TEORIA ELEMENTAR DE ANÉIS – UMA CONJECTURA DE FERMAT

SILVA, Marcelo[1]
[1]*Discente do curso de Licenciatura em Matemática, UFPel; marcelo.math@yahoo.com.br*

FURTADO, Igor[1]
[1]*Discente do curso de Licenciatura em Matemática, UFPel; igorjara@gmail.com*

NERY, Janice[2]
[2]*IFM/DME,Orientadora, UFPel; janice@mat.ufrgs.br*

1 INTRODUÇÃO

Este trabalho visa apresentar uma demonstração da conjectura de Fermat, utilizando como ferramenta fundamental a teoria elementar de anéis.

O matemático francês Pierre de Fermat (1601-1665), baseado nas suas observações das propriedades dos números inteiros, destacou que os números primos da forma $4k+1$, com $k \in \mathbb{N}$ adequado, podem ser escritos como soma de quadrados de dois inteiros, como mostra a seguinte tabela:

Primos	2	3	5	7	11	13	17	...
4k+1			5=4.1+1			13=4.3+1	17=4.4+1	...
4k+3		3=4.0+3		7=4.1+3	11=4.2+3			...
Soma de quadrados de dois inteiros	$2=1^2+1^2$		$5=1^2+2^2$			$13=2^2+3^2$	$17=1^2+4^2$	...

Desta forma, Fermat conjecturou e demonstrou o seguinte teorema:

Um número primo p é a soma de quadrados de dois inteiros se, e somente se, $p=2$ ou p é um numero primo do tipo $4k+1$, com $k \in \mathbb{N}$ adequado.

Para a demonstração que faremos utilizaremos cinco lemas e duas proposições, envolvendo teoria de grupos e teoria dos números, que servirão de suporte para, juntamente com a teoria elementar de anéis, construírem a demonstração deste teorema.

2 METODOLOGIA (MATERIAL E MÉTODOS)

Num primeiro momento fez-se necessário uma busca, após um estudo da teoria de grupos e da teoria dos números, de teoremas que fossem utilizados na demonstração desta conjectura, com o objetivo de não tornar a mesma uma prova extensa demais.

Para o desenvolvimento desta demonstração fez-se necessário também um conhecimento prévio das seguintes estruturas algébricas:

• Domínios Euclidianos

• O anel dos inteiros Gaussianos:
$(\mathbb{Z}[i], +, .)$, onde $\mathbb{Z}[i] = \{a + bi / a, b \in \mathbb{Z} \text{ e } i^2 = -1\}$, e as operações de soma e multiplicação são definidas por: $(a + bi) + (c + di) := (a + c) + (b + d)i$ e $(a + bi).(c + di) := (a.c - b.d) + (b.c + a.d)i$, com $(a + bi), (c + di) \in \mathbb{Z}[i]$;

• Domínio de fatoração única

Lemas e proposições que serão utilizados na prova do teorema:
Lema 1: Se $a + bi \in \mathbb{Z}[i]$ não é inversível, então $a^2 + b^2 \neq 1$.

Lema 2: Seja p um número primo e suponhamos que para algum inteiro c que seja relativamente primo com p, existem x, $y \in \mathbb{Z}$ tais que $x^2 + y^2 = cp$. Então p pode ser escrito como soma de quadrados de dois inteiros.

Lema 3: Seja p um inteiro primo da forma $4k + 1$, onde $k \in \mathbb{Z}$. Então a congruência $x^2 \equiv -1 \pmod{p}$ tem solução em $\mathbb{Z}$.

Lema 4: Seja $G = \{e, g_1, g_2, \ldots, g_n\}$ um grupo abeliano finito com ordem $|G| = n + 1$. Suponha que G tenha exatamente um elemento de ordem dois, digamos g_1. Então $e.g_1.g_2.\ldots.g_n = g_1$.

Lema 5 (Teorema de Wilson): Seja p um primo ímpar. Então temos que $(p - 1)! \equiv -1 \pmod{p}$.

Proposição 1: Um número inteiro primo p pode ser escrito como soma de dois quadrados se, e somente se, p se fatora num produto de dois elementos não inversíveis de $\mathbb{Z}[i]$.

Proposição 2: Todo número inteiro primo do tipo $4k + 1$, onde $k \in \mathbb{Z}$, é a soma de quadrados de dois inteiros.

3 RESULTADOS E DISCUSSÕES

Este estudo mostra mais uma aplicação da teoria elementar de anéis na teoria de números, no que diz respeito ao problema de representação de inteiros como soma de potências (neste caso quadrados). Estes problemas vem intrigando os matemáticos desde o século XVIII e tais resultados motivam estudos mais avançados na teoria de anéis e que proporcionam novas aplicações além de desenvolvimento de novos resultados.

4 CONCLUSÕES

Após a estruturação desta prova e a verificação de sua veracidade, nota-se o quão útil vem a ser a teoria de anéis, mostrando-se mais uma de suas aplicações. Esta última tem, por sua vez, o objetivo principal de descobrir propriedades dos números inteiros e, principalmente, dos números primos. Os

resultados alcançados nestes tópicos de pesquisa têm encontrado ampla aplicação, como pode-se verificar, nas áreas de criptografia e códigos corretores de erros (fundamentais para segurança de dados).

5 REFERÊNCIAS

HERSTEIN, Israel Nathan. **Topics in Algebra**. New York, 1976.

GARCIA, Arnaldo & LEQUAIN, Yves, **Elementos de Álgebra**. Rio de Janeiro: IMPA, 2008.

GONÇALVES, Adilson. **Introdução à Álgebra**. Rio de Janeiro: IMPA, 2007.

SANTOS, José Plínio. **Teoria dos Números**. Rio de Janeiro: IMPA, 2009.