Involuções e Teorema de Fermat sobre Somas de Dois Quadrados

Autor: JEAN RODRIGO TEIXEIRA DE TEIXEIRA - UFRGS
Orientador: PROF. DR. ARTUR OSCAR LOPES - UFRGS - IMAT

UFRGS PROPESQ
XXV SIC Salão Iniciação Científica
CET - Ciências Exatas e da Terra

OBJETIVO

O objetivo deste trabalho é mostrar como encontrar uma representação para qualquer primo da forma p=4k+1, como soma de dois quadrados.

TEOREMA DE FERMAT

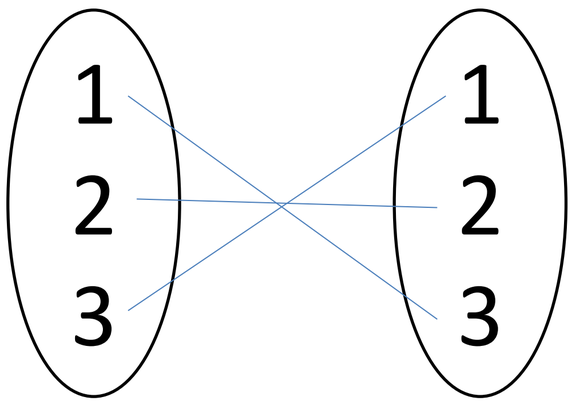
Cada primo p≡1(mod4) é soma de dois quadrados.

Encontraremos uma representação para cada primo dessa forma a partir de propriedades de involuções.

INVOLUÇÕES

Uma involução em um conjunto X é uma bijeção de X em si mesmo que é igual a sua própria inversa.

Exemplo de Involução:



Seja uma involução α em um conjunto X e um ponto P pertencente ao mesmo conjunto. Se α(P)=P, então P é chamado ponto fixo de α.

O conjunto de todos os pontos fixos de uma involução α em um conjunto qualquer é chamado Fix(α).

Se uma involução α em um conjunto qualquer não tiver pontos fixos, então α é uma involução livre.

Denotamos a cardinalidade de um conjunto por "#".

PRINCÍPIO 1

Se α e β são duas involuções no mesmo conjunto finito, então #Fix(α)≡#Fix(β)(mod2)

PRINCÍPIO 2

Se α e β são duas involuções no mesmo conjunto finito, e se α tem exatamente um ponto fixo, então β tem ao menos um ponto fixo.

Esse princípio foi utilizado para provar o Teorema de Fermat de uma forma bastante curta.

Tomamos o conjunto finito $X=X(p)=\{(a,b,c)\in N^3 \mid p=a^2+4bc\}$.

Definimos a involução α pela seguinte fórmula:

$\alpha:(a,b,c)\rightarrow(a+2c,c,b-a-c)$ se $a<b-c$
$\alpha:(a,b,c)\rightarrow(2b-a,b,a-b+c)$ se $b-c<a<2b$
$\alpha:(a,b,c)\rightarrow(a+2c,a-b+c,b)$ se $a>2b$

Definimos a involução β pela seguinte fórmula:

$\beta:(a,b,c)\rightarrow(a,c,b)$

A involução α tem, para k>0, o ponto (1,1,k) como único ponto fixo. O ponto fixo de β, cuja existência é assegurada pelo Princípio 2, é a solução desejada da equação $p=a^2+4b^2$.

O problema dessa prova é que a involução β deve ter um ponto fixo, mas não se tem ideia de que ponto é. Então, o Princípio 2 foi refinado a dar um algoritmo de forma a obter um ponto fixo de β a partir do ponto fixo de α. Partindo do ponto fixo de α, aplicamos as involuções β e α alternadamente até encontrarmos um ponto fixo de β. Indicamos a conclusão mais formalmente através do Princípio 3.

PRINCÍPIO 3

Sejam α e β duas involuções arbitrárias sobre um conjunto finito X. Então, há uma involução livre canonicamente definida ρ sobre a união disjunta dos conjuntos de ponto fixo de α e β.

REFERÊNCIAS

O presente trabalho tem por base a parte II do artigo "New Looks at Old Number Theory", de Aimeric Malter, Dierk Schleicher e Don Zagier, do The American Mathematical Monthly, 120 (2013), 243-264.

25 anos
MODALIDADE DE BOLSA
INICIAÇÃO CIENTÍFICA