O Teorema de Minkowski sobre Reticulados

Ana Paula de Melo da Costa

Universidade Federal de Goiás

anapmelocosta@gmail.com

Resumo

O matemático alemão Hermann Minkowski foi um dos precursores na criação e desenvolvimento da chamada *Geometria dos Números*. Ele definiu este termo como significando investigações geométricas de reticulados e conjuntos associados. No ano de 1891, ele introduziu o conceito de *Reticulados* como a coleção de pontos com coordenadas inteiras em um sistema de coordenadas com eixos perpendiculares. O *Teorema de Minkowski sobre Reticulados* é uma ferramenta usada para resolver diversos problemas de Teoria dos Números e Teoria Algébrica dos Números, por exemplo.

Introdução

Definição. Seja $\{e_1, e_2, \ldots, e_m\}$ um conjunto linearmente independente de vetores em $\mathbb{R}^n$. Um *reticulado* L de dimensão m é o subgrupo aditivo ($\mathbb{R}^n$, +) gerado por $e_1, e_2, \ldots, e_m$. Isto é,

$$L = \{v \in \mathbb{R}^n : v = a_1e_1 + a_2e_2 + \ldots + a_me_m | a_i \in \mathbb{Z}\}.$$

Neste caso, podemos definir o *domínio fundamental* D como o conjunto de todos os elementos $a_1e_1 + \ldots + a_ne_n$, onde $0 \leq a_i < 1$, $\forall\, i = 1, \ldots, n$.

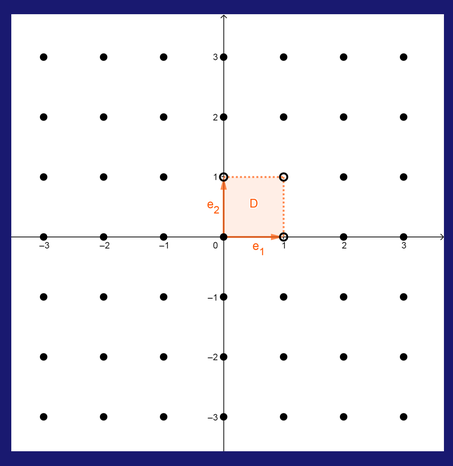

Figura 1: Reticulado de dimensão 2 em $\mathbb{R}^2$ e seu domínio fundamental.

Lema 1. Seja L um reticulado n-dimensional em $\mathbb{R}^n$, cuja base é $\{e_1, e_2, \cdots, e_n\}$. Suponha $e_i = (a_{1i}, a_{2i}, \cdots, a_{ni})$. Então o volume do domínio fundamental D de L definido por essa base é

$$v(D) = |det(a_{ij})|.$$

Observação. Bases diferentes podem gerar o mesmo reticulado, porém os domínios fundamentais associados a cada base diferem. Pelo Lema acima, temos que apesar da diferença geométrica, o volume do domínio fundamental permanece igual qualquer que seja a base considerada.

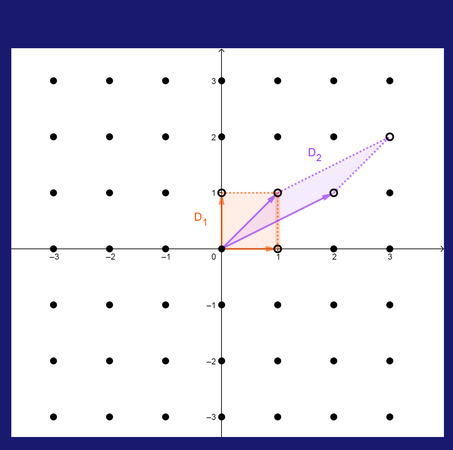

Figura 2: Domínios fundamentais D_1 e D_2 associados, respectivamente, as bases $B_1 = \{(1,0),(0,1)\}$ $B_2 = \{(2,1),(1,1)\}$ do reticulado $\mathbb{Z}^2$.

Teorema de Minkowski

Em suma, o teorema estabelece parâmetros para um subconjunto limitado, simétrico e convexo de $\mathbb{R}^n$, para que o mesmo contenha um ponto não nulo de um reticulado.

Teorema 2. [Minkowski] Sejam L um reticulado de dimensão n em $\mathbb{R}^n$ com domínio fundamental D e X um conjunto simétrico, convexo e limitado em $\mathbb{R}^n$. Se $v(X) > 2^n v(D)$, então X contém um ponto não nulo de L.

Exemplo. Considerando o reticulado $\mathbb{Z}^2$, temos que $v(D) = 1$. Logo, um conjunto X limitado, simétrico e convexo que tem uma área maior que $2^2 \cdot v(D)$ deve ser um paralelogramo de área mínima igual a 4, conforme Figura 3. Assim, o Teorema de Minkowski garante que X contém ponto, não nulo, de $\mathbb{Z}^2$.

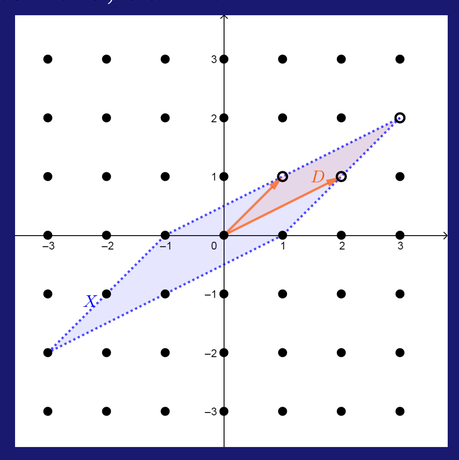

Figura 3: Conjunto X simétrico, convexo e limitado do reticulado $\mathbb{Z}^2$.

Teorema dos quatro quadrados

O *Teorema dos quatro quadrados* afirma que todo inteiro positivo pode ser representado como a soma de quatro quadrados de inteiros. Apesar de ser um resultado puramente algébrico, sua demonstração é consequência imediata do Teorema de Minkowski juntamente com os Lemas 2 e 3.

Lema 2. Se m e n são soma de quatro quadrados de inteiros, então $m \cdot n$ também é uma soma de quatro quadrados de inteiros.

Lema 3. Seja $p > 2$ um inteiro primo. Então, a equação $u^2 + v^2 + 1 \equiv 0\ (mod\ p)$ admite solução inteira no intervalo $[0, \frac{p-1}{2}]$.

Teorema 2. [Lagrange] Todo inteiro positivo n é a soma de quatro quadrados de inteiros.

Demonstração. Se $n = 1$ o resultado é imediato. Se $n \neq 1$, então pode ser decomposto como produto de primo. Daí, pelo Lema 2, basta mostrar o teorema para $n = p$, com p primo. Se $p = 2$ não há o que se fazer. Para p um primo ímpar, pelo Lema 3, existem $u, v \in \mathbb{Z}$ tais que $u^2 + v^2 + 1 \equiv 0\ (\text{mod}\ p)$. Escolha u e v dessa forma e defina $L = L(B)$, o reticulado gerado por B, onde $B = \{e_1, e_2, e_3, e_4\}$ e $e_1 = (1, 0, u, v), e_2 = (0, 1, v, -u), e_3 = (0, 0, p, 0), e_4 = (0, 0, 0, p)$. Isto é,

$L = \{z \in \mathbb{Z}^4 : c \equiv au + bv\ (\text{mod}\ p)$ e $d \equiv bu - av\ (\text{mod}\ p)\}$,

onde $z = (a, b, c, d)$. Logo, o volume de D, domínio fundamental de L nesta base, pelo Lema 1, é $v(D) = |det(e_{ij})| = p^2$.

Considere X a esfera, em $\mathbb{R}^4$, dada por $X = \{(x, y, z, w) \in \mathbb{R}^4 : x^2 + y^2 + z^2 + w^2 < 2p\}$. Então, X é um conjunto limitado, simétrico e convexo, cujo $v(X) = 2p^2\pi^2$. Logo, como $v(X) > 2^4p^2 = 2^4 \cdot v(D)$, pelo Teorema de Minkowski, existe um vetor não nulo $(a, b, c, d) \in L \cap X$. Ou seja, $0 < a^2 + b^2 + c^2 + d^2 < 2p$ e $a^2 + b^2 + c^2 + d^2 \equiv 0\ (\text{mod}\ p)$. Portanto, $a^2 + b^2 + c^2 + d^2 = p$.

Referências

[1] Şaban Alaca and Kenneth S. Williams. *Introductory algebraic number theory*. Cambridge University Press, Cambridge, 2004.

[2] Rodrigo Gondim. *Geometria aritmética em retas e cônicas*. Publicações Matemáticas do IMPA. Instituto Nacional de Matemática Pura e Aplicada (IMPA), Rio de Janeiro, 2011. 28º Colóquio Brasileiro de Matemática.

[3] Ian Stewart and David Tall. *Algebraic number theory and Fermat's last theorem*. A K Peters, Ltd., Natick, MA, third edition, 2002.