Universidade Federal de Mato Grosso
Instituto de Ciências Exatas e da Terra
Departamento de Matemática

Gerando
Ternos Pitagóricos

Nivaldo Vitor da Silva

Mestrado Profissional em Matemática: PROFMAT/SBM

Orientador: **Prof. Dr. Martinho da Costa Araújo**

Trabalho financiado pela Capes

Cuiabá - MT

setembro de 2014

Gerando
Ternos Pitagóricos

Este exemplar corresponde à redação final da dissertação, devidamente corrigida e defendida por Nivaldo Vitor da Silva e aprovada pela comissão julgadora.

Cuiabá, 26 de setembro de 2014.

Prof. Dr. Martinho da Costa Araújo
Orientador

Banca examinadora:

Prof. Dr. Martinho da Costa Araújo
Prof. Dr. José de Arimatéia Fernandes
Prof. Dr. Reinaldo de Marchi

Dissertação apresentada ao curso de Mestrado Profissional em Matemática – PROFMAT, desenvolvido pela Sociedade Brasileira de Matemática na Universidade Federal de Mato Grosso, como requisito parcial para obtenção do título **de Mestre em Matemática**.

Dados Internacionais de Catalogação na Fonte.

S586g Silva, Nivaldo Vitor da.
Gerando Ternos Pitagóricos / Nivaldo Vitor da Silva. -- 2014
xi, 91 f. : il. ; 30 cm.

Orientador: Martinho da Costa Araújo.
Dissertação (mestrado profissional) - Universidade Federal de Mato Grosso, Instituto de Ciências Exatas e da Terra, Programa de Pós-Graduação em Matemática, Cuiabá, 2014.
Inclui bibliografia.

1. Teorema de Pitágoras. 2. Ternos Pitagóricos. 3. Ternos Pitagóricos Primitivos. 4. Propriedades dos Ternos Pitagóricos. I. Título.

Ficha catalográfica elaborada automaticamente de acordo com os dados fornecidos pelo(a) autor(a).

Dissertação de Mestrado defendida em 26 de setembro de 2014 e aprovada pela banca examinadora composta pelos Professores Doutores

_____

Prof. Dr. Martinho da Costa Araújo

_____

Prof. Dr. José de Arimatéia Fernandes

_____

Prof. Dr. Reinaldo de Marchi

Dedicatória

À Minha Família, Amigos e Amigas.

Agradecimentos

Primeiramente quero agradecer a **DEUS**, por ser essencial em minha vida, por me iluminar e proteger sempre, por propiciar momentos felizes como este em minha vida e também por me amparar nos momentos de angústia. Agradecer por me dotar da determinação necessária para eu perseverar até o final desta etapa tão importante de minha vida.

Agradecer a meus pais **Benedito Francisco da Silva** e **Nilce Romoalda de Campos Silva**, que são meus maiores ídolos, nos quais eu sempre me inspirei. De maneira simples e clara, sempre souberam me transmitir os valores éticos essencias ao ser humano. Desde criança sempre recebi deles todo carinho, incentivo e apoio necessários à minha formação. Sei que palavras são insuficientes para descrever por completo o que eles significam para mim, porém, quero registrar aqui que, tudo que tenho e sou, devo a **eles**.

A minha querida irmã **Dulcinéia**, pela sua grandiosa generosidade para comigo, meu irmão **Dirceu** (*IN MEMORIAN*), que tanto me ensinou em tão pouco tempo de vida. Aos meus amados sobrinhos **Ronaldo, Darlene, Douglas** e meu cunhado **Domingos**, que também me deram todo suporte necessário e estiveram verdadeiramente ao meu lado o tempo todo, me motivando e incentivando durante esta longa caminhada.

Aos meus professores (as) do Profmat e demais professores (as) que tive ao longo da vida, em especial, **Prof. Dr. Martinho da Costa Araújo**, que desde minha graduação vem contribuindo de forma ímpar com a minha formação profissional e ainda se fazendo um grande e valioso amigo fora da sala de aula.

A todos os meus colegas de mestrado, dos quais me orgulho e sou grato. De modo especial quero agradecer a **Gilliard, Gledson, Jessé, Luiz Fernando, Marco Antonio(Bazuca)** e **Ricardo**, que além de colegas, entraram para minha seleta e valiosa lista de amigos.

Agradecer ainda, carinhosamente, a todos os demais amigos(as) que me apoiaram muito desde o início deste mestrado e compreenderam a minha ausência, até mesmo em ocasiões especiais em suas vidas durante estes dois anos. O apoio incondicional de vocês fez toda a diferença mais uma vez em minha vida.

Para finalizar, quero agradecer a todos os meus parentes, colegas de profissão, alunos (as) e todas as demais pessoas que de alguma forma me apoiaram e que torceram por mim durante esse tempo. Também à **CAPES** que me auxiliou financeiramente durante esse período.

"É bom olhar para trás e admirar a vida que soubemos fazer."

(Nando Reis).

Resumo

O referido trabalho pretende mostrar que os *Ternos Pitagóricos* podem ser inclusos no currículo ainda nos anos iniciais do Ensino Básico Regular, uma vez que, há várias maneiras de se obter tais ternos, propiciando assim, uma maior e melhor compreensão do teorema de Pitágoras e dos números inteiros, temas de grande relevância no Ensino Fundamental e Médio. Para isso, apresentar-se-á inicialmente alguns dos principais tópicos da Aritmética, os quais servirão como ferramentas para o desenvolvimento da pesquisa, em seguida, os resultados que contemplam de fato o objetivo específico deste trabalho, que é o estudo dos ternos pitagóricos. Inicia-se com a definição de *Ternos Pitagóricos* e *Ternos Pitagóricos Primitivos*, na sequência, demonstram-se fórmulas que geram os ternos, bem como um dispositivo prático que também gera infinitos ternos pitagóricos. E ainda, destacam-se algumas das principais propriedades dos ternos pitagóricos, bem como, particularidades do terno $(3, 4, 5)$. Por fim serão apresentadas aplicações sobre os ternos pitagóricos.

Palavras chave: Teorema de Pitágoras; Ternos pitagóricos; Ternos Pitagóricos Primitivos; Propriedades dos Ternos Pitagóricos.

Abstract

Such work intends to show that the *Pythagorean Triplets* can be included in the curriculum even in the years of Regular Basic Education, since there are several ways to obtain such triplets,thus enabling a greater and better understanding of the Pythagorean theorem and the integers, topics of great relevance in primary and secondary education. To do so, it shall be presented initially some of the main topics of Arithmetic, which will serve as tools for the development of research, Then the results that come in fact the specific objective of this work, which is the study of the pythagorean triplets. It starts with a definition *Pytagorean Triplets* and *Primitive Pythagorean Triplets*, following, shows up formulas which generate the Triplets as well as a practical device that also generates infinite Pythagorean Triplets. And yet, it highlights some of the main properties of pythagorean triplets, as well as particularities of the the triple $(3, 4, 5)$. Finally will be presented pythagorean triplets applications.

Key words: Pythagorean Theorem; Pythagorean Triplet; Primitive Pythagorean Triplets; Pythagorean Triplet Properties.

Sumário

Introdução

> "A Aritmética é o corpo que segura as lindas penas da matemática."
>
> (Liping Ma)

Pitágoras (569a.c - 480a.c) nasceu na Ilha de Samos, motivo pelo qual é conhecido hoje como Pitágoras de Samos. Outro grande personagem da história da matemática dessa época, foi Tales, que nasceu 50 anos antes de Pitágoras, em Miletto, cidade próxima de Samos. Foi a partir das ideias desses dois grandes personagens que a Matemática se inicia como ciência e pode se desenvolver enormemente nos séculos seguintes.

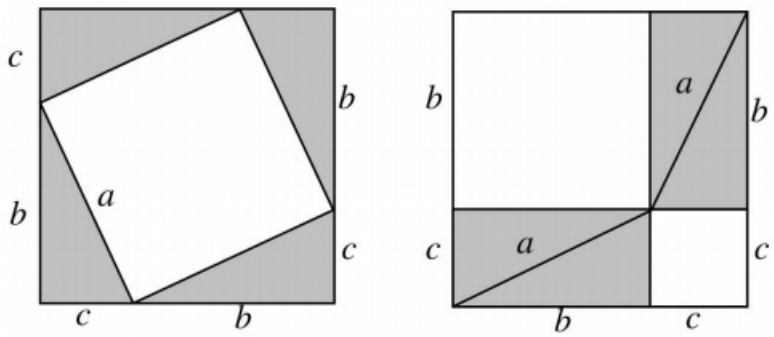
Obcecado pelo conhecimento matemático, Pitágoras viajou bastante em busca do aprimoramento desse conhecimento. Ele passou pelo Egito, Babilônia e talvez na Índia. Em cada região observou e registrou os conhecimentos matemáticos e as ideias religiosas locais.

Voltando à Grécia, fundou uma escola em Crotona, cidade hoje situada ao sudeste da Itália. Na verdade, essa escola era uma sociedade secreta, dedicada principalmente ao estudo da Matemática e da Filosofia. Como todos os documentos daquela época se perderam, tudo o que sabemos veio através de referências de outros autores que viveram séculos depois. Por isso, Pitágoras é uma figura obscura na história da Matemática e, para dificultar ainda mais as coisas, a sua escola, além de secreta, era comunitária, ou seja, todo o conhecimento e todas as descobertas eram comuns, pertenciam a todos. Assim, não sabemos sequer se foi o próprio Pitágoras que descobriu o Teorema que leva seu nome, pois era comum naquela época dar todo crédito de uma descoberta ao mestre.

O Teorema de Pitágoras é um dos mais belos e importantes teoremas da Matemática de todos os tempos, e se destaca sobre os demais teoremas, a ponto de acumular centenas de demonstrações. Em 1940, por exemplo, o americano E.S. Loomis publicou 370 demonstrações, hoje, esse número é bem superior.

O enunciado deste famoso teorema é: *Em qualquer triângulo retângulo, a soma das áreas dos quadrados que têm como lados cada um dos catetos, é igual à área do quadrado cujo lado é a hipotenusa.*

Dentre todas as demonstrações existentes, apresentaremos aqui a mais clássica de todas, que pode ter sido inclusive, a que os pitagóricos imaginaram.



Na figura da esquerda, retiramos do quadrado de lado $b + c$ quatro triângulos iguais ao triângulo retângulo dado, restando um quadrado de lado a. Na figura da direita, retiramos também do quadrado de lado $b + c$ os quatro triângulos iguais ao triângulo retângulo dado, restando um quadrado de lado b e um quadrado de lado c. Logo, a área do quadrado de lado a é igual à soma das áreas dos quadrados cujos lados medem b e c.

Se c é a medida da hipotenusa e se a e b são as medidas dos catetos, o enunciado do Teorema de Pitágoras equivale a afirmar que $a^2 + b^2 = c^2$.

Demonstra-se também que a recíproca do Teorema de Pitágoras é verdadeira, ou seja, se a, b e c são números reais positivos que satisfazem a equação $a^2 + b^2 = c^2$, então, a, b e c são lados de um triângulo retângulo em que a hipotenusa mede c. Se ainda, a, b e c forem números inteiros positivos, diremos que a, b e c são números pitagóricos ou que (a, b, c) é um triângulo pitagórico, quando estes representarem, respectivamente, as medidas dos catetos e da hipotenusa de um triângulo retângulo, ou ainda que (a, b, c) é um terno pitagórico.

Historicamente, o Teorema de Pitágoras é ligado aos Ternos Pitagóricos, assunto que foi motivo de interesse de grandes matemáticos, como por exemplo: Pitágoras, Platão, Euclides, Diofanto e Fermat. Porém, alguns ternos pitagóricos eram conhecidos, antes mesmo do próprio teorema de pitágoras. O terno $(3, 4, 5)$, por exemplo, seria facilmente encontrado aritmeticamente e isto poderia ter incentivado uma busca por outros ternos.

Na Babilônia, foram encontrados e decifrados muitos tabletes de barro datados do período entre 1800 a 1600a.C. Hoje eles se encontram em diversos museus. Um deles chamado Plimpton 322 (o nome faz referência a G.A. Plimpton da Universidade de Columbia, catalogada pelo número de 322) está na Universidade de Columbia e o fragmento que foi preservado mostra uma tabela de 15 linhas e 3 colunas de números.

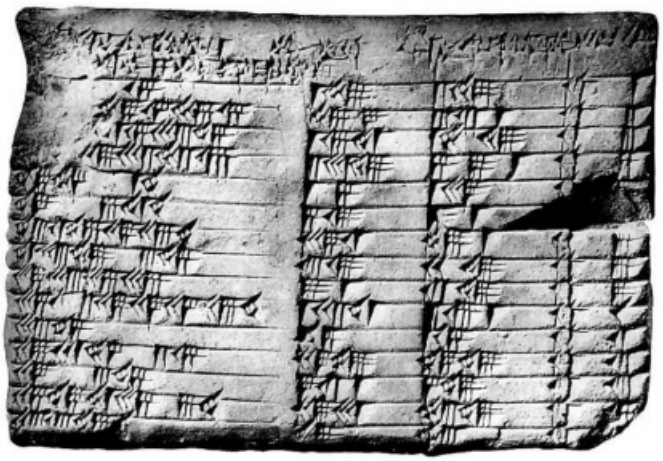


Figura 1: Plimpton 322

Os pesquisadores descobriram que esta tabela continha ternos pitagóricos. Como o que restou é apenas um pedaço de um tablete, que deveria fazer parte de um conjunto de tabletes, não se sabe como esses números foram encontrados. Porém, uma pista de que os babilônios conheciam alguma forma de encontrar esses números, está em um tablete guardado hoje no Museu Britânico. Nesse tablete está escrito o seguinte:

4 é o comprimento.

5 é a diagonal.

Qual é a altura?

4 vezes 4 dá 16.

5 vezes 5 dá 25.

Tirando 16 de 25 o resto é 9.

Quantas vezes devo tomar para ter 9?

3 vezes 3 dá 9.

3 é a altura.

Isto mostra, sem dúvida, que os babilônios tinham conhecimento da relação entre os lados de um triângulo retângulo com medidas inteiras, comprovando assim, que historicamente os Ternos Pitagóricos surgiram antes do Teorema de Pitágoras, no entanto, passou a receber este nome por se tratar de um caso particular deste teorema.

O triângulo de lados $\sqrt{2}$, $\sqrt{7}$ e 3 é retângulo? Sim, pois $(\sqrt{2})^2 + (\sqrt{7})^2 = 3^2$.

Durante toda a história antiga até hoje, temos curiosidades em encontrar triângulos retângulos cujos lados são medidos por números inteiros. O mais conhecido e notável desses triângulos é o que tem os lados com medidas iguais a $3, 4$ e 5, mas você sabia que os triângulos com medidas iguais $44, 117$ e 125 ou $372, 925$ e 997 também são retângulos? Nossa curiosidade nos leva às seguintes perguntas: Como encontrar triângulos retângulos cujos lados tenham medidas inteiras? Quantos desses ternos existem? Quais são as propriedades que esses ternos possuem?

Nosso trabalho tem como propósito responder a estas e outras perguntas, proporcionando aos professores(as) de Matemática do Ensino Fundamental, principalmente, e também aos estudantes de Matemática e demais interessados pelo assunto, uma maior compreensão dos Ternos Pitagóricos no que diz respeito às fórmulas que geram tais ternos, assim como outros resultados importantes. Para atingir os objetivos citados acima, faremos primeiramente, um breve estudo dos principais tópicos de aritmética, culminando, posteriormente, com o estudo dos Ternos Pitagóricos. Sendo assim, organizamos nosso trabalho da seguinte maneira:

No Capítulo 1, apresentaremos alguns dos resultados mais importantes da Aritmética, sendo que grande parte dos textos foram embasados no livro *Elementos de Aritmética*, Hefez [2011]. Esses resultados servirão como ferramentas para o desenvolvimento do capítulo posterior.

No Capítulo 2, apresentaremos inicialmente, a definição de Ternos Pitagóricos e Ternos Pitagóricos Primitivos, em seguida, algumas fórmulas e um dispositivo prático que geram infinitos Ternos Pitagóricos, algumas de suas propriedades, e por fim particularidades do Terno Pitagórico $(3, 4, 5)$.

No Capítulo 3, apresentaremos algumas aplicações dos Ternos Pitagóricos.

Capítulo 1

Noções de Aritmética

Neste capítulo apresentaremos alguns dos principais tópicos da Aritmética dos Inteiros, eles servirão como fundamentação teórica deste trabalho e serão imprescindíveis para o desenvolvimento do segundo capítulo deste trabalho.

1.1 Tópicos de Aritmética dos Inteiros

Nesta seção faremos um breve apanhado dos conceitos de Aritmética dos inteiros que serão úteis para este trabalho. Sendo assim, muitas definições e resultados interessantes ficarão de fora deste texto, por não serem necessários ao desenvolvimento do trabalho.

Começaremos nossa abordagem representando o conjunto dos inteiros não negativos por $\mathbb{Z}_+ = \mathbb{N} = \{0, 1, 2, 3, 4, 5, ...\}$.

Observação 1.1.1 . *Sabemos que o número* 0*(zero) é incluído no conjunto dos números naturais por alguns autores e por outros não, dependendo da conveniência. Quando quisermos excluir o* 0*(zero) desse conjunto, utilizamos o asterisco* $(*)$*. Desse modo,* $\mathbb{Z}_+^* = \mathbb{N}^* = \{1, 2, 3, 4, 5, ...\}$.

1.2 Subtração

Dados dois inteiros positivos a e b com $a < b$, sabemos que existe um inteiro positivo c tal que $b = a + c$. Neste caso, definimos o número b *menos* a, denotado por

$b - a$, como sendo o número c. Em símbolos:

$$b - a = c.$$

Dizemos que c é o resultado da *subtração* de a por b.

Portanto, temos por definição

$$c = b - a \iff b = a + c.$$

No universo dos números inteiros positivos, nem sempre existe a subtração de dois números; só existe $b - a$ quando $a \leq b$.

Note que $a - a = 0$ para todo $a \in \mathbb{Z}_+$, e que, por definição, $(b - a) + a = b$.

Exemplo 1.2.1 . *Exemplos numéricos de subtração em* $\mathbb{Z}_+$*:*

i) $8 - 5 = 3$*;*

ii) $3 - 2 = 1$*;*

iii) $8 - 3 = 5$*;*

iv) $(8 - 5) - 2 = 3 - 2 = 1$*;*

v) $8 - (5 - 2) = 8 - 3 = 5$.

Os dois últimos exemplos mostram que a subtração não é associativa.

Proposição 1.2.1 . *Sejam* $a, b, c \in \mathbb{Z}_+$*. Se* $a \leq b$*, então*

$$c \cdot (b - a) = c \cdot b - c \cdot a.$$

Demonstração: Note que, se $b \geq a$, então $c \cdot b \geq c \cdot a$, o que nos diz que $c \cdot b - c \cdot a$ está bem definido.

Suponha agora que $b - a = d$, logo $b = a + d$. Multiplicando por c ambos os membros desta última igualdade, obtemos $c \cdot b = c \cdot (a + d) = c \cdot a + c \cdot d$, o que implica

$$c \cdot d = c \cdot b - c \cdot a.$$

Substituindo d por $b - a$ na igualdade acima, obtemos

$$c \cdot (b - a) = c \cdot b - c \cdot a.$$

■

Exemplo 1.2.2 . *Exemplos numéricos da Proposição acima* ($Proposição$1.2.1) :

i) $5 \cdot (4 - 1) = 5 \cdot 4 - 5 \cdot 1$;

ii) $3 \cdot (7 - 7) = 3 \cdot 7 - 3 \cdot 7$.

1.2.1 Princípio da Indução

Embora esses próximos conceitos possam ser extendidos, com algumas hipóteses adicionais, a todo o conjunto dos números inteiros, será suficiente para este texto apresentarmos como segue.

Axioma 1.2.1 (Princípio da Indução) *Seja $\mathcal{A}$, um subconjunto não-vazio de $\mathbb{Z}_+^*$. Se:*

i) $1 \in \mathcal{A}$;

ii) $n + 1 \in \mathcal{A}$ *sempre que* $n \in \mathcal{A}$.

Então $\mathcal{A} = \mathbb{Z}_+^*$.

Usaremos este Axioma para demonstrar a seguinte afirmação.

Observação 1.2.1 . *O Princípio da Indução também é válido para o conjunto $\mathbb{Z}_+$.*

Teorema 1.2.1 (Princípio da Boa Ordenação) . *Todo subconjunto de $\mathbb{N}^*$, não-vazio possui um menor elemento.*

Demonstração: Sejam $I_n = \{p \in \mathbb{N};\ 1 \leq p \leq n\}$ e $\mathcal{X} \subset \mathbb{N}^*$, um conjunto formado pelos elementos $n \in \mathbb{N}^*$ tais que $I_n \subset \mathbb{N}^* - \mathcal{A}$.

Se $1 \in \mathcal{A}$, então claramente 1 é o menor elemento de $\mathcal{A}$.

Agora se $1 \notin \mathcal{A}$, então $1 \in \mathcal{X}$, tendo em vista que $I_1 = \{1\} \subset \mathbb{N}^* - \mathcal{A}$. Porém $\mathcal{X} \neq \mathbb{N}^*$, pois $\mathcal{A} \neq \emptyset$ e $\mathcal{X} \subset \mathbb{N}^*$.

Logo o princípio da indução não pode ser aplicado a $\mathcal{X}$, o que implica que o item (ii) do axioma 1.2.1 não vale em $\mathcal{X}$, isto é: existe um $n_0 \in \mathcal{X}$ tal que $n_0 + 1 \notin \mathcal{X}$.

Assim como $I_n \subset \mathbb{N}^* - \mathcal{A}$, temos que todos os números inteiros de 1 a n_0 pertencem a $\mathcal{X}$ e como $n_0 + 1 \notin \mathcal{X}$, temos que $n_0 + 1 \in \mathcal{A}$ e $I_n = \mathcal{X}$.

Portanto $a = n_0 + 1$ é o menor elemento de $\mathcal{A}$. ■

Na realidade o Princípio da Indução e o Princípio da Boa Ordenação (PBO) são afirmações equivalentes, e nesse sentido poderíamos ter assumido o PBO como axioma e o utilizado para demonstrar o Princípio da Indução.

O resultados acima nos fornece métodos para demonstrar e até enunciar algumas definições em matemática. Veja o exemplo abaixo.

Exemplo 1.2.3 . *Exemplo de demonstração pelo Princípio da Indução:*

Mostrar que $s_n = 1 + 2 + 3 + 4 + ... + n = \dfrac{n(n+1)}{2}$ *é válida para todo número inteiro positivo.*

Demonstração: *Lançando mão do princípio da indução, provaremos inicialmente o item* (i) *isto é, se* $n = 1$ *então* $s_1 = \dfrac{1 \cdot 2}{2}$.

De fato $s_1 = 1 = \dfrac{1 \cdot 2}{2}$.

Agora para provar (ii)*, supomos que* $s_k = 1 + 2 + 3 + 4 + ... + k = \dfrac{k(k+1)}{2}$*, para um certo* $k \in \mathbb{N}^*$ *e vamos mostrar que a expressão vale também para* $k + 1$*, isto é,* $s_{k+1} = 1 + 2 + 3 + 4 + ... + k + (k+1) = \dfrac{(k+1)[(k+1)+1]}{2}$.

De fato:

$$\begin{aligned} s_{k+1} = 1 + 2 + 3 + 4 + ... + k + (k+1) &= \frac{k(k+1)}{2} + (k+1) \\ &= \frac{k^2 + k + 2k + 2}{2} \\ &= \frac{k(k+1) + 2(k+1)}{2} \\ &= \frac{(k+1)(k+2)}{2} = \frac{(k+1)[(k+1)+1]}{2}. \end{aligned}$$

Conluímos por indução que $s_n = 1+2+3+4+...+n = \dfrac{n(n+1)}{2},\ \forall n \in \mathbb{Z}_+^*$. ■

Os conceitos abordados nesta seção, são conceitos inerentes à caracterização do conjunto dos números naturais formulada por Giuseppe Peano em 1889, onde figura o Axioma da Indução.

1.3 Divisão nos Inteiros Positivos

Como a divisão de um número inteiro positivo por outro nem sempre é possível, expressa-se esta possibilidade através da relação de divisibilidade.

Quando não existir uma relação de divisibilidade entre dois números, veremos que, ainda assim, será possível efetuar uma "divisão com resto pequeno", chamada de *divisão euclidiana*. O fato de sempre ser possível efetuar tal divisão é responsável por inúmeras propriedades dos inteiros positivos, das quais apresentaremos as principais.

1.3.1 Divisibilidade

Dados dois números inteiros positivos a e b com $a \neq 0$, diremos que a divide b, escrevendo $a|b$, quando existir $c \in \mathbb{Z}_+$ tal que $b = a \cdot c$. Neste caso, diremos também que a é um *divisor* ou um *fator* de b ou, ainda que b um *múltiplo* de a.

Observe que a notação $a|b$ não representa nenhuma operação em $\mathbb{Z}_+$, nem representa uma fração. Trata-se de uma sentença que diz ser verdade que existe c tal que $b = a \cdot c$. A negação dessa sentença é representado por $a \nmid b$, significando que não existe nenhum número inteiro positivo c tal que $b = a \cdot c$.

Exemplo 1.3.1 . *Exemplos numéricos:*

i) $1|0$, *lê-se:* 1 *divide* 0 (*zero*)*;*

ii) $2|0$, *lê-se:* 2 *divide* 0 (*zero*)*;*

iii) $1|6$, *lê-se:* 1 *divide* 6*;*

iv) $2|6$, *lê-se:* 2 *divide* 6*;*

v) $3|6$, *lê-se:* 3 *divide* 6*;*

vi) $6|6$, *lê-se:* 6 *divide* 6*;*

vii) $4 \nmid 6$, *lê-se:* 4 *não divide* 6*;*

viii) $2 \nmid 5$, *lê-se:* 2 *não divide* 5.

Suponha que $a|b$ e seja $c \in \mathbb{Z}_+$ tal que $b = ac$. O número inteiro positivo c é chamado de *quociente* de b por a e denotado por $c = \dfrac{b}{a}$.

Exemplo 1.3.2 . *Exemplos numéricos:*

i) $\frac{0}{1} = 0$*;*

ii) $\frac{0}{2} = 0$*;*

iii) $\frac{6}{1} = 6$*;*

iv) $\frac{6}{2} = 3$*;*

v) $\frac{6}{3} = 2$*;*

vi) $\frac{6}{6} = 1$.

Proposição 1.3.1 . *Sejam* $a, b \in \mathbb{Z}_+^*$ *e* $c \in \mathbb{Z}_+$. *Temos*

i) $1|a$ *,* $a|a$ *e* $a|0$.

ii) *Se* $a|b$ *e* $b|c$ *, então* $a|c$.

Demonstração:

i) Isto decorre das igualdades $a = 1 \cdot a$, $a = a \cdot 1$ e $a \cdot 0 = 0$.

ii) Se $a|b$ e $b|c$ implica que existem $f, g \in \mathbb{Z}_+$, tais que $b = a \cdot f$ e $c = b \cdot g$.

Substituindo o valor de b da primeira equação na outra, obtemos
$c = b \cdot g = (a \cdot f) \cdot g = a \cdot (f \cdot g)$ o que mostra que $a|c$.

■

Observação 1.3.1 . *O item* **i)** *da proposição acima nos diz que todo número inteiro é divisível por* 1 *e, se não nulo, por si mesmo.*

Proposição 1.3.2 . *Se* $a, b, c, d \in \mathbb{Z}_+$ *, com* $a \neq 0$ *e* $c \neq 0$*, então* $a|b$ *e* $c|d \Rightarrow a \cdot c|b \cdot d$.

Demonstração: Se $a|b$ e $c|d$, então $\exists$ $f, g \in \mathbb{Z}_+$, $b = a \cdot f$ e $d = c \cdot g$. Portanto, $b \cdot d = (a \cdot c)(f \cdot g)$, logo, $a \cdot c|b \cdot d$. ■

Em particular, se $a|b$, então $a \cdot c|b \cdot c$, para todo $c \in \mathbb{Z}_+^*$.

Proposição 1.3.3 . *Sejam a, b, $c \in \mathbb{Z}_+$, com $a \neq 0$, tais que $a|(b+c)$. Então $a|b \Leftrightarrow a|c$.*

Demonstração: Como $a|(b+c)$, existe $f \in \mathbb{Z}$ tal que $b+c = f \cdot a$.

Agora , se $a|b$, exite $g \in \mathbb{Z}_+$ tal que $b = a \cdot g$. Juntando as duas igualdades acima, temos

$$a \cdot g + c = f \cdot a = a \cdot f,$$

donde segue-se que $a \cdot f > a \cdot g$, e, consequentemente, $f > g$. Portanto, da igualdade acima e da Proposição 1.2.1 , obtemos

$$c = a \cdot f - a \cdot g = a \cdot (f - g),$$

o que implica que $a|c$, já que $(f-g) \in \mathbb{Z}+$.
A prova da outra implicação é totalmente análoga . ■

Proposição 1.3.4 . *Se $a, b, c \in \mathbb{Z}_+$, com $a \neq 0$, e $x, y \in \mathbb{Z}_+$ são tais que $a|b$ e $a|c$, então $a|(xb+yc)$; e se $xb \geq yc$, então $a|(xb-yc)$.*

Demonstração: $a|b$ e $a|c$ implicam que existem $f, g \in \mathbb{Z}_+$ tais que $b = af$ e $c = ag$. logo,

$$xb \pm yc = x(af) \pm y(ag) = a(xf \pm yg),$$

o que prova o resultado, pois, nas condições dadas, $(xf \pm yg) \in \mathbb{Z}_+$. ■

Definição 1.3.1 *Sendo a, $n \in \mathbb{Z}_+$, definimos:*

$$\begin{cases} a^0 = 1, \ se \ \ a \neq 0; \\ a^1 = a; \\ a^n = \underbrace{a \cdot a \cdot a \cdot ... \cdot a}_{n \ fatores}, \ se \ \ n > 1. \end{cases}$$

Na potência a^n, o número a é chamado de **base** da potência e o número n é chamado de **expoente**.

Proposição 1.3.5 . *Sejam $a, b, n \in Z_+$, com $a > b > 0$. Temos que $a - b$ divide $a^n - b^n$.*

Demonstração: Vamos provar isto por indução sobre n.

É óbvio que a afirmação é verdadeira para $n = 0$, pois $a - b$ divide $a^0 - b^0 = 0$.

Suponhamos, agora, que $(a-b)|(a^n - b^n)$. Escrevamos

$$a^{n+1} - b^{n+1} = aa^n - ba^n + ba^n - bb^n = (a-b)a^n + b(a^n - b^n).$$

Como $(a-b)|(a-b)$ e, por hipótese, $(a-b)|(a^n-b^n)$, decorre da igualdade acima e da Proposição 1.3.4 que $(a-b)|(a^{n+1}-b^{n+1})$. Estabelecendo o resultado para todo $n \in \mathbb{Z}_+$. ■

Exemplo 1.3.3 . *Exemplos de divisibilidade utilizando a Proposição 1.3.5:*

i) $9|10^n - 1$, *para todo* $n \in \mathbb{Z}_+$, *pois, podemos reescrever* $9|10^n - 1$ *como* $10 - 1|10^n - 1^n$, *que satisfaz a proposição acima.*

ii) $8|3^{2n} - 1$, *para todo* $n \in \mathbb{Z}_+$, *pois, podemos reescrever* $8|3^{2n} - 1$ *como* $9 - 1|9^n - 1^n$, *que satisfaz a proposição acima.*

Proposição 1.3.6 . *Sejam* $a, b, n \in \mathbb{Z}_+$ *com* $a + b \neq 0$. *Então* $a + b$ *divide* $a^{2n+1} + b^{2n+1}$.

Demonstração: Vamos provar isto também por indução sobre n.

A afirmação é, obviamente, verdade para $n = 0$, pois $a + b$ divide $a^1 + b^1 = a + b$.

Suponhamos, agora, que $(a + b)|(a^{2n+1} + b^{2n+1})$. Escrevamos

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

Como $(a + b)|(a^2 - b^2)$ e, por hipótese, $(a + b)|(a^{2n+1} + b^{2n+1})$, decorre das igualdades acima e da Proposição 1.3.4 que $(a + b)|(a^{2(n+1)+1} + b^{2(n+1)+1})$. Estabelecendo, assim, o resultado para todo $n \in \mathbb{Z}_+$. ■

Exemplo 1.3.4 . *Exemplos de divisibilidade utilizando a Proposição 1.3.6:*

i) $6|5^{2n+1} + 1$, *para todo* $n \in \mathbb{Z}_+$, *pois, podemos reescrever* $6|5^{2n+1} + 1$ *como* $5 + 1|5^{2n+1} + 1^{2n+1}$, *que satisfaz a proposição acima.*

ii) $14|3^{4n+2} + 5^{2n+1}$, *para todo* $n \in \mathbb{Z}_+$, *pois, podemos reescrever* $14|3^{4n+2} + 5^{2n+1}$ *como* $9 + 5|9^{2n+1} + 5^{2n+1}$ $(3^{4n+2} = 3^{2(2n+1)} = 9^{2n+1})$, *que satisfaz a proposição acima.*

Proposição 1.3.7 . *Sejam* $a, b, n \in \mathbb{Z}_+$ *com* $a \geq b > 0$. *Temos que* $a+b$ *divide* $a^{2n} - b^{2n}$.

Demonstração: Novamente usaremos indução sobre n. A afirmação é verdade para $n = 0$, pois $a+b$ divide $a^0-b^0 = 0$. Suponhamos, agora, que $(a+b)|(a^{2n}-b^{2n})$. Escrevamos

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

Como $(a+b)|(a^2-b^2)$ e, por hipótese, $(a+b)|(a^{2n}-b^{2n})$, decorre das igualdades acima e da Proposição 1.3.4 que $(a+b)|(a^{2(n+1)+1} + b^{2(n+1)+1})$. Estabelecendo, desse modo, o resultado para todo $n \in \mathbb{Z}_+$. ■

Exemplo 1.3.5 . *Exemplos de divisibilidade utilizando a Proposição 1.3.7:*

i) $13|9^{2n}-2^{4n}$, *para todo* $n \in \mathbb{Z}_+$, *pois, podemos reescrever* $13|9^{2n}-2^{4n}$ *como* $9+4|9^{2n}-4^{2n}$ $(2^{4n} = 2^{2\cdot 2n} = 4^{2n})$, *que satisfaz a proposição acima.*

ii) $53|7^{4n}-2^{4n}$, *para todo* $n \in \mathbb{Z}_+$, *pois, podemos reescrever* $53|7^{4n}-2^{4n}$ *como* $49+4|49^{2n}-4^{2n}$ $(7^{4n} = 7^{2\cdot 2n} = 49^{2n}$ *e* $2^{4n} = 2^{2\cdot 2n} = 4^{2n})$, *que satisfaz a proposição acima.*

1.3.2 Divisão Euclidiana

Mesmo quando um número inteiro positivo a não divide o inteiro positivo b, Euclides nos seus *Elementos* utiliza, sem enunciar explicitamente, o fato de que é sempre possível efetuar a divisão de b por a, com resto. Este resultado, cuja demostração damos abaixo, não só é um importante instrumento na obra de Euclides, como também é um resultado central da teoria da Aritmética dos inteiros.

Teorema 1.3.1 . *Sejam* a *e* b *dois números inteiros positivos com* $0 < a < b$. *Existem dois únicos números naturais* q *e* r *tais que*

$$b = a \cdot q + r, com \quad r < a.$$

Demonstração: Sejam a e b inteiros positivos com $0 < a < b$.
Considere, os números

$$b,\ b-a,\ b-2a,\ b-3a,\ \cdots,\ b-n\cdot a,\ \cdots$$

Considere agora, $S = \{b,\ b-a,\ b-2a,\ b-3a,\ \cdots,\ b-n\cdot a,\ \cdots\}$, pelo Princípio da Boa Ordem (Teorema 1.2.1), o conjunto S tem um menor elemento $r = b - q\cdot a$. Vamos provar que r tem propriedade requerida, ou seja, que $r < a$.

Se $a|b$, então $r = 0$ e nada mais temos a provar. Se, por outro lado, $a \nmid b$, então $r \neq 0$, e, portanto, basta mostrar que não pode ocorrer $r > a$. De fato, se isto ocorresse, existiria um número natural $c < r$ tal que $r = c + a$. Consequentemente, sendo $r = c + a = b - qa$, teríamos $c = b - (q + 1) \cdot a \in S$, com $c < r$, contradição com o fato de r ser o menor elemento de S.

Portanto, temos que $b = a \cdot q + r$ com $r < a$, o que prova a existência de q e r.

Agora vamos mostrar a unicidade. Note que, dados dois elementos distintos de S, a diferença entre o maior e o menor desses elementos, sendo um múltiplo de a, é pelo menos a. Logo, se $r = b - a \cdot q$ e $r' = b - a \cdot q'$, com $r < r' < a$, teríamos $r' - r \geq a$, o que acarretaria $r' \geq r + a \geq a$, absurdo. Portanto, $r = r'$, daí segue-se que $b - a \cdot q = b - a \cdot q'$, o que implica que $a \cdot q = a \cdot q'$ e, portanto, $q = q'$. ■

Nas condições do teorema acima, os números q e r são chamados, respectivamente, de *quociente* e de *resto* da divisão de b por a. A demonstração do teorema fornece um algoritmo para calcular o quociente e o resto da divisão de um número natural por outro, através de subtrações sucessivas .

Exemplo 1.3.6 . *Vamos achar o quociente e o resto da divisão de 19 por 5 .*
Considere as diferenças sucessivas : $19 - 5 = 14,\ 19 - 2 \cdot 5 = 9,\ 19 - 3 \cdot 5 = 4 < 5$.
Isto nos dá $q = 3$ *e* $r = 4$.

1.3.3 Máximo Divisor Comum

Definição 1.3.2 . *Dados dois inteiros não negativos a e b, chama-se* ***máximo divisor comum de*** *a* ***e*** *b o inteiro positivo d, que satisfaz as seguintes condições:*

1) *Se $a = b = 0$ então $d = 0$;*

2) *Se $a \neq 0$ ou $b \neq 0$ então d é caracterizado pelas propriedades:*

i) $d \mid a$ e $d \mid b$;

ii) Para cada $x \in \mathbb{Z}_+^*$, se $x \mid a$ e $x \mid b$ então $x \mid d$. Neste caso, temos $x \leq d$.

Observação 1.3.2 . *Se d é o máximo divisor comum de a e b, escrevemos $d = mdc(a, b)$. De maneira mais geral podemos definir $mdc(a_1, a_2, ..., a_n)$ para $a_1, a_2, ..., a_n \in \mathbb{Z}_+$.*

Exemplo 1.3.7 . *Os divisores positivos comuns de* 24 *e* 84 *são* $1, 2, 3, 6$ *e* 12. *Portanto,* $mdc(24, 84) = 12$. *Analogamente, olhando os conjuntos de divisores positivos comuns dos números* 35 *e* 45, 17 *e* 25, 0 *e* 8 **e** 9 *e* 15, *concluímos que* $mdc(35, 45) = 5$, $mdc(17, 25) = 1$, $mdc(0, 8) = 8$ *e* $mdc(9, 15) = 3$.

Definição 1.3.3 . *Dois inteiros positivos* a *e* b *são ditos* ***primos entre si*** *ou* ***relativamente primos*** *quando* $mdc(a, b) = 1$.

Exemplo 1.3.8 *Como* $mdc(1, 4) = mdc(3, 5) = mdc(12, 25) = mdc(14, 15) = 1$, *temos que* 1 *e* 4, 3 *e* 5, 12 *e* 25, 14 *e* 15, *são, respectivamente, primo entre si.*

A proposição seguinte garante a existência do $mdc(a, b)$ em $\mathbb{Z}_+$, para a e b não simultaneamente nulos. Além disso, fornece uma caracterização extremamente útil para esse $mdc(a, b)$.

Proposição 1.3.8 . *Sejam* a *e* b *números inteiros positivos, não simultaneamente nulos. Então, existe* $d = mdc(a, b)$ *em* $\mathbb{Z}_+$. *Além disso,*

$$d = mdc(a, b) = \min\{ma + nb > 0;\ m, n \in \mathbb{Z}_+\}.$$

Demonstração: Consideremos o conjunto $\mathcal{L} = \{ma + nb > 0;\ m, n \in \mathbb{Z}_+\} \subset \mathbb{Z}_+$. Inicialmente, note que $\mathcal{L} \neq \emptyset$. De fato, como $a \neq 0$ ou $b \neq 0$, concluímos que o inteiro $a + b > 0$ pertence a $\mathcal{L}$. Além disso, é fácil ver que $\mathcal{L}$ é limitado inferiormente. Logo, pelo Princípio da Boa Ordenação, existe $d = \min \mathcal{L}$.

Resta mostrar que $d = mdc(a, b)$.

Com efeito, por um lado, como $d \in \mathcal{L}$, podemos escrever $d = m_0a + n_0b > 0$, com $m_0, n_0 \in \mathbb{Z}_+$. Por outro lado, efetuando a divisão euclidiana de a por d, obtemos $t, r \in \mathbb{Z}_+$ tais que $a = dt + r$, com $0 \leq r < d$. Daí:

$$r = a - dt = a - (m_0a + n_0b)t = (1 - m_0t)a + (n_0t)b. \tag{1.1}$$

Isso nos permite concluir que $r = 0$. De fato, se fosse $r > 0$, teríamos $r \in \mathcal{L}$, o que não pode ocorrer, uma vez que isso implicaria em $r < d = \min \mathcal{L}$. Em vista de (1.1), e do fato que $r = 0$, podemos concluir que $a = dt$, e, portanto, $d \mid a$.

Um raciocínio análogo (efetuando a divisão euclidiana de b por d) nos permite concluir que $d \mid b$. Logo, $d \mid a$ e $d \mid b$, e a condição i) da definição de mdc está demonstrada.

Para mostrarmos que a condição ii) também ocorre, seja $x \in \mathbb{Z}$ tal que $x \mid a$ e $x \mid b$. Então, existem $u, v \in \mathbb{Z}$ tais que $a = ux$ e $b = vx$. Devemos provar que $x \mid d$.

Com efeito, uma vez que $d \in \mathcal{L}$, podemos escrever $d = m_0 a + n_0 b$, com $m_0, n_0 \in \mathbb{Z}_+$. Daí:

$$d = m_0 a + n_0 b = m_0(ux) + n_0(vx) = (m_0 u + n_0 v)x,$$

o que significa que $x \mid d$, como queríamos. ■

Corolário 1.3.1 . *Sejam $a, b \in \mathbb{Z}_+$ e $d = mdc(a, b)$. Então, existem $r, s \in \mathbb{Z}$ tais que $d = ra + sb$. Em particular, se $a, b \in \mathbb{Z}_+$ são primos entre si, então existem $r, s \in \mathbb{Z}_+$ tais que $ra + sb = 1$.*

Demonstração: Segue imediatamente do Teorema anterior. ■

Lema 1.3.1 (**Lema de Euclides**). *Sejam $a, b, n \in \mathbb{Z}_+$ com $a < na < b$. Se existir $mdc(a, b - na)$, então $mdc(a, b)$ existe e*

$$mdc(a, b) = mdc(a, b - na).$$

Demonstração: Seja $d = (a, b - na)$. Como $d|a$ e $d|(b - na)$, segue que d divide $b = b - na + na$. Logo d é um divisor comum de a e b. Suponha agora que c seja um divisor comum de a e b; logo, c é um divisor comum de a e $b - na$ e portanto, $c|d$. Isso prova que $d = mdc(a, b)$. ■

Observação 1.3.3 . *Com a mesma técnica usada na prova do Lema de Euclides, pode-se provar que, para todos $a, b, n \in \mathbb{Z}_+$,*

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

ou que, se $na > b$, então

$$mdc(a, b) = mdc(a, na - b).$$

O Lema de Euclides é efetivo para calcular *mdc*, tanto de valores numéricos como de expessões literais, conforme veremos no exemplo a seguir.

Exemplo 1.3.9 . *Veremos abaixo, alguns exemplos de mdc obtidos através da aplicação do* **Lema de Euclides***:*

i) $mdc(45, 51) = mdc(45, 6 + 1 \cdot 45) = mdc(45, 6) = mdc(3 + 7 \cdot 6, 6) = mdc(3, 6) = 3.$

ii) $mdc(372, 162) = mdc(48 + 2 \cdot 162, 162) = mdc(48, 162) = mdc(48, 18 + 3 \cdot 48) =$
$= mdc(48, 18) = mdc(12 + 2 \cdot 18, 18) = mdc(12, 18) = mdc(12, 6 + 1 \cdot 12) =$
$= mdc(12, 6) = 6.$

iii) $mdc(n, 2n + 1) = mdc(n, 1 + 2 \cdot n) = mdc(n, 1) = 1$, *para todo* $n \in \mathbb{Z}_+$.

iv) $mdc(2n + 1, 9n + 4) = mdc\,(2n + 1, n + 4 \cdot (2n + 1)) = mdc(2n + 1, n) =$
$= mdc(n + 1 + 1 \cdot n, n) = mdc(n + 1, n) = mdc(1 + 1 \cdot n, n) = mdc(1, n) = 1$, *para todo* $n \in \mathbb{Z}_+$.

Proposição 1.3.9 . *Dados inteiros a, b e c, se* $a \mid bc$ *e a e b são primos entre si, então* $a \mid c$.

Demonstração: Como a e b são primos entre si, pelo Corolário 1.3.1 existem inteiros r e s, tais que $ra + sb = 1$. Logo, multiplicando a igualdade acima por c obtemos $rac + sbc = c$. Assim, $a \mid rac$ e $a \mid sbc$ (pois $a \mid bc$). Logo $a \mid (rac + sbc)$, e portanto $a \mid c$. ■

Proposição 1.3.10 . *Dados inteiros a, b não-nulos. Se* $d = mdc(a, b)$ *então* $\frac{a}{d}$ *e* $\frac{b}{d}$ *são primos entre si.*

Demonstração: De fato, se $d = mdc(a, b)$ então, pelo Corolário 1.3.1, existem inteiros r e s tais que $d = ra + sb$ e como $d \mid a$ e $d \mid b$ temos que $1 = r \cdot \frac{a}{d} + s \cdot \frac{b}{d}$.

O que implica que $\frac{a}{d}$ e $\frac{b}{d}$ são primos entre si. ■

Proposição 1.3.11 . *Dados* $a, b, c \in \mathbb{Z}_+^*$, *se* $b|a$ *e* $c|a$, *então* $\frac{bc}{mdc(b,c)}|a$.

Demonstração: De fato, temos que $a = nb = mc$ para alguns $n, m \in \mathbb{Z}_+^*$.

$$\text{Logo,} \qquad nb = mc \Rightarrow n\frac{b}{mdc(b,c)} = m\frac{c}{mdc(b,c)}.$$

Pela Proposição 1.3.10 temos que $mdc\left(\frac{b}{mdc(b,c)}, \frac{c}{mdc(b,c)}\right) = 1$, o que implica pela proposição 1.3.9 que $\frac{b}{mdc(b,c)}|m$, que implica $\left(c \cdot \frac{b}{mdc(b,c)}\right)|(c \cdot m)$.

Como $c \cdot \frac{b}{mdc(b,c)} = \frac{bc}{mdc(b,c)}$ e $c \cdot m = a$,

$$\frac{bc}{mdc(b,c)}|a.$$

■

Apresentaremos a seguir uma proposição bastante importante, pois ela nos garante a existência da extensão do *mdc* para três ou mais números inteiros positivos, mostrando que nestes casos, calcula-se o *mdc* formando sucessivos pares a partir dos números dados inicialmente, ou seja, calcula-se o *mdc* dos dois primeiros números e em seguida efetua-se o *mdc* do número encontrado com o próximo número, formando-se um novo par, repete-se este procedimente até que forme o último par, obtendo assim, o *mdc* dos números tomados inicialmente. Em outras palavras, a proposição abaixo nos mostra que para calcular o $mdc(a_1, a_2, ..., a_n)$ podemos usar recursivamente o Algoritmo de Euclides.

Proposição 1.3.12 . *Dados números inteiros positivos* $a_1, a_2, ..., a_n$*, existe o seu mdc e*

$$mdc(a_1, a_2, ..., a_n) = mdc(a_1, a_2, ..., mdc(a_{n-1}, a_n)).$$

Demonstração: Vamos provar a proposição por indução sobre $n(\geq 2)$. Para $n = 2$, sabemos que o resultado é válido. Suponha que o resultado é válido para n. Para mostrar que o resultado é válido para $n + 1$, basta mostrar que

$$mdc(a_1, a_2, ..., a_n, a_{n+1}) = mdc(a_1, a_2, ..., mdc(a_n, a_{n+1})),$$

pois isso provará também a existência.

Seja $d = mdc(a_1, a_2, ..., mdc(a_n, a_{n+1}))$. Logo, $d|a_1, d|a_2, ..., d|a_{n-1}$ e $d|mdc(a_n, a_{n+1})$. Portanto, $d|a_1, d|a_2, ..., d|a_{n-1}$ e $d|a_{n+1}$.

Por outro lado, seja c um divisor comum de $a_1, a_2, ..., a_n, a_{n+1}$; logo, c é um divisor comum de $a_1, a_2, ..., a_{n-1}$, e $mdc(a_n, a_{n+1})$; e, portanto, $c|d$. ■

Exemplo 1.3.10 . *Exemplos de mdc de três ou mais números:*

i) $mdc(6, 10, 14) = mdc\,(mdc(6, 10), 14) = mdc(2, 14) = 2$. *Logo,* $mdc(6, 10, 14) = 2$.

ii) $mdc(10, 15, 35) = mdc\,(mdc(10, 15), 35) = mdc(5, 35) = 5$. *Logo,*
$mdc(10, 15, 35) = 5$.

iii) $mdc(12, 18, 27) = mdc\,(mdc(12, 18), 27) = mdc(6, 27) = 3$. *Logo,*
$mdc(12, 18, 27) = 3$.

iv) $mdc(4, 16, 36, 84) = mdc\,(mdc(4, 16), 36, 84) = mdc(4, 36, 84) = mdc\,(mdc(4, 36), 84) =$
$= mdc(4, 84) = 4$. *Logo,* $mdc(4, 16, 36, 84) = 4$.

v) $mdc(4, 5, 20, 60) = mdc\,(mdc(4, 5), 20, 60) = mdc(1, 20, 60) = mdc\,(mdc(1, 20), 60) =$
$= mdc(1, 60) = 1$. *Logo,* $mdc(4, 5, 20, 60) = 1$.

vi) $mdc(8, 12, 15, 24, 96) = mdc\,(mdc(8, 15), 12, 24, 96) = mdc(1, 12, 24, 96) =$
$= mdc\,(mdc(1, 12), 24, 96) = mdc(1, 24, 96) = mdc\,(mdc(1, 24), 96) =$
$= mdc(1, 96) = 1.$
Logo, $mdc(8, 12, 15, 24, 96) = 1$.

Observação 1.3.4 *Se* $a_1, a_2, ..., a_k, ..., a_{k'}, ..., a_n$ *são inteiros positivos e* $mdc(a_k, a_{k'}) = 1$*, então* $mdc(a_1, a_2, ..., a_k, ..., a_{k'}, ..., a_n) = 1$*, pois,* $mdc(1, a) = 1$*, para todo* $a \in \mathbb{Z}_+$*. Este fato está evidenciado nos dois últimos exemplos acima.*

1.3.4 Números Primos

Abordaremos agora, um dos conceitos mais importantes da Matemática, os *números primos*. Esses números desempenham um papel fundamental na Matemática, pois como veremos logo adiante, todo inteiro positivo maior que 1, é um *número primo*, ou pode ser escrito como um produto de fatores *primos*. Além disso, eles estão associados a muitos problemas famosos cujas soluções têm resistido aos esforços de várias gerações de matemáticos.

No entando, nos limitaremos aqui ao estudo de algumas das principais proposições relacionadas aos *números primos*, bem como ao **Teorema Fundamental da Aritmética** e um breve estudo sobre dois *números primos especiais*, que são *os Primos de Fermat e os Primos de Mersenne*.

Definição 1.3.4 . *Um número inteiro positivo* $p \neq 0$ *é chamado* ***primo*** *quando:*

i) $p \neq 1$*;*

ii) *Os únicos divisores de* p *são* 1 *e* p*.*

Note que, pela definição acima podemos afirmar que: $p > 1$ é primo se, e somente se, seus únicos divisores positivos são 1 e p.

Um número inteiro positivo $n \notin \{0, 1\}$ que não é primo, é chamado **composto**. Isto significa que n possui um divisor $x \neq 0$ com $x < n$, tal que $n = q \cdot x$, $q \in \mathbb{Z}_+^*$.

Provaremos agora uma proposição que é consequência imediata da definição de número primo. Na verdade este resultado que provaremos é equivalente a tal definição, sendo em muitos textos utilizado como definição.

Proposição 1.3.13 . *Sejam a, b e p números inteiros positivos com p primo. Se $p|ab$, então $p|a$ ou $p|b$.*

Demonstração: Para esta demonstração suponhamos que p é um número primo tal que $p|ab$ e $p \nmid a$, com isso mostraremos que $p \mid b$.

De fato se $p \nmid a$ então $mdc(a, p) = 1$ e pelo Corolário 1.3.1 existem inteiros r e s, tais que $ra + sp = 1$.

Multiplicando ambos os membros da igualdade acima por b, temos: $rab + spb = b$.

E como $p|ab$, temos que $p|(rab + spb)$. Logo $p|b$.

■

Por fim enunciaremos e demonstraremos o principal teorema desta seção que permite decompor um número inteiro em um produto de fatores primos, como dito anteriormente.

Corolário 1.3.2 . *Sejam p, $a_1, a_2, ..., a_n$ números inteiros com $n \geq 2$ e p primo.*

Se $p|(a_1 \cdot a_2 \cdots a_n)$ então $p|a_i$ para algum índice $i \in \{1, 2, ..., n\}$.

Demonstração: A demonstração se faz por indução sobre n. ■

Teorema 1.3.2 (Teorema Fundamental da Aritmética) . *Todo inteiro positivo $n \neq 0$ pode ser escrito na forma:*

$$n = u \cdot p_1 \cdot p_2 \cdot p_3 \cdots p_k \tag{1.2}$$

onde $u \in \{-1, 1\}$ e $p_1 \leq p_2 \leq p_3 \leq ... \leq p_k$ são primos. Além disso essa expressão é única.

Demonstração: A demonstração se faz utilizando o segundo Princípio da Indução sobre n.

Supondo então que todo número inteiro positivo m, com $1 \leq m < n$ pode ser escrito da forma acima como produto de números primos (hipótese de indução). Afirmamos que n também pode.

De fato, se n é primo, nada temos para fazer. Mas se n é composto, então existem inteiros m_1 e m_2, com $1 \leq m_1 < n$ e $1 \leq m_2 < n$, tais que $n = m_1 \cdot m_2$. Logo pela hipótese de indução existem $q_1 \leq q_2 \leq q_3 \leq ... \leq q_r$ e $q'_1 \leq q'_2 \leq q'_3 \leq ... \leq q'_s$ primos positivos tais que:

$$m_1 = q_1 \cdot q_2 \cdot q_3 \cdots q_r \quad e \quad m_2 = q'_1 \cdot q'_2 \cdot q'_3 \cdots q'_s.$$

Portanto:

$$n = n = m_1 \cdot m_2 = (q_1 \cdot q_2 \cdot q_3 \cdots q_r)(q'_1 \cdot q'_2 \cdot q'_3 \cdots q'_s). \tag{1.3}$$

e reorganizando os números primos $q_1 \leq q_2 \leq q_3 \leq ... \leq q_r$ e $q'_1 \leq q'_2 \leq q'_3 \leq ... \leq q'_s$ em (1.3) podemos escrever,

$$n = p_1 \cdot p_2 \cdot p_3 \cdots p_k,$$

com $p_1 \leq p_2 \leq p_3 \leq ... \leq p_k$ são primos positivos e $k = r + s$, como queríamos.

Para provarmos a unicidade desta decomposição, supomos

$$n = p_1 \cdot p_2 \cdot p_3 \cdots p_k = p'_1 \cdot p'_2 \cdot p'_3 \cdots p'_t \tag{1.4}$$

onde $p_1 \leq p_2 \leq p_3 \leq ... \leq p_k$ e $p'_1 \leq p'_2 \leq p'_3 \leq ... \leq p'_t$ são primos positivos.

Novamente pelo segundo princípio da indução sobre k, temos que se $k = 1$ então que $p_1 = p'_1 \cdot p'_2 \cdot p'_3 \cdots p'_t$.

Logo $p'_i \mid p_1$ para $i \in \{1, 2, ..., t\}$ e como p'_i e p_1 são primos temos que $p'_i = p_1$, implicando assim $k = 1 = t$.

Supomos agora que a unicidade acontece sempre que tivermos um produto de r fatores primos, onde $1 \leq r < k$. Vamos provar, a partir disso, que a unicidade vale para um inteiro positivo formado por um produto de k fatores primos.

De fato, se $p_1 \cdot p_2 \cdot p_3 \cdots p_k = p'_1 \cdot p'_2 \cdot p'_3 \cdots p'_t$, com $k \geq 2$ então p_1 divide algum p'_i e como os dois são números primos, temos que $p'_i = p_1$. Sem perda de generalidade podemos supor $p'_1 = p_1$.

Assim na equação (1.4) podemos cancelar $p_1' = p_1$, obtendo:

$$p_2 \cdot p_3 \cdots p_k = p_2' \cdot p_3' \cdots p_t'.$$

Note que no primeiro membro da equação acima temos $k-1$ fatores primos e pela hipótese de indução o produto $p_2 \cdot p_3 \cdots p_k$ é único. Portanto $k-1 = t-1 \implies k = t$ e assim $p_i' = p_i,\ \forall i \in \{1, 2, ..., k\}$, encerrando a demonstração. ■

Este teorema tem uma importância muito grande para o estudo do conjunto dos números inteiros.

1.3.5 Pequeno Teorema de Fermat

Desde, pelo menos, 500 anos antes de Cristo, os chineses sabiam que, se p é um número primo, então $p|2^p - 2$. Coube a Pierre de Fermat, no século XVII, generalizar este resultado, enunciando um pequeno mas notável teorema.

Para demonstrar o Teorema de Fermat, necessitaremos do lema a seguir.

Lema 1.3.2 . *Seja p um número primo. Os números $\binom{p}{i} = \frac{p!}{(p-i)!i!}$, onde $0 < i < p$, são todos divisíveis por p.*

Demonstração: O resultado vale trivialmente para $i = 1$. Podemos, então, supor $1 < i < p$. Neste caso, $i!|p(p-1)\cdots(p-i+1)$. Como $mdc(i!, p) = 1$, decorre que $i!|(p-1)\cdots(p-i+1)$, e o resultado se segue, pois

$$\binom{p}{i} = p \cdot \frac{(p-1)\cdots(p-i+1)}{i!}.$$

■

Teorema 1.3.3 (Pequeno Teorema de Fermat). *Dado um número primo p, então p divide o número $a^p - a$, para todo $a \in \mathbb{Z}_+$.*

Demonstração: Vamos provar o resultado por indução sobre a. O resultado vale claramente para $a = 1$, pois $p|0$.

Supondo o resultado válido para a, iremos prova-lo para $a+1$. Pela fórmula do binômio de Newton,

$$(a+1)^p - (a+1) = a^p - a + \binom{p}{1}a^{p-1} + \cdots + \binom{p}{p-1}a.$$

Pelo Lema 1.3.2 e pela hipótese de indução, o segundo membro da igualdade acima é divisível por p, portanto, $p|a^p - a$. ■

Corolário 1.3.3 . *Se p é um número primo e se a é um número inteiro positivo não divisível por p, então p divide $a^{p-1} - 1$.*

Demonstração: Pelo Pequeno Teorema de Fermat, $p|a(a^{p-1} - 1)$, onde p é primo e $a \in \mathbb{Z}_+$. Por hipótese, $p \nmid a$. Sendo assim, segue imediatamente que p divide $a^{p-1} - 1$. ■

Observação 1.3.5 . *O Corolário acima também será chamado de Pequeno Teorema de Fermat.*

1.3.6 Primos de Fermat e Primos de Mersenne

Estudaremos agora, dois tipos de *números primos* especiais famosos. O primeiro resultado relaciona-se com os números conhecidos como números de Fermat, em homenagem a Pierre de Fermat (1601-1665), jurista francês e matemático amador. Após Euclides e Eratóstenes, Fermat é considerado o primeiro matemático a contribuir para o desenvolvimento da Teoria dos Números do ponto de vista teórico. Muitos dos resultados e problemas deixados por Fermat motivaram o extraordinário avanço da Matemática no século XVII.

Proposição 1.3.14 . *Sejam a e n números inteiros positivos maiores do que 1. Se $a^n + 1$ é primo, então a é par e $n = 2^m$, com $m \in \mathbb{Z}_+$.*

Demonstração: Suponhamos que $a^n + 1$ seja primo, onde $a > 1$ e $n > 1$. Logo, a tem que ser par, pois, caso contrário, $a^n + 1$ seria par e maior do que dois, o que contraria o fato de ser primo.

Se n tivesse um divisor primo p diferente de 2, teríamos $n = n'p$ com $n' \in \mathbb{Z}_+^*$. Portanto, pela Proposição 1.3.6, $a^{n'} + 1$ dividiria $(a^{n'})^p + 1 = a^n + 1$, contradizendo o fato desse último número ser primo. Isto implica que n é da forma 2^m.

■

Os *números de Fermat* são os números da forma

$$F_n = 2^{2n} + 1.$$

Em 1640, Fermat escreveu em uma de suas cartas endereçadas a Mersenne, que achava que esses números eram todos primos, baseado na observação de que $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ e $F_4 = 65537$ são primos.

Em 1732, Leonhard Euler mostrou que

$$F_5 = 2^{25} + 1 = 4\ 294\ 967\ 297 = 641 \cdot 6700417,$$

portanto, composto.

Os números de Fermat primos são chamados de *primos de Fermat*. Até hoje, não se sabe se existem outros primos de Fermat além dos quatro primeiros. Em 1938, os matemáticos ingleses Godfrey Harold Hardy (1877 - 1947) e Edward Maitland Wright (1906 - 2005), escreveram juntos o livro *An Introduction to the Theory of Numbers*. Nesse livro, eles conjecturaram que os primos de Fermat são em número finito.

O segundo resultado, relaciona-se com os números conhecidos como *números de Mersenne*.

Proposição 1.3.15 . *Sejam a e n números inteiros positivos maiores que 1. Se $a^n - 1$ é primo, então $a = 2$ e n é primo.*

Demonstração: Suponhamos que $a^n - 1$ seja primo, com $a > 1$ e $n > 1$.

Suponhamos, por absurdo, que $a > 2$. Logo, $a - 1 > 1$ e $a - 1 | a^n - 1$ (Proposição 1.3.5), e, portanto, $a^n - 1$ não é primo, contradição. Consequentemente, $a = 2$.

Por outro lado, suponha, por absurdo, que n não é primo. Temos que $n = rs$ com $r > 1$ e $s > 1$. Como $2^r - 1$ divide $(2r)^s - 1 = 2^n - 1$ (novamente pela Proposição 1.3.5), segue que $2^n - 1$ não é primo, contradição. Logo, n é primo. ■

Os *números de Mersenne* são os números da forma

$$M_p = 2^p - 1,$$

onde p é um número primo.

Os registros históricos dão conta de que os números *primos de Mersenne*, como são conhecidos atualmente, já eram considerados por Euclides de Alexandria (360 a.C. - 295 a.C.), o notável matemático platônico. Ao estudar tais números, Euclides estabeleceu uma conexão com os *números perfeitos*. O nome atual, entretanto, veio exatamente em

consequência dos estudos de Marin Mersenne (1588 - 1648), matemático, teórico musical, padre mínimo, teólogo e filósofo francês, que chegou a compilar uma lista de *Mersennes Primos* até o expoente 257. Verificou-se, posteriormente, que a lista era apenas parcialmente correta, em seu trabalho, ele omitiu M_{61}, M_{89} e M_{107} (que são primos), bem como incluiu impropriamente M_{67} e M_{257} (que são compostos). Não se tem informação de como Mersenne obteve essa lista e sua verificação rigorosa, foi feita apenas dois séculos mais tarde.

No intervalo $2 \leq p \leq 5000$ os números de Mersenne que são primos, são chamados de *primos de Mersenne* e correspondem aos seguintes valores de p : $2, 3, 5, 7, 13, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253$ e 4423. Até dezembro de 2001, o maior primo de Mersenne conhecido era $M_{13466917}$, que possui no sistema decimal 4 053 946 dígitos, e é o trigésimo nono primo de Mersenne conhecido.

Os primeiros cinco *primos de Mersenne* são: $3, 7, 31, 127$ e 8191.

1.4 Congruências

Apresentaremos aqui, uma das noções mais fecundas da Aritmética, introduzida por Gauss no seu livro *Disquisitiones Arithmeticae*, de 1801. Trata-se da realização de uma Aritmética com os restos da divisão euclidiana por um número fixado. Encerrando assim, o primeiro capítulo do nosso trabalho.

1.4.1 Aritmética dos Restos

Seja m um número natural diferente de zero. Diremos que dois números inteiros positivos a e b são *congruentes* módulo m se os restos de sua divisão euclidiana por m são iguais. Quando os inteiros a e b são congruentes módulo m, escreve-se

$$a \equiv b \; mod \; m.$$

Por exemplo, $21 \equiv 13 \; mod \; 2$, já que os restos da divisão de 21 e de 13 por 2 são iguais a 1.

Quando a relação $a \equiv b \; mod \; m$ for falsa, diremos que a e b não são congruentes, ou que são incongruentes, módulo m. Escreveremos, neste caso, $a \not\equiv b \; mod \; m$.

Por exemplo, 11 e 17 não são congruentes módulo 4, ou seja, $11 \not\equiv 17 \; mod \; 4$, pois o resto da divisão de 11 por 4 é 3 e de 17 por 4 é 1.

Como o resto da divisão de um número natural qualquer por 1 é sempre nulo, temos que $a \equiv b \ mod\ 1$, quaisquer que sejam $a,\ b \in \mathbb{Z}_+$. Isto torna desinteressante a aritmética dos restos módulo 1. Portanto, doravante, consideraremos sempre $m > 1$.

Decorre, imediatamente, da definição que a congruência, módulo um inteiro fixado m, é uma relação de equivalência. Como veremos a seguir.

Proposição 1.4.1 . *Seja $m \in \mathbb{Z}_+$, com $m > 1$. Para todos $a, b, c \in \mathbb{Z}_+$, temos as propriedades*

i) Reflexiva*: $a \equiv a \ mod\ m$,*

ii) Simétrica*: Se $a \equiv b \ mod\ m$, então $b \equiv a \ mod\ m$,*

iii) Transitiva*: se $a \equiv b \ mod\ m$ e $b \equiv c \ mod\ m$, então $a \equiv c \ mod\ m$.*

Para verificar se dois números são congruentes módulo m, não é necessário efetuar a divisão euclidiana de ambos por m para depois comparar os seus restos. É suficiente aplicar o seguinte resultado:

Proposição 1.4.2 . *Suponha que $a, b \in \mathbb{Z}_+$ são tais que $b \geq a$. Então $a \equiv b \ mod\ m$ se, e somente se, $m|b - a$.*

Demonstração: Sejam $a = mq + r$, com $r < m$ e $b = mq' + r'$, com $r' < m$, as divisões euclidianas de a e b por m, respectivamente. Logo,

$$b - a = \begin{cases} m(q' - q) \ + \ (r' - r), & se\ r' \geq \ r \\ m(q' - q) \ - \ (r' - r), & se\ r \geq \ r' \end{cases}$$

onde $r' - r < m$,ou $r - r' < m$. Portanto, $a \equiv b \ mod\ m$ se, e somente se, $r = r'$, o que é equivalente a dizer que $m|b - a$. ■

Note que todo número natural é congruente módulo m ao seu resto pela divisão euclidiana por m e, portanto, é congruente módulo m a um dos números $0, 1, ..., m - 1$. Além disso, dois desses números distintos não são congruentes módulo m.

Portanto, para achar o resto da divisão de um número a por m, basta achar o número natural r dentre os números $0, 1, ..., m - 1$ que seja congruente a a módulo m.

Chamaremos de *sistema completo de resíduos* módulo m a todo conjunto de números naturais cujos resto pela divisão por m são os números $0, 1, ..., m-1$, sem repetições e em uma ordem qualquer.

Portanto, um sistema completo de resíduos módulo m possui m elementos.

É claro que, se $a_1, a_2, ..., a_m$ são m números naturais, dois a dois não congruentes módulo m, então eles formam um sistema completo de resíduos módulo m. De fato, os restos da divisão dos a_i por m são dois a dois distintos, o que implica que são os números $0, 1, ..., m-1$ em alguma ordem.

O que torna útil e poderosa a noção de congruência é o fato de ser uma relação de equivalência compatível com as operações de adição e multiplicação nos inteiros, conforme veremos na proposição a seguir.

Proposição 1.4.3 . *Seja $a, b, c, d, m \in \mathbb{Z}_+$, com $m > 1$.*

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

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

Demonstração: Suponhamos que $a \equiv b \ mod \ m$ e $c \equiv d \ mod \ m$. Podemos, sem perca de generalidade, supor que $b \geq a$ e $d \geq c$. Logo, temos que $m|b-a$ e $m|d-c$.

i) Basta observar que $m|(b-a)+(d-c)$ e, portanto, $m|(b+d)-(a+c)$, o que prova essa parte do resultado.

ii) Basta notar que $bd - ac = d(b-a) + a(d-c)$ e concluir que $m|bd-ac$.

■

Corolário 1.4.1 . *Para todos $n \in \mathbb{Z}_+^*$, $a, b \in \mathbb{Z}_+$, se $a \equiv b \ mod \ m$, então $a^n \equiv b^n \ mod \ m$.*

Demonstração: Se $n = 1$, verdadeiro, pois, por hipótese $a \equiv b \ mod \ m$.

Escrevendo $\begin{cases} a \equiv b \ mod \ m \\ a \equiv b \ mod \ m \end{cases}$,

temos pela Proposição 1.4.3, temos que $a^2 \equiv b^2 \ mod \ m$.

Supondo agora, verdadeiro para n, $n \in \mathbb{Z}_+$, temos que $a^n \equiv b^n \ mod \ m$ e por hipótese, temos que $a \equiv b \ mod \ m$, isso implica, pela Proposição 1.4.3, que

$$\begin{cases} a^n \equiv b^n \ mod \ m \\ a \equiv b \ mod \ m \end{cases} \quad \Rightarrow \quad a^n \cdot a \equiv b^n \cdot b \ mod \ m \quad \Rightarrow \quad a^{n+1} \equiv b^{n+1} \ mod \ m.$$

■

Corolário 1.4.2 . *Sejam $a, b, m \in \mathbb{Z}_+^*$, com $m > 1$. Se $a + b \equiv 0 \ mod \ m$, então, para todo $n \in \mathbb{Z}_+$, temos:*

i) $a^{2n} \equiv b^{2n} \ mod \ m$

ii) $a^{2n+1} + b^{2n+1} \equiv 0 \ mod \ m$.

Demonstração: O resultado é claramente válido para $n = 0$. Podemos ainda supor, sem perca de generalidade, que $a \geq b$.

Como $a + b \equiv 0 \ mod \ m$, segue-se que $m|a + b$ e, portanto, $m|(a + b) \cdot (a - b)$. Como $(a+b) \cdot (a-b) = a^2 - b^2$, segue-se que $a^2 \equiv b^2 \ mod \ m$. Aplicando o Corolário 1.4.1, temos que $a^{2n} \equiv b^{2n} \ mod \ m$ para todo $n \in \mathbb{Z}_+^*$.

Por outro lado, como

$$a^{2n+1} + b^{2n+1} = (a + b) \cdot (a^{2n} - ba^{2n-1} + \cdots - b^{2n-1}a + b^{2n}),$$

$$\text{e } m|a + b,$$

segue-se que $m|a^{2n+1} + b^{2n+1}$ e, portanto, $a^{2n+1} + b^{2n+1} \equiv 0 \ mod \ m$. ■

Capítulo 2

Os Ternos Pitagóricos

Neste capítulo apresentaremos inicialmente a definição de Ternos Pitagóricos e Ternos Pitagóricos Primitivos. Em seguida, apresentaremos as principais fórmulas que geram tais ternos, bem como um dispositivo prático que também gera infinitos ternos pitagóricos. Na seção subsequente, traremos uma fórmula que relaciona dois Ternos Pitagóricos de modo a gerar um novo terno pitagórico. Para finalizar o Capítulo, apresentaremos algumas propriedades dos Ternos Pitagóricos, bem como algumas particularidades do terno $(3, 4, 5)$.

2.1 Ternos Pitagóricos

Definição 2.1.1 . *Um terno pitagórico* (TP) *é uma tripla de inteiros positivos* (a, b, c)*, tal que* $a^2 + b^2 = c^2$*.*

Também chamamos o $TP(a, b, c)$ de *triângulo pitagórico* cujos catetos são a, b e hipotenusa c. Em outros termos, *terno pitagórico* é toda solução inteira e positiva da *equação diofantina*: $x^2 + y^2 = z^2$.

Exemplo 2.1.1 . *Exemplos de ternos pitagóricos:*

i) $(3, 4, 5)$ *é terno pitagórico, pois,* $3^2 + 4^2 = 5^2$*;*

ii) $(6, 8, 10)$ *é terno pitagórico, pois,* $6^2 + 8^2 = 10^2$*;*

iii) $(5, 12, 13)$ *é terno pitagórico, pois,* $5^2 + 12^2 = 13^2$*;*

iv) $(12, 35, 37)$ *é terno pitagórico, pois,* $12^2 + 35^2 = 37^2$.

Teorema 2.1.1 . *Se* (a, b, c) *é um terno pitagórico, então* (ka, kb, kc) *também é um terno pitagórico,* $\forall k \in \mathbb{Z}_+$ *e* $k > 1$.

Demonstração: Por hipótese, (a, b, c) é terno pitagórico, logo, $a^2 + b^2 = c^2$. Daí, multiplicando ambos os membros da equação por k^2, temos:

$$a^2 + b^2 = c^2$$

$$k^2 \cdot (a^2 + b^2) = k^2 \cdot (c^2)$$

$$k^2 \cdot a^2 + k^2 \cdot b^2 = k^2 \cdot c^2$$

$$(k \cdot a)^2 + (k \cdot b)^2 = (k \cdot c)^2$$

Portanto, (ka, kb, kc) é terno pitagórico. ■

Exemplo 2.1.2 . *Exemplos de Ternos Pitagóricos obtidos através da multiplicação dos elementos de um* TP *dado, por um inteiro positivo maior que* 1*:*

i) $(6, 8, 10)$ *é* TP*, pois,* $6^2 + 8^2 = 10^2$*. Como* $(3 \cdot 6, 3 \cdot 8, 3 \cdot 10) = (18, 24, 30)$*, a tripla* $(18, 24, 30)$ *também é* TP*. De fato,* $18^2 + 24^2 = 30^2$.

ii) $(8, 15, 17)$ *é* TP*, pois,* $8^2 + 15^2 = 17^2$*. Como* $(5 \cdot 8, 5 \cdot 15, 5 \cdot 17) = (40, 75, 85)$*, a tripla* $(40, 75, 85)$ *também é* TP*. De fato,* $40^2 + 75^2 = 85^2$.

Teorema 2.1.2 . *Se* (ka, kb, kc) *é um terno pitagórico, então* (a, b, c) *também é um terno pitagórico,* $\forall k \in \mathbb{Z}_+$ *e* $k > 1$.

Demonstração: Por hipótese, (ka, kb, kc) é terno pitagórico, logo, $(ka)^2 + (kb)^2 = (kc)^2$. Aplicando a propriedade da potenciação e em seguida fatorando, obtemos:

$$(ka)^2 + (kb)^2 = (kc)^2$$

$$k^2 \cdot a^2 + k^2 \cdot b^2 = k^2 \cdot c^2$$

$$k^2 \cdot (a^2 + b^2) = k^2 \cdot (c^2)$$

Por hipótese também, $k > 1$, logo, $k^2 > 1$. Daí, dividindo ambos os membros por k^2, obtemos:

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

Portanto, (a, b, c) é terno pitagórico. ■

Exemplo 2.1.3 . *Exemplos de Ternos Pitagóricos obtidos através da divisão dos elementos de um TP dado, por um inteiro positivo maior que 1:*

i) $(30, 72, 78)$ *é TP, pois,* $30^2 + 72^2 = 78^2$.

Como $(30, 72, 78) = (3 \cdot 10, 3 \cdot 24, 3 \cdot 26)$, *a tripla* $(10, 24, 26)$ *também é TP. De fato,* $10^2 + 24^2 = 26^2$.

ii) $(48, 140, 148)$ *é TP, pois,* $48^2 + 140^2 = 148^2$.

Como $(48, 140, 148) = (2 \cdot 24, 2 \cdot 70, 2 \cdot 74)$, *a tripla* $(24, 70, 74)$ *também é TP. De fato,* $24^2 + 70^2 = 74^2$.

2.2 Ternos Pitagóricos Primitivos

Definição 2.2.1 . *Um Terno Pitagórico Primitivo (TPP) é um $TP(a, b, c)$ com $mdc(a, b, c) = 1$, ou seja, a, b e c são relativamente primos. Também chamamos o $TPP(a, b, c)$ de Triângulo Pitagórico Primitivo cujos catetos são a, b e hipotenusa c.*

Exemplo 2.2.1 . *Exemplos de ternos pitagóricos primitivos:*

i) $(3, 4, 5)$ *é terno pitagórico primitivo, pois,* $3^2 + 4^2 = 5^2$ *e* $mdc(3, 4, 5) = 1$;

ii) $(5, 12, 13)$ *é terno pitagórico primitivo, pois,* $5^2 + 12^2 = 13^2$ *e* $mdc(5, 12, 13) = 1$.

Chamamos de *terno pitagórico não-primitivo ou composto*, todo $TP(a, b, c)$ com $mdc(a, b, c) \neq 1$.

Exemplo 2.2.2 . *Exemplos de ternos pitagóricos não-primitivos:*

i) $(6, 8, 10)$ *é ternos pitagóricos não-primitivos, pois,* $6^2 + 8^2 = 10^2$ *e* $mdc(6, 8, 10) = 2$;

ii) $(15, 36, 39)$ *é ternos pitagóricos não-primitivos, pois,* $15^2 + 36^2 = 39^2$ *e* $mdc(15, 36, 39) = 3$.

Notemos que a partir de um TPP qualquer, podemos gerar infinitos ternos pitagóricos não-primitivos, multiplicando seus elementos por um inteiro positivo maior que 1. Reciprocamente, sempre é possível obter um TPP a partir de um terno pitagórico não-primitivo, dividindo cada um de seus elementos pelo *mdc* dos mesmos.

Esta relação entre TPP e os seus correspondentes ternos não-primitivos, se justifica pelo fato que (a, b, c) é TP *se, e somente se*, (ka, kb, kc) é TP, para qualquer k inteiro positivo maior que 1, como vimos nos Teoremas 2.1.1 e 2.1.2.

A partir do $TPP(3, 4, 5)$, são gerados, por exemplo, os ternos compostos $(6, 8, 10)$, $(15, 20, 25)$ e $(21, 28, 35)$, multiplicando-se, respectivamente, os três elementos do primeiro terno por 2, do segundo por 3 e do terceiro por 7.

O terno$(40, 75, 85)$ é um terno pitagórico não-primitivo, pois, $40^2 + 75^2 = 85^2$ e $mdc(40, 75, 85) = 5$. Dividindo 40, 75 e 85 por 5, obtemos o $TPP(8, 15, 17)$.

2.3 Gerando Ternos Pitagóricos de Maneira Sistemática

2.3.1 Equações de Euclides

Agora que já sabemos a definição de Ternos Pitagóricos e Ternos Pitagóricos Primitivos, apresentaremos uma fórmula de relevância ímpar, que gera todos os TPP, sendo esta a mais comum nos livros de *Teoria dos Números*.

Euclides de Alexandria (300 a.C. - 295 a.C.), demonstrou que existem infinitos Ternos Pitagóricos Primitivos. Além disso, ele encontrou uma fórmula que gera tais ternos.

Lema 2.3.1 . *Se (a, b, c) é um terno pitagórico primitivo, então $a \not\equiv b \ mod\ 2$ e c é ímpar.*

Demonstração: Se $a \equiv b \ mod\ 2$, então a e b são ambos pares ou são ambos ímpares. Se a e b são ambos pares, então $2|mdc(a, b)$, o que é impossível, porque o $mdc(a, b) = 1$, já que por hipótese (a, b, c) é um TPP. E se, ao invés, a e b são ambos ímpares, então $c^2 = a^2 + b^2$ é par e, portanto, c é par, isto é, se $a = 2h + 1$ e $b = 2k + 1$, então $c = 2n$, com h, k e n inteiros positivos, e temos:

$$a^2 = 4h^2 + 4h + 1 \ \equiv \ 1 \ mod\ 4$$

$$b^2 = 4k^2 + 4k + 1 \ \equiv \ 1 \ mod \ 4$$

$$c^2 = 4n^2 \ \equiv \ 0 \ mod \ 4$$

O que implica:

$$a^2 \ + \ b^2 \ \equiv \ 2 \ mod \ 4$$

ou seja:

$$c^2 = a^2 + b^2 \ \equiv \ 2 \ mod \ 4$$

e, portanto, $2 \ \equiv \ 0 \ mod \ 4$, o que é absurdo.

Assim sendo, só pode ser $a \not\equiv \ b \ mod \ 2$, de modo que a e b são de paridade diferente, e como $a^2 + b^2 = c^2$, segue que c^2 é ímpar, o que implica c também ímpar. ■

Observação 2.3.1 . *De conformidade com o Lema 2.3.1, num terno pitagórico primitivo qualquer (a, b, c), há exatamente um elemento que é par (a ou b) e dois elementos que são ímpares (a e c ou b e c), de modo que a soma $a + b + c$ é sempre um inteiro positivo par.*

Lema 2.3.2 . *Se a e c são ambos ímpares positivos, com $a < c$, então $c + a$ e $c - a$ são pares.*

Demonstração: Por hipótese, a e c são ímpares positivos, logo, existem t,$u \in \mathbb{Z}_+^*$, $t < u$, $a = 2t + 1$ e $c = 2u + 1$. Daí,

$$c + a = (2u + 1) + (2t + 1)$$

$$c + a = 2u + 2t + 2$$

$$c + a = 2 \cdot (u + t + 1)$$

Portanto, $c + a$ é par.

Por outro lado,

$$c - a = (2u + 1) - (2t + 1)$$

$$c - a = 2u - 2t + 1 - 1$$

$$c - a = 2 \cdot (u - t)$$

Portanto, $c - a$ é par. ■

Lema 2.3.3 . *Se (a, b, c) é um terno pitagórico primitivo, então a e c são relativamente primos.*

Demonstração: Seja $mdc(a, c) = d$. Sendo assim, existem $\alpha, \beta \in \mathbb{Z}_+$, com $\alpha > \beta$, tais que $a = d\alpha$ e $c = d\beta$.

Por outro lado, por hipótese, (a, b, c) é terno pitagórico primitivo, logo $mdc(a, b, c) = 1$ e,

$$a^2 + b^2 = c^2$$

$$b^2 = c^2 - a^2.$$

Substituindo $a = d\alpha$ e $c = d\beta$ na equação acima, vem

$$b^2 = (d\beta)^2 - (d\alpha)^2$$

$$b^2 = d^2\beta^2 - d^2\alpha^2$$

$$b^2 = d^2 \cdot (\beta^2 - \alpha^2).$$

Como o produto $d^2 \cdot (\beta^2 - \alpha^2)$ é igual a um quadrado, existe $m \in \mathbb{Z}_+^*$, tal que $\beta^2 - \alpha^2 = m^2$. Sendo assim,

$$b^2 = d^2 \cdot m^2 \quad \Rightarrow \quad b = d \cdot m \quad \Rightarrow \quad d|b.$$

Desse modo, $d|a$, $d|b$ e $d|c$. Como $mdc(a, b, c) = 1$, temos $d = 1$, logo $mdc(a, c) = 1$.

Portanto, a e c são relativamente primos. ■

Teorema 2.3.1 (Equações de Euclides). *Se (a, b, c) é um terno pitagórico primitivo, então (a, b, c) é unicamente determinado por um par de inteiros positivos relativamente primos (m, n), com $m > n$ e de paridades opostas, tais que*

$$a = m^2 - n^2,\ b = 2mn \text{ e } c = m^2 + n^2.$$

Demonstração: Tomando b como par, reescreva a equação $c^2 = a^2 + b^2$ como $b^2 = c^2 - a^2 = (c-a)\cdot(c+a)$. Como a e c são ambos ímpares (de acordo com o Lema 2.3.1), tem-se pelo Lema 2.3.2 que $(c-a)$ e $(c+a)$ são pares. Assim, dividindo por 4 ambos os membros da equação $b^2 = (c-a)\cdot(c+a)$, tem-se:

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

Os dois inteiros à direita, ou seja, $\frac{(c-a)}{2}$ e $\frac{(c+a)}{2}$, são relativamente primos. Caso contrário, se d é um divisor comum deles, d divide a soma e a diferença entre eles (Proposição 1.3.4), que são c e a respectivamente. Mas c e a são relativamente primos (Lema 2.3.3), logo $d = 1$. Como $c > a > 0$, os fatores $\frac{(c-a)}{2}$ e $\frac{(c+a)}{2}$ são positivos. Além disso, eles são relativamente primos e seu produto é igual a um quadrado. Sendo assim, pelo *teorema da fatoração única em* $\mathbb{Z}_+^*$ (Teorema 1.3.2), segue que existem $m, n \in \mathbb{Z}_+$ tais que:

$$\frac{(c+a)}{2} = m^2, \text{ e } \frac{(c-a)}{2} = n^2.$$

Adicionando e subtraindo as equações $\frac{(c+a)}{2} = m^2$ e $\frac{(c-a)}{2} = n^2$, obtemos

$$c = m^2 + n^2 \text{ e } a = m^2 - n^2.$$

Então,

$$\left(\frac{b}{2}\right)^2 = m^2n^2 \quad \Rightarrow \quad \frac{b}{2} = mn \quad \Rightarrow \quad b = 2mn.$$

Resta checar que m e n têm paridade oposta. Como m e n são relativamente primos, segue que m e n não são ambos pares. Se m e n fossem ambos ímpares, então $c = m^2 + n^2$, $a = m^2 - n^2$ e $b = 2mn$ seriam pares, contradizendo o fato de que (a, b, c) é um TPP. E isto completa a prova. ■

Exemplo 2.3.1 . *Exemplos de TPP obtidos através das Equações de Euclides:*

i) *Como $2 > 1$, 2 e 1 têm paridade distinta e $mdc(2,1) = 1$, podemos tomar $m = 2$ e $n = 1$. Substituindo nas equações de Euclides, temos:*

$a = m^2 - n^2 = 2^2 - 1^2 = 4 - 1 = 3$,

$b = 2 \cdot m \cdot n = 2 \cdot 2 \cdot 1 = 4$,

$c = m^2 + n^2 = 2^2 + 1^2 = 4 + 1 = 5$.

Logo, $(3, 4, 5)$ *é terno pitagórico primitivo.*

ii) *Como* $13 > 8$, 13 *e* 8 *têm paridade distinta e* $mdc(13, 8) = 1$, *podemos tomar* $m = 13$ *e* $n = 8$. *Substituindo nas equações de Euclides, temos:*

$a = m^2 - n^2 = 13^2 - 8^2 = 169 - 64 = 105$,

$b = 2 \cdot m \cdot n = 2 \cdot 13 \cdot 8 = 208$,

$c = m^2 + n^2 = 13^2 + 8^2 = 169 + 64 = 233$.

Logo, $(105, 208, 233)$ *é terno pitagórico primitivo.*

iii) *Como* $18 > 5$, 18 *e* 5 *têm paridade distinta e* $mdc(18, 5) = 1$, *podemos tomar* $m = 18$ *e* $n = 5$. *Substituindo nas equações de Euclides, temos:*

$a = m^2 - n^2 = 18^2 - 5^2 = 324 - 25 = 299$,

$b = 2 \cdot m \cdot n = 2 \cdot 18 \cdot 5 = 180$,

$c = m^2 + n^2 = 18^2 + 5^2 = 324 + 25 = 349$.

Logo, $(299, 180, 349)$ *é terno pitagórico primitivo.*

iv) *Como* $31 > 16$, 31 *e* 16 *têm paridade distinta e* $mdc(31, 16) = 1$, *podemos tomar* $m = 31$ *e* $n = 16$. *Substituindo nas equações de Euclides, temos:*

$a = m^2 - n^2 = 31^2 - 16^2 = 961 - 256 = 705$,

$b = 2 \cdot m \cdot n = 2 \cdot 31 \cdot 16 = 992$,

$c = m^2 + n^2 = 31^2 + 16^2 = 961 + 256 = 1217$.

Logo, $(705, 992, 1217)$ *é terno pitagórico primitivo.*

Na tabela abaixo, temos 30 ternos pitagóricos primitivos, obtidos também a partir das Equações de Euclides (Teorema 2.3.1). Construímos tal Tabela, fixando os 10 primeiros inteiros positivos (1 a 10) para n, sendo que cada um deles foram fixados 3 vezes e combinados com os 3 primeiros respectivos valores de m que satisfazem as condições do referido teorema.

Tabela 2.1: Exemplos de Ternos Pitagóricos Primitivos

m	n	$a = m^2 - n^2$	$b = 2mn$	$c = m^2 + n^2$	$TPP(a, b, c)$
2	1	3	4	5	(3,4,5)
4	1	15	8	17	(15,8,17)
6	1	35	12	37	(35,12,37)
3	2	5	12	13	(5,12,13)
5	2	21	20	29	(21,20,29)
7	2	45	28	53	(45,28,53)
4	3	7	24	25	(7,24,25)
8	3	55	48	73	(55,48,73)
10	3	91	60	109	(91,60,109)
5	4	9	40	41	(9,40,41)
7	4	33	56	65	(33,56,65)
9	4	65	72	97	(65,72,97)
6	5	11	60	61	(11,60,61)
8	5	39	80	89	(39,80,89)
12	5	119	120	169	(119,120,169)
26	5	651	260	701	(651,260,701)
28	5	759	280	809	(759,280,809)
7	6	13	84	85	(13,84,85)
11	6	85	132	157	(85,132,157)
13	6	133	156	205	(133,156,205)
8	7	15	112	113	(15,112,113)
10	7	51	140	149	(51,140,149)
12	7	95	168	193	(95,168,193)
9	8	17	144	145	(17,144,145)
11	8	57	176	185	(57,176,185)
13	8	105	208	233	(105,208,233)
10	9	19	180	181	(19,180,181)
14	9	115	252	277	(115,252,277)
16	9	175	288	337	(175,288,337)
11	10	21	220	221	(21,220,221)
13	10	69	260	269	(69,260,269)
17	10	189	340	389	(189,340,389)

2.3.2 Particularizando as Equações de Euclides

Se confrontarmos as equações que Euclides desenvolveu para gerar *ternos pitagóricos primitivos* com a fórmula que os pitagóricos também desenvolveram para determinar *ternos pitagóricos primitivos*, concluiremos que este último é caso particular do primeiro, ou seja, a partir das equações de Euclides (Teorema 2.3.1), podemos gerar a fórmula $(2k+1, 2k^2+2k, 2k^2+2k+1)$ com $k \in \mathbb{Z}_+^*$, atribuída aos pitagóricos. Além desta, podemos obter outras infinitas fórmulas que geram infinitos *ternos pitagóricos primitivos.*

Apresentaremos a seguir, dois casos particulares das equações de Euclides, gerados a partir de expressões algébricas, sendo que a primeira é exatamente a fórmula pitagórica.

Lema 2.3.4 . *Se k é um inteiro positivo, então $mdc(k, k+1) = 1$.*

Demonstração: Pelo Lema de Euclides, temos
$mdc(k, k+1) = mdc(k, 1+1\cdot k) = mdc(k, 1) = 1.$ ■

O Teorema que enunciaremos a seguir, é atribuído aos pitagóricos.

Teorema 2.3.2 *Se k é um inteiro positivo, $k \geq 1$ então $(2k+1, 2k^2+2k, 2k^2+2k+1)$ é um terno pitagórico primitivo.*

Demonstração: Pelas Equações de Euclides (Teorema 2.3.1), temos que $(m^2-n^2, 2mn, m^2+n^2)$, com $m > n$, $mdc(m, n) = 1$ e $m \not\equiv n \ mod\ 2$, geram todos os ternos pitagóricos primitivos.

Por outro lado, para todo $k \in \mathbb{Z}_+^*$, $k+1 > k$, pois

$$1 > 0 \quad \Rightarrow \quad 1+k > 0+k \quad \Rightarrow \quad k+1 > k.$$

Temos ainda que, $(k+1)$ e k possuem paridade distinta $(k+1) \not\equiv k \ mod\ 2$, uma vez que são inteiros consecutivos. Além disso, $mdc(k+1, k) = 1$, conforme Lema 2.3.4.

Assim, tomando $m = k+1$ e $n = k$ e substituindo nas Equações de Euclides (Teorema 2.3.1), temos

$$\begin{cases} a = m^2 - n^2 \\ a = (k+1)^2 - (k)^2 \\ a = k^2 + 2k + 1 - k^2 \\ a = 2k+1 \end{cases}, \quad \begin{cases} b = 2\cdot m \cdot n \\ b = 2\cdot (k+1)\cdot k \\ b = (2k+2)\cdot k \\ b = 2k^2 + 2k \end{cases} \quad e \quad \begin{cases} c = m^2 + n^2 \\ c = (k+1)^2 + (k)^2 \\ c = k^2 + 2k + 1 + k^2 \\ a = 2k^2 + 2k + 1 \end{cases}.$$

Portanto, $(2k+1,\ 2k^2+2k,\ 2k^2+2k+1)$ é terno pitagórico primitivo, para qualquer k inteiro positivo, $k \geq 1$. ■

Exemplo 2.3.2 . *Exemplos de TPP gerados a partir da fórmula acima para valores aleatórios de k:*

i) *Para* $k = 1$, *temos* $(2 \cdot 1 + 1,\ 2 \cdot 1^2 + 2 \cdot 1,\ 2 \cdot 1^2 + 2 \cdot 1 + 1) = (3, 4, 5)$. *Logo,* $(3, 4, 5)$ *é* TPP.

ii) *Para* $k = 5$, *temos* $(2 \cdot 5 + 1,\ 2 \cdot 5^2 + 2 \cdot 5,\ 2 \cdot 5^2 + 2 \cdot 5 + 1) = (11, 60, 61)$. *Logo,* $(11, 60, 61)$ *é* TPP.

iii) *Para* $k = 36$, *temos* $(2 \cdot 36 + 1,\ 2 \cdot 36^2 + 2 \cdot 36,\ 2 \cdot 36^2 + 2 \cdot 36 + 1) = (73, 2664, 2665)$. *Logo,* $(73, 2664, 2665)$ *é* TPP.

Lema 2.3.5 . *Para todo k inteiro positivo,* $mdc(2k+1, 8k+6) = 1$.

Demonstração: Pelo Lema de Euclides, temos
$mdc(2k+1, 8k+6) = mdc\,(2k+1, 2+4\cdot(2k+1)) = mdc(2k+1, 2) = (2, 1+k\cdot 2) =$
$= mdc(2, 1) = 1.$ ■

Teorema 2.3.3 *Se k é um inteiro positivo, então*

$$(60k^2+92k+35,\ 32k^2+40k+12,\ 68k^2+100k+37)$$

é um terno pitagórico primitivo.

Demonstração: Notemos que para todo k inteiro positivo, $8k+6 > 2k+1$, pois

$$6k+5 > 0 \quad \Rightarrow \quad (6k+5)+(2k+1) > (2k+1) \quad \Rightarrow \quad 8k+6 > 2k+1.$$

Notemos ainda que, para todo k inteiro positivo, $8k+6$ e $2k+1$ possuem paridade distinta $(8k+6) \not\equiv (2k+1)\ mod\ 2$, pois, $2k+1$ é ímpar e $8k+6 = 2\cdot(4k+3)$ é par, além disso, $mdc(2k+1, 8k+6) = 1$, conforme o Lema 2.3.5.

Assim, tomando $m = 8k+6$ e $n = 2k+1$ e substituindo nas equações de Euclides (Teorema 2.3.1) temos

$$\begin{cases} a = m^2 - n^2 \\ a = (8k+6)^2 - (2k+1)^2 \\ a = 64k^2 + 96k + 36 - 4k^2 - 4k - 1 \\ a = 64k^2 - 4k^2 + 96k - 4k + 36 - 1 \\ a = 60k^2 + 92k + 35 \end{cases}, \quad \begin{cases} b = 2 \cdot m \cdot n \\ b = 2 \cdot (8k+6) \cdot (2k+1) \\ b = 2 \cdot (16k^2 + 8k + 12k + 6) \\ b = 2 \cdot (16k^2 + 20k + 6) \\ b = 32k^2 + 40k + 12 \end{cases} \quad e$$

$$\begin{cases} c = m^2 + n^2 \\ c = (8k+6)^2 + (2k+1)^2 \\ c = 64k^2 + 96k + 36 + 4k^2 + 4k + 1 \\ c = 64k^2 + 4k^2 + 96k + 4k + 36 + 1 \\ c = 68k^2 + 100k + 37 \end{cases}.$$

Portanto, $(60k^2+92k+35,\ 32k^2+40k+12,\ 68k^2+100k+37)$ é terno pitagórico primitivo. ■

Exemplo 2.3.3 . *Exemplos de TPP gerados a partir da fórmula acima para valores aleatórios de k:*

i) *Para* $k = 1$, *temos* $(60 \cdot 1^2 + 92 \cdot 1 + 35,\ 32 \cdot 1^2 + 40 \cdot 1 + 12,\ 68 \cdot 1^2 + 100 \cdot 1 + 37) =$
$= (187, 84, 205)$. *Logo,* $(187, 84, 205)$ *é* TPP.

ii) *Para* $k = 9$, *temos* $(60 \cdot 9^2 + 92 \cdot 9 + 35,\ 32 \cdot 9^2 + 40 \cdot 9 + 12,\ 68 \cdot 9^2 + 100 \cdot 9 + 37) =$
$= (5723, 2964, 6445)$. *Logo,* $(5723, 2964, 6445)$ *é* TPP.

iii) *Para* $k = 40$, *temos* $(60 \cdot 40^2 + 92 \cdot 40 + 35,\ 32 \cdot 40^2 + 40 \cdot 40 + 12,\ 68 \cdot 40^2 + 100 \cdot 40 + 37) =$
$= (99715, 52806, 109737)$. *Logo,* $(99715, 52806, 109737)$ *é* TPP.

Desse modo, concluímos que é possível gerar infinitas fórmulas que geram TPP em função de um inteiro positivo k ($k \geq 1$) a partir das equações de Euclides, Teorema 2.3.1, desde que tomemos expressões algébricas que satisfaçam as condições impostas por este teorema.

2.3.3 Uma Fórmula de Fácil Dedução

Em quantos ternos pitagóricos o número 12 figura como cateto? Quais são esses ternos?

A ideia central do nosso trabalho é disponibilizar ao professor(a) de Matemática do Ensino Básico Regular e ao leitor de um modo geral, variadas formas de se obter ternos pitagóricos. Pois, entendemos que tal professor(a) precisa conhecer o maior número possível de ferramentas relacionadas a qualquer assunto que ele(a) pretende ensinar, para que possa utilizá-las nos momentos certos, de acordo com a conveniência.

Diante disto, apresentaremos a seguir, mais uma fórmula (Teorema 2.3.4) que gera infinitos Ternos Pitagóricos. Esta fórmula gera **todos** os ternos pitagóricos, ou seja, os *primitivos* e os *não-primitivos*, podendo isto ser feito de maneira ordenada, ou seja, podemos obter todos os ternos pitagóricos em que o número 3 figura como cateto, em seguida, todos os ternos pitagóricos em que o número 4 figura como cateto, e assim, sucessivamente, conforme a tabela que apresentaremos no final desta subseção, que foi construída para os números de 3 a 20. Desse modo, podemos responder com segurança a pergunta que inicia esta subseção.

Outra importante característica desta fórmula é que ela requer apenas o uso de *Álgebra Elementar* em sua demonstração, oportunizando assim, ao professor de matemática dessa fase, fazer uma revisão com seus(as) alunos(as) dos principais tópicos de *Aritmética* estudados até então, afim de que estes acompanhem e compreendam perfeitamente tal demonstração.

Lema 2.3.6 . *Se b e c são inteiros positivos, com $c > b$ e $u = c + b$ e $v = c - b$, então u e v são inteiros positivos de mesma paridade.*

Demonstração: Como b e c são inteiros positivos e $c > b$, temos que $c + b > 0$ e $c - b > 0$. Logo, u e v são inteiros positivos.

Agora, para mostrar que u e v possuem a mesma paridade, analisaremos, caso a caso, as quatro possíveis combinações das paridades de b e c.

i) Se b e c forem ambos pares positivos, com $c > b$, então existem k e t inteiros positivos, com $t > k$, tais que $b = 2k$ e $c = 2t$.

Daí,

$$\begin{cases} u = c + b \\ u = 2t + 2k \\ u = 2 \cdot (t + k) \end{cases} \quad e \quad \begin{cases} v = c - b \\ v = 2t - 2k \\ v = 2 \cdot (t - k) \end{cases} .$$

Logo, u e v são pares positivos, ou seja, são inteiros positivos de mesma paridade.

ii) Se b é um par positivo e c um ímpar positivo, com $c > b$, então existem k e t inteiros positivos, com $t > k$, tais que $b = 2k$ e $c = 2t + 1$.

Daí,

$$\begin{cases} u = c + b \\ u = 2t + 1 + 2k \\ u = 2t + 2k + 1 \\ u = 2 \cdot (t + k) + 1 \end{cases} \quad e \quad \begin{cases} v = c - b \\ v = 2t + 1 - 2k \\ v = 2t - 2k + 1 \\ v = 2 \cdot (t - k) + 1 \end{cases} .$$

Logo, u e v são ímpares positivos, ou seja, são inteiros positivos de mesma paridade.

iii) Se b é um ímpar positivo e c um par positivo, com $c > b$, então existem k e t inteiros positivos, com $t > k$, tais que $b = 2k + 1$ e $c = 2t$.

Daí,

$$\begin{cases} u = c + b \\ u = 2t + 2k + 1 \\ u = 2 \cdot (t + k) + 1 \end{cases} \quad e \quad \begin{cases} v = c - b \\ v = 2t - 2k - 1 \\ v = 2 \cdot (t - k) - 1 \end{cases} .$$

$u = c + b$

Logo, u e v são ímpares positivos, ou seja, são inteiros positivos de mesma paridade.

iv) Se b e c forem ambos ímpares positivos, com $c > b$, então existem k e t inteiros positivos, com $t > k$, tais que $b = 2k + 1$ e $c = 2t + 1$.

Daí,

$$\begin{cases} u = c + b \\ u = 2t + 1 + 2k + 1 \\ u = 2t + 2k + 1 + 1 \\ u = 2t + 2k + 2 \\ u = 2 \cdot (t + k + 1) \end{cases} \quad e \quad \begin{cases} v = c - b \\ v = 2t + 1 - 2k - 1 \\ v = 2t - 2k + 1 - 1 \\ v = 2t - 2k \\ v = 2 \cdot (t - k) \end{cases} .$$

Logo, u e v são pares positivos, ou seja, são inteiros positivos de mesma paridade.

Portanto, por *i*), *ii*), *iii*) e *iv*) temos que u e v possuem a mesma paridade, quaisquer que sejam as paridades de b e c. ■

Exemplo 2.3.4 . *Exemplos numéricos:*

i) *Se* $b = 2$ *e* $c = 8$, *então* $u = 8 + 2 = 10$ *e* $v = 8 - 2 = 6$ (u *e* v *são ambos pares*);

ii) *Se* $b = 4$ *e* $c = 9$, *então* $u = 9 + 4 = 13$ *e* $v = 9 - 4 = 5$ (u *e* v *são ambos ímpares*);

iii) *Se* $b = 5$ *e* $c = 12$, *então* $u = 12 + 5 = 17$ *e* $v = 12 - 5 = 7$ (u *e* v *são ambos ímpares*);

iv *Se* $b = 7$ *e* $c = 11$, *então* $u = 11 + 7 = 18$ *e* $v = 11 - 7 = 4$ (u *e* v *são ambos pares*).

Lema 2.3.7 . *Se* u *e* v *são inteiros positivos de mesma paridade, com* $u > v$, *então* $u + v$ *e* $u - v$ *são ambos pares positivos.*

Demonstração: Por hipótese u e v são inteiros positivos de mesma paridade e $u > v$, ou seja, u e v são ambos pares ou ambos ímpares. Sendo assim, analisaremos separadamente cada uma destas possibilidades.

i) Sejam k e t inteiros positivos, com $t > k$, tais que $u = 2t$ e $v = 2k$.

Sendo assim, temos

$$\begin{cases} u + v = 2t + 2k = 2 \cdot (t + k) \\ u - v = 2t - 2k = 2 \cdot (t - k) \end{cases} .$$

Logo, $u + v$ e $u - v$ são pares positivos.

ii) Sejam k e t inteiros positivos, com $t > k$, tais que $u = 2t + 1$ e $v = 2k + 1$.

Sendo assim, temos

$$\begin{cases} u+v = 2t+1+2k+1 = 2t+2k+2 = 2\cdot(t+k+1) \\ u-v = 2t+1-(2k+1) = 2t+1-2k-1 = 2t-2k = 2\cdot(t-k) \end{cases}.$$

Logo, $u+v$ e $u-v$ são pares positivos.

Portanto, por i) e ii), temos que $u+v$ e $u-v$ são ambos pares positivos, para quaisquer possibilidades que satisfaçam a hipótese. ■

Exemplo 2.3.5 . *Exemplos numéricos:*

i) *Se* $u = 84$ *e* $v = 4$, *então* $u+v = 12$ *e* $u-v = 4$ ($u+v$ *e* $u-v$ *são pares*).

ii) *Se* $u = 16$ *e* $v = 14$, *então* $u+v = 30$ *e* $u-v = 2$ ($u+v$ *e* $u-v$ *são pares*).

iii) *Se* $u = 74$ *e* $v = 5$, *então* $u+v = 12$ *e* $u-v = 2$ ($u+v$ *e* $u-v$ *são pares*).

iv) *Se* $u = 19$ *e* $v = 13$, *então* $u+v = 32$ *e* $u-v = 6$ ($u+v$ *e* $u-v$ *são pares*).

Teorema 2.3.4 . (a,b,c) *é um terno pitagórico se, e somente se, existirem inteiros positivos* u *e* v, $u > v$, *de igual paridade, tais que* $u\cdot v$ *seja um quadrado perfeito e* $(a,b,c) = \left(\sqrt{u\cdot v},\ \dfrac{u-v}{2},\ \dfrac{u+v}{2}\right)$.

Demonstração: $\Rightarrow$) Suponhamos que (a,b,c) seja um terno pitagórico. Então, $a^2+b^2 = c^2$, de modo que, $a^2+b^2 = c^2 \ \Rightarrow\ a^2 = c^2-b^2 \ \Rightarrow\ a^2 = (c+b)\cdot(c-b)$. Tomando $u = c+b$ e $v = c-b$, temos:

i) $u\cdot v$ é um quadrado perfeito, pois, $u\cdot v = (c+b)\cdot(c-b) = a^2$.

ii) u e v são inteiros positivos, pois, $c > b$.

iii) u e v possuem a mesma paridade, conforme Lema 2.3.6.

iv) $u > v$, pois, $(c+b) > (c-b)$.

v) Adicionando membro a membro as equações $u = c+b$ e $v = c-b$, temos

$$\begin{cases} u = c+b \\ v = c-b \end{cases} \Rightarrow\ u+v = 2c \ \Rightarrow\ c = \frac{u+v}{2}.$$

Multiplicando a equação $v = c-b$ por (-1), obtemos: $-v = -c+b$. Agora, adicionando membro a membro as equações $u = c+b$ e $-v = -c+b$, vem

$$\begin{cases} u = c + b \\ -v = -c + b \end{cases} \Rightarrow \quad u - v = 2b \quad \Rightarrow \quad b = \frac{u-v}{2}.$$

Temos ainda, $a^2 = c^2 - b^2 = (c+b)\cdot(c-b) = u \cdot v \quad \Rightarrow \quad a = \sqrt{u \cdot v}$.

$\Leftarrow$) Suponhamos que u e v sejam inteiros positivos de mesma paridade, com $u > v$ e que $u \cdot v$ seja um quadrado perfeito. Tomando $a = \sqrt{u \cdot v}$, $b = \frac{u-v}{2}$ e $c = \frac{u+v}{2}$, vem

i) a é um inteiro positivo, pois $u \cdot v$ é um quadrado perfeito.

ii) b e c são inteiros positivos, conforme Lema 2.3.7.

iii) $a^2 + b^2 = \left(\sqrt{u \cdot v}\right)^2 + \left(\frac{u-v}{2}\right)^2 = \left(\frac{u+v}{2}\right)^2 = c^2$.

■

Os valores de u e v que satisfazem às condições deste Teorema, podem ser estabelecidos por tentativas, porém, isto também pode ser feito de forma sistemática, como mostraremos a seguir.

Decompondo um quadrado perfeito em números primos e escrevendo todos os seus divisores inteiros positivos em ordem crescente (ou decrescente), obtém-se todos os pares de números inteiros positivos cujo produto é exatamente o quadrado perfeito tomado inicialmente.

Para isso, basta associarmos o primeiro ao último divisor (que serão sempre o número 1 e o próprio quadrado perfeito), o segundo ao penúltimo, o terceiro ao antepenúltimo, etc...

Após a obtenção de todos esses pares, selecionamos aqueles que possuem elementos de mesma paridade e são distintos entre si.

Observação 2.3.2 *Podemos gerar valores de u e v que satisfazem o Teorema 2.3.4 a partir de qualquer quadrado perfeito maior ou igual a 9, pois todo inteiro positivo maior ou igual a 3 figura como cateto em pelo menos um terno pitagórico, conforme o Teorema 2.5.1 que veremos na Seção 2.5 e a proposição 2.7.2, que veremos na Seção 2.7.*

Exemplo 2.3.6 . *Exemplos de como gerar os números u e v que satisfazem o Teorema 2.3.4 a partir de um quadrado perfeito:*

i) *Valores de u e v gerados a partir do quadrado perfeito* 64*:*

Inicialmente, vamos decompor 64 *em fatores primos e em seguida determinar todos os seus divisores inteitos positivos:*

		1
64	2	2
32	2	4
16	2	8
8	2	16
4	2	32
2	2	64
1		

Sendo assim, os divisores positivos de 64 *em ordem crescente são:* 1*,* 2*,* 4*,* 8*,* 16*,* 32 *e* 64*.*

Logo, os pares de números inteiros positivos cujo produto é 64*, são:* $(1, 64)$*,* $(2, 32)$*,* $(4, 16)$ *e* $(8, 8)$*.*

Destes pares, apenas $(2, 32)$ *e* $(4, 16)$ *têm seus elementos distintos entre si e de mesma paridade.*

Portanto, a partir de 64*, temos:* $u = 32$ *e* $v = 2$ *ou* $u = 16$ *e* $v = 4$*.*

ii) *Valores de u e v gerados a partir do quadrado perfeito* 225*:*

		1
225	3	3
75	3	9
25	5	5, 15, 45
5	5	25, 75, 225
1		

Sendo assim, os divisores positivos de 225 *em ordem crescente são:* 1*,* 3*,* 5*,* 9*,* 15*,* 25*,* 45*,* 75 *e* 225*.*

Logo, os pares de números inteiros positivos cujo produto é 225*, são:* $(1, 225)$*,* $(3, 75)$*,* $(5, 45)$*,* $(9, 25)$ *e* $(15, 15)$*.*

Destes pares, apenas $(15, 15)$ *não satisfaz as condições do teorema, por não serem distindos.*

Portanto, a partir de 225*, temos:* $u = 225$ *e* $v = 1$*,* $u = 75$ *e* $v = 3$*,* $u = 45$ *e* $v = 5$ *ou* $u = 25$ *e* $v = 9$.

Agora, vamos gerar ternos pitagóricos a partir dos valores de u e v obtidos no exemplo acima (exemplo 2.3.6).

Substituiremos tais valores nas equações do Teorema 2.3.4, $a = \sqrt{u \cdot v}$, $b = \dfrac{u - v}{2}$ e $c = \dfrac{u + v}{2}$, obtendo assim o terno pitagórico (a, b, c).

Exemplo 2.3.7 *Ternos Pitagóricos obtidos a partir dos valores de* u *e* v *gerados pelos quadrados perfeitos* 64 *e* 225*:*

1) u *e* v *gerados por* 64*:*

i) Para $u = 32$ *e* $v = 2$*, temos:*

$$\begin{cases} a = \sqrt{u \cdot v} = \sqrt{32 \cdot 2} = \sqrt{64} = 8 \\ b = \dfrac{u - v}{2} = \dfrac{32 - 2}{2} = \dfrac{30}{2} = 15 \\ c = \dfrac{u + v}{2} = \dfrac{32 + 2}{2} = \dfrac{34}{2} = 17 \end{cases}$$

Logo, $(8, 15, 17)$ *é terno pitagórico.*

ii) Para $u = 16$ *e* $v = 4$*, temos:*

$$\begin{cases} a = \sqrt{u \cdot v} = \sqrt{16 \cdot 4} = \sqrt{64} = 8 \\ b = \dfrac{u - v}{2} = \dfrac{16 - 4}{2} = \dfrac{12}{2} = 6 \\ c = \dfrac{u + v}{2} = \dfrac{16 + 4}{2} = \dfrac{20}{2} = 10 \end{cases}$$

Logo, $(8, 6, 10)$ *é terno pitagórico.*

2) u *e* v *gerados por* 225*:*

i) Para $u = 225$ *e* $v = 1$*, temos:*

$$\begin{cases} a = \sqrt{u \cdot v} = \sqrt{225 \cdot 1} = \sqrt{225} = 15 \\ b = \dfrac{u - v}{2} = \dfrac{225 - 1}{2} = \dfrac{224}{2} = 112 \\ c = \dfrac{u + v}{2} = \dfrac{225 + 1}{2} = \dfrac{226}{2} = 113 \end{cases}$$

Portanto, $(15, 112, 113)$ *é terno pitagórico.*

ii) Para $u = 75$ *e* $v = 3$*, temos:*

$$\begin{cases} a = \sqrt{u \cdot v} = \sqrt{75 \cdot 3} = \sqrt{225} = 15 \\ b = \dfrac{u - v}{2} = \dfrac{75 - 3}{2} = \dfrac{72}{2} = 36 \\ c = \dfrac{u + v}{2} = \dfrac{75 + 3}{2} = \dfrac{78}{2} = 39 \end{cases}$$

Logo, $(15, 36, 39)$ *é terno pitagórico.*

iii) Para $u = 45$ *e* $v = 5$*, temos:*

$$\begin{cases} a = \sqrt{u \cdot v} = \sqrt{45 \cdot 5} = \sqrt{225} = 15 \\ b = \dfrac{u - v}{2} = \dfrac{45 - 5}{2} = \dfrac{40}{2} = 20 \\ c = \dfrac{u + v}{2} = \dfrac{45 + 5}{2} = \dfrac{50}{2} = 25 \end{cases}$$

Logo, $(15, 20, 25)$ *é terno pitagórico.*

iv) Para $u = 25$ *e* $v = 9$*, temos:*

$$\begin{cases} a = \sqrt{u \cdot v} \ = \ \sqrt{25.9} \ = \ \sqrt{225} = 15 \\ \\ b = \dfrac{u - v}{2} = \dfrac{25 - 9}{2} = \dfrac{16}{2} = 8 \\ \\ c = \dfrac{u + v}{2} = \dfrac{25 + 9}{2} = \dfrac{34}{2} = 17 \end{cases}$$

Portanto, $(15, 8, 17)$ *é terno pitagórico.*

Observação 2.3.3 . *Como vimos neste exemplo, a partir do quadrado perfeito* 64 *são gerados apenas dois pares de números* u *e* v *que satisfazem as condições do Teorema 2.3.4, sendo assim, podemos afirmar que existem apenas dois ternos pitagóricos que contém o número* 8 *como cateto, a menos de ordem. Vimos também que a partir do quadrado perfeito* 225 *foram gerados quatro pares de números* u *e* v *que também satisfazem o referido teorema, e que estes geraram os seguintes ternos pitagóricos:* $(15, 112, 113)$, $(15, 36, 39)$, $(15, 20, 25)$ *e* $(15, 8, 17)$, *isto responde exatamente a pergunta que inicia esta subseção. De maneira análoga, podemos determinar quantos e quais são os ternos pitagóricos em que um inteiro positivo qualquer, maior ou igual a* 3, *figura como cateto.*

Apresentaremos a seguir uma tabela que contém todos os ternos pitagóricos em que os números inteiros positivos de 3 a 20 figuram como catetos.

Tabela 2.2: Tabela dos ternos pitagóricos em que os números de 3 a 20 figuram como catetos

inteiro positivo a	a^2	u	v	$a = \sqrt{uv}$	$b = \frac{u-v}{2}$	$c = \frac{u+v}{2}$	TP(a,b,c)
3	9	9	1	3	4	5	(3,4,5)
4	16	8	2	4	3	5	(4,3,5)
5	25	25	1	5	12	13	(5,12,13)
6	36	18	2	6	8	10	(6,8,10)
7	49	49	1	7	24	25	(7,24,25)
8	64	32	2	8	15	17	(8,15,17)
8	64	16	4	8	6	10	(8,6,10)
9	81	81	1	9	40	41	(9,40,41)
9	81	27	3	9	12	15	(9,12,15)
10	100	50	2	10	24	26	(10,24,26)
11	121	121	1	11	60	61	(11,60,61)
12	144	72	2	12	35	37	(12,35,37)
12	144	36	4	12	16	20	(12,16,20)
12	144	24	6	12	9	15	(12,9,15)
12	144	18	8	12	5	13	(12,5,13)
13	169	169	1	13	84	85	(13,84,85)
14	196	98	2	14	48	50	(14,48,50)
15	225	225	1	15	112	113	(15,112,113)
15	225	75	3	15	36	39	(15,36,39)
15	225	45	5	15	20	25	(15,20,25)
15	225	25	9	15	8	17	(15,8,17)
16	256	128	2	16	63	65	(16,63,65)
16	256	64	4	16	30	34	(16,30,34)
16	256	32	8	16	12	20	(16,12,20)
17	289	289	1	17	144	145	(17,144,145)
18	324	162	2	18	80	82	(18,80,82)
18	324	54	6	18	24	30	(18,24,30)
19	361	361	1	19	180	181	(19,180,181)
20	400	200	2	20	99	101	(20,99,101)
20	400	100	4	20	48	52	(20,48,52)
20	400	50	8	20	21	29	(20,21,29)
20	400	40	10	20	15	25	(20,15,25)

2.3.4 Um Método Prático de Gerar Ternos Pitagóricos Primitivos

Podemos gerar infinitos *ternos pitagóricos primitivos* através de um método bastante simples, que consiste em somar os inversos de dois números ímpares consecutivos ou os inversos de dois pares consecutivos. Essa soma, gera os catetos de um *triângulo pitagórico primitivo*, que são exatamente o numerador e o denominador da fração (na sua forma irredutível) resultante dessa soma. A hipotenusa excede em duas unidades o denominador caso os números escolhidos inicialmente sejam ímpares e em uma unidade caso sejam escolhidos números pares.

Este método destaca-se principalmente pela sua simplicidade e praticidade, pois, de fato, dentre todas as formas de gerar ternos pitagóricos, esta é a menos burocrática.

Lema 2.3.8 . *Para qualquer k inteiro positivo, $mdc(4k, 4k^2-1, 4k^2+1) = 1$.*

Demonstração: Inicialmente iremos mostrar que $mdc(4k, 4k^2+1) = 1$.

Pelo Lema de Euclides, temos

$$mdc(4k, 4k^2+1) = mdc(4k, 1+k\cdot 4k) = mdc(4k, 1) = 1.$$

Agora, pela Proposição 1.3.12, temos

$$mdc(4k, 4k^2-1, 4k^2+1) = mdc\left(4k^2-1, mdc(4k, 4k^2+1)\right),$$

daí, usando o resultado acima, vem

$$mdc(4k, 4k^2-1, 4k^2+1) = mdc\left(4k^2-1, mdc(4k, 4k^2+1)\right) = mdc(4k^2-1, 1) = 1.$$

■

Teorema 2.3.5 . *Se $a, b \in \mathbb{Z}_+^*$ são, respectivamente o numerador e o denominador da fração resultante da soma dos inversos de dois ímpares consecutivos, então $(a, b, b+2)$ é um terno pitagórico primitivo.*

Demonstração: Note que $2k-1$ e $2k+1$, com $k \in \mathbb{Z}_+^*$, representam dois ímpares positivos consecutivos quaisquer. Efetuando a soma de seus inversos, obtemos

$$\frac{1}{2k-1} + \frac{1}{2k+1} = \frac{2k+1+2k-1}{(2k-1)(2k+1)} = \frac{4k}{4k^2-1}.$$

Daí, tomando $a = 4k$ e $b = 4k^2 - 1$, temos

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

$$a^2 + b^2 = 16k^2 + 16k^4 - 8k^2 + 1$$

$$a^2 + b^2 = 16k^4 + 16k^2 - 8k^2 + 1$$

$$a^2 + b^2 = 16k^4 + 8k^2 + 1$$

$$a^2 + b^2 = (4k^2 + 1)^2$$

$$a^2 + b^2 = [(4k^2 - 1) + 2]^2$$

$$a^2 + b^2 = (b + 2)^2$$

Logo, $(a, b, b + 2)$ é terno pitagórico.

Por outro lado, temos pelo Lema 2.3.8 que $mdc(4k, 4k^2 - 1, 4k^2 + 1) = 1$.

Portanto, $(a, b, b + 2)$ é *terno pitagórico primitivo.* ■

Assim, por exemplo, tomando 1 e 3, obtemos:

$$\frac{1}{1} + \frac{1}{3} = \frac{3+1}{3} = \frac{4}{3}.$$

Logo, $(4, 3, 3 + 2) = (4, 3, 5)$ é TPP.

Exemplo 2.3.8 . *Outros exemplos de Ternos Pitagóricos Primitivos gerados a partir de dois ímpares consecutivos:*

i) 3 *e* 5

$$\frac{1}{3} + \frac{1}{5} = \frac{5+3}{15} = \frac{8}{15}.$$

Logo, $(8, 15, 15 + 2) = (8, 15, 17)$ *é* TPP.

ii) 75 *e* 77

$$\frac{1}{75} + \frac{1}{77} = \frac{77+75}{5775} = \frac{152}{5775}.$$

Logo, $(152, 5775, 5775 + 2) = (152, 5775, 5777)$ *é* TPP.

iii) 317 *e* 319

$$\frac{1}{317}+\frac{1}{319}=\frac{319+317}{101123}=\frac{636}{101123}.$$

Logo, $(636, 101123, 101123+2) = (636, 101123, 101125)$ *é* TPP.

Lema 2.3.9 . *Para qualquer* t *inteiro positivo,* $mdc(2t+1,\ 2t^2+2t) = 1$.

Demonstração: Pelo Lema de Euclides, temos
$mdc(2t+1,\ 2t^2+2t) = mdc\,(2t+1,\ t+t\cdot(2t+1)) = mdc(2t+1,\ t) = mdc(t,\ 1+2\cdot t) =$
$= mdc(t,1) = 1.$ ■

Lema 2.3.10 . *Para qualquer* t *inteiro positivo,* $mdc(2t+1,\ 2t^2+2t,\ 2t^2+2t+1) = 1$.

Demonstração: Pela Proposição 1.3.12, temos
$mdc(2t+1,\ 2t^2+2t,\ 2t^2+2t+1) = mdc\left(2t^2+2t+1, mdc(2t+1,\ 2t^2+1)\right).$
Agora, pelo Lema 2.3.9, temos
$mdc(2t+1,\ 2t^2+2t,\ 2t^2+2t+1) = mdc\left(2t^2+2t+1, mdc(2t+1,\ 2t^2+1)\right) =$
$= mdc(2t^2+2t+1, 1) = 1.$ ■

Teorema 2.3.6 . *Se* $m, n \in \mathbb{Z}_+^*$ *são, respectivamente o numerador e o denominador da fração resultante da soma dos inversos de dois pares consecutivos, na sua forma irredutível, então* $(m, n, n+1)$ *é um terno pitagórico primitivo.*

Demonstração: Note que $2t$ e $2t+2$, com $t \in \mathbb{Z}_+^*$, representam dois pares positivos e consecutivos quaisquer. Efetuando a soma de seus inversos, obtemos

$$\frac{1}{2t}+\frac{1}{2t+2}=\frac{t+1+t}{2t(t+1)}=\frac{2t+1}{2t^2+2t}.$$

Pelo Lema 2.3.9 temos que $mdc(2t+1,\ 2t^2+2t) = 1$, sendo assim, a fração $\dfrac{2t+1}{2t^2+2t}$ está na forma irredutível.
Agora, tomando $m = 2t+1$ e $n = 2t^2+2t$, vem

$$m^2+n^2 = (2t+1)^2+(2t^2+2t)^2$$

$$m^2+n^2 = 4t^2+4t+1+4t^4+8t^3+4t^2$$

$$m^2+n^2 = 4t^4+8t^3+4t^2+4t^2+4t+1$$

$$m^2 + n^2 = 4t^4 + 8t^3 + 8t^2 + 4t + 1$$

$$m^2 + n^2 = (2t^2 + 2t + 1)^2$$

$$m^2 + n^2 = [(2t^2 + 2t) + 1]^2$$

$$m^2 + n^2 = (n + 1)^2$$

Logo, $(m, n, n + 1)$ é terno pitagórico.

Por outro lado, temos pelo Lema 2.3.10 que $mdc(2t + 1, 2t^2 + 2t, 2t^2 + 2t + 1) = 1$.

Portanto, $(m, n, n + 1)$ é *terno pitagórico primitivo.* ■

Assim, por exemplo, tomando 2 e 4, obtemos

$$\frac{1}{2} + \frac{1}{4} = \frac{2+1}{4} = \frac{3}{4}.$$

Logo, $(3, 4, 4 + 1) = (3, 4, 5)$ é TPP.

Exemplo 2.3.9 . *Outros exemplos de Ternos Pitagóricos Primitivos gerados a partir de dois pares consecutivos:*

i) 4 *e* 6

$$\frac{1}{4} + \frac{1}{6} = \frac{3+2}{12} = \frac{5}{12}$$

Logo, $(5, 12, 12 + 1) = (5, 12, 13)$ *é* TPP.

ii) 106 *e* 108

$$\frac{1}{106} + \frac{1}{108} = \frac{54+53}{5724} = \frac{107}{5724}$$

Logo, $(107, 5724, 5724 + 1) = (107, 5724, 5725)$ *é* TPP.

iii) 228 *e* 230

$$\frac{1}{228} + \frac{1}{230} = \frac{115+114}{26220} = \frac{229}{26220}$$

Logo, $(229, 26220, 26220 + 1) = (229, 26220, 26221)$ *é* TPP.

2.4 Gerando Ternos Pitagóricos a Partir de Dois Outros Ternos Pitagóricos

Uma identidade famosa atribuída ao grego Diofanto (325 - 409 d.C) mostra que dados dois inteiros que podem ser escritos como soma de dois outros quadrados, o seu produto também é soma de dois quadrados. Em outras palavras, Diofanto estabeleceu com esta identidade uma maneira de relacionar dois ternos pitagóricos, de forma que a partir destes fosse gerado um terceiro.

Teorema 2.4.1 . *Se* (a, b, c) *e* (x, y, z), *com* $a > b$ *e* $x > y$, *são ternos pitagóricos, então* $(ax - by, ay + bx, cz)$ *também é terno pitagórico.*

Demonstração: Supondo que (a, b, c) e (x, y, z) são ternos pitagóricos, com $a > b$ e $x > y$, temos que $a^2 + b^2 = c^2$ e $x^2 + y^2 = z^2$.

Daí,

$c^2 \cdot z^2 = (a^2 + b^2) \cdot (x^2 + y^2)$

$c^2 \cdot z^2 = a^2x^2 + a^2y^2 + b^2x^2 + b^2y^2$

$c^2 \cdot z^2 = a^2x^2 + a^2y^2 + b^2x^2 + b^2y^2 + 2abxy - 2abxy$

$c^2 \cdot z^2 = a^2x^2 - 2abxy + b^2y^2 + a^2y^2 + 2abxy + b^2x^2$

$c^2 \cdot z^2 = (ax)^2 - 2 \cdot (ax) \cdot (by) + (by)^2 + (ay)^2 + 2 \cdot (ay) \cdot (bx) + (bx)^2$

$c^2 \cdot z^2 = (ax - by)^2 + (ay + bx)^2$

$(c \cdot z)^2 = (ax - by)^2 + (ay + bx)^2$

Portanto, $(ax - by, ay + bx, cz)$ é terno pitagórico. ■

Exemplo 2.4.1 . *Exemplos de ternos pitagóricos gerados a partir de outros dois ternos pitagóricos:*

i) $(4, 3, 5)$ *e* $(12, 5, 13)$ *são ternos pitagóricos, pois,* $4^2 + 3^2 = 5^2$ *e* $12^2 + 5^2 = 13^2$.

Logo, $(4 \cdot 12 - 3 \cdot 5, 4 \cdot 5 + 3 \cdot 12, 5 \cdot 13) = (48 - 15, 20 + 36, 65) = (33, 56, 65)$ *é terno pitagórico.*

ii) $(15, 8, 17)$ *e* $(8, 6, 10)$ *são ternos pitagóricos, pois,* $15^2 + 8^2 = 17^2$ *e* $8^2 + 6^2 = 10^2$.

Logo, $(15 \cdot 8 - 8 \cdot 6, 15 \cdot 6 + 8 \cdot 8, 17 \cdot 10) = (120 - 48, 90 + 64, 170) = (72, 154, 170)$ *é terno pitagórico.*

iii) $(24, 7, 25)$ *é terno pitagórico, pois,* $24^2 + 7^2 = 25^2$.

Logo, relacionando $(24, 7, 25)$ *com o próprio* $(24, 7, 25)$, *temos:*

$(24 \cdot 24 - 7 \cdot 7, 24 \cdot 7 + 7 \cdot 24, 25 \cdot 25) = (576 - 49, 168 + 168, 625) = (527, 336, 625)$.

Portanto, $(527,\ 336,\ 625)$ *é terno pitagórico.*

2.5 Uma Propriedade Importante dos Ternos Pitagóricos

O teorema abaixo nos revela uma propriedade realmente importante, pois, nos garante que dado um inteiro maior ou igual a 3, existe pelo menos um *terno pitagórico* no qual este número figura como cateto.

Teorema 2.5.1 . *Para todo inteiro positivo* $a > 2$ *existem inteiros positivos* b *e* c *tais que* (a, b, c) *é um terno pitagórico.*

Demonstração: Suponhamos, primeiro, que o inteiro $a > 2$ é par. Então, $2|a$ e $4|a^2$, de modo que

$$b = \frac{a^2 - 4}{4} \text{ e } c = \frac{a^2 + 4}{4}$$

são dois inteiros positivos.
E como

$$a^2 + b^2 = a^2 + \frac{a^4 - 8a^2 + 16}{16} = \frac{16a^2 + a^4 - 8a^2 + 16}{16} = \left(\frac{a^2 + 4}{4}\right)^2 = c^2,$$

segue que (a, b, c) é um *terno pitagórico.*

Suponha, agora, que o inteiro $a > 2$ é ímpar. Então, $a = 2k + 1$ e as *fórmulas*:

$$a = 2k + 1,\ b = 2k^2 + 2k \text{ e } c = 2k^2 + 2k + 1,$$

onde k é um inteiro positivo maior ou igual a 1, dão o *terno pitagórico* (a, b, c), como vimos no Teorema 2.3.2. ■

2.6 O *Primo de Mersenne* e o *Primo de Fermat* que Dividem o Produto dos Elementos de Qualquer Terno Pitagórico

Vimos na Seção 1.3.6 que os *Primos de Mersenne e de Fermat* são números famosos, isto porque, eles homenageiam exatamente estes brilhantes matemáticos: Marin Mersenne e Pierre de Fermat, respectivamente.

Demonstraremos a seguir que o primeiro *Primo de Mersenne* e o *Primo de Fermat*, ou seja, 3 e 5, também se destacam aqui no nosso trabalho, pois eles dividem o produto dos elementos de qualquer Terno Pitagórico.

Teorema 2.6.1 . *Se* (a, b, c) *é um terno pitagórico, então* $3|ab$ *e* $5|abc$.

Demonstração: Notemos inicialmente que, é suficiente tomarmos aqui um *terno pitagórico primitivo*, pois, como já vimos no começo do capítulo 2 deste trabalho, a partir de um $TPP(a, b, c)$, geramos todos os $TP(ka, kb, kc)$, onde k é um inteiro positivo tal que $k \geq 1$. De fato, se $3|ab$ e $5|abc$, então, $3|ka \cdot kb$ e $5|ka \cdot kb \cdot kc$.

Sendo assim, usaremos aqui as Equações Paramétricas de Euclides (Teorema 2.3.1).

Logo, mostrar que $3|ab$ e $5|abc$, equivale, respectivamente, a mostra que

$$3|(m^2 - n^2) \cdot 2mn \text{ e } 5|(m^2 - n^2) \cdot 2mn \cdot (m^2 + n^2).$$

De fato, temos

i) Se $3|m$ ou $3|n$, então $3|b$, implicando que $3|ab$;

ii) Se $3 \nmid m$ e $3 \nmid n$, então, pelo *Pequeno Teorema de Fermat* (Corolário 1.3.3), temos

$$3|m^2 - 1 \text{ e } 3|n^2 - 1.$$

Logo, $\exists \alpha, \beta \in \mathbb{Z}_+$ tais que

$$\begin{cases} m^2 - 1 = 3\alpha \text{ (I)} \\ n^2 - 1 = 3\beta \text{ (II)} \end{cases}$$

Subtraindo membro a membro (II) de (I), vem

$$m^2 - n^2 = 3(\alpha - \beta) \quad \Rightarrow \quad 3|m^2 - n^2 \quad \Rightarrow \quad 3|a \quad \Rightarrow \quad 3|ab.$$

Portanto, por i) e ii), temos que $3|ab$ para quaisquer m e n que satisfaçam as condições estabelecidas no teorema 2.3.1.

Agora, de modo análogo, mostraremos que $5|abc$.

Note, inicialmente, que

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

daí,

i) Se $5|m$ ou $5|n$, então $5|b$, implicando que $5|abc$;

ii) Se $5 \not| m$ e $5 \not| n$, então, pelo *Pequeno Teorema de Fermat* (Corolário 1.3.3), temos

$$5|m^4 - 1 \text{ e } 5|n^4 - 1.$$

Logo, $\exists \delta, \theta \in \mathbb{Z}_+$ tais que

$$\begin{cases} m^4 - 1 = 5\delta \text{ (I)} \\ n^4 - 1 = 5\theta \text{ (II)} \end{cases}$$

Subtraindo membro a membro (II) de (I), vem

$$m^4 - n^4 = 5(\delta - \theta) \quad \Rightarrow \quad 5|m^4 - n^4 \quad \Rightarrow \quad 5|ac \quad \Rightarrow \quad 5|abc.$$

Portanto, por i) e ii), temos que $5|abc$ para quaisquer m e n que satisfaçam as condições estabelecidas no teorema 2.3.1.

■

Observação 2.6.1 . *Além desses dois importantes resultados, temos ainda que,* $4|abc$. *Esse fato é facilmente comprovado, pois,* m *e* n *possuem paridade distinta e* $b = 2mn$. *Daí, tomando* $m = 2k$ *e* $n = 2t+1$ *com* k *e* t *inteiros positivos, sem perca de generalidade, temos que* $b = 4 \cdot k \cdot (2t + 1)$, *logo* $4|b$, *implicando que* $4|abc$.

2.7 O Notável Terno Pitagórico: $(3, 4, 5)$

Documentos comprovam que os egípcios e os babilônicos conheciam casos particulares do Teorema de Pitágoras. Documentos datados de mais de 1000 anos a.C. comprovam que na Índia sabia-se que o triângulo de lados 3, 4 e 5 era retângulo. Portanto, é provável que alguns *ternos pitagóricos* já eram conhecidos antes mesmo do próprio teorema de Pitágoras. O terno $(3, 4, 5)$, por exemplo, seria facilmente encontrado aritmeticamente e isto poderia ter incentivado uma busca por outros ternos.

Para construir uma casa, além de todo planejamento inicial, deve-se marcar o terreno de acordo com a planta. Em geral, as paredes devem estar esquadrejadas (formar cantos com ângulos retos). Porém, como marcar esses ângulos retos?

Alguns historiadores afirmavam que os egípcios já conheciam a terna pitagórica 3, 4 e 5 e que esse terno formava um triângulo retângulo. Sendo assim, eles esticavam uma corda com 12 nós, separados igualmente, e formavam um triângulo com os lados 3, 4 e 5 e determinavam o ângulo reto.

Assim, mesmo não conhecendo formalmente o teorema de Pitágoras, foi possível edificar grandes construções como as pirâmides do Egito entre outras.

Mas afinal, porque estes números pitagóricos são os mais conhecidos e famosos? Dentre os infinitos ternos pitagóricos existentes, o que o faz ser tão especial?

Uma possível resposta a essas perguntas é o fato de que este é o terno pitagórico mais simples de todos, facilmente encontrado aritmeticamente, como já foi observado acima. Porém, além disso, ele possui outras características exclusivas, como veremos a seguir.

Proposição 2.7.1 . $(3, 4, 5)$ *é o único terno pitagórico cujos termos são três inteiros positivos consecutivos.*

Demonstração: Note que k, $k + 1$ e $k + 2$, com $k \in \mathbb{Z}_+^*$, representam três inteiros positivos consecutivos.
Supondo que (a, b, c) é um terno pitagórico e que $a = k$, $b = k + 1$ e $c = k + 2$, temos

$$a^2 + b^2 = c^2$$

$$(k)^2 + (k + 1)^2 = (k + 2)^2$$

$$k^2 + k^2 + 2k + 1 = k^2 + 4k + 4$$

$$k^2 - 2k - 3 = 0.$$

Que implica $k = -1$ ou $k = 3$.

Porém, por hipótese k é um inteiro positivo, portanto, $k = -1$ não convém. Sendo assim, temos $k = 3$, que implica: $a = 3$, $b = 4$ e $c = 5$. ■

Proposição 2.7.2 . *O número* 3 *é o menor inteiro positivo que figura como cateto em um terno pitagórico.*

Demonstração: Os inteiros positivos menores que 3 são: 0, 1 e 2.

Na primeira subseção do Capítulo 2 deste trabalho (Definição 2.1.1), vimos que, se (a, b, c) é um terno pitagórico, então a e b são números inteiros positivos que representam as medidas dos catetos de um triângulo retângulo e c, consequentemente, é também um inteiro positivo, que representa a hipotenusa deste triângulo.

Portanto, o 0 (zero) não figura como cateto de um terno pitagórico, pois, a e b representam as medidas de dois lados de um triângulo.

Sendo assim, resta mostrar que 1 e 2 não figuram como cateto em nenhum terno pitagórico e que o número 3 figura.

Seja (a, b, c) um terno pitagórico. Tomando $a = 1$, sem perca de generalidade, temos

$$1^2 + b^2 = c^2$$

$$1 + b^2 = c^2$$

$$1 = c^2 - b^2$$

$$1 = (c + b) \cdot (c - b).$$

A única forma de representar o número 1 como produto de dois inteiros positivos é:

$$1 = 1 \cdot 1.$$

Sendo assim, $c + b = 1$ e $c - b = 1$, implicando $b = 0$. Porém, como vimos acima, 0(zero) não figura como cateto de um terno pitagórico.

Logo, o número 1 não figura como cateto de um terno pitagórico.

Agora, tomando $a = 2$, de modo análogo, temos:

$$4 = (c + b) \cdot (c - b).$$

Existem apenas duas maneiras distintas de representar o número 4 como produto de dois inteiros positivos:

$$4 = 2 \cdot 2 = 4 \cdot 1.$$

Sendo assim, temos:

i) $c + b = 2$ e $c - b = 2$, que implica $b = 0$;

ii) $c + b = 4$ e $c - b = 1$, que implica $b = \dfrac{5}{2} = 2,5$.

Logo, por i) e ii), concluimos que o número 2 também não figura como cateto de um terno pitagórico.

Por outro lado, pelo Teorema 2.5, temos a garantia de que todo inteiro positivo maior ou igual a 3 figura como cateto em pelo menos um terno pitagórico. ■

Proposição 2.7.3 . *Se (a, b, c) é um terno pitagórico, então $a \neq b$.*

Demonstração: Suponhamos que exista um terno pitagórico (a, b, c) tal que $a = b$. Desse modo, existe x, $x \in \mathbb{Z}_+^*$, tal que $a = b = x$.
Daí,

$$c^2 = a^2 + b^2$$

$$c^2 = x^2 + x^2$$

$$c^2 = 2x^2$$

$$\sqrt{c^2} = \sqrt{2x^2}$$

$$c = x\sqrt{2}.$$

Sendo assim, c não é um número inteiro, contrariando a definição de terno pitagórico (Definição 2.1.1). ■

Proposição 2.7.4 . *O terno* $(3,4,5)$ *é o triângulo pitagórico de menor área e de menor perímetro.*

Demonstração: Pela Proposição 2.7.2, vimos que 3 é o menor inteiro positivo que figura como cateto num terno pitagórico e pela Proposição 2.7.3 vimos que os catetos de um terno pitagórico são sempre distintos entre si. Isto nos garante que $(3,4,5)$ é o terno pitagórico que possui os menores elementos.

Portanto, ele gera a menor área $\left(\frac{3\cdot 4}{2} = \frac{12}{2} = 6\right)$ e o menor perímetro $(3+4+5=12)$. ■

Proposição 2.7.5 . *Se* (a,b,c) *é um terno pitagórico, então o produto dos elementos do* $TP(3,4,5)$ *divide* $a\cdot b\cdot c$*, ou seja,* $60|abc$.

Demonstração: Pelo Teorema 2.6.1 e pela Observação 2.6.1, temos que $3|abc$, $4|abc$ e $5|abc$.

Sendo assim, pela Proposição 1.3.11, temos

$$\frac{3\cdot 4}{mdc(3,4)}|abc \quad \Rightarrow \quad 12|abc.$$

Agora, novamente pela Proposição 1.3.11, temos

$$\frac{12\cdot 5}{mdc(12,5)}|abc \quad \Rightarrow \quad 60|abc.$$

■

Exemplo 2.7.1 . *Daremos abaixo alguns exemplos numéricos desta proposição:*

i) $(5,12,13)$ *é terno pitagórico, pois,* $5^2+12^2=13^2$. *O produto de seus elementos é* $5\cdot 12\cdot 13 = 780$, *que é múltiplo de* 60, *pois,* $780 = 60\cdot 13$.

ii) $(96,2303,2305)$ *é terno pitagórico, pois,* $96^2+2303^2=2305^2$. *O produto de seus elementos é* $96\cdot 2303\cdot 2305 = 509\ 607\ 840$, *que é múltiplo de* 60, *pois,* $509\ 607\ 840 = 60\cdot 8\ 493\ 464$.

iii) $(840,1702,1898)$ *é terno pitagórico, pois,* $840^2+1702^2=1898^2$. *O produto de seus elementos é* $840\cdot 1702\cdot 1898 = 2\ 713\ 532\ 640$, *que é múltiplo de* 60, *pois,* $2\ 713\ 532\ 640 = 60\cdot 45\ 225\ 544$.

Capítulo 3

Aplicações

Neste Capítulo apresentaremos alguns exercícios pertinentes com o propósito de evidenciar e complementar alguns tópicos relevantes do nosso trabalho.

1ª). Construir três ternos pitagóricos (a, b, c) tais que os elementos b e c sejam inteiros consecutivos.

Seja k um inteiro positivo. Desse modo, k e $k+1$ representam dois inteiros consecutivos quaisquer.

Temos assim, $b = k$ e $c = k+1$, com $k \geq 3$, pois o menor número inteiro que figura num triângulo pitagórico como cateto é 3 (Proposição 2.7.2).

Como (a, b, c) é terno pitagórico, temos $a^2 + b^2 = c^2$. Substituindo b por k e c por $k+1$, temos

$$a^2 + b^2 = c^2$$

$$a^2 + (k)^2 = (k+1)^2$$

$$a^2 + k^2 = k^2 + 2 \cdot k \cdot 1 + 1^2$$

$$a^2 + k^2 = k^2 + 2k + 1$$

$$a^2 = 2k + 1$$

$$a = \sqrt{2k+1}.$$

Logo, $(a, b, c) = (\sqrt{2k+1},\ k,\ k+1)$.

Agora, determinaremos, quais valores de k, $k \geq 3$, geram uma tripla de inteiros positivos. Para isso, analisaremos $\sqrt{2k+1}$, que é o único elemento que não é inteiro para qualquer k inteiro.

Sendo assim, resolveremos as equações irracionais da forma $\sqrt{2k+1} = a$, para determinar os valores convenientes de k, onde, a é um número ímpar maior ou igual a 3, visto que o radicando $2k+1$ é sempre ímpar, para qualquer k inteiro positivo.

i) Para $a = 3$, temos

$$\sqrt{2k+1} = 3$$

$$(\sqrt{2k+1})^2 = (3)^2$$

$$2k + 1 = 9$$

$$2k = 8$$

$$k = 4.$$

Logo, $(a, b, c) = (\sqrt{2k+1}, 4, 4+1) = (3, 4, 5)$.

ii) Para $a = 5$, temos

$$\sqrt{2k+1} = 5$$

$$(\sqrt{2k+1})^2 = (5)^2$$

$$2k + 1 = 25$$

$$2k = 24$$

$$k = 12.$$

Logo, $(a, b, c) = (\sqrt{2k+1}, 12, 12+1) = (5, 12, 13)$.

iii) Para $a = 7$, temos

$$\sqrt{2k+1} = 7$$

$$(\sqrt{2k+1})^2 = (7)^2$$

$$2k + 1 = 49$$

$$2k = 48$$

$$k = 24.$$

Logo, $(a, b, c) = (\sqrt{2k+1}, 24, 24+1) = (7, 24, 25)$.

2ª). Construir três ternos pitagóricos (a, b, c) tais que o elemento c exceda em 8 unidades o elemento b.

Seja k um inteiro positivo. Desse modo, podemos escrever $b = k$ e $c = k + 8$. Logo,

$$a^2 + b^2 = c^2$$

$$a^2 + (k)^2 = (k+8)^2$$

$$a^2 + k^2 = k^2 + 2 \cdot k \cdot 8 + 8^2$$

$$a^2 + k^2 = k^2 + 16k + 64$$

$$a^2 = 16k + 64$$

$$a^2 = 16 \cdot (k+4)$$

$$a = \sqrt{16 \cdot (k+4)}$$

$$a = 4\sqrt{k+4}.$$

Sendo assim, $(a, b, c) = (4\sqrt{k+4},\ k,\ k+8)$.

De modo análogo ao exercício anterior, determinaremos os três primeiros valores de k que gera uma tripla de inteiros positivos.

$$\begin{cases} \sqrt{k+4} = 3 \\ (\sqrt{k+4})^2 = (3)^2 \\ k+4 = 9 \\ k = 5 \end{cases}, \quad \begin{cases} \sqrt{k+4} = 4 \\ (\sqrt{k+4})^2 = (4)^2 \\ k+4 = 16 \\ k = 12 \end{cases} \quad \text{e} \quad \begin{cases} \sqrt{k+4} = 5 \\ (\sqrt{k+4})^2 = (5)^2 \\ k+4 = 25 \\ k = 21 \end{cases}.$$

Portanto,

i) Para $k = 5$, temos: $(4 \cdot \sqrt{5+4},\ 5,\ 5+8)$=$(12, 5, 13)$.

ii) Para $k = 12$, temos: $(4 \cdot \sqrt{12+4},\ 12,\ 12+8)$=$(16, 12, 20)$.

iii) Para $k = 21$, temos: $(4 \cdot \sqrt{21+4},\ 21,\ 21+8)$=$(20, 21, 29)$.

3ª). Achar três ternos pitagóricos distintos da forma $(16, b, c)$.

Como $(16, b, c)$ é terno pitagórico, temos:

$$16^2 + b^2 = c^2$$

$$256 = c^2 - b^2$$

$$256 = (c+b) \cdot (c-b).$$

Mas,

		1
256	2	2
128	2	4
64	2	8
32	2	16
16	2	32
8	2	64
4	2	128
2	2	256
1		

Logo, os divisores de 256 em ordem crescente são: 1, 2, 4, 8, 16, 32, 64, 128 e 256.

Notemos que: $1 \cdot 256 = 2 \cdot 128 = 4 \cdot 64 = 8 \cdot 32 = 16 \cdot 16 = 256$.

Daí,

i) Tomando $c + b = 128$ e $c - b = 2$, temos:

$$\begin{cases} c + b = 128 \\ c - b = 2 \end{cases} \quad \Rightarrow \quad 2c = 130 \quad \Rightarrow \quad c = 65 \text{ e } b = 63.$$

Logo, $(16, 63, 65)$ é terno pitagórico.

ii) Tomando $c+b=64$ e $c-b=4$, temos:

$$\begin{cases} c+b=64 \\ c-b=4 \end{cases} \Rightarrow \quad 2c=68 \quad \Rightarrow \quad c=34 \text{ e } b=30.$$

Logo, $(16,30,34)$ é terno pitagórico.

iii) Tomando $c+b=32$ e $c-b=8$, temos:

$$\begin{cases} c+b=32 \\ c-b=8 \end{cases} \Rightarrow \quad 2c=40 \quad \Rightarrow \quad c=20 \text{ e } b=12.$$

Logo, $(16,12,20)$ é terno pitagórico.

Portanto, os três ternos pitagóricos primitivos da forma $(16,b,c)$ são: $(16,12,20)$; $(16,30,34)$ e $(16,63,65)$.

4ª). Achar todos os ternos pitagóricos da forma $(40,b,c)$.

De maneira análoga ao exercício anterior, concluimos que os ternos pitagóricos da forma $(40,b,c)$ são:

$$(40,\ 9,\ 41),\ (40,\ 30,\ 50),\ (40,\ 42,\ 58),\ (40,\ 75,\ 85),\ (40,\ 96,\ 104),\ (40,\ 198,\ 202) \text{ e } (40,\ 399,\ 401).$$

Porém, $mdc(40,\ 9,\ 41)=1$, $mdc(40,\ 30,\ 50)=10$, $mdc(40,\ 42,\ 58)=2$, $mdc(40,\ 75,\ 85)=5$, $mdc(40,\ 96,\ 104)=8$, $mdc(40,\ 198,\ 202)=2$ e, $mdc(40,\ 399,\ 401)=1$.

Portanto, os ternos pitagóricos primitivos da forma $(40,b,c)$ são $(40,\ 399,\ 401)$ e $(40,\ 9,\ 41)$.

5ª). Mostrar que $(3n,4n,5n)$, onde $n=1,2,3,...$, são os únicos ternos pitagóricos cujos elementos estão em progressão aritmética.

Sejam x um inteiro positivo e $n=1,2,3,...$, de modo que $x \geq n+3$.

Seja ainda, $(x-n,x,x+n)$ um terno pitagórico tal que, $x-n$, x e $x+n$, sejam, nessa ordem, uma Progressão Aritmética crescente de razão n.

Sendo assim,

$$(x-n)^2+(x)^2=(x+n)^2$$

$$x^2-2xn+n^2+x^2=x^2+2xn+n^2$$

$$-2xn+x^2=2xn$$

$$x^2=2xn+2xn$$

$$x^2=4xn \quad (\div x)$$

$$x=4n.$$

Portanto, $(x-n, x, x+n)=(3n, 4n, 5n)$.

6ª). Sejam a, b, c e q, números inteiros positivos, com $a<b<c$ e $q>1$, onde a, b e c são respectivamente, termos consecutivos de uma Prograssão Geométrica de razão q. Mostrar que (a, b, c) não é um terno pitagórico.

Por hipótese, (a, b, c) são termos consecutivos de uma Progressão Geométrica de razão q, com a, b, c e q inteiros positivos, $a<b<c$ e $q>1$. Desse modo, existem inteiros positivos a_k, com $k=1, 2, 3, 4, ...$, tais que

$$(a,\ b,\ c)=(a_k,\ a_{k+1},\ a_{k+2})=(a_k,\ a_k\cdot q,\ a_k\cdot q^2).$$

Agora, supondo que (a, b, c) é um terno pitagórico, vem

$$c^2=a^2+b^2$$

$$\left(a_k\cdot q^2\right)^2=(a_k)^2+(a_k\cdot q)^2$$

$$a_k^2\cdot q^4=a_k^2+a_k^2\cdot q^2$$

$$a_k^2\cdot q^4=a_k^2\cdot\left(1+q^2\right) \qquad \left(\div\ a_k^2\right)$$

$$q^4=1+q^2$$

$$q^4-q^2-1=0.$$

Resolvendo essa equação, obtemos como única raiz real positiva, $q = \sqrt{\dfrac{1+\sqrt{5}}{2}}$, que não é inteiro, contradizendo assim a hipótese.

Portanto, (a, b, c) não é um terno pitagórico.

7ª). Mostrar que, se a é um inteiro positivo ímpar, então existe um terno pitagórico (a, b, c) tal que $c = b + 1$.

Por hipótese, a é impar, logo, $\exists\ k$, $k \in \mathbb{Z}_+^*$, tal que $a = 2k + 1$.

Daí,

$$a^2 = (2k+1)^2$$

$$a^2 = 4k^2 + 4k + 1$$

$$a^2 = 2 \cdot (2k^2 + 2k) + 1$$

$$a^2 = 2 \cdot t + 1, \text{ para } t = 2k^2 + 2k.$$

Logo, a^2 também é ímpar.

Por outro lado, como (a, b, c) é terno pitagórico, temos:

$$a^2 + b^2 = c^2$$

$$a^2 = c^2 - b^2$$

$$a^2 = (c+b) \cdot (c-b).$$

Como a^2 é ímpar, $c + b$ e $c - b$ são, necessariamente, ímpares também.

Tomando $c + b = a^2$ e $c - b = 1$, vem

$$\begin{cases} c + b = a^2 \\ c - b = 1 \end{cases} \Rightarrow \quad 2c = a^2 + 1 \quad \Rightarrow \quad 2c = 2t + 1 + 1 \quad \Rightarrow \quad c = t + 1 \quad \Rightarrow \quad b = t\,.$$

8ª). Seja (a, b, c) um terno pitagórico. Mostrar:

$$\frac{c+b}{a} = \sqrt{\frac{c+b}{c-b}}.$$

Temos por hipótese que (a, b, c) é terno pitagórico, sendo assim, $a^2+b^2 = c^2$, o que implica que $a^2 = (c + b) \cdot (c - b)$.
Desse modo,

$$c + b = c + b$$

$$(c + b)^2 = (c + b)^2$$

$$\frac{(c + b)^2}{a^2} = \frac{(c + b)^2}{a^2}$$

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

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

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

$$\frac{c + b}{a} = \sqrt{\frac{(c + b)}{(c - b)}}.$$

9ª). Demonstrar que em um terno pitagórico (a, b, c), um dos elementos a, b ou c é divisível por 5.

Demonstração: Demonstraremos este resultado através da congruência módulo m, apresentada na Seção 1.4 (congruências) do Capítulo 1 deste trabalho.

Pelas equacões de Euclides (teorema 2.3.1), $(a,\ b,\ c)$ é TPP se, e somente se, $a = m^2 - n^2$, $b = 2mn$ e $c = m^2 + n^2$, com $m,\ n \in \mathbb{Z}_+^*$,$m > n$, m e n relativamente primos e de paridade distinta.

Primeiramente, notemos que $a \equiv 0\ mod\ m$, significa que a é um múltiplo de m, ou seja, $m|a$ (m divide a) e que todo inteiro positivo é congruente a 0, 1, 2, 3 ou 4 módulo 5, ou seja, se $a \equiv b\ mod\ 5$, com $a \in \mathbb{Z}_+$, então $b \in \{0, 1, 2, 3, 4\}$.

Notemos ainda que:

i) Se $a \equiv 0\ mod\ 5$, então $a \in \{0, 5, 10, 15, 20, 25, 30, 35, 40, ...\}$;

ii) Se $a \equiv 1\ mod\ 5$, então $a \in \{1, 6, 11, 16, 21, 26, 31, 36, 41, ...\}$;

iii) Se $a \equiv 2\ mod\ 5$, então $a \in \{2, 7, 12, 17, 22, 27, 32, 37, 42, ...\}$;

iv) Se $a \equiv 3 \ mod \ 5$, então $a \in \{3, 8, 13, 18, 23, 28, 33, 38, 43, ...\}$;

v) Se $a \equiv 4 \ mod \ 5$, então $a \in \{4, 9, 14, 19, 24, 29, 34, 39, 44, ...\}$.

Desse modo, para qualquer combinação de $m \equiv i \ mod \ 5$ e $n \equiv j \ mod \ 5$, com $i, j \in \{0, 1, 2, 3, 4\}$, existem $m, \ n \in \mathbb{Z}_+^*$, com $m > n$, m e n relativamente primos e de paridade distinta , exceto para a combinação $m \equiv 0 \ mod \ 5$ e $n \equiv 0 \ mod \ 5$, pois neste caso, temos a garantia de que 5 divide m e n, sendo assim, $mdc(m, n) \neq 1$.

Analisaremos caso a caso as possibilidades para m e n:

I) $m \equiv 0 \ mod \ 5$ e $\begin{cases} n \equiv 1 \ mod \ 5 \\ n \equiv 2 \ mod \ 5 \\ n \equiv 3 \ mod \ 5 \\ n \equiv 4 \ mod \ 5 \end{cases}$.

Para estas possibilidades, $5|b$. Pois, $5|m$, logo, $5|b = 2mn$.

II) $m \equiv 1 \ mod \ 5$ e $\begin{cases} n \equiv 0 \ mod \ 5 \\ n \equiv 1 \ mod \ 5 \\ n \equiv 2 \ mod \ 5 \\ n \equiv 3 \ mod \ 5 \\ n \equiv 4 \ mod \ 5 \end{cases}$.

i) Se $m \equiv 1 \ mod \ 5$ e $n \equiv 0 \ mod \ 5$, então $5|b$. Pois, $5|n$, logo, $5|b = 2mn$.

ii) Se $m \equiv 1 \ mod \ 5$ e $n \equiv 1 \ mod \ 5$, então $5|a$. Pois, $a = m^2 - n^2 \equiv 1^2 - 1^2 \equiv 0 \ mod \ 5$.

iii) Se $m \equiv 1 \ mod \ 5$ e $n \equiv 2 \ mod \ 5$, então $5|c$. Pois, $c = m^2 + n^2 \equiv 1^2 + 2^2 \equiv 0 \ mod \ 5$.

iv) Se $m \equiv 1 \ mod \ 5$ e $n \equiv 3 \ mod \ 5$, então $5|c$. Pois, $c = m^2 + n^2 \equiv 1^2 + 3^2 \equiv 0 \ mod \ 5$.

v) Se $m \equiv 1 \ mod \ 5$ e $n \equiv 4 \ mod \ 5$, então $5|a$. Pois, $a = m^2 - n^2 \equiv 1^2 - 4^2 \equiv 0 \ mod \ 5$.

III) $m \equiv 2 \ mod \ 5$ e $\begin{cases} n \equiv 0 \ mod \ 5 \\ n \equiv 1 \ mod \ 5 \\ n \equiv 2 \ mod \ 5 \\ n \equiv 3 \ mod \ 5 \\ n \equiv 4 \ mod \ 5 \end{cases}$.

i) Se $m \equiv 2 \ mod \ 5$ e $n \equiv 0 \ mod \ 5$, então $5|b$. Pois, $5|n$, logo, $5|b = 2mn$.

ii) Se $m \equiv 2 \ mod \ 5$ e $n \equiv 1 \ mod \ 5$, então $5|c$. Pois, $c = m^2 + n^2 \equiv 2^2 + 1^2 \equiv 0 \ mod \ 5$.

iii) Se $m \equiv 2\ mod\ 5$ e $n \equiv 2\ mod\ 5$, então $5|a$. Pois, $a = m^2 - n^2 \equiv 2^2 - 2^2 \equiv 0\ mod\ 5$.

iv) Se $m \equiv 2\ mod\ 5$ e $n \equiv 3\ mod\ 5$, então $5|a$. Pois, $a = m^2 - n^2 \equiv 2^2 - 3^2 \equiv 0\ mod\ 5$.

v) Se $m \equiv 2\ mod\ 5$ e $n \equiv 4\ mod\ 5$, então $5|c$. Pois, $c = m^2 + n^2 \equiv 2^2 + 4^2 \equiv 0\ mod\ 5$.

IV) $m \equiv 3\ mod\ 5$ e $\begin{cases} n \equiv 0\ mod\ 5 \\ n \equiv 1\ mod\ 5 \\ n \equiv 2\ mod\ 5 \\ n \equiv 3\ mod\ 5 \\ n \equiv 4\ mod\ 5 \end{cases}$.

i) Se $m \equiv 3\ mod\ 5$ e $n \equiv 0\ mod\ 5$, então $5|b$. Pois, $5|n$, logo, $5|b = 2mn$.

ii) Se $m \equiv 3\ mod\ 5$ e $n \equiv 1\ mod\ 5$, então $5|c$. Pois, $c = m^2 + n^2 \equiv 3^2 + 1^2 \equiv 0\ mod\ 5$.

iii) Se $m \equiv 3\ mod\ 5$ e $n \equiv 2\ mod\ 5$, então $5|a$. Pois, $a = m^2 - n^2 \equiv 3^2 - 2^2 \equiv 0\ mod\ 5$.

iv) Se $m \equiv 3\ mod\ 5$ e $n \equiv 3\ mod\ 5$, então $5|a$. Pois, $a = m^2 - n^2 \equiv 3^2 - 3^2 \equiv 0\ mod\ 5$.

v) Se $m \equiv 3\ mod\ 5$ e $n \equiv 4\ mod\ 5$, então $5|c$. Pois, $c = m^2 + n^2 \equiv 3^2 + 4^2 \equiv 0\ mod\ 5$.

V) $m \equiv 4\ mod\ 5$ e $\begin{cases} n \equiv 0\ mod\ 5 \\ n \equiv 1\ mod\ 5 \\ n \equiv 2\ mod\ 5 \\ n \equiv 3\ mod\ 5 \\ n \equiv 4\ mod\ 5 \end{cases}$.

i) Se $m \equiv 4\ mod\ 5$ e $n \equiv 0\ mod\ 5$, então $5|b$. Pois, $5|n$, logo, $5|b = 2mn$.

ii) Se $m \equiv 4\ mod\ 5$ e $n \equiv 1\ mod\ 5$, então $5|a$. Pois, $a = m^2 - n^2 \equiv 4^2 - 1^2 \equiv 0\ mod\ 5$.

iii) Se $m \equiv 4\ mod\ 5$ e $n \equiv 2\ mod\ 5$, então $5|c$. Pois, $c = m^2 + n^2 \equiv 4^2 + 2^2 \equiv 0\ mod\ 5$.

iv) Se $m \equiv 4\ mod\ 5$ e $n \equiv 3\ mod\ 5$, então $5|c$. Pois, $c = m^2 + n^2 \equiv 4^2 + 3^2 \equiv 0\ mod\ 5$.

v) Se $m \equiv 4\ mod\ 5$ e $n \equiv 4\ mod\ 5$, então $5|a$. Pois, $a = m^2 - n^2 \equiv 4^2 - 4^2 \equiv 0\ mod\ 5$.

Portanto, por **I**, **II**, **III**, **IV** e **V**, concluimos que num terno pitagórico (a, b, c), a, b, ou c é divisível por 5. ■

10ª). Demonstrar que em um terno pitagórico (a, b, c), um dos elementos a, b, $a + b$ ou $a - b$ é divisível por 7.

Demonstração: De modo análogo a aplicação anterior, utilizaremos aqui também a congruência, analisando caso a caso as possibilidades para m e n. Sendo assim, temos:

I) $m \equiv 0 \ mod \ 7$ e $\begin{cases} n \equiv 1 \ mod \ 7 \\ n \equiv 2 \ mod \ 7 \\ n \equiv 3 \ mod \ 7 \\ n \equiv 4 \ mod \ 7 \\ n \equiv 5 \ mod \ 7 \\ n \equiv 6 \ mod \ 7 \end{cases}$.

Para os seis casos, $7|b$. Pois, $7|m$, logo, $7|b = 2mn$.

II) $m \equiv 1 \ mod \ 7$ e $\begin{cases} n \equiv 0 \ mod \ 7 \\ n \equiv 1 \ mod \ 7 \\ n \equiv 2 \ mod \ 7 \\ n \equiv 3 \ mod \ 7 \\ n \equiv 4 \ mod \ 7 \\ n \equiv 5 \ mod \ 7 \\ n \equiv 6 \ mod \ 7 \end{cases}$.

i) Se $m \equiv 1 \ mod \ 7$ e $n \equiv 0 \ mod \ 7$, então $7|b$. Pois, $7|n$, logo, $7|b = 2mn$.

ii) Se $m \equiv 1 \ mod \ 7$ e $n \equiv 1 \ mod \ 7$, então $7|a$. Pois, $a = m^2 - n^2 \equiv 1^2 - 1^2 \equiv 0 \ mod \ 7$.

iii) Se $m \equiv 1 \ mod \ 7$ e $n \equiv 2 \ mod \ 7$, então $7|a - b$.

Pois, $\begin{cases} a^2 = m^2 - n^2 \equiv 1^2 - 2^2 \equiv 4 \ mod \ 7 \\ b = 2 \cdot m \cdot n \equiv 2 \cdot 1 \cdot 2 \equiv 4 \ mod \ 7 \end{cases}$.

Logo, $a - b \equiv 4 - 4 \equiv 0 \ mod \ 7$.

iv) Se $m \equiv 1 \ mod \ 7$ e $n \equiv 3 \ mod \ 7$, então $7|a - b$.

Pois, $\begin{cases} a^2 = m^2 - n^2 \equiv 1^2 - 3^2 \equiv 6 \ mod \ 7 \\ b = 2 \cdot m \cdot n \equiv 2 \cdot 1 \cdot 3 \equiv 6 \ mod \ 7 \end{cases}$.

Logo, $a - b \equiv 6 - 6 \equiv 0 \ mod \ 7$.

v) Se $m \equiv 1 \ mod \ 7$ e $n \equiv 4 \ mod \ 7$, então $7|a + b$.

Pois, $\begin{cases} a^2 = m^2 - n^2 \equiv 1^2 - 4^2 \equiv 6 \ mod \ 7 \\ b = 2 \cdot m \cdot n \equiv 2 \cdot 1 \cdot 4 \equiv 1 \ mod \ 7 \end{cases}$.

Logo, $a + b \equiv 6 + 1 \equiv 0 \ mod \ 7$.

vi) Se $m \equiv 1 \ mod \ 7$ e $n \equiv 5 \ mod \ 7$, então $7|a + b$.

Pois, $\begin{cases} a^2 = m^2 - n^2 \equiv 1^2 - 5^2 \equiv 4 \ mod \ 7 \\ b = 2 \cdot m \cdot n \equiv 2 \cdot 1 \cdot 5 \equiv 3 \ mod \ 7 \end{cases}$.

Logo, $a + b \equiv 4 + 3 \equiv 0 \ mod \ 7$.

vii) Se $m \equiv 1 \ mod \ 7$ e $n \equiv 6 \ mod \ 7$, então $7|a$. Pois, $a = m^2 - n^2 \equiv 1^2 - 6^2 \equiv 0 \ mod \ 7$.

III) $m \equiv 2 \ mod \ 7$ e $\begin{cases} n \equiv 0 \ mod \ 7 \\ n \equiv 1 \ mod \ 7 \\ n \equiv 2 \ mod \ 7 \\ n \equiv 3 \ mod \ 7 \\ n \equiv 4 \ mod \ 7 \\ n \equiv 5 \ mod \ 7 \\ n \equiv 6 \ mod \ 7 \end{cases}$.

i) Se $m \equiv 2 \ mod \ 7$ e $n \equiv 0 \ mod \ 7$, então $7|b$. Pois, $7|n$, logo, $7|b = 2mn$.

ii) Se $m \equiv 2 \ mod \ 7$ e $n \equiv 1 \ mod \ 7$, então $7|a + b$.

Pois, $\begin{cases} a^2 = m^2 - n^2 \equiv 2^2 - 1^2 \equiv 3 \ mod \ 7 \\ b = 2 \cdot m \cdot n \equiv 2 \cdot 2 \cdot 1 \equiv 4 \ mod \ 7 \end{cases}$.

Logo, $a + b \equiv 3 + 4 \equiv 0 \ mod \ 7$.

iii) Se $m \equiv 2 \ mod \ 7$ e $n \equiv 2 \ mod \ 7$, então $7|a$. Pois, $a = m^2 - n^2 \equiv 2^2 - 2^2 \equiv 0 \ mod \ 7$.

iv) Se $m \equiv 2 \ mod \ 7$ e $n \equiv 3 \ mod \ 7$, então $7|a + b$.

Pois, $\begin{cases} a^2 = m^2 - n^2 \equiv 2^2 - 3^2 \equiv 2 \ mod \ 7 \\ b = 2 \cdot m \cdot n \equiv 2 \cdot 2 \cdot 3 \equiv 5 \ mod \ 7 \end{cases}$.

Logo, $a + b \equiv 2 + 5 \equiv 0 \ mod \ 7$.

v) Se $m \equiv 2 \ mod \ 7$ e $n \equiv 4 \ mod \ 7$, então $7|a - b$.

Pois, $\begin{cases} a^2 = m^2 - n^2 \equiv 2^2 - 4^2 \equiv 2 \ mod \ 7 \\ b = 2 \cdot m \cdot n \equiv 2 \cdot 2 \cdot 4 \equiv 2 \ mod \ 7 \end{cases}$.

Logo, $a - b \equiv 2 - 2 \equiv 0 \ mod \ 7$.

vi) Se $m \equiv 2 \ mod \ 7$ e $n \equiv 5 \ mod \ 7$, então $7|a$. Pois, $a = m^2 - n^2 \equiv 2^2 - 5^2 \equiv 0 \ mod \ 7$.

vii) Se $m \equiv 2 \ mod \ 7$ e $n \equiv 6 \ mod \ 7$, então $7|a - b$.

Pois, $\begin{cases} a^2 = m^2 - n^2 \equiv 2^2 - 6^2 \equiv 3 \ mod \ 7 \\ b = 2 \cdot m \cdot n \equiv 2 \cdot 2 \cdot 6 \equiv 3 \ mod \ 7 \end{cases}$.

Logo, $a - b \equiv 3 - 3 \equiv 0 \ mod \ 7$.

IV) $m \equiv 3 \ mod \ 7$ e $\begin{cases} n \equiv 0 \ mod \ 7 \\ n \equiv 1 \ mod \ 7 \\ n \equiv 2 \ mod \ 7 \\ n \equiv 3 \ mod \ 7 \\ n \equiv 4 \ mod \ 7 \\ n \equiv 5 \ mod \ 7 \\ n \equiv 6 \ mod \ 7 \end{cases}$.

i) Se $m \equiv 3 \ mod \ 7$ e $n \equiv 0 \ mod \ 7$, então $7|b$. Pois, $7|n$, logo, $7|b = 2mn$.

ii) Se $m \equiv 3 \ mod \ 7$ e $n \equiv 1 \ mod \ 7$, então $7|a + b$.

Pois, $\begin{cases} a^2 = m^2 - n^2 \equiv 3^2 - 1^2 \equiv 1 \ mod \ 7 \\ b = 2 \cdot m \cdot n \equiv 2 \cdot 3 \cdot 1 \equiv 6 \ mod \ 7 \end{cases}$.

Logo, $a + b \equiv 1 + 6 \equiv 0 \ mod \ 7$.

iii) Se $m \equiv 3 \ mod \ 7$ e $n \equiv 2 \ mod \ 7$, então $7|a - b$.

Pois, $\begin{cases} a^2 = m^2 - n^2 \equiv 3^2 - 2^2 \equiv 5 \ mod \ 7 \\ b = 2 \cdot m \cdot n \equiv 2 \cdot 3 \cdot 2 \equiv 5 \ mod \ 7 \end{cases}$.

Logo, $a - b \equiv 5 - 5 \equiv 0 \ mod \ 7$.

iv) Se $m \equiv 3 \ mod \ 7$ e $n \equiv 3 \ mod \ 7$, então $7|a$. Pois, $a = m^2 - n^2 \equiv 3^2 - 3^2 \equiv 0 \ mod \ 7$.

v) Se $m \equiv 3 \ mod \ 7$ e $n \equiv 4 \ mod \ 7$, então $7|a$. Pois, $a = m^2 - n^2 \equiv 3^2 - 4^2 \equiv 0 \ mod \ 7$.

vi) Se $m \equiv 3 \ mod \ 7$ e $n \equiv 5 \ mod \ 7$, então $7|a + b$.

Pois, $\begin{cases} a^2 = m^2 - n^2 \equiv 3^2 - 5^2 \equiv 5 \ mod \ 7 \\ b = 2 \cdot m \cdot n \equiv 2 \cdot 3 \cdot 5 \equiv 2 \ mod \ 7 \end{cases}$.

Logo, $a + b \equiv 5 + 2 \equiv 0 \ mod \ 7$.

vii) Se $m \equiv 3 \ mod \ 7$ e $n \equiv 6 \ mod \ 7$, então $7|a - b$.

Pois, $\begin{cases} a^2 = m^2 - n^2 \equiv 3^2 - 6^2 \equiv 1 \ mod \ 7 \\ b = 2 \cdot m \cdot n \equiv 2 \cdot 3 \cdot 6 \equiv 1 \ mod \ 7 \end{cases}$.

Logo, $a - b \equiv 1 - 1 \equiv 0 \ mod \ 7$.

V) $m \equiv 4 \ mod \ 7$ e $\begin{cases} n \equiv 0 \ mod \ 7 \\ n \equiv 1 \ mod \ 7 \\ n \equiv 2 \ mod \ 7 \\ n \equiv 3 \ mod \ 7 \\ n \equiv 4 \ mod \ 7 \\ n \equiv 5 \ mod \ 7 \\ n \equiv 6 \ mod \ 7 \end{cases}$.

i) Se $m \equiv 4 \ mod \ 7$ e $n \equiv 0 \ mod \ 7$, então $7|b$. Pois, $7|n$, logo, $7|b = 2mn$.

ii) Se $m \equiv 4 \ mod \ 7$ e $n \equiv 1 \ mod \ 7$, então $7|a - b$.

Pois, $\begin{cases} a^2 = m^2 - n^2 \equiv 4^2 - 1^2 \equiv 1 \ mod \ 7 \\ b = 2 \cdot m \cdot n \equiv 2 \cdot 4 \cdot 1 \equiv 1 \ mod \ 7 \end{cases}$.

Logo, $a - b \equiv 1 - 1 \equiv 0 \ mod \ 7$.

iii) Se $m \equiv 4 \ mod \ 7$ e $n \equiv 2 \ mod \ 7$, então $7|a + b$.

Pois, $\begin{cases} a^2 = m^2 - n^2 \equiv 4^2 - 2^2 \equiv 5 \ mod \ 7 \\ b = 2 \cdot m \cdot n \equiv 2 \cdot 4 \cdot 2 \equiv 2 \ mod \ 7 \end{cases}$.

Logo, $a + b \equiv 5 + 2 \equiv 0 \ mod \ 7$.

iv) Se $m \equiv 4 \ mod \ 7$ e $n \equiv 3 \ mod \ 7$, então $7|a$. Pois, $a = m^2 - n^2 \equiv 4^2 - 3^2 \equiv 0 \ mod \ 7$.

v) Se $m \equiv 4 \ mod \ 7$ e $n \equiv 4 \ mod \ 7$, então $7|a$. Pois, $a = m^2 - n^2 \equiv 4^2 - 4^2 \equiv 0 \ mod \ 7$.

vi) Se $m \equiv 4 \ mod \ 7$ e $n \equiv 5 \ mod \ 7$, então $7|a - b$.

Pois, $\begin{cases} a^2 = m^2 - n^2 \equiv 4^2 - 5^2 \equiv 5 \ mod \ 7 \\ b = 2 \cdot m \cdot n \equiv 2 \cdot 4 \cdot 5 \equiv 5 \ mod \ 7 \end{cases}$.

Logo, $a - b \equiv 5 - 5 \equiv 0 \ mod \ 7$.

vii) Se $m \equiv 4 \ mod \ 7$ e $n \equiv 6 \ mod \ 7$, então $7|a-b$.

$$\text{Pois, } \begin{cases} a^2 = m^2 - n^2 \equiv 4^2 - 6^2 \equiv 6 \ mod \ 7 \\ b = 2 \cdot m \cdot n \equiv 2 \cdot 4 \cdot 6 \equiv 6 \ mod \ 7 \end{cases}.$$

Logo, $a - b \equiv 6 - 6 \equiv 0 \ mod \ 7$.

VI) $m \equiv 5 \ mod \ 7$ e $\begin{cases} n \equiv 0 \ mod \ 7 \\ n \equiv 1 \ mod \ 7 \\ n \equiv 2 \ mod \ 7 \\ n \equiv 3 \ mod \ 7 \\ n \equiv 4 \ mod \ 7 \\ n \equiv 5 \ mod \ 7 \\ n \equiv 6 \ mod \ 7 \end{cases}$.

i) Se $m \equiv 5 \ mod \ 7$ e $n \equiv 0 \ mod \ 7$, então $7|b$. Pois, $7|n$, logo, $7|b = 2mn$.

ii) Se $m \equiv 5 \ mod \ 7$ e $n \equiv 1 \ mod \ 7$, então $7|a-b$.

$$\text{Pois, } \begin{cases} a^2 = m^2 - n^2 \equiv 5^2 - 1^2 \equiv 3 \ mod \ 7 \\ b = 2 \cdot m \cdot n \equiv 2 \cdot 5 \cdot 1 \equiv 3 \ mod \ 7 \end{cases}.$$

Logo, $a - b \equiv 3 - 3 \equiv 0 \ mod \ 7$.

iii) Se $m \equiv 5 \ mod \ 7$ e $n \equiv 2 \ mod \ 7$, então $7|a$. Pois, $a = m^2 - n^2 \equiv 5^2 - 2^2 \equiv 0 \ mod \ 7$.

iv) Se $m \equiv 5 \ mod \ 7$ e $n \equiv 3 \ mod \ 7$, então $7|a-b$.

$$\text{Pois, } \begin{cases} a^2 = m^2 - n^2 \equiv 5^2 - 3^2 \equiv 2 \ mod \ 7 \\ b = 2 \cdot m \cdot n \equiv 2 \cdot 5 \cdot 3 \equiv 2 \ mod \ 7 \end{cases}.$$

Logo, $a - b \equiv 2 - 2 \equiv 0 \ mod \ 7$.

v) Se $m \equiv 5 \ mod \ 7$ e $n \equiv 4 \ mod \ 7$, então $7|a+b$.

Pois, $\begin{cases} a^2 = m^2 - n^2 \equiv 5^2 - 4^2 \equiv 2 \ mod \ 7 \\ b = 2 \cdot m \cdot n \equiv 2 \cdot 5 \cdot 4 \equiv 5 \ mod \ 7 \end{cases}$.

Logo, $a + b \equiv 2 + 5 \equiv 0 \ mod \ 7$.

vi) Se $m \equiv 5 \ mod \ 7$ e $n \equiv 5 \ mod \ 7$, então $7|a$. Pois, $a = m^2 - n^2 \equiv 5^2 - 5^2 \equiv 0 \ mod \ 7$.

vii) Se $m \equiv 5 \ mod \ 7$ e $n \equiv 6 \ mod \ 7$, então $7|a + b$.

Pois, $\begin{cases} a^2 = m^2 - n^2 \equiv 5^2 - 6^2 \equiv 3 \ mod \ 7 \\ b = 2 \cdot m \cdot n \equiv 2 \cdot 5 \cdot 6 \equiv 4 \ mod \ 7 \end{cases}$.

Logo, $a + b \equiv 3 + 4 \equiv 0 \ mod \ 7$.

VII) $m \equiv 6 \ mod \ 7$ e $\begin{cases} n \equiv 0 \ mod \ 7 \\ n \equiv 1 \ mod \ 7 \\ n \equiv 2 \ mod \ 7 \\ n \equiv 3 \ mod \ 7 \\ n \equiv 4 \ mod \ 7 \\ n \equiv 5 \ mod \ 7 \\ n \equiv 6 \ mod \ 7 \end{cases}$.

i) Se $m \equiv 6 \ mod \ 7$ e $n \equiv 0 \ mod \ 7$, então $7|b$. Pois, $7|n$, logo, $7|b = 2mn$.

ii) Se $m \equiv 6 \ mod \ 7$ e $n \equiv 1 \ mod \ 7$, então $7|a$. Pois, $a = m^2 - n^2 \equiv 6^2 - 1^2 \equiv 0 \ mod \ 7$.

iii) Se $m \equiv 6 \ mod \ 7$ e $n \equiv 2 \ mod \ 7$, então $7|a + b$.

Pois, $\begin{cases} a^2 = m^2 - n^2 \equiv 6^2 - 2^2 \equiv 4 \ mod \ 7 \\ b = 2 \cdot m \cdot n \equiv 2 \cdot 6 \cdot 2 \equiv 3 \ mod \ 7 \end{cases}$.

Logo, $a + b \equiv 4 + 3 \equiv 0 \ mod \ 7$.

iv) Se $m \equiv 6\ mod\ 7$ e $n \equiv 3\ mod\ 7$, então $7|a+b$.

Pois, $\begin{cases} a^2 = m^2 - n^2 \equiv 6^2 - 3^2 \equiv 6\ mod\ 7 \\ b = 2 \cdot m \cdot n \equiv 2 \cdot 6 \cdot 3 \equiv 1\ mod\ 7 \end{cases}$.

Logo, $a + b \equiv 6 + 1 \equiv 0\ mod\ 7$.

v) Se $m \equiv 6\ mod\ 7$ e $n \equiv 4\ mod\ 7$, então $7|a-b$.

Pois, $\begin{cases} a^2 = m^2 - n^2 \equiv 6^2 - 4^2 \equiv 6\ mod\ 7 \\ b = 2 \cdot m \cdot n \equiv 2 \cdot 6 \cdot 4 \equiv 6\ mod\ 7 \end{cases}$.

Logo, $a - b \equiv 6 - 6 \equiv 0\ mod\ 7$.

vi) Se $m \equiv 6\ mod\ 7$ e $n \equiv 5\ mod\ 7$, então $7|a-b$.

Pois, $\begin{cases} a^2 = m^2 - n^2 \equiv 6^2 - 5^2 \equiv 4\ mod\ 7 \\ b = 2 \cdot m \cdot n \equiv 2 \cdot 6 \cdot 5 \equiv 4\ mod\ 7 \end{cases}$.

Logo, $a - b \equiv 4 - 4 \equiv 0\ mod\ 7$.

vii) Se $m \equiv 6\ mod\ 7$ e $n \equiv 6\ mod\ 7$, então $7|a$. Pois, $a = m^2 - n^2 \equiv 6^2 - 6^2 \equiv 0\ mod\ 7$.

Portanto, por **I**, **II**, **III**, **IV**, **V**, **VI** e **VII**, concluimos que num terno pitagórico (a, b, c), a, b, $a + a$ ou $a - b$ é divisível por 7. ■

11ª). Demonstrar que em um *terno pitagórico primitivo* (a, b, c) qualquer, 7 não divide c.

Demonstração: Pelas equações de Euclides (Teorema 2.3.1), temos $c = m^2 + n^2$, onde c é hipotenusa de um *terno pitagórico primitivo*, com $m,\ n \in \mathbb{Z}_+^*$, m e n relativamente primos e de paridade distinta e $m > n$.

Sendo assim, de modo análogo à **9ª** e **10ª** aplicação, analisaremos aqui também,

caso a caso as possibilidades para m e n através da congruência módulo 7.

I) $m \equiv 0 \ mod \ 7$ e $\begin{cases} n \equiv 1 \ mod \ 7 \\ n \equiv 2 \ mod \ 7 \\ n \equiv 3 \ mod \ 7 \\ n \equiv 4 \ mod \ 7 \\ n \equiv 5 \ mod \ 7 \\ n \equiv 6 \ mod \ 7 \end{cases}$.

i) Se $m \equiv 0 \ mod \ 7$ e $n \equiv 1 \ mod \ 7$, então $c = m^2 + n^2 \equiv 0^2 + 1^2 \equiv 1 \ mod \ 7$. Logo, 7 não divide c.

ii) Se $m \equiv 0 \ mod \ 7$ e $n \equiv 2 \ mod \ 7$, então $c = m^2 + n^2 \equiv 0^2 + 2^2 \equiv 4 \ mod \ 7$. Logo, 7 não divide c.

iii) Se $m \equiv 0 \ mod \ 7$ e $n \equiv 3 \ mod \ 7$, então $c = m^2 + n^2 \equiv 0^2 + 3^2 \equiv 2 \ mod \ 7$. Logo, 7 não divide c.

iv) Se $m \equiv 0 \ mod \ 7$ e $n \equiv 4 \ mod \ 7$, então $c = m^2 + n^2 \equiv 0^2 + 4^2 \equiv 2 \ mod \ 7$. Logo, 7 não divide c.

v) Se $m \equiv 0 \ mod \ 7$ e $n \equiv 5 \ mod \ 7$, então $c = m^2 + n^2 \equiv 0^2 + 5^2 \equiv 4 \ mod \ 7$. Logo, 7 não divide c.

vi) Se $m \equiv 0 \ mod \ 7$ e $n \equiv 6 \ mod \ 7$, então $c = m^2 + n^2 \equiv 0^2 + 6^2 \equiv 1 \ mod \ 7$. Logo, 7 não divide c.

II) $m \equiv 1 \ mod \ 7$ e $\begin{cases} n \equiv 0 \ mod \ 7 \\ n \equiv 1 \ mod \ 7 \\ n \equiv 2 \ mod \ 7 \\ n \equiv 3 \ mod \ 7 \\ n \equiv 4 \ mod \ 7 \\ n \equiv 5 \ mod \ 7 \\ n \equiv 6 \ mod \ 7 \end{cases}$.

i) Se $m \equiv 1 \ mod \ 7$ e $n \equiv 0 \ mod \ 7$, então $c = m^2 + n^2 \equiv 1^2 + 0^2 \equiv 1 \ mod \ 7$. Logo, 7 não divide c.

ii) Se $m \equiv 1 \ mod \ 7$ e $n \equiv 1 \ mod \ 7$, então $c = m^2 + n^2 \equiv 1^2 + 1^2 \equiv 2 \ mod \ 7$. Logo, 7 não divide c.

iii) Se $m \equiv 1 \ mod \ 7$ e $n \equiv 2 \ mod \ 7$, então $c = m^2 + n^2 \equiv 1^2 + 2^2 \equiv 5 \ mod \ 7$. Logo, 7 não divide c.

iv) Se $m \equiv 1 \ mod \ 7$ e $n \equiv 3 \ mod \ 7$, então $c = m^2 + n^2 \equiv 1^2 + 3^2 \equiv 3 \ mod \ 7$. Logo, 7 não divide c.

v) Se $m \equiv 1 \ mod \ 7$ e $n \equiv 4 \ mod \ 7$, então $c = m^2 + n^2 \equiv 1^2 + 4^2 \equiv 3 \ mod \ 7$. Logo, 7 não divide c.

vi) Se $m \equiv 1 \ mod \ 7$ e $n \equiv 5 \ mod \ 7$, então $c = m^2 + n^2 \equiv 1^2 + 5^2 \equiv 5 \ mod \ 7$. Logo, 7 não divide c.

vii) Se $m \equiv 1 \ mod \ 7$ e $n \equiv 6 \ mod \ 7$, então $c = m^2 + n^2 \equiv 1^2 + 6^2 \equiv 2 \ mod \ 7$. Logo, 7 não divide c.

III) $m \equiv 1 \ mod \ 7$ e $\begin{cases} n \equiv 0 \ mod \ 7 \\ n \equiv 1 \ mod \ 7 \\ n \equiv 2 \ mod \ 7 \\ n \equiv 3 \ mod \ 7 \\ n \equiv 4 \ mod \ 7 \\ n \equiv 5 \ mod \ 7 \\ n \equiv 6 \ mod \ 7 \end{cases}$.

i) Se $m \equiv 2 \ mod \ 7$ e $n \equiv 0 \ mod \ 7$, então $c = m^2 + n^2 \equiv 2^2 + 0^2 \equiv 4 \ mod \ 7$. Logo, 7 não divide c.

ii) Se $m \equiv 2 \ mod \ 7$ e $n \equiv 1 \ mod \ 7$, então $c = m^2 + n^2 \equiv 2^2 + 1^2 \equiv 5 \ mod \ 7$. Logo, 7 não divide c.

iii) Se $m \equiv 2 \ mod \ 7$ e $n \equiv 2 \ mod \ 7$, então $c = m^2 + n^2 \equiv 2^2 + 2^2 \equiv 1 \ mod \ 7$. Logo, 7 não divide c.

iv) Se $m \equiv 2 \ mod \ 7$ e $n \equiv 3 \ mod \ 7$, então $c = m^2 + n^2 \equiv 2^2 + 3^2 \equiv 6 \ mod \ 7$. Logo, 7 não divide c.

v) Se $m \equiv 2 \ mod \ 7$ e $n \equiv 4 \ mod \ 7$, então $c = m^2 + n^2 \equiv 2^2 + 4^2 \equiv 6 \ mod \ 7$. Logo, 7 não divide c.

vi) Se $m \equiv 2 \ mod \ 7$ e $n \equiv 5 \ mod \ 7$, então $c = m^2 + n^2 \equiv 2^2 + 5^2 \equiv 1 \ mod \ 7$. Logo, 7 não divide c.

vii) Se $m \equiv 2 \ mod \ 7$ e $n \equiv 6 \ mod \ 7$, então $c = m^2 + n^2 \equiv 2^2 + 6^2 \equiv 5 \ mod \ 7$. Logo, 7 não divide c.

IV) $m \equiv 1 \ mod \ 7$ e $\begin{cases} n \equiv 0 \ mod \ 7 \\ n \equiv 1 \ mod \ 7 \\ n \equiv 2 \ mod \ 7 \\ n \equiv 3 \ mod \ 7 \\ n \equiv 4 \ mod \ 7 \\ n \equiv 5 \ mod \ 7 \\ n \equiv 6 \ mod \ 7 \end{cases}$.

i) Se $m \equiv 3 \ mod \ 7$ e $n \equiv 0 \ mod \ 7$, então $c = m^2 + n^2 \equiv 3^2 + 0^2 \equiv 2 \ mod \ 7$. Logo, 7 não divide c.

ii) Se $m \equiv 3 \ mod \ 7$ e $n \equiv 1 \ mod \ 7$, então $c = m^2 + n^2 \equiv 3^2 + 1^2 \equiv 3 \ mod \ 7$. Logo, 7 não divide c.

iii) Se $m \equiv 3 \ mod \ 7$ e $n \equiv 2 \ mod \ 7$, então $c = m^2 + n^2 \equiv 3^2 + 2^2 \equiv 6 \ mod \ 7$. Logo, 7 não divide c.

iv) Se $m \equiv 3 \ mod \ 7$ e $n \equiv 3 \ mod \ 7$, então $c = m^2 + n^2 \equiv 3^2 + 3^2 \equiv 4 \ mod \ 7$. Logo, 7 não divide c.

v) Se $m \equiv 3 \ mod \ 7$ e $n \equiv 4 \ mod \ 7$, então $c = m^2 + n^2 \equiv 3^2 + 4^2 \equiv 4 \ mod \ 7$. Logo, 7 não divide c.

vi) Se $m \equiv 3 \ mod \ 7$ e $n \equiv 5 \ mod \ 7$, então $c = m^2 + n^2 \equiv 3^2 + 5^2 \equiv 6 \ mod \ 7$. Logo, 7 não divide c.

vii) Se $m \equiv 3 \ mod \ 7$ e $n \equiv 6 \ mod \ 7$, então $c = m^2 + n^2 \equiv 3^2 + 6^2 \equiv 3 \ mod \ 7$. Logo, 7 não divide c.

V) $m \equiv 1 \ mod \ 7$ e $\begin{cases} n \equiv 0 \ mod \ 7 \\ n \equiv 1 \ mod \ 7 \\ n \equiv 2 \ mod \ 7 \\ n \equiv 3 \ mod \ 7 \\ n \equiv 4 \ mod \ 7 \\ n \equiv 5 \ mod \ 7 \\ n \equiv 6 \ mod \ 7 \end{cases}$.

i) Se $m \equiv 4 \ mod \ 7$ e $n \equiv 0 \ mod \ 7$, então $c = m^2 + n^2 \equiv 4^2 + 0^2 \equiv 2 \ mod \ 7$. Logo, 7 não divide c.

ii) Se $m \equiv 4 \ mod \ 7$ e $n \equiv 1 \ mod \ 7$, então $c = m^2 + n^2 \equiv 4^2 + 1^2 \equiv 3 \ mod \ 7$. Logo, 7 não divide c.

iii) Se $m \equiv 4 \ mod \ 7$ e $n \equiv 2 \ mod \ 7$, então $c = m^2 + n^2 \equiv 4^2 + 2^2 \equiv 6 \ mod \ 7$. Logo, 7 não divide c.

iv) Se $m \equiv 4 \ mod \ 7$ e $n \equiv 3 \ mod \ 7$, então $c = m^2 + n^2 \equiv 4^2 + 3^2 \equiv 4 \ mod \ 7$. Logo, 7 não divide c.

v) Se $m \equiv 4 \ mod \ 7$ e $n \equiv 4 \ mod \ 7$, então $c = m^2 + n^2 \equiv 4^2 + 4^2 \equiv 4 \ mod \ 7$. Logo, 7 não divide c.

vi) Se $m \equiv 4 \ mod \ 7$ e $n \equiv 5 \ mod \ 7$, então $c = m^2 + n^2 \equiv 4^2 + 5^2 \equiv 6 \ mod \ 7$. Logo, 7 não divide c.

vii) Se $m \equiv 4 \ mod \ 7$ e $n \equiv 6 \ mod \ 7$, então $c = m^2 + n^2 \equiv 4^2 + 6^2 \equiv 3 \ mod \ 7$. Logo, 7 não divide c.

VI) $m \equiv 1 \ mod \ 7$ e $\begin{cases} n \equiv 0 \ mod \ 7 \\ n \equiv 1 \ mod \ 7 \\ n \equiv 2 \ mod \ 7 \\ n \equiv 3 \ mod \ 7 \\ n \equiv 4 \ mod \ 7 \\ n \equiv 5 \ mod \ 7 \\ n \equiv 6 \ mod \ 7 \end{cases}$.

i) Se $m \equiv 5 \ mod \ 7$ e $n \equiv 0 \ mod \ 7$, então $c = m^2 + n^2 \equiv 5^2 + 0^2 \equiv 4 \ mod \ 7$. Logo, 7 não divide c.

ii) Se $m \equiv 5 \ mod \ 7$ e $n \equiv 1 \ mod \ 7$, então $c = m^2 + n^2 \equiv 5^2 + 1^2 \equiv 5 \ mod \ 7$. Logo, 7 não divide c.

iii) Se $m \equiv 5 \ mod \ 7$ e $n \equiv 2 \ mod \ 7$, então $c = m^2 + n^2 \equiv 5^2 + 2^2 \equiv 1 \ mod \ 7$. Logo, 7 não divide c.

iv) Se $m \equiv 5 \ mod \ 7$ e $n \equiv 3 \ mod \ 7$, então $c = m^2 + n^2 \equiv 5^2 + 3^2 \equiv 6 \ mod \ 7$. Logo, 7 não divide c.

v) Se $m \equiv 5 \ mod \ 7$ e $n \equiv 4 \ mod \ 7$, então $c = m^2 + n^2 \equiv 5^2 + 4^2 \equiv 6 \ mod \ 7$. Logo, 7 não divide c.

vi) Se $m \equiv 5 \ mod \ 7$ e $n \equiv 5 \ mod \ 7$, então $c = m^2 + n^2 \equiv 5^2 + 5^2 \equiv 1 \ mod \ 7$. Logo, 7 não divide c.

vii) Se $m \equiv 5 \ mod \ 7$ e $n \equiv 6 \ mod \ 7$, então $c = m^2 + n^2 \equiv 5^2 + 6^2 \equiv 5 \ mod \ 7$. Logo, 7 não divide c.

VII) $m \equiv 1 \ mod \ 7$ e $\begin{cases} n \equiv 0 \ mod \ 7 \\ n \equiv 1 \ mod \ 7 \\ n \equiv 2 \ mod \ 7 \\ n \equiv 3 \ mod \ 7 \\ n \equiv 4 \ mod \ 7 \\ n \equiv 5 \ mod \ 7 \\ n \equiv 6 \ mod \ 7 \end{cases}$.

i) Se $m \equiv 6 \ mod \ 7$ e $n \equiv 0 \ mod \ 7$, então $c = m^2 + n^2 \equiv 6^2 + 0^2 \equiv 1 \ mod \ 7$. Logo, 7 não divide c.

ii) Se $m \equiv 6 \ mod \ 7$ e $n \equiv 1 \ mod \ 7$, então $c = m^2 + n^2 \equiv 6^2 + 1^2 \equiv 2 \ mod \ 7$. Logo, 7 não divide c.

iii) Se $m \equiv 6 \ mod \ 7$ e $n \equiv 2 \ mod \ 7$, então $c = m^2 + n^2 \equiv 6^2 + 2^2 \equiv 5 \ mod \ 7$. Logo, 7 não divide c.

iv) Se $m \equiv 6 \ mod \ 7$ e $n \equiv 3 \ mod \ 7$, então $c = m^2 + n^2 \equiv 6^2 + 3^2 \equiv 3 \ mod \ 7$. Logo, 7 não divide c.

v) Se $m \equiv 6 \ mod \ 7$ e $n \equiv 4 \ mod \ 7$, então $c = m^2 + n^2 \equiv 6^2 + 4^2 \equiv 3 \ mod \ 7$. Logo, 7 não divide c.

vi) Se $m \equiv 6 \ mod \ 7$ e $n \equiv 5 \ mod \ 7$, então $c = m^2 + n^2 \equiv 6^2 + 5^2 \equiv 5 \ mod \ 7$. Logo, 7 não divide c.

vii) Se $m \equiv 6 \ mod \ 7$ e $n \equiv 6 \ mod \ 7$, então $c = m^2 + n^2 \equiv 6^2 + 6^2 \equiv 2 \ mod \ 7$. Logo, 7 não divide c.

Portanto, por **I**, **II**, **III**, **IV**, **V**, **VI** e **VII**, concluimos que num terno pitagórico primitivo (a, b, c), 7 não divide c. ■

Considerações Finais

.

Neste trabalho apresentamos inicialmente alguns dos principais tópicos da Aritmética, onde utilizamos como texto base Hefez[2011], que complementamos sempre que possível ou necessário, com exemplos numéricos ou comentários, com o propósito de facilitar o entendimento do leitor menos familiarizado com o assunto.

Em seguida, apresentamos as definições de Ternos Pitagóricos e Ternos Pitagóricos Primitivos, mostrando que a partir deste último podemos obter infinitos ternos pitagóricos não-primitivos, multiplicando seus respectivos elementos por um inteiro positivo qualquer, maior que 1, assim como podemos obter um terno pitagórico primitivo a partir de qualquer terno pitagórico não-primitivo, bastando para isso, efetuar a divisão de cada um dos elementos deste pelo seu respectivo *mdc*. Na sequência, apresentamos, sob forma de teorema, as Equações de Euclides, que geram infinitos ternos pitagóricos primitivos ou fórmulas em função de uma única variável que também geram infinitos ternos pitagóricos primitivos. As Equações de Euclides são as mais comuns nos livros de textos universitários, no que se refere às fórmulas que geram ternos pitagóricos, porém, pode ser trabalhada ainda no Ensino Médio, desde que adaptada a este nível.

Outra fórmula geradora de ternos pitagóricos que apresentamos neste trabalho, foi intitulada de *Fórmula de Fácil Dedução*, pois, diferentemente das Equações de Euclides, ela requer apenas conhecimentos básicos de aritméticas estudados no Ensino Fundamental, em sua demonstração. Esta fórmula gera todos os ternos pitagóricos, ou seja, os primitivos e os não-primitivos. Através dela podemos obter todos os ternos pitagóricos nos quais um número inteiro maior ou igual a 3 figura como cateto, sendo portanto, uma excelente ferramenta na resolução de problemas relacionados a este assunto.

Com o intuito de disponibilizar uma maneira prática, eficiente e inovadora de gerar infinitos ternos pitagóricos, desenvolvemos a partir de uma ideia encontrada no en-

dereço eletrônico: $< www.educ.fc.ul.pt/icm/icm98/icm14/teorema.htm >$, um dispositivo prático que gera ternos pitagóricos a partir de dois ímpares consecutivos positivos ou dois pares consecutivos positivos. Estes resultados foram também apresentados através de teoremas.

Para finalizar nosso trabalho, apresentamos uma identidade que relaciona dois ternos pitagóricos, gerando um terceiro terno pitagórico distinto. Apresentamos ainda, algumas propriedades dos ternos pitagóricos e particularidades do terno $(3, 4, 5)$ e algumas aplicações no Capítulo 3.

Com isto, esperamos ter atingido nosso objetivo central que é o de disponibilizar ao professor de Matemática do Ensino Básico Regular, assim como aos demais leitores interessados pelo assunto, um material alternativo que contém os principais resultados a respeito deste tema que julgamos imprescindível ao currículo escolar.

Referências Bibliográficas

[1] ALENCAR FILHO, Edgard de. *Teoria Elementar dos Números*. 3ª edição. Nobel. São Paulo - SP. 1985.

[2] ARAUJO, Fabio. *Teorema de Pitágoras: mais que uma relação entre áreas*. 5º Encontro da RPM. Universidade Federal da Bahia. Bahia. 2011.

[3] BOYER, Carl B.. *História da Matemática*. Segunda Edição. Editora Edgard Blücher. São Paulo-SP. 2001.

[4] CANDEIAS, Carla Sofia da Silva, e BATALHA, Graciete Pedroso. 1998. *O Teorema de Pitágoras*. Disponível em <www.educ.fc.ul.pt/icm/icm98/icm14/teorema.htm>. Acessado em 02 de dezembro de 2013.

[5] EVES, Howard.. *Introdução à História da Matemática.* 3ª edição. Unicamp. Campinas-SP. 2002.

[6] FOSSA, John A., e ERICKSON, Glenn W.. *Sobre a Classificação dos Triângulos Pitagóricos*. v.8. n.10. p.75 − 85. Natal. 2001.

[7] HEFEZ, Abramo. *Curso de Álgebra*. Coleção Matemática Universitária. Volume I. 4ª edição. Instituto de Matemática Pura e Aplicada. Rio de Janeiro - RJ. 2010.

[8] HEFEZ, Abramo. *Elementos da Aritmética*. Textos Universitários. Sociedade Brasileira de Matemática. 2ª edição. Rio de Janeiro-RJ. 2011.

[9] NASCIMENTO, Thais Silva do *Propriedades do Grupo dos Ternos Pitagóricos*. Monografia de Graduação. Licenciatura Plena em Matemática. Universidade Federal de Mato Grosso. Cuiabá. 2010.

[10] ROTHBART, Andréa, e PAUSELL, Bruce. *Números Pitagóricos: Uma Fórmula de Fácil Dedução e Algumas Aplicações Geométricas*. Revista do Professor de Matemática.SBM.n.7.p.49 − 51.São Paulo-SP.1985.

[11] SANTOS, José Plínio de Oliveira. *Introdução à Teoria dos Números*. Coleção Matemática Universitária. Instituto de Matemática Pura e Aplicada. Terceira Edição (sétima impressão). IMPA. Rio de Janeiro - RJ. 2011.

[13] SILVA, Georgiane A.. *Estudo Histórico e Pedagógico sobre Ternos Pitagóricos à Luz de Eugène Bahier*. Dissertação de Mestrado.Programa de Pós-Graduação em Ensino de Ciências Naturais e Matemática. Universidade Federal do Rio Grande do Norte. Natal. 2009.

[13] SILVA, Georgiane A.. *Resgate Histórico dos Ternos Pitagóricos como Ferramenta Pedagógica para Compreensão do Teorema de Pitágoras*. XIII Conferência Iteramericana de Educação Matemática. Recife. 2011.

[14] WAGNER, Eduardo. 2009. *Teorema de Pitágoras e Áreas - obmep*. Disponível em $< www.obmep.org.br/docs/Apostila3 - teorema\_de\_pitagoras.pdf >$. Acessado em 25 de novembro de 2013.