Interrelação entre Curvas Elípticas e Números Congruentes

Douglas Matheus Gavioli Dias
Graduando em Matemática, FEIS, UNESP
Orientador: Jaime Edmundo Apaza Rodriguez
15385000, Ilha Solteira, SP
E-mail: mgaviolidias@gmail.com

Resumo

O Problema dos Números Congruentes nos leva para uma época longícua, mais expecificamente para 900 a.C. onde apareceu pela primeira vez em manuscritos árabes. Mas o que é um número congruente? Definiremos isto mais a frente, usando uma definição. O outro objeto de pesquisa deste projeto, são as Curvas Elpticas. As mesmas possuem uma história longa, além de ter participação em diversas áreas da matemática. Uma curva elíptica é uma curva cúbica (grau 3) em um plano algébrico. Toda curva elíptica pode ser escrita da forma:

$$y^2 = x^3 + ax + b$$

Também conhecida como forma de Weierstrass.
Vamos agora formalizar, brevemente o conceito de números congruentes.
Um número livre de quadrados é um número n tal que quando é decomposto em primos, não apresenta nenhum primo com multiplicidade maior do que 1 em sua decomposição, ou seja, $n = \prod(p_i)$ onde os $p_i's$ são diferentes uns dos outros.

Definição 1. *Um número inteiro positivo é dito um número congruente se existirem* $x, y, z \in \mathbb{Q}$ *tais que* $x^2 + y^2 = z^2$ *e* $\frac{xy}{2} = n$.

Note que se existe $s \in \mathbb{Q} - 0$ tal que $s^2 n \in \mathbb{Z}$ é livre de quadrados, então o triângulo retângulo de lados sx, sy e sz tem área igual a $s^2 n$. Veremos a baixo o conceito de pontos singulares, fundamental para demonstrar um teorema fundamental para o nosso trabalho.

O conceito de pontos singulares vem de certas curvas elípticas ou cúbicas em que a tangente tem declividade 0, por exemplo a curva $y^2 = x^3 + x^2$, em certos pontos esta curva tem tangente igual a 0, isso nos leva a seguinte definição:

Definição 2. *Uma curva elíptica* E *(ou uma curva no geral) tem um ponto singular* (x, y) *se,*

$$\frac{\delta E}{\delta x}(x, y) = 0 \ e \ \frac{\delta E}{\delta y}(x, y) = 0$$

Globalizando esta definição, diríamos que uma curva elíptica é singular, se para todo $(x, y) \in E$:

$$\frac{\delta E}{\delta x}(x, y) = 0 \text{ e } \frac{\delta E}{\delta y}(x, y) = 0$$

Equivalentemente, todo ponto multiplo de um ponto singular também é um ponto singular.

Uma curva elíptica possui uma característica diferente em relação as outras curvas, as mesmas em satisfazem aos axiomas de grupo abeliano sobre um corpo K. Mais específicamente, o corpo que usaremos será o corpo dos racionais, ou seja, os pontos racionais de uma curva elíptica, incluindo um ponto $\boldsymbol{O}$, caracterizam um grupo finitamente gerado. Este resultado é explorado através do Teorema de Mordell-Weil que vamos enunciar e esboçar uma demonstração a seguir.

Teorema 1. *Para toda curva elíptica em $\mathbb{Q}$, o grupo $E(\mathbb{Q})$ é finitamente gerado.*

É possível associar um número congruente n a uma curva Elíptica. Seja $x, y, z \in \mathbb{Q}$ com $0 < x < y < z$. Se $x^2 + y^2 = z^2$ e $n = \frac{xy}{2}$, então conpletando quadrados chegamos a :

$$(x \pm y)^2 = z^2 \pm 2xy \Rightarrow (x \pm y)^2 = z^2 \pm 4n \Rightarrow (\tfrac{x \pm y}{2})^2 = (\tfrac{z}{2})^2 \pm n$$

Sem perder a generalidade chegamos a:

$$(\tfrac{x-y}{4})^2 = (\tfrac{z}{2})^4 - n^2$$

Chamando $w = \frac{x-y}{4}$ e $u = \frac{z}{2}$, chegamos a $w^2 = u^4 - n$ multiplicando tudo por u^2, chegamos a $u^2w^2 = (u^2)^3 - nu^2$, fazendo uma pequena mudança de variáveis ($a = uw$ e $b = u^2$) chegamos a curva elíptica $a^2 = b^3 - nb$. Porém nem sempre o par (a, b) provem de um triângulo retângulo, são necessárias alguams condições para que isso ocorra (determinadas por outra proposição).

Todo o nosso trabalho nos trás até aqui, onde enunciaremos um teorema que é o objetivo desta pesquisa.

Teorema 1. *Um número inteiro n é congruente, se, somente se, o posto da curva elíptica $y^2 = x^3 + nx$ é positivo.*

Este teorema é demonstrado usando a seção anterior e todos os conceitos vistos nesta pesquisa.

Este trabalho é muito mais abrangente do que foi mostrado aqui, pois para chegar nos resultados, apenas resumidos acima, é preciso estudar sobre, curvas algébricas, plano projetivo, Teoria de Corpos, Grupos, Anéis, Teorema de Bézout, entre vários outros conceitos.

Bibliografia

[1] PACHECO, Amílcar. Números Congruentes e Curvas Elíticas. Matemática Universitária, São Paulo, v. 26, n. 25, p.18-31, jul. 1997. Anual

[2] STAR, Jonathan. Elliptic Curves and The Congruent Number Problem. 2015. 34 f. Dissertação (Mestrado) - Curso de Matemática, Claremont College, Claremont, 2015

[3] TRAN,Austin. Elliptic Curves and Congruent Numbers. University of Washington, jun. 2016.