Trabalho apresentado no XXXVIII CNMAC, Campinas - SP, 2018.

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Um clássico resultado: O Teorema de Mordell

Jaime Edmundo Apaza Rodriguez[1]
Departamento de Matemática, UNESP, Ilha Solteira
Douglas Matheus Gavioli Dias[2]
UFScar, SP

O objetivo deste trabalho é apresentar um clássico resultado da Teoria das Curvas Elípticas: O Teorema de Mordell. Este resultado foi conjecturado em 1900 por Poincaré e provado na década dos anos 20 por Mordell. O Teorema de Mordell afirma que o conjunto de pontos racionais de uma curva elíptica E forma um grupo abeliano finitamente gerado.

Existem resultados complementares ao Teorema de Mordell, tais como o Teorema de Nagell-Lutz e o Teorema de Mazur. O primeiro dá uma descrição dos pontos de ordem finita em uma curva elíptica, e o segundo descreve algumas propriedades do conjunto dos pontos de ordem finita da curva E. Tais resultados também serão discutidos ([1],[2]).

[Teorema (Teorema de Mordell)]([4]) Sejam E a curva elíptica dada por $E : y^2z = x^3 + ax^2z + bxz^2 + cz^3$ onde a, b, c são inteiros, e $E(\mathbb{Q}) = \{|x : y : z| \in E : x, y, z \in \mathbb{Q}\}$. Então $E(\mathbb{Q})$ é um grupo abeliano finitamente gerado.

Sejam P um ponto em $E(\mathbb{Q})$ e $H(P)$ a sua altura (abscissa de um ponto racional da curva elíptica onde os coeficientes são inteiros). Temos que $h(P) = logH(P)$, onde $h(P)$ satisfaz as propriedades ([4]):

1) Para todo número real positivo M, o conjunto $\{P \in E(\mathbb{Q}) : h(P) \leq M\}$ é finito, ou seja, o número de pontos racionais P numa curva elíptica cuja altura é finita é finito.

2) Seja P_0 ponto racional fixo em $E : f(x) = y^2 = x^3 + ax^2 + bx + c$. Existe uma constante k_0, dependendo de P_0 e de a, b, c tal que:

$$h(P + P_0) \leq 2h(P) + k_0, \forall p \in E(\mathbb{Q})$$

3) Existe uma constante k, dependendo de a, b, c, tal que:

$$h(2P) \leq 4h(P) - k, \forall P \in E(\mathbb{Q})$$

4) O índice $[E(\mathbb{Q}) : 2E(\mathbb{Q})]$ é finito.

Estas propriedades permitem demonstrar o Teorema de Mordell ([4]).

O Teorema de Mordell é equivalente a afirmar que existe $\{P_1, P_2, ..., P_r\} \subset E(\mathbb{Q})$ tal que todo $P \in E(\mathbb{Q})$ pode ser escrito em termos de $\{P_1, P_2, ..., P_r\}$, ou seja $P = n_1P_1 + n_2P_2 + n_rP_r$ para únicos $n_1, ..., n_r \in \mathbb{Z}$. Assim temos

[1]aqpjaime@gmail.com
[2]mgaviolidias@hotmail.com

© 2018 SBMAC

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

onde r é dito o posto da curva elíptica e $E(\mathbb{Q})_{tor}$ o subgrupo de torsão, ou seja, o subgrupo dos elementos de ordem finita.

Em geral o subgrupo de torsão é fácil de calcular.

[Teorema (Teorema de Mazur)]([4]) Seja $E(\mathbb{Q})_{tor}$ (grupo de torsão) não trivial. Este grupo é isomorfo a um dos seguintes grupos:

(i) $\mathbb{Z}_n$, para $1 \leq n \leq 10$ ou $n = 12$.

(ii) $\mathbb{Z}_2 \oplus \mathbb{Z}_{2n}$ com $1 \leq n \leq 4$.

Este teorema afirma que a ordem dos pontos de $E(\mathbb{Q})_{tor}$ é no máximo 12, com excessão de 11. Se o ponto com maior ordem de $E(\mathbb{Q})_{tor}$ for 5, por exemplo, então $E(\mathbb{Q})_{tor} \simeq \mathbb{Z}_5$.

O resultado a seguir foi provado independentemente por Lutz e por Nagell na década dos anos 30 e permite, em geral, uma rápida determinação dos pontos de torsão de uma curva elíptica sobre $\mathbb{Q}$.

[Teorema (Teorema de Nagell-Lutz)]([4]) Seja $E : f(x) = y^2 = x^3 + ax^2 + bx + c$ uma curva elíptica não singular com coeficientes inteiros e discriminante (Δ) dado por:

$$\Delta = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c.$$

Se $P = (x, y)$ for um ponto de ordem finita, então:

(i) x e y são inteiros;

(ii) $y = 0$ tem ordem 2 ou y^2 divide Δ.

O Teorema de Nagell-Lutz determina quando um ponto tem ordem finita ou não em uma curva elíptica.

Referências

[1] A. Pacheco. Números Congruentes e Curvas Elípticas. Matemática Universitária, Rio de Janeiro, 1997.

[2] P. Salehyan. Introdução às Curvas Elípticas e Aplicações. Publicações Matemáticas. Rio de Janeiro, 2015.

[3] B. A. Souza. Curvas Elípticas e Números Congruentes. Dissertação de Mestrado UFU, 2013.

[4] L. Washington, Elliptic Curves, Numer Theory and Criptography, CRC Press, 2008.

© 2018 SBMAC