DOI: 10.22481/intermaths.v3i1.10132

Article | Artigo

INTERMATHS
ISSN 2675-8318
Vol. 3, N. 1, Jan - Jun 2022, pp. 88 – 106

Conexões entre Números Congruentes e Curvas Elípticas

Jaime Edmundo Apaza Rodriguez

Universidade Estadual Paulista (UNESP), Câmpus de Ilha Solteira, SP, Brasil

jaime.rodriguez@unesp.br

Connections between Congruent Numbres and Elliptic Curves

Resumo

As Curvas Elípticas têm sido muito usadas para o tratamento de problemas importantes como a Criptografia, o Problema do Empacotamento de Esferas, o Problema dos Números Congruentes, entre outros. Uma das principais características de uma Curva Elíptica E é que o conjunto de seus pontos racionais, $E(\mathbb{Q})$, tem uma estrutura de grupo abeliano finitamente gerado. Especificamente tem-se o famoso teorema provado por Mordell para Curvas Elípticas Racionais (em 1922) e generalizado por Weil para Curvas Elípticas sobre Corpos de Números (em 1928), o qual afirma que $E(\mathbb{Q})$ é um grupo abeliano finitamente gerado. O teorema de estrutura para grupos finitamente gerados garante que é possível decompor o grupo $E(\mathbb{Q})$ na forma $E(\mathbb{Q}) = E(\mathbb{Q})_{tor} \oplus \mathbb{Z}^r$, onde $E(\mathbb{Q})_{tor}$ é o subgrupo de pontos de torção (elementos de ordem finito) e r é um número inteiro chamado o posto de $E(\mathbb{Q})$ (posto algébrico da curva elíptica, é um invariante da curva). Por outro lado, um número racional é dito congruente se ele representa a área de um triângulo retângulo cujos lados são números racionais. O problema dos Números Congruentes consiste precisamente em determinar se um dado número racional é congruente ou não. Neste trabalho apresentamos este problema e discutimos um resultado que estabelece a relação entre Números Congruentes e Curvas Elípticas.

Palavras-chave: Números Congruentes; Curvas Elípticas; Conexões.

Abstract

Elliptical Curves have been widely used to treat problems important as Cryptography, the Problem of Packing Spheres, the Problem of Congruent Numbers, and others. One of the main characteristics of an Elliptic Curve E is that the set of rational points, $E(\mathbb{Q})$, it has a finitely generated abelian group structure. Specifically there is the famous theorem proved by Mordell to Rational Elliptic Curves (in 1922) and generalized by Weil to Elliptic Curves over the Bodies of Numbers (1928). The structure theorem for finitely generated groups guarantees that it is possible to decompose the group $E(\mathbb{Q})$ into the form $E(\mathbb{Q}) = E(\mathbb{Q})_{tor} \oplus \mathbb{Z}^r$, where $E(\mathbb{Q})_{tor}$ is the subgroup of torsion points (finite order elements) and r is a integer called the rank of $E(\mathbb{Q})$ (algebraic rank of the elliptic curve, which is an invariant of the curve). On the other hand, a rational number is called congruent if it represents the area of a right triangle whose sides are rational numbers. The Problem of Numbers Congruents consists precisely in determining whether a given rational number is congruent or not. In this work we present this problem and discuss a result that establishes the relationship between Congruent Numbers and Elliptic Curves.

Keywords: Congruent Numbers; Elliptic Curves; Connections.

MSC (2020): 14H52; 97F60.

Submetido em: 11 de janeiro de 2022 – **Aceito em**: 16 de abril de 2022

1 INTRODUÇÃO

Sabe-se que o 6 é o menor número natural que representa a área de um triângulo retângulo cujos comprimentos dos lados são números inteiros. O triângulo retângulo de lados $3, 4\ e\ 5$ é o único triângulo cuja área é 6.

Em 1225, o matemático italiano Leonardo Pisano (Fibonacci) descobriu um triângulo retângulo de lados $3/2, 20/3\ e\ 41/6$, cuja área é 5, o qual é um número natural menor do que 6. Isto levantou a seguinte pergunta: É possível que cada número natural n possa ser representado como a área de um triângulo retângulo cujos lados sejam números racionais? Há 350 anos atrás, Fermat mostrou que a resposta é negativa para $n = 1, 2$ ou 3 (e portanto para $n = 4$, por ser um quadrado).

O problema dos Números Congruentes consiste em determinar quais são os números naturais que são números congruentes. Um número congruente é um inteiro positivo que pode ser representado pela área de um triângulo retângulo, cujos lados sejam números racionais. Uma definição mais geral inclui todos os números racionais com esta propriedade.

A sequência dos números congruentes começa com $5, 6, 7, 13, 14, 15, 20, 21, 22, 23, 24, \cdots$ Por exemplo, 5 é um número congruente porque representa a área de um triângulo da lados $20/3, 3/2, 41/6$. Similarmente, 6 é um número congruente pois representa a área de um triângulo de lados $3, 4, 5$, enquanto que 3 não é um número congruente por não estar dentro dessas especificações.

Se q é um número (racional) congruente então s^2q também é um número congruente para qualquer número racional s (apenas multiplicar cada lado do triângulo por s). Isso leva à conclusão de que se um número racional q, diferente de zero, é um número congruente, esse fato depende apenas de seus resíduos no grupo quociente $\mathbb{Q}^*/\mathbb{Q}^{*2}$. Cada classe nesse grupo contém exatamente um número inteiro livre de quadrados, de modo que quando se fala em números congruentes, basta considerar números inteiros livre de quadrados.

Ainda hoje não existe um algoritmo incondicional que decida, em um número finito de passos, se um dado número natural n é congruente ou não. É claro que uma forma de provar que um dado número natural n é congruente é produzir um triângulo racional com área n. Mas encontrar tal triângulo é uma tarefa difícil. O matemático americano D. Bernard Zagier demorou um tempo razoável para encontrar um triângulo com todos os lados de comprimento racional e cuja área é o número primo 157.

Se dois triângulos são similares, então seus lados são proporcionais. Se k é a constante de proporcionalidade, a razão entre suas áreas é k^2. Portanto, para tratar o caso geral é necessário considerar unicamente o Problema dos Números Congruentes para números naturais n que não tenham nenhum fator quadrado maior do que 1. Por exemplo, como 1 e 2 não são números congruentes, então $4 = 2^2 \cdot 1,\ 8 = 2^2 \cdot 2\ \ e\ \ 9 = 3^2 \cdot 1$ não podem ser números

congruentes. Assim vamos assumir que os números congruentes são livres de quadrados, ou seja, sem fatores primos repetidos.

Entre os seis números naturais livres de quadrado menores do que 10, três ($5, 6\ e\ 7$) são números congruentes, enquanto os outros não são.

Recentemente o problema dos Números Congruentes veio a tona de novo com a descoberta de uma forte relação deste problema com a Aritmética das Curvas Elípticas, um assunto que se tornou muito popular nas últimas décadas. E nestas notas estudaremos precisamente como acontece essa relação.

2 CURVAS ELÍPTICAS

Nesta seção vamos considerar um corpo $\mathbb{K}$ de característica diferente de 2 e de 3. A forma mais simples de definir um Curva Elíptica é a seguinte.

Definição 2.1. *Uma curva elíptica E sobre $\mathbb{K}$ é uma curva projetiva plana não singular de grau 3, juntamente com o ponto racional O (este ponto é o ponto no infinito).*

Definição 2.2. *Um ponto P sobre uma curva elíptica E é dito ponto de inflexão se a multiplicidade de interseção da reta tangente com a curva E em P é maior ou igual do que 3.*

A multiplicidade de interseção é o número de vezes que se repete esse ponto na interseção da curva com a reta tangente à curva nesse ponto.

O resultado a seguir fornece formas equivalentes de definir uma curva elíptica.

Proposição 2.3. *As seguintes afirmações sobre curvas elípticas são equivalentes:*

(1) Uma curva elíptica E sobre $\mathbb{K}$ é uma curva projetiva plana não singular de grau 3, onde o ponto racional O é ponto de inflexão.

(2) Uma curva elíptica E sobre $\mathbb{K}$ é uma curva projetiva plana não singular de grau 3 da forma

$$E : y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_5z^3,$$

onde os coeficientes $a_i \in \mathbb{K}$ ([2]).

O Teorema de Bezout garante que duas curvas cúbicas projetivas se intersectam em 9 pontos, contando suas multiplicidades.

Dada uma curva elíptica E sobre $\mathbb{K}$, vamos definir uma lei de grupo no conjunto $E(\mathbb{K})$ com os pontos dessa curva. Para tal efeito, definiremos (de forma geométrica) uma operação que denotaremos por $*$. Dados os pontos P e Q na curva E, consideremos a reta passando por estes pontos e que, pelo Teorema de Bezout, interseta à curva E num terceiro ponto

que denotaremos por $P * Q$. Agora, a reta passando pelos pontos O e $P * Q$ interseta à cúbica num novo ponto que denotaremos por $P + Q$. Assim, por construção, temos que $P + Q = O * (P * Q)$.

Teorema 2.4. *Seja E uma curva elíptica sobre $\mathbb{K}$, com um ponto O em $E(\mathbb{K})$. Então $E(\mathbb{K})$ é um grupo abeliano com a operação $+$ anteriormente definida.*

Prova:

a) A operação é comutativa: A reta que passa por $P\ e\ Q$ é a mesma passando por $Q\ e\ P$.

b) $P + O = P$. Seja L é a reta passando por $P\ e\ O$. Pelo Teorema de Bezout, existe um terceiro ponto, $P * O$, na interseção de E com L. Observar que a reta passando por O e $P * O$ é a mesma reta L e portanto o terceiro ponto de interseção é P. Assim $P + O = P$, ou seja, o ponto O é o elemento neutro da lei de grupo.

c) Inverso de um ponto P. Seja L_1 a reta tangente a E no ponto O e Q o terceiro ponto de interseção de E com L_1. Agora, seja L_2 a reta passando por $P\ e\ Q$. Então $-P$ será o terceiro ponto de interseção de E com L_2 (a reta passando por $P\ e\ -P$ é L_2). Logo $P + (-P) = Q$. A reta passando por O e Q é a reta L_1, ou seja, $O + Q = O$. Assim, $P + (-P) = O$.

d) A operação é associativa: Sejam P, Q, R três pontos de E. Para mostrar que $(P + Q) * R = P * (Q + R)$, basta mostrar que $(P + Q) + R = P + (Q + R)$.

Sejam as retas L_1 passando por $P, Q\ e\ P * Q$, e T_1 passando por $O, P * Q\ e\ P + Q$,

L_2 passando por $P + Q,\ R\ e\ (P + Q) * R$, e T_2 passando por $Q, R\ e\ Q * R$,

L_3 passando por $O,\ Q * R\ e\ Q + R$, e T_3 passando por $P,\ Q + R\ e\ P * (Q + R)$.

Considere também as cúbicas E_L definida pela união de $L_1, L_2\ e\ L_3$ e E_T definida pela união de $T_1, T_2\ e\ T_3$.

Observar que $E\ e\ E_L$ se intersectam em 8 pontos: $P,\ Q,\ P*Q,\ R,\ (P+Q)*R,\ O,\ Q*R\ e\ Q + R$.

Também $E\ e\ E_T$ se intersectam nos pontos: $O,\ P * Q,\ P + Q,\ Q,\ R,\ Q * R,\ Q + R,\ P\ e\ P * (Q + R)$.

Assim $E \cap E_L\ e\ E \cap E_T$ têm 8 pontos em comum. Logo o nono ponto de interseção deve ser o mesmo, ou seja, $(P + Q) * R = P * (Q + R)$.

A prova da propriedade associativa está baseada no seguinte resultado.

Proposição 2.5. *Se duas curvas cúbicas em $\mathbb{P}^2(\mathbb{K})$ se intersectam em exatamente 9 pontos, então toda cúbica que passa por 8 destes pontos também passará pelo nono ponto.*

Prova: Sejam $C_f\ e\ C_g$ duas cúbicas, se intersetando em 9 pontos: $P_1, P_2, \cdots, P_9$. Seja h

a cúbica passando por 8 pontos $P_1, \cdots, P_8$. Deve-se mostrar que $P_9 \in h$.

Consideremos uma cúbica da forma

$$f(x, y, z) = a_1x^3 + a_2x^2y + \cdots + a_{10}z^3,$$

com os 10 coeficientes $a_1, \cdots, a_{10}$ em $\mathbb{K}$.

A condição de que C_f passa por um ponto $P = (x : y : z)$ é uma condição linear nos coeficientes a_i, dada por $a_1x^3 + a_2x^2y + \cdots + a_{10}z^3 = 0$.

Os 8 pontos

$$P_1 = (x_1, y_1, z_1), \cdots, P_8 = (x_8, y_8, z_8),$$

estão em "posição geral" se os vetores $(x_i^3, x_i^2y_i, \cdots, z_i^3)$, para $i = 1, \cdots, 8$, são linearmente independentes.

Agora, consideremos o conjunto

$$\Lambda = \{\text{cúbicas passando por } P_1, \cdots, P_8\}.$$

Então, visto como espaço vetorial sobre $\mathbb{K}$, tem-se que $dim(\Lambda) = 2$. Se $C_f \neq C_g$, então f e g são linearmente independentes e $\Lambda = \langle f, g\rangle$. Sendo assim, $h = af + bg$, com $a, b \in \mathbb{K}$. Como $f(P_9) = g(P_9) = 0$, então $h(P_9) = 0$.

Quando os P_i não estão em posição geral, se analisa caso por caso ([4]).

3 FÓRMULAS EXPLÍCITAS PARA A LEI DE GRUPO

É importante saber que qualquer cúbica pode ser transformada em uma nova forma especial, chamada Forma Normal de Weierstrass, que basicamente consiste numa equação da forma $y^2 = 4x^3 - b_2x - b_3$. Em nosso caso usaremos uma forma mais geral que chamaremos de Forma de Weierstrass. Assim, seja E uma curva elíptica (projetiva) sobre $\mathbb{K}$ dada por

$$E : y^2z + a_1xyz + a_3y^2z = x^3 + a_2x^2z + a_4xz^2 + a_6z^3.$$

Para eliminar o termo xyz fazemos a substituição de variáveis

$$x = x',\ y = y' - \frac{a_1}{2}x'\ e\ z = z'.$$

Logo, para eliminar o termo y fazemos a substituição

$$x' = x'' + \frac{a_2}{3}z'', y' = y'' - \frac{a_3}{2}z''\ e\ z' = z''.$$

Desta forma obtemos uma equação da forma

$$y^2z = x^3 + ax^2z + bxz^2 + cz^3.$$

Finalmente fazendo $z = 1$ obtemos a equação (afim)

$$E : y^2 = x^3 + ax^2 + bx + c,$$

que será a equação que usaremos. Dessa forma foi mostrado o seguinte resultado.

Teorema 3.1. *Seja $\mathbb{K}$ um corpo de característica diferente de 2 e de 3. Então toda curva elíptica E é isomorfa a uma curva da forma*

$$E : y^2z = x^3 + ax^2z + bxz^2 + cz^3.$$

Agora vamos encontrar as fórmulas explícitas da lei de grupo de uma curva elíptica. Na equação $y^2z = x^3 + ax^2z + bxz^2 + cz^3$ fazemos $z = 0$ e temos $x^3 = 0$, de onde obtemos o ponto $(0 : 1 : 0)$ de multiplicidade 3 na interseção de E com o plano $z = 0$. Este ponto é o ponto de inflexão da cúbica E. Deste modo, para uma curva elíptica dada na forma de Weierstrass, o ponto $O = (0 : 1 : 0)$ é aquele que se encontra no infinito (em relação ao plano afim $z = 1$).

Podemos afirmar então que o conjunto de pontos $E(\mathbb{K})$ da curva elíptica E é o conjunto de pares (x, y) satisfazendo a equação $y^2 = x^3 + ax^2 + bx + c$, junto com o ponto no infinito $O = (0 : 1 : 0)$.

Dados os pontos $P_1 = (x_1, y_1)$ e $P_2 = (x_2, y_2) \in E(\mathbb{K})$, vamos determinar as coordenadas de $P_1 + P_2$. Sendo $P_1 * P_2 = (x_3, y_3)$ temos que $P_1 + P_2 = (x_3, -y_3)$. A reta passando por P_1 e P_2 é dada por $y = \lambda x + \beta$, onde $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ e $\beta = y_1 - \lambda x_1 = y_2 - \lambda x_2$.

Pelo teorema de Bezout, esta reta corta à cúbica nos pontos P_1, P_2 e $P_1 * P_2$. Para obter o terceiro ponto de interseção basta substituir a equação da reta na cúbica:

$$y^2 = (ax + b)^2 = x^3 + ax^2 + bx + c,$$

de onde obtemos a equação cúbica

$$x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\beta)x + (c - \beta^2) = 0,$$

cujas raízes são as abscissas x_1, x_2 e x_3 dos pontos P_1, P_2 e $P_1 * P_2$ respectivamente. Assim temos

$$x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\beta)x + (c - \beta^2) = (x - x_1)(x - x_2)(x - x_3),$$

de onde, igualando os coeficientes do termo x^2 em ambos os lados, segue

$$a - \lambda^2 = -x_1 - x_2 - x_3,$$

$$x_3 = \lambda^2 - a - x_1 - x_2.$$

Portanto obtemos $P_3 = (x_3, y_3) = (\lambda^2 - a - x_1 - x_2, \lambda x_3 + \beta)$, que são as fórmulas para o cálculo de $P_1 + P_2 = P_3 = (x_3, y_3)$.

Exemplo 3.2. Seja a curva elíptica $E : y^2 = x^3 + 17$ e os pontos $P_1 = (-1, 4)$ e $P_2 = (2, 5)$ em E. Vamos calcular $P_1 + P_2$.

Dado que $\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{5-4}{2-(-1)} = \frac{1}{3}$ e $\beta = y_1 - \lambda x_1 = y_2 - \lambda x_2 = \frac{13}{3}$, então a reta passando por P_1 e P_2 é dada por $y = \frac{1}{3}x + \frac{13}{3}$. Assim temos

$$x_3 = \lambda^2 - a - x_1 - x_2 = -\frac{8}{9} \qquad y_3 = \lambda x_3 + \beta = \frac{109}{27}.$$

Portanto

$$P_1 + P_2 = (x_3, -y_3) = (-\frac{8}{9}, -\frac{109}{27}).$$

4 PONTOS DE ORDEM FINITA

Nesta seção iremos considerar o corpo $\mathbb{K} = \mathbb{Q}$ e faremos um breve estudo sobre os pontos de ordem finita do grupo $E(\mathbb{Q})$.

Definição 4.1. *Dizemos que um ponto P de um grupo tem ordem m se*

$$mP = \underbrace{P + P + \cdots + P}_{m \text{ vezes}} = O,$$

mas $nP \neq O$, para todo n tal que $1 \leq n < m$.

Se m existir, então P tem ordem finita; caso contrário P é de ordem infinita.

A curva elíptica E será dada por

$$E : y^2z = x^3 + ax^2z + bxz^2 + cz^3,$$

com $a, b, c \in \mathbb{Z}$ e $\Delta = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2 \neq 0$.

O modelo afim desta curva é

$$E : y^2 = x^3 + ax^2 + bx + c.$$

Denotaremos por $E(\mathbb{Q})_{tor}$ o subgrupo de torção, ou seja, o grupo dos pontos racionais de ordem finita e $E[m](\mathbb{Q})$ o subgrupo de $E(\mathbb{Q})$ dos pontos P tais que $mP = O$.

Observar que

$$E(\mathbb{Q})_{tor} = \bigcup_{m\geq 1} E[m](\mathbb{Q}).$$

No que segue veremos em particular pontos de ordem 2 e de ordem 3.

Proposição 4.2. *Seja E uma curva cúbica não singular, dada por*

$$E : y^2 = x^3 + ax^2 + bx + c.$$

Então

(1) Um ponto $P = (x, y) \neq O$ em E tem ordem 2 se, e somente se, $y = 0$.

(2) E tem exatamente 3 pontos de ordem 2. Estes pontos, juntamente com o ponto O formam o grupo $E[2]$, o qual é isomorfo a $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

Prova: (1) Temos que

$$2P = O \iff P + P = O \iff P + O = -P \iff P = -P$$

$$\iff (x, y) = (x, -y) \iff y = 0.$$

(2) De (1) temos que se $O \neq P = (x, y) \in E$ tem ordem 2, então $y = 0$. Assim $x^3 + ax^2 + bx + c = 0$. Segue que esta equação tem 3 raízes em $\overline{\mathbb{Q}}$. Como a curva é não singular, as 3 raízes são distintas. Logo existem 3 pontos de ordem 2 e portanto $E[2](\mathbb{Q}) = \{O, P_1, P_2, P_3\}$, onde cada $P_i \neq O$. Agora, como $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ é o único grupo com 4 elementos que não possui elementos de ordem 4 segue que

$$E[2] \cong \{O, P_1, P_2, P_3\} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

Proposição 4.3. *Seja E uma curva cúbica não singular, dada por*

$$E : y^2 = x^3 + ax^2 + bx + c.$$

Então

(1) Um ponto $P = (x, y) \neq O$ em E tem ordem 3 se, e somente se, x raiz do polinômio

$$3x^4 + 4ax^3 + 6bx^2 + 12cx + (4ac - b^2) = 0.$$

(2) E tem exatamente 8 pontos de ordem 3. Estes pontos, juntamente com o ponto O formam o grupo $E[3]$ que é isomorfo a $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$.

Prova: (1) Seja $P = (x, y) \neq O$ em E. Então

$$3P = O \iff 2P = -P \iff x(2P) = x(-P) = x(P).$$

Pela fórmula de duplicação de um ponto ([5]) temos que

$$\frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c} = x,$$

ou seja,

$$\phi(x) = 3x^4 + 4ax^3 + 6bx^2 + 12cx + (4ac - b^2) = 0.$$

Reciprocamente, se x é raiz do polinômio

$$\phi(x) = 3x^4 + 4ax^3 + 6bx^2 + 12cx + (4ac - b^2),$$

temos que

$$\frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c} = x,$$

ou seja, $x(2P) = x(P) = x(-P)$. Portanto segue que P tem ordem 3.

(2) Por (1) temos que $\phi(x) = 3x^4 + 4ax^3 + 6bx^2 + 12cx + (4ac - b^2) = 0$. Derivando obtemos $\phi'(x) = 12(x^3 + ax^2 + bx + c) = 12f(x)$ e $\phi(x) = 2f(x)f''(x) - f'(x)^2 = 0$. Então ϕ tem raiz múltipla se, e somente se, $12f(x) = 0$ *e* $2f(x)f''(x) - f'(x)^2 = 0$. Isto implica que $f(x) = f'(x) = 0$, o que é impossível. Portanto, ϕ possui 4 raízes distintas. Sejam $\beta_1, \beta_2, \beta_3$ *e* β_4 tais raízes. Então para cada valor de x temos dois valores para y na equação da cúbica, ou seja, para cada raiz x existem dois pontos sobre a cúbica E. Logo a curva tem exatamente 8 pontos de ordem 3. Deste modo, $E[3] = \{O, P_1, \cdots, P_8\}$, onde cada P_i é diferente de O. Como $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ é o único grupo (abeliano) com 9 elementos, a menos de isomorfismo (tais que cada elemento tem ordem 3), temos que

$$E[3] \cong \{O, P_1, P_2, \cdots, P_8\} = \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}.$$

5 ALGUNS RESULTADOS FUNDAMENTAIS

Teorema 5.1. *(**Nagell-Lutz**) Seja a curva elíptica $E : y^2 = f(x) = x^3 + ax^2 + bx + c$, com $a, b, c \in \mathbb{Z}$. Suponha que $f(x)$ não possui raízes múltiplas. Seja $\Delta = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2 \neq 0$ o discriminante do polinômo cúbico. Se $P = (x, y)$ é um ponto racional de ordem finita sobre E, então $x, y \in \mathbb{Z}$ e $y = 0$ (neste caso P tem ordem 2) ou y^2 divide Δ.*

O teorema acima fornece um algoritmo para encontrar todos os pontos racionais de torção da curva elíptica $E : y^2 = x^3 + ax^2 + bx + c$. Para cada $y \in \mathbb{Z}$ satisfazendo $y = 0$ ou $y^2|\Delta$, devem-se achar as raízes inteiras da equação $x^3 + ax^2 + bx + c - y^2 = 0$ e logo verificar que

$P = (x : y : 1) \in E(\mathbb{Q})$ é um ponto de torção.

A recíproca deste teorema não é válida: Um ponto $P = (x : y : 1) \in E(\mathbb{Q})$ pode satisfazer as condições do teorema sem que ele seja necessariamente ponto de torção. Também o teorema pode ser usado para provar que um ponto $P \in E(\mathbb{Q})$ é de ordem finita.

O teorema de Nagell-Lutz segue dos próximos dois resultados.

Proposição 5.2. *Seja $P = (x_1 : x_2 : 1) \in E(\mathbb{Q})$. Se P e $2P$ têm coordenadas inteiras então $y_1 = 0$ ou $y_1^2 | \Delta$.*

Prova: Sejam $P = (x_1 : y_1 : 1)$ e $2P = (x_2 : y_2 : 1) \in E(\mathbb{Q})$ com coordenadas inteiras e $y_1 \neq 0$. Pelas fórmulas de duplicação temos

$$x_2 = \frac{x_1^4 - 2bx_1^2 - 8cx_1 + b^2 - 4ac}{4x_1^3 + 4ax_1^2 + 4bx_1 + 4c}.$$

Fazendo $f(x) = x^3 + ax^2 + bx + c$ e $g(x) = x^4 - 2bx^2 - 8cx + b^2 - 4ac$, temos que $x_2 = \frac{g(x_1)}{4f(x_1)} \in \mathbb{Z}$. Dado que $y_1^2 = f(x_1)$ segue que $y_1^2 | f(x_1)$ e $y_1^2 | g(x_1)$. Por outro lado, da identidade

$$\begin{aligned}(3x^3 - ax^2 - 5bx + 2ab - 27c)f(x) - (3x^2 + 2ax + 4b - a^2)g(x) \; &= \\ -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2,&\end{aligned}$$

segue que $y_1^2 | \Delta$.

Observação 5.3. Os polinômios $3x^3 - ax^2 - 5bx + 2ab - 27c$ e $3x^2 + 2ax + 4b - a^2$ foram obtidos usando o Sistema de Álgebra Computacional Máxima (SACM).

Proposição 5.4. *Se $P = (x : y : 1) \in E(\mathbb{Q})_{tor}$, então $x, y \in \mathbb{Z}$.*

O resultado a seguir descreve possibilidades para o subgrupo de torção de curvas elípticas racionais.

Teorema 5.5. *(**Mazur**) Seja E uma curva elíptica definida sobre $\mathbb{Q}$ e suponha que $E(\mathbb{Q})$ contenha um ponto de ordem m. Então*

$$1 \leq m \leq 10 \quad ou \quad m = 12.$$

Mas especificamente, o conjunto dos pontos de ordem finita de $E(\mathbb{Q})$ forma um grupo isomorfo a um dos grupos seguintes:

(1) $\mathbb{Z}/n\mathbb{Z}$, onde $1 \leq n \leq 10$ ou $n = 12$,

(2) $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}$, onde $1 \leq n \leq 4$.

Teorema 5.6. *(**Mordell**) Seja E uma curva elíptica dada por*

$$E : y^2z = x^3 + ax^2z + bxz^2 + cz^3,$$

onde $a, b, c \in \mathbb{Z}$ e seja $E(\mathbb{Q}) = \{(x : y : z) \in E : x, y, z \in \mathbb{Q}\}$. então $E(\mathbb{Q})$ é um grupo abeliano finitamente gerado.

O resultado a seguir sobre grupos abelianos finitamente gerados será útil.

Teorema 5.7. *Seja G grupo abeliano finitamente gerado e G_{tor} seu subgrupo de torção. Então*

(1) Existe um número inteiro r e um subgrupo $H \cong \mathbb{Z}^r$ tais que $G = G_{tor} \oplus H$

(2) Existem números inteiros $r \geq 0$, unicamente determinados, e $p_1^{v_1}, \cdots, p_u^{v_u}$, com $p_1 \leq \cdots \leq p_u$ números primos e com $v_i \leq 1$, tais que

$$G \cong \frac{\mathbb{Z}}{p_1^{v_1}} \times \cdots \times \frac{\mathbb{Z}}{p_u^{v_u}} \times \mathbb{Z}^r.$$

Observação 5.8. (a) Pelo teorema anterior segue que

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{tor} \oplus \mathbb{Z}^r.$$

(b) O número inteiro r é o posto da curva elíptica E.

(c) O grupo $E(\mathbb{Q})$ é finito se, e somente se, o posto de E é igual a zero.

Observação 5.9. Todos os resultados anteriormente apresentados podem ser vistos em [5] e [6].

6 OS NÚMEROS CONGRUENTES E AS CURVAS ELÍPTICAS

Nesta seção analisamos a relação entre os Números Congruentes e as Curvas Elípticas, apresentando um resultado que caracteriza tais números congruentes.

Definição 6.1. *Um número inteiro $n \geq 1$ é dito Número Congruente se existir um triângulo retângulo cujos lados sejam números racionais e cuja área seja n.*

Uma definição mais geral inclui todos os números racionais positivos com esta propriedade.

Observação 6.2. Um número inteiro n é dito livre de quadrados se n pode ser escrito na forma $n = \prod_{i=1}^{r} p_i$, onde os p_i são números primos distintos.

Definição 6.3. *Um número racional positivo n é dito congruente se existem $x, y, z \in \mathbb{Q}$ positivos tais que $x^2 + y^2 = z^2$ e $n = \frac{xy}{2}$.*

Observação 6.4. Se $n \in \mathbb{Q} - \{0\}$, então existe $s \in \mathbb{Q} - \{0\}$ tal que $s^2 n$ é um número inteiro livre de quadrados. Assim, se n for um número congruente, área de um triângulo retângulo de lados x, y, z, então a área do triângulo retângulo de lados sx, sy, sz é igual a $s^2 n$. Em resumo, n é congruente se, e somente se, $s^2 n$ é congruente. Portanto podemos sempre supor que n seja livre de quadrados.

Em um dos trabalhos sobre Teoria dos Números (que enviou a Huygens em 1959), Fermat afirmava ter demonstrado, usando o chamado método do descenso infinito (entre outros resultados), que não existe um triângulo retângulo com lados sendo números inteiros e cuja área seja o quadrado de um inteiro. Nessa carta, Fermat comenta apenas uma ideia geral do método usado. Os detalhes da prova desse resultado pode ser encontrados na margem do livro A Aritmética de Diofanto, junto à última proposição dessa obra.

Fermat mostrou que a equação $x^4 - y^4 = z^2$ não tem soluções inteiras não triviais (analogamente como se mostra que a equação $x^4 + y^4 = z^2$ não tem soluções inteiras não triviais) e logo usando este fato, conclui que a equação $x^4 + y^4 = z^4$ não tem soluções inteiras não triviais.

Teorema 6.5. *Nenhum quadrado de um número inteiro positivo pode representar a área de um triângulo retângulo cujos lados sejam números inteiros.*

Prova: Suponha m o número inteiro e que a área de um triângulo retângulo de lados (inteiros) a, b, c seja o quadrado de m, ou seja, $m^2 = \frac{ab}{2}$. Então temos que

$$(a+b)^2 = a^2 + b^2 + 2ab = c^2 + 4m^2,$$

e

$$(a-b)^2 = a^2 + b^2 - 2ab = c^2 - 4m^2,$$

de onde segue que

$$(a^2 - b^2)^2 = (a-b)^2(a+b)^2 = c^4 - (2m)^4.$$

Assim, a equação $z^2 = x^4 - y^4$ teria solução não trivial $x = c,\ y = 2m,\ z = a^2 - b^2$, o que contradiz os resultados de Fermat.

Exemplo 6.6. 1) Segue do resultado acima que os números $n = 1, 2, 3, 4$ não são congruentes, mas $n = 5$ é congruente pois é a área do triângulo retângulo de lados $x = \frac{20}{3},\ y = \frac{3}{2}\ e\ z = \frac{41}{6}$.

2) 6 é o menor número inteiro positivo congruente pois existe o triângulo retângulo de lados (inteiros) $3, 4\ e\ 5$.

A questão de determinar se um dado número n é congruente é chamado de O Problema do Número Congruente. Existe um resultado, O Teorema de Tunnel ([2]) o qual fornece um critério para determinar se um dado número é congruente, mas tal resultado depende da

conjectura de Birch e Swinnerton, ainda não provada, e que faz parte de um dos 7 problemas do milênio.

A seguir apresentamos um resultado elementar que caracteriza um número congruente.

Proposição 6.7. *Seja $n \geq 1$ um número inteiro livre de quadrados. Sejam $x, y, z \in \mathbb{Q}$ tais que $0 < x < y < z$. Então existe uma bijeção entre o conjunto de triângulos retângulos de lados x, y, z e área n e o conjunto de números racionais w tais que $w - n, w, w + n \in \mathbb{Q}^2$ dada por*

$$(x, y, z) \quad \longmapsto \quad w = (\frac{z}{2})^2,$$

cuja inversa é dada por

$$w \ \longmapsto \ (\sqrt{w+n} - \sqrt{w-n},\ \sqrt{w+n} + \sqrt{w-n},\ 2\sqrt{n}),$$

Em particular, n é congruente se, e somente se, existir um número racional w tal que $w,\ w+n,\ w-n \in \mathbb{Q}^2$.

Prova: Se $x^2 + y^2 = z^2$ e $n = \frac{xy}{2}$, então $(x \pm y)^2 = z^2 \pm 4n$. Logo

$$\left(\frac{x \pm y}{2}\right)^2 = \left(\frac{z}{2}\right)^2 \pm n.$$

Tomando $w = (\frac{z}{2})^2$ temos que $w,\ w+n,\ w-n \in \mathbb{Q}^2$.

Reciprocamente, dado $w \in \mathbb{Q}$ tal que $w,\ w+n,\ w-n \in \mathbb{Q}^2$, então

$$x = \sqrt{w+n} - \sqrt{w-n}, \quad y = \sqrt{w+n} + \sqrt{w-n} \quad e \quad z = 2\sqrt{n},$$

satisfazem as condições $0 < x < y < z, \quad xy = 2n \quad e \quad x^2 + y^2 = z^2$.

7 EQUAÇÕES CÚBICAS

Nesta seção iremos associar a números congruentes soluções de uma certa equação cúbica. Seja n um número congruente e $x, y, z \in \mathbb{Q}$, tais que $0 < x < y < z \ \ e \ \ n = \frac{xy}{2}$. Então temos que

$$\left(\frac{x^2 - y^2}{4}\right)^2 = \left(\frac{z}{2}\right)^4 - n^2.$$

Isto significa que existe uma solução racional $u = \frac{z}{2}\ e\ v = \frac{x^2-y^2}{4}$ para a equação $u^4 - n^2 = v^2$. Multiplicando ambos lados desta equação por u^2 obtemos

$$(u^2)^3 - n^2u^2 = (uv)^2.$$

Logo, $a = u^2$ e $b = uv$ fornecem uma solução racional (a, b) para a equação cúbica $y^2 = x^3 - n^2x$.

Reciprocamente, dada uma solução racional (a, b) da equação cúbica $y^2 = x^3 - n^2x$, será que (a, b) provêm de um triângulo retângulo como antes mencionado?. Isto nem sempre ocorre. Para isso acontecer, deve-se ter $a \in \mathbb{Q}^2$ e além disso, o denominador de a tem que ser par. De fato, dada um terna pitagórica $x < y < z$, seja s o mínimo múltiplo comum dos denominadores de x, y e z. Então $x' = sx,\ y' = sy$ e $z' = sz$ são números primos entre si. Neste caso, x' e y' tem paridades distintas, digamos x' ímpar e y' par. Em particular z' é ímpar. Portanto, $a = (\frac{z}{2})^2 = (\frac{z'}{2s})^2$ tem denominador par.

Sejam x_1, y_1, z_1 os denominadores de x, y, z respectivamente e $2^{x'_1},\ 2^{y'_1}$ e $2^{z'_1}$ as maiores potências de 2 dividindo $x_1,\ y_1$ e z_1. Seja 2^{s_1} a maior potência de 2 dividindo s. Como sx e sz são ímpares e sy é par, concluimos que $s_1 = x'_1 = z'_1$ e $s_1 < y'_1$. Mas estas condições nem sempre são satisfeitas. Por exemplo, a solução $\left(\frac{1681}{7^2}, \frac{29520}{7^3}\right)$ da equação $y^2 = x^3 - (31)^2x$ não provêm de nenhum triângulo retângulo.

Definição 7.1. *Uma terna de inteiros positivos (x, y, z) tal que $x^2 + y^2 = z^2$ é chamada de terna pitagórica.*

Se $\mathrm{mdc}(x, y, z) = 1$, tal terna é dita terna pitagórica primitiva.

Lema 7.2. *Seja (x, y, z) uma terna pitagórica primitiva, com y par. Então existem $\alpha, \beta \in \mathbb{Z}$, com $\mathrm{mdc}(\alpha, \beta) = 1$, tais que $x = \alpha^2 - \beta^2,\ y = 2\alpha\beta$ e $z = \alpha^2 + \beta^2$.*

Prova: ([7]).

Proposição 7.3. *Seja $(a, b) \in \mathbb{Q} \times \mathbb{Q}$ uma solução de $y^2 = x^3 - n^2x$ tal que $a \in \mathbb{Q}^2$ com denominador par. Então existe um triângulo retângulo de área n e lados $\sqrt{a+n} - \sqrt{a-n},\ \sqrt{a+n} + \sqrt{a-n}$ e $\sqrt{2a}$.*

Prova: Sejam $u = \sqrt{a} \in \mathbb{Q},\ u > 0$ e $v = \frac{b}{u}$. Então temos $v^2 = \frac{b^2}{a} = a^2 - n^2$. Seja t o denominador de u. Logo, os denominadores de v^2 e a^2 são iguais a t^4. Em particular, a terna (t^2v, t^2n, t^2a) é pitagórica com t^2n par e $\mathrm{mdc}(t^2v, t^2n, t^2a) = 1$. Assim, do lema acima segue que existem inteiros positivos α, β tais que $t^2v = \alpha^2 - \beta^2,\ t^2n = 2\alpha\beta$ e $t^2a = \alpha^2 + \beta^2$. Deste modo, o triângulo retângulo de lados $(2\alpha/t, 2\beta/t, 2u)$ tem área $\frac{2\alpha\beta}{t^2} = n$. Assim, esta terna corresponde a $(\frac{2u}{2})^2 = u^2 = a$. Portanto existe um triângulo retângulo de lados $\sqrt{a+n} - \sqrt{a-n},\ \sqrt{a+n} + \sqrt{a-n}$ e $2\sqrt{a}$, e de área n.

8 REDUÇÃO MÓDULO P

Sejam p número primo, $\mathbb{F}_p$ o corpo finito de p elementos, $\mathbb{P}^2(\mathbb{F}_p)$ e $\mathbb{P}^2(\mathbb{Q})$ os planos projetivos definidos sobre $\mathbb{F}_p$ e $\mathbb{Q}$ respectivamente. Dado um ponto $(a : b : c) \in \mathbb{P}^2(\mathbb{Q})$, pode-se escolher sempre números inteiros a_0, b_0, c_0 tais que $\mathrm{mdc}(a_0, b_0, c_0) = 1$ (basta multiplicar

pelo mmc dos denominadores). Assim, podemos definir a aplicação (redução módulo p)

$$\begin{array}{rccc} \phi: & \mathbb{P}^2(\mathbb{Q}) & \longrightarrow & \mathbb{P}^2(\mathbb{F}_p) \\ P=(a_0:b_0:c_0) & \longmapsto & \overline{P}=(\overline{a_0},\overline{b_0},\overline{c_0}), & \end{array}$$

onde $\overline{x_0} \equiv x_0 (mod\ p)$.

Dada uma curva elíptica $E: y^2 = x^3 + ax + b$, sempre é possível escolher um modelo dela, de modo que seus coeficientes sejam números inteiros e, reduzindo módulo p estes coeficientes, podemos considerar a curva reduzida $\overline{E}: y^2 = x^3 + \overline{a}x + \overline{b}$, definida sobre o corpo finito $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Temos os dois casos a seguir:

(1) $\overline{E}$ continue sendo não singular e portanto uma curva elíptica. Neste caso temos uma boa redução módulo p. Isto significa que a aplicação ϕ é injetiva ou seja, $p \nmid 2\triangle E$.

(2) $\overline{E}$ é singular e portanto não é uma boa redução módulo p.

Em particular, se $P \in E(\mathbb{Q})$, então $\phi(P) = \overline{P} \in \overline{E}(\mathbb{F}_p)$.

Sabemos que o fato de $E: y^2 = x^3 + ax + b$ ser não singular é equivalente a afirmar que $\Delta \neq 0$. Sendo assim, o discriminante, $\overline{\Delta}$, do polinômio $f(x) = x^3 + \overline{a}x + \overline{b}$, que define a curva $\overline{E}$ é a redução, módulo p, de Δ. Isto quer dizer que $\overline{E}$ é não singular se, e somente se, p não divide Δ. Neste caso se mostra que a aplicação $\Phi: E(\mathbb{Q}) \longrightarrow \overline{E}(\mathbb{F}_p)$ é um homomorfismo injetivo. Notar que $p|\Delta$ apenas para um número finito de primos p.

Proposição 8.1. *Para $i = 1, 2$, sejam $P_i = (x_i, y_i, z_i) \in \mathbb{P}^2(\mathbb{Q})$ e $\phi: \mathbb{P}^2(\mathbb{Q}) \longrightarrow \mathbb{P}^2(\mathbb{F}_p)$. Então $\phi(P_1) = \phi(P_2)$ se, e somente se, p divide simultaneamente os números $y_1z_2 - y_2z_1,\ \ x_2z_1 - x_1z_2\ \ e\ \ x_1y_2 - x_2y_1$, que são as coordenadas provenientes do produto vetorial $P_1 \times P_2$.*

Prova: Sejam $\phi(P_1) = (\overline{x_1}, \overline{y_1}, \overline{z_1})\ e\ \phi(P_2) = (\overline{x_2}, \overline{y_2}, \overline{z_2})$ e suponha $\phi(P_1) = \phi(P_2)$. Então

$$x_1 - x_2 = \lambda_1 p, \qquad y_1 - y_2 = \lambda_2 p, \qquad z_1 - z_2 = \lambda_3 p.$$

Deve-se mostrar que p divide $(y_1z_2 - y_2z_1)$. Temos que:

$$y_1z_2 - y_2z_1 = (y_1 - y_2)z_2 + y_2z_2 - y_2z_1 = (y_1 - y_2)z_2 + y_2(z_2 - z_1).$$

Substituindo as igualdades $y_1 - y_2 = \lambda_2 p\ \ e\ \ z_1 - z_2 = \lambda_3 p$ na expressão acima obtemos que $y_1z_2 - y_2z_1 = p(\lambda_2 z_2 + y_2\lambda_3)$ e portanto p divide $y_1z_2 - y_2z_1$. Analogamente se mostra que p divide também $x_2z_1 - x_1z_2\ \ e\ \ x_1y_2 - x_2y_1$.

Reciprocamente, suponha que p divide simultaneamente os números $y_1z_2 - y_2z_1,\ \ x_2z_1 - x_1z_2\ \ e\ \ x_1y_2 - x_2y_1$. Dado que $\mathrm{mdc}(x_1, y_1, z_1) = 1$, então $p \nmid x_1\ ou\ p \nmid y_1\ \ ou\ \ p \nmid z_1$. Sem

perda de generalidade, suponha que $p \nmid x_1$. Então temos

$$\phi(P_2) = (\overline{x_2}, \overline{y_2}, \overline{z_2}) = (\overline{x_1x_2}, \overline{x_1y_2}, \overline{x_1z_2}).$$

Dado que $p|(x_1y_2 - x_2y_1)$ e $p|(x_2z_1 - x_1z_2)$, então $\overline{x_1y_2} = \overline{x_2y_1}$ e $\overline{x_1z_2} = \overline{x_2z_1}$ respectivamente. Segue que

$$\phi(P_2) = (\overline{x_2}, \overline{y_2}, \overline{z_2}) = (\overline{x_1x_2}, \overline{x_1y_2}, \overline{x_1z_2}) = (\overline{x_1x_2}, \overline{x_2y_1}, \overline{x_2z_1}).$$

Se $p|x_2$, então $\phi(P_2) = (0, 0, 0)$, o que é impossível. Logo, multiplicando a terna $(\overline{x_1x_2}, \overline{x_2y_1}, \overline{x_2z_1})$ pelo inverso de $\overline{x_2}$ concluímos que

$$\phi(P_2) = (\overline{x_1}, \overline{y_1}, \overline{z_1}) = \phi(P_1).$$

Corolário 8.2. *Seja E uma curva elíptica definida sobre $\mathbb{Z}$ e suponha que p é um número primo suficientemente grande de modo que não divida as coordenadas de todos os produtos vetoriais dos pontos em $E(\mathbb{Q})_{tor}$ nem o discriminante de E. Então a restrição do homomorfismo de redução módulo p*

$$\Phi_p : E(\mathbb{Q})_{tor} \longrightarrow \overline{E}(\mathbb{F}_p)$$

é injetivo.

Prova: Sejam $P_1 \neq P_2$ em $E(\mathbb{Q})_{tor}$. Como p é primo suficientemente grande, de modo que não divide as coordenadas de todos os produtos vetoriais em $E(\mathbb{Q})$ e nem o discriminante de E, segue do lema anterior que $\Phi(P_1) \neq \Phi(P_2)$ e portanto Φ_p é injetivo.

Lema 8.3. *Seja a curva elíptica $E_a : y^2 = x^3 - a^2x$ e p um número primo tal que $p \nmid \Delta_a = 4a^6$, $p \geq 7$ e $p \equiv 3(mod\ 4)$. Então $\overline{E}_a(\mathbb{F}_p)$ tem exatos $p + 1$ pontos.*

Prova: Em primeiro lugar, $\overline{E}(\mathbb{F}_p)$ contém os 4 pontos $(0, 0), (-a, 0), (a, 0)$ e O. Tem-se que se $x \neq 0, a, -a$, considerando o par $x, -x$, observa-se que, pelo fato de $f(x) = x^3 - a^2x$ ser uma função ímpar e $p \equiv 3(mod\ 4)$, segue que -1 não é um quadrado módulo p. Assim exatamente um dos elementos $f(x)$ ou $f(-x)$ é um quadrado em $\mathbb{F}_p$. Portanto se tem duas raízes quadradas que dão lugar aos pontos $(x, \pm\sqrt{f(x)})$ ou $(-x, \pm\sqrt{f(x)})$, o que fornece um total de $p - 3$ pontos extras em $\overline{E}(\mathbb{F}_p)$, os quais, juntamente com os 4 pontos mencionados no início, totalizam os $p + 1$ pontos requeridos.

Teorema 8.4. $|E_a(\mathbb{Q})_{tor}| = 4.$

Prova: Basta mostrar que $|E_a(\mathbb{Q})_{tor}|$ divide 4. Seja p um número primo suficientemente grande. Pelo teorema de Lagrange, a ordem de $E_a(\mathbb{Q})_{tor}$ divide a ordem de $E_a(\mathbb{F}_p)$ e pelo lema acima, a ordem de $E_a(\mathbb{F}_p)$ é $p + 1$, se $p \equiv 3(mod\ 4)$.

Agora, o teorema de Dirichlet garante a existência de infinitos primos p da forma $8n+3$. Assim, existe um primo $p \equiv 3(mod\ 8)$, satisfazendo as condições do lema acima e, portanto, $|\overline{E}_a(\mathbb{F}_p)| = p+1$. Por outro lado, $|E_a(\mathbb{Q})_{tor}|$ divide $p+1$ e como $p+1 \equiv 4(mod\ 8)$, então 8 não divide $|E_a(\mathbb{Q})_{tor}|$.

De novo, pelo teorema de Dirichlet, existem infinitos primos da forma $12n+7$. Analogamente ao caso anterior, 3 não divide $|E_a(\mathbb{Q})_{tor}|$ pois $3 \nmid (p+1) \equiv 12n+8$. Similarmente, se $q > 3$ é um primo qualquer, existem infinitos primos $p \equiv 3(mod\ 4q)$. Podemos escolher tal primo que não divida o discriminante de $E_a(\mathbb{Q})$. Logo, esse primo satisfaz as condições do lema anterior e portanto $|\overline{E}_a(\mathbb{F}_p)| = p+1$ e como $p+1 \equiv 4(mod\ 4q)$, segue que $q \nmid p+1$, o que implica que $q \nmid |E_a(\mathbb{Q})_{tor}|$. Portanto, os únicos divisores de $|E_a(\mathbb{Q})_{tor}|$ são 1, 2 ou 4 e como $E_a(\mathbb{Q})_{tor}$ contém os 4 pontos óbvios, então sua ordem é exatamente 4.

9 NÚMEROS CONGRUENTES E CURVAS ELÍPTICAS: CONEXÃO

Com base nos resultados vistos nas seções anteriores, apresentamos o resultado que relaciona os Números Congruentes com as Curvas Elípticas.

Teorema 9.1. *Um número n é congruente se, e somente se, o posto da curva elíptica E : $y^2 = x^3 - n^2x$ é positivo, ou seja, n é congruente se, e somente se, E tem infinitos pontos racionais.*

Prova: Suponha n número congruente, livre de quadrados, e seja $(a,b) \in E(\mathbb{Q})$ a solução da equação cúbica $y^2 = x^3 - a^2x$ obtida na seção 7. Sendo assim, $a \in \mathbb{Q}^2$, com denominador par. Se (a,b) tiver ordem finita, segue do teorema acima, que (a,b) seria um ponto de ordem 2. Logo, sua primeira coordenada só pode ser $0, n\ ou\ -n$. Mas temos que $0, n\ e\ -n \notin \mathbb{Q}^2$. Assim, pelo teorema de Mordell, concluímos que (a,b) tem que ser um ponto de ordem infinita em $E(\mathbb{Q})$. Em particular, o posto de E é positivo.

Reciprocamente, dado um ponto $P = (x,y) \in E(\mathbb{Q})$ de ordem infinita, pela fórmula de duplicação de um ponto, temos que

$$x = \frac{x^4 + 2n^2x^2 + n^4}{(2y)^2},$$

que satisfaz as condições da proposição 7.1. Portanto n é um número congruente.

Exemplo 9.2. Vamos verificar que $n = 5$ é um número congruente. A curva elíptica E associada a $n = 5$ é:

$$E : y^2 = x^3 - 5^2x = x(x+5)(x-5).$$

Observar que $P = (45, 300)$ satisfaz a equação que define a curva E. Além disso, $y \neq 0$ e $y^2 = 90000 \nmid 62500 = \Delta$. Logo, pelo teorema de Nagell-Lutz temos que P é de ordem infinita, o que implica, pelo resultado acima, que 5 é um número congruente.

Observemos que, além de verificar que $n = 5$ é um número congruente, é possível determinar, através do ponto $P = (45, 300)$, os lados do triângulo retângulo que tornam 5 número congruente.

Pela fórmula de duplicação de um ponto temos que $2P = ((\frac{41}{12})^2, \frac{62279}{12^2})$. Logo, se tomamos $w = (\frac{41}{12})^2$, então os lados do triângulo retângulo são

$$\sqrt{w+n} - \sqrt{w-n} = \frac{3}{2},$$

$$\sqrt{w+n} + \sqrt{w-n} = \frac{20}{3},$$

$$2\sqrt{w} = \frac{41}{6}.$$

10 CONSIDERAÇÕES FINAIS

No presente trabalho foi mostrado como é que se dá a relação entre os Números Congruentes (um assunto bem antigo) e as Curvas Elípticas (um tópico relativamente recente). Como visto no teorema 9.1, para que um número racional n seja congruente é necessário e suficiente que a Curva Elíptica E, vinculada a esse valor n, tenha infinitos pontos racionais. Como se sabe, a Curva Elíptica E, definida sobre o corpo dos números racionais $\mathbb{Q}$, possui um conjunto de pontos, $E(\mathbb{Q})$, o qual está munido de uma estrutura de grupo abeliano. Sendo assim, qualquer ponto $(a, b) \in E(\mathbb{Q})$, sendo solução da equação cúbica que define a curva, deve ter ordem infinita.

Para que tudo isto seja possível de acontecer e de entender é necessário lidar com alguns conceitos e resultados clássicos (e importantes) das Curvas Elípticas (curvas cúbicas não-singulares) e por outro lado, com o conceito simples de número congruente, ou seja, números que representem a área de triângulos retângulos, ou em termos simples, com a ideia de ternas pitagóricas.

Espera-se que este trabalho possa servir de motivação para os interessados nesta linha de pesquisa e, no mínimo, despertar a curiosidade daqueles que não são desta área.

REFERENCES

[1] A. Bressan, "Unique Solutions for a Class of Discontinuous Differential Equations", *Proceedings of the American Mathematical Society*, vol. 104, no. 3, pp. 772–778, 1988. https://doi.org/10.1090/S0002-9939-1988-0964856-0

[2] A. Pacheco, "Números Conguentes e Curvas Elípticas", Matemática Universitária, N. 22/23, pp 18-29, 1997.

[3] J. S. Milne, "Elliptic Curves", Booksurge Publishing, 2006.

[4] J. S. Chahal, "Congruent Numbers and Elliptic Curves", The Mathematical Association of America, Vol. 113, No. 4, Apr., 2006.

[5] R. J. Walker, "Algebraic Curves", Princeton Mathematical Series, Vol. 13. Princeton University Press, 1962.

[6] L. C. Washington, "Elliptic Curves, Number Theory and Cryptography", CRC Press, Taylor and Francis Group, Second Edition, 2008.

[7] N. Koblitz, "Introduction to Elliptic Curves and Modular Forms", Springer-Verlag, v. 97, 1984

[8] B. Andrade, "Curvas Elípticas e Números Congruentes", Dissertação de Mestrado, UFU, Brasil, 2013.

BREVE BIOGRAFIA

Jaime Edmundo Apaza Rodriguez https://orcid.org/0000-0002-1359-9898

Possui graduação em Matemática pela Universidad Nacional de San Agustin Arequipa (1982), mestrado em Matemática pela Pontificia Universidad Católica Del Perú (1986) e doutorado em Matemática pela Pontifícia Universidade Católica do Rio de Janeiro (2002). Atualmente é professor assistente da Universidade Esta-dual Paulista Júlio de Mesquita Filho. Tem experiência na área de Matemática, com ênfase em GeometriaAlgébrica (Curvas Algébricas não-Singulares), Códigos de Goppa e Criptografia com curvas Elípticas.