a$ pois $mdc(a, b) = 1$. Assim temos:

$ax^2 + by^2 + cz^2 \equiv by^2 + cz^2 \equiv b^{-1}((by)^2 + bcz^2) \equiv b^{-1}((by)^2 - u^2z^2) \equiv b^{-1}(by - uz)(by + uz) \equiv (y - b^{-1}uz)(by + uz) \equiv L_1(x, y, z)M_1(x, y, z) \mod a$, onde

$L_1(x, y, z) = d_1x + e_1y + f_1z$, $M_1(x, y, z) = g_1x + h_1y + i_1z$ com $d_1 = g_1 = 0$, $e_1 = 1$, $f_1 = -b^{-1}u$, $h_1 = b$ e $i_1 = u$.

Do mesmo modo, $ax^2 + by^2 + cz^2 \equiv L_2(x, y, z)M_2(x, y, z) \mod b$ e $ax^2 + by^2 + cz^2 \equiv L_3(x, y, z)M_3(x, y, z) \mod c$, onde $L_k(x, y, z) = d_kx + e_ky + f_kz$, $M_k(x, y, z) = g_kx + h_ky + i_kz$, $k = 2, 3$. Como a, b e c são primos entre si dois a dois, podemos, pelo Teorema Chinês dos Restos, encontrar duas formas lineares $L(x, y, z) = dx + ey + fz$, $M(x, y, z) = gx + hy + iz$ tais que $L \equiv L_1 \mod a$, $L \equiv L_2 \mod b$ e $L \equiv L_3 \mod c$, e $M \equiv M_1 \mod a$, $M \equiv M_2 \mod b$ e $M \equiv M_3 \mod c$ (basta resolver o sistema de congruências coeficiente a coeficiente). Logo

$$ax^2 + by^2 + cz^2 \equiv L(x, y, z)M(x, y, z) \mod abc.$$

Consideremos agora todas as triplas $(x, y, z) \in \mathbb{Z}^3$ com $0 \leq x \leq \sqrt{|bc|}$, $0 \leq y \leq \sqrt{|ac|}$, $0 \leq z \leq \sqrt{|ab|}$. Temos [1] $(\lfloor\sqrt{|bc|}\rfloor + 1)(\lfloor\sqrt{|ac|}\rfloor + 1)(\lfloor\sqrt{|ab|}\rfloor + 1) > abc$ de tais triplas, donde pelo Princípio da Casa dos Pombos existem duas triplas distintas dentre elas, (x_1, y_1, z_1) e (x_2, y_2, z_2), com $L(x_1, y_1, z_1) \equiv L(x_2, y_2, z_2) \mod abc \iff L(x_1 - x_2, y_1 - y_2, z_1 - z_2) \equiv 0 \mod abc$, donde, fazemos $\tilde{x} = x_1 - x_2$, $\tilde{y} = y_1 - y_2$ e $\tilde{z} = z_1 - z_2$, temos

$$a\tilde{x}^2 + b\tilde{y}^2 + c\tilde{z}^2 \equiv L(\tilde{x}, \tilde{y}, \tilde{z})M(\tilde{x}, \tilde{y}, \tilde{z}) \equiv 0 \mod abc \tag{2.5}$$

Notemos que $(\tilde{x}, \tilde{y}, \tilde{z}) \neq (0, 0, 0)$, $|\tilde{x}| < \sqrt{|bc|}$, $|\tilde{y}| < \sqrt{|ac|}$ e $|\tilde{z}| < \sqrt{|ab|}$, pois como a, b, c são coprimos dois a dois e livres de quadrados, não pode ocorrer a igualdade.

Como $a, b < 0$ e $c > 0$ temos que

$$-2abc = a|bc| + b|ac| < a\tilde{x}^2 + b\tilde{y}^2 \leq a\tilde{x}^2 + b\tilde{y}^2 + c\tilde{z}^2 \leq c\tilde{z}^2 < |ab|c = abc$$

Por 2.5, $abc|a\tilde{x}^2 + b\tilde{y}^2 + c\tilde{z}^2$, devemos então ter $a\tilde{x}^2 + b\tilde{y}^2 + c\tilde{z}^2 = 0$, o que resolve o problema, ou $a\tilde{x}^2 + b\tilde{y}^2 + c\tilde{z}^2 = -abc$, mas nesse caso, temos $0 = (a\tilde{x}^2 + b\tilde{y}^2 + c\tilde{z}^2 + abc)(\tilde{z}^2 + ab) = a(\tilde{x}\tilde{z} + b\tilde{y})^2 + b(\tilde{y}\tilde{z} - a\tilde{x})^2 + c(\tilde{z}^2 + ab)^2$, o que nos dá a solução $(\tilde{x}\tilde{z} + b\tilde{y}, \tilde{y}\tilde{z} - a\tilde{x}, \tilde{z}^2 + ab)$ com $\tilde{z}^2 + ab \neq 0$.

□

O Teorema 2.3 permite determinar quando uma curva algébrica plana de grau 2, $Ax^2 + Bxy + Cy^2 + Dx + Ey + F = 0$ com $A, B, C, D, E \in \mathbb{Q}$, possui algum *ponto racional* $(x, y) \in \mathbb{Q}^2$. De fato, fazendo $\tilde{x} = x + \frac{B}{2A}y$ (podemos supor que $A \neq 0$ se não fazemos uma mudança de coordenadas como $y = \tilde{y} + x$), a curva fica da forma $\tilde{A}\tilde{x}^2 + \tilde{C}\tilde{y}^2 + \tilde{D}\tilde{x} + \tilde{E}\tilde{y} + \tilde{F} = 0$, e, fazendo $\bar{x} = \tilde{x} + \frac{\tilde{D}}{2\tilde{A}}$ e $\bar{y} = \tilde{y} + \frac{\tilde{E}}{2\tilde{C}}$, a curva fica da forma $\bar{A}\bar{x}^2 + \bar{C}\bar{y}^2 + \bar{F} = 0$. Multiplicando pelo mmc dos denominadores dos coeficientes, podemos supor $\bar{A}$, $\bar{C}$ e $\bar{F}$ são inteiros, e, escrevendo $\bar{A} = k^2\hat{A}$, $\bar{C} = l^2\hat{C}$ e $\bar{F} = m^2\hat{F}$, com $\hat{A}$, $\hat{C}$ e $\hat{F}$ livre de quadrados, obtemos fazendo $\hat{x} = \frac{k}{m}\bar{x}$ e $\hat{y} = \frac{l}{m}\bar{y}$ a expressão $\hat{A}\hat{x}^2 + \hat{C}\hat{y}^2 + \hat{F} = 0$. Assim fazendo $\hat{x} = \frac{p}{q}$ e $\hat{y} = \frac{r}{q}$, obtemos a equação

$$\hat{A}p^2 + \hat{C}r^2 + \hat{F}q^2 = 0 \tag{2.6}$$

[1] $\lfloor x \rfloor$ = parte inteira de x

Podemos supor $mdc(\hat{A}, \hat{C}, \hat{F}) = 1$ (se não dividimos por $mdc(\hat{A}, \hat{C}, \hat{F})$) e que $mdc(p, r, q) = 1$. Além disso, se $mdc(\hat{A}, \hat{C}) = d$ devemos ter $d|\hat{F}q^2$, e logo $d|q$ (pois d é livre de quadrados), donde $q = dq'$, e obtemos a equação

$$\frac{\hat{A}}{d}p^2 + \frac{\hat{C}}{d}r^2 + (\hat{F}d)q'^2 = 0 \tag{2.7}$$

com $\frac{\hat{A}}{d}$, $\frac{\hat{C}}{d}$, $\hat{F}d$ livres de quadrados e

$$\left|\frac{\hat{A}}{d}\frac{\hat{C}}{d}\hat{F}d\right| = \left|\frac{\hat{A}\hat{C}\hat{F}}{d}\right| < |\hat{A}\hat{C}\hat{F}| \tag{2.8}$$

se $d > 1$.

Após algumas reduções deste tipo, obtemos uma equação equivalente como nas hipóteses do Teorema 2.3, que pode então ser usado para decidir a existência de um ponto racional na curva. Note que a hipótese sobre a, b, c não terem o mesmo sinal no Teorema 2.3 equivale à existência de pontos reais não triviais na curva.

Se há algum ponto racional (x_0, y_0) numa tal curva, então há infinitos. Isto pode ser visto a partir do exemplo a seguir, que ilustra o método geométrico que permite encontrar todos os pontos racionais explicitamente.

Exemplo 2.4. Encontre todos os pontos racionais da elipse $\frac{x^2}{5/2} + \frac{y^2}{5/3} = 1$.

Inicialmente podemos encontrar um destes pontos racionais, digamos $(x, y) = (1, 1)$, pois fazendo $x = 1$ temos,

$$\frac{1^2}{5/2} + \frac{y^2}{5/3} = 1$$

$$\frac{y^2}{5/3} = 1 - \frac{2}{5}$$

$$y^2 = \frac{3}{5}.\frac{5}{3}$$

$$y^2 = 1$$

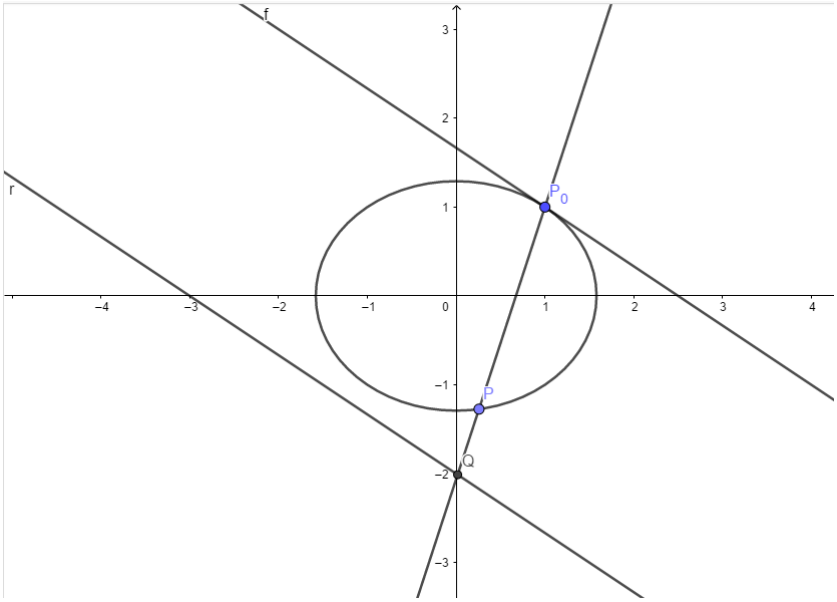
$$y = \pm 1$$

Para encontrar os demais pontos começamos traçando uma reta r de coeficientes racionais paralela à reta tangente à elipse no ponto $P_0 = (1, 1)$. Derivando implicitamente a equação da elipse em relação à x, obtemos $\frac{4x}{5}\frac{dx}{dx} + \frac{6y}{5}\frac{dy}{dx} = 0 \Rightarrow \frac{dy}{dx} = \frac{-2xy}{3}$. Logo, para

$(x, y) = (1, 1)$, temos $y' = \frac{-2}{3}$.

Portanto podemos tomar (por exemplo) a reta r de equação $y = \frac{-2x}{3} - 2$. Agora, para um ponto $P \neq P_0$ da elipse, seja a reta que liga P a $P_0 = (1, 1)$; como esta reta não é paralela a r, temos que r e s determinam um ponto Q, como na figura a seguir.

Figura 2.2: Elipse Exemplo 2



Agora vamos mostrar que existe uma bijeção $P \longmapsto Q$ entre os pontos racionais da elipse e os pontos racionais da reta r.

Temos que se P é um ponto racional da elipse então a equação da reta s, que liga dois pontos racionais P e P_0, possui coeficientes racionais. Logo Q será um ponto racional, sendo a intersecção de duas retas r e s cujas equações têm coeficientes racionais.

Reciprocamente, suponha que $Q = (a, b)$ é um ponto racional de r. Então a equação da reta s, determinada pelos pontos racionais P_0 e Q, terá coeficientes racionais: $y - 1 = \frac{b-1}{a-1}.(x - 1)$. Como a equação da elipse também tem coeficientes racionais, a intersecção $P \neq P_0$ de s com a elipse será um ponto racional, já que isolando y na equação de s e substituindo na equação da elipse obtemos uma equação quadrática com coeficientes racionais

$$\frac{2}{5}x^2 + \frac{3}{5}\left(1 + \frac{b-1}{a-1}.(x-1)\right)^2 - 1 = 0$$

Sabemos que a abscissa $x = 1$ de P_0 é uma das raízes, logo a outra raiz (que é a abscissa de P) é racional também pelas relações de Girard. Como P pertence à reta s

cuja equação tem coeficientes racionais, a ordenada de P também será racional, ou seja, P será um ponto racional.

Realizando algumas contas, obtemos a seguinte fórmula para P em função de $Q = (a, b)$:

$$P = \left(\frac{10a^2 + 90a + 21}{10a^2 + 24a + 87}, \frac{10a^2 - 20a - 111}{10a^2 + 24a + 87} \right)$$

.

Assim, os pontos racionais P da elipse são obtidos fazendo a percorrer todos os racionais $a \in \mathbb{Q}$ juntamente com $a = \infty$, isto é, o limite para $a \to \infty$ na expressão acima, que fornece o ponto inicial $P_0 = (1, 1)$, que corresponde ao "ponto no infinito" de r, intersecção de r com a reta s tangente à elipse no ponto P_0, no plano projetivo.

2.2.1 Soma de Dois Quadrados

A soma de dois números quadrados é uma Equação Diofantina que pode ser expressa como $n = x^2 + y^2$, e podemos estabelecer quando essa equação tem solução, como mostraremos abaixo, de acordo com o que é feito em (MARTINEZ et al., 2011).

Teorema 2.5. *Os únicos números que podem se expressar como soma de dois quadrados são os $n = 2^s d^2 l$, onde s é um número natura, $d \in \mathbb{Z}$ e l é um número livre de quadrados tais que seus fatores primos são da forma $4k + 1$.*

Para provarmos tal afirmação, observamos inicialmente que se p é um primo da forma $4k+3$ que divide $n = a^2 + b^2$, então $p|a$ e $p|b$. De fato, se isto não ocorresse, b seria invertível módulo p, ou seja, $b \cdot b^{-1} \equiv 1 \ mod \ p$.

Logo, de $a^2 + b^2 \equiv 0 \ mod \ p \Rightarrow a^2 \equiv -b^2 (mod \ p)$ teríamos que -1 é resíduo quadrático módulo p, $a^2 \cdot (b^{-1})^2 \equiv (-1)(b)^2(b^{-1})^2 = -1 \mod p \Rightarrow (ab^{-1})^2 \equiv -1 \mod p$, o que é absurdo, pois, pelo Critério de Euler (Ver Apêndice A), $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{(p-1)}{2}} = -1 \mod p$ já que $p \equiv 3 \ (mod \ 4)$.

Logo, $p^2|n$ e repetindo o processo com $\frac{n}{p^2} = \left(\frac{a}{p}\right)^2 + \left(\frac{b}{p}\right)^2$ no lugar de n, concluímos que todo primo da forma $4k + 3$ aparece com expoente par na fatoração canônica de n. Assim, apenas os números da forma descrita na afirmação inicial podem ser soma de dois quadrados.

Agora, todo natural n pode ser escrito como $n = k^2m$ onde k e m são inteiros positivos e m livre de quadrados, e assim, se m pode ser escrito como soma de dois quadrados ($m = a^2 + b^2$), então o mesmo ocorre com n, pois

$$n = k^2m = k^2(a^2 + b^2) = (ka)^2 + (kb)^2$$

Além disso, se temos dois números que são soma de dois quadrados, tais como $m = a^2+b^2$ e $n = c^2+d^2$), pelo que sabemos de números complexos ($|z| = |a+bi| = \sqrt{a^2 + b^2}$), temos que o produto mn também é soma de dois quadrados, pois:

$$mn = (a^2 + b^2)(c^2 + d^2) = |a + bi|^2 \cdot |c + di|^2$$

$$= |(a + bi)(c + di)|^2 = |(ac - bd) + (ad + bc)i|^2 = (ac - bd)^2 + (ad + bc)^2$$

Assim, para mostrar que todo n da forma $2^s d^2 l$ é soma de dois quadrados, basta mostrar que 2 e todo primo da forma $4k+1$ são somas de dois quadrados. Se $p = 2$ temos que $2 = 1^2 + 1^2$ é soma de dois quadrados. Para $4k + 1$ precisamos do lema seguinte.

Lema 2.6. *(Lema de Thrue) Se $m > 1$ é um número natural e a é um inteiro primo relativo com m então existem números naturais x e y não nulos menores do que ou iguais a $\sqrt{m}$ e tais que algum dos números $ax \pm y$ é divisível por m.*

Demonstração. Seja $q = \lfloor \sqrt{m} \rfloor$, então

$$q + 1 > \sqrt{m} \Rightarrow (q + 1)^2 > m$$

Consideremos todos os $(q + 1)^2$ números da forma $ax - y$ onde x e y tomam os valores $0, 1, ..., q$. Como só existem m restos ao se dividir um número por m, pelo Princípio da Casa dos Pombos, dois dos números anteriores, digamos $ax_1 - y_1$ e $ax_2 - y_2$, com $(x_1, y_1) \neq (x_2, y_2)$, são congruentes módulo m. Portanto a diferença $a(x_1 - x_2) - (y_1 - y_2)$ é divisível por m. Temos

$$0 \leq x_i, y_i \leq \sqrt{m} \rightarrow |x_1 - x_2|, |y_1 - y_2| \leq \sqrt{m}$$

.

Se $x_1 - x_2 = 0$, então $y_1 - y_2$ será divisível por m, o que implica $y_1 = y_2$, mas definimos os pares (x_1, y_1) e (x_2, y_2) diferentes, portanto, uma contradição.

Da mesma maneira, se $y_1 - y_2 = 0$ então $a(x_1 - x_2)$ será divisível por m, mas a e m são primos relativos, logo $m|x_1 - x_2$ e assim $x_1 = x_2$, o que novamente, é uma contradição.

Logo $x = |x_1 - x_2|$ e $y = |y_1 - y_2|$ satisfazem as condições do enunciado do Lema. □

De volta ao problema inicial,se p é um número primo da forma $p = 4k + 1$, então, pelo Critério de Euler, $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{(p-1)}{2}} = 1 \mod p$, logo existe a tal que $p|a^2 + 1$.

Aplicando o Lema 2.6, existem inteiros $0 < x, y < \sqrt{p}$ tais que algum dos números $ax \pm y$ é divisível por p, portanto o número $(ax + y)(ax - y) = a^2x^2 - y^2$ é divisível por p. Então

$$x^2 + y^2 = x^2 + a^2x^2 - a^2x^2 + y^2 = x^2(a^2 + 1) - (a^2x^2 - y^2)$$

é divisível por p, mas como $0 < x, y < \sqrt{p}$ então $0 < x^2 + y^2 < 2p$, portanto $p = x^2 + y^2$. Assim provamos o Teorema 2.5.

Afim de verificarmos o que é provado pelo Teorema 2.5 numericamente, notemos o exemplo a seguir:

Exemplo 2.7. Vamos tomar aleatoriamente um número n tal que este seja soma de dois quadrados, que seja então

$$n = 21^2 + 47^2$$

Então temos que $n = 441 + 2209 = 2650$

Fatorando n temos

$$n = 2.5^2.53$$

Portanto n é da forma indicada no Teorema 2.3, sendo $s = 1$, $d = 5$ e $l = 53$.

Exemplo 2.8. Sejam $d \in \{1, 2, 3, 7\}$ e p é primo ímpar tal que $\left(\frac{-d}{p}\right) = 1$, então existem $e, f \in \mathbb{N}$ tais que $p = e^2 + df^2$.

Demonstração. Para provar tal afirmação, vamos tomar $a \in \mathbb{N}$ tal que $a^2 \equiv -d \mod p$. Pelo Lema 2.6, existem inteiros x, y tais que

$$(x + ay)(x - ay) \equiv 0 \mod p \Rightarrow x^2 - a^2y^2 \equiv 0 \mod p$$

Como $a^2 \equiv -d(\mod p)$, multiplicando ambos os lados por $-y^2$ e somando também de ambos os lados x^2, chegamos que $x^2 - a^2y^2 \equiv x^2 + dy^2 \mod p \iff p|x^2 + dy^2$ e $0 < x^2 + dy^2 < (d+1)p$.

Assim, temos $x^2 + dy^2 = kp$ com $k \in \{1, 2, ..., d\}$

Observemos que se $k = d$, x é múltiplo de d:

$$x^2 = dp - dy^2$$

$$x^2 = d(p - y^2)$$

e fazendo $x = dz$ temos

$$d^2z^2 + dy^2 = dp$$

$$dz^2 + y^2 = p$$

Assim podemos desconsiderar $k = d$, pois chegamos a uma equação igual a do enunciado do exemplo, com $e = y$ e $f = z$.

Se $d = 1$ ou $d = 2$ o problema está resolvido. Consideremos então os outros casos.

1. Se $d = 3$ então $x^2+3y^2 = p$ ou $2p$. No caso $x^2+3y^2 = 2p$ temos que x e y têm a mesma paridade, assim, se x, y são pares temos $4|x^2+3y^2 = 2p$, que é contraditório. No caso em que x, y são ímpares temos $x^2 \equiv y^2 \equiv 1(\mod 8)$, portanto $2p = x^2 + 3y^2 \equiv 4(\mod 8)$, que também é contraditório. Assim concluímos que $x^2 + 3y^2 = p$.

2. Se $d = 7$ então $x^2 + 7y^2 = ip$ com $i \in \{1, 2, 3, 4, 5, 6\}$. No caso que x, y são ímpares, como $x^2 \equiv y^2 \equiv 1(\mod 8)$, temos que $x^2+7y^2 \equiv 0(\mod 8)$, o que é contraditório, e no caso em que x, y são pares, dividimos toda a expressão por 4, logo podemos supor que i é ímpar. Assim resta considerar os casos em que $i = 3$ ou 5. Mas -7 não é resto quadrático módulo 3 nem 5, portanto $x^2 + 7y^2 = p$

□

2.2.2 Soma de Quatro Quadrados

Vamos mostrar que qualquer número inteiro positivo pode ser escrito como soma de, no máximo, quatro quadrados, de acordo com a prova de Lagrange, a primeira publicada e apresentada em (MARTINEZ et al., 2011). Ou seja, provaremos que qualquer

inteiro positivo p pode ser escrito como $p = a^2+b^2+c^2+d^2$. Para tal prova necessitaremos dos lemas seguintes.

Lema 2.9. *(Identidade de Euler) Para todo a, b, c, d, w, x, y, z temos que*

$$(a^2 + b^2 + c^2 + d^2)(w^2 + x^2 + y^2 + z^2)$$
$$= (aw+bx+cy+dz)^2+(ax-bw-cz+dy)^2+(ay+bz-cw-dx)^2+(az-by+cx-dw)^2.$$

Demonstração. A comprovação de tal lema pode ser feita de maneira direta, como abaixo:

$$(a^2 + b^2 + c^2 + d^2)(w^2 + x^2 + y^2 + z^2) =$$

$$a^2w^2 + a^2x^2 + a^2y^2 + a^2z^2 + b^2w^2 + b^2x^2 + b^2y^2 + b^2z^2$$

$$+c^2w^2 + c^2x^2 + c^2y^2 + c^2z^2 + d^2w^2 + d^2x^2 + d^2y^2 + d^2z^2$$

$$= a^2w^2 + b^2x^2 + c^2y^2 + d^2z^2 + 2abwx - 2abwx + 2acwy - 2acwy + 2adwz - 2adwz$$

$$+2bcxy - 2bcxy + 2bdxz - 2bdxz + 2cdyz - 2cdyz + a^2x^2 + b^2w^2 + c^2z^2 + d^2y^2$$

$$+2acxz - 2acxz + 2adxy - 2adxy + 2bcwz - 2bcwz + 2bdwy - 2bdwy + a^2y^2 + b^2z^2$$

$$+c^2w^2 + d^2x^2 + 2abyz - 2abyz + 2cdwz - 2cdwx + a^2z^2 + b^2y^2 + c^2x^2 + d^2w^2$$

$$= (aw+bx+cy+dz)^2+(ax-bw-cz+dy)^2+(ay+bz-cw-dx)^2+(az-by+cx-dw)^2$$

Pode ser comprovado também utilizando a seguinte identidade de matrizes complexas, onde a barra denota conjugado:

$$\begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \begin{pmatrix} \gamma & \delta \\ -\bar{\delta} & \bar{\gamma} \end{pmatrix} = \begin{pmatrix} \alpha\gamma - \beta\bar{\delta} & \alpha\delta + \beta\bar{\gamma} \\ -\overline{(\alpha\delta + \beta\bar{\gamma})} & \overline{\alpha\gamma - \beta\bar{\delta}} \end{pmatrix}$$

Calculando determinantes, obtemos

$$(|\alpha|^2 + |\beta|^2)(|\gamma|^2 + |\delta|^2) = |\alpha\gamma - \beta\bar{\delta}|^2 + |\alpha\delta + \beta\bar{\gamma}|^2$$

Substituindo $\alpha = a-bi$, $\beta = -c-di$, $\gamma = w+xi$ e $\delta = y+zi$, obtemos a identidade desejada:

$$(|a - bi|^2 + | - c - di|^2)(|w + xi|^2 + |y + zi|^2)$$

$$= |(a-bi)(w+xi) - (-c-di)(y-zi)|^2 + |(a-bi)(y+zi) + (-c-di)(w-xi)|^2$$

$$\Rightarrow (a^2+b^2+c^2+d^2)(w^2+x^2+y^2+z^2)$$

$$= |aw+axi-bwi+bx-(-cy+czi-dyi-dz)|^2+|ay+azi-byi+bz+(-cw+cxi-dwi-dx)|^2$$

$$\Rightarrow (a^2+b^2+c^2+d^2)(w^2+x^2+y^2+z^2)$$

$$= |aw+bx+cy+dz+(ax-bw-cz+dy)i|^2+|ay+bz-cw-dx+(az-by+cx-dw)i|^2$$

$$\Rightarrow (a^2+b^2+c^2+d^2)(w^2+x^2+y^2+z^2)$$

$$= (aw+bx+cy+dz)^2+(ax-bw-cz+dy)^2+(ay+bz-cw-dx)^2+(az-by+cx-dw)^2$$

□

Lema 2.10. *Se $2m$ é soma de dois quadrados, então m também é soma de dois quadrados, ou seja $2m = x^2+y^2 \iff m = w^2+z^2$.*

Demonstração. Como $2m = x^2+y^2$ então x e y têm a mesma paridade. Fazendo $w = \left(\frac{x+y}{2}\right)$ e $z = \left(\frac{x-y}{2}\right)$, obtemos o resultado procurado, pois

$$m = w^2+z^2 = \left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2 = \frac{x^2+2xy+y^2+x^2-2xy+y^2}{4}$$

$$= \frac{2x^2+2y^2}{4} = \frac{x^2+y^2}{2} = m \iff 2m = x^2+y^2$$

□

Exemplo 2.11. Temos que 208 é soma de dois quadrados, pois $208 = 8^2+12^2$ e $208 = 2\cdot(104)$. Vamos mostrar que 104 também é soma de dois quadrados.

$$208 = 8^2+12^2 \Rightarrow 2\cdot(104) = 2\cdot(32)+2\cdot(72) \Rightarrow 104 = 2^2+10^2$$

Lema 2.12. *Se p é primo ímpar, então existem inteiros a, b, k tais que $a^2+b^2+1 = kp$.*

Demonstração. Considere os conjuntos $A = \left\{a^2 \in \mathbb{Z}/p\mathbb{Z} \mid 0 \leq a \leq \frac{p-1}{2}\right\}$ e $B = \left\{-b^2-1 \in \mathbb{Z}/p\mathbb{Z} \mid 0 \leq b \leq \frac{p-1}{2}\right\}$

Como cada conjunto possui $\frac{p+1}{2}$ elementos de $\mathbb{Z}/p\mathbb{Z}$ então $A \cap B \neq \varnothing$, isto é, existem a e b tais que $a^2 \equiv (-b^2 - 1)(mod\ p)$. □

Teorema 2.13. *Todo inteiro positivo n pode se escrever como soma de quatro quadrados.*

Demonstração. Pelo Lema 2.9, basta provar o resultado para os números primos. Como $2 = 1^2 + 1^2$, podemos supor p primo ímpar.

Pelo Lema 2.12, é possível encontrar a, b, c, d e m inteiros com $m > 0$ tais que $mp = a^2 + b^2 + c^2 + d^2$ (Basta tomar $A = \left\{a^2 + c^2 \in \mathbb{Z}/p\mathbb{Z} \mid 0 \leq a \leq \frac{p-1}{2}\right\}$ e $B = \left\{ -b^2 - d^2 \in \mathbb{Z}/p\mathbb{Z} \mid 0 \leq b \leq \frac{p-1}{2}\right\}$ com $c, d \in \mathbb{Z}$ e proceder com a demonstração de maneira semelhante a do Lema) . Assim, para terminar a demonstração, basta provar que se $m > 1$ então existe um $0 < n < m$ tal que np pode se escrever como soma de quatro quadrados.

De fato, se m é par, então nenhum, dois ou quatro dos números a, b, c, d são pares, assim aplicando apropriadamente o Lema 2.10, basta tomar $n = \frac{m}{2}$. Portanto podemos supor que m é ímpar maior que 1. Sejam w, x, y, z inteiros tais que

$$w \equiv a(\mod m)$$

$$x \equiv b(\mod m)$$

$$y \equiv c(\mod m)$$

$$z \equiv d(\mod m)$$

onde $w, x, y, z \in \left(-\frac{m}{2}, \frac{m}{2}\right)$, logo

$w^2 + x^2 + y^2 + z^2 < 4 \cdot \frac{m^2}{4} = m^2$ e $w^2 + x^2 + y^2 + z^2 \equiv 0(\mod m)$.

Portanto $w^2 + x^2 + y^2 + z^2 = nm$ com $0 < n < m$. Pela escolha de w, x, y, z temos que os números $ax - bw - cz + dy$, $ay + bz - cw - dx$ e $az - by + cx - dw$ são divisíveis por m e $aw + bx + cy + dz \equiv a^2 + b^2 + c^2 + d^2 \equiv 0(\mod m)$, portanto, pelo Lema 2.9 temos que

$$np = \frac{1}{m^2}(mp)(nm) = \frac{1}{m^2}(a^2 + b^2 + c^2 + d^2)(w^2 + x^2 + y^2 + z^2)$$
$$= \left(\frac{aw + bx + cy + dz}{m}\right)^2 + \left(\frac{ax - bw - cz + dy}{m}\right)^2$$

$$+\left(\frac{ay+bz-cw-dx}{m}\right)^2+\left(\frac{az-by+cx-dw}{m}\right)^2$$

é soma de quatro quadrados, como desejado. □

2.2.3 Soma de Três Quadrados

O Teorema seguinte, provado por Gauss, mostra uma condição para um número ser soma de três quadrados.

Teorema 2.14. *(Teorema dos Três Quadrados de Gauss) Um inteiro $n \geq 0$ é soma de três quadrados se, e somente se, n não é da forma $4^a(8b+7)$, com $a, b \in \mathbb{N}$.*

Demonstração. Notemos inicialmente que, como k^2 só deixa restos $0, 1$ e 4 na divisão por 8 para todo $k \in \mathbb{N}$, uma soma de três quadrados não pode ser congruente a $7 \mod 8$.

Suponha que $n = x^2+y^2+z^2 = 4^a(8b+7) \Rightarrow x^2+y^2+z^2 \equiv 0 \mod 4 \Rightarrow x, y, z$ são pares $\Rightarrow 2|mdc(x,y,z) \Rightarrow \left(\frac{x}{2}\right)^2+\left(\frac{y}{2}\right)^2+\left(\frac{z}{2}\right)^2 = 4^{a-1}(8b+7) \equiv 0 \mod 4$, novamente $\left(\frac{x}{2}\right)$, $\left(\frac{y}{2}\right)$, $\left(\frac{z}{2}\right)$ são pares, então $2^2|mdc(x,y,z)$ e repetindo esse processo, concluímos que $2^a|mdc(x,y,z)$, e logo $\left(\frac{x}{2^a}\right)^2+\left(\frac{y}{2^a}\right)^2+\left(\frac{z}{2^a}\right)^2 = 8b+7 \equiv 7 \mod 8$ o que é um absurdo, mostrando a necessidade da condição.

Para mostrar a suficiência é necessário o Lema seguinte.

Lema 2.15. *Se $n \in \mathbb{N}$ é soma de três quadrados de números racionais, então n é soma de três quadrados de inteiros.*

Demonstração. Se $n = x_1^2+x_2^2+x_3^2$ com $x_1, x_2, x_3 \in \mathbb{Q}$ e sendo $q \in \mathbb{N}$ um denominador comum para x_1, x_2, x_3 temos que $q^2n = p_1^2+p_2^2+p_3^2$, onde $p_1 = qx_1$, $p_2 = qx_2$, $p_3 = qx_3$ são inteiros.

Seja $d > 0$ o menor inteiro positivo para o qual existem $y_1, y_2, y_3 \in \mathbb{Z}$ com $y_1^2+y_2^2+y_3^2 = d^2n$

Queremos mostrar que $d = 1$. Então suponhamos por absurdo que $d > 1$. Escrevemos $y_1 = dy_1'+z_1$, $y_2 = dy_2'+z_2$ e $y_3 = dy_3'+z_3$, com $y_i', z_i \in \mathbb{Z}$, $|z_i| \leq \frac{d}{2}, i = 1, 2, 3$.

Definimos

$$a = {y_1'}^2+{y_2'}^2+{y_3'}^2-n$$

$$b = 2(nd-y_1y_1'-y_2y_2'-y_3y_3')$$

$$d' = ad + b$$

$$y_i'' = ay_i + by_i'$$

,para $i = 1, 2, 3$

Temos então

$$\sum_{1\leq i\leq 3} {y_i''}^2 = \sum_{1\leq i\leq 3} (ay_i + by_i')^2 = \sum_{1\leq i\leq 3} (a^2{y_i}^2 + 2aby_iy_i' + b^2{y_i'}^2)$$

$$= a^2 \sum_{1\leq i\leq 3} {y_i}^2 + 2ab \sum_{1\leq i\leq 3} y_iy_i' + b^2 \sum_{1\leq i\leq 3} {y_i'}^2$$

$$= a^2({y_1}^2 + {y_2}^2 + {y_3}^2) + 2ab(y_1y_1' + y_2y_2' + y_3y_3') + b^2({y_1'}^2 + {y_2'}^2 + {y_3'}^2)$$

$$= a^2d^2n + 2ab(\frac{-b}{2} + nd) + b^2(a + n) = a^2d^2n + 2abnd - ab^2 + ab^2 + b^2n$$

$$= n(a^2d^2 + 2abd + b^2) = n(ad + b)^2 = d'^2n$$

e

$$dd' = d(ad + b) = ad^2 + bd = d^2 \left(\sum_{1\leq i\leq 3} {y_i'}^2 - n \right) + 2d \left(nd - \sum_{1\leq i\leq 3} y_i'y_i \right)$$

$$= d^2 \sum_{1\leq i\leq 3} {y_i'}^2 - d^2n + 2d^2n - 2d \sum_{1\leq i\leq 3} y_i'y_i = d^2 \sum_{1\leq i\leq 3} y_i' + d^2n - 2d \sum_{1\leq i\leq 3} y_iy_i'$$

$$= \sum_{1\leq i\leq 3} {y_i}^2 - 2d \sum_{1\leq i\leq 3} y_iy_i' + d^2 \sum_{1\leq i\leq 3} {y_i'}^2 = \sum_{1\leq i\leq 3} (y_i - dy_i')^2 = \sum_{1\leq i\leq 3} {z_i}^2 \leq \frac{3}{4}d^2$$

o que resulta que $0 \leq d' \leq \frac{3}{4}d < d$. Se $d' > 0$, então temos uma contradição com a minimalidade de d.

Se $d' = 0$, então $\sum_{1 \leq i \leq 3} {z_i}^2 = dd' = 0$, onde $z_1 = z_2 = z_3 = 0$ e logo ${y'_1}^2 + {y'_2}^2 + {y'_3}^2 = n$, o que é uma contradição, pois $1 < d$. Logo, $d = 1$.

□

Para concluir a prova do Teorema 2.14, dado $n \in \mathbb{N}$ que não seja da forma $4^a(8b+7)$, dividindo-o por uma potência de 4 conveniente podemos supor $n \mod 8 \in \{\bar{1}, \bar{2}, \bar{3}, \bar{5}, \bar{6}\}$.

Basta provar então que existem um inteiro $m > 0$ e racionais x, y, z, t com $t \neq 0$ tais que $x^2 + y^2 = m$ e $nt^2 - z^2 = m$, pois $n = \left(\frac{x}{t}\right)^2 + \left(\frac{y}{t}\right)^2 + \left(\frac{z}{t}\right)^2$ será soma de três quadrados racionais e, pelo Lema 2.15 provado anteriormente soma de três inteiros.

Podemos supor que n é livre de quadrados: sempre podemos escrever $n = a^2 \cdot \tilde{n}$, onde $\tilde{n}$ é livre de quadrados, e se $\tilde{n} = x^2 + y^2 + z^2$ então $n = (ax)^2 + (ay)^2 + (az)^2$. Além disso, como n não é múltiplo de 4, então a é ímpar, e logo $a^2 \equiv 1(mod\ 8)$, donde $n = a^2\tilde{n} \equiv \tilde{n} \mod 8$.

Temos agora alguns casos:

1. Se $n \equiv 1 \mod 4$ ou seja $n \mod 8 \in \{\bar{1}, \bar{5}\}$, tomamos m primo

   $m \equiv 1 \mod 4$ e $m \equiv -1 \mod n$.

   Tal primo existe pois, pelo Teorema Chinês dos Restos, existe um $a \in \mathbb{Z}$ com $a \equiv 1 \mod 4$ e $a \equiv -1 \mod n$ e pelo Teorema de Dirichlet existem infinitos primos congruentes com $a \mod 4n$.

   Como $m \equiv 1 \mod 4$ e m é primo, do Teorema 2.5, existem x, y tais que $x^2 + y^2 = m$.

   Por outro lado, existem t e z racionais com $nt^2 - z^2 = m$ se, e somente se, existem u, v e w inteiros não nulos tais que $nu^2 - v^2 - mw^2 = 0$.

   Pelo Teorema 2.3, isso equivale a n ser quadrado módulo m e $-m$ ser quadrado módulo n, mas $-m \equiv 1 = 1^2 \mod n$.

   Além disso, se $n = p_1 p_2 ... p_k$ com os p_i primos, usando o fato que $m \equiv 1 \mod 4$ e pela Lei da Reciprocidade Quadrática (Ver Apêndice A) obtemos:

$$\left(\frac{n}{m}\right) = \prod_{1 \leq i \leq k} \left(\frac{p_i}{m}\right) = \prod_{1 \leq i \leq k} \left(\frac{m}{p_i}\right)$$

.

Mas $m \equiv -1(\mod n)$, em particular $m \equiv -1(\mod p_i)$, assim $\left(\frac{m}{p_i}\right) = \left(\frac{-1}{p_i}\right) = (-1)^{\frac{p_i-1}{2}}$.

Mas o número de fatores p_i de n congruentes com $3(\mod 4)$ é par, pois $n \equiv 1(\mod 4)$, portanto $\left(\frac{n}{m}\right) = 1$.

2. Se n é par, ou seja, $n \mod 8 \in \{\bar{2}, \bar{6}\}$, temos que $n = 2p_ip_2...p_k$, onde os p_i são primos ímpares distintos. Tomemos como antes m primo, $m \equiv 1(\mod 4)$ e $m \equiv -1(\mod \frac{n}{2}$; ainda temos o direito de escolher a classe de congruência de m módulo 8, que pode ser 1 ou 5. Lembramos que se $m \equiv 1(\mod 8)$ então $\left(\frac{2}{m}\right) = 1$ e se $m \equiv 5(\mod 8)$ então $\left(\frac{2}{m}\right) = -1$.

   Temos como antes $-m \equiv 1(\mod n)$, onde $-m$ é um quadrado módulo n, pelo Teorema 2.3. Basta mostrar que m pode ser escolhido de modo que n seja quadrado módulo m. Temos

$$\left(\frac{n}{m}\right) = \left(\frac{2}{m}\right) \prod_{1\leq i\leq k} \left(\frac{p_i}{m}\right) = \left(\frac{2}{m}\right) \prod_{1\leq i\leq k} \left(\frac{m}{p_i}\right) = \left(\frac{2}{m}\right) \prod_{1\leq i\leq k} \left(\frac{-1}{p_i}\right)$$

   .

   Basta então escolher a classe de congruência de m módulo 8 de modo que $\left(\frac{2}{m}\right) = \prod_{1\leq i\leq k} \left(\frac{-1}{p_i}\right)$ para que tenhamos $\left(\frac{n}{m}\right) = 1$.

3. Se $n \equiv 3(\mod 8)$, tomamos $m = 2q$ com q primo, $q \equiv 1(\mod 4)$ e $2q \equiv -1(\mod n)$. Temos, como antes, $-m \equiv 1(\mod n)$, onde $-m$ é um quadrado módulo n.

   Vamos mostrar que n é quadrado módulo m, como n é quadrado módulo 2, basta mostrar que é quadrado módulo q.

   Sendo $n = p_1p_2...p_k$, com p_i primos, temos

$$\left(\frac{n}{q}\right) = \prod_{1\leq i\leq k} \left(\frac{p_i}{q}\right) = \prod_{1\leq i\leq k} \left(\frac{q}{p_i}\right) = \prod_{1\leq i\leq k} \left(\frac{2}{p_i}\right)\left(\frac{2q}{p_i}\right) = \prod_{1\leq i\leq k} \left(\frac{2}{p_i}\right)\left(\frac{-1}{p_i}\right)$$

e $\left(\frac{2}{p_i}\right)\left(\frac{-1}{p_i}\right) = \begin{cases} 1, \ se \ p_i \mod 8 \in \{\bar{1}, \bar{3}\} \\ -1, \ se \ p_i \mod 8 \in \{\bar{5}, \bar{7}\} \end{cases}$

Como $1 \cdot 1 \equiv 3 \cdot 3 \equiv 5 \cdot 5 \equiv 7 \cdot 7 \equiv 1(\mod 8)$, $1 \cdot 3 \equiv 5 \cdot 7 \equiv 3(\mod 8)$, $1 \cdot 5 \equiv 3 \cdot 7 \equiv 5(\mod 8)$ e $1 \cdot 7 \equiv 3 \cdot 5 \equiv 7(\mod 8)$, n deve ter uma quantidade par de fatores pertencentes a $\{\bar{5}, \bar{7}\} \mod 8$, pois caso contrário $n \mod 8 \in \{\bar{5}, \bar{7}\}$. Assim temos $\left(\frac{n}{q}\right) = 1$.

□

3 ÚLTIMO TEOREMA DE FERMAT

3.1 Descenso Infinito de Fermat

De acordo com o que é apresentado em (MARTINEZ et al., 2011), dada uma equação

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

o método do descenso infinito, quando possível sua utilização, permite mostrar que esta equação não possui soluções inteiras positivas ou, sob certas condições, até mesmo encontrar todas as suas soluções inteiras. Se o conjunto de soluções de f

$$A = \{(x_1, ..., x_n) \in \mathbb{Z}^n \mid f(x_1, ..., x_n) = 0\}$$

é diferente de vazio, o método consiste em considerar a menor solução, no sentido de construir uma função $\phi : A \to \mathbb{N}$ a partir de f e considerar a solução $(x_1, ..., x_n) \in A$ com $\phi(x_1, ..., x_n)$ mínimo. O descenso consiste em obter, a partir desta solução mínima, uma ainda menor, o que nos conduz claramente a uma contradição, provando que A é de fato vazio.

Para ilustrar este método vamos considerar os exemplos seguintes, baseado em (MARTINEZ et al., 2011).

Exemplo 3.1. (Fermat) Demonstrar que a equação $x^4 + y^4 = z^2$ não possui soluções inteiras positivas.

Suponhamos que $x^4 + y^4 = z^2$ possui uma solução inteira com $x, y, z > 0$. Logo existe uma solução (a, b, c) na qual c é mínimo. Em particular, temos que a e b são primos entre si, pois se $d = mdc(a, b) > 1$ poderíamos substituir (a, b, c) por $\left(\frac{a}{d}, \frac{b}{d}, \frac{c}{d^2}\right)$ e obter uma solução com c menor.

De $(a^2)^2+(b^2)^2 = c^2$ temos portanto que (a^2, b^2, c) é uma tripla pitagórica primitiva e assim existem inteiros positivos m e n primos relativos tais que $a^2 = m^2 - n^2$, $b^2 = 2mn$ e $c = m^2 + n^2$.

De $a^2 = m^2 - n^2$, temos que (a, n, m) é uma tripla pitagórica primitiva e portanto m é ímpar. Assim, de $b^2 = 2mn$ concluímos que b e n são números pares. Observando ainda que $b^2 = (2n)m$ é um quadrado perfeito e $mdc(2n, m) = 1$, concluímos que tanto $2n$ como m são quadrados perfeitos, donde podemos encontrar inteiros positivos s e t tais que $2n = 4s^2$ e $m = t^2$.

Por outra parte, dado que $a^2 + n^2 = m^2$ também é uma tripla pitagórica, então existirão inteiros positivos i e j, primos entre si, tais que $a = i^2 - j^2$, $n = 2ij$ e $m = i^2 + j^2$. Portanto se $2n = 4s^2 \Rightarrow s^2 = \frac{n}{2} = ij$, logo i e j serão quadrados perfeitos, digamos $i = u^2$ e $j = v^2$.

Logo temos que $m = i^2 + j^2$, $i = u^2$, $j = v^2$ e $m = t^2$. Então $t^2 = (u^2)^2 + (v^2)^2 = u^4 + v^4$, isto é, (u, v, t) é outra solução da equação original. Porém $t \leq t^2 = m \leq m^2 < m^2 + n^2 = c$ e $t \neq 0$ porque m é diferente de 0. Como c é mínimo, temos uma contradição.

Observemos além disso que, uma vez que esta equação não possui soluções inteiras positivas, então a equação $x^4 + y^4 = z^4$ e, mais geralmente $x^{4n} + y^{4n} = z^{4n}$ também não possuem.

Exemplo 3.2. Encontrar todas as soluções inteiras positivas da equação $m^2 - mn - n^2 = \pm 1$

Note que $m^2 = n^2 + mn \pm 1 \geq n^2 \Rightarrow m \geq n$, com igualdade se, e somente se, $(m, n) = (1, 1)$, que é claramente uma solução. Agora seja (m, n) uma solução com $m > n$. Demonstremos que $(n, m - n)$ também é solução.

$$n^2 - n(m - n) - (m - n)^2 = \pm 1$$

$$n^2 - nm + n^2 - (m^2 - 2mn + n^2) =$$

$$n^2 - nm + n^2 - m^2 + 2mn - n^2 =$$

$$n^2 + mn - m^2 =$$

$$-(m^2 - mn - n^2) = \mp 1$$

Como (m, n) é solução, então $m^2 - mn - n^2 = \pm 1$, logo

$$n^2 - n(m-n) - (m-n)^2 = -(\pm 1) = \mp 1.$$

Assim, se temos uma solução (m, n), podemos encontrar uma cadeia descendente de soluções, e este processo parará quando atingirmos uma solução (a, b) com $a = b$, ou seja, a solução $(1, 1)$.

Invertendo o processo, encontraremos, portanto, todas as soluções, isto é, se (m, n) é solução então $(m + n, m)$ é solução. Portanto todas as soluções positivas são:

$$(1,1), (2,1), (3,2), ..., (F_{n+1}, F_n), ...$$

onde F_n representa o n-ésimo termo da sequência de Fibonacci.

Exemplo 3.3. Determine todos os pares de inteiros positivos (a, b) para os quais

$$\frac{a^2}{2ab^2 - b^3 + 1}$$

é um inteiro positivo.

Seja (a, b) uma solução inteira positiva. Logo $2ab^2 - b^3 + 1 \geq 1$ e portanto

$$2ab^2 - b^3 \geq 1 - 1 \Rightarrow$$

$$2ab^2 \geq b^3 \Rightarrow$$

$$a \geq \frac{b^3}{2b^2} \Rightarrow$$

$$a \geq \frac{b}{2}.$$

No caso $a = \frac{b}{2}$, é fácil verificar que obtemos uma solução. Para qualquer outra solução, $a > \frac{b}{2}$ e nesse caso

$$a^2 \geq 2ab^2 - b^3 + 1 \Rightarrow a^2 \geq b^2(2a - b) + 1 > b^2 \Rightarrow a > b \tag{3.1}$$

Agora, se $\frac{a^2}{2ab^2 - b^3 + 1} = k \in \mathbb{N}$, então $a^2 = k(2ab^2 - b^3 + 1)$, e daí a é raiz do polinômio com coeficientes inteiros $x^2 - 2kb^2x + k(b^3 - 1) = 0$.

Mas este polinômio possui outra solução inteira. Como

$$\Delta = 4k^2b^4 - 4k(b^3 - 1) = 4k(kb^4 - b^3 + 1) \geq 0$$

então as raízes são dadas por

$$\frac{2kb^2 \pm \sqrt{4(k^2b^4 - kb^3 + k)}}{2} = kb^2 \pm \sqrt{k^2b^4 - kb^3 + k}$$

Então

$$x_1 = kb^2 + \sqrt{k^2b^4 - kb^3 + k}$$

e

$$x_2 = kb^2 - \sqrt{k^2b^4 - kb^3 + k}$$

Temos que $x_1 + x_2 = 2kb^2$. Se $x_1 = a \Rightarrow x_2 \geq 0$ e de forma análoga, se $x_2 = a \Rightarrow x_1 \geq 0$, pois, considerando $x_1 = a$, então $2kb^2 - a = 2kb^2 - kb^2 - \sqrt{k^2b^4 - kb^3 + k} = kb^2 - \sqrt{k^2b^4 - kb^3 + k} = a_1$.

Logo, $a_1 = 2kb^2 - a = \frac{k(b^3-1)}{a} \geq 0$

Assim (a_1, b) também é solução do problema se $b > 1$, pois se $b = 1 \Rightarrow a_1 = 0$. Supondo que a é a maior raiz, de $a \geq a_1$, teremos que $a \geq kb^2$ e assim

$$a_1 = \frac{k(b^3 - 1)}{a} \leq \frac{k(b^3 - 1)}{kb^2} < b.$$

Desta forma, de 3.1 ou $b = 1$ ou $a_1 = \frac{b}{2}$ e neste último caso

$$a_1 = \frac{b}{2} = kb^2 - \sqrt{k^2b^4 - kb^3 + k}$$

$$(\sqrt{k^2b^4 - kb^3 + k})^2 = (kb^2 - \frac{b}{2})^2$$

$$k^2b^4 - kb^3 + k = k^2b^4 - kb^3 + \frac{b^2}{4}$$

$$k = \frac{b^2}{4}$$

e como

$$a + a_1 = 2kb^2$$

$$a = 2 \cdot \frac{b^2}{4} \cdot b^2 - a_1$$

$$a = \frac{b^4}{2} - \frac{b}{2}.$$

Portanto as soluções do problema são $(a, b) = (l, 2l), (2l, 1)$ ou $(8l^4 - l, 2l)$, com $l \in \mathbb{N}$.

3.1.1 Equação de Markov

A equação de Markov é a equação diofantina em inteiros positivos

$$x^2 + y^2 + z^2 = 3xyz.$$

Vamos analisá-la de acordo com o que é apresentado em (MARTINEZ et al., 2011).

É fácil verificar que $(1, 1, 1)$ e $(1, 1, 2)$ são soluções da equação. Além disso, como a equação é simétrica, podemos considerar, sem perda de generalidade, somente as soluções com as coordenadas $x \leq y \leq z$ ordenadas de forma não decrescente.

Assim suponhamos que (x, y, z) é uma solução com $x \leq y \leq z$ com $z > 1$. Fazendo $z = T$, o polinômio quadrático $T^2 - 3xyT + (x^2 + y^2) = 0$ possui duas soluções, pois

$$\Delta = (-3xy)^2 - 4 \cdot 1 \cdot (x^2 + y^2) = 9xy - 4(x^2 + y^2)$$

então temos

$$x_1 = \frac{3xy + \sqrt{9xy - 4(x^2 + y^2)}}{2}$$

$$x_2 = \frac{3xy - \sqrt{9xy - 4(x^2 + y^2)}}{2}$$

Temos que $x_1 + x_2 = 3xy$. Fazendo $x_1 = z$, então $z' = 3xy - z = \frac{x^2+y^2}{z} \in \mathbb{Z} \setminus \{0\}$.

Temos que se $y > 1$ então $z' < y$, e assim (z', x, y) é também uma solução (menor) da equação de Markov. Para isto, suponhamos por contradição que $\frac{x^2+y^2}{z} = z' \geq y$, isto é

$$\frac{x^2 + y^2}{z} \geq y \Rightarrow yz \leq x^2 + y^2 \leq 2y^2$$

em particular $z \leq 2y$. Segue que

$$2y \geq z \Rightarrow 4y^2 \geq z^2 \Rightarrow 5y^2 \geq y^2 + z^2 = 3xyz - x^2 = x(3yz - x) \geq xy(3z - 1)$$

e portanto $5y \geq x(3z - 1)$.

Observemos que se $x \geq 2$, então $5y \geq 2(3z - 1) \geq 5z$ e portanto $x = y = z = 2$, que não é solução, o que é contraditório. Logo $x = 1$ e $\frac{1+y^2}{y} \geq z$, assim $\frac{1}{y} + y = z$, e neste caso $y = 1$ e $z = 2$, o que contradiz $y > 1$, ou $y = z$ e substituindo na equação original temos que $1 + y^2 + y^2 = 3y^2$, o que implica que $z = y = 1$, o que contradiz o fato de $z > 1$.

Do fato anterior, temos que dada uma solução da equação de Markov (x, y, z) com $z \geq 2$ é sempre possível encontrar uma solução menor (z', x, y) e este processo somente termina quando chegamos à solução $(1, 1, 1)$, isto é, estamos gerando uma árvore de soluções:

$$\begin{array}{ccc}
 & (1,1,1) & \\
 & \downarrow & \\
 & (1,1,2) & \\
 & \downarrow & \\
 & (1,2,5) & \\
\swarrow & & \searrow \\
(1,5,13) & & (2,5,29) \\
\swarrow\ \searrow & & \swarrow\ \searrow \\
(1,13,34)\ (5,13,194) & & (2,29,169)\ (5,29,433)
\end{array}$$

Um importante problema em aberto relacionado com a equação de Markov é o *problema da unicidade*, proposto por Frobenius há cerca de 100 anos: para quaisquer inteiros positivos x_1, x_2, y_1, y_2, z com $x_1 \leq y_1 \leq z$ e $x_2 \leq y_2 \leq z$ tais que (x_1, y_1, z) e (x_2, y_2, z) são soluções da equação de Markov temos necessariamente $(x_1, y_1) = (x_2, y_2)$?

Se o problema da unicidade admitir uma solução afirmativa, para cada t real, sua pré-imagem $k^{-1}(t)$ pela função k definida pelos *Espectros de Markov e Lagrange* consistirá de uma única classe de $GL_2(\mathbb{Z})$-equivalência.

3.1.2 Último Teorema de Fermat

Pierre de Fermat, matemático francês do século $XVII$, tinha o costume de fazer anotações nas margens de livros, e uma dessas anotações gerou um dos mais famosos problemas da História da Matemática.

O chamado "Último Teorema de Fermat"foi enunciado nas margens da cópia do livro de Diofanto, e o teorema afirma ser impossível encontrar inteiros positivos x, y, z tais que

$$x^n + y^n = z^n \tag{3.2}$$

quando n é um inteiro maior do que 2.

Fermat afirmou: "encontrei uma demonstração verdadeiramente maravilhosa para isto, mas a margem é demasiado pequena para contê-la".

Ao longo da história muitos casos particulares foram mostrados, mas a demonstração do Último teorema de Fermat somente foi obtida depois de mais de trezentos anos após sua formulação. Tal demonstração, devida a Andrew Wiles e Richard Taylor, insere-se no contexto mais geral da chamada *conjectura de Taniyama-Shimura-Weil* sobre curvas elípticas, que implica a solução do último teorema de Fermat, como conjecturado por G. Frey em 1985 e provado por K. Ribet em 1986.

Para dar uma ideia da dificuldade deste problema, vejamos uma demonstração baseada na prova feita por Leonhard Euler para o caso $n = 3$ e presente em (MARTINEZ et al., 2011). A demonstração original dada por Euler para o caso $n = 3$ é incompleta já que supõe a fatoração única em irredutíveis para extensões de $\mathbb{Z}$.

Lema 3.4. *Todas as soluções de $s^3 = a^2 + 3b^2$ em inteiros positivos tais que $mdc(a, b) = 1$ e s é ímpar são dadas por*

$$s = m^2 + 3n^2, a = m^3 - 9mn^2, b = 3m^2n - 3n^3,$$

com $m + n$ ímpar e $mdc(m, 3n) = 1$.

Demonstração. É fácil verificar que tais números fornecem uma solução da equação e, além disso, $mdc(a, b) = mdc(m(m^2 - 9n^2), 3n(m^2 - n^2)) = mdc(m^2 - 9n^2, m^2 - n^2) = mdc(8n^2, m^2 - n^2) = 1$.

Reciprocamente, suponhamos que (a, b, s) é solução da equação. Seja p um número primo tal que $p|s$. Note que, como $mdc(a, b) = 1$ e s é ímpar, $p \nmid a$, $p \nmid b$ e $p > 3$. Então $a^2 \equiv -3b^2 (mod\ p)$ e como b é invertível módulo p temos

$$\left(\frac{-3}{p}\right) = 1 \Longleftrightarrow p \equiv 1 (mod\ 6)$$

pela lei da reciprocidade quadrática (Apendice A).

Pelo exemplo (2.8) visto anteriormente, sabemos que existem inteiros m_1 e n_1 tais que $p = {m_1}^2 + 3{n_1}^2$, e teremos $p^3 = c^2 + 3d^2$ onde $c = {m_1}^3 - 9m_1{n_1}^2$ e $d = 3{m_1}^2n_1 - 3{n_1}^3$. Note que $mdc(p, m_1) = mdc(p, n_1) = 1$ e $p > 3$ e portanto $mdc(p, c) = mdc(p, d) = 1$, como na demonstração acima de que $mdc(a, b) = 1$.

Procederemos por indução sobre o número de divisores primos de s. Se $s = 1$ o resultado é evidente. O caso em que s tem um divisor primo é exatamente o resultado anterior. Agora suponhamos que o resultado valha para todo s que tenha k fatores primos (não necessariamente distintos). Se s tem $k + 1$ fatores primos, digamos $s = pt$ com p primo ($p > 3$), observemos que

$$t^3p^6 = s^3p^3 = (a^2 + 3b^2)(c^2 + 3d^2) = (ac \pm 3bd)^2 + 3(ad \mp bc)^2. \tag{3.3}$$

Além disso, como

$$(ad + bc)(ad - bc) = (ad)^2 - (bc)^2 = d^2(a^2 + 3b^2) - b^2(c^2 + 3d^2) = p^3(t^3d^2 - b^2),$$

então $p^3|(ad + bc)(ad - bc)$. Se p divide os dois fatores, teremos que $p|ad$ e $p|bc$. Lembre que $mdc(p, c) = mdc(p, d) = 1$, o que implica que $p|a$ e $p|b$, o que contradiz a hipótese $mdc(a, b) = 1$.

Assim, p^3 divide exatamente um dos fatores, e tomando adequadamente os sinais em (3.3) teremos que

$$u = \frac{ac \pm 3bd}{p^3}, v = \frac{ad \mp bc}{p^3}$$

são inteiros tais que $t^3 = u^2 + 3v^2$. Como t tem k fatores primos segue por hipótese de indução que

$$t = {m_2}^2 + 3{n_2}^2, u = {m_2}^3 - 9m_2{n_2}^2, v = 3{m_2}^2n_2 - 3{n_2}^3.$$

Agora, dado que $a = uc + 3vd$ e $b = \pm(ud - vc)$, substituindo t, u, v, c e d em termos de m_i e n_i $(i = 1, 2)$ em s, a e b e fazendo $m = m_1m_2 + 3n_1n_2$, $n = m_1n_2 - m_2n_1$, obteremos o que queríamos demonstrar:

$$a = uc + 3vd$$

$$= (m_2^3 - 9m_2n_2^2)(m_1^3 - 9m_1n_1^2) + 3(3m_2^2n_2 - 3n_2^3)(3m_1^2n_1 - 3n_1^3)$$

$$= m_1^3m_2^3+9m_1^2m_2^2n_1n_2+27m_1m_2n_1^2n_2^2+27n_1^3n_2^3-9(m_1m_2+3n_1n_2)(m_1^2n_2^2-2m_1m_2n_1n_2+m_2^2n_1^2)$$

$$= (m_1m_2 + 3n_1n_2)^3 - 9(m_1m_2 + 3n_1n_2)(m_1n_2 - m_2n_1)^2$$

$$= m^3 - 9mn^2$$

$$b = \pm(ud - vc)$$

$$= \pm[(m_2^3 - 9m_2n_2^2)(3m_1^2n_1 - 3n_1^3) - (3m_2^2n_2 - 3n_2^3)(m_1^3 - 9m_1n_1^2)]$$

$$= \mp[3(m_1^3m_2^2n_2 + 6m_1^2m_2n_1n_2^2 + 9m_1n_1^2n_2^3 - m_1^2m_2^3n_1 - 6m_1m_2^2n_1^2n_2 - 9m_2n_1^3n_2^2)$$

$$-3(m_1^3n_2^3 - 3m_1^2m_2n_1n_2^2 + 3m_1m_2^2n_1^2n_2 - m_2^3n_1^3)]$$

$$= \mp[3(m_1m_2 + 3n_1n_2)^2(m_1n_2 - m_2n_1) - (m_1n_2 - m_2n_1)^3]$$

$$= \mp[3m^2n - 3n^3]$$

e

$$s^3 = a^2 + 3b^2$$

$$= (m^3 - 9mn^2)^2 + 3(3m^2n - 3n^3)^2$$

$$= m^6 + 9m^4n^2 + 27m^2n^4 + 27n^6$$

$$= (m^2 + 3n^2)^3$$

extraindo a raiz cúbida, concluímos que

$$s = m^2 + 3n^2$$

□

Proposição 3.5. *A equação diofantina $x^3 + y^3 = z^3$ não possui soluções inteiras com $xyz \neq 0$.*

Demonstração. Suponhamos que a equação $x^3+y^3 = z^3$ possui uma solução com $x, y, z \neq 0$ e escolhemos esta solução de tal forma que xyz seja mínimo. Como qualquer fator comum de dois destes números é também fator do terceiro, podemos afirmar que x, y, z são primos relativos dois a dois. Em particular, um deles será par.

Note que $x = y$ é impossível pois caso contrário $2x^3 = z^3$ e o expoente da maior potência de 2 do lado direito seria múltiplo de 3, enquanto que do lado esquerdo não. Assim, sem perda de generalidade, podemos assumir que $x > y$.

Suponha primeiro que x e y são ímpares e z par, podemos escrever $x = p + q$ e $y = p - q$ com $p > 0$ e $q > 0$ primos relativos (pois x e y são primos relativos) e de diferente paridade, assim

$$z^3 = x^3 + y^3 = (x + y)(x^2 - xy + y^2)$$

$$= 2p((p + q)^2 - (p + q)(p - q) + (p - q)^2)$$

$$= 2p(p^2 + 3q^2)$$

Portanto $2p(p^2+3q^2)$ é um cubo perfeito. De igual forma, no caso em que z é ímpar e x ou y é par, podemos supor sem perda de generalidade que y é ímpar, e substituindo $z = q + p$ e $y = q - p$ obteremos

$$x^3 = z^3 - y^3$$

$$= 2p((p + q)^2 + (p + q)(q - p) + (q - p)^2)$$

$$= 2p(p^2 + 3q^2)$$

Como p^2+3q^2 é ímpar, digamos $p^2+3q^2 = 2k+1$ e $2p(p^2+3q^2)$ é um cubo perfeito, temos

$$2p(p^2 + 3q^2) = x^3$$

$$2p(2k + 1) = x^3$$

$$p = \frac{x^3}{(4k + 2)}$$

e como x^3 é par, então p é par. Calculando o máximo divisor comum entre p e $p^2 + 3q^2$, obtemos

$$mdc(p, p^2 + 3q^2) = mdc(p, 3q^2) = mdc(p, 3)$$

Portanto há dois casos: $mdc(p, 3) = 1$ e $mdc(p, 3) = 3$.

No primeiro caso, como $2p(p^2 + 3q^2)$ é um cubo perfeito, existem naturais a e b tais que $a^3 = 2p$ e $b^3 = p^2 + 3q^2$. Neste caso sabemos, pelo Lema 3.4, que existem inteiros m e n de diferente paridade e primos relativos tais que

$$b = m^2 + 3n^2, p = m^3 - 9mn^2, q = 3m^2n - 3n^3$$

Logo $a^3 = 2m(m - 3n)(m + 3n)$.

Observemos que os números $2m$, $m-3n$ e $m+3n$ são primos relativos, logo existem inteiros e, f e g tais que $f^3 + g^3 = e^3$. Como $e \cdot f \cdot g = a^3 = 2p \leq x + y < xyz$, teremos uma solução menor, o que contradiz a escolha de x, y, z.

No segundo caso, em que $3|p$, então $p = 3r$ com $mdc(r, q) = 1$, logo

$z^3 = 18r(3r^2 + q^2)$ ou $x^3 = 18r(3r^2 + q^2)$ e portanto existem inteiros positivos a e b tais que $18r = a^3$ e $3r^2 + q^2 = b^3$. De novo, existiriam inteiros m e n tais que

$$b = m^2 + 3n^2, q = m^3 - 9mn^2, r = 3m^2n - 3n^3$$

Daqui segue que $a^3 = 27(2n)(m - n)(m + n)$. De igual forma teremos que os números $2n$, $m - n$ e $m + n$ são primos relativos, portanto existem inteiros positivos e, f

e g tais que

$$2n = e^3, m - n = f^3, m + n = g^3$$

Segue que $e^3 + f^3 = g^3$, que também contradiz a minimalidade da solução (x, y, z).

□

Exemplo 3.6. Demonstrar que a equação $x^2 + 432 = y^3$ não tem soluções racionais diferentes de $(\pm 36, 12)$.

Suponhamos que a equação possui uma solução (a, b) com $b \neq 12$. Como a e b são racionais, então $\frac{a}{36} = \frac{k}{n} \neq \pm 1$ e $\frac{b}{12} = \frac{m}{n} \neq 1$ com $k, m, n \in \mathbb{Z}$.

Seja $u = n + k \neq 0$, $v = n - k \neq 0$ e $w = 2m$. Como

$$u^3 + v^3 - w^3 = 2n^3 + 6nk^2 - 8m^3$$

e $k = \frac{an}{36}$, $m = \frac{bn}{12}$, substituindo temos

$$u^3 + v^3 - w^3 = 2n^3 + \frac{n^3a^2}{6^3} - \frac{n^3b^3}{6^3} = \frac{n^3}{216}(432 + a^2 - b^3) = 0$$

o que gera uma solução não trivial da equação $x^3 + y^3 = z^3$, um absurdo.

4 ALGUMAS SOLUÇÕES DA EQUAÇÃO $p^3 + q^2 = z^3$

Neste capítulo, iremos avaliar a existência e o número de soluções da equação $p^3 + q^2 = z^3$, quando p é um número primo e $q > 1$, baseado nos estudos feitos no artigo de (BURSHTEIN, 2017).

Teorema 4.1. *Suponha que p é primo e $q > 1$. Então a equação $p^3 + q^2 = z^3$ tem exatamente quatro soluções em todas as quais $p = 7$. Em uma solução q é primo, e em todas as outras soluções q é composto.*

Demonstração. Temos

$$p^3 + q^2 = z^3 \Rightarrow q^2 = z^3 - p^3 = (z - p)(p^2 + pz + z^2)$$

Denote $z - p = T$, onde $T \geq 1$. Substituindo $z = p + T$ resulta em

$$q^2 = T(3p^2 + 3pT + T^2)$$

Temos dois casos em que a igualdade anterior pode ser satisfeita:

(i) Quando $T > 1$ e $3p^2 + 3pT + T^2$ são quadrados simultaneamente. Que podemos provar ser impossível:

Suponha que $T > 1$ e $3p^2 + 3pT + T^2$ são quadrados simultaneamente, o que significa que $T = U^2$ e $3p^2 + 3pT + T^2 = V^2$. Então

$$3p^2 + 3pU^2 + (U^2)^2 = V^2 \Rightarrow 3p(p + U^2) = V^2 - (U^2)^2 = (V - U^2)(V + U^2) \quad (4.1)$$

o que indica que p divide pelo menos um dos valores $(V-U^2), (V+U^2)$, o que não é válido. De fato, se $p|(V-U^2)$, denote $pR = V - U^2 \Rightarrow V = pR + U^2$. Então fazendo a substituição em (4.1) temos

$$3p(p+U^2) = (pR+U^2)^2 - (U^2)^2$$

$$3p(p+U^2) = p^2R^2 + 2pRU^2 + (U^2)^2 - (U^2)^2$$

$$3p^2 + 3pU^2 = p^2R^2 + 2pRU^2$$

$$3p^2 + 3pU^2 - p^2R^2 - 2pRU^2 = 0$$

$$p^2(3-R^2) + pU^2(3-2R) = 0$$

$$p^2(R^2-3) + pU^2(2R-3) = 0$$

o que é impossível para todos os valores R. Daí $p \nmid (V-U^2)$.

Se $p|(V+U^2)$, indica $pS = V+U^2$ com $S \in \mathbb{Z}$. Então $V = pS - U^2$. Então fazendo a substituição novamente em (4.1) temos

$$3p^2 + 3pU^2 + (U^2)^2 = V^2$$

$$3p^2 + 3pU^2 + (U^2)^2 = (pS - U^2)$$

$$3p^2 + 3pU^2 + (U^2)^2 = p^2S^2 - 2pSU^2 + (U^2)^2$$

$$0 = p^2(S^2-3) - pU^2(2S+3)$$

$$pU^2(2S+3) = p^2(S^2-3)$$

$$p = U^2 \cdot \left(\frac{2S+3}{S^2-3}\right).$$

Os divisores de p são 1 e p, mas $T > 1$ assim sendo $T = U^2 > 1$ ou $U > 1$. Então segue que

(a) $\frac{U^2}{S^2-3} = 1$ e $2S + 3 = p$, ou

(b) $U = p$ e $\frac{U(2S+3)}{S^2-3} = \frac{p(2S+3)}{S^2-3} = 1$

(c) $U^2 = p$ e $\frac{2S+3}{S^2-3} = 1$

Se (a), então $\frac{U^2}{S^2-3} = 1 \Rightarrow U^2 = S^2 - 3$. Mas $S^2 - U^2 = 3$ tem a única solução $U = 1$ e $S = 2$, o que é impossível.

Se (b), então $\frac{p(2S+3)}{S^2-3} = 1 \Rightarrow p = \frac{S^2-3}{2S+3}$, o que é impossível, pois $\frac{S^2-3}{2S+3} \notin \mathbb{Z}$.

Se (c) $U^2 = p$ e $\frac{2S+3}{S^2-3} = 1 \Rightarrow S \notin \mathbb{Z}$.

Portanto $p \nmid (V + U^2)$, e o caso (i) está completo.

(ii) Quando $T \geq 1$ e $3p^2+3pT+T^2$ não são necessariamente quadrados simultaneamente.

Suponha $T \geq 1$ e $3p^2 + 3pT + T^2$ não são necessariamente quadrados simultaneamente. Na igualdade $q^2 = T(3p^2 + 3pT + T^2)$ fazemos $3p^2 + 3pT + T^2 = TA^2$ para algum valor A que garante que a igualdade é de fato um quadrado, ou seja $q^2 = (TA)^2$.

Então, segue que $T|3p^2$. O valor T pode assumir todos os possíveis divisores de $3p^2$, que são:

$$T = 1, T = 3, T = p, T = 3p, T = p^2, T = 3p^2$$

Os seis casos são considerados separadamente.

- O caso $T = 1$. Substituindo $T = 1$ obtemos $q^2 = 3p^2 + 3p + 1$, do qual

$$q^2 - 1 = (q - 1)(q + 1) = 3p(p + 1). \tag{4.2}$$

Assim sendo, qualquer $p|(q - 1)$ ou $p|(q + 1)$. Observe que $p \neq 2$. Se $p|(q - 1)$, significa $Bp = q - 1$, onde $B \geq 1$. Substituindo $q = Bp + 1$ em (4.2) resulta em

$$q^2 = 3p^2 + 3p + 1 \Rightarrow B^2p^2 + 2Bp + 1 = 3p^2 + 3p + 1,$$

e depois de simplificações implica que

$$p(B^2p + 2B) = p(3p + 3)$$

$$B^2p - 3p = 3 - 2B$$

$$p(B^2 - 3) = 3 - 2B$$

$$p = \frac{3 - 2B}{B^2 - 3}$$

A sentença $\frac{3-2B}{B^2-3}$ é negativa para todos valores $B \geq 1$, e, portanto, é impossível. Portanto $p \nmid (q - 1)$ e $p|(q + 1)$. Se $p|(q + 1)$, significa $Cp = q + 1$ onde $C \geq 1$. Então $q = Cp - 1$ e de (4.2) segue que

$$q^2 = C^2p^2 - 2Cp + 1 = 3p^2 + 3p + 1$$

$$p(C^2p - 2C) = p(3p + 3)$$

$$C^2p - 3p = 3 + 2C$$

$$p(C^2 - 3) = 3 + 2C$$

$$p = \frac{3 + 2C}{C^2 - 3}$$

Sendo assim, o único valor que C pode assumir é $C = 2$. Consequentemente, $C = 2$, então $\frac{3+2\cdot 2}{2^2-3} = 7 = p$. Os valores $p = 7$, $q = 2 \cdot 7 - 1 = 13$ primo, e $z = T + p = 1 + 7 = 8$ forma uma solução da equação $p^3 + q^2 = z^3$. O caso

$T = 1$ está completo.

- O caso $T = 3$. Fazendo a substituição obtemos

$$q^2 = 3(3p^2 + 3p \cdot 3 + 3^2) \Rightarrow q^2 = 9p^2 + 27p + 27 = 3^2(p^2 + 3p + 3)$$

implica que $p^2 + 3p + 3$ deve ser igual a um quadrado, dizemos A^2.

Se $p^2 + 3p + 3 = A^2$, então $A^2 - p^2 = (A - p)(A + p) = 3(p + 1)$. Nós agora mostramos que $3 \nmid (A - p)$ e $3 \nmid (A + p)$, o que implica que $T \neq 3$.

Se $3|(A-p)$, significa $3D = A-p$, onde $D \geq 1$, consequentemente, $3D(A+p) = 3(p+1)$ ou seja, $D(A+p) = p+1$. Mas como $A > p$, esta equação é impossível, logo $3 \nmid (A - p)$.

Se $3|(A + p)$ então $3E = A + p$. Nós temos então que

$p^2+3p+3 = (3E-p)^2 \Rightarrow p^2+3p+3 = 9E^2-6Ep+p^2 \Rightarrow 3E(3E-2p) = 3(p+1)$ ou seja, $E(3E - 2p) = p + 1$. Portanto, $3E^2 - 2Ep = p + 1 \Rightarrow 3E^2 - 1 = 2Ep + p \Rightarrow p(2E + 1) = 3E^2 - 1$ e $p = \frac{3E^2-1}{2E+1}$.

Mas essa fração nunca é igual a um inteiro, e portanto, segue-se que $3 \nmid (A+p)$. Portanto $T \neq 3$. Como consequência imediata, segue-se que para todo primo $p, p^2 + 3p + 3$ nunca é igual a um quadrado.

- No caso $T = p$. Substituindo, nós obtemos $q^2 = p(3p^2 + 3p \cdot p + p^2) = p(7p^2) = 7p^3$, implicando que $p = 7$ e $q^2 = 7^4$. Portanto, os valores $p = 7$, $q = 7^2$ e $z = 2p = 14$ formam uma solução para a equação $p^3 + q^2 = z^3$.

- O caso $T = 3p$. Substituindo $T = 3p$, então $q^2 = 3p(3p^2 + 3p \cdot 3p + (3p)^2) \Rightarrow q^2 = 9p^3 + 27p^3 + 27p^3 = 3^2 7p^3$. Portanto, $p = 7$ e $q^2 = 3^2p^4 = 3^2 7^4$ e os valores $p = 7$, $q = 3 \cdot 7^2$ e $z = 4p = 28$ formam uma solução para a equação $p^3 + q^2 = z^3$.

- O caso $T = p^2$. Substituindo, temos $q^2 = p^2(3p^2+3p\cdot p^2+(p^2)^2 = p^4(3+3p+p^2)$. Segue-se agora que o valor $p^2 + 3p + 3$ deve ser igual a um quadrado. Digamos M^2, então $q^2 = (p^2M)^2$. Mas, $p^2 + 3p + 3 \neq M^2$ como foi mostrado no caso $T = 3$. Portanto $T \neq p^2$.

- No caso $T = 3p^2$. Substituindo, obtemos $q^2 = 3p^2(3p^2 + 3p \cdot 3p^2 + (3p^2)^2) \Rightarrow q^2 = 9p^4 + 27p^5 + 27p^6 = 9p^4(1 + 3p + 3p^2)$. Assim sendo, o valor $3p^2 + 3p + 1$ deve ser igual a um quadrado digamos N^2, para que $q^2 = (3p^2N)^2$.

O valor $3p^2 + 3p + 1$ aparece na igualdade (4.2) do caso $T = 1$, e é de fato igual a um quadrado somente quando $p = 7$. Consequentemente temos $p = 7$, $q = 3p^2(3p^2 + 3p + 1)^{\frac{1}{2}} = 3 \cdot 7^2 \cdot 13$ e $z = p + 3p^2 = p(3p + 1) = 2 \cdot 7 \cdot 11$ que forma uma solução para a equação $p^3 + q^2 = z^3$.

Assim temos que a equação diofantina $p^3 + q^2 = z^3$ tem quatro soluções inteiras, nas quais todas $p = 7$ e em apenas uma delas q é primo:

1. $7^3 + 13^2 = (2^3)^3$
2. $7^3 + (7^2)^2 = (2 \cdot 7)^3$
3. $7^3 + (3 \cdot 7^2)^2 = (2^2 \cdot 7)^3$
4. $7^3 + (3 \cdot 7^2 \cdot 13)^2 = (2 \cdot 7 \cdot 11)^3$

□

5 EQUAÇÕES DIOFANTINAS NA EDUCAÇÃO BÁSICA

Elaboramos como exemplo diante das diversas possibilidades existentes, uma Sequência Didática, onde abordamos a modelagem e resolução de problemas afim de aguçar a curiosidade e desafiar os alunos.

Através do nome Sequência Didática, podemos definir o que representa. A palavra sequência remete a ação de seguir, então podemos dizer que uma Sequência Didática trata-se de um conjunto de atividades sequenciais, sobre determinado tema, que tem o objetivo de ensinar um conteúdo, através de etapas definidas.

Abordando um pouco de História da Matemática, e utilizando como uma das formas de resolução, tentativa e erro, acreditamos que a Sequência Didática desenvolvida possa levar os alunos à valorização dos conteúdos matemáticos estudados e sua aprendizagem, como facilitadores na resolução de problemas práticos.

Considerando que para desenvolver as atividades contidas nesta Sequência Didática seja necessário alguma noção de Álgebra, com relação ao significado e uso de variáveis e incógnitas, seria interessante trabalhá-la com turmas de 7° ou 8° ano do Ensino Fundamental, não se descartando a possibilidade de adaptações e diferentes abordagens do tema nas demais fases do ensino.

5.1 Sequência Didática: Uma abordagem com Equações Diofantinas

Leia a atividade e tente resolver os problemas propostos, utilizando a estratégia que julgar mais adequada. Em seguida, discuta com um colega suas soluções e modos de representar a atividade. Ao final faremos um debate coletivo para compartilharmos

nossos conhecimentos e descobertas.

- **Diofanto de Alexandria**

  Diofanto de Alexandria foi um matemático grego que contribuiu de maneira significativa com a Matemática, com destaque na Álgebra, principalmente com relação a notação e linguagem que utilizamos hoje em dia para resolver problemas. Não sabemos muito de sua vida, mas podemos tirar algumas conclusões através do problema seguinte:

  "... sua infância durou $\frac{1}{6}$ de sua vida; casou-se depois de mais $\frac{1}{7}$; sua barba cresceu depois de $\frac{1}{12}$, e seu filho nasceu 5 anos depois; o filho viveu a metade da idade do pai e o pai morreu quatro anos depois do filho."

  Baseado nas informações acima, tente descobrir com quantos anos Diofanto faleceu.

- **Equações Diofantinas**

  As Equações Diofantinas, nome dado em homenagem a Diofanto, são equações polinomiais com duas ou mais incógnitas que admitem apenas valores inteiros. Elas podem não ter solução, podem ter uma, várias, ou infinitas soluções.

  O problema resolvido anteriormente sobre a idade em que Diofanto de Alexandria faleceu pode ser representado por uma equação diofantina? Porquê?

  Vejamos alguns exemplos de situações que podem ser representadas por equações, e analise se possuem ou não solução **inteira**:

  1. Considere que os ingressos de um cinema custam $R\$9,00$ para estudantes e $R\$15,00$ para o público geral, e que, em certo dia a arrecadação nas bilheterias

desse cinema foi de $R\$246,00$. Quais as possíveis quantidades de estudantes e público geral neste dia?

2. Agora suponha que em outro dia, neste mesmo cinema, a arrecadação foi de $R\$251,00$. Quais as possíveis quantidades de estudantes e público geral neste dia? O que pode ter ocorrido?

- **Equações Diofantinas Lineares com duas incógnitas**

  Existe um resultado que nos permite saber se uma Equação Diofantina Linear com duas incógnitas, como as anteriores, possui ou não solução inteira antes mesmo de as resolvermos.

  Sejam $a, b \in \mathbb{Z} \setminus \{0\}$ e $c \in \mathbb{Z}$. A equação $ax + by = c$ admite solução em números inteiros se, e somente se, $mdc(a, b)|c$.

- **Equações Diofantinas não Lineares**

  As Equações Diofantinas também podem ter termos elevados a potências, como por exemplo a equação

$$a^2 + b^2 = c^2$$

As soluções desta equação são chamadas de Triplas Pitagóricas, por serem possíveis comprimentos dos lados de um triângulo retângulo de acordo com o Teorema de Pitágoras, onde a e b são catetos e c é a hipotenusa.

Sabendo disso, tente descobrir pelo menos três soluções diferentes para esta equação.

- **Soma de Quadrados**

  Existem diversos Teoremas e resultados que provam condições para se obter soluções para algumas Equações Diofantinas. Vamos ver alguns:

  1. **Teorema:** Os únicos números que podem se expressar como soma de dois quadrados são os $n = 2^s d^2 l$, onde s é um número natural e l é um número livre de quadrados tais que seus fatores primos são da forma $4k + 1$.

     Escreva três números que são soma de dois quadrados.

     Agora tente escrever os números que você escolheu na forma como é definida no Teorema e veja se a afirmação é válida nestes casos.

     ---

  2. **Lema:** Se $2m$ é soma de dois quadrados, então m também é soma de dois quadrados, ou seja $2m = x^2 + y^2 \iff m = w^2 + z^2$.

     Teste a afirmação acima. Escolha um número que é soma de dois quadrados e que também seja par. Depois verifique se este número divido por dois também é soma de dois quadrados.

     ---

3. **Teorema:** Todo inteiro positivo n pode se escrever como soma de quatro quadrados.

   O Teorema acima foi comprovado, e portanto, qualquer número inteiro pode ser escrito como soma de quatro números inteiros elevados ao quadrado. Vamos ver alguns exemplos:

   $0 = 0^2 + 0^2 + 0^2 + 0^2$

   $1 = 1^2 + 0^2 + 0^2 + 0^2$

   $2 = 1^2 + 1^2 + 0^2 + 0^2$

   $21 = 4^2 + 2^2 + 1^2 + 0^2$

   $102 = 10^2 + 1^2 + 1^2 + 0^2$

   $155 = 12^2 + 3^2 + 1^2 + 1^2$

   Agora é sua vez. Escreva os números abaixo como soma de quatro quadrados:

   $13 =$ _____

   $35 =$ _____

   $42 =$ _____

   $111 =$ _____

   $107 =$ _____

   $1035 =$ _____

- **Último Teorema de Fermat**

  Agora vamos aumentar um pouco a potência! E para a equação $x^3 + y^3 = z^3$, você consegue encontrar alguma solução?

  _____

  _____

  _____

  Pierre de Fermat, matemático francês do século $XVII$, tinha o costume de fazer anotações nas margens de livros, e uma dessas anotações gerou um dos mais famosos problemas da História da Matemática.

  O chamado "Último Teorema de Fermat"foi enunciado nas margens da cópia do livro de Diofanto, e o teorema afirma ser impossível encontrar inteiros positivos x, y, z tais que $x^n + y^n = z^n$ quando n é um inteiro maior do que 2.

Fermat afirmou saber demonstrar, mas que esta demonstração não caberia nas margens do livro, e a mesma nunca foi encontrada.

Ao longo da história muitos casos particulares foram mostrados por diversos matemáticos, mas a comprovação deste Teorema somente foi obtida depois de mais de trezentos anos após sua formulação.

CONSIDERAÇÕES FINAIS

Verificamos as grandes contribuições de Diofanto e outros matemáticos que se interessaram e contribuíram para o estudo da teoria. Diofanto contribuiu de forma significativa no desenvolvimento da Álgebra, principalmente no que diz respeito a notação algébrica, fazendo uso de abreviações em seus estudos, o que permitiu que se desenvolvesse na forma em que conhecemos hoje em dia, com organização e uso de símbolos.

As Equações Diofantinas vêm sendo estudadas e despertam o interesse de matemáticos a centenas de anos. Com uma breve análise de alguns casos, podemos verificar que além de sua importância teórica, as Equações Diofantinas também podem ser aplicadas em diversas situações do cotidiano.

Propomos também a possibilidade de abordarmos as Equações Diofantinas não só na Educação Superior, como é feito normalmente, mas também na Educação Básica, como um tema para mediar discussões, aguçar a curiosidade e desafiar os alunos a criar suas próprias estratégias e argumentações.

Acreditamos que a elaboração de estratégias através da resolução de problemas tematizados nas Equações Diofantinas podem proporcionar ao aluno melhor compreensão sobre o papel da escrita algébrica como uma ferramenta facilitadora.

Referências Bibliográficas

BRASIL. *Base Nacional Comum Curricular*. Brasília: MEC/Secretaria de Educação Básica, 2018.

BURSHTEIN, N. All the solutions of the diophantine equation $p^3 + q^2 = z^3$. *Annals of Pure and Applied Mathematics*, 2017.

HEFEZ, A. *Aritmética (Coleção PROFMAT)*. Rio de Janeiro: SBM - Sociedade Brasileira de Matemática, 2016.

MARTINEZ, F. B. et al. *Teoria dos números: um passeio com primos e outros números familiares pelo mundo inteiro*. 2. ed. Rio de Janeiro: IMPA, 2011.

O'CONNOR, J. J.; ROBERTSON, E. F. *Diophantus of Alexandria*. 1999. Acessado em: 01/08/2019. Disponível em: ⟨http://www-history.mcs.st-and.ac.uk/Biographies/Diophantus.html⟩.

POMMER, W. M. *Equações Diofantinas Lineares no Ensino Básico: Uma abordagem didáticoepistemológica*. 1. ed. São Paulo: STOA - Universidade de São Paulo, 2013. v. 1.

SOUZA, R. S. *Equações diofantinas lineares, quadráticas e aplicações*. Tese (Mestrado em Matemática) — Universidade Estadual Paulista, Instituto de Geociências e Ciências Exatas, Rio Claro, 2017.

A Lei da Reciprocidade Quadrática

Para melhor compreensão de alguns tópicos abordados no trabalho, segue abaixo alguns resultados importantes.

A.1 Resíduos Quadráticos

Sejam p um primo ímpar e $a, b, c \in \mathbb{Z}$ tal que $mdc(a, p) = 1$. Estamos interessados no estudo das soluções para as congruências da forma

$$x^2 \equiv a \mod p,$$

onde p é um primo ímpar e $mdc(a, p) = 1$.

Definição A.1. Sejam $a \in \mathbb{Z}$ e p um primo ímpar tal que $mdc(a, p) = 1$. Dizemos que a é um **resíduo quadrático** módulo p se a congruência $x^2 \equiv a \mod p$ possui solução. Caso contrário, dizemos que a não é um resíduo quadrático módulo p.

Exemplo A.2. 4 é um resíduo quadrático módulo 5, pois $3^2 \equiv 4 \mod 5$. Mas 2 não é um resíduo quadrático módulo 5, pois esta congruência $x^2 \equiv 2 \mod 5$ não possui solução. De fato, pois se x_0 fosse uma solução de $x^2 \equiv 2 \mod 5$, pelo algoritmo da divisão, $x_0 = 5q + r$ com $0 \leq r < 5$. Assim, $r^2 \equiv (x_0)^2 \equiv 2 \mod 5$, o que é impossível.

Teorema A.3. *Para p primo ímpar e $a \in \mathbb{Z}$ tal que $mdc(a, p) = 1$, a congruência $x^2 \equiv a \mod p$, caso tenha solução, tem exatamente duas soluções incongruentes módulo p.*

Demonstração. Se esta congruência possui uma solução x_0 então $-x_0$ também é uma solução, pois $(-x_0)^2 = (x_0)^2 \equiv a \mod p$. Mostremos então que estas duas soluções x_0 e $-x_0$ são incongruentes módulo p. Suponha que $x_0 \equiv -x_0 \mod p$ então $2x_0 \equiv 0 \mod p$, isto é, $p|2x_0$. Mas como $p > 2$ primo, então $p|x_0$. Como $p|(x_0)^2 - a$, das propriedades

de divisibilidade, segue que $p|a$, contradição, pois $mdc(a,p) = 1$. Mostremos agora que existem apenas duas soluções incongruentes. Seja $y \in \mathbb{Z}$ uma solução de $x^2 \equiv a \mod p$, isto é, $y^2 \equiv a \mod p$. Como x_0 é solução, temos que $(x_0)^2 \equiv y^2 \equiv a \mod p$, ou seja, $(x_0 - y)(x_0 + y) \equiv 0 \mod p$. Logo $p|x_0 - y$ ou $p|x_0 + y$, o que implica que $y \equiv x_0 \mod p$ ou $y \equiv -x_0 \mod p$. □

Exemplo A.4. Vamos determinar todos os resíduos quadráticos módulo 13. Para isto, é suficiente considerarmos os quadrados dos números $1, 2, ..., 12$ que formam um sistema reduzido de resíduos módulo 13.

$$\begin{array}{ll} 1^2 \equiv 1 \mod 13 & 7^2 \equiv 10 \mod 13 \\ 2^2 \equiv 4 \mod 13 & 8^2 \equiv 12 \mod 13 \\ 3^2 \equiv 9 \mod 13 & 9^2 \equiv 3 \mod 13 \\ 4^2 \equiv 3 \mod 13 & 10^2 \equiv 9 \mod 13 \\ 5^2 \equiv 12 \mod 13 & 11^2 \equiv 4 \mod 13 \\ 6^2 \equiv 10 \mod 13 & 12^2 \equiv 1 \mod 13 \end{array}$$

Note que ambas as colunas de congruências figuram apenas os números $1, 3, 4, 9, 10, 12$. Estes são todos os resíduos quadráticos módulo 13. O fato de haver repetição na segunda coluna, é que $(13 - k)^2 \equiv k^2 \mod 13$, para $k \in \{1, 2, 3, 4, 5, 6\}$.

Teorema A.5. *Seja p primo ímpar. Dentre os números $1, 2, ..., p-1$, temos $\frac{p-1}{2}$ resíduos quadráticos e $\frac{p-1}{2}$ que não são.*

Demonstração. Consideremos os quadrados dos números $1, 2, ..., \frac{p-1}{2}$, isto é,

$$1^2, 2^2, 3^2, ..., \left(\frac{p-1}{2}\right)^2.$$

Vamos mostrar que estes quadrados são incongruentes módulo p. Sejam $x, y \in \{1, 2, ..., \frac{p-1}{2}\}$ e suponha que $x^2 \equiv y^2 \mod p$. Logo $x^2 - y^2 = (x + y)(x - y) \equiv 0 \mod p$, e portanto, $p|(x + y)(x - y)$. Como $x + y < p$, segue que $p \nmid (x + y)$. Logo $p|(x - y)$, o que implica que $x \equiv y \mod p$, e portanto, $x = y$. Desta forma, concluímos que todos os quadrados acima são incongruentes módulo p. Agora, observe que se $k \in \{1, 2, ..., \frac{p-1}{2}\}$ então

$$p - k \in \{\frac{p+1}{2}, \frac{p+3}{2}, ..., p-1\}.$$

Logo, como $(p-k)^2 \equiv k^2 \mod p$, segue que os resíduos quadráticos pertencem as classes de congruência que contem os quadrados

$$1^2, 2^2, 3^2, ..., \left(\frac{p-1}{2}\right)^2.$$

Portanto, $\frac{p-1}{2}$ é o número de resíduos quadráticos dentre os números $1, 2, ..., p-1$. Os outros $\frac{p-1}{2}$ não são resíduos quadráticos. □

Proposição A.6. *Seja $p > 2$ um número primo. Então a congruência $x^2 \equiv -1 \mod p$ possui solução se, e somente se, $p \equiv 1 \mod 4$.*

Demonstração. ($\Rightarrow$) Suponha que a congruência $x^2 \equiv -1 \mod p$ tenha solução. Então existe $b \in \mathbb{Z}$ tal que $b^2 \equiv -1 \mod p$. Disto segue que $mdc(p, b) = 1$ e logo, do Pequeno Teorema de Fermat, obtemos

$$1 \equiv b^{p-1} = (b^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \mod p$$

e daí $(-1)^{\frac{p-1}{2}} = 1$, pois $-1 \not\equiv 1 \mod p$. Disto, segue que $\frac{p-1}{2}$ é par, isto é, $\frac{p-1}{2} = 2k$, ou ainda, $p - 1 = 4k$. Portanto $p \equiv 1 \mod 4$.

($\Leftarrow$) Suponha que $p \equiv 1 \mod 4$. Pelo Teorema de Wilson, $(p-1)! \equiv -1 \mod p$. Mas observe que

$$-1 \equiv (p-1)! = 1 \cdot 2 \cdot ... \cdot \frac{p-1}{2} \cdot \frac{p+1}{2} \cdot ... \cdot (p-2) \cdot (p-1) = \prod_{j=1}^{\frac{p-1}{2}} j(p-j) \mod p.$$

Como $j(p-j) \equiv -j^2 \mod p$, temos

$$-1 \equiv \prod_{j=1}^{\frac{p-1}{2}} j(p-j) \equiv \prod_{j=1}^{\frac{p-1}{2}} (-j^2) = (-1)^{\frac{p-1}{2}} \left(\prod_{j=1}^{\frac{p-1}{2}} j\right)^2 = (-1)^{\frac{p-1}{2}} \left[\left(\frac{p-1}{2}\right)!\right]^2 \mod p.$$

Mas $p \equiv 1 \mod 4$, logo $(-1)^{\frac{p-1}{2}} = 1$, e portanto

$$\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv -1 \mod p.$$

Portanto, $x = \left(\frac{p-1}{2}\right)!$ é uma solução da congruência $x^2 \equiv -1 \mod p$. □

Definição A.7. Seja p um primo ímpar e $a \in \mathbb{Z}$ tal que $mdc(a,p) = 1$. O **símbolo de Legendre** é o símbolo $\left(\frac{a}{p}\right)$ definino por

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & , \text{ se } a \text{ é resíduo quadrático módulo } p \\ -1 & , \text{ se } a \text{ não é resíduo quadrático módulo } p \end{cases}$$

Exemplo A.8. Do exemplo A.4, segue que

$$\left(\frac{1}{13}\right) = \left(\frac{3}{13}\right) = \left(\frac{4}{13}\right) = \left(\frac{9}{13}\right) = \left(\frac{10}{13}\right) = \left(\frac{12}{13}\right) = 1,$$

enquanto

$$\left(\frac{2}{13}\right) = \left(\frac{5}{13}\right) = \left(\frac{6}{13}\right) = \left(\frac{7}{13}\right) = \left(\frac{8}{13}\right) = \left(\frac{11}{13}\right) = -1.$$

Teorema A.9 (Critério de Euler)**.** *Seja p um primo ímpar e $a \in \mathbb{Z}$ tal que $mdc(a,p) = 1$. Então*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p.$$

Demonstração. Primeiro, observe que como $mdc(a,p) = 1$, então do Pequeno Teorema de Fermat, $a^{p-1} \equiv 1 \mod p$. Como p é ímpar, então $p-1$ é par, e logo

$$a^{p-1} - 1 = \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \mod p.$$

Assim, $p \mid \left(a^{\frac{p-1}{2}} - 1\right)$ ou $p \mid \left(a^{\frac{p-1}{2}} + 1\right)$, isto é, $a^{\frac{p-1}{2}} \equiv \pm 1 \mod p$.

- Suponha que a é um resíduo quadrático módulo p. Assim, existe $b \in \mathbb{Z}$ tal que $b^2 \equiv a \mod p$ e $mdc(b,p) = 1$, pois $mdc(a,p) = 1$. Então, segue do Pequeno Teorema de Fermat, que

$$a^{\frac{p-1}{2}} \equiv \left(b^2\right)^{\frac{p-1}{2}} = b^{p-1} \equiv 1 \mod p \Rightarrow \left(\frac{a}{p}\right) = 1 \equiv a^{\frac{p-1}{2}} \mod p.$$

- Suponha agora que a não seja um resíduo quadrático módulo p. Para todo $r \in \{1, 2, ..., p-1\}$, a congruência linear $rx \equiv a \mod p$ possui exatamente uma solução $s \in \{1, 2, ..., p-1\}$, pois $\{1, 2, ..., p-1\}$ é um sistema completo de resíduos módulo p. Mais ainda, temos que $r \not\equiv s \mod p$, pois se $r \equiv s \mod p$, teríamos que $a \equiv rs \equiv s^2 \mod p$, ou seja, a seria um resíduo quadrado, contradição! Logo, podemos rescrever

o conjunto $\{1, 2, ..., p-1\}$ como

$$\{1, 2, ..., p-1\} = \{r_1, s_1, r_2, s_2, ..., r_{\frac{p-1}{2}}, s_{\frac{p-1}{2}}\}$$

tal que $r_i s_i \equiv a \mod p$ para $1 \leq i \leq \dfrac{p-1}{2}$. Assim, do Teorema de Wilson,

$$-1 \equiv (p-1)! = \prod_{i=1}^{\frac{p-1}{2}} r_i s_i \equiv \prod_{i=1}^{\frac{p-1}{2}} a = a^{\frac{p-1}{2}} \mod p \Rightarrow \left(\frac{a}{p}\right) = -1 \equiv a^{\frac{p-1}{2}} \mod p.$$

□

Exemplo A.10. Seja $p = 29$ e $a = 3$. Então

$$\left(\frac{3}{29}\right) \equiv 3^{\frac{29-1}{2}} = 3^{14} \mod 29$$

Como $3^3 \equiv -2 \mod 29$ e $3^{14} = (3^3)^4 \cdot 3^2$, então

$$\left(\frac{3}{29}\right) \equiv 3^{14} = \left(3^3\right)^4 \cdot 3^2 \equiv (-2)^4 \cdot 9 = 16 \cdot 9 = 144 \equiv 28 \equiv -1 \mod 29$$

Portanto 3 não é um resíduo quadrático módulo 29.

Proposição A.11. *Seja p um primo ímpar e $a, b \in \mathbb{Z}$ tais que $mdc(a, p) = mdc(p, b) = 1$. Então valem*

a) Se $a \equiv b \mod p$ então $\left(\dfrac{a}{p}\right) = \left(\dfrac{b}{p}\right)$.

b) $\left(\dfrac{a^2}{p}\right) = 1$

c) $\left(\dfrac{ab}{p}\right) = \left(\dfrac{a}{p}\right) \cdot \left(\dfrac{b}{p}\right)$

Demonstração. Os itens (a) e (b) são consequências imediatas da definição e do critério de Euler. Mostremos o item (c).

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) \mod p.$$

Logo $p\left|\left(\frac{ab}{p}\right)-\left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right)\right.$, mas $p>2$ e $\left|\left(\frac{ab}{p}\right)-\left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right)\right|\leq 2$, então

$$\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right).$$

□

Exemplo A.12. $\left(\frac{12}{29}\right)=\left(\frac{2^2\cdot 3}{29}\right)=\left(\frac{2^2}{29}\right)\cdot\left(\frac{3}{29}\right)=\left(\frac{3}{29}\right)=-1$

O critério de Euler já nos fornece uma maneira de identificar resíduos quadráticos. Veremos agora dois resultados muito fortes aos quais facilitarão a identificação de resíduos quadráticos.

Teorema A.13. *Para p um primo ímpar, temos*

$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}=\begin{cases}1 & , \text{ se } p\equiv\pm 1 \mod 8\\ -1 & , \text{ se } p\equiv\pm 3 \mod 8\end{cases}$$

Teorema A.14 (Reciprocidade Quadrática de Gauss)**.** *Sejam p e q dois primos ímpares distintos. Então*

$$\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right)=(-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}.$$

Exemplo A.15. 1) Verifiquemos se 2 é um resíduo quadrático módulo 1019.

Como $1019\equiv 3 \mod 8$, segue que $\left(\frac{2}{1019}\right)=-1$. Portanto, 2 não é um resíduo quadrático módulo 1019.

2) Verifiquemos se 31 é um resíduo quadrático módulo 1997.

Pela Reciprocidade quadrática de Gauss, temos

$$\left(\frac{31}{1997}\right)=(-1)^{\left(\frac{31-1}{2}\right)\left(\frac{1997-1}{2}\right)}\left(\frac{1997}{31}\right)=\left(\frac{1997}{31}\right).$$

Mas $1997\equiv 13 \mod 31$, logo

$$\left(\frac{1997}{31}\right)=\left(\frac{13}{31}\right)=(-1)^{\left(\frac{31-1}{2}\right)\left(\frac{13-1}{2}\right)}\left(\frac{31}{13}\right)=\left(\frac{31}{13}\right).$$

Como $31\equiv 5 \mod 13$, segue que

$$\left(\frac{31}{13}\right)=\left(\frac{5}{13}\right)=(-1)^{\left(\frac{5-1}{2}\right)\left(\frac{13-1}{2}\right)}\left(\frac{13}{5}\right)=\left(\frac{13}{5}\right).$$

Mas $13 \equiv 3 \mod 5$, e então, pelo critério de Euler,

$$\left(\frac{13}{5}\right) = \left(\frac{3}{5}\right) \equiv 3^{\frac{5-1}{2}} = 3^2 \equiv -1 \mod 5.$$

Portanto,

$$\left(\frac{31}{1997}\right) = -1.$$