EQUAÇÕES DIOFANTINAS NÃO LINEARES

Marcus Vinicius Ribeiro Bernardo Silvério, Fernando Pereira de Souza, Antonio Carlos Tamarozzi

Universidade Federal de Mato Grosso do Sul – UFMS, Curso de Matemática, rês Lagoas, MS, e-mail: marcao.bernardo@hotmail.com.

Agência de fomento: Programa de Educação Tutorial

RESUMO

Um tópico na teoria dos números é o estudo de equações com coeficientes inteiros. Esse estudo é chamado de Equações Diofantinas, pois a sua investigação se refere ao matemático grego Diofanto de Alexandria. Do algoritmo de Euclides decorre a possibilidade de se estudar um tipo especial de equação: as equações diofantinas lineares. Neste trabalho apresentaremos um estudo de duas equações diofantinas não lineares, tais equações exige um conhecimento sobre números complexos que será abordado durante o texto.

Palavras chave: Equações Diofantinas, Números Complexos, soluções

NON-LINEAR DIOPHANTINE EQUATIONS

ABSTRACT

A topic in number theory is the study of equations with integer coefficients. This study is called Diophantine Equations, because its investigation refers to the Greek mathematician Diophantus of Alexandria. From the Euclidean algorithm, we can study a special type of equation: the linear diophantine equations. In this paper we present a study of two non-linear Diophantine equations, such equations require a knowledge about complex numbers that will be addressed during the text.

Keywords: Diophantine Equations, Complex Numbers, Solutions.

INTRODUÇÃO

Equações diofantinas lineares foram estudadas por Diofanto, e em sua homenagem receberam o nome de equações diofantinas, conforme cita GALEÃO [2009/2010] e UFCG [2012]. Diofante foi um matemático e filósofo grego, teve uma influência maior sobre a teoria moderna dos números do que qualquer outro algebrista grego não geométrico. As equações diofantinas lineares podem ser obtidas aplicando o algoritmo de Euclides para o cálculo do máximo divisor comum. Não existe um algoritmo para resolver uma equação diofantina genérica, e é por isso que eles podem ser muito difíceis de resolver. Na verdade, muitos problemas abertos, como a hipótese de Riemann, podem ser incorporados em questões sobre máquinas de Turing, que podem, por sua vez, ser convertidas em equações diofantinas complicadas. Mesmo provando a inexistência de soluções inteiras positivas para a equação $x^n + y^n = z^n$ ($n \geq 3$) (último Teorema de Fermat), esta equação ocupou muitos matemáticos por três séculos antes de finalmente ser resolvido por Andrew Wiles. O objetivo deste trabalho é apresentar duas equações diofantinas não lineares, que a saber são $y^2 + 1 = x^3$ que não possui solução e $y^2 + 2 = x^3$ que possui duas soluções. Para o estudo destas equações faremos o uso de alguns resultados de números complexos que serão abordados neste artigo.

METODOLOGIA

No desenvolvimento deste trabalho foram realizados estudos dirigidos com o orientador e apresentação de seminários expositivos, bem como matéria bibliográfica especificada que possibilitou uma boa apreciação sobre o tema.

RESULTADOS

Inteiros de Gauß

Os inteiros de Gauß são os elementos do conjunto:

$$\mathbb{Z}[i] \stackrel{\text{def}}{=} \{a + bi \in \mathbb{C} | a, b \in \mathbb{Z}\}$$

subconjunto dos números complexos. É um conjunto fechado em relação as operações de soma e produto, formando assim o *anel dos inteiros de Gauß*. Neste conjunto podemos desenvolver uma aritmética similar à aritmética dos inteiros.

Definimos a norma de um inteiro de Gauß como:

$$N: \mathbb{Z}[i] \rightarrow \mathbb{Z} \\ z = a + bi \mapsto |z|^2 = z\bar{z} = a^2 + b^2.$$

Propriedade 1: Sejam $z, w \in \mathbb{Z}[i]$, então:

$$N(zw) = N(z)N(w).$$

Dem: Seja $z = a + bi$ e $w = c + di$, temos

$$\begin{aligned} N(zw) &= N((a + bi)(c + di)) \\ &= N(ac - bd + (ad + bc)i) \\ &= (ac - bd)^2 + (ad + bc)^2 \\ &= a^2c^2 - 2acbd + b^2d^2 + a^2d^2 + 2adbc + b^2c^2 \\ &= a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2 \\ &= a^2(c^2 + d^2) + b^2(c^2 + d^2) \\ &= (a^2 + b^2)(c^2 + d^2) \\ &= N(z)N(w). \end{aligned}$$

Podemos definir divisibilidade de maneira usual nos inteiros de Gauß, como sendo:

$$\alpha | \beta \Leftrightarrow \text{existe } \gamma \in \mathbb{Z}[i] \text{ tal que } \beta = \alpha\gamma.$$

Exemplo 1: Sejam $z = 2 + i$ e $w = 7 + i$, temos que $z | w$ pois

$$\frac{w}{z} = \frac{7 + i}{2 + i} = \frac{7 + i}{2 + i} \frac{2 - i}{2 - i} = \frac{15 - 5i}{5} = 3 - i,$$

Assim, obtemos:

$$w = 7 + i = (2 + i)(3 - i) = z\gamma,$$

onde $\gamma = 3 - i$.

Propriedade 2: Sejam $\alpha, \beta \in \mathbb{Z}[i]$. Se $\alpha|\beta$ então $N(\alpha)|N(\beta)$.

Dem: Suponhamos que $\alpha|\beta$, então existe $\gamma \in \mathbb{Z}[i]$ tal que $\beta = \alpha\gamma$, aplicando a função norma temos:

$$\begin{aligned} N(\beta) &= N(\alpha\gamma) \\ N(\beta) &= N(\alpha)N(\gamma) \\ N(\alpha) &|N(\beta). \end{aligned}$$

Definição 1: Seja A um domínio, isto é, um anel em que se $ab = 0$, então $a = 0$ ou $b = 0$. Dizemos que um elemento $u \in A$ é uma unidade se ele possui inverso multiplicativo em A , isto é, existe $v \in A$ tal que $uv = 1$.

O próximo Lema será fundamental na demonstração do nosso principal resultado.

Lema 1: As unidades em $\mathbb{Z}[i]$ são $\{\pm 1, \pm i\}$. Em particular u é uma unidade em $\mathbb{Z}[i]$ se, e somente se, $N(u) = 1$.

Dem: Seja u uma unidade em $\mathbb{Z}[i]$, então existe $v \in \mathbb{Z}[i]$ tal que $uv = 1$, então $N(u)N(v) = N(uv) = N(1) = 1$. Como $N(u)$, $N(v)$ são inteiros positivos, temos $N(u) = N(v) = 1$. Escrevendo $u = a + bi$ com $a, b \in \mathbb{Z}$, temos:

$$N(u) = 1 \Leftrightarrow a^2 + b^2 = 1 \Leftrightarrow (a, b) = (\pm 1, 0) \text{ ou } (a, b) = (0, \pm 1),$$

ou seja, $u \in \{\pm 1, \pm i\}$.

Lema 2: As unidades em $\mathbb{Z}[\sqrt{-2}]$ são $\{\pm 1\}$.

Dem: Seja u uma unidade em $\mathbb{Z}[\sqrt{-2}]$, então existe $v \in \mathbb{Z}[\sqrt{-2}]$ tal que $uv = 1$, então $N(u)N(v) = N(uv) = N(1) = 1$. Como $N(u)$, $N(v)$ são inteiros positivos, temos $N(u) = N(v) = 1$. Escrevendo $u = a + b\sqrt{-2}$ com $a, b \in \mathbb{Z}$, temos:

$$N(u) = 1 \Leftrightarrow a^2 + 2b^2 = 1 \Leftrightarrow (a, b) = (\pm 1, 0),$$

ou seja, $u \in \{\pm 1\}$.

EQUAÇÕES DIOFANTINAS NÃO LINEARES

No estudo de equações diofantinas lineares ($ax + by = c$), as soluções são encontradas nos casos onde $\text{mdc}(a, b)|d$ e são obtidas através do algoritmo de Euclides. Vejamos dois exemplos de equações diofantina não lineares, a saber:

- I. $y^2 + 1 = x^3$, com $x, y \neq 0 \in \mathbb{Z}$
- II. $y^2 + 2 = x^3$, com $x, y \neq 0 \in \mathbb{Z}$

Exemplo 2: Considere a seguinte equação diofantina:

$$y^2 + 1 = x^3.$$

Encontre todas as soluções inteiras dessa equação, com $x, y \neq 0$ em $\mathbb{Z}$.

Vamos supor que x é par, então $x = 2k$, com $k \in \mathbb{Z}$, assim temos que:

$$y^2 + 1 = x^3 = 8k^3, \tag{1}$$

assim, temos

$$y^2 + 1 \equiv 8k^3 \equiv 0 \pmod{8},$$

isto implica que

$$y^2 \equiv -1 \equiv 7 \pmod{8}. \tag{2}$$

Da equação (1) temos que $y^2 = 8k^3 - 1 = 2(4k^3) - 1$, temos que y^2 é ímpar, logo, y é ímpar. Escrevendo $y = 2t + 1$, com $t \in \mathbb{Z}$, obtemos:

$$y^2 = (2t + 1)^2 = 4t^2 + 4t + 1 = 4t(t + 1) + 1,$$

mas $t(t + 1)$ é par, assim $t(t + 1) = 2s$, com $s \in \mathbb{Z}$, e:

$$y^2 = 4 \cdot 2s + 1 \Rightarrow y^2 \equiv 1 \pmod{8}. \quad (3)$$

De (2) e (3) temos um absurdo, logo x é ímpar, então $x = 2k + 1$, desta forma, temos:

$$y^2 + 1 = x^3 = (2k + 1)^3 = 2(4k^3 + 6k^2 + 3k) + 1,$$

ou seja, y^2 é par, portanto y é par.

Operando em $\mathbb{Z}[i]$ temos:

$$y^2 + 1 = (y + i)(y - i) = x^3$$

Seja $\delta \in \mathbb{Z}[i]$ diferente da unidade, note que se

$$\delta | y + i \text{ e } \delta | y - i$$

então,

$$\delta | (y + i) - (y - i) \Rightarrow \delta | 2i.$$

Portanto, existe $z \in \mathbb{Z}[i]$ tal que $2i = \delta z$. Desta forma, temos:

$$2i(-i) = z\delta(-i)$$

$$-2i^2 = z\delta(-i)$$

$$2 = z\delta(-i)$$

$$\delta | 2.$$

Utilizando as propriedades de norma de um número, concluímos que

$$N(\delta) | N(2)$$

$$N(2) = N(\delta) \cdot p, \quad \text{com } p \in \mathbb{Z}$$

$$4 = N(\delta) \cdot p. \quad (4)$$

Pelo fato de δ não ser uma unidade, então $N(\delta) \neq 1$, assim da equação (4) temos que $N(\delta)$ é necessariamente par. Sabemos que y é par, então

$$N(y + i) = N(2k + i) = (2k)^2 + 1^2 = 4k^2 + 1,$$

ou seja, $N(y + i)$ é ímpar.

Assim temos que se $\delta | y + i$ e $\delta | y - i$ então $N(\delta) | N(y + i)$ com $N(\delta)$ par e $N(y + i)$ ímpar, o que é um absurdo, logo temos que ter δ como uma unidade.

Então, $y - i$ e $y + i$ não possuem nenhum fator em comum diferente da unidade e sabendo que $(y + i)(y - i) = y^2 + 1 = x^3$ é um cubo perfeito, temos $(y + i) = u(a + bi)$ e $(y - i) = u_1(a_1 + b_1i)$, onde u e u_1 são unidades. As unidades em $\mathbb{Z}[i]$ são ± 1 e $\pm i$, que são cubos perfeitos, e podemos assumir que $y + i = (a + bi)^3$, daí:

$$y + i = a^3 + 3a^2bi - 3ab^2 - b^3 - b^3i = a^3 - ab^2 + (3a^2b - b^3)i.$$

Comparando as partes imaginárias, temos:

$$1 = 3a^2b - b^3 = b(3a^2 - b^2);$$

Isto implicaria que $b = 1$ e $b(3a^2 - b^2) = 1$, ou seja, $3a^2 = 2$,

o que é um absurdo, portanto, a equação $y^2 + 1 = x^3$ não tem solução em $\mathbb{Z}$.

Exemplo 3: Considere a seguinte equação diofantina:

$$y^2 + 2 = x^3.$$

Encontre todas as soluções inteiras dessa equação, com $x, y \neq 0$ em $\mathbb{Z}$.

Supondo que x é par, então $x = 2k$, com $k \in \mathbb{Z}$, assim temos que:

$$y^2 + 2 = (2k)^3 = 8k^3, \quad (5)$$

Assim, temos que

$$y^2 + 2 \equiv 0 \pmod{4} \Rightarrow y^2 \equiv -2 \equiv 2 \pmod{4}. \quad (6)$$

Da equação (5) temos $y^2 = 8k^3 - 2 = 2(4k^3 - 1)$, ou seja, y^2 é par, logo, y é par, então $y = 2t$, com $t \in \mathbb{Z}$. Note que:

$$y^2 = (2t)^2 = 4t^2 \Rightarrow y^2 \equiv 0 \pmod{4},$$

o que contradiz (6). Portanto temos que ter x ímpar, que implica que y é ímpar também.

Operando em $\mathbb{Z}[\sqrt{-2}]$ temos:

$$y^2 + 2 = (y + \sqrt{-2})(y - \sqrt{-2}) = x^3$$

Suponhamos que exista $\delta \in \mathbb{Z}[\sqrt{-2}]$ diferente da unidade, tal que:

$$\delta | (y + \sqrt{-2}) \text{ e } \delta | (y - \sqrt{-2}), \quad (7)$$

então

$$\delta | (y + \sqrt{-2}) - (y - \sqrt{-2}) \Rightarrow \delta | 2\sqrt{-2}.$$

Segue que $2\sqrt{-2} = \delta z$ para algum $z \in \mathbb{Z}[\sqrt{-2}]$, desta forma temos

$$N(\delta z) = N(2\sqrt{-2}) \Rightarrow N(\delta)N(z) = 8,$$

pelo fato de δ não ser uma unidade, então $N(\delta) \neq 1$, assim devemos ter que $N(\delta)$ é par. Por outro lado, de (7) deve existir $t \in \mathbb{Z}[\sqrt{-2}]$ tal que:

$$t\delta = y + \sqrt{-2} \Rightarrow N(\delta)N(t) = N(y + \sqrt{-2}) = y^2 + 2,$$

mas $y^2 + 2$ é ímpar e $y^2 + 2 = N(\delta)N(t)$ que é par, um absurdo. Portanto segue que δ é uma unidade em $\mathbb{Z}[\sqrt{-2}]$. Então, $y - \sqrt{-2}$ e $y + \sqrt{-2}$ não possuem nenhum fator em comum diferente da unidade e sabendo que $(y + \sqrt{-2})(y - \sqrt{-2})$ é um cubo perfeito temos $(y + \sqrt{-2}) = u(a + b\sqrt{-2})$ e $(y - \sqrt{-2}) = u_1(a_1 + b_1\sqrt{-2})$, onde u e u_1 são unidades. Logo, como as unidades em $\mathbb{Z}[\sqrt{-2}]$ são ± 1 , que são cubos perfeitos, e podemos assumir que $y + \sqrt{-2} = (a + b\sqrt{-2})^3$, assim:

$$y + \sqrt{-2} = a^3 - 6ab^2 + (3a^2b - 2b^3)\sqrt{-2}.$$

Comparando as partes real e imaginária, temos

$$y = a^3 - 6ab^2 \text{ e } 1 = 3a^2b - 2b^3.$$

Segue que:

$$b(3a^2 - 2b) = 1 \Rightarrow b = \pm 1.$$

Desta forma, obtemos:

$$b = 1 \Rightarrow (3a^2 - 2b) = 1 \Rightarrow a = \pm 1$$

$$b = -1 \Rightarrow (3a^2 - 2b) = -1 \Rightarrow 3a^2 = 1 \text{ (não tem solução)}.$$

Assim, temos que ter $b = 1$ que implica em $a = \pm 1$. Se $b = 1$ e $a = 1$ temos $y = -5$, Se $b = 1$ e $a = -1$ temos $y = 5$. Então $y = \pm 5$, o que implica em $x = 3$. Portanto, as soluções inteiras para esta equação são $y = \pm 5$ e $x = 3$.

DISCUSSÃO

O presente estudo mostra a importância da análise dos pré-requisitos oriundos dos números complexos. Neste contexto, nosso principal interesse neste trabalho foi compreender a resolução de duas equações diofantinas não lineares. Em cada exemplo foi importante escolher adequadamente em qual domínio trabalhar, enquanto na primeira equação foi necessário resolver a equação em $\mathbb{Z}[i]$, na segunda equação foi fundamental solucionar em $\mathbb{Z}[\sqrt{-2}]$.

CONCLUSÃO

O estudo das equações diofantinas não lineares permitiu desenvolver um trabalho com vários conceitos matemáticos e resultados importantes normalmente não estudados em cursos de Licenciatura em Matemática. Um exemplo é o da função norma que nos permitiu calcular facilmente as unidades em $\mathbb{Z}[i]$ e em $\mathbb{Z}[\sqrt{-2}]$. Esta é uma pesquisa em andamento, sendo este trabalho uma parcial da principal finalidade, que é estudar os ternos pitagóricos.

REFERÊNCIAS

- [1] Alencar Filho, Edgard de. Teoria Elementar dos números, NOBEL, São Paulo, 1988.
- [2] GALEÃO. Cantinho da Matemática. Núcleo de Estágio, 2009/2010.
http://www.estagiariasgaleao.hostoi.com/index.php?p=1_8_Diofante-Alexandria. Acesso em 15/01/2013.

[3] MOREIRA, C.G; Martínez, F.E.B; Saldanha, N C. Tópicos de Teoria dos Números, SBM, Rio de Janeiro, 2012.

[4] Paula, A.R.B., Bollauf, M.F., Araújo, M.A., Wainer, S.A., Domínios Euclidianos e Equações Diofantinas, Universidade Estadual de Campinas, 2012.

[5] UFCG. Biografias, 2012. <http://www.dec.ufcg.edu.br/biografias/DiofanAl.html>. Acesso em 16/12/2012.