**UNIVERSIDADE FEDERAL DO CEARÁ**

**CENTRO DE CIÊNCIAS**

**DEPARTAMENTO DE MATEMÁTICA**

**PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA EM REDE NACIONAL**

**MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL**

**ANTONIO WESLEY DE BRITO VIEIRA**

# O PROBLEMA DOS NÚMEROS CONGRUENTES: UMA JORNADA DA ANTIGUIDADE ÀS CURVAS ELÍPTICAS

**FORTALEZA**

**2025**

ANTONIO WESLEY DE BRITO VIEIRA

# O PROBLEMA DOS NÚMEROS CONGRUENTES: UMA JORNADA DA ANTIGUIDADE ÀS CURVAS ELÍPTICAS

Dissertação apresentada ao Curso de Mestrado Profissional em Matemática em Rede Nacional do Programa de Pós-Graduação em Matemática em Rede Nacional do Centro de Ciências da Universidade Federal do Ceará, como requisito parcial à obtenção do título de mestre em Matemática. Área de Concentração: Matemática na Educação Básica.

Orientador: Prof. Dr. José Alberto Duarte Maia.

FORTALEZA

2025

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Sistema de Bibliotecas
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

---

V713p Vieira, Antonio Wesley de Brito.
O problema dos números congruentes: uma jornada da antiguidade às curvas elípticas / Antonio Wesley de Brito Vieira. – 2025.
87 f. : il. color.

Dissertação (mestrado) – Universidade Federal do Ceará, Centro de Ciências, Departamento de Matemática, Programa de Pós-Graduação em Matemática em Rede Nacional, Fortaleza, 2025.
Orientação: Prof. Dr. José Alberto Duarte Maia.

1. Números congruentes. 2. Curvas elípticas. I. Título.

CDD 510

---

ANTONIO WESLEY DE BRITO VIEIRA

# O PROBLEMA DOS NÚMEROS CONGRUENTES: UMA JORNADA DA ANTIGUIDADE ÀS CURVAS ELÍPTICAS

Dissertação apresentada ao Curso de Mestrado Profissional em Matemática em Rede Nacional do Programa de Pós-Graduação em Matemática em Rede Nacional do Centro de Ciências da Universidade Federal do Ceará, como requisito parcial à obtenção do título de mestre em Matemática. Área de Concentração: Matemática na Educação Básica.

Aprovada em: 25/07/2025.

BANCA EXAMINADORA

---

Prof. Dr. José Alberto Duarte Maia (Orientador)
Universidade Federal do Ceará (UFC)

---

Prof. Dr. Fernando Antonio Amaral Pimentel
Universidade Federal do Ceará (UFC)

---

Prof. Dr. Joserlan Perote da Silva
Universidade da Integração Internacional da Lusofonia Afro-Brasileira (UNILAB)

À memória de Mel, minha fiel companheira.

## AGRADECIMENTOS

Agradeço primeiramente a **Deus**, pois "tudo posso naquele que me fortalece" (*Filipenses 4:13*).

Agradeço à minha esposa, *Vanessa Barreto*, pelo companheirismo e apoio incondicional ao longo desta jornada e de toda a vida. Sua paciência, seu apoio incondicional e sua capacidade de compreender minhas ausências durante as longas horas de estudo me deram a tranquilidade necessária para sempre seguir em frente. Esta conquista é tão sua quanto minha.

Aos meus pais, *Kuerly Vieira* e *João Alves*, minha mais profunda gratidão. À minha mãe, por todo o afeto e carinho, que sempre foram meu refúgio e minha paz. Ao meu pai, pela confiança inabalável e pelo exemplo de força, que me deram a segurança necessária para enfrentar cada desafio. Sem o incentivo, o apoio financeiro e o amor de vocês, esta conquista não seria possível.

Aos colegas de mestrado, minha profunda gratidão. Levo comigo não apenas as valiosas reflexões, críticas e sugestões, mas, sobretudo, a memória da leveza das nossas conversas e brincadeiras de toda quarta-feira, que foram essenciais para aliviar a tensão desta jornada.

Agradeço a todos os professores do programa e, em especial, ao meu orientador, Prof. Dr. José Alberto Duarte Maia, por sua confiança, paciência e por toda a fundamental orientação neste projeto.

Aos professores participantes da banca examinadora Prof. Dr. Fernando Antonio Amaral Pimentel e o Prof. Dr. Joserlan Perote da Silva pelo seu tempo e pelas valiosas colaborações e sugestões.

Por fim, guardo um lugar especial nesta dissertação para deixar um agradecimento final e póstumo à minha inesquecível *Pet Mel*. Sua partida durante o mestrado deixou um vazio que a saudade teima em preencher. Ela era mais que um animal de estimação; era o meu porto seguro nas longas noites de estudo, a companhia silenciosa que tornava a solidão mais branda, especialmente com minha esposa residindo em outra cidade para seus estudos. A tranquilidade que ela me proporcionou foi fundamental para que eu chegasse até aqui.

"A mente que se abre a uma nova ideia, jamais voltará ao seu tamanho original." (Albert Einstein)

## RESUMO

Esta dissertação tem como foco a investigação do problema dos números congruentes, um tema clássico da Teoria dos Números que questiona quais inteiros podem ser a área de um triângulo retângulo com lados racionais. Embora sua formulação seja elementar, o problema revela uma notável profundidade, conectando a matemática histórica às fronteiras da pesquisa contemporânea, como a Conjectura de Birch e Swinnerton-Dyer. O trabalho perpassa por três formulações equivalentes do problema: a definição clássica via áreas de triângulos, a perspectiva de progressões aritméticas de três quadrados racionais, e a elegante conexão com a teoria das curvas elípticas. São abordados resultados fundamentais, como a não congruência do número 1 por Fermat e o critério de Tunnell, que representa o avanço mais significativo em direção a uma solução completa. Como principal contribuição de natureza pedagógica, este estudo apresenta, em apêndice, uma sequência didática intitulada "Explorando o Mundo dos Números Congruentes no Ensino Médio", elaborada para auxiliar professores do Ensino Médio na introdução deste fascinante tema em sala de aula.



**Palavras-chave**: números congruentes; áreas de triângulos retângulos; progressões aritméticas; curvas elípticas; matemática - programas de atividades.

**ABSTRACT**

This dissertation focuses on the investigation of the congruent number problem, a classical topic in Number Theory that questions which integers can be the area of a right-angled triangle with rational sides. Although its formulation is elementary, the problem reveals a remarkable depth, connecting historical mathematics to the frontiers of contemporary research, such as the Birch and Swinnerton-Dyer Conjecture. The work covers three equivalent formulations of the problem: the classical definition via triangle areas, the perspective of arithmetic progressions of three rational squares, and the elegant connection to the theory of elliptic curves. Fundamental results are addressed, such as the non-congruence of the number 1 by Fermat and Tunnell's criterion, which represents the most significant advance toward a complete solution. As a primary pedagogical contribution, this study presents, in an appendix, a didactic sequence titled "Exploring the World of Congruent Numbers in High School,"designed to assist high school teachers in introducing this fascinating topic in the classroom.

**Keywords**: congruent numbers; areas of right triangles; arithmetic progressions; elliptic curves; mathematics - activity programs.

## LISTA DE FIGURAS

## LISTA DE TABELAS

## SUMÁRIO

# 1 INTRODUÇÃO

Os números congruentes constituem um tema clássico na Teoria dos Números, com aplicações que perpassam desde problemas históricos, como os estudados pelos matemáticos gregos e árabes, até questões modernas em criptografia e geometria algébrica. Apesar de sua definição aparentemente simples  um número racional positivo que é a área de um triângulo retângulo com lados racionais , que será formalizada na Definição 1.0.1, a determinação de quais números são congruentes permanece um desafio em aberto, vinculado a profundas conjecturas, como a de Birch e Swinnerton-Dyer. Este trabalho se justifica pela relevância do tema tanto para a matemática pura quanto para aplicações práticas, além da carência de material didático acessível sobre o assunto em língua portuguesa.

Assim, este trabalho tem como objetivo investigar o problema dos números congruentes, abordando sua formulação clássica, evolução histórica, métodos de resolução e conexões com a teoria das curvas elípticas.

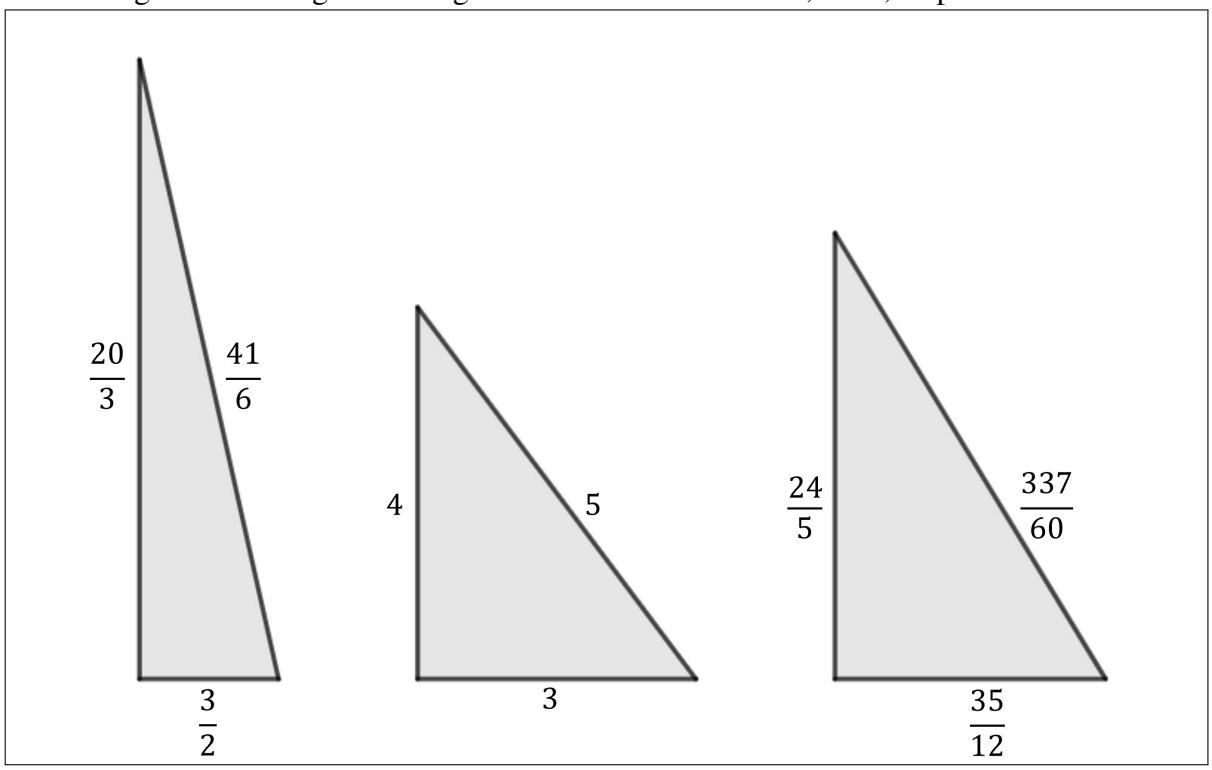
Um triângulo retângulo é chamado de racional quando todos os seus lados são números racionais. Qualquer triângulo retângulo racional naturalmente tem uma área racional, mas não necessariamente qualquer número racional pode ser obtido como área de um triangulo retângulo racional. Este questionamento é o ponto de partida que da base ao nosso estudo: quais números racionais ocorrem como a área de um triângulo retângulo racional?

**Definição 1.0.1.** *Um número racional positivo n é dito congruente se existe um triangulo retângulo racional de área n: existem racionais a, b, c > 0, tais que* $a^2 + b^2 = c^2$ *e* $(1/2)ab = n$.

De um modo geral, encontrar racionais $a$, $b$ e $c$, não necessariamente positivos, que satisfaçam as equações da Definição 1.0.1 acima, já garante que $n$ é um número congruente, pois o terno $(|a|, |b|, |c|)$ define um triângulo retângulo racional de área $n$.

Na Figura 1 a seguir, temos exemplos de triângulos retângulos racionais de áreas 5, 6 e 7 respectivamente, ou seja, tais números são congruentes.

Figura 1 – Triângulos retângulos racionais com áreas 5, 6 e 7, respectivamente




Fonte: Elaborado pelo autor (2025).

Além desta introdução, a presente dissertação organiza-se em quatro capítulos subsequentes e um apêndice.

O Capítulo 2 é dedicado às origens e ao contexto histórico do problema dos números congruentes, revisitando as contribuições de matemáticos proeminentes ao longo da história.

No Capítulo 3, explora-se a definição clássica de número congruente como sendo a área de um triângulo retângulo com lados racionais, que apesar de historicamente não ser a primeira definição do problema, é a definição mais intuitiva para início dos estudos. São abordados também os ternos pitagóricos e sua parametrização, além da demonstração de resultados fundamentais, como a não congruência do número 1.

O Capítulo 4 introduz a formulação que historicamente é atribuída como a primeira definição para o problema dos números congruentes, associando números congruentes a progressões aritméticas de três quadrados racionais perspectiva esta que conferiu o nome "congruente" ao problema. Apresenta-se, ainda, o argumento do matemático italiano Angelo Genocchi, um dos pioneiros a demonstrar a não congruência para uma classe inteira de números, mais especificamente, primos $p$ tais que $p \equiv 3 \pmod 8$.

Posteriormente, o Capítulo 5 investiga o conceito de curvas elípticas, um campo de estudo fascinante e complexo da matemática. Embora a conexão com os números congruen-

tes não seja imediatamente aparente, demonstra-se como estas curvas oferecem uma terceira perspectiva para o problema e podem deter uma das chaves para a solução completa do mesmo. Destaca-se o teorema formulado por Tunnell, que utilizando a teoria das curvas elípticas, propõe um critério para determinar a congruência de um número, ressalvando-se que a validade completa de sua recíproca depende de uma conjectura ainda não resolvida na matemática.

Por fim, como contribuição de natureza prática e pedagógica, esta dissertação apresenta, em apêndice, um produto educacional. Trata-se de uma sequência didática elaborada com o intuito de auxiliar professores na introdução deste fascinante tema dos números congruentes em salas de aula da educação básica, buscando revelar aos estudantes a riqueza matemática que pode emergir de questionamentos aparentemente simples e fomentar o interesse pela disciplina.

# 2 HISTÓRIA E FUNDAMENTOS MATEMÁTICOS

A aparente simplicidade de certos problemas da Teoria dos Números frequentemente oculta uma história rica e uma complexidade surpreendente. O problema dos números congruentes é um caso exemplar. O que hoje pode ser formulado em termos geométricos sobre áreas de triângulos, na verdade, tem suas raízes em questões puramente algébricas que remontam à matemática árabe medieval. Este capítulo se dedica a explorar essa evolução, investigando as origens do problema e destacando as contribuições de figuras-chave que, ao longo dos séculos, ajudaram a moldar nosso entendimento sobre ele.

## 2.1 Origem do problema

O estudo dos números congruentes pode ser rastreado até a Idade Média, em manuscritos escritos pelo matemático persa Al-Karaji (953 - 1029). Em sua primeira versão, o problema dos números congruentes não considera triângulos, a questão discutida por Al-Karaji foi; "para quais inteiros $n$, existe um $a \in \mathbb{Q}$ tal que $a^2 - n$ e $a^2 + n$ são ambos racionais quadrados?", Quando isso for verdade, é dito que $n$ é número congruente. Daí vem o nome "número congruente", do fato de existirem três quadrados congruentes modulo $n$; $a^2 - n$, $a^2$ e $a^2 + n$. Al-Karaji foi fortemente influenciado pela tradução árabe das obras do matemático grego Diofanto de Alexandria (210 - 290), onde Diofanto já estudava e elaborava problemas similares.

## 2.2 Fibonacci e o Livro dos Quadrados

O termo "número congruente" foi popularizado posteriormente por Fibonacci, no seu famoso "Liber Quadratorum" (Livro dos Quadrados), publicado em 1225. Equivalentemente a Al-Kiraji, Fibonacci definiu um número como congruente se existirem três quadrados que formem uma progressão aritmética com razão igual ao número em questão. Fibonacci foi influenciado por estudos anteriores e contribuiu significativamente para a resolução de equações diofantinas, cujas soluções inteiras ou racionais estavam no cerne do problema dos números congruentes. Seu trabalho marcou o início da tentativa de classificar e entender quais números podiam ser congruentes.

## 2.3 O papel de Fermat e a não congruência de 1

O matemático francês Pierre de Fermat (1601 - 1665) desempenhou um papel crucial na compreensão da impossibilidade de alguns números serem congruentes. Ele demonstrou que o número 1 não pode ser congruente, ou seja, não pode ser a área de um triângulo retângulo com lados racionais (discutiremos este resultado no próximo capítulo). Isso foi provado por Fermat usando seu método da descida infinita, uma técnica que se tornou central para muitas de suas descobertas. Fermat argumentou que a equação que expressa a área de um triângulo retângulo racional não pode ser satisfeita quando o valor da área é 1, resolvendo um dos primeiros casos significativos do problema.

## 2.4 Desafios do século XIX e os avanços recentes

O problema dos números congruentes continuou a ser um desafio no século XIX. Diversos matemáticos tentaram classificar quais números são congruentes e quais não são. Em particular, os números primos que satisfazem certas condições modulares começaram a ser explorados de forma mais sistemática. Ao mesmo tempo, as conexões entre o problema dos números congruentes e outras áreas da teoria dos números começaram a emergir, principalmente através do estudo de curvas elípticas e equações diofantinas.

No século seguinte, em 1983, o matemático americano Jerrold Bates Tunnell (1950 - 2022) fez progressos significativos na relação entre curvas elípticas e números congruentes, formulando um teorema fundamental, que será detalhado posteriormente no decorrer deste trabalho, o qual estabelece uma conexão direta entre a congruência de um número e a quantidade de soluções inteiras de certas funções. Porém, a total validade deste teorema está associada a um caso particular de um dos problemas em aberto na matemática, a conjectura de Birch e Swinnerton-Dyer. Esta conjectura é um dos "Sete Problemas do Milênio" do *Clay Mathematics Institute*, este instituto oferece um prêmio de um milhão de dólares para quem resolver qualquer um destes problemas (até a publicação deste trabalho, apenas um destes sete problemas já foi resolvido, a *Conjectura de Poincaré*).

# 3 A PERSPECTIVA GEOMÉTRICA DOS NÚMEROS CONGRUENTES

Embora a abordagem original do problema, como discutido no capítulo anterior, seja de natureza puramente algébrica e remeta aos textos de Al-Karaji a cerca de mil anos atrás, a interpretação de um número congruente como a área de um triângulo retângulo de lados racionais, conforme apresentado na Definição1.0.1 tornou-se a formulação clássica e o ponto de partida mais intuitivo para sua investigação. Portanto, aprofundaremos o estudo do problema dos números congruentes a partir de sua formulação mais difundida: a geométrica. Partindo desta definição, este capítulo explorará a relação fundamental com os ternos pitagóricos, a importância de analisar os inteiros livres de quadrados e a apresentação de resultados cruciais, como a demonstração de Fermat sobre a não congruência do número 1.

## 3.1 Inteiros livres de quadrados e os números congruentes

Inicialmente vamos definir formalmente o conceito de inteiro livre de quadrados.

**Definição 3.1.1.** *Dado um $n \in \mathbb{Z}^+$ dizemos que $n$ é um inteiro livre de quadrados quando $\forall\, p \in \mathbb{Z}^+$, se $p^2 \mid n$, então $p = 1$.*

O problema dos números congruentes, em sua essência, investiga quais números racionais podem ser a área de um triângulo retângulo racional. Contudo, não é necessário analisar todo o universo dos números racionais, a proposição apresentada a seguir, nos permite reduzir o escopo desta análise.

**Proposição 3.1.2.** *Para todo número racional positivo $q$, existe um racional $k$ tal que o produto $q \cdot k^2$ é um inteiro livre de quadrados.*

*Demonstração.* Seja $q$ um número racional positivo. Podemos escrevê-lo como uma fração de dois inteiros positivos; $q = \frac{a}{b}$, onde $a, b \in \mathbb{Z}^+$, com $b \neq 0$. E, pelo *Teorema Fundamental da Aritmética*, podemos escrever $a$ e $b$ em fatores primos, em particular, tomemos:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m} \quad \text{e} \quad b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_m^{\beta_m}.$$

Onde $p_i$ são números primos e os expoentes $\alpha_i, \beta_i \geq 0$ são inteiros (note que, caso exista algum $p_i$ que aparece na fatoração de $b$, mas não aparece na fatoração de $a$, então $\alpha_i = 0$, do contrário, $\beta_i = 0$). Assim, a fatoração em primos do número racional $q$ é:

$$q = \frac{a}{b} = \frac{p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}}{p_1^{\beta_1} p_2^{\beta_2} \cdots p_m^{\beta_m}} = p_1^{\alpha_1-\beta_1} p_2^{\alpha_2-\beta_2} \cdots p_m^{\alpha_m-\beta_m} = \prod_{i=1}^{m} p_i^{\gamma_i}.$$

Onde cada expoente $\gamma_i = \alpha_i - \beta_i$ é inteiro (positivo, negativo ou zero).

Para cada expoente $\gamma_i$, podemos usar o algoritmo da divisão para escrevê-lo na forma $\gamma_i = 2t_i + r_i$, com $t_i$ inteiro e o resto $r_i$ igual a 0 ou 1. O valor de $r_i$ simplesmente nos diz se $\gamma_i$ é par ($r_i = 0$) ou ímpar ($r_i = 1$). Substituindo isso na fatoração de $n$, temos:

$$q = \prod_{i=1}^{m} p_i^{2t_i+r_i} = \left(\prod_{i=1}^{m} p_i^{r_i}\right) \cdot \left(\prod_{i=1}^{m} p_i^{2t_i}\right) = \left(\prod_{i=1}^{m} p_i^{r_i}\right) \cdot \left(\prod_{i=1}^{m} p_i^{t_i}\right)^2. \tag{3.1}$$

Note que o primeiro fator da ultima igualdade da equação (3.1) acima, por construção, é um inteiro livre de quadrados, pois todos os expoentes $r_i$ são 0 ou 1. Enquanto o segundo fator é um racional quadrado. Portanto, tomando:

$$k = \frac{1}{\prod_{i=1}^{m} p_i^{t_i}},$$

obtemos que:

$$q \cdot k^2 = \prod_{i=1}^{m} p_i^{r_i}.$$

Que, como dito, é um inteiro livre de quadrados. ■

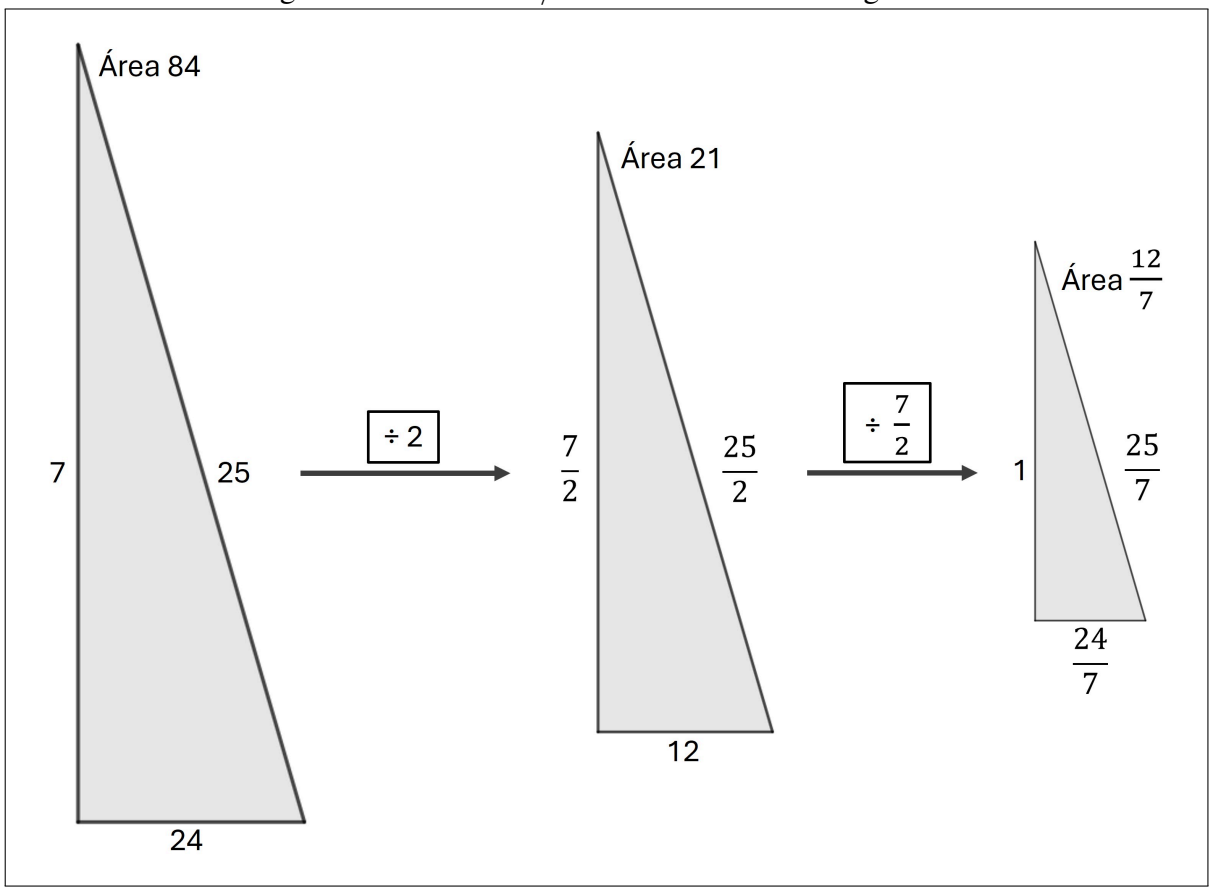
Note que a demonstração da Proposição 3.1.2 acima é construtiva, oferecendo um algoritmo explícito para se obter o inteiro livre de quadrados $n$ e o fator $k^2$ a partir de um racional $q$ qualquer. Dada a fatoração em primos de $q$ (tomando um produto com expoentes negativos ao invés de uma fração), o inteiro $n$ livre de quadrados procurado é formado pelo produto dos primos que originalmente possuem um expoente ímpar. Os fatores restantes de $q$, por sua vez, formam necessariamente um quadrado racional, digamos $s^2$, de modo que temos a decomposição $q = n \cdot s^2$. Assim, o fator $k^2$ que buscamos é simplesmente o inverso de $s^2$, ou seja, $k^2 = 1/s^2$, garantindo que $q \cdot k^2 = n$.

Portanto, se para qualquer racional positivo $q$, podemos encontrar um inteiro livre de quadrados $n$ tal que $q \cdot k^2 = n$ para algum racional $k$. Decorre disso uma equivalência fundamental: $q$ é um número congruente se, e somente se, seu correspondente inteiro livre de quadrados $n$

também o for. A justificativa para essa equivalência é geométrica e baseia-se no princípio de que a área de uma figura é alterada pelo quadrado do fator de escala aplicado a seus lados. Assim, para obter um triângulo retângulo racional com tal área $q$, basta escalonar os lados do triângulo de área $n$ (correspondente) por um fator de $1/k$, onde $k$ é obtido como indicado.

**Exemplo 3.1.3.** Seja o racional $q = 12/7$. Sua fatoração em primos, $2^2 \cdot 3 \cdot 7^{-1}$, revela pela Proposição 3.1.2 que seu correspondente inteiro livre de quadrados é $n = 3 \cdot 7 = 21$ (tomando os fatores de expoente ímpar). Como $12/7 = 21 \cdot 2^2 \cdot 7^{-2}$, temos que o racional quadrado que multiplicado por $12/7$ resulta no inteiro livre de quadrados 21 é dado por $1/(2^2 \cdot 7^{-2}) = (7/2)^2$. Assim, $12/7$ é um número congruente, se, e somente se 21 também o for. Em particular, tomando o triângulo $(7, 24, 25)$ que tem área $84 = 2^2 \cdot 21$, podemos chegar a um triângulo retângulo racional de área 21, e em seguida escalona-lo novamente para obter um triângulo retângulo racional de área $12/7$. Este processo está esquematizado na Figura 2 a seguir.

Figura 2 – Obtendo $12/7$ como um racional congruente




Fonte: Elaborado pelo autor (2025).

Deste modo, podemos reduzir nosso estudo sobre quais números são congruentes analisando apenas os inteiros livres de quadrados.

## 3.2 Ternos pitagóricos

**Definição 3.2.1.** *Dados três números a, b e $c \in \mathbb{Z}^+$, estes determinam um terno pitagórico se $a^2 + b^2 = c^2$.*

Naturalmente que o nome vem do *Teorema de Pitágoras*, pois se três números satisfazem tais condição então eles podem representar lados de um triângulo retângulo. Diremos que um terno pitagórico é primitivo se $mdc(a, b, c) = 1$, do contrário, diremos que é um terno pitagórico derivado. Nosso objetivo fundamental nesta seção é apresentar as formulas de Euclides (300 a.C) usadas para obter ternos pitagóricos. Para deduzir tais formulas, antes provaremos o seguinte lema:

**Lema 3.2.2.** *Dado dois números naturais a e b coprimos, se $a \cdot b$ é um quadrado perfeito, então tanto a quanto b são quadrados perfeitos.*

*Demonstração.* Suponha que $a \cdot b = c^2$ para algum $c \in \mathbb{N}$. Seja então $d = mdc(a, c)$, logo podemos escrever $a = a_1 d$ e $c = c_1 d$, com $mdc(a_1, c_1) = 1$, pois do contrário $d$ não seria o $mdc$ de $a$ e $b$. Assim, substituindo $a$ e $c$ descritos na equação original temos:

$$a_1 db = c_1^2 d^2 \qquad \Rightarrow \qquad a_1 b = c_1^2 d. \tag{3.2}$$

Ora, como $mdc(a_1, c_1) = 1$, então $mdc(a_1, c_1^2)$ também é 1. Portanto, na última igualdade de (3.2) temos que $c_1^2 \mid b$, ou seja, $b = c_1^2 \cdot l$ para algum $l \in \mathbb{N}$. Substituindo $b$ em (3.2) temos:

$$a_1 l c_1^2 = c_1^2 d \qquad \Rightarrow \qquad l a_1 = d. \tag{3.3}$$

Como $l \mid b$ e $d \mid a$, então $mdc(d, l) \mid mdc(a, b) = 1$, logo $mdc(d, l) = 1$. Assim, da equação (3.3) e de que $mdc(d, l) = 1$ temos que $d \mid a_1$, ou seja $a_1 = \lambda d$ que quando substituída em (3.3) obtemos $\lambda l = 1$, logo $\lambda = l = 1$. Deste modo $a_1 = d$ e $b = c_1^2$, logo, $a = d a_1 = d^2$. ■

De posse de tal lema, podemos formular uma maneira de obter ternos pitagóricos primitivos.

**Teorema 3.2.3.** *[Fórmulas de Euclides para Ternos Pitagóricos Primitivos] Sejam $a, b, c \in \mathbb{Z}^+$, então $(a, b, c)$ determina um terno pitagórico primitivo, isto é:*

$$a^2 + b^2 = c^2, \quad mdc(a, b, c) = 1.$$

*Se, e somente se, existem inteiros $m > n > 0$, com $mdc(m, n) = 1$ e $m \not\equiv n \pmod 2$, tais que:*

$$a = m^2 - n^2, \quad b = 2mn, \quad c = m^2 + n^2.$$

*Demonstração.* Seja $(a, b, c)$ um terno pitagórico, então se $mdc(a, b, c) = 1$, quaisquer termos dois a dois são coprimos. Para tal, suponha sem perda de generalidade que $mdc(a, c) = d > 1$, daí se $d \mid a$ e $d \mid c$, então $d \mid a^2$ e $d \mid c^2$, consequentemente $d \mid c^2 - a^2 = b^2$. Ora, se $d \mid b^2$, então existe pelo menos um fator $p$ primo divisor de $d$, tal que $p \mid b$, neste caso, temos $p \mid b$ e $p \mid d = mdc(a, c)$, logo $p \mid mdc(a, b, c) = 1$, absurdo!

Assim por $a$, $b$ e $c$ serem dois a dois coprimos, e satisfazerem a igualdade $a^2 + b^2 = c^2$ temos que há dois números impares. É fácil ver que os dois impares não podem ser $a$ e $b$ simultaneamente (basta analisar a congruência de $a$, $b$ e $c$ modulo 4), logo $a$ e $b$ tem paridades opostas, e consequente $c$ será impar. Supondo que a seja o outro número mpar, podemos reescrever $a^2 + b^2 = c^2$ como $b^2 = c^2 - a^2$, e mais ainda, podemos escrever:

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

Note que $\frac{c+a}{2}$ e $\frac{c-a}{2}$ são inteiros, pois $a$ e $c$ são impares, e além disso, são coprimos, pois seu $mdc$ deve dividir sua soma e sua subtração que são respectivamente $c$ e $a$, e estes são coprimos. Portanto, pelo Lema 3.2.2 temos que existem inteiros positivos $m$ e $n$, tais que:

$$\frac{c+a}{2} = m^2, \quad \frac{c-a}{2} = n^2,$$

Assim, isolando temos:

$$a = m^2 - n^2, \quad b = 2mn, \quad c = m^2 + n^2.$$

Com $m$ e $n$ com paridades distintas, visto que $a$ e $c$ são impares e com $d = mdc(m, n) = 1$, pois $d \mid mdc(a, b, c) = 1$.

Reciprocamente, dado dois números $m, n \in \mathbb{N}$ com $m > n > 0$, $mdc(m, n) = 1$ e com paridades distintas. Colocando $a = m^2 - n^2$, $b = 2mn$ e $c = m^2 + n^2$ vamos verificar $(a, b, c)$ é terno pitagórico primitivo. De fato, a verificação de que $(m^2 - n^2)^2 + (2mn)^2 = (m^2 + n^2)^2$ é imediata, mas, além disso, devemos ter que $mdc(a, b, c) = 1$.

Suponha que exista um $p$ primo, tal que $p \mid mdc(b, c)$, ora, neste caso, $p \mid b = 2mn$, portanto, como $mdc(m, n) = 1$, temos três opções;

(1) $p \mid 2 \Rightarrow p = 2$, ora, mas $m$ e $n$ tem paridades distintas, logo $m^2$ e $n^2$ também tem, portanto $c = m^2 + n^2$ é ímpar, e deste modo $p = 2 \nmid c$.

(2) $p \mid m$, então $p \mid m^2$, mas se $p \mid c$, então $p \mid n^2$ e logo, $p \mid n$, absurdo, dado que $mdc(m, n) = 1$.

(3) $p \mid n$, então $p \mid n^2$, mas se $p \mid c$, então $p \mid m^2$ e logo, $p \mid m$, novamente um absurdo, dado que $mdc(m, n) = 1$.

Logo, como em todos os casos não podemos obter um $p$ primo tal que $p \mid mdc(b, c)$, então $mdc(b, c) = 1$, e consequentemente, para qualquer a, temos $mdc(a, b, c) = 1$. Assim $a$, $b$ e $c$ escolhidos geram um terno pitagórico primitivo. ■

Assim, em posse do Teorema 3.2.3 de Euclides, temos um método para gerar ternos pitagóricos primitivos a partir da escolha de inteiros $m$ e $n$ coprimos e de paridades opostas. Podemos usar esta ferramenta para construir triângulos retângulos de áreas inteiras e, consequentemente, gerar novos números congruentes ao analisar a parte livre de quadrados de cada área obtida.

## 3.3 Um algoritmo para obter números congruentes

A tabela abaixo contém os ternos pitagóricos gerados por todas as possíveis escolhas de $m$, $n$, tal que $m + n < 10$. Em cada terno pitagórico vamos destacar o número congruente obtido pela parte livre de quadrado da área do respectivo triângulo determinado.

Tabela 1 – Números congruentes obtidos por ternos pitagóricos

| n | m | $(a, b, c)$ | **Área** | **Parte livre de quadrados** |
|---|---|---|---|---|
| 1 | 2 | (3, 4, 5) | 6 | 6 |
| 1 | 4 | (15, 8, 17) | 60 | 15 |
| 1 | 6 | (35, 12, 37) | 210 | 210 |
| 1 | 8 | (63, 16, 65) | 504 | 126 |
| 2 | 3 | (5, 12, 13) | 30 | 30 |
| 2 | 5 | (21, 20, 29) | 210 | 210 |
| 2 | 7 | (45, 28, 53) | 630 | 70 |
| 3 | 4 | (7, 24, 25) | 84 | 21 |
| 4 | 5 | (9, 40, 41) | 180 | 5 |

Fonte: CONRAD. K. (2008).

Convém retomar que para satisfazer o Teorema 3.2.3 os $m$, $n$ que geram ternos pitagóricos devem ser escolhidos tais que $n < m$, $mdc(m, n) = 1$ e $m \not\equiv n \pmod 2$.

Assim, os números que aparecem na última coluna da Tabela 1 além de serem inteiros livres de quadrados, são números congruentes, ou seja, são áreas de triângulos retângulos de lados racionais. E tais triângulos são facilmente obtidos analisando esta tabela, por exemplo, para obter um triângulo racional de área 5, basta notar que 5 aparece como a parte livre de quadrados do 180, que é a área de um triangulo retângulo representado pelo terno pitagórico $(9, 40, 41)$, assim como $180 = 5 \cdot 6^2$, então basta dividir todos os lados do terno em questão por 6, obtendo o triângulo $(3/2, 20/3, 41/6)$ de área igual a 5. Naturalmente que a Tabela 1 pode ser estendida à medida que aumentamos o valor da soma $m+n$.

Embora útil para gerar exemplos, o método de construção de números congruentes a partir dos ternos pitagóricos não é sistemático. A análise da Tabela 1 revela deficiências claras: os resultados não surgem em uma ordem aparente e um número pode aparecer mais de uma vez, como é o caso do 210. Consequentemente, não é possível garantir quando, ou mesmo se um número específico vai aparecer a medida que estendemos a tabela, o que torna esta abordagem inadequada para determinar se um dado inteiro é ou não congruente.

Podemos ver que a tabela em questão não fornece um método prático ao tomarmos o 53 como exemplo. O 53 é um número congruente, porém a primeira vez que ele aparece na tabela é quando a estendemos de modo a aparecer $m = 1873180325$ e $n = 1158313156$, tais valores geram o terno pitagórico $(2167115162604425289, 4339458828015711400, 4850493897329785961)$, cuja a área deste triângulo é igual a $53 \cdot 2978556542849787902$, valores nem um pouco práticos.

Outro resultado que ilustra a complexidade do problema dos números congruentes é o caso do número 157. Apesar de ser um número relativamente pequeno, o triângulo retângulo racional $(a, b, c)$ que tem área 157 é dado pelos seguintes valores:

$$a = \frac{411340519227716149383203}{21666555693714761309610},$$

$$b = \frac{6803298487826435051217540}{411340519227716149383203},$$

$$c = \frac{224403517704336969924557513090674863160948472041}{8912332268928859588025535178967163570016480830}.$$

A demonstração de que 157 é um número congruente deve-se ao matemático americano D. B. Zagier (Koblitz, 1993). Sua congruência foi provada não pela descoberta de um triângulo, mas de maneira teórica. Zagier demonstrou a existência de uma solução utilizando

ferramentas avançadas, como a teoria das formas modulares, no contexto da célebre Conjectura de Birch e Swinnerton-Dyer — conceitos que conectam o problema a teoria das curvas elípticas, tema que abordaremos no Capítulo 5. Somente após esta garantia teórica foi possível que especialistas em computação, como John E. Cremona, utilizassem algoritmos para finalmente determinar e exibir os lados deste triângulo de área igual a 157 (Cremona, 1997).

## 3.4 Fermat e os números congruentes

Durante o século XIII, Fibonacci discutiu sobre a congruência de diversos números inteiros, ele provou que 7 é um número congruente, mas apenas afirmou que o 1 não é congruente, tal afirmação só veio a ser demonstrada no século XVII por Fermat. Este é um dos principais resultados referentes a números não congruentes, e veremos o porquê nesta seção.

**Teorema 3.4.1.** *Fermat (1640). O número 1 não é congruente.*

*Demonstração.* Suponha que 1 seja um número congruente, ou seja, existe pelo menos uma tripla de números racionais positivos $(a, b, c)$ tais que $a^2 + b^2 = c^2$ e $(1/2)ab = 1$.

Daí, para qualquer escolha $(a, b, c)$ que determinem um triângulo retângulo de área 1, podemos tomar o produto de seus lados por um fator $m$ — o mínimo múltiplo comum dos denominadores — para obter um triângulo de lados inteiros $(a', b', c')$, com área igual a um quadrado perfeito; $m^2$. O conjunto de todas essas possíveis áreas quadradas é não vazio e, pelo *Princípio da Boa Ordenação*, admite um elemento mínimo. Assim, podemos assumir, sem perda de generalidade, que estamos trabalhando com um triângulo retângulo de lados inteiros cuja área é o menor quadrado perfeito possível dentre todas as soluções. Tal triângulo não necessariamente é único, assim como ocorre com o 210 na Tabela 1, porém, a existência de ao menos uma dessas soluções já é suficiente.

Seja então $(a', b', c')$ um terno pitagórico primitivo (sabe-se que é primitivo pela minimalidade da área), então pelo Teorema 3.2.3 de Euclides, existe um par de inteiro $p$ e $q$ coprimos e de paridades distintas, tais que:

$$a' = p^2 - q^2, \quad b' = 2pq, \quad c' = p^2 + q^2.$$

Como a área $m^2 = (1/2)a'b'$, temos:

$$m^2 = \frac{2pq(p^2-q^2)}{2} \quad \Rightarrow \quad m^2 = pq(p-q)(p+q).$$

Ora, $p$ e $q$ são coprimos de paridades distintas, então os quatro fatores de $m^2$ da última igualdade acima, também são coprimos dois a dois, logo, pelo Lema 3.2.2 só geram um quadrado perfeito se cada um destes fatores for por si só um quadrado perfeito. Assim temos:

$$p = x^2, \quad q = y^2, \quad p-q = z^2, \quad p+q = w^2,$$

onde $x$, $y$, $z$ e $w$ são inteiros positivos. Usando estas igualdades, podemos obter que:

$$(w+z)^2 + (w-z)^2 = (2x)^2.$$

Logo $(w+z, w-z, 2x)$ formam um terno pitagórico, e o triangulo retângulo formado tem área $\frac{1}{2} \cdot (w+z)(w-z) = q = y^2$, o que é uma contradição, pois o triângulo $(a', b', c')$ de área $m^2$ tinha área minimal igual a um quadrado perfeito, e $y^2 = q < m^2$. Portanto 1 não é um número congruente. ■

Com um raciocínio análogo ao utilizado na demonstração do teorema anterior, prova-se que os números 2 e 3 também não são congruentes. Embora não haja um registro explícito dessas demonstrações nas obras de Fermat, a autoria desses resultados é comumente atribuída a ele. Provaremos no Teorema 3.4.4 deste capítulo que 2 não é congruente. No próximo capítulo demonstraremos que 3 não é congruente, mais precisamente, que nenhum $p$ primo, tal que $p \equiv 3 \pmod 8$ é congruente.

Como consequência direta do Teorema 3.4.1, obtemos um importante resultado, conhecido como o triângulo retângulo de Fermat.

**Corolário 3.4.2.** *(O Triângulo Retângulo de Fermat) Nenhum número que seja um quadrado de um número racional é área de um triângulo de lados racionais.*

*Demonstração.* Suponha que exista um triângulo retângulo de lados racionais definido pelo terno $(a, b, c)$, com $a^2 + b^2 = c^2$ cuja sua área seja $(1/2)ab = q^2$, para algum $q \in \mathbb{Q}$. Consideremos o seguinte triângulo semelhante a $(a, b, c)$:

$$a' = \frac{a}{q}, \quad b' = \frac{b}{q}, \quad c' = \frac{c}{q}.$$

O triângulo retângulo $(a', b', c')$ tem área igual a:

$$\frac{1}{2}a'b' = \frac{1}{2}\frac{ab}{qq} = \left(\frac{1}{2}ab\right)\cdot\frac{1}{q^2} = \frac{q^2}{q^2} = 1.$$

Ora, mas neste caso o triângulo retângulo $(a', b', c')$ tem lados racionais e área igual a 1, e portanto 1 seria um número congruente, o que é uma contradição pelo Teorema 3.4.1. Logo não existe nenhum triângulo retângulo de lados racionais com área igual a um racional quadrado. ■

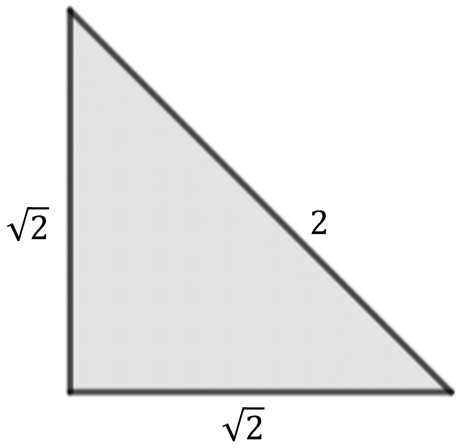
Mais precisamente o fato de o 1 não ser congruente e o Corolário 3.4.2 nos dizem que nenhum racional quadrado é um número congruente.

Adicionalmente, o Teorema 3.4.1 pode ser aplicado para fornecer uma demonstração para um resultado clássico da matemática: a irracionalidade de $\sqrt{2}$.

**Corolário 3.4.3.** *$\sqrt{2}$ não é um número racional.*

*Demonstração.* Suponha que $\sqrt{2} \in \mathbb{Q}$, neste caso, o triângulo retângulo representado na Figura 3 a seguir tem lados racionais. Este triângulo é retângulo (verifica-se por Pitágoras) e tem área igual a $(1/2)\cdot\sqrt{2}\cdot\sqrt{2} = 1$. Ora, se $\sqrt{2}$ é racional, então temos um triângulo retângulo de lados racionais cuja a área é igual a 1, ou seja, 1 é um número congruente. Contradição pelo Teorema 3.4.1. Logo $\sqrt{2}$ não é um número racional.

Figura 3 – Triângulo retângulo de área 1




Fonte: Elaborado pelo autor (2025).

■

**Teorema 3.4.4.** *2 não é um número congruente.*

*Demonstração.* Suponha que exista pelo menos um triângulo retângulo racional $(a, b, c)$ de área 2. Seja $d$ o mínimo múltiplo comum dos denominadores de $(a, b, c)$, multiplicando tais lados por $d$ obtemos um triângulo $(a', b', c')$ de lados inteiros e área $2d^2$. Dentre todos os triângulos com tais propriedade, pelo *Principio da Boa Ordem*, podemos tomar aquele cuja $d$ seja o menor possível. Assim temos:

$$a'^2 + b'^2 = c'^2 \quad \text{e} \quad a'b' = 4d^2.$$

Como $d$ é o menor possível, então o terno pitagórico $(a, b, c)$ é primitivo e podemos parametriza-lo. Logo existem $p$ e $q$ coprimos e de paridades distintas, tais que $a = p^2 - q^2$, $b = 2pq$ e $c = p^2 + q^2$. Onde temos que:

$$a'b' = 4d^2 \quad \Rightarrow \quad pq(p+q)(p-q) = 2d^2.$$

Como $p$, $q$, $p+q$ e $p-q$ são dois a dois coprimos (com um deles par), e o produto da equação acima é o dobro de um quadrado, então, novamente pelo Lema 3.2.2, cada um dos termos são quadrados, a exceção do termo par (sem perda de generalidade, digamos $p$) que será o dobro de um quadrado perfeito. Deste modo temos:

$$p = 2x^2, \quad q = y^2, \quad p+q = z^2, \quad p-q = w^2.$$

Logo tempos que:

$$2x^2 + y^2 = z^2 \quad \text{e} \quad 2x^2 - y^2 = w^2.$$

Somando as duas equações acima, obtemos que $w^2 + z^2 = 4x^2 = (2x)^2$, ou seja $(w, z, 2x)$ definem um terno pitagórico.

É fácil ver que como a hipotenusa deste terno é par, então $z$ e $w$ são ambos pares (basta analisar a congruência módulo 4 em $w^2 + z^2 = 4x^2$), e consequentemente $w^2$ e $z^2$ também são pares. Absurdo, dado que $w^2 = p - q$ e $z^2 = p + q$, onde $p$ e $q$ tem paridades distintas. Logo 2 não é um número congruente. ■

Outro importante resultado sobre incongruência refere-se ao matemático italiano Angelo Genocchi, um dos primeiros matemáticos a provar que toda uma classe de números não é congruente. Genocchi provou que nenhum primo $p$, tal que $p \equiv 3 \pmod 8$ é um número congruente. Como mencionado, apresentaremos o argumento de Genocchi no próximo capítulo.

A análise dos números congruentes sob a perspectiva geométrica, fundamentada nos ternos pitagóricos, revela a fascinante profundidade que um problema de enunciado simples pode conter. Embora o método de Euclides nos permita gerar uma infinidade de exemplos, ele também expõe sua própria limitação: a falta de um critério sistemático. Como vimos nos casos de 53 e 157, a busca por triângulos pode se tornar impraticável. Fica claro, portanto, que, apesar de elegante, a abordagem geométrica por si só é insuficiente para responder de maneira definitiva se um número qualquer é ou não congruente, o que motiva a busca por outras formas de atacar o problema dos números congruentes, este trabalho se dedicará a isto nos capítulos que se seguem.

# 4 PROGRESSÕES ARITMÉTICAS E A ESSÊNCIA DA CONGRUÊNCIA

Este capítulo investiga a essência por trás do nome "número congruente", retornando às suas origens algébricas. Conforme abordado no Capítulo 2, foi a perspectiva popularizada por Fibonacci em seu *Livro dos Quadrados* publicado em 1225, focada em progressões aritméticas, que historicamente conferiu o nome ao problema. A "congruência" evocada no título refere-se à relação entre três quadrados racionais que estão em uma progressão de razão $n$, mais precisamente, estes três quadrados são congruentes modulo $n$. Esta formulação, anterior à interpretação geométrica, não apenas revela a profundidade histórica do tema, mas também revela a aritmética por trás do problema.

## 4.1 Números congruentes e progressões aritméticas

**Definição 4.1.1.** *Um número inteiro n é dito congruente se existir $a \in \mathbb{Q}$, tal que $a^2+n$ e $a^2-n$ sejam ambos racionais quadrados.*

Note que, se a definição acima for válida, então estamos dizendo que existem três números racionais quadrados $(a^2-n, a^2, a^2+n)$ que estão em uma progressão aritmética de razão $n$, e além disso, como dito, tais números são congruentes módulo $n$, é deste fato que decorre o emprego do nome de "número congruente" a números com essa propriedade.

Segundo Fibonacci a definição acima é equivalente a Definição 1.0.1 inicialmente apresentada, provaremos isso no seguinte teorema.

**Teorema 4.1.2.** *Seja $n > 0, n \in \mathbb{Q}$. Existe uma correspondência biunívoca entre triângulos retângulos racionais com área n, e três racionais quadrados em progressão aritmética de razão n. Ou seja, os conjuntos:*

$$\{(a,b,c) \in \mathbb{Q}^3 \mid a^2+b^2=c^2, (1/2)ab=n\}, \quad \{(r,s,t) \in \mathbb{Q}^3 \mid s^2-r^2=n, t^2-s^2=n\}.$$

*São equivalentes, e a correspondência entre eles é dada por:*

$$(a,b,c) \mapsto \left(\frac{(b-a)}{2}, \frac{c}{2}, \frac{b+a}{2}\right), \quad (r,s,t) \mapsto (t-r, t+r, 2s).$$

*Demonstração.* Primeiramente, veja que dizer que $(r,s,t)$ são tais que $s^2-r^2=n$ e $t^2-s^2=n$ significa que $(r^2, s^2, t^2)$ são três racionais quadrados em progressão aritmética de razão $n$, pois $r^2=s^2-n$ e $t^2=s^2+n$, logo tomando $s=a$, encontramos nosso racional procurado, satisfazendo a segunda definição (Definição 4.1.1) para o problema dos números congruentes.

($\Rightarrow$) Suponha que $(a, b, c)$ sejam três racionais positivos tais que $a^2+b^2=c^2$ e $\frac{1}{2}ab=n$. Defina:

$$r=\frac{b-a}{2}, \quad s=\frac{c}{2}, \quad t=\frac{b+a}{2}.$$

Vamos provar que $(r, s, t)$ satisfaz $s^2-r^2=n$ e $t^2-s^2=n$.

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

Como $c^2=a^2+b^2$, temos:

$$s^2-r^2=\frac{a^2+b^2-(b^2-2ab+a^2)}{4}=\frac{2ab}{4}=\frac{1}{2}ab=n.$$

De maneira análoga, em $t^2-s^2$, temos que:

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

E, novamente substituindo $c^2$ por $a^2+b^2$, obtemos:

$$t^2-s^2=\frac{(b^2+2ab+a^2)-a^2-b^2}{4}=\frac{2ab}{4}=\frac{1}{2}ab=n.$$

Logo a tripla de racionais $(r, s, t)$ definidos a partir de $(a, b, c)$ satisfaz $s^2-r^2=n$ e $t^2-s^2=n$, portanto $(r^2, s^2, t^2)$ definem um tripla de racionais quadrados que estão em progressão aritmética de razão $n$.

($\Leftarrow$) Vamos tomar agora uma tripla de racionais $(r, s, t)$, com $s^2-r^2=n$ e $t^2-s^2=n$, vamos definir $(a, b, c)$ como:

$$a=t-r, \quad b=t+r, \quad c=2s.$$

Vamos verificar que $(a, b, c)$ satisfaz:

$$a^2+b^2=c^2 \quad \text{e} \quad \frac{1}{2}ab=n.$$

Primeiramente temos que:

$$\begin{aligned} a^2+b^2 &= (t-r)^2+(t+r)^2 \\ &= (t^2-2tr+r^2)+(t^2+2tr+r^2) \\ &= 2t^2+2r^2 \\ &= 2(t^2+r^2). \end{aligned}$$

Ora, mas por definição, $s^2 - r^2 = n \Rightarrow r^2 = s^2 - n$, assim como $t^2 - s^2 = n \Rightarrow t^2 = s^2 + n$, logo:

$$\begin{aligned} a^2 + b^2 &= 2(t^2 + r^2) \\ &= 2(s^2 + n + s^2 - n) \\ &= 4s^2 \\ &= (2s)^2 \\ &= c^2. \end{aligned}$$

Resta verificar que $(1/2)ab = n$, vejamos:

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

Veja que somando $s^2 - r^2 = n$ com $t^2 - s^2 = n$ obtemos $t^2 - r^2 = 2n$, assim concluimos que:

$$\frac{1}{2}ab = \frac{1}{2}(t^2 - r^2) = \frac{1}{2}(2n) = n.$$

Como queríamos. Portanto a tripla $(a, b, c)$ definidos como indicado a partir dos racionais $(r, s, t)$ satisfaz $a^2 + b^2 = c^2$ e $(1/2)ab = n$.

Por fim, note que, como as correspondências entre os ternos $(a, b, c)$ e $(r, s, t)$ utilizam apenas operações fundamentais, então $(a, b, c) \in \mathbb{Q}^3$ se, e somente se $(r, s, t) \in \mathbb{Q}^3$. Além de que pela forma como foi definida tal correspondência preserva a positividade e monotonicidade dos números, ou seja, $0 < a < b < c$ se, e somente se $0 < r < s < t$. Portanto a correspondência é válida e está bem definida nos racionais. ■

Assim, pelo teorema acima, de fato temos que as definições 1.0.1 e 4.1.1 são equivalentes. Portanto temos agora duas maneiras de mostrar que um número racional $n$ é congruente; encontrar um triângulo retângulo racional de área $n$, ou encontrar um $a$ racional, tal que $a^2 - n$ e $a^2 + n$ sejam racionais quadrados. Pelo Teorema 4.1.2 podemos olhar para alguns números congruentes já conhecidos por meio de triângulos retângulos racionais apresentados de maneira que eles sejam razões de progressões aritméticas de três racionais quadrados.

**Exemplo 4.1.3.** Já sabemos que o 6 é congruente pois ele é a área do triângulo definido pelo terno $(3, 4, 5)$, mas aplicando a correspondência do Teorema 4.1.2 obtemos $(r, s, t) = (1/2, 5/2, 7/2)$, ou seja, 6 é um número congruente pois ele é a razão da progressão aritmética de três racionais quadrados; $1/4$, $25/4$ e $49/4$.

**Exemplo 4.1.4.** Já observamos pela Tabela 1 que 5 é um número congruente, obtido pela parte livre de quadrados do $180 = 5 \cdot 6^2$ que é a área do triângulo determinado pelo terno pitagórico $(9, 40, 41)$, simplificando tal terno por 6, obtemos o terno de números racionais $(3/2, 20/3, 41/6)$ que gera um triângulo retângulo de área 5. Aplicando a correspondência do Teorema 4.1.2, obtemos o terno $(r, s, t) = (31/12, 41/12, 49/12)$, logo os racionais quadrados $(31/12)^2$, $(41/12)^2$ e $(49/12)^2$ formam uma progressão aritmética de diferença comum igual a 5.

**Exemplo 4.1.5.** Outra observação interessante é que como mostramos no Teorema 3.4.1 que 1 não é congruente, então conectando-o com Teorema 4.1.2, sabemos que o sistema de equações abaixo:

$$\begin{cases} s^2 - r^2 = 1 \\ t^2 - s^2 = 1. \end{cases}$$

É impossível para $r, s, t \in \mathbb{Q}$.

O resultado apresentado no exemplo acima não é valido apenas para quando as equações são igual a 1, mas sim para qualquer valor que não seja um número congruente. Assim por exemplo, como 4 (quadrado perfeito) também não é um número congruente, então não existem três números racionais quadrados que tenham uma diferença comum igual a 4.

## 4.2 O argumento de Genocchi

O Italiano Angelo Genocchi (1817 - 1889) foi um dos primeiros matemáticos a provar que uma classe inteira de números não é congruente. Genocchi publicou em 1885 um trabalho (posteriormente traduzido para o inglês por Brett Hemenway) onde mostrou que se $p$ é um número primo, tal que $p \equiv 3 \pmod 8$, então $p$ não é um número congruente.

Usaremos na demonstração a caracterização que Fibonacci deu para números congruentes. Um dos quatro números racionais; $a$, $b$, $a+b$ e $a-b$ é congruente se os outros três forem racionais quadrados. Essencialmente este argumento é equivalente o a Definição 4.1.1 apresentada no início deste capítulo.

**Teorema 4.2.1** (Genocchi)**.** *Seja p um número primo, tal que* $p \equiv 3 \pmod 8$*, então p não é um número congruente.*

*Demonstração.* Suponha que $n$ seja um número congruente. A quatro casos a se considerar na caracterização de Fibonacci.

- Caso 1: $a$ é congruente.

$$a = nf^2, b = g^2, a+b = h^2, a-b = k^2.$$

Assim, temos:

$$a^2 - b^2 = (a+b)(a-b) = (hk)^2 \quad \Rightarrow \quad a^2 = b^2 + (hk)^2.$$

Portanto $(b, hk, a)$ definem um terno pitagórico. Sem perda de generalidade, vamos sempre supor que os ternos pitagóricos obtidos sejam primitivos (do contrário, bastaria reduzir os termos do terno por seu *mdc*). Logo, por Euclides, existem inteiros $r$ e $s$, com $r > s$, coprimos e de paridades distintas, tal que $a = r^2 + s^2$ e $b = r^2 - s^2$ ou $b = 2rs$. Deste modo, temos:

$$g^2 = b = r^2 - s^2 = (r+s)(r-s) \quad \text{ou} \quad g^2 = b = 2rs.$$

No primeiro caso, como $r$ e $s$ são coprimos, então se $r+s$ e $r-s$ são fatores de um quadrado $g^2$, então eles também são quadrados, digamos; $r+s = \alpha^2$ e $r-s = \beta^2$. Isolando $r$ e $s$ em função de $\alpha$ e $\beta$ e substituindo em $nf^2 = a = r^2 + s^2$, obtemos:

$$\alpha^4 + \beta^4 = 2nf^2. \tag{4.1}$$

E, no segundo caso, obtemos:

$$\alpha^4 + 4\beta^4 = nf^2. \tag{4.2}$$

- Caso 2: $a-b$ é congruente.

$$a = f^2, b = g^2, a+b = h^2, a-b = nk^2.$$

Já obtemos diretamente que $f^2 + g^2 = h^2$. Ou seja, que $(f, g, h)$ determinam um terno pitagórico, com $(f, g) = (r^2 - s^2, 2rs)$ ou $(f, g) = (2rs, r^2 - s^2)$. Partindo então de $f^2 - g^2 = nk^2$, temos:

$$(r^2 - s^2)^2 - (2rs)^2 = \pm nk^2.$$

Onde, desenvolvendo, temos:

$$r^4 - 6r^2s^2 + s^4 = \pm nk^2. \tag{4.3}$$

- Caso 3: $a+b$ é congruente.

$$a = f^2, b = g^2, a+b = nh^2, a-b = k^2.$$

Temos que $f^2 = g^2 + k^2$. Assim, $(k, g, f)$ definem um terno pitagórico. E, parametrizando, temos $f = r^2 + s^2$ e g = $r^2 - s^2$ ou $g = 2rs$. Substituindo na equação:

$$f^2 + g^2 = nh^2,$$

obtemos:

$$(r^2+s^2)^2 + (r^2-s^2)^2 = nh^2 \quad \text{ou} \quad (r^2+s^2)^2 + (2rs) = nh^2.$$

No primeiro caso, temos:

$$2r^4 + 2s^4 = nh^2. \tag{4.4}$$

E, no segundo caso, obtemos:

$$r^4 + 6r^2s^2 + s^4 = nh^2. \tag{4.5}$$

- Caso 4: $b$ é congruente.

$$a = f^2, b = ng^2, a+b = h^2, a-b = k^2.$$

Deixamos este caso por último, pois aqui somos forçados a seguir por um caminho diferente dos três primeiros casos. Visto que as equações $f^2 + ng^2 = h^2$ e $f^2 - ng^2 = k^2$ não definem ternos pitagóricos. Mas, veja que elas garantem que $n$ é um número congruente, basta dividi-las por $g^2$ para se adequar aos moldes da Definição 4.1.1. Ora, se $n$ é congruente, então existem $x_1, x_2, x_3 \in \mathbb{Q}$, tais que:

$$x_2^2 - n = x_1^2 \quad e \quad x_2^2 + n = x_3^2.$$

Como $x_1, x_2$ e $x_3$ são números racionais, podemos escrevê-los na forma de fração. Em particular, podemos encontrar um menor inteiro $q$, tal que, $x_i = \frac{p_i}{q}$, onde cada $p_i \in \mathbb{Z}$. Assim podemos reescrever as equações anteriores como:

$$p_2^2 - nq^2 = p_1^2 \quad e \quad p_2^2 + nq^2 = p_3^2.$$

Isolando $p_2^2$ nas duas equações, e igualando, obtemos:

$$p_3^2 - p_1^2 = 2nq^2.$$

Logo $p_1 \equiv p_3 \pmod 2$. Deste modo, podemos definir os seguintes inteiros:

$$r_1 = \frac{p_3 + p_1}{2} \quad e \quad r_2 = \frac{p_3 - p_1}{2}.$$

Onde tem-se:

$$r_1^2 + r_2^2 = p_2^2.$$

Assim, temos o terno pitagórico $(r_1, r_2, p_2)$, que pode ser parametrizado como:

$$r_1 = 2ab, \quad r_2 = a^2 - b^2, \quad p_2 = a^2 + b^2.$$

Além disso, como $2r_1r_2 = nq^2$, substituindo nossa parametrização em $r_1$ e $r_2$, temos:

$$nq^2 = 4ab(a-b)(a+b).$$

Ora, mas como $n$ é congruente, pela caracterização de Fibonacci, sabemos que podemos encontrar inteiros $a$, $b$, $a+b$ e $a-b$, tais que três deles sejam quadrados e $n$ divida o quarto. Assumindo que não estamos em um dos três casos anteriores, se $n$ for primo, devemos ter $n \mid b$. Logo:

$$f^2 + ng^2 = h^2 \quad \text{e} \quad f^2 - ng^2 = k^2.$$

Assim, nessas equações, temos:

$$nq^2 = 4f^2k^2ng^2(ng^2 + f^2).$$

Portanto, $ng^2 < nq^2$, absurdo, dada a minimalidade de $q$. Logo $n$ não é primo neste caso. Resta mostrar que $n$ também não pode ser primo nos três primeiros casos. Reunindo as equações de (4.1) a (4.5) e unificando as notações, temos que:

$$2nf^2 = r^4 + s^4, \tag{6.6}$$

$$2nf^2 = r^4 + 4s^4, \tag{6.7}$$

$$\pm nf^2 = r^4 - 6r^2s^2 + s^4, \tag{6.8}$$

$$nf^2 = r^4 + 6r^2s^2 + s^2, \tag{6.9}$$

$$nf^2 = 2r^4 + 2s^4. \tag{6.10}$$

Se $p \equiv 3 \pmod 8 \mid n$, então, tomando todos os restos modulo $p$ nas equações acima, vamos chegar que as equações (6.6), (6.7) e (6.10) são congruentes a $-1$ modulo $p$. Portanto, impossíveis, pois $-1$ não é um quadrado modulo $p$. Já, para a equação (6.8), temos que:

$$nf^2 = r^4 - 6r^2s^2 + s^4 = (r^2 - 3s^2)^2 - 2(2s^2)^2,$$

ou

$$nf^2 = -r^4 + 6r^2s^2 - s^4 = (r^2 + s^2)^2 - 2(r^2 - s^2)^2.$$

Em ambos os casos (estamos analisando dois casos, pois a equação (6.8) inicia com $\pm nf^2$), para que a congruência a zero modulo $p$ de $nf^2$ seja obedecida, deveríamos ter que 2 é um quadrado modulo $p$, absurdo. Por último, na equação (6.9), temos:

$$nf^2 = r^4 + 6r^2s^2 + s^2 = (r^2 + 3s^2)^2 - 2(2s^2)^2.$$

Novamente, como 2 não é um quadrado modulo $p$, tal equação não tem solução. Portanto, para todos os possíveis casos, concluímos que se $p \equiv 3 \pmod 8$, $p$ primo, então $p$ não é um número congruente. ■

# 5 CURVAS ELÍPTICAS

Nos capítulos anteriores, estabelecemos que um número $n$ é congruente se for a área de um triângulo retângulo de lados racionais, uma condição que se provou equivalente à existência de três quadrados racionais em progressão aritmética de razão $n$. Neste capítulo, a investigação avança para uma terceira e poderosa formulação do problema, revelando sua profunda conexão com as soluções racionais de uma única equação: $y^2 = x^3 - n^2x$, denominada *curva elíptica*. Embora esta curva possua três soluções racionais triviais — a saber, $(0,0)$, $(n,0)$ e $(-n,0)$ —, o interesse recai sobre as soluções racionais não triviais com $y \neq 0$. Mas, antes de explorar essa equivalência, definiremos formalmente o conceito de curvas elípticas.

**Definição 5.0.1.** *Uma curva elíptica é uma curva algébrica plana definida por uma equação cúbica da forma*

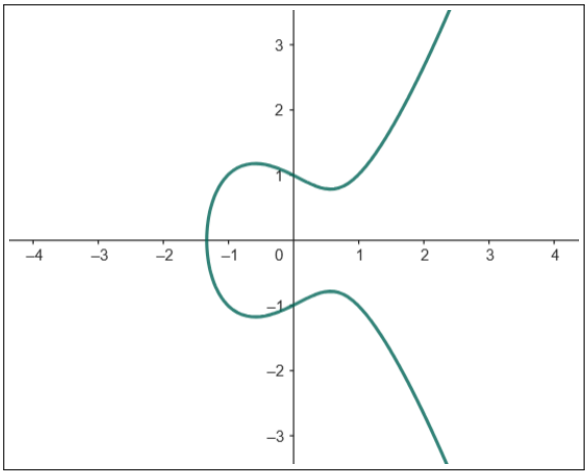
$$E : y^2 = x^3 + ax + b, \quad (a, b \in \mathbb{Z})$$

*com* $\Delta = 4a^3 + 27b^2 \neq 0$.

O número $\Delta$ é o descriminante do polinômio cubico $f(x) = x^3 + ax + b$, e restringir a condição de que $\Delta \neq 0$ garante que $f(x)$ não tem raízes repetidas em $\mathbb{C}$, isso garante que a curva não tenha "bicos" ou pontos de autointerseção, tornando a curva derivável em todos os pontos. Em termos geométricos e algébricos, isso assegura que a curva seja suave, e portanto, uma curva elíptica válida. Veremos abaixo alguns exemplos de curvas elípticas.

**Exemplo 5.0.2.** A equação cúbica $y^2 = x^3 - x + 1$ define uma curva elíptica, pois $a = -1$ e $b = 1$, consequentemente $\Delta = 4 \cdot (-1)^3 + 27 \cdot (1)^2 = 23 \neq 0$, esta curva define o gráfico abaixo:

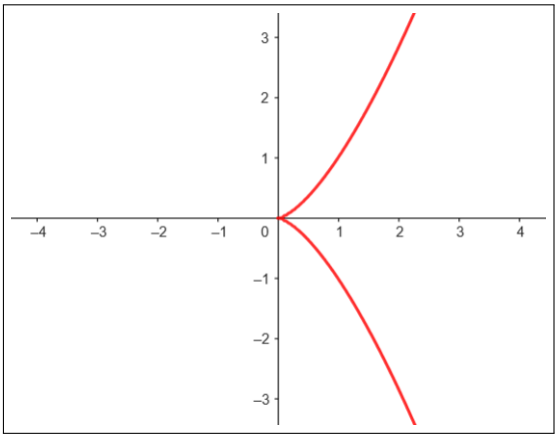
Figura 4 – Gráfico de $y^2 = x^3 - x + 1$




Fonte: Elaborado pelo autor (2025).

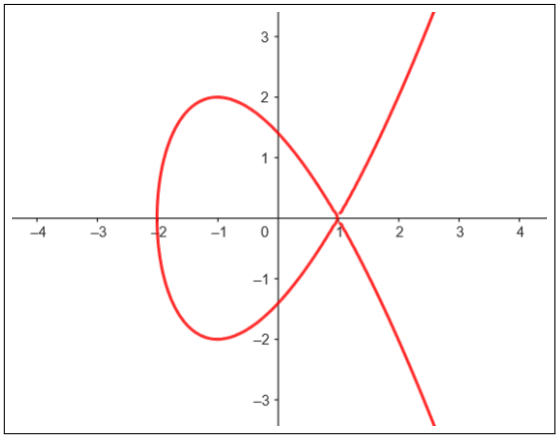
**Exemplo 5.0.3.** Porém nem todas as equações cúbicas no modelo $y^2 = x^3 + ax + b$ vão definir curvas elípticas, é o caso das equações $y^2 = x^3$ e $y^2 = x^3 - 3x + 2$, tais equações definem os gráficos representados nas seguintes figuras.

Figura 5 – Gráfico de $y^2 = x^3$




Fonte: Elaborado pelo autor (2025).

Figura 6 – Gráfico de $y^2 = x^3 - 3x + 2$




Fonte: Elaborado pelo autor (2025).

Em ambas as figuras acima, temos curvas em que $\Delta = 0$, ou seja, curvas que não são elípticas. Na Figura 5 a esquerda temos um "bico" sendo formado no ponto $(0, 0)$, isso ocorre pois $f(x) = x^3$ tem raiz tripla $x = 0$. Já a curva da Figura 6 a direita tem um ponto de autointerseção em $x = 1$, isso ocorre pois $f(x) = x^3 - 3x + 2 = (x-1)^2 \cdot (x+2)$, ou seja, $f(x)$ tem raiz dupla em $x = 1$. Nos seus respectivos pontos críticos citados, tais curvas não são diferenciáveis.

Assim, o exemplo acima nos mostra que curvas cúbicas do tipo $y^2 = x^3 + ax + b$ não são elípticas se o polinômio $f(x)$ possuir alguma raiz com multiplicidade maior que 1 (raiz repetida).

## 5.1 Adição de pontos

Seja $E(\mathbb{Q})$ o conjuntos dos pontos $(x, y)$ da curva $E$, tal que $(x, y) \in \mathbb{Q}^2$, junto de um ponto $\mathcal{O}$ no infinito, este ponto $\mathcal{O}$ deve ser considerado como um ponto que esta em ambas as "pontas" de uma reta vertical (também é muito comum utilizar o simbolo de $\infty$ para representar este ponto). Podemos definir uma operação de adição com propriedades muito interessantes em $E(\mathbb{Q})$. Primeiramente daremos uma descrição geométrica para esta operação de adição.

**Descrição geométrica**. Sejam $P$ e $Q$ dois pontos sobre $E(\mathbb{Q})$, então a soma $P + Q$ é um ponto que pertence a $E(\mathbb{Q})$, onde $P + Q$ é obtido da seguinte forma:

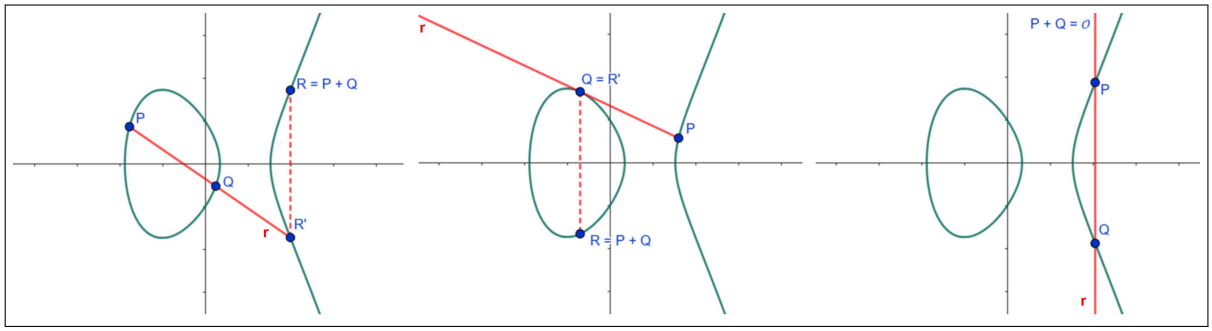
Se $P \neq Q$, consideraremos a reta $r$ que passa por $P$ e $Q$ em $\mathbb{R}^2$. Se $r$ não é uma reta vertical (não é paralela ao eixo $y$), chamaremos de $R'$ o terceiro ponto de interseção da reta $r$ com a curva $E$. A soma $P+Q$ é definida como o ponto $R$, onde $R$ é a reflexão de $R'$ em relação ao eixo $x$.

Note que mesmo que a reta não seja vertical, pode ocorrer de não existir um terceiro ponto de interseção. Isso ocorre se a reta $r$ for tangente a curva em um dos pontos $P$ ou $Q$, neste caso, tomamos $R'$ como sendo o próprio ponto de tangencia.

Para que a operação de adição fique bem definida, no caso em que a reta $r$ seja vertical, ou seja, que $P$ e $Q$ sejam pontos opostos com relação ao eixo $x$, então considera-se $\mathcal{O}$ como o terceiro ponto de interseção da reta $r$ com a curva $E$, neste caso $P+Q=\mathcal{O}$.

Agora, no caso de $P=Q$ então a reta $r$ considerada sera a tangente a curva $E$ no ponto $P$, e $R'$ sera a interseção de $r$ com $E(\mathbb{Q})$, e como antes, tomemos $R=P+Q$ como sendo a reflexão de $R'$. A figura abaixo apresenta a visualização geométrica para alguns exemplos da soma $P+Q$ em diferentes disposições de $P$ e $Q$ sobre uma curva elíptica.

Figura 7 – Exemplos do comportamento geométrico da adição em curvas elípticas




Fonte: Elaborado pelo autor (2025).

Entendido o conceito de adição em curvas elípticas por meio da geometria, podemos agora defini-lo algebricamente, ou seja, podemos buscar as coordenadas do ponto $R$ obtido pela soma $P+Q$.

**Proposição 5.1.1** (*Descrição algébrica*)**.** *Dados dois pontos $P=(x_1,y_1)$ e $Q=(x_2,y_2)$ pertencentes a $E(\mathbb{Q})$ e $r: y=mx+c$ a reta que passa por estes dois pontos. Então, a soma $R=P+Q$ (conforme definida na "Descrição geométrica") também pertence a $E(\mathbb{Q})$, e suas coordenadas são dadas por:*

$$R=(m^2-(x_1+x_2),\, m[(x_1+x_2)-m^2]-c),\ \textit{onde}\ \begin{cases} m=\dfrac{y_2-y_1}{x_2-x_1},\ \textit{se } P\neq Q, \\ m=\dfrac{3x_1^2+a}{2y_1},\ \textit{se } P=Q. \end{cases}$$

*Demonstração.* Deixaremos de lado os casos triviais em que a reta que passa por $P$ e $Q$ é vertical (nestes casos a descrição geométrica já deixa clara a visualização de que $P+Q=\mathcal{O}$). Vamos calcular as cordeadas de $R=P+Q$. Seja então $y=mx+c$ as coordenadas da reta $r$ que passa pelos pontos $P$ e $Q$, temos dois casos a considerar:
*1ž caso*: $P\neq Q$, logo a reta $r$ é secante a curva e, portanto, $m=\dfrac{y_2-y_1}{x_2-x_1}\in\mathbb{Q}$.
*2ž caso*: $P=Q=(x_1,y_1)$, a reta $r$ é tangente a curva, e logo o coeficiente $m$ é obtido ao derivar $y^2=x^3+ax+b$ com relação a $x$ no ponto $P$, onde se obtêm $m=\dfrac{3x_1^2+a}{2y_1}\in\mathbb{Q}$.

Em ambos os casos, substituindo $y=mx+n$ na equação da cúbica temos:

$$(mx+c)^2=x^3+ax+b \quad \Rightarrow \quad x^3-m^2x^2+(a-2mc)x+b-c^2=0. \tag{5.1}$$

Ora, as soluções da igualdade acima são $x_1$, $x_2$ e $x_3$, e como o coeficiente líder na incógnita $x$ desta equação é 1, vale que $(x-x_1)(x-x_2)(x-x_3)=0$, expandindo temos:

$$x^3-(x_1+x_2+x_2)x^2+(x_1x_2+x_1x_3+x_2x_3)x-x_1x_2x_3=0. \tag{5.2}$$

Como os polinômios das equações (5.1) e (5.2) são iguais, então os coeficientes dos termos de mesmo grau são idênticos, comparando especificamente os coeficientes do termo de grau 2, obtemos:

$$-(x_1+x_2+x_3)=-m^2 \quad \Rightarrow \quad x_3=m^2-(x_1+x_2).$$

Aplicando então o valor de $x_3$ na equação da reta $r$:

$$y_3=mx_3+c \quad \Rightarrow \quad y_3=m[m^2-(x_1+x_2)]+c.$$

Finalmente, veja que as coordenadas $(x_3,y_3)$ obtidas referem-se ao terceiro ponto $R'$ onde a reta $r$ que passa por $P$ e $Q$ intersecta a curva $E(\mathbb{Q})$, porém como definido, o ponto $R$ dado por $R=P+Q$ é a reflexão do ponto $R'$, logo tem coordenadas $(x_3,-y_3)$. Portanto temos

$$R=(m^2-(x_1+x_2),m[(x_1+x_2)-m^2]-c),\ \text{onde}\ \begin{cases} m=\dfrac{y_2-y_1}{x_2-x_1},\ \text{se P}\neq\text{Q},\\ m=\dfrac{3x_1^2+a}{2y_1},\ \text{se P = Q}. \end{cases}$$

Com $x_1=x_2$ se $P=Q$. Como $c\in\mathbb{Q}$ (basta ver que $c=y_1-mx_1$, com $x_1$, $y_1$ e $m$ todos racionais), então as coordenadas do ponto $R$ são números racionais, logo $P+Q=R\in E(\mathbb{Q})$. ■

O resultado acima também seria valido para curvas elípticas definidas nos reais, ou seja, para $E(\mathbb{R})$. Mas como o objetivo principal deste trabalho é o estudo dos números congruentes, é suficiente analisar as curvas definidas sobre $\mathbb{Q}$.

## 5.2 Grupo abeliano

Nesta seção abordaremos um tópico cujas as demonstrações em sua totalidade estão fora do âmbito deste trabalho. No entanto, a sua importância e aplicação a teoria das curvas elípticas justificam sua menção. Mas antes, vamos definir o conceito de *grupo abeliano*.

**Definição 5.2.1.** *Um grupo abeliano (ou grupo comutativo) é um conjunto G com uma operação binaria $+$, tal que sejam validas as propriedades:*

1. ***Comutatividade:*** $a+b=b+a$;
2. ***Elemento neutro:*** *existe um elemento* $0 \in G$ *tal que* $a+0=a=0+a$;
3. ***Elemento inverso:*** *para todo* $a \in G$, *existe um elemento* $-a \in G$ *tal que* $a+(-a)=0$;
4. ***Associatividade:*** $(a+b)+c=a+(b+c)$.

Estabelecida a definição de grupo abeliano, podemos agora enunciar um dos resultados mais fundamentais da teoria das curvas elípticas: o conjunto de seus pontos racionais junto ao ponto $\mathcal{O}$ no infinito, quando munido de uma operação de adição, forma precisamente um grupo abeliano. Embora a demonstração completa deste teorema esteja fora do escopo deste trabalho, apresentaremos a seguir as ideias centrais que sustentam seu raciocínio.

**Teorema 5.2.2.** *O conjunto $E(\mathbb{Q})$ dos pontos racionais de uma curva E junto ao ponto $\mathcal{O}$ no infinito, com a operação de adição conforme definido na Seção 5.1, determina um grupo abeliano.*

*Demonstração.* Analisaremos se tal conjunto $E(\mathbb{Q})$ satisfaz cada um dos pontos que definem um grupo abeliano.

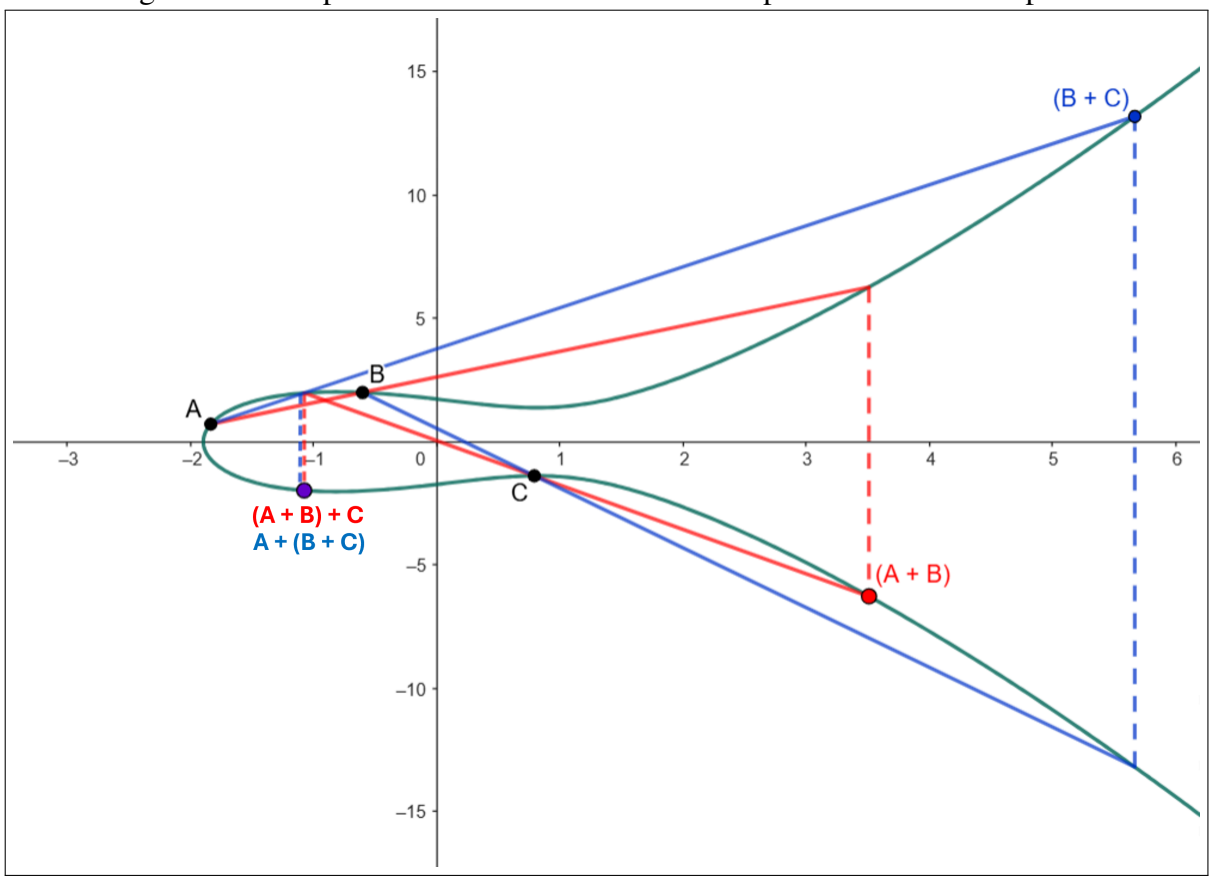
A *comutatividade* segue diretamente da demonstração geométrica dada, pois a reta que passa por dois pontos quaisquer é a mesma, independente da ordem que os pontos foram tomados.

Para o *elemento inverso*, seja $P=(x_1, y_1)$ um ponto que pertence a curva elíptica $E: y^2=x^3+ax+b$, então seu inverno (com relação ao eixo $x$), $-P=(x_1,-y_1)$, também pertence a $E$. E como a reta que passa por $P$ e $-P$ é vertical, então $P+(-P)=\mathcal{O}$ (e portanto $\mathcal{O}$ deve ser o elemento neutro)

De fato, $\mathcal{O}$ desempenha o papel de *elemento neutro*, pois da forma a qual foi definido, a reta que passa por $P$ e $\mathcal{O}$ é vertical, deste modo o terceiro ponto de interseção desta reta com a curva será $-P$, o qual reflete de volta no próprio $P$, assim, $P+\mathcal{O}=\mathcal{O}+P=P$.

Por fim, a *associatividade* da operação de adição conforme foi definida é um resultado nada trivial e com muitos casos a considerar. Como dito, isso foge do âmbito do trabalho em questão, ficaremos com a ideia geométrica de um dos possíveis casos na Figura 8 abaixo.

Figura 8 – Exemplo da associatividade da soma de pontos em curvas elípticas




Fonte: Elaborado pelo autor (2025).

■

## 5.3 A conexão entre curvas elípticas e números congruentes

Até o momento no presente capítulo, discutimos sobre como curvas elípticas são um objeto de estudo muito interessante da matemática. Porém, nosso trabalho se fundamenta nos números congruentes, então; onde está a relação entre números congruentes e curvas elípticas? É sobre isso que discutiremos nessa seção.

No decorrer deste trabalho definimos que um número $n$ é congruente se existe uma terna de números racionais $(a, b, c)$ que satisfazem as equação $(1/2)ab = n$, com $a^2 + b^2 = c^2$. Em seguida no Capítulo 4 vimos que tal situação é equivalente a encontrar um terno de números racionais positivos $(r, s, t)$ tais que $s^2 - r^2 = n$ e $t^2 - s^2 = n$. Veremos agora uma terceira

formulação para o problema dos números congruentes.

**Definição 5.3.1.** *Um número inteiro n é dito congruente se a curva elíptica definida pela equação* $E : y^2 = x^3 - n^2x$, *possui pelo menos um ponto racional* $(x, y)$ *com* $y \neq 0$.

Note que a equação $E$ da Definição 5.3.1 tem três soluções triviais; $(0, 0)$, $(n, 0)$ e $(-n, 0)$, todas com $y = 0$. Tais soluções existem independentemente da congruência de $n$, mas o que esta última definição afirma é que a congruência de $n$ é garantida pela existência de pontos racionais não triviais ($y \neq 0$) em $E$. Vale destacar que tal equação de fato define uma curva elíptica, pois nessas condições, os coeficientes $a$ e $b$ da curva são respectivamente $-n^2$ e 0, logo $\Delta = 4(-n^2)^3 + 27 \cdot 0^2 = -4n^6 = 0 \Leftrightarrow n = 0$, mas como estamos buscando os $n$ que possam ser números congruentes, já partimos de $n \neq 0$, logo $\Delta \neq 0$, satisfazendo assim as condições da Definição 5.0.1, portanto a equação em questão define precisamente uma curva elíptica.

É claro que definir números congruentes como na Definição 5.3.1 só faz sentido se esta definição for equivalente a algumas das duas definições já conhecidas (definições 1.0.1 e 4.1.1). De fato, demonstraremos a equivalência da Definição 5.3.1 com a existência de triângulos retângulos racionais de área $n$ com o teorema a seguir.

**Teorema 5.3.2.** *Seja* $n > 0$, *existe uma correspondência biunívoca entre os seguintes conjuntos:*

$$\{(a, b, c) \in \mathbb{Q}^3 \mid a^2 + b^2 = c^2, \frac{1}{2}ab = n\}, \quad \{(x, y) \in \mathbb{Q}^2 \mid y^2 = x^3 - n^2x, y \neq 0\}.$$

*As correspondências mutualmente inversas entre esses dois conjuntos são dadas por:*

$$(a, b, c) \longmapsto \left(\frac{nb}{c-a}, \frac{2n^2}{c-a}\right), \quad (x, y) \longmapsto \left(\frac{x^2 - n^2}{y}, \frac{2nx}{y}, \frac{x^2 + n^2}{y}\right).$$

*Demonstração.* Seja $(a, b, c)$ um terno de racionais tais que $a^2 + b^2 = c^2$ com $(1/2)ab = n$, $n > 0$, afirmamos que $\left(\frac{nb}{c-a}, \frac{2n^2}{c-a}\right)$ é uma solução da curva elíptica $y^2 = x^3 - n^2x$, onde, $c - a \neq 0$, pois $c - a = 0 \Rightarrow b = 0$ em $a^2 + b^2 = c^2$, mas deste modo teríamos $(1/2)ab = 0$, o que é um absurdo, dado que $n > 0$ por hipótese. Logo $\left(\frac{nb}{c-a}, \frac{2n^2}{c-a}\right)$ está bem definido, substituindo então na equação da curva temos:

$$\left(\frac{2n^2}{c-a}\right)^2 - \left(\frac{nb}{c-a}\right)^3 + n^2\left(\frac{nb}{c-a}\right).$$

Desenvolvendo e igualando os denominadores, obtemos:

$$\frac{4n^4(c-a) - n^3b^3 + n^3b(c-a)^2}{(c-a)^3}.$$

Com $n^3b$ em evidência, temos:

$$\frac{4n^4(c-a)-n^3b(b^2-(c-a)^2)}{(c-a)^3}.$$

E como $c^2=a^2+b^2$, desenvolvendo e substituindo, temos:

$$\begin{aligned}
&\frac{4n^4(c-a)-n^3b(b^2-c^2-a^2+2ac)}{(c-a)^3}\\
&=\frac{4n^4(c-a)-n^3b(b^2-(a^2+b^2)-a^2+2ac)}{(c-a)^3}\\
&=\frac{4n^4(c-a)-n^3b(-2a^2+2ac)}{(c-a)^3}\\
&=\frac{4n^4(c-a)-2n^3ab(c-a)}{(c-a)^3}.
\end{aligned}$$

E, por fim, como $(1/2)ab=n\Rightarrow ab=2n$, concluímos que:

$$\frac{4n^4(c-a)-2n^3ab(c-a)}{(c-a)^3}=\frac{4n^4(c-a)-4n^4(c-a)}{(c-a)^3}=0.$$

Logo, $\left(\frac{nb}{c-a},\frac{2n^2}{c-a}\right)$ é uma solução racional da curva $y^2=x^3-n^2x$ com $y=\frac{2n^2}{c-a}\neq 0$.

Queremos mostrar agora que dada a curva $y^2=x^3-n^2x$, se $(x,y)$ é uma solução racional desta curva, com $y\neq 0$, então $n$ é um número congruente, ou seja, existem $a$, $b$ e $c$ racionais com $a^2+b^2=c^2$ e $(1/2)ab=n$, onde $(a,b,c)=\left(\frac{x^2-n^2}{y},\frac{2nx}{y},\frac{x^2+n^2}{y}\right)$. Verifiquemos:

$$\begin{aligned}
a^2+b^2&=\left(\frac{x^2-n^2}{y}\right)^2+\left(\frac{2nx}{y}\right)^2\\
&=\frac{x^4-2x^2n^2+n^4}{y^2}+\frac{4x^2n^2}{y^2}\\
&=\frac{x^4+2x^2n^2+n^4}{y^2}\\
&=\left(\frac{x^2+n^2}{y}\right)^2\\
&=c^2.
\end{aligned}$$

Resta então verificar se $(1/2)ab=n$. Ora, de fato:

$$\frac{1}{2}ab=\frac{1}{2}\cdot\frac{x^2-n^2}{y}\cdot\frac{2nx}{y}.$$

Colocando $2n$ em evidência e usando que $y^2=x^3-n^2x$, temos:

$$\frac{1}{2}\cdot\frac{x^2-n^2}{y}\cdot\frac{2nx}{y}=\frac{2x^3n-2n^3x}{2y^2}=\frac{(2n)(x^3-n^2x)}{2y^2}=\frac{2ny^2}{2y^2}=n.$$

Portando vale a correspondência biunívoca. ■

Note que a correspondência do Teorema 5.3.2 preserva a positividade e a racionalidade dos números. A positividade é preservada pois, dados $a$, $b$ e $c$ racionais positivos, então de $(c-a)(c+a) = c^2 - a^2 = b^2 > 0$ temos que $c-a$ é positivo, portando $x = \frac{nb}{c-a}$ e $y = \frac{2n^2}{c-a}$ são ambos positivos. Por outro lado, se $x$ e $y$ são positivos, então como $y^2 = x^3 - n^2x = x(x^2 - n^2)$, temos que $x^2 - n^2 > 0$, logo $a = \frac{x^2-n^2}{y}$, $b = \frac{2nx}{y}$ e $c = \frac{x^2+n^2}{y}$ são todos positivos. Já a racionalidade se mantém diretamente das operações aplicadas na correspondência, tais operações levam racionais em racionais. Portanto $a$, $b$ e $c$ são racionais, se, e somente se $x$ e $y$ também são.

Veja também que qualquer solução para $a^2 + b^2 = c^2$ e $(1/2)ab = n$ com $n > 0$ precisa que $a$ e $b$ tenham o mesmo sinal (visto que o produto $(1/2)ab$ é positivo). Assim, a menos de um ajuste de sinais, existe uma solução de racionais positivos $a$, $b$ e $c$ se existir uma solução racional qualquer (com $a \cdot b > 0$). Logo, o racional $n > 0$ é um número congruente se e somente se a equação $y^2 = x^3 - n^2x$ possui uma solução racional $(x, y)$, com $y \neq 0$, sem a necessidade de se preocupar que $x$ e $y$ sejam positivos, pois qualquer solução $(x, y)$ gera um trio de racionais $(a, b, c)$, onde, na pior das hipóteses, o triângulo racional $(|a|, |b|, |c|)$ satisfaz o nosso problema.

Consequentemente, se $n$ não é um número congruente, então as únicas soluções racionais para a equação $y^2 = x^3 - n^2x$ são as soluções triviais; $(0, 0)$, $(n, 0)$ e $(-n, 0)$. Assim podemos concluir por exemplos que equações como $y^2 = x^3 - x$ não tem soluções racionais com $y \neq 0$, pois já sabemos pelo Teorema 3.4.1 que 1 não é um número congruente.

### *5.3.1 Derivação das fórmulas do Teorema 5.3.2*

Neste momento, é natural surgir uma eventual curiosidade na mente do leitor; "como encontraram as formulas do Teorema 5.3.2?". O objetivo desta subseção é sanar tal dúvida, pois, de fato este teorema é de suma importância, visto que ele liga triângulos retângulos racionais de área $n$ a soluções racionais da curva elíptica $y^2 = x^3 - n^2x$, com $y \neq 0$. Faremos a seguir uma demonstração algébrica de como as relações do teorema são obtidas.

*Demonstração.* Seja $n \neq 0$ (o sinal de $n$ será irrelevante). Em $a^2 + b^2 = c^2$, podemos escrever $c = a + t$. Assim temos:

$$a^2 + b^2 = (a+t)^2 \quad \Rightarrow \quad b^2 = t^2 + 2at,$$

ou, equivalentemente:

$$2at = b^2 - t^2. \tag{5.3}$$

Como $ab = 2n \neq 0$, visto que $n \neq 0$, então tanto $a$ quanto $b$ são não nulos. Assim podemos escrever $a = \frac{2n}{b}$, e substituindo na equação (5.3), temos:

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

Multiplicando tudo por $\frac{b}{t^3}$ (veja que $t \neq 0$, pois $a \neq c$. Do contrário, $a = c$, implica $b = 0$, e teríamos $n = (1/2)ab = 0$, absurdo por hipótese), obtemos:

$$\frac{4n}{t^2} = \left(\frac{b}{t}\right)^3 - \frac{b}{t}.$$

Por fim, multiplicando tudo por $n^3$, temos:

$$\left(\frac{2n}{t}\right)^2 = \left(\frac{nb}{t}\right)^3 - n^2\left(\frac{nb}{t}\right). \tag{5.4}$$

Assim, na equação (5.4) acima, basta tomar $x = \frac{nb}{t}$ e $y = \frac{2n^2}{t}$ que obtemos a equação procurada da curva; $y^2 = x^3 - n^2x$. Voltando $t$ para $c - a$ (que é diferente de zero), concluímos que:

$$x = \frac{nb}{c-a} \qquad \text{e} \qquad y = \frac{2n^2}{c-a}.$$

Em conformidade com o Teorema 5.3.2. Agora, para obter a reciproca, tomemos:

$$x = \frac{nb}{c-a}, \quad y = \frac{2n^2}{c-a}.$$

Onde, da segunda igualdade:

$$c - a = \frac{2n^2}{y}.$$

Como $c^2 - a^2 = b^2$, temos:

$$c^2 - a^2 = b^2 \quad \Rightarrow \quad (c-a)(c+a) = b^2 \quad \Rightarrow \quad \left(\frac{2n^2}{y}\right)(c+a) = \left(\frac{2nx}{y}\right)^2.$$

Resolvendo a ultima igualdade, obtemos:

$$c + a = \frac{2x^2}{y}.$$

Portanto, temos agora que:

$$c + a = \frac{2x^2}{y}, \quad c - a = \frac{2n^2}{y}.$$

Assim, somando e subtraindo:

$$2c = \frac{2x^2 + 2n^2}{y} \quad \Rightarrow \quad c = \frac{x^2 + n^2}{y},$$

e

$$2a = \frac{2x^2 - 2n^2}{y} \quad \Rightarrow \quad a = \frac{x^2 - n^2}{y}.$$

Portanto:

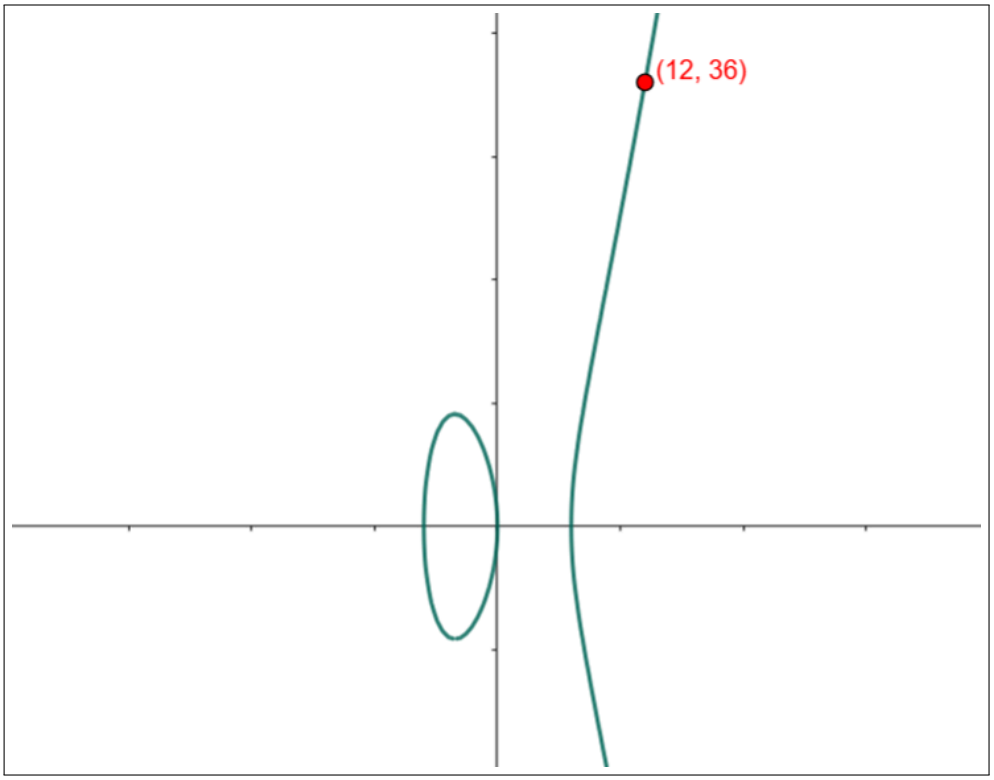
$$(x, y) \longmapsto \left( \frac{x^2 - n^2}{y}, \frac{2nx}{y}, \frac{x^2 + n^2}{y} \right).$$

Conforme a correspondência do Teorema 5.3.2. ■

Nos exemplos a seguir analisaremos a relação entre números congruentes já conhecidos e suas relações como raízes racionais da equação $y^2 = x^3 - n^2x$.

**Exemplo 5.3.3.** Já sabemos que 6 é um número congruente, pois é a área do clássico terno pitagórico $(3, 4, 5)$. Mas, pelo Teorema 5.3.2, temos uma maneira equivalente de demonstrar que 6 é um número congruente, pois aplicando a correspondência deste teorema, obtemos que $(x, y) = (12, 36)$ é a solução racional correspondente ao terno $(3, 4, 5)$ na equação $y^2 = x^3 - 36x$.

Figura 9 – Gráfico da equação $y^2 = x^3 - 36x$




Fonte: Elaborado pelo autor (2025).

Note que, apesar das semelhanças, encontrar racionais $a$, $b$, e $c$ que sejam soluções das equações $a^2 + b^2 = c^2$ e $(1/2)ab = n$ não é equivalente a encontrar um triângulo retângulo

racional de área $n$, pois a primeira situação admite soluções com racionais negativos (desde que $a$ e $b$ tenham o mesmo sinal). De maneira geral, isso significa que tomar soluções racionais $(a, b, c)$ com nem todos positivos geram outros pontos na curva $y^2 = x^3 - n^2x$. Por exemplo, $(-3, -4, 5)$ é uma das soluções de $a^2 + b^2 = c^2$ e $(1/2)ab = 6$ e tal solução pela correspondência do Teorema 5.3.2 gera outro ponto racional da curva $y^2 = x^3 - 36x$, o ponto $(-3, 9)$. Portanto, como já dito, não precisamos se preocupar com os sinais de uma solução racional $(x, y)$ para curvas elípticas. Se houver uma solução qualquer, ela vai gerar racionais $(a, b, c)$ para o problema dos números congruentes, e se este terno não for composto apenas por números positivos, basta tomar a versão positiva destes números para obter um triângulo retângulo racional de área $n$.

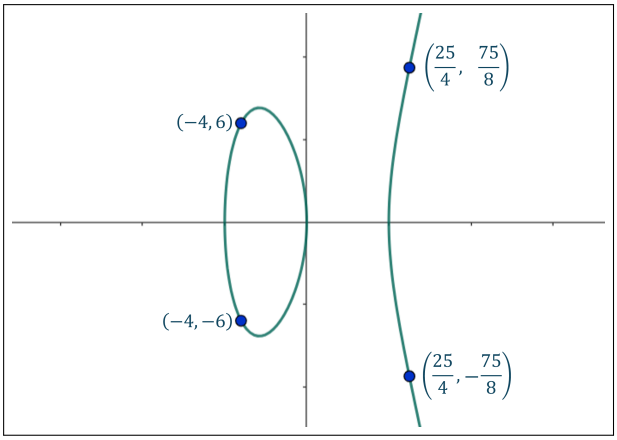
**Exemplo 5.3.4.** Outro número que já sabemos que é congruente é o 5 (vide Tabela 1), o triângulo que mostra isso é formado pelo terno $\left(\frac{3}{2}, \frac{20}{3}, \frac{41}{6}\right)$. Pelo Teorema 5.3.2 este terno equivale a solução racional $\left(\frac{25}{4}, \frac{75}{8}\right)$ para a equação $y^2 = x^2 - 25x$. Porém, como já dito no exemplo anterior, podemos encontrar outras soluções analisando todas as combinações de sinais em $(\pm 3/2, \pm 20/3, \pm 41/6)$ onde as duas primeiras coordenadas têm sinais iguais. Tais opções de escolha de sinais e a solução $(x, y)$ correspondente estão expressas na tabela e na figura a seguir.

Tabela 2 – Soluções da equação $y^2 = x^3 - 25x$

| **Sinais de** $(3/2, 20/3, 41/6)$ | **Solução** $(x, y)$ |
|---|---|
| $(+, +, +)$ | $(25/4, 75/8)$ |
| $(+, +, -)$ | $(-4, -6)$ |
| $(-, -, +)$ | $(-4, 6)$ |
| $(-, -, -)$ | $(25/4, -75/8)$ |

Fonte: Elaborado pelo autor (2025).

Figura 10 – Gráfico da equação $y^2 = x^3 - 25x$




Fonte: Elaborado pelo autor (2025).

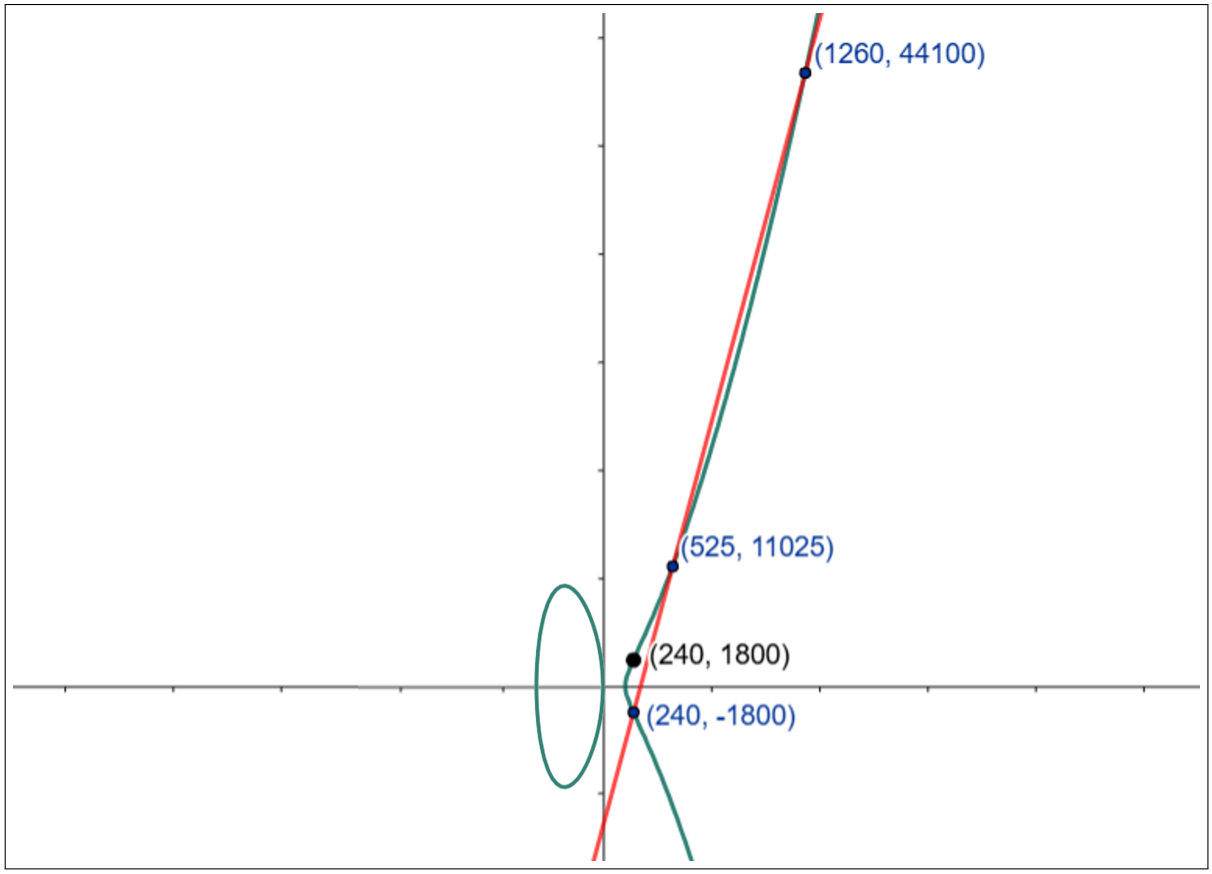
Assim, dada uma solução $(a, b, c)$ para o problema dos números congruentes, esta solução corresponde a um ponto racional $(x, y)$ na curva elíptica $y^2 = x^3 - n^2x$. E, como ilustrado no Exemplo 5.3.4, a partir daí, uma estratégia natural para encontrar novos pontos na curva é investigar como as variações de sinal no terno $(\pm a, \pm b, \pm c)$ se traduzem em novos pontos $(x', y')$. Essa abordagem algébrica possui uma interpretação geométrica, que envolve a construção de novos pontos a partir de pontos já conhecidos usando retas secantes, método que será detalhado na seção a seguir.

## 5.4 Método das secantes: buscando novos triângulos racionais

Conforme estabelecido na Seção 5.2, o conjunto $E(\mathbb{Q})$ de pontos racionais da curva elíptica $y^2 = x^3 - n^2x$, juntamente com o ponto no infinito $\mathcal{O}$, forma um grupo abeliano sobre a operação de adição estabelecida na Seção 5.1. Uma consequência direta desta estrutura é que a soma de dois pontos racionais da curva, resulta em um terceiro ponto da curva de coordenadas racionais. Esta propriedade algébrica tem uma consequência geométrica notável para o problema dos números congruentes. Visto que o Teorema 5.3.2 estabelece uma correspondência entre pontos racionais não triviais e triângulos retângulos de área $n$, a capacidade de gerar um novo ponto $R$ a partir de dois pontos conhecidos $P$ e $Q$ equivale à capacidade de construir um novo triângulo retângulo racional de área $n$ a partir de dois triângulos já conhecidos. O exemplo a seguir ilustra este processo.

**Exemplo 5.4.1.** A Tabela 1 fornece dois triângulos que demonstram a congruência de um mesmo número, o $n = 210$, gerados pelos ternos $(21, 20, 29)$ e $(35, 12, 37)$. Conforme o Teorema 5.3.2, estes correspondem, respectivamente, aos pontos racionais $P = (525, 11025)$ e $Q = (1260, 44100)$ na curva $y^2 = x^3 - 210^2x$. A estrutura de grupo desta curva permite gerar uma nova solução a partir da soma $R = P + Q$. Geometricamente, a reta secante a curva que passa pelos pontos $P$ e $Q$ intersecta a curva em um terceiro ponto, $(240, -1800)$, e a soma $R$ é definida como a reflexão deste ponto, resultando em $R = (240, 1800)$, onde tais coordenadas são obtidas diretamente pela fórmula apresentadas na Proposição 5.1.1. Finalmente, a aplicação da correspondência inversa do Teorema 5.3.2 a este novo ponto $R$ nos fornece um terceiro e distinto triângulo retângulo racional de área 210, com lados $(15/2, 56, 113/2)$. A Figura 11 representa este processo.

Figura 11 – Gráfico da equação $y^2 = x^3 - 210^2x$ (desenho fora de proporção)




Fonte: Elaborado pelo autor (2025).

Obter um terceiro triângulo racional de área $n$ a partir de dois previamente conhecidos é um resultado notável. Veja que não a nada nas definições de números congruentes apresentadas até aqui que indique isso. Entretanto, por vezes conhecemos apenas um triângulo que demonstra a congruência de um dado número $n$, nestes casos, é natural se questionar como podemos obter um segundo triângulo que represente a mesma congruência para $n$.

Sabe-se que dado um triângulo retângulo racional de área $n$, o Teorema 5.3.2 nos permite mapeá-lo a um ponto racional não trivial $P = (x, y)$ na curva $y^2 = x^3 - n^2x$. Uma vez conhecido o ponto $P$, um caminho natural a se considerar é usar o método das secantes (como no Exemplo 5.4.1) tomando os outros pontos conhecidos em qualquer curva elíptica; suas soluções triviais. Assim, vamos analisar os pontos obtidos ao traçar as retas secantes a curva que conectam $P$ às três soluções triviais; $(0,0)$, $(n,0)$ e $(-n,0)$. Por exemplo, tomando a reta que passa por $P$ e $(0,0)$, esta reta intersecta a curva em um terceiro ponto, onde aplicando a Proposição 5.1.1 e substituindo $y^2$ por $x^3 - n^2x$ obtemos que as coordenadas deste ponto são $\left(\frac{-n^2}{x}, \frac{-n^2y}{x^2}\right)$. Ao repetir este processo considerando as retas que passam por $P$ e cada uma das soluções triviais, e recordando também que a cada novo ponto obtido, sua reflexão também pertence a curva,

obtém-se um conjunto de seis novos pontos, conforme sistematizado na Tabela 3 a seguir.

Tabela 3 – Terceiro ponto de interseção da reta com a curva $y^2 = x^3 - n^2x$

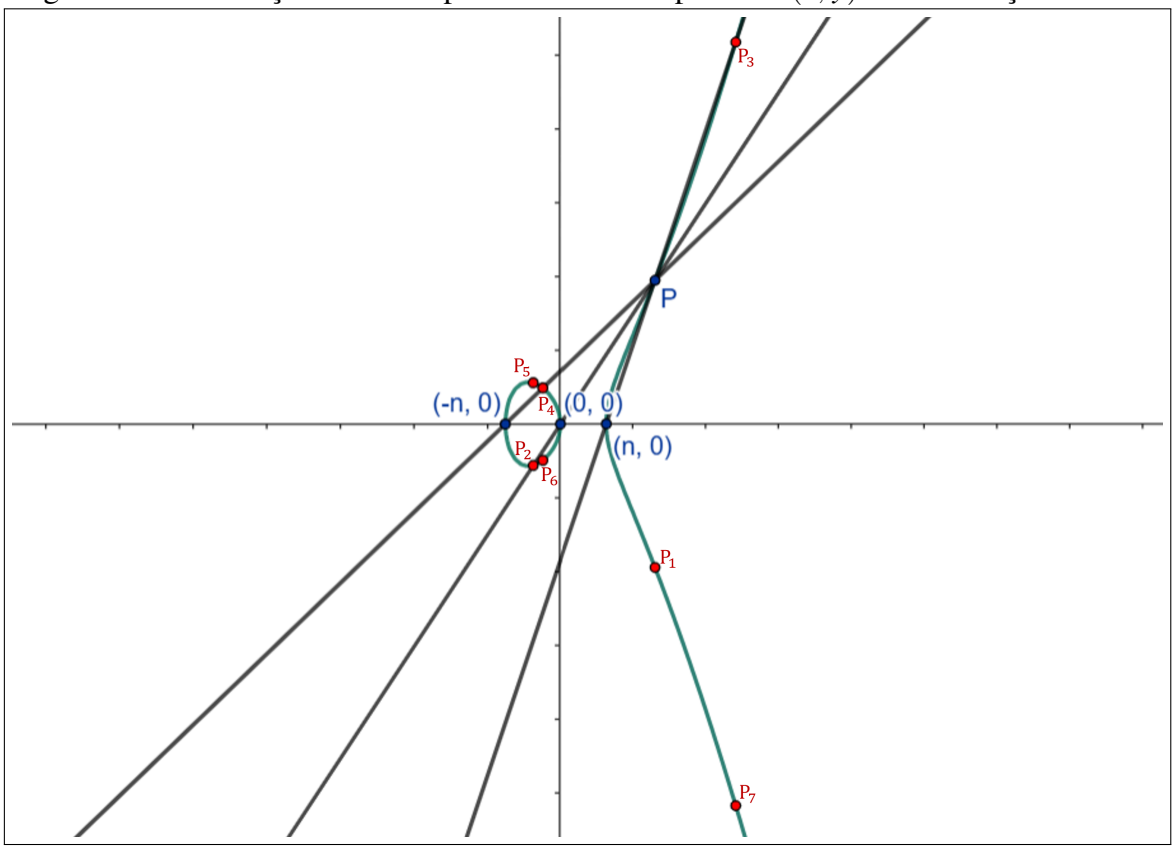
| **Primeiro ponto** | **Segundo ponto** | **Terceiro ponto** | **Reflexão** |
|---|---|---|---|
| $(x, y)$ | $(0, 0)$ | $\left(\frac{-n^2}{x}, \frac{-n^2y}{x^2}\right)$ | $\left(\frac{-n^2}{x}, \frac{n^2y}{x^2}\right)$ |
| $(x, y)$ | $(n, 0)$ | $\left(\frac{n(x+n)}{x-n}, \frac{2n^2y}{(x-n)^2}\right)$ | $\left(\frac{n(x+n)}{x-n}, \frac{-2n^2y}{(x-n)^2}\right)$ |
| $(x, y)$ | $(-n, 0)$ | $\left(\frac{-n(x-n)}{x+n}, \frac{2n^2y}{(x+n)^2}\right)$ | $\left(\frac{-n(x-n)}{x+n}, \frac{-2n^2y}{(x+n)^2}\right)$ |

Fonte: Elaborado pelo autor (2025).

Vale ressaltar aqui, que tomar as reta que passam por $(x, -y)$, que também pertencem a curva, pois é apenas a reflexão de $(x, y)$ e suas soluções triviais, gera os mesmos seis pontos apresentados na tabela acima. Portanto o conjunto de pontos gerados é fechado, independentemente se partimos de $(x, y)$ ou $(x, -y)$.

Representamos na Figura 12 a seguir este processo de construção de novos pontos na curva $y^2 = x^3 - n^2x$ a partir de um ponto $(x, y)$ dado e suas soluções triviais. Em sequência, na Tabela 4, apresenta as coordenadas destes pontos e suas correspondências via Teorema 5.3.2.

Figura 12 – Construção de novos pontos na curva a partir de $(x, y)$ e suas soluções triviais




Fonte: Elaborado pelo autor (2025).

Tabela 4 – Correspondência entre os pontos e os trios correspondentes pelo Teorema 5.3.2

| **Ponto da curva** | **Trio correspondente** |
|---|---|
| $(x, y)$ | $(a, b, c)$ |
| $(x, -y)$ | $(-a, -b, -c)$ |
| $\left(\frac{-n^2}{x}, \frac{-n^2y}{x^2}\right)$ | $(a, b, -c)$ |
| $\left(\frac{-n^2}{x}, \frac{n^2y}{x^2}\right)$ | $(-a, -b, c)$ |
| $\left(\frac{n(x+n)}{x-n}, \frac{2n^2y}{(x-n)^2}\right)$ | $(b, a, c)$ |
| $\left(\frac{n(x+n)}{x-n}, \frac{-2n^2y}{(x-n)^2}\right)$ | $(-b, -a, -c)$ |
| $\left(\frac{-n(x-n)}{x+n}, \frac{2n^2y}{(x+n)^2}\right)$ | $(-b, -a, c)$ |
| $\left(\frac{-n(x-n)}{x+n}, \frac{-2n^2y}{(x+n)^2}\right)$ | $(b, a, -c)$ |

Fonte: Elaborado pelo autor (2025).

Assim, a Tabela 4 acima responde o questionamento deixado ao fim da seção anterior sobre quais pontos de uma curva elíptica referem-se a quais variações de ordem ou de sinais no terno $(a, b, c)$. Entretanto, fica claro que o método das secantes é insuficiente para encontrar um triângulo genuinamente novo quando se conhece apenas um ponto racional não trivial de uma curva elíptica. É precisamente este desafio que abordaremos a seguir.

## 5.5 Método da tangente

Seja $E : y^2 = x^3 - n^2x$ uma curva na qual $P = (x_1, y_1)$ é o único ponto racional não trivial conhecido. Uma reta candidata a ser analisada na busca por um novo ponto racional não trivial de $E$ é a reta tangente a curva neste ponto. A tangente a curva $E$ no ponto $P$ é dada por $y = m(x - x_1) + y_1$ onde $m$ é obtido derivando $E$ com relação $x$. Como obtido na Proposição 5.1.1, $m = \frac{3x_1^2+a}{2y_1}$, em particular, $a = -n^2$.

**Exemplo 5.5.1.** O triângulo pitagórico $(3, 4, 5)$ tem área 6 e, conforme visto no Exemplo 5.3.3, corresponde ao ponto $P = (12, 36)$ na curva elíptica $E : y^2 = x^3 - 36x$. Para encontrar um novo ponto, usaremos a reta tangente a $E$ em $P$. Embora a Proposição 5.1.1 nos dê diretamente a coordenada deste novo ponto, faremos o cálculo detalhado neste primeiro exemplo. Seja então:

$$m = \frac{3 \cdot 12^2 - 36}{2 \cdot 36} = \frac{11}{2}.$$

Assim:

$$y = \frac{11}{2}(x-12)+36 \quad \Rightarrow \quad y = \frac{11}{2}x - 30.$$

Substituindo na equação da curva $E$, temos:

$$\left(\frac{11}{2}x - 30\right)^2 = x^3 - 36x.$$

Desenvolvendo e eliminando os denominadores, vamos chegar em:

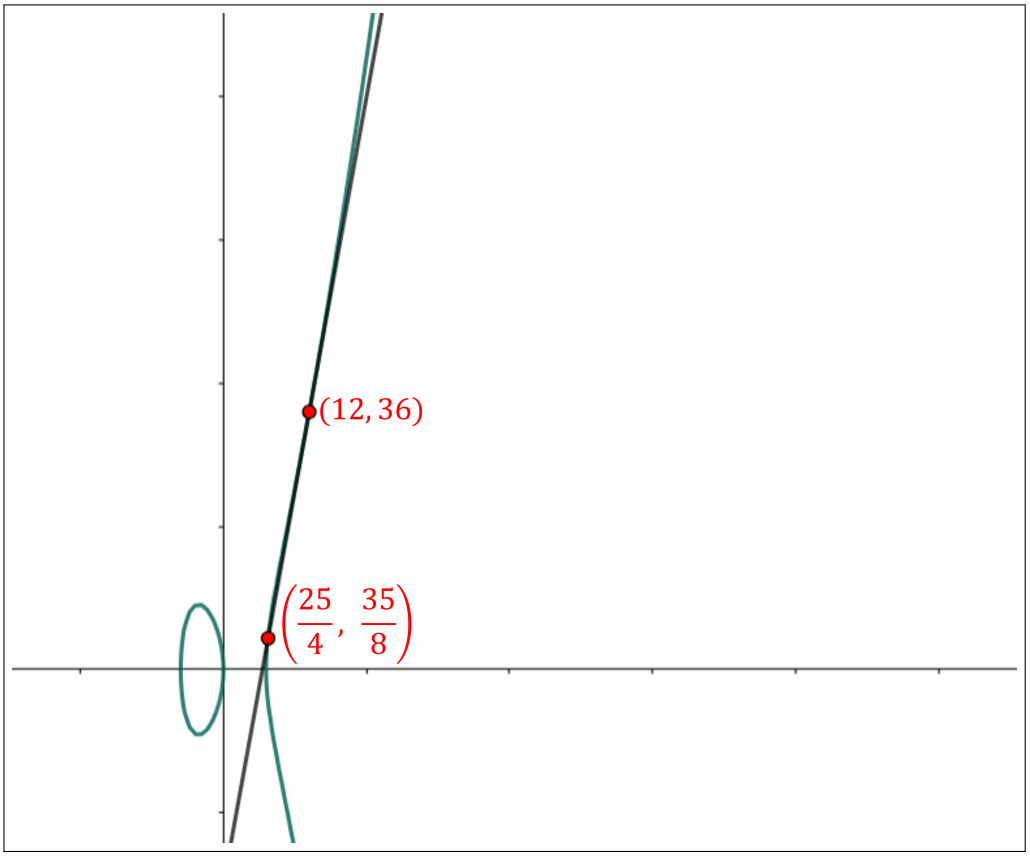
$$4x^3 - 121x^2 + 1176 - 3600 = 0.$$

Ora, já sabemos que o ponto $(12, 36)$ é um dos pontos de intercessão entre a reta tangente e a curva $E$, logo $x = 12$ é uma das raízes do polinômio acima, assim podemos fatorá-lo por $(x-12)$, temos então:

$$4x^3 - 121x^2 + 1176 - 3600 = (x-12)(4x^2 - 73x - 300).$$

Onde, pela *fórmula de Bhaskara*, o polinômio $4x^2 - 73x - 300$ tem raízes 12 (já conhecida) e $\frac{25}{4}$. Substituindo $x = \frac{25}{4}$ na equação da reta tangente, obtêm-se $y = \frac{35}{8}$. Assim, temos outro ponto racional pertencente a curva $E$; $\left(\frac{25}{4}, \frac{35}{8}\right)$. A figura abaixo esquematiza este processo.

Figura 13 – Construção de um novo ponto da curva $y^2 = x^3 - 36x$ a partir de uma tangente




Fonte: Elaborado pelo autor (2025).

Finalmente, aplicando a correspondência do Teorema 5.3.2, o ponto $\left(\frac{25}{4}, \frac{35}{8}\right)$ corresponde ao triângulo retângulo $\left(\frac{7}{10}, \frac{120}{7}, \frac{1201}{70}\right)$ de área 6.

É claro que o procedimento feito no Exemplo 5.5.1 sobre a tangente a curva no ponto $(12, 36)$ pode ser repetido no ponto $\left(\frac{25}{4}, \frac{35}{8}\right)$. Assim a equação da reta tangente a curva neste ponto é dada por:

$$y = \frac{1299}{140}x - \frac{6005}{112}.$$

Onde, pela Proposição 5.1.1 esta tangente intersecta a curva no ponto:

$$\left(\frac{1442401}{19600}, \frac{1726556399}{2744000}\right).$$

O triângulo retângulo racional de área 6 correspondente a este ponto é:

$$\left(\frac{1437599}{168140}, \frac{2017680}{1437599}, \frac{2094350404801}{241717895860}\right).$$

Portanto, com o método da tangente, podemos agora obter outros triângulos retângulos racionais de área $n$ a partir de um único triângulo inicial com essas propriedades.

Pode-se interpretar geometricamente que o método da secante "soma" dois pontos distintos da curva, enquanto o método da tangente é o caso especial para "dobrar" um ponto. Ambas as construções podem ser usadas como base da estrutura de grupo abeliano que o conjunto de pontos racionais de uma curva elíptica $y^2 = x^3 - n^2x$, junto ao ponto no infinito $\mathcal{O}$, possui. Um resultado complexo, mas fundamental neste contexto é o *Teorema de Mordell-Weil* (Silverman e Tate, 1992) de 1928, dos matemáticos Louis Mordell (1888 - 1972) e André Weil (1906 - 1998), que estabelece que este grupo é *finitamente gerado*. Uma consequência direta é que a existência de uma única solução racional não trivial implica a existência de infinitas outras. Por equivalência, se houver um triângulo retângulo de área $n$, então haverá infinitos, assim como, em conexão com o Capítulo 4, haverá infinitas progressões aritméticas de três quadrados com razão $n$.

Estabelecemos assim, três formulações equivalentes para o problema dos números congruentes. Onde, a existência de uma solução em qualquer uma delas implica a existência de infinitas soluções em todas. Formalmente, um número $n$ é dito congruente se qualquer uma das condições abaixo for satisfeita.

- Existe um triângulo retângulo de lados racionais com área $n$ (Definição 1.0.1).
- Existem três racionais quadrados em progressão aritmética de razão $n$ (Definição 4.1.1).
- Existe uma solução racional para a equação $y^2 = x^3 - n^2x$, com $y \neq 0$ (Definição 5.3.1).

## 5.6 Teorema de Tunnell e a busca por uma solução definitiva

Até o momento, analisamos o problema dos números congruentes sobre três pontos de vista, desde a definição clássica envolvendo triângulos retângulos, até as versões envolvendo progressões aritméticas e curvas elípticas. Pois bem, a importância de analisar números congruentes em termos da curva elíptica $y^2 = x^3 - n^2x$ como discutido até aqui neste capítulo, vai muito além de apenas buscar construir novos triângulos retângulos racionais de área $n$.

Em 1952, o matemático alemão Kurt Heegner (1893 - 1965) mostrou um dos primeiros avanços significativos utilizando a teoria de curvas elípticas aplicadas a números congruentes. Utilizando técnicas profundas que envolviam formas modulares e a construção do que hoje conhecemos como *pontos de Heegner* sobre curvas elípticas, ele foi capaz de provar a congruência para classes infinitas de números primos. Heegner provou que os números primos da sequência; 5, 13, 21, 29, 37, ..., são todos números congruentes, ou seja, Heegner provou que dado $p$ primo, se $p \equiv 5 \pmod 8$, então $p$ é um número congruente. Um resultado de grande impacto para a época.

Mas, foi em 1983, que o matemático estadunidense Jerrold Bates Tunnell mostrou que curvas elípticas de fato podem levar a uma solução definitiva para o problema dos números congruentes. Ele usou as propriedades aritméticas da curva elíptica $y^2 = x^3 - n^2x$ para definir uma condição necessária para que um número $n$ seja congruente. O resultado de Tunnell esta descrito no teorema a seguir.

**Teorema 5.6.1** (Tunnell)**.** *Seja n um número inteiro positivo livre de quadrados. Definem-se as seguintes funções de contagem:*

$$
\begin{aligned}
f(n) &= \#\left\{(x,y,z) \in \mathbb{Z}^3 \mid x^2 + 2y^2 + 8z^2 = n\right\}, \\
g(n) &= \#\left\{(x,y,z) \in \mathbb{Z}^3 \mid x^2 + 2y^2 + 32z^2 = n\right\}, \\
h(n) &= \#\left\{(x,y,z) \in \mathbb{Z}^3 \mid x^2 + 4y^2 + 8z^2 = \frac{n}{2}\right\}, \\
k(n) &= \#\left\{(x,y,z) \in \mathbb{Z}^3 \mid x^2 + 4y^2 + 32z^2 = \frac{n}{2}\right\}.
\end{aligned}
$$

*Então, para n ímpar; se n for congruente, então* $f(n) = 2g(n)$*. Caso n seja par; se n for congruente, então* $h(n) = 2k(n)$*.*

Além disso, caso a *conjectura de Birch and Swinnerton-Dyer* seja verdadeira, então a reciproca de ambas as implicações será válida. Assim teríamos que; $f(n) = 2g(n)$ com $n$ ímpar, se, e somente se, $n$ é congruente. E para n par, h(n) = 2k(n) se, e somente se, $n$ é congruente.

A conjectura de Birch e SwinnertonDyer, é um dos problemas em aberto mais importantes da matemática moderna, tanto que aparece na lista de problemas do milênio do *Instituto Clay de Matemática*. Ela prevê uma relação profunda entre o número de soluções racionais de uma curva elíptica e o comportamento analítico de uma função associada a ela, chamada função $L$. No contexto do Teorema 5.6.1 de Tunnell, a conjectura aparece como a ponte que permite transformar uma condição de contagem aritmética (de soluções inteiras) em uma verificação da congruência de um número. Embora não seja necessário compreender os detalhes técnicos da conjectura para acompanhar esta dissertação, sua menção destaca a profundidade e a importância do problema dos números congruentes no cenário atual da teoria dos números.

A demonstração do Teorema 5.6.1 não é nada elementar, e não abordaremos aqui, pois esta fora do contexto deste trabalho. Mas fica a ressalva de que Tunnell provou as implicação descritas em seu teorema relacionando curvas elípticas racionais com ponto de ordem infinita e formas modulares (Tunnell, 1983). Apenas as reciprocas do teorema necessitam que a conjectura de Birch e SwinnertonDyer seja verdadeira.

**Exemplo 5.6.2.** É fácil ver que $f(1) = g(1) = 2$ nas equações de Tunnell, pois as únicas soluções tanto para $f$ quanto para $g$ são dadas por $(\pm 1, 0, 0)$. Enquanto que $f(3) = g(3) = 4$, onde as mesmas quatro soluções para $f$ e para $g$ são dadas pelas possíveis combinações de sinais em $(\pm 1, \pm 1, 0)$. Logo, $f(1) \neq 2g(1)$, assim como $f(3) \neq 2g(3)$. Portanto, pelo Teorema 5.6.1, 1 e 3 não são números congruentes.

**Exemplo 5.6.3.** Para verificar que 2 não é congruente, note que $h(2) = k(2) = 2$, pois as únicas soluções são dada por $(\pm 1, 0, 0)$. Portanto, $h(2) \neq 2k(2)$, logo, pelo Teorema 5.6.1, 2 não é um número congruente. De maneira análoga, $h(10) = k(10) = 4$, novamente, as quatro soluções das funções $h$ e $k$ são dadas pelas quatro combinações de sinais possíveis em $(\pm 1, \pm 1, 0)$. Logo, $h(10) \neq 2k(10)$, então, novamente pelo Teorema 5.6.1, 10 não é um número congruente.

**Exemplo 5.6.4.** Note que não existem $(x, y, z) \in \mathbb{Z}^3$, que sejam soluções para $f(5)$ e $g(5)$. Logo, $f(5) = g(5) = 0$, portanto $f(5) = 2g(5)$. O mesmo vale para $f(7) = g(7) = 0$, assim, $f(7) = 2g(7)$. Portanto, se a conjectura de Birch e Swinnerton-Dyer for válida, o Teorema 5.6.1 de Tunnell diz que 5 e 7 são números congruentes. De fato, recorde-se que os triângulos retângulos racionais $(3/2, 20/3, 41/6)$ e $(24/5, 35/12, 337/60)$ tem áreas iguais a 5 e 7 respectivamente.

Os exemplos anteriores evidenciam que, de momento, o Teorema 5.6.1 de Tunnell é principalmente um critério poderoso para demonstrar que um certo número $n$ não é congruente.

Pois, se $f(n) \neq 2g(n)$ com $n$ ímpar (ou analogamente, se $h(n) \neq 2k(n)$, com $n$ par), então $n$ não é um número congruente. Porém, obter por exemplo que $f(n) = 2g(n)$ para algum $n$ ímpar, apenas garante que $n$ é congruente se a conjectura de Birch e Swinnerton-Dyer for válida. Ou seja, a igualdade das equações de Tunnell é uma condição necessária, mas não suficiente, para que um número $n$ seja congruente. E apesar desta conjectura ser "apoiada por muitas evidências experimentais" como cita o próprio Instituto Clay em seu site, ela ainda não foi completamente demonstrada, e mesmo com o prêmio de um milhão de dólares (oferecido pelo mesmo instituto) a quem resolver este ou qualquer um dos demais problemas do milênio em aberto, a conjectura de Birch e Swinnerton-Dyer segui sendo um dos problemas mais desafiadores da matemática moderna. Joseph H. Silverman apresenta devidamente em seu livro *The Aritimetic of Elliptic Curves* (Silverman e Tate, 1992) a conjectura de Birch e Swinnerton-Dyer além de apresentar algumas das diversas evidencias que apoiam a veracidade da mesma.

Um importante resultado, que depende da validade da recíproca do Teorema 5.6.1 de Tunnell, é apresentado no corolário a seguir. É fundamental contrastar este resultado com o de Heegner, mencionado no início desta seção. O Corolário 5.6.5 é mais abrangente, pois se aplica a todos os inteiros nas condições dadas, não apenas aos primos, e inclui as classes de congruência $n \equiv 6 \pmod 8$ e $n \equiv 7 \pmod 8$. No entanto, o grande mérito de Heegner reside em sua natureza incondicional, ou seja, Heegner usou argumentos complexos, mas que não dependem da da Conjectura de Birch e Swinnerton-Dyer.

**Corolário 5.6.5** (condicional)**.** *Se a Conjectura de Birch e Swinnerton-Dyer for verdadeira para as curvas da forma $y^2 = x^3 - n^2x$, então todo inteiro n livre de quadrados, tal que $n \equiv 5, 6, 7 \pmod 8$ é um número congruente.*

*Demonstração.* Devemos provar que $f(n) = 2g(x)$ para os casos em que $n \equiv 5, 7 \pmod 8$ e $h(n) = 2k(n)$ quando $n \equiv 6 \pmod 8$.

Se $n \equiv 5, 7 \pmod 8$, então $n$ é ímpar, assim devemos analisar as funções $f$ e $g$ do teorema 5.6.1. Como $8z^2, 32z^2 \equiv 0 \pmod 8$, basta analisarmos $x^2 + 2y^2$ nas funções $f$ e $g$. Ora, mas $x^2 \equiv 0, 1, 4 \pmod 8$, $\forall x \in \mathbb{Z}$, assim, analisando as possibilidades de congruência de $x^2$ e $2y^2$, temos que $x^2 + 2y^2 \equiv 0, 1, 2, 3, 4,$ ou $6 \pmod 8$. Portanto $f(n) = 0$ e $g(n) = 0$, visto que $x^2 + 2y^2 \not\equiv 5, 7 \pmod 8$. Ou seja, $f(n) = 2g(n)$, portanto, pelo Teorema 5.6.1, se a Conjectura de Birch e Swinnerton-Dyer for válida, $n$ é congruente.

Caso $n \equiv 6 \pmod 8$, e portanto par, devemos tomar as funções $h$ e $k$ do teorema. Primeiramente, note que se $n \equiv 6 \pmod 8$, então $\frac{n}{2} \equiv 3 \pmod 4$. Assim, basta analisarmos os

termos não congruentes a zero em modulo 4 nas funções $h$ e $k$ de Tunnell, ou seja, devemos analisar apenas o termo $x^2$. E, como $x^2 \equiv 0$ ou $1 \pmod 4$, $\forall x \in \mathbb{Z}$, temos que $h(n) = k(n) = 0$. Logo, $h(n) = 2k(n)$, então, novamente pelo Teorema 5.6.1, se a Conjectura de Birch e Swinnerton-Dyer for válida, $n$ é congruente. ■

# 6 CONCLUSÕES E TRABALHOS FUTUROS

Este trabalho dedicou-se a uma imersão no problema dos números congruentes, um tema clássico da Teoria dos Números que, apesar de sua formulação elementar, descortina uma paisagem matemática de extraordinária riqueza e complexidade. O escopo deste trabalho abrangeu não apenas a revisão das definições fundamentais e dos marcos históricos que delinearam este desafio ao longo dos séculos  desde seus primeiros vestígios em manuscritos árabes até as contribuições seminais de matemáticos como Fibonacci e Fermat  mas também a exploração das diversas perspectivas teóricas através das quais o problema pode ser compreendido e investigado.

A jornada investigativa percorreu a análise de números congruentes sob a perspectiva clássica, em sua importante relação com ternos pitagóricos e a noção de inteiros livres de quadrados. Mas, além disso, foi explorada a elegante equivalência do problema com a existência de três quadrados racionais em progressão aritmética  a formulação que historicamente conferiu o nome *congruente* a estes números. Por fim, o estudo culminou na exploração da profunda conexão entre os números congruentes e a teoria das curvas elípticas, revelando uma terceira e poderosa formulação do problema através da busca por pontos racionais não triviais para estas curvas. A investigação alcançou as fronteiras da matemática contemporânea ao abordar o teorema de Tunnell, que oferece um critério computável para a congruência, embora sua totalidade esteja intrinsecamente ligada à Conjectura de Birch e Swinnerton-Dyer, um dos grandes desafios em aberto da matemática moderna.

Paralelamente a esta investigação teórica, visto a riqueza que os números congruentes tem a oferecer, este trabalho também se propôs a transpor parte desse conhecimento para o contexto da educação básica. Como resultado, foi desenvolvida uma sequência didática, intitulada *"Explorando o Mundo dos Números Congruentes no Ensino Médio"*, apresentada em detalhe no apêndice. Este material pedagógico visa oferecer aos professores do Ensino Médio um recurso prático e fundamentado para introduzir este fascinante tema em sala de aula. A sequência foi elaborada para promover não apenas a compreensão de conceitos matemáticos, mas também o desenvolvimento do raciocínio lógico, a apreciação pela história da matemática e a percepção das conexões entre diferentes áreas do conhecimento.

Olhando adiante, os trabalhos futuros desdobram-se em múltiplas direções. No campo da teoria dos números, persistem questões abertas e caminhos para aprofundamento, desde de a busca por classes completas de números congruentes a relação com formas modulares e outros aspectos da Conjectura de Birch e Swinnerton-Dyer continuam a ser um vasto campo de

pesquisa. Cuja espera-se que a demonstração desta conjectura esteja em um horizonte próximo, onde sua veracidade garantirá a reciproca do teorema de Tunnell, ligando a congruência ou não de um número a funções de contagens. No âmbito da educação matemática, o desenvolvimento mais significativo seria a aplicação e validação da sequência didática proposta em ambientes de sala de aula do Ensino Médio. Um estudo criterioso dos resultados, dificuldades encontradas por alunos e professores, e o impacto no engajamento e aprendizado dos estudantes, forneceria subsídios valiosos para o refinamento e a ampliação do material.

Em suma, o problema dos números congruentes exemplifica a beleza e a perenidade dos desafios matemáticos. Uma questão aparentemente simples, com raízes fincadas na história, que continua até os dias de hoje a estimular a pesquisa avançada e, simultaneamente, oferece um terreno fértil para experiências de aprendizado significativas na educação básica, ilustrando, no cotidiano da sala de aula, como questionamentos simples podem florescer em teorias matemáticas complexas e elegantes, servindo como fonte de inspiração e atração para futuros talentos na área. Espera-se que esta dissertação tenha contribuído para uma melhor compreensão deste intrigante problema e, através da proposta pedagógica, para a sua potencial exploração em sala de aula, reforçando a matemática como uma ciência viva e conectada.

# REFERÊNCIAS

CONRAD, K. **The congruent number problem**. 2008. [*S. l.*], Disponível em: https://kconrad.math.uconn.edu/blurbs/ugradnumthy/congnumber.pdf. Acesso em: 5 jan. 2025.

CREMONA, J. E. **Algorithms for modular elliptic curves**. 2nd ed. Cambridge: Cambridge University Press, 1997.

FIBONACCI, L. **The book of squares**. Orlando, Florida: Academic Press, 1986. Traduzido do latin Liber Quadratorum por L. E. Sigler.

HEMENWAY, B. **On recognizing congruent primes**. Dissertação (Mestrado em Ciência) – Departamento de Matemática, Universidade Simon Fraser, 2006. Disponível em: https://summit.sfu.ca/item/6418. Acesso em: 12 jan. 2025.

KOBLITZ, N. **Introduction to elliptic curves and modular forms**. 2nd ed. [*S. l.*]: Springer-Verlag, 1993. (Graduate Texts in Mathematics).

RODRIGUEZ, J. E. A.; SOUZA, N. R. d. O problema dos números congruentes: três versões equivalentes. **Proceeding Series of the Brazilian Society of Applied and Computational Mathematics**, [*s. l.*], v. 5, n. 1, p. 1–7, 2017. Disponível em: https://proceedings.sbmac.org.br/sbmac/article/viewFile/1428/1441. Acesso em: 03 fev. 2025.

SILVERMAN, J. H.; TATE, J. T. **Rational points on elliptic curves**. New York: Springer-Verlag, 1992.

TUNNELL, J. A classical diophantine problem and modular forms of weight 3/2. **Inventiones mathematicae**, [*s. l.*], v. 72, p. 323–334, 1983. Disponível em: http://eudml.org/doc/143024. Acesso em: 17 jan. 2025.

# APÊNDICE A – PROPOSTA DE SEQUÊNCIA DIDÁTICA: EXPLORANDO O MUNDO DOS NÚMEROS CONGRUENTES

Nas paginas que se seguem, é apresentado o produto educacional desenvolvido no âmbito desta dissertação: uma sequência didática sobre o problema dos números congruentes visando a possibilidade de apresentação e abordagem do tema (de maneira mais branda) em salas de aula de Ensino Médio.

Este material foi concebido para ser funcional e autocontido, permitindo sua aplicação direta por professores do Ensino Médio. Todavia, para uma melhor fundamentação teórica sobre o tema e uma maior propriedade na condução das atividades propostas, a leitura prévia dos capítulos que compõem este trabalho é fortemente recomendada.

**UNIVERSIDADE FEDERAL DO CEARÁ**

**CENTRO DE CIÊNCIAS**

**DEPARTAMENTO DE MATEMÁTICA**

**PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA EM REDE NACIONAL**

**MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL**

**ANTONIO WESLEY DE BRITO VIEIRA**

# PROPOSTA DE SEQUÊNCIA DIDÁTICA: EXPLORANDO O MUNDO DOS NÚMEROS CONGRUENTES NO ENSINO MÉDIO

**FORTALEZA**

**2025**

**SUMÁRIO**

# 1 INTRODUÇÃO E JUSTIFICATIVA

O presente apêndice apresenta um recurso educacional derivado desta dissertação; uma sequência didática sobre números congruentes. Visto que os conceitos fundamentais do tema podem ser explorados com alunos do ensino médio sem a necessidade de aprofundamento teórico extensivo ou demonstrações de todos os teoremas, propõe-se um conjunto de aulas introdutórias. Embora este material tenha sido concebido para funcionar de maneira autônoma, como um guia prático para o educador, recomenda-se veementemente a leitura integral da dissertação para os professores que desejarem aprofundar sua base teórica sobre o tema, capacitando-os a ministrar estas aulas com a máxima propriedade e segurança conceitual. As definições e teoremas aqui contidos estão simplificados e suas devidas demonstrações estão presentes no corpo desta dissertação.

A concepção desta sequência didática foi fundamentada nos pressupostos teóricos apresentados por Dailson Evangelista e Tadeu Oliver na obra *"Compreensões, Abordagens, Conceitos e Definições de Sequência Didática na área de Educação Matemática"* (Costa e Gonçalves, 2022), que discutem as compreensões e definições de sequências didáticas na educação matemática, onde buscou-se seguir o modelo da *Sequencia Fedathi* (Santana *et al.*, 2004) idealizada por Hermínio Borges Neto (UFC). O objetivo foi estruturar um material que apresentasse coesão interna entre as atividades e que maximizasse o potencial de aproveitamento e engajamento tanto para o professor, na condução das aulas, quanto para o aluno, na construção de seu conhecimento.

Esta sequência didática visa trazer o encanto e a profundidade do problema dos números congruentes para a sala de aula do Ensino Médio. Ao explorar conceitos como ternos pitagóricos, números racionais, áreas de triângulos e a própria natureza investigativa da matemática, busca-se não apenas introduzir o problema dos números congruentes, mas também desenvolver o raciocínio lógico, a capacidade de resolução de problemas e a apreciação pela história da matemática. A carência de material didático acessível em língua portuguesa sobre o assunto reforça a relevância desta proposta.

Acredita-se, que ao trilhar os caminhos históricos e as diferentes formulações do problema, os alunos poderão vivenciar a matemática como uma ciência viva, em constante evolução, e perceber como diferentes áreas podem se conectar de maneiras surpreendentes.

# 2 APLICAÇÃO DA SEQUÊNCIA DIDÁTICA

**Público-alvo**: Alunos de 1ł ou 2ł série do Ensino Médio. Pressupõe-se que os alunos já tenham familiaridade com o teorema de Pitágoras, cálculo de área de triângulos e operações básicas com números racionais. Conteúdos geralmente trabalhados nos anos finais do ensino fundamental.

**Objetivo geral**: Compreender o problema dos números congruentes a partir de suas diferentes formulações, investigando as ferramentas matemáticas fundamentais para sua análise e as relações entre os conceitos apresentados.

**Objetivos específicos**: Ao final desta sequência didática, espera-se que o aluno seja capaz de:

- Compreender a definição de um número congruente em sua formulação clássica.
- Identificar e gerar ternos pitagóricos.
- Relacionar ternos pitagóricos com a obtenção de números congruentes inteiros.
- Compreender a ideia de escalonamento de triângulos e sua influência na área, bem como a relevância dos inteiros livres de quadrados para o problema.
- Valorizar a perspectiva histórica da matemática e a evolução de um problema ao longo do tempo.
- Conhecer exemplos de números congruentes e não congruentes, incluindo o caso histórico do número 1.
- Ter uma introdução à segunda formulação do problema dos números congruentes (progressão aritmética de quadrados).
- Identificar a equação da curva elíptica $y^2 = x^3 - n^2x$ como uma terceira forma de caracterizar os números congruentes.
- Desenvolver o pensamento crítico e a argumentação matemática.

**Duração estimada**: 6 aulas de 50 minutos cada. As aulas são subdivididas em atividades com estimativas de tempo, cabendo ao professor a flexibilidade para adaptar essa distribuição conforme julgar necessário.

**Recursos gerais**: lousa ou quadro branco, pincéis ou giz, projetor multimídia, cópias de atividades propostas, calculadoras (para verificação rápida dos cálculos), software de geometria dinâmica (GeoGebra ou similar) e acesso à internet para pesquisa.

## 2.1 Alinhamento com a Base Nacional Comum Curricular (BNCC)

Embora o tema "Números Congruentes" não seja explicitamente listado na Base Nacional Curricular Comum (BNCC), sua exploração em sala de aula é uma via rica para o desenvolvimento de diversas competências e habilidades gerais e específicas da área de Matemática e suas Tecnologias. A natureza investigativa do problema, sua profunda conexão com a história da matemática, e os conceitos de geometria e teoria dos números que mobiliza, permitem que os alunos desenvolvam o pensamento algébrico e geométrico, a capacidade de argumentação, o raciocínio lógico e uma apreciação pela matemática como ciência em evolução. Esta sequência didática, portanto, busca promover uma relação direta com as seguintes competências:

**Competências gerais**:

- **CG02 (Pensamento científico, crítico e criativo):** Exercitar a curiosidade intelectual e recorrer à abordagem própria das ciências, incluindo a investigação, a reflexão, a análise crítica, a imaginação e a criatividade, para investigar causas, elaborar e testar hipóteses, formular e resolver problemas e criar soluções (inclusive tecnológicas) com base nos conhecimentos das diferentes áreas.
- **CG04 (Comunicação):** Utilizar diferentes linguagens verbal (oral ou visual-motora, como Libras, e escrita), corporal, visual, sonora e digital , bem como conhecimentos das linguagens artística, matemática e científica, para se expressar e partilhar informações, experiências, ideias e sentimentos em diferentes contextos e produzir sentidos que levem ao entendimento mútuo.
- **CG05 (Cultura digital):** Compreender, utilizar e criar tecnologias digitais de informação e comunicação de forma crítica, significativa, reflexiva e ética nas diversas práticas sociais (incluindo as escolares) para se comunicar, acessar e disseminar informações, produzir conhecimentos, resolver problemas e exercer protagonismo e autoria na vida pessoal e coletiva.

**Competências específicas de matemática**:

- **CEMAT01:** Utilizar estratégias, conceitos e procedimentos matemáticos para interpretar situações em diversos contextos, sejam atividades cotidianas, sejam fatos das Ciências da Natureza e Humanas, das questões socioeconômicas ou tecnológicas, divulgados por diferentes meios.
- **CEMAT02:** Propor ou participar de ações para investigar desafios do mundo contemporâ-

neo e tomar decisões éticas e socialmente responsáveis, com base na análise de problemas sociais, como os voltados a situações de saúde, sustentabilidade, das implicações da tecnologia no mundo do trabalho, entre outros, mobilizando e articulando conceitos, procedimentos e linguagens próprios da Matemática.

**Habilidades específicas (Ensino Médio)**:

- **(EM13MAT301):** Resolver e elaborar problemas do cotidiano, da Matemática e de outras áreas do conhecimento, que envolvem equações lineares, quadráticas e exponenciais, além de sistemas lineares, utilizando estratégias diversas, como a modelagem matemática e o uso de tecnologias digitais.
- **(EM13MAT307):** Empregar diferentes métodos para a obtenção da medida da área de uma superfície (reconfigurações, aproximação por cortes etc.) e deduzir expressões de cálculo para aplicá-las em situações reais (terrenos, plantações, ambientes etc.), inclusive com o uso de tecnologias digitais.
- **(EM13MAT309):** Resolver e elaborar problemas que envolvam o cálculo de áreas de figuras planas e de poliedros em contextos como plantas de imóveis, objetos tridimensionais, embalagens etc., com e sem apoio de tecnologias digitais.
- **(EM13MAT402):** Converter representações algébricas de funções polinomiais de 2ž grau em representações geométricas no plano cartesiano, distinguindo os casos nos quais uma variável for diretamente proporcional ao quadrado da outra, recorrendo ou não a softwares ou aplicativos de álgebra e geometria dinâmica, entre outros materiais.
- **(EM13MAT501):** Investigar relações entre números expressos em diferentes formas (percentual, racional, irracional, real), observando regularidades e estabelecendo generalizações associadas a sequências numéricas e progressões aritméticas e geométricas.
- **(EM13MAT502):** Investigar propriedades de figuras geométricas planas e espaciais, como simetrias, posições relativas entre elas, congruência e semelhança de figuras, utilizando transformações geométricas como translação, rotação, reflexão e homotetia, inclusive com o apoio de tecnologias digitais.

# 3 PLANOS DE AULAS

## 3.1 Aula 1: Revisões e introdução - o problema dos números congruentes

**Duração**: 50 minutos.

**Conteúdo**: Teorema de Pitágoras, cálculo de área de triângulos retângulos, números racionais como medidas de lados de triângulos, introdução ao problema dos números congruentes, definição clássica de número congruente (área de triângulo retângulo racional).

**Objetivo geral da aula:** Revisitar o teorema de Pitágoras e o cálculo de área de triângulos retângulos, e introduzir a problemática que motivou o surgimento do problema dos números congruentes.

**Objetivos específicos**: Ao final desta aula, o aluno deverá ser capaz de:

- Aplicar o Teorema de Pitágoras para verificar se um triângulo com lados dados é retângulo.
- Calcular a área de triângulos retângulos cujos lados são números inteiros.
- Calcular a área de triângulos retângulos cujos lados são números racionais.
- Apresentar o questionamento que motivou o surgimento do problema dos números congruentes.

**Recursos/Materiais:** Lousa, pincel, calculadora (opcional).

**Metodologia/Procedimentos**:

1. **Revisão (15 min)**:
   - Inicie com uma breve revisão do Teorema de Pitágoras $\left(a^2+b^2=c^2\right)$ e da fórmula da área de um triângulo $\left(A=\frac{\text{base}\times\text{altura}}{2}\right)$.
   - Propor exemplos com números inteiros para os lados, como o triângulo $(3,4,5)$ e calcular sua área (6).
2. **Introduzindo lados racionais (20 min)**:
   - Questione aos alunos: "Os lados de um triângulo retângulo precisam ser sempre números inteiros?". Introduzir a ideia de lados racionais (frações/decimais).
   - Apresentar o triângulo com lados $\frac{3}{2}$, $\frac{20}{3}$ e $\frac{41}{6}$. Pedir aos alunos para verificarem se é um triângulo retângulo (usando o Teorema de Pitágoras) e calcularem sua área.
     - Verificação:

       $$\left(\frac{3}{2}\right)^2+\left(\frac{20}{3}\right)^2=\frac{9}{4}+\frac{400}{9}=\frac{81+1600}{36}=\frac{1681}{36}=\left(\frac{41}{6}\right)^2.$$ É retângulo!

     - Área: $\frac{1}{2}\cdot\frac{3}{2}\cdot\frac{20}{3}=\frac{60}{12}=5$.

- Evidenciar ao aluno que triângulos racionais sempre tem área racional.

3. **Problema central (15 min)**:
   - Lançar a pergunta central que motiva o estudo: "Será que qualquer número racional (ou, mais especificamente, qualquer número inteiro) positivo pode ser a área de um triângulo retângulo com lados racionais?".
   - Promover uma breve discussão. Anotar as hipóteses dos alunos.

**Avaliação**: A avaliação será contínua e participativa, observando o interesse do aluno e a resolução dos cálculos propostos.

## 3.2 Aula 2: Em busca dos números congruentes e o papel dos ternos pitagóricos

**Duração**: 50 minutos.

**Conteúdo**: Definição de números congruentes, ternos pitagóricos (primitivos e derivados), fórmula de Euclides para geração de ternos pitagóricos primitivos.

**Objetivo geral da aula**: Formalizar o problema dos números congruentes, e analisar o papel dos ternos pitagóricos.

**Objetivos específicos**: Ao final desta aula, o aluno deverá ser capaz de:

- Definir o que são ternos pitagóricos primitivos e derivados.
- Aplicar a Fórmula de Euclides para gerar ternos pitagóricos primitivos, dadas as condições para $m$ e $n$.
- Calcular a área do triângulo retângulo associado a um terno pitagórico.

**Recursos/Materiais:** Lousa, pincel, calculadora (opcional).

**Metodologia/Procedimentos**:

1. **Formalizar o problema (10 min)**:
   - Apresentar a definição formal de números congruentes:

     **Definição 3.2.1** *Um número racional positivo n é dito congruente se existe um triangulo retângulo racional de área n: existem racionais* $a, b, c > 0$*, tais que* $a^2 + b^2 = c^2$ *e* $(1/2)ab = n$.

2. **Ternos pitagóricos (15 min)**:
   - Defina como **Ternos Pitagóricos** uma tripla de inteiros positivos $(a, b, c)$ tais que $a^2 + b^2 = c^2$.
   - Definir que um terno pitagórico é dito primitivo, se $mdc(a, b, c) = 1$. Do contrário ele é dito derivado.
   - Exemplificar: $(3, 4, 5)$ é primitivo; $(6, 8, 10)$ é derivado.
   - Pedir aos alunos que procurem outros exemplos de ternos pitagóricos.
3. **Gerando ternos pitagóricos fórmula de Euclides (20 min)**:
   - Dialogar com os alunos sobre a importância de possuir um bom método de gerar ternos pitagóricos para assim obter mais triângulos retângulos (e consequentemente, mais números congruentes).
   - Apresentar a **Fórmula de Euclides** para gerar ternos pitagóricos primitivos:

**Teorema 3.2.2** *Dados $m > n > 0$ inteiros, primos entre si, e com paridades opostas, então $a = m^2 - n^2$, $b = 2mn$, $c = m^2 + n^2$ definem um terno pitagórico primitivo.*

- Atente os alunos as condições de $m$ e $n$ no Teorema 3.2.2 acima.
- **Atividade em Grupo:** Dividir a turma em grupos e pedir para cada grupo gerar 2 a 3 ternos pitagóricos primitivos usando diferentes valores de $m$ e $n$ que satisfaçam as condições da fórmula de Euclides.
  - Exemplo: $m = 2, n = 1 \Rightarrow a = 3, b = 4, c = 5$. Área = $\frac{1}{2} \cdot 3 \cdot 4 = 6$.
  - Exemplo: $m = 3, n = 2 \Rightarrow a = 5, b = 12, c = 13$. Área = $\frac{1}{2} \cdot 5 \cdot 12 = 30$.
  - Exemplo: $m = 4, n = 1 \Rightarrow a = 15, b = 8, c = 17$. Área = $\frac{1}{2} \cdot 15 \cdot 8 = 60$.

4. **Conclusão (5 min)**: Para concluir a aula, proponha aos alunos que completem em casa uma tabela contendo de 5 a 6 entradas (similar ao exemplo fornecido abaixo). A tarefa consistirá em identificar e adicionar números congruentes à tabela.

Tabela 1 – Tabela para registro de ternos pitagóricos e números congruentes

| **Valor de $m$** | **Valor de $n$** | **Terno $(a, b, c)$** | **Número congruente obtido (área)** |
|---|---|---|---|

Fonte: Elaborado pelo autor (2025).

**Avaliação**: A avaliação será contínua e participativa, observando o interesse do aluno com foco na participação na atividade em grupo proposta.

## 3.3 Aula 3: Os inteiros livres de quadrados

**Duração**: 50 minutos.

**Conteúdo**: Inteiros livres de quadrados, semelhança e razão entre áreas de figuras semelhantes.

**Objetivo geral da aula:** Definir o conceito de inteiros livres de quadrados e sua importante relação com o problema dos números congruentes.

**Objetivos específicos**: Ao final desta aula, o aluno deverá ser capaz de:

- Definir o que é um inteiro livre de quadrados.
- Encontrar a parte livre de quadrados de um inteiro qualquer.
- Reconhecer a possibilidade de converter qualquer número racional em um inteiro livre de quadrados através da multiplicação por um fator adequado.
- Compreender que a razão entre as áreas de duas figuras semelhantes, é o quadrado da razão de semelhança.
- Obter novos números congruentes (inteiros ou racionais) a partir de números congruentes já conhecidos.
- Entender como o escalonamento de triângulos permite reduzir o problema da congruência de um racional à congruência de um inteiro livre de quadrados.

**Recursos/Materiais**: Lousa, pincel.

**Metodologia/Procedimentos**:

1. **Retomando a aula anterior (5 min)**:
   - Peça para que alguns alunos apresentem os números que utilizaram para preencher a tabela deixada ao fim da aula anterior (Tabela 1). Analise se os valores estão corretos.
2. **Áreas e inteiros livres de quadrados (35 min):**
   - Introduzir a definição de **inteiro livre de quadrados**:

     **Definição 3.3.1** *Um inteiro positivo $n$ é dito livre de quadrados se, dado um inteiro $p$, tal que $p^2 \mid n$, então $p = 1$.*

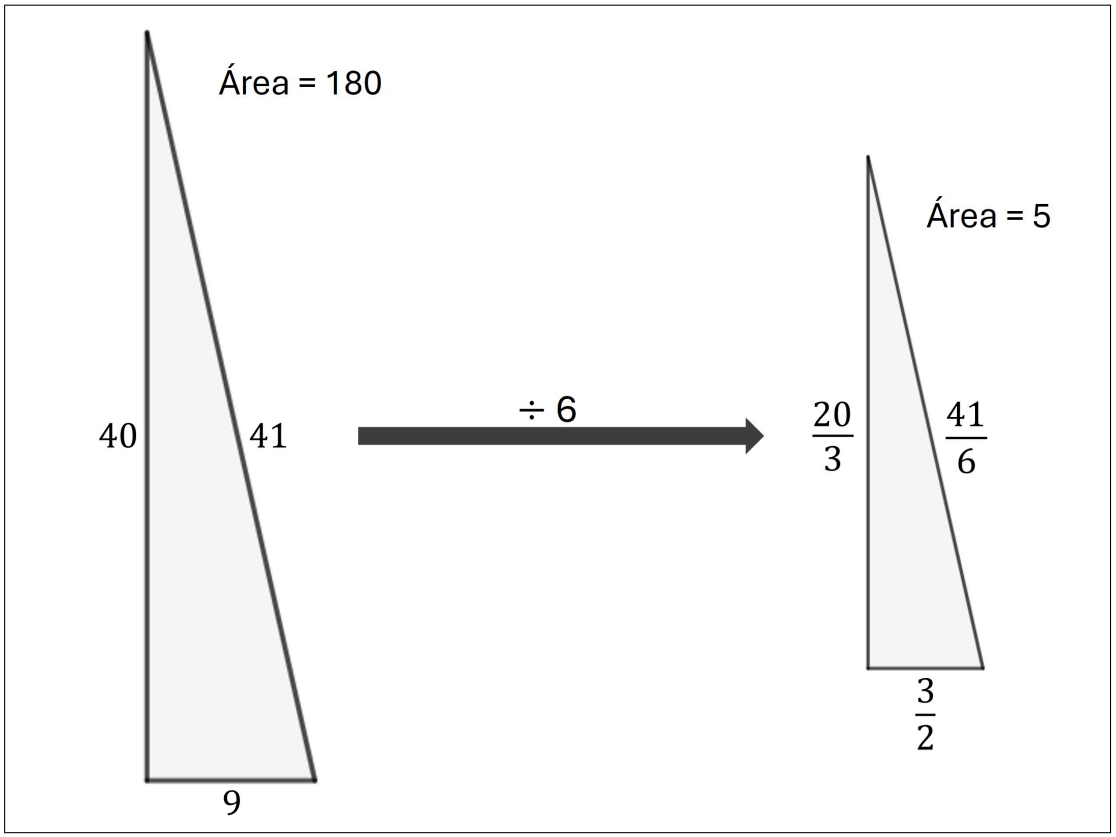
     - Simplifique a Definição 3.3.1 acima, argumentando aos alunos que um inteiro $n$ é dito livre de quadrados simplesmente se não é divisível por nenhum quadrado perfeito maior que 1.
   - **(Atividade sugerida)** Peça para que cada aluno encontre a parte livre de quadrados das áreas obtidas na tabela deixada na aula anterior (última coluna da Tabela 1).
   - Dialogue/revise que; "a razão entre as áreas, é o quadrado da razão de semelhança".

Em seguida apresente a ideia de que basta focar na procura de números congruentes entre os inteiros livres de quadrados, pois, por exemplo, se 6 é congruente, então qualquer número da forma $6 \cdot k^2$, $k \in \mathbb{Q}$, será congruente, basta multiplicar os lados de um triângulo de área 6 pelo fator $k$.

  - Exemplo: Como 6 é congruente, então $24 = 6 \cdot 2^2$ também é congruente, basta tomar o triângulo definido pelo terno $(3, 4, 5)$ que tem área 6 e multiplicar seus lados por 2, obtendo assim um triângulo $(6, 8, 10)$ de área 24.

– Argumente que qualquer racional $q$ pode ser "convertido" em um inteiro livre de quadrados ao multiplica-lo por um racional quadrado "bem escolhido". Ou seja, $q$ é congruente, se o inteiro livre de quadrados obtido também for.
  - Exemplo: $\frac{12}{7}$ quando multiplicado por $\left(\frac{7}{2}\right)^2$ resulta em 21 (livre de quadrados).
  - Exemplo: $\frac{23}{18}$ quando multiplicado por $(3 \cdot 2)^2$ resulta em 46 (livre de quadrados).
– Mostrar que 5 é congruente; tomando $m = 5$ e $n = 4$ nas fórmulas de Euclides, obtemos que 180 é um número congruente, pois é á área do triângulo definido pelo terno $(9, 40, 41)$. Como $180 = 5 \cdot 6^2$, então dividindo os lados deste triângulo por 6, obtemos o triângulo $\left(\frac{9}{6}, \frac{40}{6}, \frac{41}{6}\right) = \left(\frac{3}{2}, \frac{20}{3}, \frac{41}{6}\right)$, que tem área 5 (figura 1).

Figura 1 – Escalonamento do triângulo de área 180 (imagem fora de escala)




Fonte: Elaborado pelo autor (2025).

3. **Discussão final (10 min)**:
   - Questione os alunos sobre o seguinte fato; "As formulas de Euclides nos ajudam a encontrar números congruentes, mas e como saber se um número escolhido ao acaso é congruente?"
   - Mostre aos alunos que o número 53, só é gerado pelos ternos pitagóricos de Euclides quando; $n = 1873180325$ e $m = 1158313156$, tais valores vão gerar o terno pitagórico; $(2167115162604425289, 4339458828015711400, 4850493897329785961)$.
   - Dialogue que exemplos como o 53 revelam que o problema dos números congruentes, por mais simples que aparente ser, esconde um grande desafio na busca por demonstrar quais números são ou não congruentes.

**Avaliação**: A avaliação será contínua e participativa, observando o interesse do aluno, a resolução dos cálculos propostos e a entrega da atividade de casa proposta na aula anterior.

## 3.4 Aula 4: Contexto histórico e uma outra face dos números congruentes

**Duração**: 50 minutos.

**Conteúdo**: Contexto histórico do problema dos números congruentes, a não congruência do 1 e suas implicações, conexão da irracionalidade do $\sqrt{2}$ com números congruentes.

**Objetivo geral da aula**: Apresentar o contexto histórico do problema dos números congruentes, discutir o significado e as implicações da não congruência do número 1, e introduzir a conexão com a irracionalidade da $\sqrt{2}$.

**Objetivos específicos**: Ao final desta aula, o aluno deverá ser capaz de:

- Identificar marcos importantes e matemáticos chave na história do problema dos números congruentes, como Fibonacci e Fermat.
- Reconhecer que o problema dos números congruentes, apesar de sua formulação simples, é um problema antigo e ainda relevante na matemática.
- Explicar a importância do resultado da não congruência do 1, incluindo a consequência de que nenhum quadrado de um número racional pode ser um número congruente.
- Compreender o argumento que utiliza a não congruência do número 1 para demonstrar a irracionalidade de $\sqrt{2}$ a partir do triângulo retângulo de área 1 com catetos $\sqrt{2}$.

**Recursos/Materiais**: Lousa, pincel, projetor, calculadora.

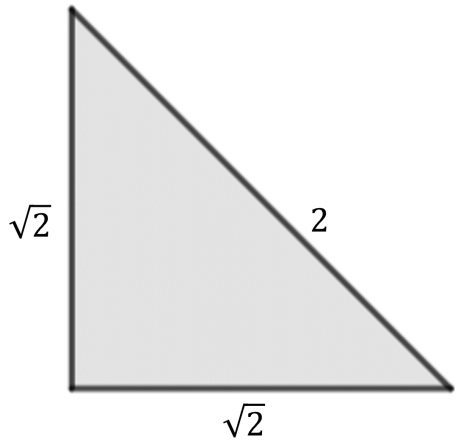
**Metodologia/Procedimentos**:

1. **A história do problema (20 min)**:
    - Relembrar o questionamento final da aula passada; "como saber se um número qualquer dado é congruente?". Destaque que este é um dos motivos que torna o problema dos números congruentes tão intrigante.
    - Dialogue um pouco sobre o contexto histórico do problema para chamar a atenção dos alunos. Cite que os primeiros vestígios do problema vêm de manuscritos árabes de cerca de mil anos atrás e que o problema ganhou força no "Livro dos Quadrados", publicado em 1225 por Fibonacci. Ou seja, apesar de ser um problema de formulação simples, ele já está em estudo a cerca de mil anos.
    - Comente que nos dias de hoje, para que o problema esteja totalmente resolvido, ele depende de um outro problema (conjectura) ainda em aberto na matemática, e que este problema, junto de outros seis (conhecidos como os *Sete Problemas do Milênio*), tem uma premiação de um milhão de dólares (pago pelo *Instituto Clay de Matemática*, localizado em Cambridge, Massachusetts, nos Estados Unidos) para

quem resolver qualquer um destes problemas. Até o momento apenas um destes sete problemas já foi resolvido.

2. **A não congruência do 1 (10 min)**:
   - Comente que no século XVII, o matemático francês *Fermat*, provou que o 1 não é congruente.
   - Destaque a importância deste resultado, mostrando que se 1 fosse congruente, então todo número racional quadrado seria congruente, pois para provar que $q^2$, $q \in \mathbb{Q}$, é congruente, bastava escalonar o triângulo retângulo racional de área 1 (se existisse) multiplicando seus lados por $q$ para obter um triângulo retângulo racional de área $q^2$.
3. **Consequência da "incongruência"do 1 (10 min)**:
   - Apresente aos alunos o triângulo retângulo isósceles apresentado na figura abaixo (figura 2). Este triângulo possui catetos de medida $\sqrt{2}$ e, consequentemente, hipotenusa igual a 2. A sua área é calculada como; Área $= \frac{1}{2} \cdot \sqrt{2} \cdot \sqrt{2} = 1$. Se $\sqrt{2}$ fosse um número racional, então os lados deste triângulo $(\sqrt{2}, \sqrt{2}, 2)$ seriam racionais. Neste caso, por definição, sua área que é igual a 1, seria um número congruente. Contudo, é sabido que 1 não é um número congruente. Essa contradição implica que a premissa inicial de que $\sqrt{2}$ é racional é falsa. Portanto, $\sqrt{2}$ é um número irracional.

Figura 2 – Triângulo retângulo (não racional) de área 1




Fonte: Elaborado pelo autor (2025).

   - (opcional) Para os estudantes que já conhecem outras demonstrações da irracionalidade de $\sqrt{2}$, comente que esta abordagem ressalta uma interessante conexão da teoria dos números congruentes com um problema de outra área, oferecendo uma

perspectiva alternativa. Reforçando a inegável relevância do problema.

4. **Conclusão (10 min)**: Finalize a aula mostrando (se possível com auxílio de projetor) aos alunos a Tabela 2 a seguir, contendo todos os números congruentes até o 100, e alguns números (ou classes de números) não congruentes.

Tabela 2 – Exemplos de Números congruentes e não congruentes

| **Números congruentes** | **Números não congruentes** |
|---|---|
| 5 6 7 13<br>14 15 20 21<br>22 23 24 26<br>28 29 30 31<br>33 34 37 38<br>39 41 45 46<br>47 52 53 54<br>55 56 57 58<br>60 61 62 63<br>65 66 69 70<br>71 73 74 77<br>78 79 80 82<br>84 85 86 87<br>88 89 92 93<br>94 95 96 97<br>... | – 1, 2, 3.<br>– Todo primo $p$ tal que $p \equiv 3 \pmod 8$ (resultado devido a Genocchi). Ex: 11, 19, 43, ...<br>– $q^2$, para todo $q \in \mathbb{Q}$ (i.e., nenhum quadrado de um racional é congruente). Ex: $\frac{1}{9}$, 0.25, 4, 36, ... |

Fonte: Elaborado pelo autor (2025).

**Avaliação**: A avaliação será contínua e participativa, observando o interesse do aluno e a resolução dos cálculos propostos.

## 3.5 Aula 5: Números congruentes - uma outra interpretação

**Duração**: 50 minutos.

**Conteúdo**: Definição de números congruentes por progressão aritmética, origem do nome "número congruente", teorema de equivalência entre as definições de números congruentes.

**Objetivo geral da aula**: Introduzir a segunda definição de números congruentes, relacionada a progressões aritméticas de três quadrados racionais.

**Objetivos específicos**. Ao final desta aula, o aluno deverá ser capaz de:

- Enunciar a segunda definição de número congruente: um número $n$ é congruente se existem três quadrados de números racionais em progressão aritmética de razão $n$.
- Compreender que existe uma equivalência entre as definições de números congruentes por área de triângulos e por progressão aritmética.
- Verificar se três quadrados racionais dados formam uma progressão aritmética de razão $n$.
- Encontrar três racionais quadrados em progressão aritmética de razão $n$ a partir de um triângulo retângulo com lados racionais e área $n$.

**Recursos/Materiais**: Lousa, pincel, projetor, calculadora.

**Metodologia/Procedimento**:

1. **Uma nova perspectiva (15 min)**:
   - Relembrar a primeira definição de número congruente (área).
   - Introduzir a segunda definição:

     **Definição 3.5.1** *Um número inteiro n é um número congruente se existir um $a^2$ (com $a \in \mathbb{Q}$) tal que $a^2 - n$ e $a^2 + n$ sejam ambos racionais quadrados.*

   - Ressaltar que a definição 3.5.1 é equivalente a dizer que existem três racionais quadrados; $a^2 - n$, $a^2$ e $a^2 + n$ que formam uma progressão aritmética de razão $n$. Mencionar que esta definição está ligada à origem do nome "número congruente", pois quando *Fibonacci* assim define números congruentes, ele está tomando três números $(a^2 - n, a^2$ e $a^2 + n)$, onde todos são **congruentes** modulo $n$ (todos deixam o mesmo resto na divisão por $n$).
2. **A equivalência (10 min)**:
   - Apresentar o Teorema 3.5.2 a seguir, que estabelece a equivalência entre as duas definições. Não é preciso demonstrá-lo, mas citar que ele mostra a correspondência matemática que transforma um triângulo $(a, b, c)$ de área $n$ em uma terna $(r, s, t)$ tal

que $r^2$, $s^2$ e $t^2$ são os quadrados em *PA* de razão $n$, e vice-versa.

**Teorema 3.5.2** *Seja $n > 0, n \in \mathbb{Q}$. Existe uma correspondência biunívoca entre triângulos retângulos $(a,b,c)$ de área n racionais com área n, e os trios de racionais $(r,s,t)$ tais que $s^2 - r^2 = t^2 - s^2 = n$ (ou seja, $r^2$, $s^2$ e $t^2$ estão em PA de razão n. Essa correspondência é dada por:*

$$(a,b,c) \mapsto \left(\frac{(b-a)}{2}, \frac{c}{2}, \frac{b+a}{2}\right), \quad (r,s,t) \mapsto (t-r, t+r, 2s).$$

3. **Exemplos práticos (20 min)**:
   - O triângulo $(3,4,5)$ tem área 6. A correspondência $(a,b,c) \mapsto \left(\frac{b-a}{2}, \frac{c}{2}, \frac{b+a}{2}\right)$ do Teorema 3.5.2 leva $(3,4,5)$ em $\left(\frac{1}{2}, \frac{5}{2}, \frac{7}{2}\right)$.
     - Verificação: $\left(\frac{5}{2}\right)^2 - \left(\frac{1}{2}\right)^2 = \frac{25}{4} - \frac{1}{4} = \frac{24}{4} = 6$. E $\left(\frac{7}{2}\right)^2 - \left(\frac{5}{2}\right)^2 = \frac{49}{4} - \frac{25}{4} = \frac{24}{4} = 6$ Portanto, $\frac{1}{4}$, $\frac{25}{4}$ e $\frac{49}{4}$ formam uma *PA* de quadrados racionais com razão 6.
   - Pedir aos alunos que encontrem três quadrados racionais em progressão aritmética de razão 5 a partir do triângulo $\left(\frac{3}{2}, \frac{20}{3}, \frac{41}{6}\right)$ (mantenha a correspondência do Teorema 3.5.2 sempre disponível para visualização dos alunos).
     - Cálculos:
       $r = \frac{\frac{20}{3} - \frac{3}{2}}{2} = \frac{\frac{40-9}{6}}{2} = \frac{31}{12}, \quad s = \frac{\frac{41}{6}}{2} = \frac{41}{12}, \quad t = \frac{\frac{20}{3} + \frac{3}{2}}{2} = \frac{\frac{40+9}{6}}{2} = \frac{49}{12}.$
     - Quadrados:
       $\left(\frac{31}{12}\right)^2 = \frac{961}{144}, \left(\frac{41}{12}\right)^2 = \frac{1681}{144}, \left(\frac{49}{12}\right)^2 = \frac{2401}{144}.$
     - Verificação:
       $\frac{1681}{144} - \frac{961}{144} = \frac{720}{144} = 5$. E $\frac{2401}{144} - \frac{1681}{144} = \frac{720}{144} = 5$.
4. **Conclusão (5 min)**: Debata sobre a flexibilidade que a matemática proporciona ao dar múltiplas formas de enxergar e atacar um mesmo problema, são essas diferentes perspectivas que podem levar a novas descobertas e conexões.

**Avaliação**: A avaliação será contínua e participativa, observando o interesse do aluno e a resolução dos cálculos propostos.

## 3.6 Aula 6 - Números congruentes, curvas elípticas e as fronteiras da matemática

**Duração**: 50 minutos.

**Conteúdo**: Definição de curvas elípticas e sua relação com o problema dos números congruentes e a ideia para obtenção de novos triângulos retângulos de área $n$ a partir de soluções racionais conhecidas da curva elíptica.

**Objetivo geral da aula**: Definir superficialmente o conceito de curvas elípticas e apresentar brevemente a conexão do problema dos números congruentes com curvas elípticas, mostrando que este é um problema que apesar de ter surgido a centenas de anos, ainda é relevante na matemática moderna.

**Objetivos específicos**: Ao final desta aula, o aluno deverá ser capaz de:

- Identificar a equação da curva elíptica $y^2 = x^3 - n^2x$ como uma terceira forma de caracterizar os números congruentes.
- Reconhecer as soluções triviais $(0,0)$, $(n,0)$, $(-n,0)$ desta curva.
- Compreender que um número $n$ é congruente se e somente se a curva elíptica associada possui uma solução racional $(x, y)$ com $y \neq 0$.
- Saber que a existência de uma solução racional não trivial em tal curva implica a existência de infinitas outras, correspondendo a infinitos triângulos de área $n$.

**Recursos/Materiais**: Lousa, pincel, calculadora, projetor e acesso a internet (para construção e exposição de gráficos de curvas elípticas via softwares, ex: GeoGebra)

**Metodologia/Procedimentos**:

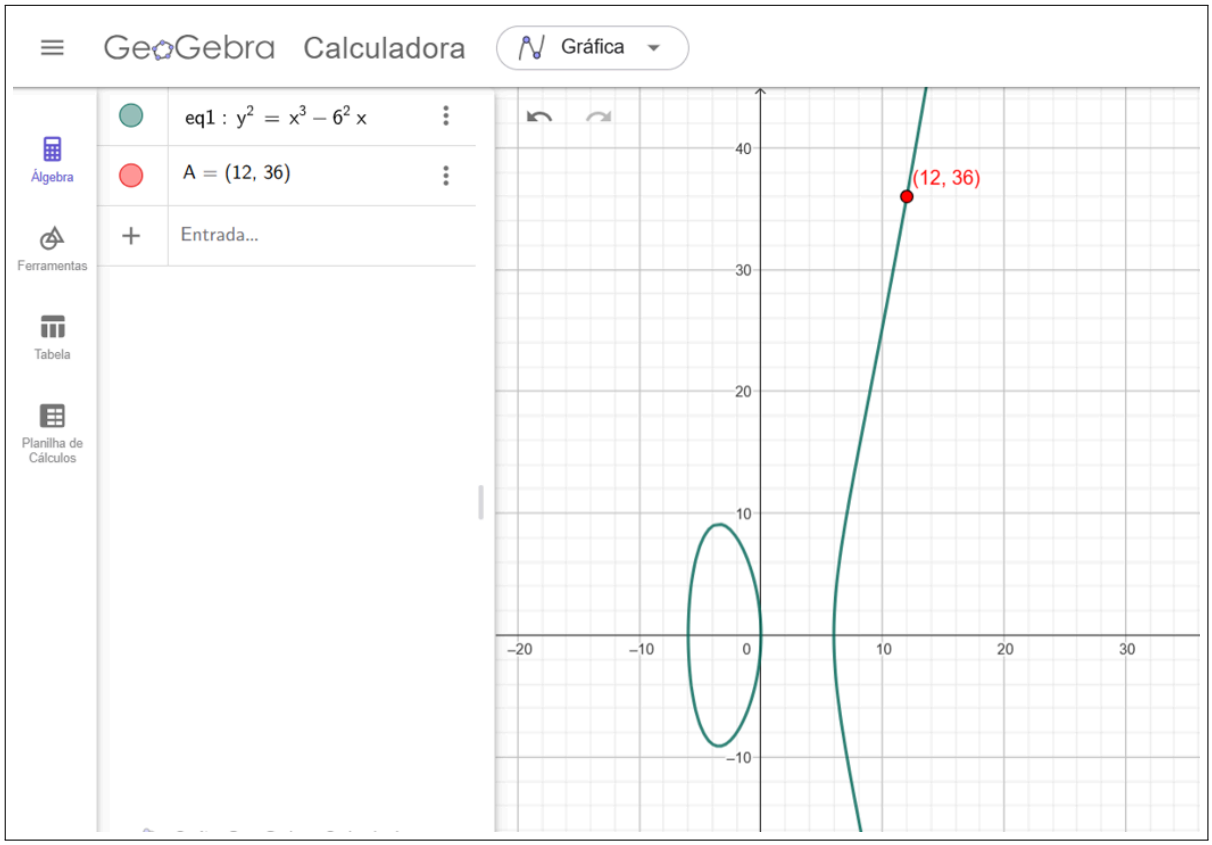
1. **Uma terceira conexão (15 min)**:
   - Relembrar as duas definições de números congruentes (área de triângulos racionais e *PA* de quadrados racionais).
   - Mencionar que o problema também está ligado a encontrar soluções racionais para equações de uma forma específica, chamadas *curvas elípticas*; $y^2 = x^3 - n^2x$.
   - Afirmar que $n$ é congruente se, e somente se, esta equação tem uma solução racional $(x,y)$ com $y \neq 0$.
   - (opcional) Mencionar que existem três soluções triviais ("obvias"); $(0,0)$, $(n,0)$ e $(-n,0)$. Estas soluções valem para qualquer valor de $n$ seja ele racional ou não.
   - Apresentar o Teorema 3.6.1 a seguir (sem demonstra-lo), que faz corresponder a cada triângulo retângulo racionais de área $n$ uma solução racional da curva $y^2 = x^3 - n^2x$.

**Teorema 3.6.1** *Seja $n > 0$, existe uma correspondência biunívoca (ida e volta) entre os triângulos retângulos racionais $(a, b, c)$ de área n, e as soluções $(x, y)$ da equação $y^2 = x^3 - n^2x$. Essa correspondência é dada por:*

$$(a, b, c) \mapsto \left( \frac{nb}{c-a}, \frac{2n^2}{c-a} \right), \quad (x, y) \mapsto \left( \frac{x^2 - n^2}{y}, \frac{2nx}{y}, \frac{x^2 + n^2}{y} \right).$$

2. **Visualizando curvas elípticas (15 min)**:
   - Mostrar o gráfico da curva para $n = 6$ ($y^2 = x^3 - 36x$). Como 6 é congruente (triângulo de lados 3, 4 e 5), existe um ponto racional com $y \neq 0$. Tal triângulo corresponde ao ponto $(x, y) = (12, 36)$ na curva. (Visualizar com GeoGebra, como exemplificado na figura a seguir). Faça os cálculos de correspondia do Teorema 3.6.1 junto aos alunos, para mostrar a veracidade de que $(3, 4, 5) \mapsto (12, 36)$.

Figura 3 – Renderização do gráfico da curva elíptica $y^2 = x^3 - 6^2x$ (software *GeoGebra*)

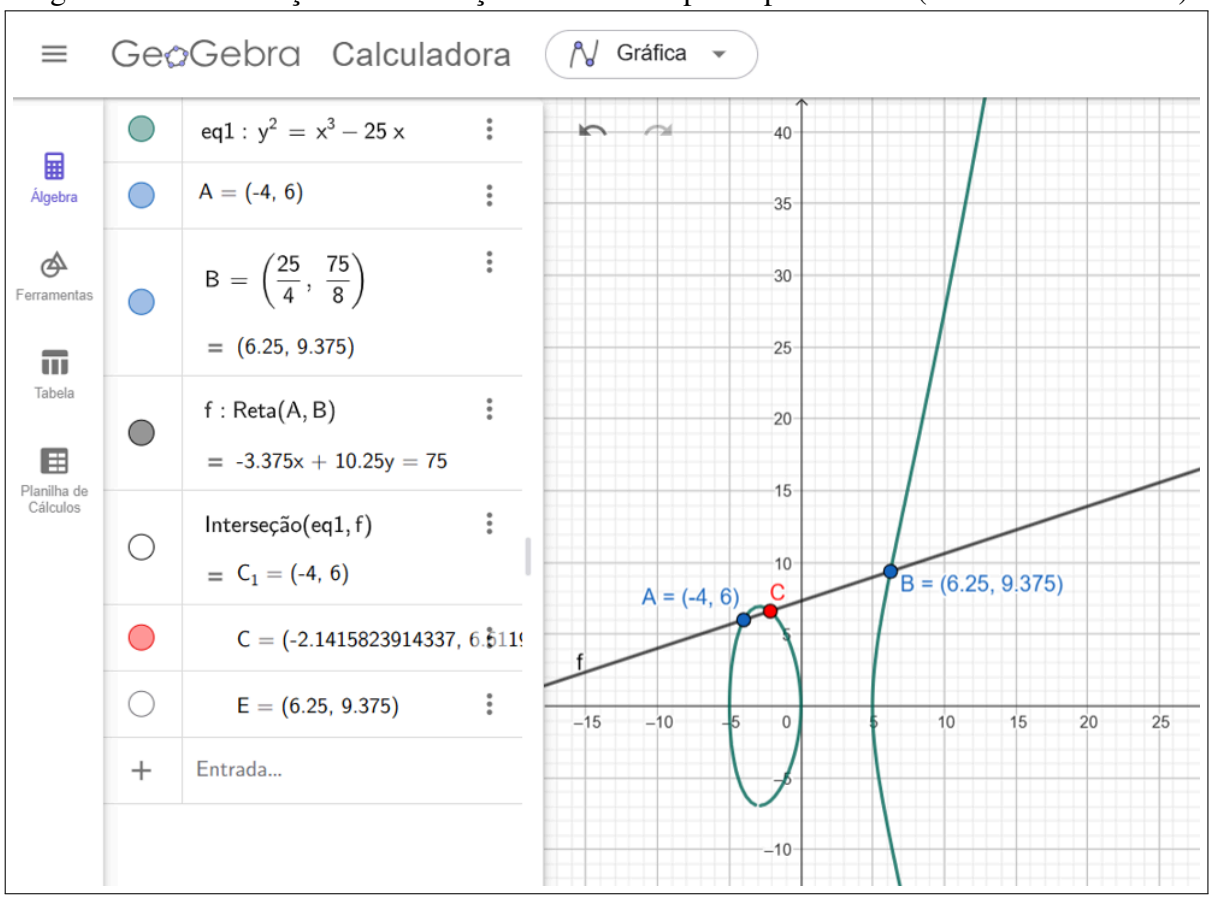



Fonte: Elaborado pelo autor (2025).

   - Afirme que uma curva elíptica não representa uma função. Questione aos alunos se eles podem provar isso (indique que o gráfico pode ajudar).
     - Existem valores de $x$ com mais de um correspondente $y$. Para $x = 12$ na curva $y^2 = x^3 - 36x$, $y$ pode ser igual a 36 ou $-36$.

3. **Gerando novas soluções (10 min)**:
   - Apresente aos alunos a ideia de buscar novos pontos da curva usando pontos já conhecidos. Dado dois pontos da curva, pode-se obter um terceiro ponto (e consequentemente uma terceira solução) tomando a reta que passar por estes dois pontos e analisando sua terceira interseção com a curva elíptica. Utilize o GeoGebra (ou software similar) para construir essas retas em tempo real.
     - O exemplo da Figura 4 abaixo contém a curva $y^2 = x^3 - 25x$, onde o ponto $C$ é obtido a partir da interseção da reta que passa pelos pontos $A$ e $B$.
     - (observação ao professor) A coordenada do ponto $C$ pode ser encontrada, mas não é o objetivo desta aula, dado o foco na educação básica.

Figura 4 – Renderização da construção de um novo ponto por secante (software *GeoGebra*)




Fonte: Elaborado pelo autor (2025).

4. **Conclusões e reflexões (10 min)**:
   - Reflita com os alunos concluindo esse ciclo de aulas sobre como o problema dos números congruentes, que começou com uma pergunta geométrica simples, hoje se conecta com áreas avançadas da matemática.

- Discuta com os alunos que as curvas elípticas vão muito além de apenas mais uma interpretação para o problema dos números congruentes, mas que podem ser a chave para responder de maneira definitiva quais números são ou não congruentes.
- Comente que o resultado que mais se aproxima de solucionar o problema de maneira definitiva deve-se ao matemático estadunidense *Jerrold Tunnell*. Mas a completude do seu resultado ainda depende de um problema em aberto na matemática, como já citado, problema este que o *instituto Clay de Matemática* oferece uma premiação de um milhão de dólares a quem resolve-lo.

**Avaliação**: A avaliação será contínua e participativa, observando o interesse do aluno e a resolução dos cálculos propostos.

# 4 SUGESTÕES DE AVALIAÇÃO

Visto que este conjunto de aulas propõe a explanação de um conteúdo à parte dos livros didáticos, não recomenda-se a realização de uma avaliação por meio de prova única, mas como exposto ao longo dos planos de aula, a avaliação deve ser contínua e processual, considerando as particularidades dos alunos, a realização das atividades propostas durantes as aulas e a capacidade de explicar os conceitos com suas próprias palavras. Abaixo seguem algumas sugestões de atividades que podem compor a avaliação:

- **Observação da participação** em discussões e atividades em grupo.
- **Resolução de listas de exercícios** contendo:
  - Verificação se um trio de números forma um terno pitagórico.
  - Geração de ternos pitagóricos usando a fórmula de Euclides.
  - Cálculo de áreas de triângulos retângulos com lados racionais.
  - Identificação da parte livre de quadrados de um número.
  - Conversão de um trio de racionais $(a, b, c)$ que representam os lados de um triângulo de área $n$ em três racionais quadrados que determinam uma *PA* de razão $n$ (permitir consulta ao Teorema 3.5.2).
  - Conversão de um trio de racionais $(a, b, c)$ que representam os lados de um triângulo de área $n$ em uma solução racional para a equação $y^2 = x^3 - n^2x$ (permitir consulta ao Teorema 3.6.1).
- **Um pequeno projeto de pesquisa (opcional):**
  - Encontrar triângulos que provem a congruência de pelo menos três exemplos da Tabela 2 dentre os que não foram demonstrados ao decorrer das aulas.
- **Um problema desafio ao final da sequência**:
  - Exemplo: "Números como o 4, 9 e 16, são congruentes? Justifique com base no que aprendeu." (Espera-se que usem o resultado sobre quadrados não serem congruentes).

# REFERÊNCIAS

BRASIL. **Base Nacional Comum Curricular**. Brasília, DF: Ministério da Educação, 2018. Disponível em: https://basenacionalcomum.mec.gov.br/images/BNCC_EI_EF_110518_versaofinal_site.pdf. Acesso em: 09 mar. 2025.

COSTA, D. E.; GONÇALVES, T. O. Compreensões, abordagens, conceitos e definições de sequência didática na área de educação matemática. **Bolema: Boletim de Educação Matemática**, v. 36, n. 72, p. 358–388, 2022. Disponível em: https://www.scielo.br/j/bolema/a/TBtxkXdxLr5JnHCrcyWfSWL/?format=pdf&lang=pt. Acesso em: 09 mar. 2025.

RODRIGUEZ, J. E. A.; SOUZA, N. R. d. O problema dos números congruentes: três versões equivalentes. **Proceeding Series of the Brazilian Society of Applied and Computational Mathematics**, [*s. l.*], v. 5, n. 1, p. 1–7, 2017. Disponível em: https://proceedings.sbmac.org.br/sbmac/article/viewFile/1428/1441. Acesso em: 03 fev. 2025.

SANTANA, J. R.; NETO, H. B.; ROCHA, E. M. A seqüência fedathi: uma proposta de mediação pedagógica no ensino de matemática. In: SBEM. **Anais do 8º Encontro Nacional de Educação Matemática**. Recife, PE, Brasil, 2004. p. 1–11. Disponível em: http://www.sbembrasil.org.br/files/viii/pdf/07/MC15472834830.pdf. Acesso em: 08 mar. 2025.