UNIVERSIDADE FEDERAL DE ALAGOAS-UFAL
CAMPUS ARAPIRACA
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL-PROFMAT

JADIEL JOSÉ ARAÚJO DA SILVA JÚNIOR

TRIÂNGULOS PITAGÓRICOS E O PROBLEMA DE FERMAT

ARAPIRACA
2025

Jadiel José Araújo da Silva Júnior

TRIÂNGULOS PITAGÓRICOS E O PROBLEMA DE FERMAT

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional do Campus Arapiraca da Universidade Federal de Alagoas como parte dos requisitos exigidos para a obtenção do grau de Mestre em Matemática.

Orientador: Prof. Dr. Iury Rafael Domingos de Oliveira

Arapiraca
2025

Universidade Federal de Alagoas – UFAL
Campus Arapiraca
Biblioteca Setorial *Campus* Arapiraca - BSCA

S586t Silva Júnior, Jadiel José Araújo da
Triângulos pitagóricos e o problema de Fermat [recurso eletrônico] / Jadiel José Araújo da Silva Júnior. – Arapiraca, 2025.
82 f.: il.

Orientador: Prof. Dr. Iury Rafael Domingos de Oliveira.
Dissertação (Mestrado Profissional em Matemática em Rede Nacional) - Universidade Federal de Alagoas, *Campus* Arapiraca, Arapiraca, 2025.
Disponível em: Universidade Digital (UD) – UFAL (*Campus* Arapiraca).
Referências: f. 82.

1. Matemática. 2. Geometria. 3. Aritmética. 4. Teorema de Fermat. I. Oliveira, Iury Rafael Domingos de. II. Título.

CDU 51

Bibliotecário responsável: Márcio Thiago dos Santos Albuquerque
CRB - 4 / 2052

Jadiel José Araújo da Silva Júnior

TRIÂNGULOS PITAGÓRICOS E O PROBLEMA DE FERMAT

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional do Campus Arapiraca da Universidade Federal de Alagoas como parte dos requisitos exigidos para a obtenção do grau de Mestre em Matemática.

Data de Aprovação: 04/08/2025

Banca Examinadora

Prof. Dr. Iury Rafael Domingos de Oliveira
Universidade Federal de Alagoas-UFAL
Campus Arapiraca
(Orientador)

Prof. Dr. Moreno Perreira Bonutti
Universidade Federal de Alagoas-UFAL
Campus Arapiraca
(Examinador Interno)

Prof. Dr. Deigo Alves Adauto
Universidade Estadual do Rio Grande do Norte-UERN
Campus Central - Mossoró
(Examinador Externo)

A minha digníssima esposa, Inayana, e a nossa Zoe que virá a nascer.

AGRADECIMENTOS

Ser grato é uma das virtudes que mais impactam a vida. Não podia ser diferente em minha vida. Em primeiro lugar, sou grato a Deus por sua infinita bondade e cuidado sobre minha vida. Sem a força e a certeza da ação de Deus em minha vida não teria conseguido finalizar esta etapa.

Em segundo lugar, queria agradecer a minha digníssima esposa, Inayana Barros. Ela, sem dúvidas, foi a minha maior fonte de motivação para que pudesse estar aqui. Desde o dia da seleção do mestrado, até o dia de hoje, tenho em minha esposa uma fonte de motivação inesgotável. Nos momentos difíceis dessa trajetória foi quem me acolheu e confiou, muitas vezes mais até do que eu, que daria certo. Serei eternamente grato a você, meu amor. Além de tudo isso, você me proporcionou a realização de um sonho, um presente humanamente insuperável, a graça de ser Pai. Zoe, papai te ama.

Agradeço a minha família, que tanto me incentivou a estudar e mostrou que o melhor caminho para a transformação é o estudo. Os esforços de minha mãe, Emília Caribé, foram fundamentais para que tivesse oportunidades que outrora ninguém em minha família tinha tido. Agradeço ao meu Pai, Jadiel Araújo, meus avôs, Jerônimo, Fátima, Antônio, Cícera, as minhas irmãs, Jamilly e Sara, meus tios, Marcílio e Sayonara, e a todos os membros da minha família.

Agradeço também aos meus amigos que me acompanharam neste período do mestrado, cada conversa, reunião para resolvermos questões, discussões em sala, foram fundamentais para meu processo construtivo no mestrado. Weverton, Natiely, Vagner, Ediclaudio, Jaelson, Mateus, Dani e Jhonnes, vocês foram fundamentais nesse processo.

Agradeço aos meus queridos professores que nos acompanharam nesse período de Mestrado. Prof. Dr. Moreno Bonutti, Prof. Me. Eben Alves, Prof. Dr. Alcindo Teles, Prof. Dr. Iury Domingos, Prof. Dr. Rodolfo Carneiro, Prof. Dr. Elthon Oliveira, Prof. Dr. Sidney Silva e Prof. Dr. José Barros, vocês foram essenciais nesse processo formativo.

Por fim, gostaria de agradecer aos mebros da banca examinadora, o Prof. Dr. Iury Domingos, o Porf. Dr. Moreno Bonutti e o Prof. Dr. Diego Adauto, que aceitaram paraticipar desta banca. Um agradecimento especial ao Prof. Dr. Iury Domingos, meu orientador, que me acompanhou no processo de escrita deste trabalho. Suas orientações e sugestões foram fundamentais para que este trabalho chegasse a esta forma final.

Tudo o que vier às suas mãos para fazer, faça-o conforme as suas forças, porque na sepultura, que é para onde você vai, não há obra, nem projetos, nem conhecimento, nem sabedoria alguma.

Eclesiastes 9:10 (NAA)

RESUMO

Alguns problemas que aparecem no dia a dia em sala de aula podem passar despercebidos. Muitas vezes, encaramos situações problemas no cotidiano com naturalidade e a curiosidade para gerar uma demonstração bem estruturada é deixada de lado pelo pragmatismo diário. Neste trabalho será construída a demonstração de um dos teoremas propostos por Pierre de Fermat, onde a área de um triângulo pitagórico nunca poderá ser expressa como um quadrado perfeito. Para fazer isso de maneira coesa e fluida, a dissertação foi dividida em quatro capítulos. O primeiro tratará da construção histórica, o segundo analisará a construção aritmética, o terceiro abordará a construção geométrica e, por fim, o quarto se dedicará à demonstração do Teorema de Fermat.

Palavras-chave: teorema de Fermat; área; triângulo pitagórico; aritmética; geometria.

ABSTRACT

Some problems that arise in the classroom on a daily basis can go unnoticed. Often, we face everyday problem situations with nonchalance, and the curiosity to generate a well-structured demonstration is set aside by daily pragmatism. In this work, the proof of one of the theorems proposed by Pierre de Fermat will be constructed, where the area of a Pythagorean triangle can never be expressed as a perfect square. To do this in a cohesive and fluid manner, the dissertation has been divided into four chapters. The first will address the historical construction, the second will analyze the arithmetic construction, the third will cover the geometric construction, and finally, the fourth will be dedicated to the proof of Fermat's Theorem.

Keywords: Fermat's theorem; area; pythagorean triangle; arithmetic; geometry

SUMÁRIO

1 INTRODUÇÃO

É preciso parar e pensar: será que os problemas matemáticos que aparecem no dia a dia são verdadeiramente levados a sério em todos os seus detalhes? Muitas vezes dá-se atenção a problemas que requerem muita reflexão e cuidado de um bom matemático. Todavia, todos os problemas matemáticos possuem seu valor e, muitas vezes, aquilo que parece muito simples é, na verdade, um ponto de riqueza matemática que é desprezado.

Um dos problemas que muitas vezes parece óbvio de definir, mas não tanto de provar, foi enunciado e provado por Pierre de Fermat em uma carta de 1659, endereçada a Pierre de Carcavi. Fermat enunciou que a área de um triângulo pitagórico não pode ser expressa como um quadrado perfeito. Na prática diária dos problemas que envolvem áreas de triângulos pitagóricos, triângulos retângulos de lados inteiros, muitas vezes deixamos passar detalhes que são deveras importantes e que podem ser muito bem aproveitados no processo construtivo.

Além disso, vê-se uma clara relação estrutural entre a aritmética e a geometria, e isso se dá de maneira muito perfeita no problema de Fermat discutido neste trabalho. Um triângulo pitagórico está associado a uma terna pitagórica e isso é deveras significativo para o nosso estudo. Assim, detalhar um problema, explicá-lo em riqueza de detalhes e analisar suas múltiplas colaborações para o processo de construção matemática é o que motiva a escrita deste trabalho.

Construir um problema vai muito além de prová-lo. Uma construção precisa de uma base forte, para que se possa construir toda a casa de uma maneira segura. Assim, este trabalho será dividido em quatro capítulos e cada um dos quatro tem sua significância na construção final da demonstração.

No primeiro capítulo, analisaremos a construção histórica do problema. Neste capítulo, passearemos ao longo de povos e épocas que trataram dos triângulos pitagóricos. Iniciaremos este passeio passando pela tábua Plimpton 322, uma tábua de 13 cm de comprimento, 9 cm de largura e 2 cm de espessura, de origem babilônica, mas com um caráter importantíssimo para os triângulos pitagóricos. Após isso, vamos até a Grécia Antiga para discutirmos os problemas que envolvem Pitágoras e a proposição do Teorema de Pitágoras, que caracterizam um triângulo retângulo. Por fim, chegaremos à França e conheceremos Pierre de Fermat, suas contribuições para a matemática e como ele propôs e provou o problema que é a base deste trabalho.

Em nosso segundo capítulo, serão feitas as construções aritméticas necessárias para que possamos demonstrar as consequências aritméticas do problema de Fermat. Neste capítulo, construiremos com máximo rigor as construções de MDC e os princípios de divisibilidade. Neste

capítulo, também temos uma construção feita por Diofanto, que dá um excelente ponto de partida na forma de representarmos parametricamente uma terna pitagórica primitiva.

Assim como a construção aritmética, a construção geométrica é necessária e fundamental para a construção deste problema. Assim, no terceiro capítulo deste trabalho, será feita a construção geométrica, onde trabalharemos a ideia de triângulo retângulo e também a área de um triângulo retângulo.

O quarto e último capítulo deste trabalho construirá propriedades dos ternos pitagóricas e dos triângulos pitagóricos, que baseiam o ponto de partida do problema de Fermat. No ponto central deste capítulo estão duas demonstrações do problema de Fermat que dão o nome a esta dissertação. Por fim, que este trabalho possa ser uma boa fonte de leitura e também de pesquisa para aqueles que queiram conhecer mais sobre os triângulos pitagóricos e o problema de Fermat.

2 CONSTRUÇÃO HISTÓRICA DO PROBLEMA

Qual é a origem de um problema? Como se deu a evolução do problema ao longo da história? Quais foram os teóricos que discutiram esse tema? Essas perguntas são cruciais e, ao respondê-las, obtém-se uma compreensão mais profunda da estruturação e demonstração do problema. O presente trabalho analisará um teorema proposto por Pierre de Fermat, mas esse problema requer algumas construções que antecedem Fermat e também sua demonstração, que foi proposta em uma carta a Pierre de Carcavi.

Com isso, este capítulo tem como objetivo fornecer todo o aparato teórico do problema e como as construções realizadas ao longo da história geram uma uniformização do problema. Para isso, serão discutidas a origem dos triângulos pitagóricos, bem como os teóricos que fundamentaram e otimizaram o estudo dos triângulos pitagóricos até a proposição do Teorema por Fermat.

2.1 A Tábua de Plimpton 322

O ponto de partida para o estudo coerente dos triângulos pitagóricos se dá no estudo da tábua conhecida como Plimpton 322 (seu nome indica a tábua da coleção G. A. Plimpton da Universidade de Colúmbia, catalogada sob o número 322). Segundo Eves (2004), vê-se que essa tábua foi escrita no período Babilônico Antigo (aproximadamente entre 1900 a.C. e 1600 a.C.), e a primeira descrição do seu estudo foi feita em 1945.

Figura 1 – Tábua Plimpton 322

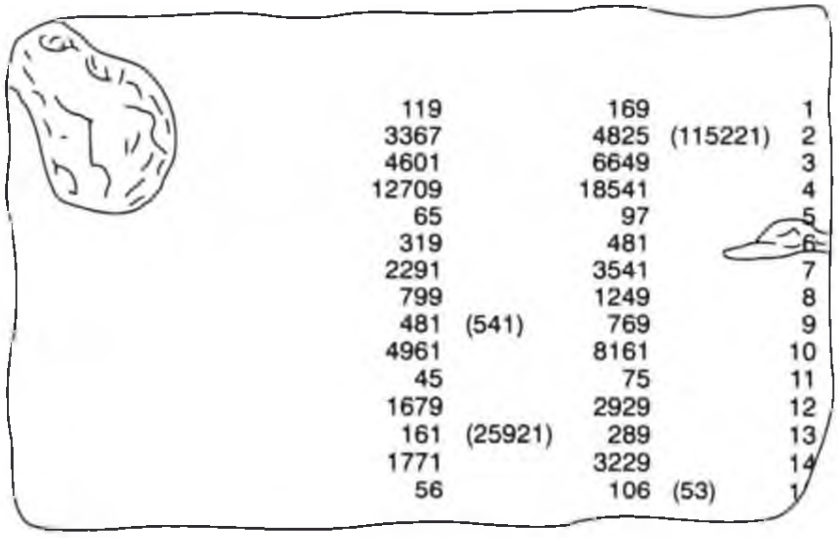
Fonte: Eves (2004)

A Figura 1 acima é um retrato da tábua Plimpton 322. Eves (2004) relata que, infelizmente, um pedaço do seu lado esquerdo foi perdido, e sabe-se disso por uma rachadura na tábua. Além disso, a tábua foi posteriormente danificada, perdendo uma lasca profunda do seu lado direito,

à altura da metade, e também apresentando um descamamento no canto superior esquerdo. É possível que a parte que falta ainda exista, mas que esteja como uma agulha no palheiro, perdida entre as coleções dessas tábuas antigas.

A tábua contém três colunas praticamente completas de caracteres, mas também existe uma quarta coluna incompleta, que era uma coluna de caracteres ao longo do lado quebrado. Eves (2004) propõe uma tábua em base decimal com as seguintes informações:

Figura 2 – TábuLa de Plimpton 322



Fonte: Eves (2004)

A coluna mais à direita serve para numerar as linhas, mas as duas mais à esquerda parecem ser colunas de números aleatórios. Todavia, com exceção de quatro casos, que estão com os respectivos números antigos entre parênteses e os corrigidos na lista, temos uma coluna com hipotenusas e outra com um dos catetos de um triângulo retângulo de lados inteiros, ou seja, um triângulo pitagórico.

Com essa análise foi possível descobrir o outro cateto e formar assim os lados de um triângulo pitagórico. Segundo Eves (2004) um terno de números inteiros, como $(3, 45)$, cujos termos são lados de um triângulo retângulo, é chamado de terno pitagórico. Além disso,se o único fator inteiro positivo comum aos elementos de um terno pitagórico for a unidade, ele é um primitivo.

Eves (2004) pondera que um dos grandes feitos matemáticos dos gregos, posterior muitos séculos à tábula de Plimpton 322, foi mostrar que todos os ternos pitagóricos primitivos (x, y, z) são dados parametricamente por $x = 2 \cdot u \cdot v$, $y = u^2 - v^2$ e $z = u^2 + v^2$, onde u e v são primos entre si, com paridades diferentes e $u > v$. Podemos assim, determinar, por meio da Figura 2, o

outro cateto juntamento com os número u e v. Considere que x será o cateto descoberto e já se tem o cateto y e a hipotenusa z. Assim, na linha 1

$$u^2 - v^2 = 119 \ [\star]$$

$$u^2 + v^2 = 169 \ [\star\star]$$

somando $[\star]$ e $[\star\star]$, tem-se que

$$2u^2 = 288 \Longrightarrow u^2 = 144 \Longrightarrow u = 12$$

agora sabemos que $u = 12$ e vamos substituir esse valor em $[\star\star]$ e daí

$$12^2 - v^2 = 119 \Longrightarrow -v^2 = 119 - 144 \Longrightarrow v^2 = 25 \Longrightarrow v = 5.$$

Logo, $u = 12$ e $v = 5$ e como $x = 2 \cdot u \cdot v$,

$$x = 2 \cdot 12 \cdot 5 = 120.$$

Seguindo o mesmo racício para as quinze linhas da Figura 2, teremos

1. $x = 120$, $y = 119$ e $z = 169$, com $u = 12$ e $v = 5$;
2. $x = 3456$, $y = 3367$ e $z = 4825$, com $u = 64$ e $v = 27$;
3. $x = 4800$, $y = 4601$ e $z = 6649$, com $u = 75$ e $v = 32$;
4. $x = 13500$, $y = 12709$ e $z = 18541$, com $u = 125$ e $v = 54$;
5. $x = 72$, $y = 65$ e $z = 97$, com $u = 9$ e $v = 4$;
6. $x = 360$, $y = 319$ e $z = 481$, com $u = 20$ e $v = 9$;
7. $x = 2700$, $y = 2291$ e $z = 3541$, com $u = 54$ e $v = 25$;
8. $x = 960$, $y = 799$ e $z = 1249$, com $u = 32$ e $v = 15$;
9. $x = 600$, $y = 481$ e $z = 769$, com $u = 25$ e $v = 12$;
10. $x = 6480$, $y = 4961$ e $z = 8161$, com $u = 81$ e $v = 40$;
11. $x = 60$, $y = 45$ e $z = 75$, com $u = 2$ e $v = 1$ (Esse terno não é primitivo e tem fator 15, ou seja substitua $u = 2$ e $v = 1$ e após descobrir o terno (x, y, z) multiplique por 15);

12. $x = 2400$, $y = 1679$ e $z = 2929$, com $u = 48$ e $v = 25$;

13. $x = 240$, $y = 161$ e $z = 289$, com $u = 15$ e $v = 8$;

14. $x = 2700$, $y = 1771$ e $z = 3229$, com $u = 50$ e $v = 27$;

15. $x = 56$, $y = 90$ e $z = 106$, com $u = 7$ e $v = 2$. (Nesse último caso vamos determinar o y e o fator gerador é o fator 2).

Algumas coissa são importantes de notarmos, apenas os ternos das linhas 11 e 15 não são primitivos. Eves (2004) nos diz que parece evidente que os babilônios desse remoto período tinham ciência da representação paramétrica geral dos ternos pitagóricos primitivos como foi dada acima. Vê-se isso quando notamos que u, v e x são números sexagesimais regulares, número onde se seu inverso multiplicativo admite uma representação sexagesimal finita.

A escolha de u e v deve ter sido motivada por algum processo subsequente envolvendo divisão, pois os números regulares aparecem em tábuas de inversos múltiplicativos e são usados para reduzir a divisão à multiplicação. Uma análise cuidadosa da tábula Plimpton 322 nos permite ver que a análise de triângulos pitagóricos já era trabalhada muito tempo antes dos estudos mais comuns sobre triângulos pitagóricos.

2.2 Pitágoras

Falar sobre Pitágoras é necessariamente entrar no campo das hipóteses. Eves (2004) diz que, ao contrário do que ocorre com a matemática antiga do Egito e da Babilônia, quase não se dispõe de nenhuma fonte primária para lançar luz sobre a primitiva matemática grega. A vida de Pitágoras é envolta em certo misticismo, pois, como a maioria dos materiais de conhecimento sobre a cultura antiga grega foram escritos muito depois dos acontecimentos, pouco se sabe sobre ele com algum grau de certeza.

Ao que parece, Pitágoras nasceu por volta de 572 a.C. na ilha grega de Samos. Há uma possibilidade, de certa forma até plausível, de ele ter sido discípulo de Tales de Mileto. Isso se dá pelo fato de Pitágoras ser cinquenta anos mais novo que Tales e também de residir próximo a Mileto. Ao percorrermos os escritos sobre Pitágoras, vê-se que, ao que parece, ele residiu um tempo no Egito e pode até mesmo ter feito viagens mais extensas.

Quando esteve de volta à ilha de Samos, segundo Eves (2004), encontrou o poder nas mãos do tirano Polícrates e a Jônia sob o domínio persa; decidiu então emigrar para o porto

marítimo de Crotona, uma colônia grega situada no sul da Itália. Em Crotona, Pitágoras fundou sua famosa escola, a Escola Pitagórica, que, além de ser um centro de estudo de filosofia, matemática e ciências naturais, era também uma irmandade profundamente unida por ritos secretos e cerimônias (aparentemente havia uma escola com caráter de seita religiosa).

A filosofia pitagórica estava baseada na suposição de que a última causa das várias características do homem e da matéria são os números inteiros. Essa definição é muito significativa, pois a escola pitagórica exaltava os números inteiros e também o estudo profundo de suas propriedades, junto à geometria, à música e à astronomia, que constituíam as artes liberais básicas do programa de estudos pitagóricos, segundo Eves (2004). Os ensinamentos da escola eram orais e era muito comum que a irmandade atribuísse todas as descobertas ao fundador da escola. Assim, é bem difícil saber com exatidão aquilo que foi descoberto por Pitágoras e aquilo que foi descoberto por um dos seus discípulos.

Admite-se a Pitágoras e à escola pitagórica os primeiros passos no sentido do desenvolvimento da aritmética e da teoria dos números, assim como o lançamento das bases do futuro misticismo numérico. Eves (2004) conta que Jâmblico, um influente filósofo neoplatônico que viveu por volta de 320 d.C., atribui a Pitágoras e seus seguidores a descoberta dos números amigáveis. Dois números são chamados amigáveis quando cada um deles é igual à soma dos divisores próprios (todos os divisores de um número, com exceção do próprio número) do outro.

O primeiro par de números amigáveis descoberto foi 284 e 220. Se analisarmos os divisores próprios de 284 teremos $D_{284} = \{1, 2, 4, 71, 142\}$ e ao somarmos esses números $1 + 2 + 4 + 71 + 142 = 220$. Analogamente, se analisarmos os divisores próprios de 220 teremos $D_{220} = \{1, 2, 4, 5, 10, 11, 20, 22, 44, 55, 110\}$ e ao somarmos esses números $1 + 2 + 4 + 5 + 10 + 11 + 20 + 22 + 44 + 55 + 110 = 284$. Eves (2004) comenta que esse par de números alcançou uma aura mística, e rezava a surpestição posterior que dois talismãs com esses números selariam uma amizade perfeita entre os que os usassem.

Os números amigáveis são tão brilhantes que ao que parece nenhum novo par de números amigáveis foi descoberto até que Pierre de Fermat, um dos grandes especialistas em Teoria dos Números, em 1636 anunciou um novo par formado pelso números 17296 e 18416. Dois anos depois de Fermat, René Descartes, filósofo e matemático francês, deu um terceiro par. Um estudo primoroso dos chamados números amigáveis foi feito pelo brilhante matemático suíço Leonhard Euler que, em 1747, deu uma lista de trinta pares de números amigáveis que logo mais foi aumentada para sessenta pares de números amigáveis.

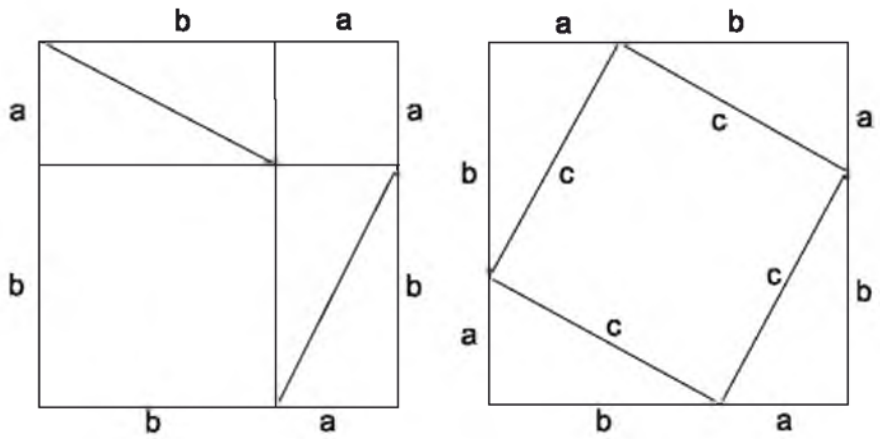
Eves (2004) declara que também se atribuem aos pitagóricos os números perfeitos, deficientes e abundantes, que apresentam ligações místicas essenciais a especulações numerológicas. Um número se diz perfeito se é igual à soma de seus divisores próprios; deficiente, se excede a soma de seus divisores; e abundante, se é menor que a soma de seus divisores próprios. Essa associação numerológica se manifestava na criação, como Deus criou o mundo em seis dias e seis é um número perfeito, já que $6 = 1 + 2 + 3$. Todos os números perfeitos que encontramos são pares; a existência ou não de números perfeitos ímpares é uma das célebres questões abertas da teoria dos números.

É também atribuído a Pitágoras e à escola pitagórica a originalidade dos números figurados, que expressam os números de pontos em certas configurações geométricas. São exemplo de números figurados os números triangulares, números quadrados, números pentagonais e assim por diante. Uma última atribuição à Pitágoras, antes do famoso teorema, se dá na relação entre intervalos musicais e razões numéricas. Esses resultados levaram os pitagóricos a iniciar o estudo científico das escalas musicais.

A tradição é unânime em atribuir a Pitágoras a descoberta independente do teorema sobre triângulos retângulos hoje conhecido como Teorema de Pitágoras, onde o quadrado sobre a hipotenusa de um triângulo retângulo é igual à soma dos quadrados sobre os catetos. A primeira demonstração foi proposta por Pitágoras, mesmo que os babilônios já tivessem conhecimento dessa relação um milênio antes.

Eves (2004) defende que mesmo tendo sido feitas muitas conjecturas quanto à demonstração que Pitágoras poderia ter dado, mas ao que parece foi uma demonstração por decomposição. Considere o triângulo retângulo de catetos a, b e hipotenusa c.

Figura 3 – Teorema de Pitágoras



Fonte: Eves (2004)

Eves (2004) propõe que consideremos os dois quadrados da figura 3, cada um de lados iguais a $a + b$. O primeiro quadrado será decomposto em seis partes — a saber, os dois quadrados sobre os catetos e quatro triângulos retângulos congruentes ao triângulo dado. O segundo quadrado está decomposto em cinco partes — a saber, o quadrado sobre a hipotenusa e quatro triângulos retângulos congruentes ao triângulo dado. Subtraindo-se iguais de iguais, conclui-se que o quadrado sobre a hipotenusa é igual à soma dos quadrados sobre os catetos.

2.3 Pierre de Fermat

É necessário que discutamos a construção do problema conhecendo também um pouco da história de Pierre de Fermat. Eves (2004) comenta que Fermat nasceu em Beaumont-de-Lomagne, perto de Toulouse, em 17 de agosto de 1601. Sabe-se que morreu em Castres ou Toulouse a 12 de janeiro de 1665. Todavia, há uma divergência entre essas datas. Em sua laje tumular, originalmente na igreja dos Agostinianos em Toulouse e depois transferida para o museu local, consta a data precedente como a da morte de Fermat, com 57 anos de idade. Devido a esse conflito de datas, costuma-se escrever (1601?-1665) para nascimento e morte de Fermat.

Em sua vida, havia grande probabilidade de não seguir uma carreira na matemática. Eves (2004) nos diz que Fermat era filho de um comerciante de couro e recebeu sua educação inicial em casa. Aos 30 anos, alcançou o posto de conselheiro do Parlamento de Toulouse, mas foi um advogado humilde e discreto, e isso foi deveras importante para que um gênio da matemática surgisse. Em seu tempo de lazer, dedicou-se à matemática.

Fermat foi um contemporâneo de René Descartes e contribuiu de maneira extremamente significativa para a construção da geometria analítica moderna. A atribuição da prioridade a Fermat se apoia numa carta escrita a Roberval em setembro de 1636, na qual afirma que suas ideias já tinham então sete anos. Os detalhes a respeito apareceram no artigo Isogoge ad Locos Planos et Solidos, publicado postumamente, segundo Eves (2004).

Esse artigo mostra algumas descobertas de Fermat e nele estão a equação geral da reta, a equação geral da circunferência e uma discussão sobre hipérboles, elipses e parábolas. Fermat foi tão brilhante no estudo da geometria analítica que prôpos muito mais curvas que Descartes. Eves (2004) relata que as curvas $x^m \cdot y^n = a$, $y^n = a \cdot x^m$ e $r^n = a \cdot \theta$ são ainda conhecidas como hipérboles, parábolas e espirais de Fermat.

Embora publicasse muito pouco durante sua vida, Fermat manteve correspondência científica com muitos dos principais matemáticos de seu tempo e, dessa maneira, exerceu considerável

influência sobre seus contemporâneos. Fermat enriqueceu tantos ramos da matemática com tantas contribuições importantes que é considerado o maior matemático francês do século XVII, como explica muito bem Eves (2004). O trabalho de Fermat foi brilhante diante da Geometria Analítica, mas igualmente fantástico diante da Aritmética.

Eves (2004) é preciso ao dizer que a atenção de Fermat para a teoria dos números provavelmente foi despertada pela tradução latina da Aritmética de Diofanto, feita por Bachet de Méziriac em 1621. Muitas das contribuições de Fermat ao assunto se deram na forma de enunciados e notas escritos nas margens do exemplar que ele possuía do trabalho de Bachet.

Dentre suas muitas contribuições na Teoria dos Números, está o famoso Pequeno Teorema de Fermat, conferir Teorema 3.15, que é de fundamental importância na aritmética dos restos e no estudo dos números primos. O interessante é que Fermat nunca provou este teorema, apenas o enunciou em uma carta de 18 de outubro de 1640 a Frénicle de Bessy. A primeira demonstração publicada desse teorema data de 1736 e é devida a Euler.

Fermat também enunciou e provou que um número primo ímpar pode ser escrito como a diferença entre dois quadrados, e essa maneira é única. Mas uma contribuição de Fermat chama muito a atenção e é a base deste trabalho. Fermat propôs um teorema muito importante, conferir Teorema 5.5, onde a área de um triângulo retângulo de lados inteiros não pode ser um quadrado perfeito inteiro.

Fermat propôs essa demonstração em uma carta que foi endereçada a Carcavi e datada de 1659. As datas das várias notas sobre Diofanto não são conhecidas, mas é provável que esta nota tenha sido escrita em algum momento entre 1636 e 1641, ou pelo menos, em números redondos, vinte anos antes da carta. Este fato é importante, pois a nota e a carta não concordam — pelo menos na aparência, como cita Walsh (1927).

Walsh (1927) informa que o assunto comum da Nota e da passagem na Carta é o novo método de prova por "descendência infinita ou indefinida", conforme aplicado à proposição de que a área de um triângulo retângulo em números (inteiros) não pode ser um quadrado (perfeito) - ou, em outras palavras, que em soluções integrais de $x^2 + y^2 = z^2$, $\frac{x \cdot y}{2}$ não pode ser um quadrado. Walsh também nos propõe como foi essa prova dada por Fermat, onde segue-se alguns passos.

> Se a área de um triângulo [retângulo] fosse um quadrado, (1) seriam dados dois biquadrados cuja diferença seria um quadrado; de onde se segue que (2) seriam dados dois quadrados tais que tanto sua soma quanto sua diferença seriam quadrados. Portanto, (3) um número igual a um quadrado [isto é, um número quadrado] é dado que é composto de um quadrado e o dobro de um quadrado, com a condição de que os quadrados que o compõem [tomados isoladamente] formem um quadrado. Mas (4) se um número quadrado é composto de um

> quadrado e o dobro de outro quadrado, seu lado [raiz] é similarmente composto de um quadrado e o dobro de um quadrado, como podemos demonstrar muito facilmente. Portanto, será concluído que (5) esse lado é a soma dos lados sobre o ângulo reto em um [ou o] triângulo retângulo, e que um dos quadrados que compõem a soma forma a base e o outro lado que é perpendicular (isto é, os dois catetos deste triângulo são eles próprios, um um único quadrado, e outro o dobro de um quadrado). (6) Esse triângulo retângulo, portanto, será composto de dois quadrados cuja soma e diferença serão quadrados. Mas (7) esses dois quadrados serão provados menores do que os quadrados originais obtidos primeiro [em (2)], cuja soma e diferença é um quadrado. Assim, se dois quadrados são dados cuja soma e diferença são quadrados, será dado, em números inteiros, uma soma de dois quadrados da mesma natureza (isto é, tal que sua diferença também é um quadrado), menor do que a (soma) precedente. (8) Pelo mesmo raciocínio, será dada outra [soma] menor que esta, encontrada da [mesma] maneira [que] a precedente [foi encontrada], e sempre em infinitum números inteiros menores serão encontrados apresentando a mesma [propriedade]; (9) o que é impossível, porque quando qualquer número inteiro é dado, uma infinidade de números inteiros não pode ser dada menor que ele. A inserção da demonstração completa e detalhada [da série de somas cada vez menores] é impedida pela estreiteza da margem.(Walsh, 1927, p.412-413)

Uma das mentes mais brilhantes que o mundo já viu fez uma prova extremamente interessante em um cantinho da margem do papel e compartilhou com alguém com quem discutia matemática. Esse problema, sua base aritmética, sua base geométrica e sua demonstração seguem nos capítulos subsequentes.

3 CONSTRUÇÃO ARITMÉTICA DO PROBLEMA

Construir a parte histórica deste trabalho é deveras importante para o entendimento correto do problema, mas ainda mais importante é conter a fundamentação aritmética e geométrica do problema. Neste capítulo dar-se-a importância a construção aritmética, onde será discutindo todos os pontos que traçarão uma linha construtiva da demonstração do Teorema de Fermat. A fundamentação teórica deste problema está pautada em (Hefez, 2006), (Santos,1998), (Morgado, 2014), (Faria, 2015) e (Feiten, 2024).

3.1 Axiomas de Peano

Antes de iniciar uma construção mais detalhada no problema sobre os triângulos pitagóricos e as relações aritméticas, é de fundamental importância entender o conceito de número natural. Os números naturais constituem um modelo matemático que permite a operação de contagem. Podendo representá-los por:

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

Todavia, nem sempre foi tão fácil entender os números naturais, e deve-se a Giuseppe Peano (1858-1932) a constatação de que se pode elaborar toda a teoria dos números naturais a partir de quatro fatos básicos, conhecidos atualmente como os axiomas de Peano.

Assim, os números naturais $(\mathbb{N})$ possuem quatro propriedades fundamentais, das quais resultam, como conseqüências lógicas, todas as afirmações verdadeiras que se podem fazer sobre esses números.

Definição 3.1. O conjuntos do números naturais $(\mathbb{N})$ é caracterizado pelas seguintes propriedades:

1. Existe uma funçaõ $s : \mathbb{N} \to \mathbb{N}$ que associa a cada $n \in \mathbb{N}$ um elemento $s(n) \in \mathbb{N}$, chamado sucessor de n;
2. A Função $s : \mathbb{N} \to \mathbb{N}$ é injetiva;
3. Existe um único elemento 1 no conjunto $\mathbb{N}$, tal que $1 \neq s(n)\ \forall\ n \in \mathbb{N}$;
4. Se um subconjunto $X \subset \mathbb{N}$ é tal que $1 \in X$ e $s(X) \subset X$ (isto é, se $n \in X \Rightarrow s(n) \in X$), então $X = \mathbb{N}$.

Com essa caracterização vê-se que o conjunto dos naturais possui um menor elemento, o 1, que não é sucessor de nenhum outro e todo número que pertence aos naturais possui sucessor.

Além disso, por ser injetiva, cada sucessor é único e por isso cada número possui apenas um único sucessor.

Observação 3.1. Há uma outra forma de escrever os axiomas de Peano, com igual rigor e uma linguagem mais objetiva,

1. Todo $n \in \mathbb{N}$ possui um sucessor, que é representado pro $n + 1$;
2. Se $m + 1 = n + 1$ então $m = n$;
3. Existe um único elemento 1 no conjunto $\mathbb{N}$, tal que $1 \neq n + 1 \; \forall \; n \in \mathbb{N}$;
4. Se um subconjunto $X \subset \mathbb{N}$ é tal que $1 \in \mathbb{N}$ e $n + 1 \in X$, para cada $n \in X$, então $X = \mathbb{N}$.

Observação 3.2. O quarto axioma de Peano é chamado de axioma de indução, esse axioma dá origem ao Príncipio da Indução Finita, que será tratado na seção seguinte.

3.2 Princípio da Indução Finita

O ponto de partida deste capítulo se dá no estudo do Princípio da Indução Finita (PIF). O PIF é um dos métodos de prova mais utilizado na demonstração de propriedades. O Princípio da Indução Finita é um dos axiomas que caracterizam o conjunto dos números naturais.

Teorema 3.1. *(Princípio da Indução Finita) Seja $P(n)$ uma proposição acerca de um número natural n maior ou igual a um número natural n_0 fixado. Se p possui as seguintes propriedades:*

1. *(Base de Indução) $P(n_0)$ é verdadeira.*
2. *(Passo Indutivo) Se $P(n)$ é verdadeira para algum $n \geq n_0$, então $P(n + 1)$ também será verdadeira.*

   então $P(n)$ é válida para todo $n \geq n_0$.

Demonstração. Em primeiro lugar, considere $n_0 = 1$ e assim tome $X = \{n \in \mathbb{N} / P(n) \; verdadeira\} \subset \mathbb{N}$. Por hipótese, pela base de indução, $P(1)$ é verdadeira, então $1 \in X$. Além disso, pelo passo indutivo, $P(n + 1)$ é verdadeira uma vez que $P(n)$ verdade implica que $P(n + 1)$ também é verdade. Logo, se $P(n + 1)$ é verdadeira, $n + 1 \in X$ pela construção do conjunto X. Assim, pelo quarto axioma de Peano, o axioma da indução, tem-se que $X = \mathbb{N}$. Portanto, $P(n)$ vale $\forall \; n \in \mathbb{N}$, como era desejado.

Em segundo lugar, como é possível que o processo indutivo não inicie em $n_0 = 1$, considere que $X = \{n \in \mathbb{N} / P(n_0 + n - 1)\ verdadeira\}$ e daí tem-se que:

1. $1 \in X$, pois $P(n_0 + 1 - 1) = P(n_0)$, que é válida por 1;

2. $n \in X \Rightarrow n + 1 \in X$.

Suponha que $n \in X$ e, por definição de X, $P(n_0 + n - 1)$ é verdadeira. Perceba que:

$$n \geq 1 \Rightarrow n_0 + n - 1 \geq 1 + n_0 - 1 = n_0 \tag{1}$$

E por fim, como $n_0 + n - 1 \geq n_0$ e $P(n_0 + n - 1)$ é verdadiera, pelo passo indutivo, segue que $P(n_0 + n)$ é verdadeira, ou seja, $n + 1 \in X$. E pelo axioma de indução, o quarto axioma de Peano, $X = \mathbb{N} \Rightarrow P(n_0 + n - 1)$ é verdadeira $\forall\ n \in \mathbb{N}$. □

O processo do Princípio da Indução Finita é deveras coeso, onde na Base de Indução é provado se a propriedade é válida para $n = n_0$, que é um valor inicial. O passo indutivo consiste em mostrar como utilizar a validade da propriedade para um dado n, a chamada hipótese de indução, para provar a validade da mesma propriedade para o inteiro seguinte $n + 1$. Ao verificar-se a base de indução e o passo indutivo, tem-se uma série de implicações como consequência onde,

$$P(n_0) \Rightarrow P(n_0 + 1) \Rightarrow P(n_0 + 2) \Rightarrow P(n_0 + 3) \Rightarrow ... \Rightarrow P(n) \tag{2}$$

Asssim, se $P(n_0)$ for verdadeira pelo passo indutivo $P(n_0+1)$ é verdadeira. Daí $P(n_0+2)$ é verdadeira e por consequência tem-se $P(n)$ verdadeiro $\forall$ natural $n \geq n_0$,

Exemplo 3.1. Mostre que, dado $x \neq 1$, tem-se: $1 + x + x^2 + x^3 + ... + x^{n-1} = \frac{x^n - 1}{x - 1}$, $\forall n \in \mathbb{N}$.

$Sol.$ Utilizando o Princípio da Indução Finita (PIF), têm-se:

$$P(1) : \frac{x^1 - 1}{x - 1} = 1$$

Com isso, vê-se que a base de indução é verdadeira. Após o primeiro passo considere que $P(n)$ é verdadeira para algum $n \geq 1$ e assim $P(n) : 1 + x + x^2 + x^3 + ... + x^{n-1} = \frac{x^n - 1}{x - 1}$ é verdadeira. E partindo disso ver-se-a a veracidade de $P(n + 1)$:

$$P(n + 1) : 1 + x + x^2 + x^3 + ... + x^{n-1} + x^n = \frac{x^{n+1} - 1}{x - 1}$$

Por hipótese de indução, têm-se:

$$\frac{x^n - 1}{x - 1} + x^n = \frac{x^{n+1} - 1}{x - 1}$$

$$\frac{x^n - 1 + x^{n+1} - x^n}{x - 1} = \frac{x^{n+1} - 1}{x - 1}$$

$$\frac{x^{n+1} - 1}{x - 1} = \frac{x^{n+1} - 1}{x - 1}$$

Assim, $P(n+1)$ é verdadeira e daí conclui-se que $P(n)$ é verdadeira $\forall\ n \geq 1$.

Há também uma outra caracterização para o Princípio da Indução Finita, chamada de Indução Forte.

Teorema 3.2. *(Princípio da Indução Forte) Seja $P(n)$ um enunciado que descreve uma propriedade sobre um número natural n maior ou igual aum número natural n_0 fixado. Se pudermos definir duas condições:*

1. *(Base de Indução) $P(n_0)$ é verdadeira.*
2. *(Passo Indutivo) Se $P(k)$ é verdadeira $\forall\ k \in \mathbb{N}$ tal que $n \geq k \geq n_0$, então $P(n+1)$ também será verdadeira.*

   Se isso ocorrer pode-se afirmar que $P(n)$ é válida para todo $n \geq n_0$.

Demonstração. Em primeiro lugar, considere $n_0 = 1$. Assim, tome a sentença aberta $Q(k)$: $P(k)$ verdadeira, $\forall\ k \leq n$. Pela base de indução, $P(1)$ é verdadeira e assim $Q(1)$ também. Suponhamos agora que $Q(n)$ é verdadeira e isso tem como consequência que $P(k)$ é válida $\forall\ k \leq n$, mas pelo passo indutivo, ve-se que $P(n+1)$ é verdadeiro. Isso implica que $P(k)$ é verdadeiro $\forall\ k \leq n+1$ e asssim $Q(n+1)$ também é válida. Portanto, pelo PIF, $Q(n)$ é verdadeira $\forall\ n \in \mathbb{N}$, de onde decorre a validade de $P(n)\ \forall\ n \in \mathbb{N}$. □

Exemplo 3.2. (Teorema Fundamental da Aritmética) Todo $n \in \mathbb{N}$ com $n > 1$ é primo ou pode ser escrito como um produto de números primos.

$Sol.$ Utilizando o Princípio da Indução Forte, têm-sê que a base de indução é facilmente demonstrada pois está sendo considerando um $n \geq 2$ e para $n = 2$ temos já um número primo. Assim, considere como hipótese de indução que $P(k)$ é válida $\forall\ 2 \leq k \leq n$ e daí é preciso mostrar que $P(k+1)$ também é válido. Se $k+1$ for primo a solução é trivial, mas se $k+1$ não for primo têm-se que $k+1 = a.b$, com $a < k+1$ e $b \leq k+1$ e pela hiótese de indução a e

b podem ser decompostos em um produto de números primos e assim $k+1$ também pode ser decomposto em um produto de números primos. Com isso conclui-se que todo $n \in \mathbb{N}$ com $n > 1$ é primo ou pode ser escrito como um produto de números primos.

Alinhado ao Princípio da Indução Finita tem-se uma última caracterização chamada de Princípio da Boa Ordenação, onde há a garantia de que qualquer subconjunto não vazio X de $\mathbb{N}$ possui um menor elemento.

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

Demonstração. Demonstrar o princípio da boa ordenação é o equivalente a provar que todo $X \subset \mathbb{N}$ que não possui menor elemento é vazio, ou seja, $X^c = \mathbb{N}$. Assim, considere que X é um o conjunto que não possui menor elemento. Considere que $P(n) : n \in X^c$. E daí,

1. $P(1)$ vale, pois $1 \notin X$, já que $1 \in X \Rightarrow 1$ é menor elemento de X;
2. $P(k)$ vale, $\forall\ 1 \leq k \leq n \Rightarrow P(n+1)$.

Suponha qie $P(k)$ é verdade, para todo $1 \leq k \leq n$. Todavia isso implica que $n+1 \notin X$, pois se pertencesse seria o menor elemento de X, o que é um absurdo pois X não possui menor elemento. Assim, $n+1 \in X^c \Rightarrow P(n+1)$ ocorre. Pelo PIF, $P(n)$ é válida $\forall\ n \in \mathbb{N}$. Logo $X^c = \mathbb{N}$ e assim $X = \emptyset$. □

3.3 Recorrências

Uma sequência é definida recursivamente se ela for dada por uma regra (recorrência) que permite calcular um termo qualquer por meio de um ou mais termos anteriores. Uma das sequências recursivas mais famosas são as progressões aritméticas e progressões geométricas, que são definidas de maneira muito simples por meio de uma recorrência. Além disso, tem-se também o fatorial, potências com números naturais e a famosa sequência de Fibonacci.

Exemplo 3.3. Algumas sequências Recursivas:

1. Progressões Aritméticas: $a_n = a_{n-1} + r$;
2. Progressões Geométrica: $a_n = a_{n-1} \cdot q$;
3. Fatorial: $a_n = n \cdot a_{n-1}$;

4. Potências com Expoente Natural: $a^n = a \cdot a^{n-1}$

5. Sequência de Fibonacci: $F_{n+2} = F_{n+1} + F_n$, co $F_1 = F_2 = 1$

Uma recorrência por si só não define uma sequência. Se parar um pouco e pensar a recorrência $x_{n+1} = x_n + 2$ é satisfeita para a sequência dos números ímpares, a sequência dos números pares e também para todas as progressões aritméticas que possuem razão 2. Assim, para que a sequência seja definida de maneira perfeita é necessário que se tenha o conhecimento do(s) primeiro(s) termo(s). Este tópico ater-se-a as recorrências lineares de primeira ordem, buscando sempre determinar uma fórmula fechada em função de n.

Exemplo 3.4. Resolva a recorrência $x_{n+1} = x_n + 2^n$, com $x_1 = 1$.

$Sol.$ Para determinar uma fórmula em fechada em função de n é preciso que se analise os póximos termos da recorrência. Sabe-se que $x_1 = 1$ e pela recorrência vê-se que $x_2 = x_1 + 2^1 = 1 + 2 = 3$, $x_3 = x_2 + 2^2 = 3 + 4 = 7$ e assim por diante. Todavia é preciso que se desenvolva uma fórmula fechada em função de n e para isso,

$$x_2 = x_1 + 2^1$$

$$x_3 = x_2 + 2^2$$

$$x_4 = x_3 + 2^3$$

$$x_5 = x_4 + 2^4$$

$$... \quad ... \quad ...$$

$$x_n = x_{n-1} + 2^{n-1}$$

Daí, soma-se os dois lados das equações e ter-se-a:

$$x_2 + x_3 + x_4 + +... + x_{n-1} + x_n = x_1 + x_2 + x_3 + ... + x_{n-1} + 2 + 2^2 + 2^3 + ... + 2^{n-1}$$

$$x_n = x_1 + 2 + 2^2 + 2^3 + ... + 2^{n-1}$$

$$x_n = 1 + 2 + 2^2 + 2^3 + ... + 2^{n-1}$$

$$x_n = \frac{1.(2^n - 1)}{2 - 1}$$

$$x_n = 2^n - 1$$

Exemplo 3.5. Quantas são as sequências de 10 termos, pertencentes a $\{0, 1, 2\}$, que não possuem dois termos consecutivos iguais a 0?

Sol. Chame x_n o número de sequências com n termos, o valor de x_{n+2} será a soma das seguintes quantidades:

1. O número de sequências de $n + 2$ termos que começam por 1 e não possuem dois zeros consecutivos. Isso é precisamente igual a x_{n+1}, pois se o primeiro termo é 1, para formar a sequência basta determinar os termos a partir do promeiro, o que pode ser feito de x_{n+1} modos.

2. O números de sequências de $n+2$ termos que começam por dois e não possuem dois zeros consecutivos. Analogamente ao item 1, tem-se que isso pode ser feito de x_{n+1} modos.

3. O número de sequências de $n + 2$ termos que começa por zero e não possuem dois zeros consecutivos. Se o primeiro termo é zero, tem-se duas opções para a escolha do segundo termo (1 ou 2) e, escolhido o segundo termo, tem-se x_n modos de escolher os demias. Há assim $2x_n$ sequências começadas em 0.

Assim, a recorrência para determinar quantas sõa as sequência de 10 termos pertencentes a $\{0, 1, 2\}$, que não possuem dois termos consecutivos iguais a zero é $x_{n+2} = 2(x_{n+1}+x_n)$. Além disso sabe-se que $x_1 = 3$ $(0, 1, 2)$ e $x_2 = 8$ $(01, 02, 10, 11, 12, 20, 21, 22)$. Com isso, teremos que:

$$x_3 = 2 \cdot (8 + 3) = 2 \cdot 11 = 22$$

$$x_4 = 2 \cdot (22 + 8) = 2 \cdot 30 = 60$$

$$x_5 = 2 \cdot (60 + 22) = 2 \cdot 82 = 164$$

$$x_6 = 2 \cdot (164 + 60) = 2 \cdot 224 = 448$$

$$x_7 = 2 \cdot (448 + 164) = 2 \cdot 612 = 1224$$

$$x_8 = 2 \cdot (1224 + 448) = 2 \cdot 1672 = 3344$$

$$x_9 = 2 \cdot (3344 + 1224) = 2 \cdot 4568 = 9136$$

$$x_{10} = 2 \cdot (9136 + 3344) = 2 \cdot 12480 = 24960$$

Sendo assim, existem 24960 sequências de 10 termos, pertencentes a $\{0, 1, 2\}$, que não possuem dois termos consecutivos iguais a zero.

3.4 Divisibilidade

O problema dos triângulos pitagóricos está situado dentro dos números naturais, assim a seção de divisibilidade estará fundamentada dentro do mesmo conjunto. A divisão de um número natural por outro número natural nem sempre é possível. Assim, expressa-se essa possibilidade por meio da relação de divisibilidade.

Quando não existe uma relação de divisibilidade entre dois números, ainda assim é possível efetuar uma "divisão de resto pequeno", chamada de divisão euclidiana. O estudo dos restos é algo muito importante na Teoria dos Números. O fato de poder realizar essa divisão tem como consequência muitas propriedades dos números naturais.

Definição 3.2. Dados $a, b \in \mathbb{N} \cup \{0\}$, com $a \neq 0$, diremos que a divide b, escrevendo $a \mid b$ quando existir $c \in \mathbb{N} \cup \{0\}$ tal que $b = a \cdot c$. Neste caso, diremos também que a é um divisor ou um fator de b ou, ainda, que b é um múltiplo de a.

Observação 3.3. É importante observar que a notação $a \mid b$ não representa nenhma operação em $\mathbb{N} \cup \{0\}$, nem representa uma fração.

Observação 3.4. A negação de $a \mid b$ é representada por $a \nmid b$, significando que não existe $c \in \mathbb{N} \cup \{0\}$ tal que $b = a \cdot c$.

Exemplo 3.6. $1 \mid 0$, $2 \mid 4$, $12 \mid 36$, $5 \nmid 4$, $2 \nmid 5$.

Definição 3.3. Suponha que $a \mid b$ e seja $c \in \mathbb{N}$ tal que $b = a \cdot c$. Assim, c é chamado de quociente de b por a e denotado pro $c = \frac{b}{a}$ (Lembre-se que por definição $a \neq 0$).

Exemplo 3.7. $\frac{0}{1} = 0$, $\frac{4}{2} = 2$, $\frac{36}{12} = 3$, $\frac{12}{3} = 4$.

Proposição 3.1. *Sejam $a, b \in \mathbb{N}$ e $c \in \mathbb{N} \cup \{0\}$. Tem-se que:*

1. $1 \mid c$, $a \mid a$ *e* $a \mid 0$.
2. *Se* $a \mid b$ *e* $b \mid c$, *então* $a \mid c$

Demonstração. Para o item 1, tem-se claramente consequências lógicas que decorrem da definição 3.2., assim $c = 1.c$, $a = a.1$ e $0 = a.0$. Para o item 2, veja que pela Definição 3.2.

$$a \mid b \iff \exists\, d \in \mathbb{N} \cup \{0\}; b = a \cdot d \tag{3}$$

$$b \mid c \iff \exists\, e \in \mathbb{N} \cup \{0\}; c = b \cdot e \tag{4}$$

Ao olhar-se para (3) e substituí-lo em (4), tem-se

$$c = b \cdot e \Longleftrightarrow c = (a \cdot d) \cdot e \Longleftrightarrow c = a \cdot (d \cdot e)$$

O que nos mostra que $a \mid c$. □

Observação 3.5. O item 1 da proposição acima diz que todo número natural é divisível por 1 e por si mesmo.

Observação 3.6. Não é considerado neste trabalho que o 0 seja um número natural. Se caso o leitor considerar, a observação 3.5 ficaria definida como todo número natural é divisível por um e, se não nulo, por si mesmo.

Proposição 3.2. *Se* $a, b, c, d \in \mathbb{N} \cup \{0\}$*, com* $a \neq 0$ *e* $c \neq 0$*, então,*

$$a \mid b \textit{ e } c \mid d \Longrightarrow (a.c) \mid (b.d)$$

Demonstração. Vai-se utilizar o mesmo racíocio do item 2, da Proposição 3.1. Assim, pela Definição 3.2.

$$a \mid b \Longleftrightarrow \exists\, e \in \mathbb{N} \cup \{0\}; b = a \cdot e; \tag{5}$$

$$c \mid d \Longleftrightarrow \exists\, f \in \mathbb{N} \cup \{0\}; d = c \cdot f \tag{6}$$

Assim, fazendo o produto de (5) e (6), tem-se

$$b \cdot d = (a \cdot e) \cdot (c \cdot f)$$

$$b \cdot d = (a \cdot c) \cdot (e \cdot f)$$

Logo, $(a \cdot c) \mid (b \cdot d)$. □

Observação 3.7. Em particular, se $a \mid b$, então $(a \cdot c) \mid (b \cdot c)$, $\forall\, c \in \mathbb{N}$.

Proposição 3.3. *Sejam* $a, b, c \in \mathbb{N} \cup \{0\}$*, com* $a \neq 0$*, tais que* $a \mid (b + c)$*, então*

$$a \mid b \Longleftrightarrow a \mid c.$$

Demonstração. Pela Definição 3.2. tem-se que

$$a \mid (b + c) \Longleftrightarrow \exists\, d \in \mathbb{N} \cup \{0\}; b + c = a \cdot d. \tag{7}$$

Como é um se, somente se, é preciso fazer a ida e a volta

$\Rightarrow$) Pela definição 3.2., tem-se

$$a \mid b \Longleftrightarrow \exists\, e \in \mathbb{N} \cup \{0\}; b = a \cdot e. \tag{8}$$

Assim, substituindo (8) em (7), tem-se

$$a \cdot e + c = a \cdot d$$

$$c = a \cdot (d - e)$$

Sendo assim, tem-se que $a \mid c$.

$\Leftarrow$) Pela definição 3.2., tem-se

$$a \mid c \Longleftrightarrow \exists\, f \in \mathbb{N} \cup \{0\}; c = a \cdot f. \tag{9}$$

Assim, substituindo (9) em (7), tem-se

$$b + a \cdot f = a \cdot d$$

$$b = a \cdot (d - f)$$

Sendo assim, tem-se que $a \mid b$. Portanto, se $a \mid (b + c)$, então $a \mid b \Longleftrightarrow a \mid c$. □

Proposição 3.4. *Se* $a, b, c, \in \{\mathbb{N} \cup 0\}$*, com* $a \neq 0$ *e* $b \geq c$*, tais que* $a \mid (b - c)$*. Então:*

$$a \mid b \Longleftrightarrow a \mid c.$$

Demonstração. Pela Definição 3.2. tem-se que

$$a \mid (b - c) \Longleftrightarrow \exists\, d \in \mathbb{N} \cup \{0\}; b - c = a \cdot d. \tag{10}$$

Como é um se, somente se, é preciso fazer a ida e a volta

$\Rightarrow$) Pela definição 3.2., tem-se

$$a \mid b \Longleftrightarrow \exists\, e \in \mathbb{N} \cup \{0\}; b = a \cdot e. \tag{11}$$

Assim, substituindo (11) em (10), tem-se

$$a \cdot e - c = a \cdot d$$

$$-c = a \cdot (d - e)$$

$$c = a \cdot (e - d)$$

Sendo assim, tem-se que $a \mid c$.

$\Leftarrow$) Pela definição 3.2., tem-se

$$a \mid c \Longleftrightarrow \exists\, f \in \mathbb{N} \cup \{0\}; c = a \cdot f. \tag{12}$$

Assim, substituindo (12) em (10), tem-se

$$b - a \cdot f = a \cdot d$$

$$b = a \cdot (d + f)$$

Sendo assim, tem-se que $a \mid b$.

Portanto, se $a \mid (b - c)$, então $a \mid b \Longleftrightarrow a \mid c$. □

Proposição 3.5. *Se $a, b, c \in \mathbb{N} \cup \{0\}$, com $a \neq 0$ e $x, y \in \mathbb{N} \cup \{0\}$ são tais que $a \mid b$ e $a \mid c$, então $a \mid (xb + yc)$; e se $xb \geq yc$, então $a \mid (xb - yc)$.*

Demonstração. Pela definição 3.2, tem-se que:

$$a \mid b \Longleftrightarrow \exists\, d \in \mathbb{N} \cup \{0\}; b = a \cdot d; \tag{13}$$

$$a \mid c \Longleftrightarrow \exists\, e \in \mathbb{N} \cup \{0\}; c = a \cdot e. \tag{14}$$

Assim, Por (13) e (14)

$$xb \pm yc = x(a \cdot d) \pm y(a \cdot e) = a(x \cdot d) \pm a(y \cdot e) = a(x \cdot d \pm y \cdot e).$$

Assim, $a \mid (xb + yc)$ e $a \mid (xb - yc)$, já que nas condições dadas, $xd \pm ye \in \mathbb{N} \cup \{0\}$. □

Proposição 3.6. *Dados $a, b \in \mathbb{N}$, temos que*

$$a \mid b \Longrightarrow a \leq b.$$

Demonstração. Pela definição 3.2., tem-se

$$a \mid b \Longleftrightarrow \exists\, c \in \mathbb{N}; b = a \cdot c; \tag{15}$$

Sabe-se que como $c \in \mathbb{N}$, $c \geq 1$, e daí

$$a \leq a \cdot c \Longrightarrow a \leq b.$$

Em particular, se $a \mid 1$, então $a \leq 1$ e, portanto, $a = 1$. □

Observação 3.8. Claramente a recíproca da proposição 3.6 não é válida, pois, por exemplo, $3 \geq 2$, no entanto $2 \nmid 3$.

Observação 3.9. Uma observação interesante é que a relação de divisibilidade em $\mathbb{N}$ é uma relação de ordem, pois

1. Reflexiva: $\forall\, a \in \mathbb{N}$, $a \mid a$. (Proposição 3.1., item 1);

2. Transitiva: se $a \mid b$ e $b \mid c$, então $a \mid c$. (Porposição 3.1., item 2);

3. Anti-Simétrica: se $a \mid b$ e $b \mid a$, então $a = b$. (Segue-se claramente da Proposição 3.6.).

Um dos teoremas mais importantes da aritmética trata realmente sobre quando um número natural a não divide o número natural b. Dá-se a Euclides, em seu livro os Elementos, a primeira menção, mesmo que sem prova, de que é sempre possível efetuar a divisão de b por a, com resto.

Teorema 3.4. *(Divisão Euclidiana) Sejam a e b dois números naturais com $0 < a < b$. Existem dois únicos números naturais q e r tais que*

$$b = a \cdot q + r, \textit{com } r < a.$$

Demonstração. Suponha que $b > a$ e considere, equanto fizer sentido, os números

$$b, b - a, b - 2a, \ldots, b - n \cdot a, \ldots$$

Pelo Teorema 3.3., o conjunto S formado pelos termos acima tem um menor elemento $r = b - q \cdot a$. Daí, é preciso demonstrar que $r < a$. Se $a \mid b$, então $r = 0$ e nada mais tem-se a provar. Se por outro lado, $a \nmid b$, então $r \neq a$, e portanto, basta mostrar que não pode ocorrer $r > a$. Se $r > a$, existiria $c < r$ tal que $r = a + c$. Como foi definido que $r = b - q \cdot a$, tem-se que,

$$c = b - (q + 1) \cdot a \in S, \text{ com } c < r,$$

o que é uma contradição, já que r é o menor elemento de S. Assim, tem-se que $b = a \cdot q + r$ com $r < a$, o que prova a existência de q e r.

Agora que a existência foi provada, é preciso mostrar a unicidade. É importante notar que dois elementos distintos de S, a diferença entre o maior e o menor desses elementos, sendo um múltiplo de a, é pelo menos a. Assim, se $r = b - q \cdot a$ e $r^{'} \geq b - q^{'} \cdot a$, com $r < r' < a$, teríamos $r' - r \geq a$, o que acarretaria $r^{'} \geq r + a \geq a$, o que é um absurdo. Portanto $r = r'$ e daí $q = q^{'}$. □

Observação 3.10. Nas condições do Teorema 3.4., os números q e r são chamados, respectivamente, de $quociente$ e de $resto$ da divisão de b por a.

Observação 3.11. É importante notar duas coisas:

1. O resto da divisão de b por a só será 0 se, e somente se, a divide b;
2. A demonstração do Teorema 3.4. fornece um algoritmo, um procedimento executável. para calcular o quociente e o resto da divisão de um número por outro, por subtrações sucessivas.

Exemplo 3.8. Determine o quociente e o resto da divisão de 51 por 7.

$Sol.$ Vai-se utilizar as subtrações sucessivas em decorrÊncia do Teorema 3.4. Assim,

$$51 - 1 \cdot 7 = 44$$

$$51 - 2 \cdot 7 = 37$$

$$51 - 3 \cdot 7 = 30$$

$$51 - 4 \cdot 7 = 23$$

$$51 - 5 \cdot 7 = 16$$

$$51 - 6 \cdot 7 = 9$$

$$51 - \mathbf{7} \cdot 7 = \mathbf{2} < 7$$

Assim, vê-se que $q = 7$ e $r = 2$. Futuramente ver-se-ão outras formas de determinar, principalmente, o resto da divisão entre dois números.

Corolário 3.1. *Dados dois números*

$$a, b \in \mathbb{N} \cup \{0\}$$

com $1 < a \leq b$*, existe um número* $n \in \mathbb{N} \cup \{0\}$*, tal que*

$$na \leq b < (n+1)a.$$

Demonstração. Pelo Teorema 3.4., tem-se que existem $q, r \in \mathbb{N} \cup \{0\}$ com $r < a$, univocamente determinados, tais que $b = a \cdot q + r$. Sabe-se que

$$0 \leq r < a \iff 0 \leq b - a \cdot q < a \iff a \cdot q \leq b < a + a \cdot q \iff a \cdot q \leq b < (q+1)b.$$

Para demonstrar esse corolário basta tomar $n = q$. Assim,

$$a \cdot n \leq b < (n+1) \cdot a$$

□

Observação 3.12. A afirmação contida no Corolário 3.1. foi feita por Euclides, no livro Elementos, mesmo que sem demonstração. Essa afirmação era o que permitia deduzir a divisão euclidiana.

3.5 Máximo Divisor Comum

Definição 3.4. Dados dois números $a, b \in \{\mathbb{N} \cup 0\}$, não simultâneamente nulos, diremos que o número natural $d \in \mathbb{N}$ é um divisor comum de a e b se $d \mid a$ e $d \mid b$.

Percebe-se com um olhar simples que os números $1, 2, 3$ e 6 são os divisores comuns de 6 e 12, por exemplo. Todavia, nesta seção busca-se entender qual é o maior divisor entre dois números, não simultanemanete nulos, o que nesse caso é o 6. Euclides definiu, em seu livro Elementos, da seguinte maneira.

Definição 3.5. d é um máximo divisor comum (mdc) de a e b, não simultanemante nulos, se possuir as seguintes propriedades:

1. d é um divisor comum de a e b;
2. d é divisível por todo divisro comum de a e b, ou seja, se c é divisor comum de a e b, então $c \mid d$.

Observação 3.13. Deve-se observar que na Definição 3.4. é exigido que os números sejam não simultanemante nulos, pois caso contrário seria impossível determinar seu máximo divisor comum, pois qualquer $c \in N$ seria um divisor comum de a e b.

Observação 3.14. Se d é o mdc de a, b e c é um divisor comum de a e b, então $c \leq d$. Como o mdc é o maior divisor comum a dois números, então no máximo tem-se $c = d$, e na maioria dos casos $c < d$. Isso mostra que d é efetivamente o maior dentre todos os divisores comuns de a e b.

Observação 3.15. Isso quer dizer que se d e d' são dois mdc de um mesmo par de números, tem-se que $d = d'$.

Observação 3.16. A partir deste momento considere que mdc de a e b será deotado por (a, b), assim:

$$d = (a, b)$$

Teorema 3.5. *Seja* $d = (a, b)$*, então* $\exists\, x, y \in \mathbb{N} \cup \{0\};\ d = x \cdot a + y \cdot b$

Demonstração. Esse teorema é muito importante e facilmente demosntrável. Considere que $\exists\, c \in \mathbb{N}$, tal que $c = x \cdot a + y \cdot b$. Assim,

$$d \mid a \iff \exists\, k \in \mathbb{N} \cup \{0\}; a = d \cdot k; \tag{16}$$

$$d \mid b \iff \exists\, l \in \mathbb{N} \cup \{0\}; b = d \cdot l. \tag{17}$$

Assim, substituindo (16) e (17) em $c = x \cdot a + y \cdot b$, tem-se

$$c = d(x \cdot k + y \cdot l) \iff d \mid c$$

Se $d \mid c$ tem-se que $d \leq c$ e como $d = (a, b)$ isso implica que $d = c$. Portanto, $d = a \cdot x + b \cdot y$. □

Observação 3.17. Uma outra maneira, igualmente válida e mais rápida, de demonstrar esse teorema consistem em ver que $d \mid a$ e $d \mid b$ por definição e pela Proposição 3.5., $d \mid (a \cdot x + b \cdot y)$. Como $d \leq a \cdot x + b \cdot y$ e $d = (a, b)$, e por isso precisa ser o maior divisor comum, tem-se que $d = a \cdot x + b \cdot y$.

Proposição 3.7. *Para todo* $c \in \mathbb{N}$ *tem-se* $(ca, cb) = c \cdot (a, b)$.

Demonstração. Considere que $d = (ca, cb)$ e $d_1 = (a, b)$. Pelo Teorema 3.5. tem-se que $\exists\, x, y; d = cax + cby$ daí $d = c(ax + by)$ e como $d_1 = ax + by$, tem-se que $d = c \cdot d_1$. Portanto, $(ca, cb) = c \cdot (a, b)$. □

Proposição 3.8. *Se* $c \in \mathbb{N}$ *e* a *e* b *são divisíveis por* c*, então:*

$$\left(\frac{a}{c}, \frac{b}{c}\right) = \frac{1}{c} \cdot (a, b)$$

Demonstração. Como a e b são divisíveis por c, tem-se que $\frac{a}{c}$ e $\frac{b}{c}$ são naturais. Assim, utilizando a Proposição 3.7

$$\left(\frac{1}{c} \cdot a, \frac{1}{c} \cdot b\right) = \frac{1}{c} \cdot (a, b)$$

□

Corolário 3.2. *Se* $(a, b) = d$*, tem-se que* $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Demonstração. Pela Proposição 3.8, tem-se

$$\left(\frac{a}{d}, \frac{b}{d}\right) = \left(\frac{1}{d} \cdot a, \frac{1}{d} \cdot b\right) = \frac{1}{d} \cdot (a, b)$$

Como $(a, b) = d$, tem-se que:

$$\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{1}{d} \cdot d = 1$$

Sendo assim, $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

□

Proposição 3.9. *Seja* $a, b \in \mathbb{N} \cup \{0\}$*, naõ simultaneamente nulos, onde* $\exists\ d \in \mathbb{N}$ *tal que* $d = (a, b)$*, então*

1. $(0, a) = a$
2. $(a, a) = a$
3. $(1, a) = 1$
4. $(a, b) = (b, a)$

Demonstração. Para demonstrar a proposição acima, considere a definição de mdc, o Teorema 3.5. e a Proposição 3.7. Assim,

[1] Considere $(a, 0) = d$, daí tem-se que $d \mid a$ e $d \mid 0$, como qualquer número $n \in \mathbb{N}$ divide 0 e quer-se o maior divisor comum entre a e 0, o próprio a exerce esse valor. Assim $(a, 0) = a$.

[2] Considere $(a, a) = a(1, 1)$, pela Proposição 3.7, e perceba que $(1, 1) = 1$ pois $d \mid 1$ e como d é o mairo divisor comum de 1,tem-se que $d = 1$. Asssim, $(a, a) = a \cdot 1 = a$.

[3] Conside $(a, 1) = d$, tem-se que $d \mid a$ e $d \mid 1$ e por $d \mid 1$ o maior divisor comum de a e 1 é o próprio 1.

[4] Conside $(a, b) = d$ isso implica que $d \mid a$ e $d \mid b$ e se $(b, a) = d_1$ isso implica que $d_1 \mid a$ e $d_1 \mid b$ como o mdc é único $d = d_1$. E portanto, $(a, b) = (b, a)$. □

Proposição 3.10. *Se* $a, b \in \mathbb{N} \cup \{0\}$ *então:*

$$a \mid b \iff (a, b) = a$$

Demonstração. Como tem-se um se, e somente se, é preciso mostrar a ida e a volta. Assim

$\Rightarrow$) Considere que $a \mid b$. Se isso ocorrer, a é um divisor comum de a e b e como a é o mairo divisor de a e consequentemente de b, então se $a \mid b = (a, b) = a$.

$\Leftarrow$) Considere que $(a, b) = a$. Sendo assim, $a \mid a$ e $a \mid b$.

Sendo assim, $a \mid b \iff (a, b) = a$. □

Lema 3.1. *(Lema de Euclides) Sejam* $a, b, n \in \mathbb{N} \cup \{0\}$ *com* $a < na < b$. *Se* $\exists\ (a, b - na)$, *então* $\exists\ (a, b)$ *e*

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

Demonstração. Seja $d = (a, b)$ e $e = (a, b - na)$. Pelo Teorema 3.5, tem-se que:

$$\exists x, y \in \mathbb{N} \cup \{0\}; d = ax + by$$

$$d = ax + by + ayn - ayn = a(x + ny) + (b - na)y$$

daí, ve-se que $e \mid d$, já que $\exists\ x_0, y_0 \in \{\mathbb{N} \cup 0\};\ e = ax_0 + (b - na)y_0$. Já que $d \mid a$ e $d \mid b$, pela Preposição 3.5, tem-se que $d \mid (b - na)$ e como todo divisor comum de a e $b - na$ é divisor de f, assim $d = f$. E assim, $(a, b) = (a, b - na)$ □

Teorema 3.6. *Para* $a, b, n \in \mathbb{N} \cup \{0\}$ *tem-se (a,b)=(a,b+na)*

Demonstração. Para demonstrar este teorema é preciso usar os mesmos passos que foram usados na demonstração do Lema de Euclides. Assim, seja $d = (a, b)$ e $e = (a, b + na)$. Pelo Teorema 3.5, tem-se que:

$$\exists x, y \in \mathbb{N} \cup \{0\}; d = ax + by$$

$$d = ax + by + ayn - ayn = a(x - ny) + (b + na)y$$

daí, ve-se que $e \mid d$, já que $\exists\ x_0, y_0 \in \mathbb{N} \cup \{0\};\ e = ax_0 + (b + na)y_0$. Já que $d \mid a$ e $d \mid b$, pela Preposição 3.5, tem-se que $d \mid (b + na)$ e como todo divisor comum de a e $b + na$ é divisor de f, assim $d = f$. E assim, $(a, b) = (a, b + na)$ □

Exemplo 3.9. Pelo Teorema 3.6, tem-se que $(3, 18) = (3, 18 - 4 \cdot 3) = (3, 18 + 2 \cdot 3)$

Teorema 3.7. *Se* $a \mid bc$ *e* $(a, b) = 1$, *então* $a \mid c$.

Demonstração. Como $(a, b) = 1$, pelo Teorema 3.5, tem-se que

$$\exists\ x, y \in \mathbb{N} \cup \{0\};\ ax + by = 1 \tag{18}$$

Como $a \mid bc$, tem-se que $bc = a \cdot k$. Se multiplicar-se (18) por c, ter-se-a

$$c = (ac)x + (bc)y = a(cx) + a(ey) = a(cx + ey)$$

E assim, conclui-se que $a \mid c$. □

Exemplo 3.10. Se $4 \mid (27 \cdot 20)$, isso implica pelo Teorema 3.7, que $4 \mid 20$, pois $(4, 27) = 1$.

Teorema 3.8. *Se $a, b \in \mathbb{N} \cup \{0\}$ e $b = qa + r$, onde $q, r \in \mathbb{N} \cup \{0\}$, entaõs $(a, b) = (a, r)$.*

Demonstração. Sabe-se que $b = aq + r$ e pela Proposição 3.5, tem-se que todo divisor de a e r é divisor de b. Ao mesmo tempo, pode-se escrever a mesma relação da seguinte forma $r = b - qa$ e pela Proposição 3.5, tem-se que todo divisor de a e b é um divisor de r. Assim, o conjuntos d e divisores comuns a a e b é idêntico ao conjunto de divisores comuns a a e r. Portanto, $(a, b) = (a, r)$ □

Observação 3.18. Esse resultado é de grande importância na demonstração do Algoritmo de Euclides, que será o próximo Teorema a ser apresentado.

Exemplo 3.11. Qual o $(158, 48)$?

$Sol.$ Utilizando o Teorema 3.4, tem-se

$$158 = 3 \cdot 48 + 14$$

$$48 = 3 \cdot 14 + 6$$

$$14 = 2 \cdot 6 + 2$$

$$6 = 3 \cdot 2 + 0$$

Assim, o $(6, 2) = 2$ e pelo Teorema 3.8, $(6, 2) = (14, 6) = (48, 14) = (158, 48) = 2$.

Teorema 3.9. *(Algoritmo de Euclides) Sejam $a, b \in \mathbb{N} \cup \{0\}$ com $a \neq 0$. Se o algoritmo da divisão for aplicado sucessivamente para se obter*

$$b = aq_1 + r_1, \;\; 0 \leq r_1 < b$$

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

$$r_1 = r_2q_3 + r_3, \;\; 0 \leq r_2 < r_3$$

$$\ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots$$

$$r_{n-2} = r_{n-1}q_n + r_n, \;\; 0 \leq r_n < r_{n-1}$$

$$r_{n-1} = r_nq_{n+1}$$

até algum r_n dividir r_{n-1}. Assim $(a, b) = r_n$, ou seja, o (a, b) é o último resto não-nulo no processo de divisão anterior.

Demonstração. Esse teorema é muito importante e o ponto de partida para uma demonstração é observar que a aplicação sucessiva do algoritmo da divisão é finita e que cada novo resto é sempre menor que o anterior, ou seja, $r_1 > r_2 > r_3 > ... > r_n$. Como esta-se trabalhando com $\mathbb{N} \cup 0$, após um número finito de aplicações do algoritmo da divisão tem-se resto 0. Analisando as igualdades do Teorema 3.9 de baixo para cima e utilizando o Teorema 3.8, tem-se

$$(a, b) = (a, r_1) = (r_1, r_2) = ... = (r_n, r_{n-1}) = r_n$$

□

3.6 Números Primos

O conceito de número primo é um dos conceitos mais importantes da matemática. Eles desemoenham um papel fundamental e muito signifcativo na matemática e em muitos problemas associados a eles.

Definição 3.6. Um número $p \in \mathbb{N}$ maior que 1 e que só é divisível por 1 e por si próprio é chamado de número primo.

Proposição 3.11. *Dados dois números primos p, q e $a \in \mathbb{N} \cup \{0\}$ decorrem os seguintes fatos:*

1. *Se $p \mid q$, então $p = q$;*

2. *Se $p \nmid a$, então $(p, a) = 1$.*

Demonstração. [1] Para mostrar o item 1 tem-se que se $p \mid q$ isso quer dizer que $\exists\, c \in \mathbb{N}; q = p \cdot c$. Todavia, como q é primo, tem-se que pela definição 3.6 $p = 1$ ou $p = q$. Como p também é primo, obrigatóriamente $p > 1$ (Definição 3.6), logo $p = q$.

[2] Para mostra o item 2 considere que $(p, a) = d$ tem-se que $d \mid p$ e $d \mid a$. Todavia como p é primo, ou $d = 1$ ou $d = p$. Por definição $d \neq p$, pois $d \mid a$ e $p \nmid a$, logo $d = 1$. Sendo asism, $(p, a) = 1$. □

Proposição 3.12. *Sejam $a, b, p \in \mathbb{N}$, com p primo, $p \mid (a \cdot b)$, p primo, então $p \mid a$ ou $p \mid b$.*

Demonstração. Se $p \mid (a \cdot b)$ então $\exists\, c \in \mathbb{N}; ab = p \cdot c$. Assim, tem-se três casos que precisam ser analisados:

1. Se $p \mid a$ e $p \mid b$, é a opção mais óbvia e já está provado o que quer-se mostrar.

2. Se $p \nmid a$, tem-se que $(p, a) = 1$ e pelo Teorema 3.7, $p \mid b$.

3. Se $p \nmid b$, o raciocínio é análogo ao item 2, e assim, $p \mid a$.

□

Teorema 3.10. *(Teorema Fundamental da Aritmética) Todo número natural maior que* 1 *ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como um produto de números primos*

Observação 3.19. O Teorema 3.10 foi provado no Exemplo 3.2 como exemplo de uma demonstração pelo Princípio da Indução Finita (PIF).

Teorema 3.11. *Existem infinitos números primos.*

Demonstração. Suponha que exista um número finito de números primos $p_1, p_2, \ldots, p_r$. E assim, considere $n = p_1 p_2 \ldots p_r + 1$. Pelo Teorema 3.10, o número n possui um fator primo p que, portanto, deve ser um dos $p_1, p_2, \ldots, p_r$ e, consequentemente, divide o produto $p_1 p_2 \ldots p_r$. Se isso, ocorre, então $p \mid 1$, o que é um absurdo. Portanto, existem infinitos números primos. □

Lema 3.2. *Se um número natural* $n > 1$ *não é divisível por nenhum número primo* p *tal que* $p^2 \leq n$*, então ele é primo.*

Demonstração. Suponha, por absurdo, que n não seja divisível por nenhum número primo p tal que $p^2 \leq n$ e que não seja primo. Seja q o menor número primo que divide n; então $\exists\, r \in \mathbb{N}; n = q \cdot r$, com $q \leq r$ [1]. Ao multiplicar [1] por q, já que $q \in \mathbb{N}$, ter-se-a $q^2 \leq q \cdot r = n$. Logo, sabe-se que $q \mid n$, onde $q \leq n$, o que é um absurdo. Assim, seja $n \in \mathbb{N}; n$ 1 não divisível por nenhum primo p tal que $p^2 \leq n$, então n é primo. □

Observação 3.20. O Lema 3.2 também fornece um texte de primalidade, pois, para verificar se um número n é primo, basta verificar que não é divisível por nenhum primo $p \leq \sqrt{n}$.

Exemplo 3.12. Determine todos os números primos de 2 a 50.

$Sol.$ Para isso vamos utilizar o Lema 3.2, e para saberr os números primos de 2 a 50 deve-se exluir os múltiplos de 2, 3, 5 e 7, pois $p \leq \sqrt{50}$. (O próximo primo é 11, e $11^2 = 121$, o que passa do valor desejado). Assim, os números a seguir não são primos, pois:

$$M(2) = 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50;$$

$$M(3) = 9, 15, 21, 27, 33, 39, 45;$$

$$M(5) = 25, 35;$$

$$M(7) = 49.$$

Assim, os números primos entre 2 e 50 são os números $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47$.

Observação 3.21. Dados dois números $a, b \in \mathbb{N}$. Os números a e b são chamados primos entre si, quando $(a, b) = 1$.

3.7 Congruência

Nesta seção será trabalhada uma das noções mais importantes da aritmética, que foi amplamente fundamentada por Carl Friedrich Gauss, em seu livro Disquisitiones Arithmeticae de 1801. O estudo de congruência trata-se da realização de uma aritmética com os restos da divisão euclidiana por um número fixado. O trabalho desenvolvido por Gauss foi tão importante que até a notação utilizada por ele, introduzida neste momento, é utilizada até hoje. Para iniciar o processo, é importantíssimo definir o conjunto dos números inteiros e, logo após, as definições de congruência.

Definição 3.7. O conjunto dos números Inteiros, denotado por $\mathbb{Z}$, é definido por

$$\mathbb{Z} = \{a, b, \in (\mathbb{N} \cup 0); a - b\}$$

Definição 3.8. Se $a, b \in \mathbb{Z}$ dizemos que a é congruemte a b módulo m, com $m > 0$, se $m \mid (a-b)$. Denotamos isso por $a \equiv b \ (mod\ m)$. Se $m \nmid (a - b)$ dizenos que a é incongruente a b módulo m e denotamos por $a \not\equiv b \ (mod\ m)$.

Exemplo 3.13. $11 \equiv 3 \ (mod\ 2)$, pois $2 \mid (11 - 3) = 8$. Da mesma forma $17 \not\equiv 11 \ (mod\ 5)$, pois $5 \nmid (17 - 11) = 6$.

Proposição 3.13. *Se $a, b \in \mathbb{Z}$ dizemos que $a \equiv b \ (mod\ m)$ se, e somente se, existir um $k \in \mathbb{Z}; a = b + km$.*

Demonstração. Como há um se, e somente se, é necessário mostrar a ida e a volta. Assim

$\Rightarrow$) Se $a \equiv b \ (mod\ m)$, tem-se que $m \mid (a - b)$ e assim $\exists\ k \in \mathbb{Z}; a - b = mk$, e assim $a = b + mk$.

$\Leftarrow$) Se $a = b + mk$, tem-se que $a - b = mk$ e assim, $m \mid (a - b)$. Pela Definição 3.8, $a \equiv b \ (mod\ m)$.

Assim, $a \equiv b \ (mod\ m)$ se, e somente se, $k \in \mathbb{Z}; a = b + km$. □

Proposição 3.14. *Se $a, b, m, d \in \mathbb{Z}$, com $m > 0$, as seguintes sentenças são verdadeiras:*

1. $a \equiv b \ (mod\ m)$;
2. *Se* $a \equiv b \ (mod\ m)$, *então* $b \equiv a \ (mod\ m)$;
3. *Se* $a \equiv b \ (mod\ m)$ *e* $b \equiv d \ (mod\ m)$, *então* $a \equiv d \ (mod\ m)$.

Demonstração. As três proposições serão demostradas abaixo:

[1] Sabe-se que $m \mid 0$ e assim $m \mid (a - a)$. Pela Definição 3.8, $a \equiv a \ (mod\ m)$.

[2] Se $a \equiv b \ (mod\ m)$, então pela Proposição 3.13, $a = b + mk$. Assim, $b = a - mk \Longrightarrow b - a = m(-k)$. Por consequência $m \mid (b - a)$ e pela Definição 3.8, $b \equiv a \ (mod\ m)$.

[3] Se $a \equiv b \ (mod\ m)$, então $m \mid (a - b)$. Analogamente, se $b \equiv d \ (mod\ m)$, então $m \mid (b - d)$. Pela preposição 3.13, tem-se que $\exists\ k \in \mathbb{Z}; a = b + mk$ e $\exists\ l \in \mathbb{Z}; b = d + ml$. Daí,

$$a = b + mk = d + ml + mk = d + m(l + k)$$

$$a = d + m(k + l) \Longleftrightarrow a \equiv d \ (mod\ m).$$

□

Teorema 3.12. *Se $a, b, c, m \in \mathbb{Z}$ tais que $a \equiv b \ (mod\ m)$, então*

1. $a \pm c \equiv b \pm c \ (mod\ m)$
2. $ac \equiv bc \ (mod\ m)$.

Demonstração. Os dois itens serão demostradas abaixo:

[1] Como $a \equiv b \ (mod\ m)$, pela Proposição 3.13, $a = b + km$. Pode-se representar da seguinta maneira $a - b = mk$ e daí,

$$(a \pm c) - (b \pm c) = mk \Longleftrightarrow a \pm c \equiv b \pm c \ (mod\ m)$$

[2] Como $a \equiv b \ (mod\ m)$, pela Proposição 3.13, $a = b + km$. Multiplicando c em ambos os lados, teremos $ac = bc + m(kc)$ e pela Proposição 3.13, tem-se $ac \equiv bc \ (mod\ m)$. □

Teorema 3.13. *Se $a, b, c, d, m \in \mathbb{Z}$, tias que $a \equiv b \ (mod\ m)$ e $c \equiv d \ (mod\ m)$, então*

1. $a + c \equiv b + d \ (mod\ m)$;
2. $a - c \equiv b - d \ (mod\ m)$;

3. $ac \equiv bd \ (mod\, m)$.

Demonstração. Os três itens serão demosntrados abaixo:

[1] Se $a \equiv b \ (mod\, m)$, então $\exists\, k \in \mathbb{Z}; a-b = km \ (*)$. Analogamente, se $c \equiv d \ (mod\, m)$ tem-se $l \in \mathbb{Z}; c-d = lm \ (**)$. Somando $(*)$ e $(**)$, tem-se:

$$(a-b)+(c-d) = m(k+l)$$

$$(a+c)-(b+d) = m(k+l)$$

$$(a+c) = (b+d)+m(k+l) \iff a+c \equiv b+d \ (mod\, m).$$

[2] Se $a \equiv b \ (mod\, m)$, então $\exists\, k \in \mathbb{Z}; a-b = km \ (*)$. Analogamente, se $c \equiv d \ (mod\, m)$ tem-se $l \in \mathbb{Z}; c-d = lm \ (**)$. Subtraindo $(*)$ e $(**)$, tem-se:

$$(a-b)-(c-d) = m(k-l)$$

$$(a-c)-(b-d) = m(k-l)$$

$$(a-c) = (b-d)+m(k-l) \iff a-c \equiv b-d \ (mod\, m).$$

[3] Se $a \equiv b \ (mod\, m)$, então $\exists\, k \in \mathbb{Z}; a-b = km \ (*)$. Analogamente, se $c \equiv d \ (mod\, m)$ tem-se $l \in \mathbb{Z}; c-d = lm \ (**)$. Multiplicando $(*)$ por c e $(**)$ por b,

$$ac - bc = m(kc) \ [*]$$

$$bc - bd = m(lb) \ [**]$$

Somando $[*]$ e $[**]$, tem-se

$$ac - bd = m(kc - lb)$$

$$ac = bd + m(kc - lb) \iff ac \equiv bd \ (mod\, m)$$

□

Teorema 3.14. *Se* $a, b, c, m \in \mathbb{Z}$ *e* $ac = bc \ (mod\, m)$*, então* $a \equiv b \ (mod\, \frac{m}{d})$ *onde* $d = (c, m)$.

Demonstração. Sabe-se que $ac = bc \ (mod\, m)$ e dái $\exists\, k \in \mathbb{Z}; ac - bc = mk$. Daí $c(a-b) = mk$ e se dividirmos por $d = (c, m)$, teremos $\frac{c}{d} \cdot (a-b) = k \cdot (\frac{m}{d})$. Portanto, $\frac{m}{d} \mid \left[\frac{c}{d} \cdot (a-b)\right]$, pelo Corolário 3.2 o $\left(\frac{m}{d}, \frac{c}{d}\right) = 1$ e pelo Teorema 3.7 $\frac{m}{d} \mid (a-b)$. E por fim, $a - b = \frac{m}{d} \cdot l$ e assim $a \equiv b \ (mod\, \frac{m}{d})$. □

Proposição 3.15. *Se* $a, b, k, m \in \mathbb{Z}$*, com* $k > 0$ *e* $a \equiv b \ (mod\, m)$*, então* $a^k \equiv b^k \ (mod\, m)$.

Demonstração. Para mostrar essa identidade, é importante lembrar que

$$a^k - b^k = (a-b) \cdot (a^{k-1} + a^{k-2} \cdot b + \cdots + a \cdot b^{k-2} + b^{k-1})[*]$$

Como $a \equiv b \ (mod\ m)$ tem-se que $\exists\ l \in \mathbb{Z}; a - b = ml[**]$, assim substituindo $[**]$ em $[*]$,

$$a^k - b^k = m \cdot (la^{k-1} + la^{k-2} \cdot b + \cdots + la \cdot b^{k-2} + lb^{k-1})$$

Pela Proposição 3.13, assim

$$a^k = b^k \ (mod\ m)$$

□

Teorema 3.15. *(Pequeno Teorema de Fermat) Seja p primo. Se $p \nmid a$ então $a^{p-1} \equiv 1 \ (mod\ p)$.*

Demonstração. Considere os números $a, 2a, 3a, \ldots, (p-1)a$. Como $(p, a) = 1$ nenhum dos núemros $ka, 1 \leq i \leq (p-1)$ é divisível por p. Isso quer dizer que quaisquer dois deles são incongruentes módulo p. Com isso, cada um dos númeors considerados é congruente a exatamente um dentre os elementos $1, 2, 3, \ldots, (p-1)$. Multiplicando as congruências geradas uma a uma ter-se-a:

$$a \cdot (2a) \cdot (3a) \ldots (p-1) \cdot a \equiv 1 \cdot 2 \cdot 3 \ldots (p-1) \ (mod\ p)$$

$$a^{p-1} \cdot (p-1)! \equiv (p-1)! \ (mod\ p)$$

E como o $(p, (p-1)!) = 1$, pode-se cancelar o fator $(p-1)!$. Asim,

$$a^{p-1} \equiv 1 \ (mod\ p)$$

□

3.8 Equações Diofantinas e o Método de Diofanto

Definição 3.9. Uma Equação Diofantina é qualquer equação com uma ou mais incógnitas que assumem apenas valores inteiros.

Exemplo 3.14. Alguns Exemplos de equações diofantinas

1. (Equações Diofantinas Lineares) $ax + by = c$
2. (Ternos Pitagóricos) $x^2 + y^2 = z^2$

3. (Último Teorema de Fermat) $x^n + y^n = z^n$

Observação 3.22. O termo Diofantina se refere ao matemático grego do século III, Diofanto de Alexandria. Ele estudou tais equações e foi um dos primeiros a introduzir o uso de símbolos matemáticos na álgebra.

Neste trabalho será discutida a mais estudada das Equações Diofantinas Quadráticas, os Ternos Pitagóricos associados à construção de Triângulos Pitagóricos. Para iniciar as discussões, é importante salientar um problema respondido por Diofanto de Alexandria, o problema oito do livro II de Aritmética. O problema consiste em decompor um quadrado em uma soma de dois quadrados.

Suponha que quer-se decompor o número n^2 em dois quadrados. Considere que x^2 seja o primeiro quadrado e que seja y^2 o seguundo quadrado. Assim, $y^2 = n^2 - x^2[*]$. Diofanto propôs que o número $y^2 = (mx - \sqrt{n^2})^2$ com $m \in \mathbb{Q}$, com $m > 1$.

Observação 3.23. Dado $q \in \mathbb{Z}; q \neq 1$ e $q \neq -1$, o inverso de q não existe em $\mathbb{Z}$ $\left(\frac{1}{q} \notin \mathbb{Z}\right)$. Assim, chama-se $\mathbb{Q}$ o conjunto do númeors racionais tal que

$$\mathbb{Q} = \left\{ \frac{a}{b}; a, b \in \mathbb{Z}, \text{ com } b \neq 0 \right\}.$$

Assim, continuando a ideia de Diofanto,

$$n^2 - x^2 = (mx - n)^2$$

$$n^2 - x^2 = m^2x^2 - 2mnx + n^2$$

$$x^2(m^2 + 1) - 2mnx = 0 \Longrightarrow x\left[x(m^2 + 1) - 2mn\right] = 0$$

Como $x > 0$, então

$$x = \frac{2mn}{m^2 + 1}$$

E daí, substituindo em $[*]$

$$y^2 = n^2 - \left(\frac{8m}{m^2 + 1}\right)^2 \Longrightarrow y^2 = \frac{n^2(m^2 - 1)^2}{(m^2 + 1)^2}$$

Como $y > 0$ e $m > 1$, tem-se

$$y = \frac{n(m^2 - 1)}{m^2 + 1}$$

Com isso, sempre tem-se um terno pitagórica tal que $\left(\frac{2mn}{m^2+1}, \frac{n(m^2-1)}{(m^2+1)}, n\right)$/, com $m \in \mathbb{Q}$, com $m > 1$ e $n \in \mathbb{N}$. E assim:

$$n^2 = \left(\frac{2mn}{m^2 + 1}\right)^2 + \left(\frac{n(m^2 - 1)}{m^2 + 1}\right) \tag{19}$$

Observação 3.24. Se $m \in \mathbb{Z}$, assim pode-se multiplicar (19) por $\frac{(m+1)^2}{n^2}$ e assim,

$$n^2 \cdot \frac{(m+1)^2}{n^2} = \left(\frac{2mn}{m^2+1}\right)^2 \cdot \frac{(m+1)^2}{n^2} + \left(\frac{n(m^2-1)}{m^2+1}\right) \cdot \frac{(m+1)^2}{n^2}$$

$$(m+1)^2 = (2m)^2 + (m^2-1)^2 \tag{20}$$

E assim, ter-se-a o terno pitagórico $(2m, m^2-1, m^2+1)$..

Observação 3.25. No caso que $m \in \mathbb{Q}$, com $m = \frac{p}{q}$, com $q \neq 0$. Assim, substuindo em (20),

$$\left(\left(\frac{p}{q}\right)^2 + 1\right)^2 = \left(2 \cdot \frac{p}{q}\right)^2 + \left(\left(\frac{p}{q}\right)^2 - 1\right)^2$$

$$\left(\frac{p^2+q^2}{q^2}\right)^2 = \left(\frac{2 \cdot p}{q}\right)^2 + \left(\frac{p^2-q^2}{q^2}\right)^2$$

Multiplicando por q^4, ter-se-a

$$(p^2+q^2) = (2pq)^2 + (p^2-q^2)^2 \tag{21}$$

Assim, tem-se o terno pitagórico $(2pq, p^2-q^2, p^2+q^2)$, com $p, q \in \mathbb{Z}$ e $p > q$.

4 CONSTRUÇÃO GEOMÉTRICA DO PROBLEMA

Após construirmos a base aritmética do problema, é deveras importante construir a base geométrica. Aritmeticamente, analisaremos as triplas pitagóricas, mas geometricamente associaremos as triplas a triângulos pitagóricos. Sendo assim, neste capítulo será necessário definir o conceito de triângulo e suas consequências. Essa seção é fundamentada pelos autores Dolce (2013) e Doria (2007).

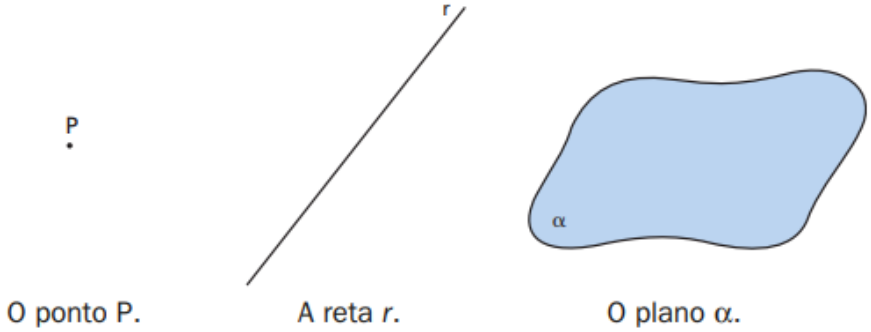
Assim, vamos a alguns conceitos preliminares. Existem dois conceitos que são basicamente intrínsecos ao estudo inicial da geometria: a ideia de ponto e reta. Esses conceitos serão trabalhados como noções primitivas e não serão definidos.

Definição 4.1. O plano é visto como o conjunto onde os pontos são seus elementos e as retas, seus subconjuntos.

Observação 4.1. A notação de ponto, reta e plano é feita da seguinte maneira

1. Ponto - letras latinas maiúsculas - $A, B, C, D, \ldots$
2. Reta - letras latinas minúsculas - $a, b, c, d, \ldots$
3. Plano - letras gregas minúsculas - $\alpha, \beta, \gamma, \delta, \ldots$

Figura 4 – Ponto, reta e plano



Fonte: Dolce (2013)

Definição 4.2. Dados dois pontos distintos, a reunião do conjunto desses dois pontos com o conjunto dos pontos que estão entre eles é um segmento de reta.

Definição 4.3. Dado dois pontos distintos A e B, a reunião do segmento de reta $\overline{AB}$ com o conjunto dos pontos X tais que B está entre A e X é a semirreta AB (INDICADA POR $\overrightarrow{AB}$).

Definição 4.4. Considere dois pontos A e B, assim

1. chamamos A e B de colineares se ambos estão contidos em uma mesma reta;

2. chamamos A e B de não colineares se ambos não esão contidos na mesma reta.

Definição 4.5. Duas retas são paralelas $(//)$ se, e somente se, são coincidentes (iguais) ou são coplanares (estão no mesmo plano) e não têm nenhum ponto comum.

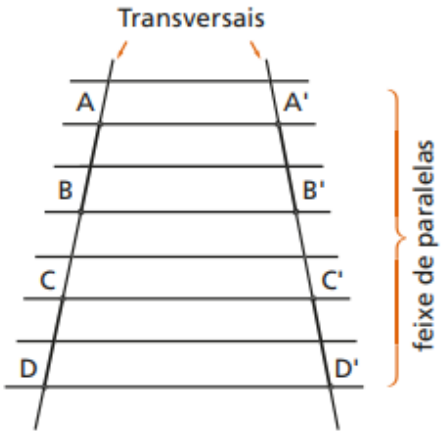
Definição 4.6. Feixe de retas paralelas é um conjunto de retas coplanares (mesmo plano) paralelas entre si.

Definição 4.7. Transversal do feixe de retas paralelas é uma reta do plano do feixe que concorre com todas as retas do feixe.

Definição 4.8. Pontos correspondentes de duas transversais são pontos destas transversais que estão numa mesma reta do feixe.

Definição 4.9. Segmentos correspondentes de duas transversais são segmentos cujas extremidades são os respectivos pontos correspondentes.

Figura 5 – Feixe de Paralelas Cortada por duas Trasnversais



Fonte: Dolce (2013)

Observação 4.2. Olhando a Figura 5 temos que

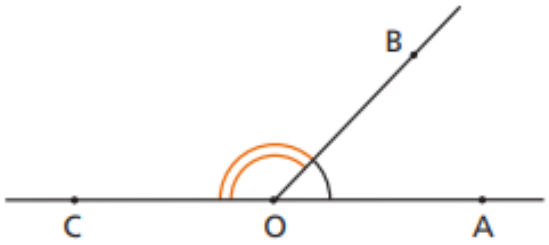
1. A e A', B e B', C e C', D e D' são pontos correspondentes;

2. $\overline{AB}$ e $\overline{A'B'}$, $\overline{CD}$ e $\overline{C'D'}$ são segmentos correspondentes.

Definição 4.10. Chama-se ângulo à reunião de duas semirretas de mesma origem, não contidas numa mesma reta (não colineares).

Definição 4.11. Considere o ângulo $A\widehat{O}B$, a semirreta $\overrightarrow{OC}$ oposta a semirreta $\overrightarrow{OA}$ e a semirreta $\overrightarrow{OB}$ determinam um ângulo $B\widehat{O}C$ que se chama ângulo suplementar adjacente ou suplemento adjacente de $A\widehat{O}B$.

Figura 6 – Suplemento Adjacente

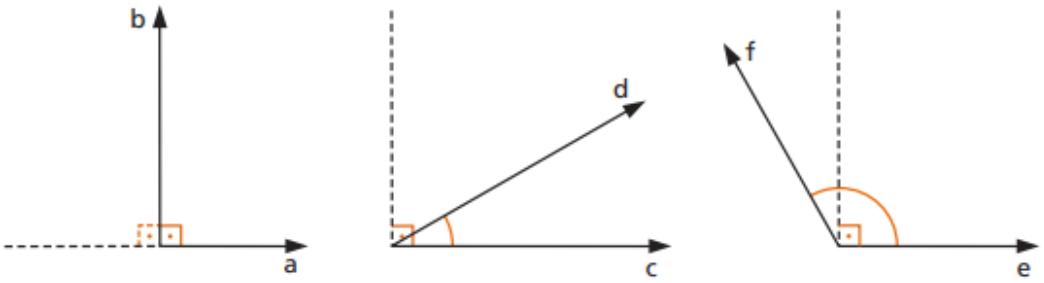


Fonte: Dolce (2013)

Definição 4.12. Podemos classificar os ângulos da seguinte maneira:

1. Ângulo Reto é todo ângulo congruente a seu suplementar adjacente (Possui $90°$);
2. Ângulo agudo é um ângulo menor que o ângulo reto;
3. Ângulo obtuso é um ângulo maior que o ângulo reto.

Figura 7 – Ângulo Reto, Agudo e Obtuso



Fonte: Dolce (2013)

Observação 4.3. Ângulos com a mesma medida são chamados de congruentes.

Observação 4.4. Pode-se estender o conceito de Ângulo para se ter o ângulo nulo, cujos lados são coincidentes, ou o ângulo raso, cujos lados são semirretas opostas. Então, podemos dizer que a medida α de um ângulo é tal que

$$0° \leq \alpha \leq 180°$$

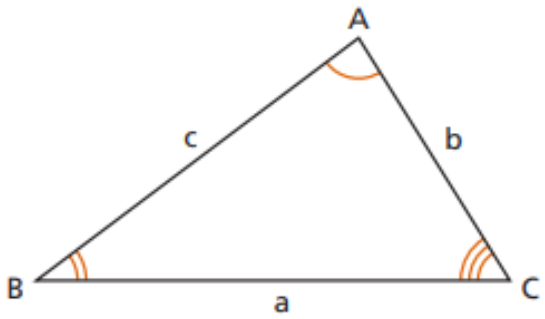
Definição 4.13. Dados dois ângulos $\widehat{A}$ e $\widehat{B}$, tem-se que:

1. $\widehat{A}$ e $\widehat{B}$ são ângulos complementares, quando $\widehat{A} + \widehat{B} = 90°$;
2. $\widehat{A}$ e $\widehat{B}$ são ângulos suplementares, quando $\widehat{A} + \widehat{B} = 180°$

4.1 Triângulos

Definição 4.14. Dados três pontos, A, B e C, não colineares, à reunião dos segmentos $\overline{AB}$, $\overline{AC}$ e $\overline{BC}$ chama-se triângulo ABC.

Figura 8 – Triângulo Qualquer



Fonte: Dolce (2013)

Observação 4.5. Em um triâmgulo temos alguns elementos que são notáveis. Assim,

1. Vértice: São os pontos A, B e C;
2. Lados: Os segmentos $\overline{AB}$ (de medida c), $\overline{AC}$ (de medida b) e $\overline{BC}$ (de medida a);
3. Ângulos: Os ângulos $B\widehat{A}C$ ou $\widehat{A}$, $A\widehat{B}C$ ou $\widehat{B}$ e $A\widehat{C}B$ ou $\widehat{C}$ (esses são os ângulos internos).

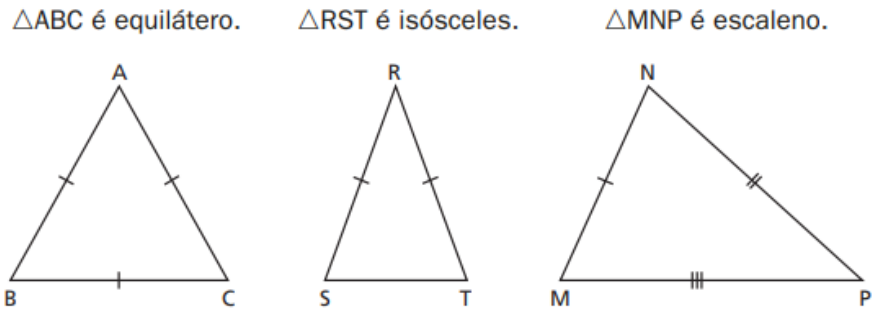
Observação 4.6. Os lados $\overline{AB}$, $\overline{AC}$ e $\overline{BC}$ e os ângulos $\widehat{C}$, $\widehat{B}$, $\widehat{A}$ são, respectivamente, opostos.

Um triângulo pode ser classificado quanto aos seus lados e quanto aos seus ângulos. E assim, temos as primeiras definições que são fundamentais ao nosso trabalho. A definição quanto aos ângulos é deveras importante para o presente trabalho.

Definição 4.15. Quanto aos lados, os triângulos se classificam em:

1. Equilátero, quando possui três lados dois a dois congruentes;
2. Isósceles, quando possui dois lados congruentes entre si (o terceiro lado é chamado de base do triângulo isósceles e o ângulo oposoto à base é chamado de ângulo do vértice);
3. Escaleno, aquele que em quaisquer dois de seus lados tem medidas diferentes.

Figura 9 – Triângulo Equilátero, Isósceles e Escaleno

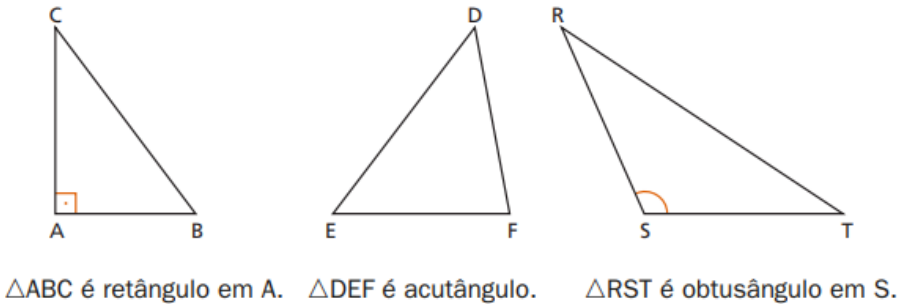


Fonte: Dolce (2013)

Definição 4.16. Quanto aos ângulos, os triângulos se classificam em:

1. Retângulo, quando possui um ângulo reto, $90°$. Neste caso, o lado oposto ao ângulo reto é chamado $hipotenusa$ e os outros dois lados de $catetos$.
2. Acutângulo, quando possui os três ângulos agudos;
3. Obtusângulo, quando possui um ângulo obtuso.

Figura 10 – Triângulo Retângulo, Acutângulo e Obtusângulo

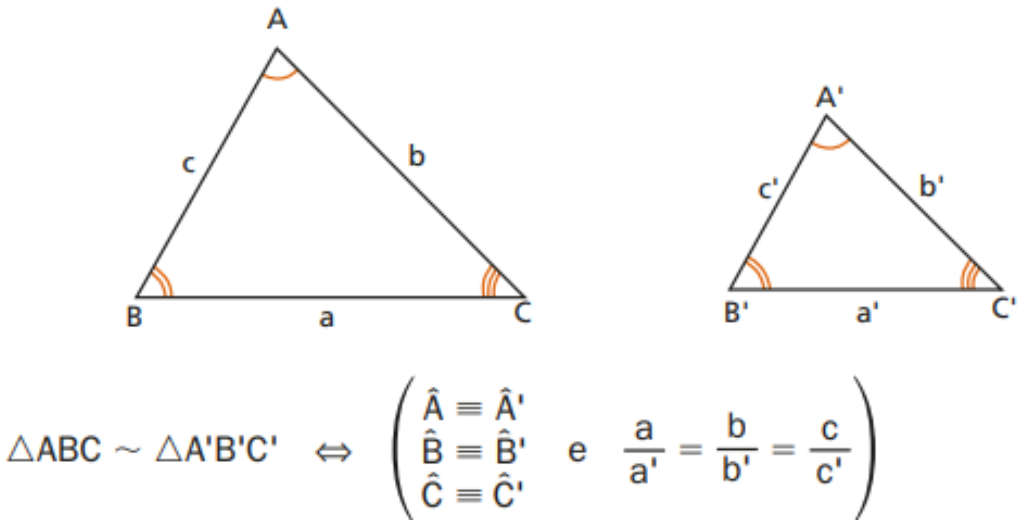


Fonte: Dolce (2013)

Observação 4.7. Temos também um triângulo equiângulo, um caso particular do triângulo acutângulo, que é aquele que possui os seus ângulos dois a dois congruentes.

Definição 4.17. Dois triângulos são ditos semelhantes se, e somente se, possuem os três ângulos ordenadamente congruentes e os lados homólogos (mesmo lugar) porporcionais.

Figura 11 – Semelhança de Triângulos



Fonte: Dolce (2013)

Observação 4.8. O símbolo $\sim$ significa semelhante. Logo, $\triangle ABC \sim \triangle A'B'C'$ siginifica que o $\triangle ABC$ é semelhante ao $\triangle A'B'C'$.

Observação 4.9. Chamamos de razão de semelhança um certo $k \in \mathbb{N}$, tal que

$$\frac{a}{a'} = \frac{b}{b'} = \frac{c}{c'} = k \tag{22}$$

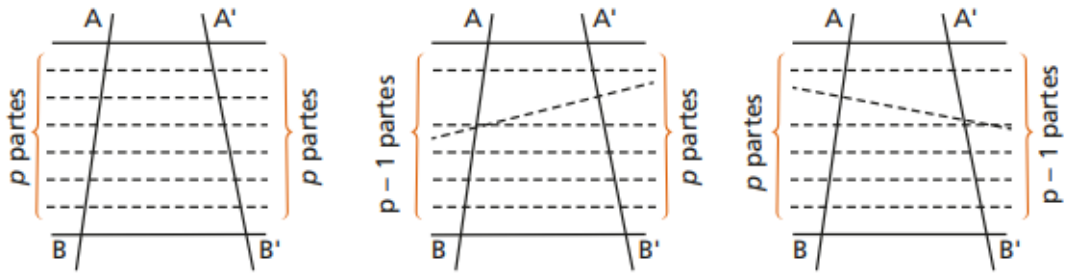
Se $k = 1$, temos que os triângulos são congruentes.

Proposição 4.1. *Se duas retas são transversais de um feixe de retas paralelas distintas e um segmento de uma delas é dividido em p partes congruentes entre si e pelos pontos de divisão são conduzidas retas do feixe, então o segmento correspondente da outra transversal:*

1. *também é dividido em p partes;*
2. *e essas partes também são congruentes entre si.*

Demonstração. [1]. Considere a Figura 5, $\overline{AB}$ e $\overline{A'B'}$ são segmentos correspondentes e por hipótese, $\overline{AB}$ é dividido em p partes por retas do feixe. Se $\overline{A'B'}$ ficasse dividido em menos partes (ou até mais partes), pelo menos duas retas do feixe encontra-se-iam em pontos de $\overline{AB}$ (ou de $\overline{A'B'}$), o que é absurdo, pois as retas do feixe são paralelas.

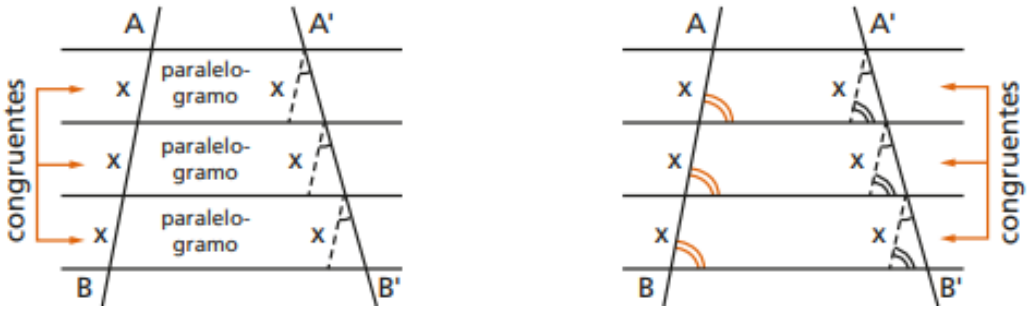
Figura 12 – Proposição 4.1 - Item 1



Fonte: Dolce (2013)

[2]. $\overline{AB}$ é dividio em partes congruentes a x. Pelos pontos de divisão de $\overline{A'B'}$, conduzindo paralelas a $\overline{AB}$, obtemos um triângulo para cada divisão. Todos os triângulos são congruentes pois possuem dois ângulos congrunetes e um lado entre os ângulos que é congruente. Assim, $\overline{A'B'}$ é dividido em partes congruentes pelos pontos de divisão.

Figura 13 – Proposição 4.1 - Item 2



Fonte: Dolce (2013)

□

Teorema 4.1. *(Teorema de Tales) Se duas retas são transversais de um feixe de retas paralelas, então a razão entre dois segmentos quaisquer de uma delas é igual à razão entre os respectivos segmentos correspondentes da outra.*

Demonstração. Temos como hipótese que $\overline{AB}$ e $\overline{CD}$ são dois segmentos de uma transversal, e $\overline{A'B'}$ e $\overline{C'D'}$ são os respectivos correspondentes da outra e queremos mostrar que $\frac{\overline{AB}}{\overline{CD}} = \frac{\overline{A'B'}}{\overline{C'D'}}$. Pela proposição 4.1, temos que se $\overline{AB}$ está dividio em p partes, $\overline{A'B'}$ também está dividio em p partes. Se $\overline{CD}$ for dividida em q parte, $\overline{C'D'}$ também será. (Conferir a Figura 14).

Existe um segmento x que é submúltiplo de $\overline{AB}$ e de $\overline{CD}$. Asssim, $\overline{AB} = p \cdot x$ e

$\overline{CD} = q \cdot x$. Se dividirmos $\overline{AB}$ por $\overline{CD}$,

$$\frac{\overline{AB}}{\overline{CD}} = \frac{p \cdot x}{q \cdot x} = \frac{p}{q} \tag{23}$$

Conduzindo retas do feixe pelos pontos de divisão de $\overline{AB}$ e $\overline{CD}$ (vide Figura 14) e aplicando a Proposição 4.1, $\overline{A'B'} = p \cdot x$ e $\overline{C'D'} = q \cdot x$. Se dividirmos $\overline{A'B'}$ por $\overline{C'D'}$,

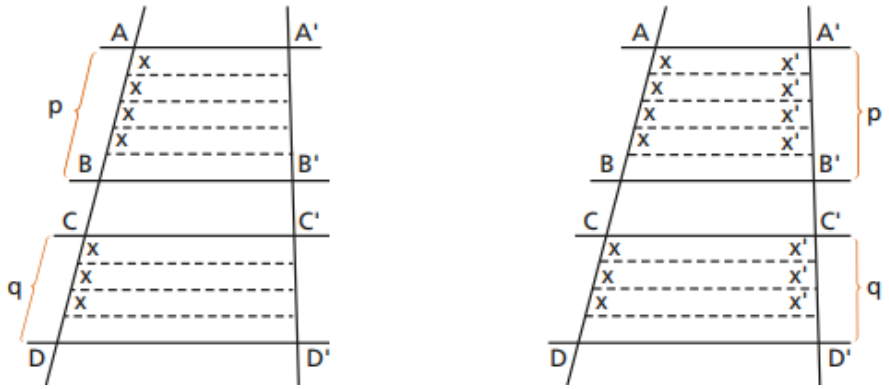
$$\frac{\overline{A'B'}}{\overline{C'D'}} = \frac{p \cdot x}{q \cdot x} = \frac{p}{q} \tag{24}$$

Assim, comparando (23) e (24), temos que

$$\frac{\overline{AB}}{\overline{CD}} = \frac{\overline{A'B'}}{\overline{C'D'}}$$

E sendo assim, provamos que se duas retas são trasnversias de uma feixe de retas paralelas, então a razão entre dois segmentos quaisquer de uma delas é igual à razão entre os respectivos segomentos correspondentes da outra. □

Figura 14 – Teorema de Tales



Fonte: Dolce (2013)

Teorema 4.2. *Se uma reta é paralela a um dos lados de um triângulo e intercepta os outros dois em pontos distintos, então o triângulo que ela determina é semelhante ao primeiro.*

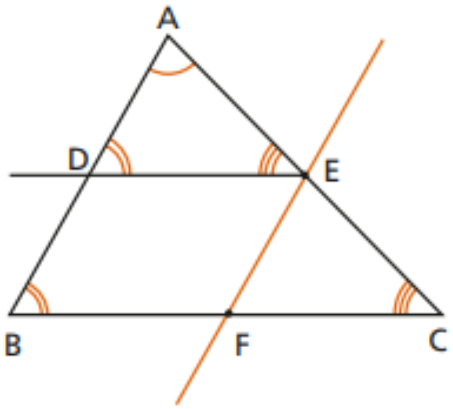
Demonstração. Nosso teorema diz que daodo $\triangle ABC$ se $\overleftrightarrow{DE}//\overleftrightarrow{AB} \Longrightarrow \triangle ADE \sim \triangle ABC$. Pel definição 3.12, é preicos mostrar que $\triangle ADE$ e $\triangle ABC$ possuem ângulos ordenadamente congruentes e lados homólogos proporcionais.

[1] Para os ângulos congruentes, perceba que se $\overleftrightarrow{DE}//\overleftrightarrow{AB}$, então $\widehat{D} \equiv \widehat{B}$ e $\widehat{E} \equiv \widehat{C}$ e como $\widehat{A}$ é comum aos dois, os ângulos dos $\triangle ADE$ e $\triangle ABC$ são ordenadamente congruentes.

[2] Para os lados proporcionais, temos pelo Teorema de Tales que

$$\frac{AD}{AB} = \frac{AE}{AC} \tag{25}$$

Figura 15 – Teorema 4.2



Fonte: Dolce (2013)

Por E contruimos $\overleftrightarrow{EF}$ paralela a $\overleftrightarrow{AB}$, com $F \in \overline{BC}$, conferir Figura 18. Com isso gerou-se o paralelogramo $BDEF$ e pela definição de paralelogramo, temos que lados opostos possuem o mesmo valor.

Logo $\overline{DE} \equiv \overline{BF}$ $[*]$ e $\overline{DB} \equiv \overline{EF}$. Além diss, novamente pelo Teorema de Tales, tem-se que:

$$\frac{AE}{AC} = \frac{BF}{BC} \tag{26}$$

Substituindo $[*]$ em (24) , temos que

$$\frac{AE}{AC} = \frac{DE}{BC} \tag{27}$$

por (25) e (27), temos que:

$$\frac{AD}{AB} = \frac{AE}{AC} = \frac{DE}{BC} \tag{28}$$

Portanto, por $[1]$ e $[2]$, $\triangle ADE \sim \triangle ABC$. □

Observação 4.10. Um quadrilátero plano convexo é um paralelogramo se, e somente se, possui os lados opostos paralelos. Todo paralelogramo possui lados opostos congruentes e ângulos oposotos congruentes.

Proposição 4.2. *Dados dois triângulos, $\triangle ABC$ e $\triangle A'B'C'$, eles serão semelhantes se se encaixarem em um dos três casos abaixo*

1. *Se dois triângulos possuem dois ângulos ordenadamente congruentes, então eles são semelhantes;*

2. *Se dois lados de um triângulo são proporcionais aos homólogos de outro triângulo e os ângulos compreendidos são congruentes, então os triângulos são semelhantes;*

3. Se dois triângulos tên os lados homólogos proporcionais, então eles são semelhantes.

Demonstração. Vamos mostrar os três casos de semelhança.

[1]. O item 1 é também conhecido como caso AA (ângulo-ângulo) e temos como hipótese que se dois triângulos, $\triangle ABC$ e $\triangle A'B'C'$, possuem dois ângulos congruentes, $\widehat{A} \equiv \widehat{A'}$ e $\widehat{B} \equiv \widehat{B'}$, então $\triangle ABC \sim \triangle A'B'C'$. Assim, suponha que os triângulos não são congruentes e que $\overline{AB} > \overline{A'B'}$ e seja D um ponto de $\overline{AB}$ tal que $\overline{AD} \equiv \overline{A'B'}$ e o $\triangle ADE$ com $\widehat{D} \equiv \widehat{B}$ e E no lado $\overline{AC}$.

Como $\widehat{A} \equiv \widehat{A'}$, $\overline{AD} \equiv \overline{A'B'}$ e $\widehat{D} \equiv \widehat{B'}$, pelo caso de congruência ALA (ângulo-lado-ângulo) $\triangle ADE \equiv \triangle A'B'C'$ $(*)$. Pelo Teorema 4.2, temos que como $\overleftrightarrow{DE} \,//\, \overleftrightarrow{BC}$ então $\triangle ABC \sim \triangle ADE$ $(**)$. Portanto, por $(*)$ e $(**)$, concluimos que $\triangle ABC \sim \triangle A'B'C'$.

[2]. O item 2 é também conhecido como caso LAL (lado - ângulo - lado) e temos como hiótese que sedois lados dos triÂngulos $\triangle ABC$ e $\triangle A'B'C'$ possuem lados proporcionais, e o ângulo entre os lados for congruente então os triângulos são semelhantes. Usando o mesmo raciocínio do item 1, suponha que os triângulos não são congruentes e que $\overline{AB} > \overline{A'B'}$ e seja D um ponto de $\overline{AB}$ tal que $\overline{AD} \equiv \overline{A'B'}$ e o $\triangle ADE$ com $\overline{AD} \equiv \overline{A'B'}$, $\overline{AE} \equiv \overline{A'C'}$ e E no lado $\overline{AC}$.

Como $\widehat{A} \equiv \widehat{A'}$, $\overline{AD} \equiv \overline{A'B'}$ e $\overline{AE} \equiv \overline{A'C'}$, pelo caso de congruência LAL (lado - ângulo - lado) $\triangle ADE \equiv \triangle A'B'C'$ $(@)$. Pelo Teorema 4.2, temos que como $\overleftrightarrow{DE} \,//\, \overleftrightarrow{BC}$ então $\triangle ABC \sim \triangle ADE$ $(@@)$. Portanto, por $(@)$ e $(@@)$, concluimos que $\triangle ABC \sim \triangle A'B'C'$.

[3]. O item 3 é também conhecido como caso LLL (lado - lado - lado) e temos como hiótese que se dois triângulos $\triangle ABC$ e $\triangle A'B'C'$ têm os lados homólogos proporcionais, entãos eles são semelhantes. Usando o mesmo racicínio dos itens 1 e 2, suponha que os triângulos não são congruentes e que $\overline{AB} > \overline{A'B'}$ e seja D um ponto de $\overline{AB}$ tal que $\overline{AD} \equiv \overline{A'B'}$ e o $\triangle ADE$ com $\overline{AD} \equiv \overline{A'B'}$, $\overline{AE} \equiv \overline{A'C'}$, $\overline{DE} \equiv \overline{B'C'}$ e E no lado $\overline{AC}$.

Como $\overline{AD} \equiv \overline{A'B'}$, $\overline{AE} \equiv \overline{A'C'}$ e $\overline{DE} \equiv \overline{B'C'}$, pelo caso de congruência LlL (lado - lado - lado) $\triangle ADE \equiv \triangle A'B'C'$ $(\star)$. Pelo Teorema 4.2, temos que como $\overleftrightarrow{DE} \,//\, \overleftrightarrow{BC}$ então $\triangle ABC \sim \triangle ADE$ $(\star\star)$. Portanto, por $(\star)$ e $(\star\star)$, concluimos que $\triangle ABC \sim \triangle A'B'C'$.

□

Observação 4.11. Nos três itens acima foram utilizados casos de congruência de triêngulos. O caso LAL é tomado como um postulado e diz que se dois triângulos tem ordenadamente congruentes dois lados e o ângulo compreendido, então les são congruentes. Os dois casos sõa proposições e dizem que

1. ALA - Se dois triângulos tem ordenadamente congruentes um lado e os dois ângulos adjacentes, então esses triÂngulos são congruentes;

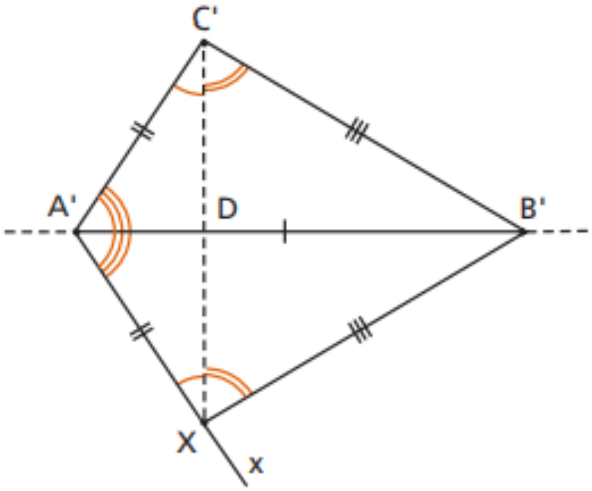
2. LLL - Se dois triângulos têm ordenadamente congruentes os três lados, então esses triângulos são congruentes.

Demonstração. [1]. Considere dois triângulos, $\triangle ABC$ E $\triangle A'B'C'$. Por hipótese temos que um lado e os ângulos adjacentes a ele são congruentes. Assim, considere $\overline{BC} \equiv \overline{B'C'}$, $\widehat{B} \equiv \widehat{B'}$ e $\widehat{C} \equiv \widehat{C'}$, e vamos mostrar que $\overline{BA} \equiv \overline{B'A'}$. Dado um segmento $\overline{BA}$ e uma semirreta de origem em B', existe sobre esta semirreta um único ponto A' tal que $\overline{B'A'}$ seja congruente a $\overline{BA}$.

Assim, na semirreta $\overrightarrow{A'B'}$ temos um ponto X, tal que $\overline{B'X} \equiv \overline{BA}$ e pelo caso LAL, $\triangle ABC \equiv \triangle XB'C'$ e isso nos garante que $B\widehat{C}A \equiv B'\widehat{C'}X$. Por definição $B\widehat{C}A \equiv B'\widehat{C'}A'$ e assim $\overleftrightarrow{B'A'}$ e $\overleftrightarrow{C'X}$ se interceptam em um único ponto $X = A'$. Com isso, mostramos que $\overline{BA} \equiv \overline{B'A'}$ e pelo caso LAL, $\triangle ABC \equiv \triangle A'B'C'$.

[2]. Considere dois triângulos, $\triangle ABC$ E $\triangle A'B'C'$. Por hipótese temos que se os três lados são ordenadamente congruntes então os triângulos são congruentes. Com um raciocínio bem semelhante ao item anterior, pelo transporte de sgmento e de ângulo, temos um ponto X tal que $X\widehat{A'}B' \equiv C\widehat{A}B$ e $\overline{A'X} \equiv \overline{AC} \equiv \overline{A'C'}$. Seja D o ponto de interscção entre $\overline{C'X}$ com a reta $\overleftrightarrow{A'B'}$.

Figura 16 – Caso LLL



Fonte: Dolce (2013)

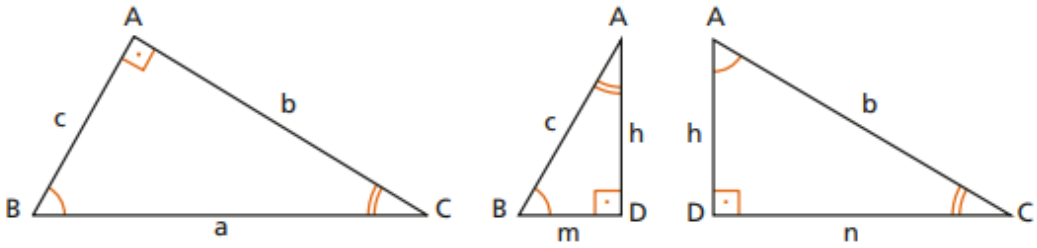
Como $X\widehat{A'}B' \equiv C\widehat{A}B$, $\overline{AB} \equiv \overline{A'B'}$ e $\overline{A'X} \equiv \overline{AC}$, pelo caso LAL, $\triangle ABC \equiv \triangle A'B'X$ e isso implica que $\overline{XB'} \equiv \overline{CB} \equiv \overline{C'B'}$. Como $\overline{XB'} \equiv \overline{C'B'}$ o $\triangle B'C'X$ é isóceles de base $\overline{C'X}$ e daí $B'\widehat{C'}X \equiv B'\widehat{X}C'(\star)$ e analogamente $A'\widehat{C'}X \equiv A'\widehat{X}C'(\star\star)$. Somando $(\star)$ e $(\star\star)$ temos

que $A'\widehat{C'}B' \equiv A'\widehat{X}B'$. Como $\overline{A'X} \equiv \overline{A'C'}$, $\overline{XB'} \equiv \overline{C'B'}$ e $A'\widehat{C'}B' \equiv A'\widehat{X}B'$ pelo caso LAL, $\triangle A'B'C' \equiv \triangle A'B'X \equiv \triangle ABC$. □

4.2 Triângulo Retângulo

O primeiro tema de grande importância desta seção está em definir as relações proeminentes do triângulo retângulo. Vimos na definição 4.16 que um triângulo retângulo é aquele que possui um ângulo reto. Daí, temos algumas relações que são fundamentais em nosso estudo dos triângulos retângulos. Considere o triângulo abaixo como base para o estudo das relações trigonométricas:

Figura 17 – Relações Métricas



Fonte: Dolce (2013)

Observação 4.12. Ao olharmos a Figura 17, temos que $a = m + n$ e

1. a - hipotenusa
2. b, c - catetos
3. h - altura relativa a hipotenusa
4. m - projeção do cateto c sobre a hipotenusa
5. n - projeção do cateto b sobre a hipotenusa

Proposição 4.3. *Cada cateto é média geométrica entre sua projeção sobre a hipotenusa e a hipotenusa.*

Demonstração. Temos dois catetos e precisamos mostrar essa proposição para os dois. Considere que $\triangle ABC \sim \triangle DBA$ pelo caso AA e daí temos que

$$\frac{a}{c} = \frac{c}{m} \Longrightarrow c^2 = a \cdot m$$

Analogamente, $\triangle ABC \sim \triangle DAC$ pelo caso AA e daí,

$$\frac{a}{b} = \frac{b}{n} \Longrightarrow b^2 = a \cdot n$$

Sendo assim, mostramos a proposição definida. □

Proposição 4.4. *A altura relativa à hipotenusa é média geométrica entre os segmentos que determina sobre a hipotenusa.*

Demonstração. Temos que $\triangle DBA \sim \triangle DAC$ pelo caso AA e daí temos que,

$$\frac{h}{n} = \frac{m}{h} \Longrightarrow h^2 = m \cdot n$$

Com isso, mostramos a proposição. □

Proposição 4.5. *O produto dos catetos é igual ao produto da hipotenusa pela altura realativa a ela.*

Demonstração. Temos que $\triangle ABC \sim \triangle DAC$ pelo caso AA e daí temos que,

$$\frac{a}{b} = \frac{c}{h} \Longrightarrow b \cdot c = a \cdot h$$

Com isso, mostramos a proposição □

Proposição 4.6. *O produto de um cateto pela altura relativa à hipotenusa é igual ao produto do outro cateto pela projeção dp primeiro sobre ahipotenusa.*

Demonstração. Temos dois catetos e precisamos mostrar que essa relação é válida para os dois. Sabemos que $\triangle ABC \sim \triangle DAC$ pelo caso AA e daí temos que,

$$\frac{b}{n} = \frac{c}{h} \Longrightarrow b \cdot h = c \cdot n$$

Analogamente, como $\triangle ABC \sim \triangle DBA$ pelo caso AA e daí temos que,

$$\frac{b}{h} = \frac{c}{m} \Longrightarrow c \cdot h = b \cdot m$$

E assim, mostramos a proposição. □

Teorema 4.3. *(Teorema de Pitágoras) A área do quadrado cujo lado é a hipotenusa de um triângulo retângulo é igual a soma das áreas dos quadrados que têm como lado cada um dos catetos.*

Demonstração. Ao considerarmos o Triângulo da Figura 17, vemos que a área cujo lado é hipotenusa vale $A_1 = a^2$ e as áreas cujos lados são catetos valem $A_2 = b^2$ e $A_3 = c^2$. Portanto, precisamos mostrar que $A_1 = A_2 + A_3$, ou então que $a^2 = b^2 + c^2$. Para demostrarmos o Teorema de Pitágoras é só somarmos as duas relações que descobirmos na Proposição 4.4, assim

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

Como sabemos que $a = m + n$, então

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

$$A_2 + A_3 = A_1$$

Com isso, demosntramos o Teorema de Pitágoras. □

Teorema 4.4. *(Recíproca do Teorema de Pitágoras) Se num triângulo o quadrado de um lado é igual à soma dos quadrados dos outros dois, então o triângulo é retângulo.*

Demonstração. Aqui faremos exatamente o contrário do Teorema 4.3. Assim, sabemos que temos um triângulo de lados a, b e c e se $a^2 = b^2 + c^2$ então o triângulo é retângulo. Construindo um outro triângulo, $\triangle DEF$, retângulo em D e cujos catetos $\overline{DE}$ e $\overline{DF}$ sejam respectivamnete congruentes a $\overline{AB}$ e $\overline{AC}$. Como $\triangle DEF$ é retângulo, então $\overline{EF}^2 = \overline{DE}^2 + \overline{DF}^2$ e como $\overline{DE} \equiv \overline{AB}$ e $\overline{DF} \equiv \overline{AC}$, temos que $\overline{EF}^2 = \overline{AB}^2 + \overline{AC}^2 = \overline{BC}^2$. Sendo assim, $\overline{EF} \equiv \overline{BC}$. Portanto, pelo caso de congruência LLL, $\triangle ABC \equiv \triangle DEF$ e como $\triangle DEF$ é retângulo, então o $\triangle ABC$ também é. □

O Teorema de Pitágoras é de extrema importância no estudo dos triângulos Pitagóricos. As relações que faremos nesse trabalho estão intimamente ligadas a triplas pitagóricas, que estão conectadas a equação diofantina $x^2 + y^2 = z^2$, que conectam a tripla (x, y, z) a um triângulo retângulo de hipotenusa z e catetos x e y.

4.3 Área de um Triângulo

A última construção geométrica que precisamos fazer é termos o real entendimento de área. O problema de Fermat discute a área de uma triângulo pitagórico e para podermos discuti-lo de maneira perfeita no próximo capítulo, vamos definir o que é área e como determinar a área de um triângulo.

Definição 4.18. Área de uma superfície limitada é um número real positivo associado à superfície de forma tal que:

1. Às superfícies equivalentes estão associadas áreas iguais (números iguais) e reciprocamente.

$$A \approx B \iff (\text{Área de } A = \text{Área de } B)$$

2. A uma soma de superfícies está associada uma área (número) que é a soma das áreas das superfícies parcelas.

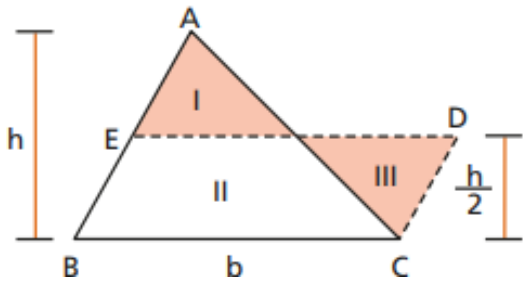
$$(C = A + B) \implies (\text{Área de } C = \text{Área de } A + \text{Área de } B)$$

3. Se uma superfície está contida em outra, então sua área é menor (ou igual) que a área da outra.

$$B \subset A \implies \text{Área de } B \leq \text{Área de } A$$

Teorema 4.5. *Todo triângulo é equivalente a um paralelogramo de base congruente à do triângulo e altura metade da altura do triângulo.*

Figura 18 – Teorema 4.5



Fonte: Dolce (2013)

Demonstração. Tome o $\triangle ABC$ e pelo o ponto médio E do lado $\overline{AB}$ conduzimos $\overline{ED}$ paralela a $\overline{BC}$ e completamos o paralelogramo $BCDE$.

Sabemos que $I \equiv III$ $(\star)$ e $II \equiv II$ $(\star\star)$ e somando $(\star)$ e $(\star\star)$, tem-se que $(I + II) \approx (II + III)$. Com isso, $ABC \approx BCDE$. □

Observação 4.13. Um quadrilátero plano convexo é um paralelogramo se, e somente se, possui os lados opostos paralelos.

Definição 4.19. Um quadrilátero plano convexo é um retângulo se, e somente se, possui os quatro ângulos congruentes.

Definição 4.20. Um quadrilátero plano convexo é um quadrado se, e somente se, possui os quatro ângulos congruentes e os quatro lados congruentes.

Teorema 4.6. *A razão entre dois retângulos de bases congruentes (ou alturas congruentes) é igual à razão entre suas alturas (ou bases).*

Demonstração. Temos dois retângulos que possuem a mesma base se dividrimos o primeiro retângulo em p partes de altura x e dividirmos o segundo retângulo em q partes de altura x temos que $h_1 = p \cdot x$ e $h_2 = q \cdot x$. Daí

$$\frac{h_1}{h_2} = \frac{p \cdot x}{q \cdot x} = \frac{p}{q} \tag{29}$$

Ao fazermos isso teremos p retângulos $X(b, x)$ no primeiro retângulo e q retângulos $X(b, x)$ no segundo retângulo. Com isso, $R_1 = p \cdot X$ e $R_2 = q \cdot X$. Daí

$$\frac{R_1}{R_2} = \frac{p \cdot X}{q \cdot X} = \frac{p}{q} \tag{30}$$

Por (29) e (30),

$$\frac{R_1}{R_2} = \frac{h_1}{h_2} \tag{31}$$

O racíocínio é o mesmo para a base. Se dividrimos o primeiro retângulo em p partes de base x e dividirmos o segundo retângulo em q partes de base x temos que $b_1 = p \cdot x$ e $b_2 = q \cdot x$. Daí

$$\frac{b_1}{b_2} = \frac{p \cdot x}{q \cdot x} = \frac{p}{q} \tag{32}$$

Ao fazermos isso teremos p retângulos $X(x, h)$ no primeiro retângulo e q retângulos $X(x, h)$ no segundo retângulo. Com isso, $R_1 = p \cdot X$ e $R_2 = q \cdot X$. Daí

$$\frac{R_1}{R_2} = \frac{p \cdot X}{q \cdot X} = \frac{p}{q} \tag{33}$$

Por (32) e (33),

$$\frac{R_1}{R_2} = \frac{h_1}{h_2} \tag{34}$$

□

Teorema 4.7. *A razão entre dois retângulos quaisquer é igual ao produto da razão entre as bases pela razão entre as alturas.*

Demonstração. Considere dois retângulos, $R_1(b_1, h_1)$ e $R_2(b_2, h_2)$, e cosntrua também um retângulo auxiliar $R(b_1, h_2)$. Aplicando o Teorema 4.6 em R_1 e R, teremos

$$\frac{R_1}{R} = \frac{h_1}{h_2} \tag{35}$$

Aplicando o Teorema 4.6 em R e R_2, teremos

$$\frac{R}{R_2} = \frac{b_1}{b_2} \tag{36}$$

Multiplicando (35) por (36), teremos

$$\frac{R_1}{R_2} = \frac{b_1}{b_2} \cdot \frac{h_1}{h_2} \tag{37}$$

□

Proposição 4.7. *A área de um retângulo é* $A_R = b \cdot h$.

Demonstração. Considere um retângulo $R(b, h)$ e um quadrado fixo $Q(1, 1)$, como unitário. Pelo Teorema 4.7, temos que

$$A_R = \frac{R(b,h)}{Q(1,1)} = \frac{b}{1} \cdot \frac{h}{1} = b \cdot h$$

□

Observação 4.14. Como o paralelogramo $P(b, h)$ é equivalente a um retângulo $R(b, h)$, temos que $A_P = A_R = b \cdot h$.

Proposição 4.8. *A área do triângulo é* $A_T = \frac{b \cdot h}{2}$.

Demonstração. Pelo Teorema 4.5, sabemos que um triângulo é equivalente a um paralelogramo cuja base mede b e a altura $\frac{h}{2}$. Assim

$$A_T = A_P = b \cdot \frac{h}{2} = \frac{b \cdot h}{2}.$$

□

Acabamos de concluir que a área de um triângulo qualquer é exatamente igual ao produto de sua base por sua altura divido por 2. Em um triângulo retângulo vemos que os lados que exercem as funções de base e altura são os catetos e assim, a área é dade pelo produto os catetos dividido por 2. Logo,

$$A_{\triangle \text{RETÂNGULO}} = \frac{b \cdot c}{2} \tag{38}$$

onde b, c são os catetos do triângulo retângulo de hipotenusa a. Com essa conclusão, temos todo o arcabouço necessário para discutirmos o probelam de Fermart, o que será feito no próximo capítulo.

5 A ÁREA DE UM TRIÂNGULO PITAGÓRICO, O PROBLEMA DE FERMAT

O destino final dessa viagem passa seriamente por este capítulo. Há uma grande significância em tudo o que foi feito até aqui. Falar sobre a proposição histórica do problema, assim como falar sobre suas construções aritméticas e geométricas, fortalece a construção de tudo o que será desenvolvido neste capítulo.

Neste capítulo discutiremos os ternos pitagóricos, depois os associaremos aos triângulos pitagóricos para assim chegarmos ao Problema de Fermat. O foco do presente trabalho é mostrar que a área de um triângulo pitagórico nunca é um quadrado perfeito e isso será feito na parte final deste capítulo. Este capítulo está fortemente baseado na obra de Sierpiński (1962, 1988), Bahier (2015) e Alencar Filho (1984). De formas mais esporádicas, também houve o uso de Souza (2017) e Brochero (2018).

5.1 Ternos Pitagóricos

Para iniciarmos a construção do problema, definiremos algumas características importantes sobre os ternos pitagóricos e sua forte ligação com as equações diofantinas, assim como também sua íntima conexão com os triângulos pitagóricos.

Definição 5.1. Chama-se terno pitagórico todo terno de inteiros positivos (a, b, c) tais que

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

Observação 5.1. Em outras palavras, terno pitagórico é toda solução inteira e positiva da equação diofantina:

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

Exemplo 5.1. Os ternos $(3, 4, 5)$, $(6, 8, 10)$, $(5, 12, 13)$ e $(12, 35, 37)$ são ternos pitagóricos, pois

$$3^2 + 4^2 = 9 + 16 = 25 = 5^2$$

$$6^2 + 8^2 = 36 + 64 = 100 = 10^2$$

$$5^2 + 12^2 = 25 + 144 = 169 = 13^2$$

$$12^2 + 35^2 = 144 + 1225 = 1369 = 37^2$$

Proposição 5.1. *Se (x, y, z) é um terno pitagórico, então (kx, ky, kz), onde $k > 1$ com $k \in \mathbb{N}$, também é um terno pitagórico.*

Demonstração. Sabemos que (x, y, z) é um terno pitagórico, logo

$$x^2 + y^2 = z^2 \tag{39}$$

Se multiplicarmos (39) por k^2, teremos que:

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

$$(kx)^2 + (ky)^2 = (kz)^2$$

Como mostramos que $(kx)^2 + (ky)^2 = (kz)^2$, então o terno (kx, ky, kz) é um terno pitagórico. □

Ao longo da história foram desenvolvidas algumas fórmulas que geram ternos pitagóricos. É importante lembrarmos de duas delas que são extremamente importantes para o estudo dos ternos pitagóricos.

Proposição 5.2. *(Fórmula de Pitágoras) O terno (x, y, z) é um terno pitagórico se $x = 2k + 1$, $y = 2k \cdot (k + 1)$ e $z = 2k \cdot (k + 1) + 1$, com $k \in \mathbb{N}$.*

Demonstração. Para mostramos que é um terno pitagórico vamos usar a definição se $x^2+y^2 = z^2$. Sabemos que $x = 2k + 1$ e $y = 2k \cdot (k + 1)$ assim,

$$x^2 + y^2 = (2k + 1)^2 + [2k \cdot (k + 1)]^2 = 4k^2 + 4k + 1 + [4k^2(k^2 + 2k + 1)]$$

$$x^2 + y^2 = (2k + 1)^2 + [2k \cdot (k + 1)]^2 = 4k^4 + 8k^3 + 8k^2 + 4k + 1$$

$$x^2 + y^2 = (2k + 1)^2 + [2k \cdot (k + 1)]^2 = (2k^2 + 2k + 1)^2 = z^2$$

Logo, a fórmula $x = 2k + 1$, $y = 2k \cdot (k + 1)$ e $z = 2k \cdot (k + 1) + 1$ gera ternos pitagóricos. □

Observação 5.2. Essa fórmula, atribuída a Pitágoras, determina todos os triângulos pitagóricos que possuem $z = y + 1$. Ou seja, determina os ternos pitagóricos onde z é sucessor de y.

Exemplo 5.2. Se $k = 1$, teremos $x = 3$, $y = 4$ e $z = 5$, logo o terno $(3, 4, 5)$ é pitagórico. Se $k = 2$, teremos $x = 5$, $y = 12$ e $z = 13$, logo o terno $(5, 12, 13)$ é pitagórico. Se $k = 3$, teremos $x = 7$, $y = 24$ e $z = 25$, logo o terno $(7, 24, 25)$ é um terno pitagórico.

Proposição 5.3. *(Fórmula de Platão) O terno (x, y, z) é um terno pitagórico se $x = 2pq$, $y = p^2 - q^2$ e $z = p^2 + q^2$, onde $p, q \in \mathbb{N}$ com $p > q$.*

Demonstração. Para mostramos que é um terno pitagórico vamos usar a definição se $x^2+y^2 = z^2$. Sabemos que $x = 2pq$ e $y = p^2 - q^2$ assim,

$$x^2 + y^2 = (2pq)^2 + (p^2 - q^2) = 4p^2q^2 + p^4 - 2p^2q^2 + q^4$$

$$x^2 + y^2 = (2pq)^2 + (p^2 - q^2) = p^4 + 2p^2q^2 + q^4$$

$$x^2 + y^2 = (2pq)^2 + (p^2 - q^2) = (p^2 + q^2)^2 = z^2$$

Logo, a fórmula $x = 2pq$, $y = p^2 - q^2$ e $z = p^2 + q^2$ gera ternos pitagóricos. □

Exemplo 5.3. Se $p = 2$ e $q = 1$, temos que $x = 4$, $y = 3$ e $z = 5$, logo o terno $(3, 4, 5)$ é pitagórico. Se $p = 3$ e $q = 2$, temos que $x = 12$, $y = 5$ e $z = 13$, logo o terno $(12, 5, 13)$ é pitagórico. Se $p = 4$ e $q = 2$, temos que $x = 16$, $y = 12$ e $z = 20$, logo o terno $(16, 12, 20)$ é pitagórico.

Observação 5.3. A partir deste momento considere que mdc de a e b será deotado por $mdc(a, b)$. Essa mudança será feita para que não se confunda o terno (x, y, z) com o $mdc(x, y, z)$.

Definição 5.2. Chama-se terno pitagórico primitivo todo terno pitagórico (x, y, z) tal que $mdc(x, y, z) = 1$.

Observação 5.4. Essa definição garante que todo terno pitagórico primitivo é aquele que possui x,y e z primos entre si.

Proposição 5.4. *Seja* (x, y, z) *um terno pitagórico primitivo então* $mdc(x, y) = mdc(x, z) = mdc(y, z) = 1$.

Demonstração. Temos três casos que são importantes para mostrarmos aqui. Em primeiro lugar considere que $d = mdc(x, y)$ e assim $d \mid x$ e $d \mid y$, considere que $\exists\, a, b \in \mathbb{N}$, tal que $x = a \cdot d$ e $y = b \cdot d$. Por definição, se o terno é primitivo $mdc(x, y, z) = 1$ e $x^2 + y^2 = z^2$. Assim,

$$(a \cdot d)^2 + (b \cdot d)^2 = z^2$$

$$a^2 \cdot d^2 + b^2 \cdot d^2 = z^2$$

$$d^2 \cdot (a^2 + b^2) = z^2$$

Como $a^2 + b^2 = m^2$, temos que

$$d^2 \cdot m^2 = z^2 \Longrightarrow d \cdot m = z \Longrightarrow d \mid z.$$

Assim, $d \mid x$, $d \mid y$ e $d \mid z$. Como $mdc(x, y, z) = 1$, $mdc(x, y) = 1$.

Em segundo lugar considere que $d = mdc(x, z)$ e assim $d \mid x$ e $d \mid z$, considere que $\exists\, a, b \in \mathbb{N}$, tal que $x = a \cdot d$ e $z = b \cdot d$. Por definição, se o terno é primitivo $mdc(x, y, z) = 1$ e $x^2 + y^2 = z^2$. Assim,

$$(a \cdot d)^2 + y^2 = (b \cdot d)^2$$

$$y^2 = b^2 \cdot d^2 - a^2 \cdot d^2$$

$$y^2 = d^2 \cdot (b^2 - a^2)$$

Como $b^2 - a^2 = m^2$, temos que

$$y^2 = d^2 \cdot m^2 \Longrightarrow y = d \cdot m \Longrightarrow d \mid y.$$

Assim, $d \mid x$, $d \mid y$ e $d \mid z$. Como $mdc(x, y, z) = 1$, $mdc(x, z) = 1$.

Por fim, considere que $d = mdc(y, z)$ e assim $d \mid y$ e $d \mid z$, considere que $\exists\, a, b \in \mathbb{N}$, tal que $y = a \cdot d$ e $z = b \cdot d$. Por definição, se o terno é primitivo $mdc(x, y, z) = 1$ e $x^2 + y^2 = z^2$. Assim,

$$x^2 + (a \cdot d)^2 = (b \cdot d)^2$$

$$x^2 = b^2 \cdot d^2 - a^2 \cdot d^2$$

$$x^2 = d^2 \cdot (b^2 - a^2)$$

Como $b^2 - a^2 = m^2$, temos que

$$x^2 = d^2 \cdot m^2 \Longrightarrow x = d \cdot m \Longrightarrow d \mid x.$$

Assim, $d \mid x$, $d \mid y$ e $d \mid z$. Como $mdc(x, y, z) = 1$, $mdc(y, z) = 1$. □

Exemplo 5.4. Os ternos $(3, 4, 5)$ e $(8, 15, 17)$ são ternos pitagóricos primitivos, pois $mdc(3, 4, 5) = 1$ e $mdc(8, 15, 17) = 1$. Já os ternos $(6, 8, 10)$ e $(15, 20, 25)$ não são ternos pitagóricos primitivos, pois $mdc(6, 8, 10) = 2 \neq 1$ e $mdc(15, 20, 25) = 5 \neq 1$.

Proposição 5.5. *Se (x, y, z) é um terno pitagórico não primitivo então $mdc(x, y) \mid z$.*

Demonstração. Sabemos que (x, y, z) é um terno pitagórico e também que $mdc(x, y) = d \neq 1$. Logo $\exists\, a, n$ tal que $x = a \cdot d$ e $y = b \cdot d$ e por definição

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

$$(a \cdot d)^2 + (b \cdot d)^2 = z^2$$

$$a^2 \cdot d^2 + b^2 \cdot d^2 = z^2$$

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

Como $a^2 + b^2 = m^2$, temos que

$$d^2 \cdot m^2 = z^2 \Longrightarrow d \cdot m = z \Longrightarrow d \mid z \Longrightarrow mdc(x, y) \mid z$$

Logo, se $mdc(x, y, z) \neq 1$, então $mdc(x, y) \mid z$. □

Proposição 5.6. *Se o terno (x, y, z) é um terno pitagórico não primitivo, então $\left(\frac{x}{d}, \frac{y}{d}, \frac{z}{d}\right)$ é um terno pitagórico primitivo.*

Demonstração. Considere $d = mdc(x, y, z)$. Se $\left(\frac{x}{d}, \frac{y}{d}, \frac{z}{d}\right)$ é um terno potagórico, então $mdc\left(\frac{x}{d}, \frac{y}{d}, \frac{z}{d}\right) = 1$ e vale que $(x, y, z) = d \cdot \left(\frac{x}{d}, \frac{y}{d}, \frac{z}{d}\right)$. Por definição,

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

Logo, $\left(\frac{x}{d}, \frac{y}{d}, \frac{z}{d}\right)$ é um terno pitagórico primitivo. □

Com isso, vemos que de qualquer terno pitagórico não primitivo se pode obter um terno pitagórico primitivo onde $(x, y, z) = d \cdot \left(\frac{x}{d}, \frac{y}{d}, \frac{z}{d}\right)$. Assim, todas as soluções de $x^2 + y^2 = z^2$ resultam da solução de $\left(\frac{x}{d}\right)^2 + \left(\frac{y}{d}\right)^2 = \left(\frac{z}{d}\right)^2$, onde $mdc\left(\frac{x}{d}, \frac{y}{d}, \frac{z}{d}\right) = 1$.

Exemplo 5.5. Assim $(15, 36, 39)$ e $(25, 60, 65)$ resultam do terno pitagórico primitivo $(5, 12, 13)$ multiplicando-se os elementos deste respectivamente pelos inteis 3 e 5.

Observação 5.5. Com todos os elementos menores que 1000 são conhecidos 158 ternos pitagóricos primitivos, e aquele que tem os maiores elementos é $(372, 924, 997)$.

Teorema 5.1. *Para todo $x \in \mathbb{N}$, com $x > 2$ existem $y, z \in \mathbb{N}$ tais que (x, y, z) é um terno pitagórico.*

Demonstração. Inicialmente, considere que x é par. Assim, $x = 2 \cdot k$ e sabemos que $2 \mid x$ e $4 \mid x^2$. Daí, temos que por $4 \mid x^2$ existem dois inteiros $y = \frac{x^2-4}{4}$ e $z = \frac{x^2+4}{4}$ e pela definição de terno pitagórico

$$x^2 + y^2 = x^2 + \left(\frac{x^2 - 4}{4}\right)^2 = x^2 + \frac{x^4 - 8x^2 + 16}{16} = \frac{x^4 + 8x^2 + 16}{16} = \left(\frac{x^2 + 4}{4}\right)^2 = z^2$$

Assim, o terno (x, y, z) é um terno pitagórico. Em segundo lugar, se x é ímpar, logo $x = 2k + 1$ e pela Porposição 5.2, temos que $y = 2k \cdot (k + 1)$ e $z = 2k \cdot (k + 1) + 1$, onde $k \in \mathbb{N}$ e assim tem-se sempre um terno pitagórico (x, y, z). □

Teorema 5.2. *Um terno (x, y, z) é um terno pitagórico se, e somente se, existem u e v inteiros que verifiquem as seguintes condições:*

1. $u > v > 0$;
2. $u \equiv v \ (mod\ 2)$;
3. $u \cdot v$ *é um quadrado perfeito;*
4. $x = \sqrt{u \cdot v}$, $y = \frac{u-v}{2}$, $z = \frac{u+v}{2}$.

Demonstração. Como temos um se, e somente, se é preciso que se mostre a ida e a volta. Assim

$\Rightarrow$) Suponha que (x, y, z) é um terno pitagórico e vamos buscar inteiros u e v tal que todas as quatro condições do Teorema 4.2 sejam satisfeitas. Sejam $u = z + y$ e $v = z - y$, e por definição $z > y$. Assim, $u > v > 0$, o que satisfaz [1]. Sabemos que $u - v = 2y$ o que implica que $2 \mid (u - v)$ e daí $u \equiv v \ (mod\ 2)$, o que satisfaz [2].

Para mostrar a [3] condição é só mostrarmos que $(z + y) \cdot (z - y)$ é um quadrado perfeito. Portanto,

$$u \cdot v = (z + y) \cdot (z - y) = z^2 - y^2 = x^2$$

E isso mostra a condição [3], pois $u \cdot v = x^2$. E assim, a condição [4] também é satisfeita pois

$$u \cdot v = x^2 \Longrightarrow x = \sqrt{u \cdot v}$$

$$\frac{u - v}{2} = \frac{2y}{2} = y$$

$$\frac{u + v}{2} = \frac{2z}{2} = z$$

$\Leftarrow$) A volta é mais simples, pois consideramos todos os critérios como válidos. Suponha que $u, v \in \mathbb{N}$, por [1] e [4] temos que x, y e z são positivos. Por [3] e [4], $x \in \mathbb{N}$ e por [2] e [4], $y, z \in \mathbb{N}$. Finalmente, por [4],

$$x^2 + y^2 = (\sqrt{u \cdot v})^2 + \left(\frac{u - v}{2}\right)^2$$

$$x^2 + y^2 = u \cdot v + \frac{u^2 - 2 \cdot u \cdot v + v^2}{4}$$

$$x^2 + y^2 = \frac{u^2 + 2 \cdot u \cdot v + v^2}{4}$$

$$x^2 + y^2 = \left(\frac{u + v}{2}\right)^2 = z^2$$

Sendo assim, (x, y, z) é um terno pitagórico.

Exemplo 5.6. Mostrar que $(360, 319, 481)$ é um terno pitagórico.

Sol. Considere que $u = 481+319 = 800$ e $v = 481-319 = 162$ e se as quatro condições do Teorema 5.2, então é um triângulo pitagórico. $u > v > 0$ e além disso $800 \equiv 162\ (mod\ 2)$ e isso satisfaz $[1]$ e $[2]$. É fácil ver que $800 \cdot 162 = 129600 = 360^2$ e assim satifaz $[3]$. Por fim, $x = \sqrt{360^2} = 360$, $y = \frac{800-162}{2} = \frac{638}{2} = 319$ e $z = \frac{800+162}{2} = \frac{962}{2} = 481$. Logo, $(360, 319, 481)$ é um terno pitagórico. □

Teorema 5.3. *Se (x, y, z) é um terno pitagórico primitivo, então z é ímpar e $x \not\equiv y\ (mod\ 2)$.*

Demonstração. Se (x, y, z) é um triângulo pitagórico primitivo, então $mdc(x, y) = mdc(y, z) = mdc(x, z) = mdc(x, y, z) = 1$. Assim, considere que $x \equiv y\ (mod\ 2)$ então ou x e y são pares ou x e y são ímpares. Se x e y são pares temos que $x = 2k$ e $y = 2t$ e por isso $2 \mid mdc(x, y)$. Essa conclusão é impossível pois $mdc(x, y) = 1$ e $2 \nmid 1$. Se por acoso, x e y sejam ímpares, então $x = 2k + 1$ e $y = 2t + 1$, como (x, y, z) é um terno pitagórico

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

$$z^2 = 4k^2 + 4k + 1 + 4t^2 + 4t + 2 = 2 \cdot (2k^2 + 2k^2 + 2t^2 + 2t + 1)$$

Logo, concluímos que z^2 é par e se $z^2 = 2k$, então $z = 2s$. Logo temos que

$$z^2 \equiv 0\ (mod\ 4) \tag{40}$$

$$x^2 \equiv 1\ (mod\ 4) \tag{41}$$

$$y^2 \equiv 1\ (mod\ 4) \tag{42}$$

Se somamros (41) e (42), teremos

$$x^2 + y^2 \equiv 2\ (mod\ 4)$$

Pelo fato de $z^2 = x^2 + y^2$ e por (40),

$$z^2 \equiv 2\ (mod\ 4)$$

O que é uma contradição pois um quadrado perfeito dividido por 4 deixa resto 0 ou 1. Logo, a premissa é falsa e $x \not\equiv y\ (mod\ 2)$ de modo que x e y possuem paridade diferente. Sendo assim, suponhamos sem perda de generalidade que $x = 2k$ e $y = 2t + 1$, logo

$$z^2 = (2k)^2 + (2t + 1)^2 = 4k^2 + 4t^2 + 4t + 1 = 2 \cdot (2k^2 + 2t^2 + 2t) + 1$$

o que nos garante que z^2 é ímpar e para que o quadrado de um número seja ímpar, o próprio número é ímpar, o que conclui nossa demonstração. □

Observação 5.6. O que aprendemos com o Teorema 5.3 é que num triângulo pitagórico primitivo qualquer (x, y, z), há exatamente um elemente que é par (ou x ou y) e dois elementos que são ímpares (ou x e z ou y e z), de modo que $x + y + z = 2k$.

Proposição 5.7. *O terno pitagórico primitivo (x, y, z) é da forma*

$$x = m^2 - n^2, \quad y = 2m \cdot n, \quad z = m^2 + n^2$$

com $mdc(m, n) = 1$ e $m + n$ é ímpar.

Demonstração. Para mostramos isso, utilizaremos a definição de terno pitagórico, onde:

$$x^2 + y^2 = z^2 \Longrightarrow y^2 = z^2 - x^2 = (z + x) \cdot (z - x) \tag{43}$$

Pelo Lema 3.1, temos que $mdc(z + x, z - x) = mdc(z + x, 2z) = 2$, pois como o triângulo pitagórico é primitivo $mdc(x, z) = 1$ e $mdc(z, z + x) = 1$. Pelo Teorema 5.3, sabemos que z é ímpar e portanto $z + x$ é par. Com isso, $mdc\left(\frac{z-x}{2}, \frac{z+x}{2}\right) = 1$ e Pelo Teorema 3.10

$$\frac{z + x}{2} = m^2, \quad \text{e} \quad \frac{z - x}{2} = n^2$$

E daí, teremos

$$z + x = 2m^2 \tag{44}$$

$$z - x = 2n^2 \tag{45}$$

Substituindo (44) e (45) em (43),

$$y^2 = 2m^2 \cdot 2n^2 = 4 \cdot m^2 \cdot n^2$$

$$y = 2 \cdot m \cdot n \tag{46}$$

Relacionando (44) e (45),

$$z = m^2 + n^2 \tag{47}$$

$$x = m^2 - n^2 \tag{48}$$

Por $(46), (47)$ e (48) mostramos que todo terno pitagórico primitivo é da forma proposta com $mdc(m, n) = 1$. A condição de $m + n$ ser ímpar garante que a tripla é primitiva, pois como $mdc(m, n) = 1$, temos que $(m^2, m^2 + n^2) = 1$. Assim, $mdc(x, z) = mdc(m^2 - n^2, m^2 + n^2) =$

$mdc(2m^2, m^2 + n^2) = mdc(2, m^2 + n^2) = 1$, se, e somente se,$m^2 + n^2$ for ímpar (Se fosse par $mdc(x, z) = 2$, o que é um absurdo). Logo $m^2 + n^2$ é ímpar e isso só é possível se $m \not\equiv n \ (mod\ 2)$. □

Exemplo 5.7. Determinando ternos pitagóricos primitivos:

1. Se $m = 2$ e $n = 1$, teremos $x = 3,\ y = 4$ e $z = 5$;
2. Se $m = 3$ e $n = 2$, teremos $x = 5,\ y = 12$ e $z = 13$;
3. Se $m = 4$ e $n = 1$, teremos $x = 15,\ y = 8$ e $z = 17$;
4. Se $m = 4$ e $n = 3$, teremos $x = 7,\ y = 24$ e $z = 25$;
5. Se $m = 5$ e $n = 2$, teremos $x = 21,\ y = 20$ e $z = 29$;
6. Se $m = 5$ e $n = 4$, teremos $x = 9,\ y = 40$ e $z = 41$;
7. Se $m = 6$ e $n = 1$, teremos $x = 35,\ y = 12$ e $z = 37$;
8. Se $m = 6$ e $n = 3$, teremos $x = 27,\ y = 36$ e $z = 45$;
9. Se $m = 6$ e $n = 5$, teremos $x = 11,\ y = 60$ e $z = 61$;
10. Se $m = 7$ e $n = 2$, teremos $x = 45,\ y = 28$ e $z = 53$;

Observação 5.7. Os demais ternos pitagóricos que não são primitivos podem ser gerados multiplicando os terno pitagóricos primitvos por uma constante.

Proposição 5.8. *Se (x, y, z) é um terno pitagórico, então $x \neq y$.*

Demonstração. Pela definição de terno pitagórico, sabemos que para $x, y, z \in \mathbb{N}$. Suponha que seja verdade e por definição:

$$z^2 = x^2 + x^2 = 2x^2$$

$$z = x \cdot \sqrt{2}$$

Isso é impossível, pois $z \notin \mathbb{N}$. Logo, para que haja um terno pitagórico é preciso que $x \neq y$. □

Observação 5.8. A proposição 5.8 é de extrema importância em uma conclusão que pode-se ter em relação ao Teorema de Fermat que discutiremos na última seção deste capítulo.

5.2 Triângulos Pitagóricos

Após concluirmos a seção sobre ternos pitagóricos é importante perceber que todo terno pitagórico (x, y, z) está associado a um triângulo retângulo que possui hipotenusa z e catetos x e y. Esse triângulo retângulo associado a um terno pitagórico é chamado de triângulo pitagórico.

Definição 5.3. Um triângulo retângulo XYZ, $\triangle XYZ$, de catetos x, y e hipotenusa z é dito pitagórico se as medidas dos seus lados são números inteiros.

Observação 5.9. Para que o triângulo retângulo seja pitagórico precisamos que os lados sejam números naturais, os inteiros positivos, já que não podemos ter uma lado não-positivo. Além disso como temos uma associação a um terno pitagórico e também todo triângulo retângulo tem como implicação a validade do Teorema de Pitágoras.

Observação 5.10. Quando usarmos os triângulos pitagóricos de lados (x, y, z), estaremos dizendo que o triângulo possui os catetos x, y e a hipotenusa z.

Exemplo 5.8. O triângulo de lado $(3, 4, 5)$ é um triângulo pitagórico pois $3^2 + 4^2 = 5^2$ e todos os lados são números inteiros. O triângulo de lados $(2, 3, 4)$ não é pitagórico pois mesmo que seus lados sejam inteiros, não é satisfeito o teorema de pitágoras, pois $2^2 + 3^2 \neq 4^2$. O triângulo $(1, 1, \sqrt{2})$ não é pitagórico, pois mesmo qeu satifaça o teorema de pitágoras, não possui lados inteiros ($\sqrt{2} \notin \mathbb{N}$).

Definição 5.4. Um triângulo pitagórico de lados (x, y, z) é chamado de primitivo quando seus lados são primos entre si, ou seja $mdc(x, y) = mdc(x, z) = mdc(y, z) = mdc(x, y, z) = 1$.

Proposição 5.9. *Dois triângulos pitagóricos primitivos distintos não são semelhantes.*

Demonstração. Sejam os $\triangle XYZ$ e $\triangle ABC$ primitivos, de lados (x, y, z) e (a, b, c). Sabemos que $mdc(x, y) = mdc(x, z) = mdc(y, z) = mdc(x, y, z) = 1$ e $mdc(a, b) = mdc(a, c) = mdc(b, c) = mdc(a, b, c) = 1$. Suponha que os $\triangle XYZ$ e $\triangle ABC$ sejam semelhantes. Assim existe um k tal que,

$$\frac{x}{a} = \frac{y}{b} = \frac{z}{c} = k$$

com $k > 1$ e assim, temos que $x = a \cdot k$, $y = b \cdot k$ e $z = c \cdot k$. Daí temos que o $\triangle XYZ$ possui os lados $(x, y, z) = (k \cdot a, k \cdot b, k \cdot c)$ e sabemos que $mdc(k \cdot a, k \cdot b, k \cdot c) = k$ o que é um absurdo já que por definição $mdc(x, y, z) = 1$. □

Proposição 5.10. *Se um triângulo pitagórico é primitivo então:*

1. *O cateto y é sempre um múltiplo de 4.*

2. *Um dos catetos, x ou y, é sempre um múltiplo de 3.*

3. *Um dos três lados é múltiplo de 5.*

Demonstração. Sabemos que se um triângulo pitagórico é primitivo, então $x = m^2 - n^2$, $y = 2 \cdot m \cdot n$ e $z = m^2 + n^2$.

[1]. Por (46) sabemos que $y = 2 \cdot m \cdot n$ e como $mdc(m, n) = 1$, temos que m e n possuem paridade diferente e assim $y = 4k$.

[2]. Se m ou n forem múltiplos de 3 então obrigatoriamente $y = 3k$. Se nem m nem n são múltiplos de 3, então eles possuem duas formas,

$$a = 3k + 1 \Longrightarrow a^2 = (3k + 1)^2 = 9k^2 + 6k + 1 = 3(3k^2 + 2k) + 1 = 3t + 1$$

$$a = 3k + 2 \Longrightarrow a^2 = (3k + 2)^2 = 9k^2 + 12k + 4 = 3(3k^2 + 4k + 1) + 1 = 3b + 1$$

logo, os dois casos são da forma 3k+1 e assim $x = m^2 - n^2 = 3k$.

[3]. Se $m = 5k$ ou $n = 5l$ teremos que $y = 5k$. Se nenhum deles é múltiplo de 5 temos quatro opções $5k + 1$, $5k + 2$, $5k + 3$ ou $5k + 4$. E daí,

$$a = 5k + 1 \Longrightarrow a^2 = (5k + 1)^2 = 25k^2 + 10k + 1 = 5(5k^2 + 2k) + 1 = 5t + 1$$

$$a = 5k + 2 \Longrightarrow a^2 = (5k + 2)^2 = 25k^2 + 20k + 4 = 5(5k^2 + 4k) + 4 = 5t + 4$$

$$a = 5k + 3 \Longrightarrow a^2 = (5k + 3)^2 = 25k^2 + 30k + 9 = 5(5k^2 + 6k + 1) + 4 = 5t + 4$$

$$a = 5k + 4 \Longrightarrow a^2 = (5k + 4)^2 = 25k^2 + 40k + 16 = 5(5k^2 + 8k + 3) + 1 = 5t + 1$$

Se m e n são da mesma forma, $5k + 1$ ou $5k + 4$, então $x = m^2 - n^2 = 5k$ e se m e n são de formas diferentes, um é $5k + 1$ e o outro $5k + 4$, então $z = m^2 + n^2 = 5k$. □

5.3 O Problema de Fermat

Um dos pontos que são mais importantes no estudo deste capítulo está fundamentado na área de um triângulo pitagórico. Vimos no capítulo 3, por (38) vemos que a área de um triângulo retângulo de lados (x, y, z) é $A = \frac{x \cdot y}{2}$. Nesta seção vamos discutir algumas particularidades do estudo das áreas de triângulos pitagóricos, que são triângulos retângulos que possuem lados inteiros.

Proposição 5.11. *A área de um triângulo pitagórico é sempre um múltiplo de 6.*

Demonstração. Vemos pela Proposição 5.10 que em um triângulo pitagórico primitivo, temos que o cateto y é um múltiplo de 4 e um dos dois cateto, x ou y, é um múltiplo de 3. Assim, temos duas opções ou $x = 3k$ e $y = 4l$ ou $y = 12k$. Analisando as duas opções,

[1]. Sendo $x = 3k$ e $y = 4l$, teremos

$$A = \frac{x \cdot y}{2} = \frac{3k \cdot 4l}{2} = \frac{12 \cdot (k \cdot l)}{2} = 6 \cdot (k \cdot l)$$

logo, $A = 6t$.

[2]. Sendo $y = 12k$, termos

$$A = \frac{x \cdot y}{2} = \frac{x \cdot 12k}{2} = \frac{12 \cdot (x \cdot k)}{2} = 6 \cdot (x \cdot k)$$

logo, $A = 6t$. E com isso, provamos que a área de um triângulo pitagórico primitivo é sempre um múltiplo de 6. Como um triângulo pitagórico primitivo gera os triângulos pitagóricos não primitivos, todos os não primitivos são também múltiplos de seis. □

Exemplo 5.9. Observe os triângulo pitagóricos primitivos abaixo

1. Se $x = 3,\ y = 4$ e $z = 5$, então $A = 6$;
2. Se $x = 5,\ y = 12$ e $z = 13$, então $A = 30$;
3. Se $x = 15,\ y = 8$ e $z = 17$, então $A = 60$;
4. Se $x = 7,\ y = 24$ e $z = 25$, então $A = 84$;
5. Se $x = 21,\ y = 20$ e $z = 29$, então $A = 210$;
6. Se $x = 9,\ y = 40$ e $z = 41$, então $A = 180$;
7. Se $x = 35,\ y = 12$ e $z = 37$, então $A = 210$;
8. Se $x = 27,\ y = 36$ e $z = 45$, então $A = 486$;
9. Se $x = 11,\ y = 60$ e $z = 61$, então $A = 330$;
10. Se $x = 45,\ y = 28$ e $z = 53$, então $A = 630$.

Exemplo 5.10. Observe os triângulos pitagóricos não primitivos abaixo,

1. Se $x = 9,\ y = 12$ e $z = 15$, então $A = 54$;
2. Se $x = 15,\ y = 36$ e $z = 39$, então $A = 270$;

3. Se $x = 30,\ y = 16$ e $z = 34$, então $A = 240$;

4. Se $x = 21,\ y = 72$ e $z = 75$, então $A = 756$;

Observação 5.11. Todas as áreas do Exemplo 5.9 e do Exemplo 5.10 são múltiplos de 6.

Observação 5.12. Nosso foco aqui será voltado de maneira primária aos triângulos pitagóricos primitivos, pois os não primitivos são gerados múltiplicando os lados por um certo $k \in \mathbb{N}$.

Quando observamos as áreas dos triângulos pitagóricos algumas coisas saltam aos olhos. Se observarmos os triângulos pitagóricos primitivos de lados $(21, 20, 29)$ e $(35, 12, 37)$, no Exemplo 5.9, veremos que suas áreas sõa iguais a 210. Assim, temos triângulos pitagóricos que possuem elementos completamente distintos, mas possuem a mesma área.

Proposição 5.12. *Se dois triângulos pitagóricos, $\triangle XYZ$ e $\triangle ABC$, de lados (x, y, z) e (a, b, c) possuem a mesma área e a mesma hipotenusa, então esses triângulos são congruentes.*

Demonstração. Por hipótese os dois triângulos possuem a mesma área e assim $x \cdot y = a \cdot b$. Além disso, sabemos, também por hiótese, que as hipotenusas são iguais $(z = c)$. Como os triânglos são pitagóricos, temos que $a^2 + b^2 = c^2$ e $x^2 + y^2 = z^2$ e por hipótese

$$a^2 + b^2 = x^2 + y^2 \tag{49}$$

Por outro lado, $(a+b)^2 = a^2 + 2ab + b^2$ e $(x+y)^2 = x^2 + 2xy + y^2$. Por (49) e por $a \cdot b = x \cdot y$, temos que $(a+b)^2 = (x+y)^2$ e assim, $a + b = x + y$. Analogamente, $a - b = x - y$ e porntanto $x = a$ e $y = b$. Logo, se dois triângulos pitagóricos possuem a mesma área e a mesma hipotenusa, então eles são congruentes. □

Proposição 5.13. *Se um terno pitagórico primitivo (x, y, z) é da forma*

$$x = m^2 - n^2, \quad y = 2m \cdot n, \quad z = m^2 + n^2$$

com $mdc(m, n) = 1$ e $m + n$ é ímpar. Assim sua área pode ser expressa por

$$A = m \cdot n \cdot (m + n) \cdot (m - n)$$

Demonstração. Sabemos que a área de um triângulo pitagórico é dada por $A = \frac{x \cdot y}{2}$ e como temos um triângulo pitagórico primitivo então $x = m^2 - n^2$ e $y = 2 \cdot m \cdot n$, assim

$$A = \frac{x \cdot y}{2} = \frac{2 \cdot m \cdot n \cdot (m^2 - n^2)}{2} = m \cdot n \cdot (m + n) \cdot (m - n)$$

□

Lema 5.1. *Se* $mdc(m,n) = 1$*, sendo um dos dois par, então* $mdc(m,n) = mdc(m,m-n) = mdc(m,m+n) = mdc(n,m-n) = mdc(n,m+n) = mdc(m-n,m+n) = 1$.

Demonstração. Já sabemos que $mdc(m,n) = 1$ por definição. Pelo Lema de Euclides $mdc(m,n) = mdc(m,m-n) = mdc(m,m+n) = mdc(n,m-n) = mdc(n,m+n) = 1$. Por fim, $mdc(m+n,m-n) = 1$, pois se houvesse um divisor comum a $m+n$ e $m-n$ teríamos que esse número também dividiria a soma $2m$ e a diferença $2n$, e como esse divisor seria impar, dividiria x e y. □

Lema 5.2. *Se* $mdc(m,n) = 1$*, sendo* m *ímpar, então* $mdc(m,2n) = mdc(m,m-n) = mdc(m,m+n) = mdc(2n,m-n) = mdc(2n,m+n) = mdc(m-n,m+n) = 1$.

Demonstração. Como m é ímpar e $mdc(m,n) = 1$, então $mdc(m,2n) = 1$. Pelo Lema de Euclides $mdc(m,n) = mdc(m,m-n) = mdc(m,m+n) = 1$ e pelo Lema 5.1, $mdc(m+n,m-n) = 1$. Por fim, basta mostrar qur $mdc(2n,m+n) = mdc(2n,m-n) = 1$. Sabemos que $m+n$ e $m-n$ são ímpares e sendo assim não adimitem o fator 2. Além disso, pelo Lema 5.1, $mdc(n,m+n) = mdc(n,m-n) = 1$. Portanto, $mdc(2n,m+n) = mdc(2n,m-n) = 1$. □

Com isso estabelecido, progrediremos para o ponto final deste trabalho. Fermat propôs que a área de um triângulo pitagórico não pode ser representada por um quadrado perfeito e, com a fundamentação necessária para demonstrarmos esse problema, prosseguiremos para a mais bela e importante etapa deste trabalho.

Teorema 5.4. *Não existem dois númeors naturias tal que a soma e a diferença de seus quadrados sejam quadrados.*

Demonstração. Suponha que existam números naturais x e y tal que $x^2+y^2 = z^2$ e $x^2-y^2 = t^2$, onde $z,t \in \mathbb{N}$, com $z > t$. De todos os pares x,y existe um onde x^2+y^2 é mínimo, onde devemos ter $mdc(x,y) = 1$. Pois se $d \mid x$ e $d > y$, com $d \mid 1$, então, como $x^2+y^2 = z^2$ e $x^2-y^2 = t^2$, teríamos que $d^2 \mid z^2$, $d^2 \mid t^2$, de onde $d \mid z$ e $d \mid t$. Se isso ocorrer, implicaria que toda a equação poderia ser dividida por d^2, contrariando a suposição de x,y denotam a solução de x^2+y^2 sendo mínima.

Por $x^2+y^2 = z^2$ e $x^2-y^2 = t^2$, temos que $2x^2 = z^2+t^2$. Se a z^2+t^2 é par, isso implica que z,t são ou pares ou ímpares. O que nos garante que $z+t$ e $z-t$ são obrogatoriamente

números pares e isso nos garnate que $\frac{z+t}{2}, \frac{z-t}{2} \in \mathbb{N}$. Se $d \mid \frac{z+t}{2}$ e $d \mid \frac{z-t}{2}$ e $d > 1$, então

$$x^2 = \left(\frac{z+t}{2}\right)^2 + \left(\frac{z-t}{2}\right)^2 \tag{50}$$

e isso implica que $d^2 \mid x^2$ e consequentemenda $d \mid x$. Logo, como $x^2 + y^2 = z^2$, teríamos que $d \mid y$ e isso é impossível pois $mdc(x, y) = 1$, logo

$$mdc\left(\frac{z+t}{2}, \frac{z-t}{2}\right) = 1 \tag{51}$$

de (50) e (51) temos que

$$\left(\frac{z+t}{2}, \frac{z-t}{2}, x\right)$$

formam os lados de um triângulo pitagórico primitivo e pela Proposição 5.7, existem $m, n \in \mathbb{N}$, com $m > n$, $mdc(m, n) = 1$ e m e n com paridades diferentes. Tais que,

$$\frac{z+t}{2} = m^2 - n^2 \quad \text{e} \quad \frac{z-t}{2} = 2 \cdot m \cdot n$$

ou

$$\frac{z-t}{2} = m^2 - n^2 \quad \text{e} \quad \frac{z+t}{2} = 2 \cdot m \cdot n$$

Se multiplicarmos os dois lados, nos dois casos possíveis, teremos a mesma solução $z^2 - t^2 = 4 \cdot (m^2 - n^2) \cdot 2 \cdot m \cdot n[\star]$. Vemos por $x^2 + y^2 = z^2$ e $x^2 - y^2 = t^2$, teremos que $2y^2 = z^2 - t^2[\star\star]$. Por $[\star]$ e $[\star\star]$, teremos que $2y^2 = 4 \cdot (m^2 - n^2) \cdot 2 \cdot m \cdot n$ e por conseguinte $y^2 = (m^2 - n^2) \cdot 4 \cdot m \cdot n$. Vemos que y^2 é um múltiplo de quatro e daí y é um múltiplo de 2, $y = 2k$, com $k \in \mathbb{N}$, e daí

$$k^2 = (m^2 - n^2) \cdot m \cdot n \tag{52}$$

Sabemos que $mdc(m, n) = 1$ e pelo Lema de Euclides $mdc(m, n) = mdc(m \pm n, m) = mdc(m^2 - n^2, m) = mdc(m^2 - n^2, n) = 1$. Por (52) e Pelo Teorema Fundamental da Aritmética, temos que m, n e $m^2 - n^2$ são um quadrado de um número natural. Assim, considere que

$$m = a^2, \quad n = b^2, \quad m^2 - n^2 = c^2 \quad \text{com } a, b, c \in \mathbb{N}$$

e pelo Lema 5.1, temos que $mdc(m+n, m-n) = 1$. Assim, $(m+n) \cdot (m-n) = m^2 - n^2 = c^2$, pelo teorema fundamental da aritmética, $m + n$ e $m - n$ são qudrados perfeitos. Como $m = a^2$, $n = b^2$ os números $a^2 + b^2 = m + n$ e $a^2 - b^2 = m - n$ são quadrados. Mas,

$$a^2 + b^2 = m + n < 2 \cdot m \leq 2 \cdot m \cdot n \leq \frac{z+t}{2} < z \leq z^2 = x^2 + y^2$$

e assim, $a^2 + b^2 < x^2 + y^2$ e isso contraria a ideia de que o par x, y é o mínimo. Assim, a suposição de que existem números naturais para os quais a soma e a diferença de seus quadrados são quadrados leva a uma contradição. Sendo assim, não existem dois números naturais tal que a soma e a diferença de seus quadrados sejam quadrados. □

Definição 5.5. Seja $n \in \mathbb{N}$, n é um quadrado perfeito se, e somente se, $\exists\ a \in \mathbb{N}$ tal que $n = a^2$.

Teorema 5.5. ***(Teorema de Fermat)*** *Não existe um triângulo pitagórico cuja a área seja um quadrado de um número natural.*

Demonstração. Nossa demonstração focará em um triângulo pitagórico primitivo, pois garantindo para os primitivos consequentemente garantimos para os não primitivos. Sabemos que um triâmgulo pitagórico primitivo tem seus (x, y, z) gerados por m e n da seguinte maneira,

$$x = m^2 - n^2 \quad , \quad y = 2 \cdot m \cdot n \quad \text{e} \quad z = m^2 + n^2 \tag{53}$$

sabemos que $mdc(m, n) = 1$ e também que ambos possuem paridade diferente. Sabemos também que x é ímpar e y é par, pois como $x \not\equiv y\ (mod\ 2)$ e $y = 4k = 2(2k)$, temos que isso acontece. Sabemos também que a área do triângulo pitagórico é dada por,

$$A = \frac{x \cdot y}{2} = m \cdot n \cdot (m + n) \cdot (m - n) \tag{54}$$

Suponhamos que $A = t^2$, que a área seja um quadrado perfeito. Então, como x é ímpar e $\frac{y}{2}$ é par, temos que $mdc(x, \frac{y}{2}) = 1$. Pelo Lema 5.1, $mdc(m, n) = mdc(m, m - n) = mdc(m, m + n) = mdc(n, m - n) = mdc(n, m + n) = mdc(m - n, m + n) = 1$. Pelo Teorema Fundamental da Aritmética temos que os seis número devem ser um quadrado perfeito.

Assim, $x = a^2$ e por (53),

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

como $mdc(m, n) = 1$ e possuem paridades diferentes, temos que a e n são catetos de um triângulo primitivo de hipotenusa m. Evidentemente o triângulo gerado é menor que o triângulo primitivo original e se a área do primeiro é um quadrado perfeito, então a áres deste triângulo pitagórico primitivo de lados (a, n, m) é um quadrado perfeito.

Se o triângulo gerado é primitivo, temos que u e v são números geradores e assim,

$$a = u^2 - v^2 \quad , \quad n = 2 \cdot u \cdot v, \quad \textbf{e} \quad m = u^2 + v^2 \tag{55}$$

sabemos que m e n são quadrados perfeitos e temos que $m = b^2$ e $n = 4c^2$. Daí, teremos que $b^2 = u^2 + v^2$ e $\frac{u \cdot v}{2} = c^2$. Assim temos que o triângulo pitagórico primitivo de lados (u, v, b) com área igula a $\frac{u \cdot v}{2} = c^2$. Ese novo triângulo é menor do que o orignial e se aplicarmos esse raciocínio de maneira sucessiva vamos encontrar infinitos triângulos pitagóricos primitivos cada vez menores e os números naturias, dos quais é necessário ter lados naturais para ser um triângulo pitagórico, são limitados inferiormente pelo 1. Logo, temos um absurdo e não podemos ter que a área de um triângulo pitagórico é um quadrado perfeito. □

Observação 5.13. Para os queridos leitores que compreendem a demonstração acima muito longa e de racicínio muito complexo ou até para aqueles que se incomodam com a demonstração ser apenas para os triângulos pitagóricos pirmitivos, propomos uma outra demonstração.

Demosntração Alternativa do Teorema 5.5. Suponha que exista um triângulo pitagórico de lados (x, y, z) e assim, teremos

$$x^2 + y^2 = z^2 \tag{56}$$

e assim, pela fórmula da área de um triângulo pitagórico temos que,

$$A = \frac{x \cdot y}{2} \Longrightarrow x \cdot y = 2A$$

Se a área de um triângulo pitagórico é um quadrado perfeito, então $A = n^2$ e assim, $2 \cdot x \cdot y = 4 \cdot n^2 = (2n)^2$. Sabemos que

$$(x + y)^2 = x^2 + 2 \cdot x \cdot y + y^2 = (x^2 + y^2) + (2 \cdot x \cdot y) = z^2 + (2n)^2 \tag{57}$$

$$(x - y)^2 = x^2 - 2 \cdot x \cdot y + y^2 = (x^2 + y^2) - (2 \cdot x \cdot y) = z^2 - (2n)^2 \tag{58}$$

Pelo Teorema 5.4, temos que não existem dois números naturais tal que a soma e a diferença de seus quadrados sejam quadrados, mas por (57) e (58) temos que isso acontece na suposição. Logo, a suposição é falsa e assim não existe um triângulo pitagórico cuja a área seja um quadrado de um número natural. □

Observação 5.14. Se considerarmos o triângulo retângulo de lados $(2\sqrt{2}, 2\sqrt{2}, 4)$, veremos que a área desse triângulo retângulo é dada por $A = \frac{2\sqrt{2} \cdot 2\sqrt{2}}{2} = \frac{4 \cdot \sqrt{4}}{2} = 4$. E uma pergunta pode surgir, o Teorema 5.5, proposto por Fermat, diz que não podemos ter um tirângulo pitagórico cuja a área seja um quadrado perfeito e esse caso nos dá uma área com valor 4, que é um quadrado perfeito. Como isso é possível?

Para que um triângulo seja pitagórico, temos que os seus lados precisam ser obrigatoriamente inteiros positivos, $x, y, z \in \mathbb{N}$, na situação porposta os catetos além de serem iguais, o que é proibido pela porposição 5.8, são números irracionais que não são válidos na definição do nosso problema.

6 CONSIDERAÇÕES FINAIS

Neste trabalho foi discutido e demonstrado o problema de Fermat, onde a área de um triângulo pitagórico, triângulo retângulo de lados inteiros e positivos, nunca pode ser expressa por meio de um quadrado perfeito. Para que isso fosse feito de maneira coesa e fluida, foi necessário construir os aspectos históricos que fundamentam o problema, assim como as bases aritméticas e geométricas que constroem as definições dos triângulos pitagóricos e de sua área.

Construímos os conceitos básicos que fundamentam a ideia dos triângulos pitagóricos, as condições que permeiam a parametrização dos lados do triângulo retângulo e todas as propriedades que envolvem os triângulos pitagóricos primitivos. Após isso, foi preparado o Teorema de Fermat e demonstrado de duas maneiras, uma delas usando o descenso infinito de Fermat, que é um método de prova por contradição ou absurdo, e um outro método que está baseado no fato de que dois quadrados somados e subtraídos não podem gerar como resposta um número quadrado.

Com essas construções, fundamentamos tudo que era preciso para que possamos trabalhar o problema de Fermat, demonstramos o teorema e com isso foi mostrado que a área de um triângulo pitagórico nunca pode ser um quadrado perfeito, pois se isso ocorrer, teremos triângulos cada vez menores cuja área seria um quadrado perfeito de um número natural e, como essa construção se tornaria infinita, chegaria um ponto onde teríamos um triângulo que não corresponde às condições de existência do problema.

A área de um triângulo pitagórico nunca pode ser um quadrado de um número natural e o teorema de Fermat nos permite garantir que isso não pode existir. Com isso, fundamentamos e demonstramos um teorema que aparece de maneira constante na formação básica de matemática do ensino básico e que traz um detalhe não muito explorado, mas significativo no processo construtivo dos triângulos pitagóricos.

REFERÊNCIAS

ALENCAR FILHO, E. de. **Teoria Elementar dos Números**. 1. ed. São Paulo: Nobel, 1984.

BROCHERO, F. E.; MOREIRA, C. G.; SALDANHA, N.C.; TENGAS, E. **Teoria dos Números**: um passeio com primos e outros números familiares pelo mundo inteiro. 5. ed. Rio de Janeiro: IMPA, 2018.

DOLCE, O.; POMPEO, J. N. **Fundamento de Matemática Elementar**: Geometria Plana v.9. 9. ed. São Paulo: Atual, 2013.

DORIA, C. M. **Geometria II**. 2. ed. Florianópolis: UFSC, 2007.

EVES, H. **Introdução à história da Matemática**. Campinas: UNICAMP, 2004.

FALLAS, J. J. Ternas pitagóricas: métodos para generarlas y algunas curiosidades. **Revista Digital Matemática Educación e Internet**, v. 9, n. 2, p. 1-21, 2009. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.redalyc.org/pdf/6079/607972920002.pdf. Acesso em: 29 nov. 2024.

FARIA, A. A. C. **Teoria dos Números**: Uma Introdução Motivadora Direcionada aos Docentes do Ensino Básico. 2015. Dissertação (Mestrado em Matemática) — Universidade Federal de Alagoas, Maceió, 2015.

FEITEN, V. V. D. **O Princípio da Indução Finita e Sua Aplicação na Educação Básica**. 2024. Dissertação (Mestrado em Matemática) — Universidade Tecnológica Federal do Paraná, Toledo, 2024.

HEFEZ, A. **Elementos de Aritmética**. 2. ed. Rio de Janeiro: SBM, 2006.

MORGADO, A.C.; CARVALHO, P.C. **Matemática Discreta**. 1.ed. Rio de Janeiro: SBM, 2014.

SANTOS, J. P. O. **Introdução À Teoria dos Númeors**. Rio de Janeiro: SBM, 1998.

SIERPÍNSKI, W. **Elementary Theory of Numbers**. Amsterdã: North-Holland, 1988.

SIERPÍNSKI, W. **Pythagorean triangles**. New York: Dover Publications, 1962.

SOUZA, R. S. **Equações Diofantinas Lineares, Quadráticas e Aplicações**. 2017. Dissertação(Mestrado em Matemática) — Universidade Estadual Paulista "Júlio de Mesquita Filho", Rio Claro, 2017.

WALSH, C. M. Fermat's Note XLV. **Annals of Mathematics**, v. 29, n. 1/4, 1927, p. 412–432. JSTOR, Disponível em: https://doi.org/10.2307/1968013. Accesso em: 7 fev. 2025.