A caracterização dos números inteiros que podem ser escritos como soma de dois quadrados

Autora: Marília Luiza Matte

Orientador: Dr. Jaime Bruck Ripoll

Introdução

Este trabalho trata de uma importante aplicação da teoria de anéis à teoria de números: a caracterização dos números inteiros que podem ser escritos como soma de dois quadrados.

Para tanto, utilizamos a caracterização dos primos que podem ser escritos de tal forma, conforme proposto e demonstrado por Fermat, trabalhando com as propriedades de fatoração única e com a função norma no conjunto dos inteiros de Gauss.

Alguns exemplos:

Vemos que 0, 1 e 2 podem ser escritos como soma de dois quadrados:

$0=0^2+0^2$ $\quad$ $1=1^2+0^2$

$2=1^2+1^2$

Note que a decomposição em soma de quadrados não é necessariamente única:

$25=5^2+0^2=3^2+4^2$

E pode ocorrer também para números que não são quadrados perfeitos:

$125=10^2+5^2=11^2+2^2$

A sequência para a demonstração:

De acordo com o Pequeno Teorema de Fermat,

$$\bar{x}^{p-1} - \bar{1} = \bar{0}, \quad \forall\, \bar{x} \in Z_p \setminus \{0\}$$

Com esse fato, podemos demonstrar que, dado um primo p, são equivalentes as seguintes afirmações:

i) $p = 2$ *ou* $p \equiv 1 (\mathrm{mod}\, 4)$

ii) $\exists\, a \in Z$ *tq* $a^2 \equiv -1 (\mathrm{mod}\, p)$

iii) *p não é irredutível em* $Z[i]$

iv) *p é soma de dois quadrados*.

E, a partir dessas afirmações, podemos caracterizar os elementos irredutíveis do conjunto $Z[i]$.

Através do lema que garante que o produto de dois números que são soma de dois quadrados ainda é uma soma de dois quadrados e tendo demonstrado que os irredutíveis de $Z[i]$ têm norma igual à soma de dois quadrados, chegamos ao teorema final, descrito a seguir.

O Teorema:

Seja n um inteiro positivo, cuja fatoração irredutível em Z *é*

$$n = 2^r . p_1^{u_1} \ldots p_t^{u_t} . q_1^{v_1} \ldots q_s^{v_s}$$

com $p_1, \ldots, p_t$ *primos do tipo 4k+1 e* $q_1, \ldots, q_s$ *primos do tipo 4k+3.*

Então n é soma de dois quadrados se, e somente se, $v_1, \ldots, v_s$ *são pares.*

Referência: GARCIA, ARNALDO; LEQUAIN, YVES. Elementos de Álgebra. 5 ed. Rio de Janeiro: IMPA, 2008.