MT803D - Tópicos em Matemática Aplicada

Reticulados, Teoremas de Minkowski Revisitados e Teoremas de Somas de Quadrados

# 1 Definições Iniciais

Os teoremas de Minkowski e Blitchfield, bem como suas respectivas generalizações, tornam-se ferramentas poderosas quando consideramos transformações lineares aplicadas no conjunto de vetores inteiros $\mathbb{Z}^n$, isto é, conjuntos do tipo $B\mathbb{Z}^n$, $B \in \mathbb{R}^{n\times n}$. Tais conjuntos, denominados reticulados (euclidianos), serão nosso objeto de estudo.

Sejam $m \leq n$ vetores linearmente independentes $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m \in \mathbb{R}^n$. Um *reticulado* $\Lambda$ com base $\{\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m\}$ é o conjunto de todas as combinações lineares inteiras de $\boldsymbol{a}_i$, $i = 1, \ldots, m$, isto é:

$$\Lambda = \{u_1\boldsymbol{a}_1 + \ldots + u_m\boldsymbol{a}_m : u_1, \ldots, u_m \in \mathbb{Z}\}. \tag{1}$$

O conjunto $\{\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m\}$ é denominado uma *base* de $\Lambda$. A matriz $A$ cujas colunas são os vetores $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$ é dita uma *matriz geradora* de $\Lambda$. Durante o texto, representaremos também um reticulado gerado pela matriz $A$ por $\Lambda(A) = \Lambda(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m) = \Lambda$, intercambiando livremente as notações quando não houver ambiguidade. O número de vetores de uma base de $\Lambda$ é chamado de *posto* ou *dimensão*. Caso $m = n$, dizemos que $\Lambda$ possui *posto completo*. A partir de agora, trataremos apenas de reticulados de posto completo (apesar de reticulados de posto incompleto, definidos por projeções/interseções serem bastante estudados na teoria). Podemos re-escrever (1) matricialmente como

$$\Lambda(A) = A\mathbb{Z}^n = \{A\boldsymbol{u} : \boldsymbol{u} \in \mathbb{Z}^n\}, \tag{2}$$

Dizemos que um conjunto $M \subset \mathbb{R}^n$ é *discreto* se existe $\varepsilon > 0$ tal que $\boldsymbol{x} + B_2(\varepsilon) \cap \boldsymbol{y} + B_2(\varepsilon) = \emptyset$. Da definição, é intuitivo que $\Lambda$ seja um subgrupo aditivo e discreto do $\mathbb{R}^n$. O teorema abaixo mostra que esta condição é suficiente para caracterizar um reticulado. Ele encaixa-se no grupo de teoremas denominados por D. West como TONCAs ("The Obvious Necessary Condition is Also Sufficient").

**Teorema 1.** *Um conjunto $\Lambda \subset \mathbb{R}^n$ é um reticulado se, e somente se, é um subgrupo aditivo discreto de $\mathbb{R}^n$.*

Demonstraremos a versão do Teorema 1 para $\Lambda$ de posto completo, a saber: Um conjunto $\Lambda \subset \mathbb{R}^n$ não contido em nenhum subespaço $(n-1)$-dimensional do $\mathbb{R}^n$ é um reticulado de posto completo se, e somente se, é um subgrupo aditivo discreto de $\mathbb{R}^n$. A generalização para reticulados de posto incompleto é direta.

*Demonstração.* ($\Rightarrow$) (*Easy*) É claro que para $\boldsymbol{x}, \boldsymbol{y} \in \Lambda$, $-\boldsymbol{x} \in \Lambda$ e $\boldsymbol{x}+\boldsymbol{y} \in \Lambda$. Para mostrar que $\Lambda$ é discreto, considere primeiro $\Lambda = \mathbb{Z}^n$. Temos que para qualquer $\varepsilon < 1$, $\boldsymbol{x} + B_2(\varepsilon) \cap \boldsymbol{y} + B_2(\varepsilon) = \emptyset$ para todos $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{Z}^n$, $\boldsymbol{x} \neq \boldsymbol{y}$. Portanto, para um reticulado geral (gerado pela matriz $A$) temos

$$A\boldsymbol{x} + AB_2(\varepsilon) \cap A\boldsymbol{y} + AB_2(\varepsilon) = \emptyset, \forall \boldsymbol{x}, \boldsymbol{y} \in \mathbb{Z}^n, \boldsymbol{x} \neq \boldsymbol{y}.$$

Mas $AB_2(\varepsilon)$ é um elipsoide e portanto contém uma bola $B_2(\varepsilon')$, demonstrando a condição necessária.

($\Leftarrow$) Assumimos agora que $\Lambda$ seja um subgrupo aditivo e discreto do $\mathbb{R}^n$. Mostraremos que $\Lambda$ é um reticulado construindo, indutivamente, uma base de vetores.

(i) Escolha do primeiro vetor: Tome $\boldsymbol{a}_1$ com a propriedade de que o segmento de reta aberto $\lambda \boldsymbol{a}_1, \lambda \in (0,1)$ não contenha nenhum outro ponto de $\Lambda$. A existência de $\boldsymbol{a}_1$ é garantida pelo fato de que $\Lambda$ é discreto.

(ii) Suponhamos que $\boldsymbol{a}_1, \ldots \boldsymbol{a}_j$ foram escolhidos. Tome $\boldsymbol{c}_{j+1} \notin \Lambda(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_j)$ e considere o paralelotopo fechado

$$\mathcal{P}_j = \{\alpha_1 \boldsymbol{a}_1 + \ldots + \alpha_j \boldsymbol{a}_j + \alpha_{j+1} \boldsymbol{c}_{j+1} : \alpha_i \in [0,1]^n\}.$$

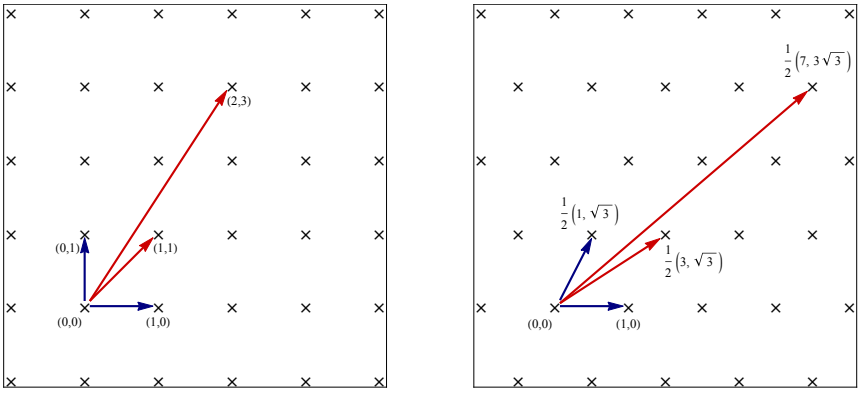
Como $\Lambda$ é discreto e $\mathcal{P}_j$ é limitado, $\Lambda \cap \mathcal{P}_j$ é finito. Escolhemos para o próximo vetor $\boldsymbol{a}_{j+1}$ o elemento de $\Lambda \cap \mathcal{P}_j$ tal que $\alpha_{j+1} > 0$ seja mínimo. (iii) Considere que $n$ vetores foram escolhidos. É claro que $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ são LI e, como $\Lambda$ é um subgrupo, $\Lambda(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n) \subset \Lambda$. Ademais, afirmamos que todo ponto de $\Lambda$ pode ser escrito como combinação inteira de $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$. Com efeito, escrevemos qualquer ponto $\boldsymbol{x} \in \Lambda$ como combinação (possivelmente não-inteira) dos vetores $\boldsymbol{a}_i$, isto é:

$$\boldsymbol{x} = u_1 \boldsymbol{a}_1 + \ldots + u_n \boldsymbol{a}_n, u_i \in \mathbb{R}.$$

Suponha que $u_n$ não seja inteiro e considere $\bar{\boldsymbol{x}} = \lfloor u_1 \rfloor \boldsymbol{a}_1 + \ldots + \lfloor u_n \rfloor \boldsymbol{a}_n \in \Lambda$.

$$\boldsymbol{z} := \boldsymbol{x} - \bar{\boldsymbol{x}} = (u_1 - \lfloor u_1 \rfloor)\boldsymbol{a}_1 + \ldots + (\lfloor u_n \rfloor - u_n)\boldsymbol{a}_n \in \Lambda.$$

À partir de $\boldsymbol{z}$, obteríamos um vetor em $\mathcal{P}_n$ com $\alpha_n$ menor que o mínimo possível, a menos que $u_n = \lfloor u_n \rfloor$ (ou $u_n$) seja inteiro. Continuando esse argumento, mostramos que $u_{n-1}, \ldots, u_1 \in \mathbb{Z}$. $\square$




(a) Reticulado $\mathbb{Z}^2$ (b) Reticulado Hexagonal

Figura 1: Bases distintas para o mesmo reticulado em cada figura

Um reticulado $\Lambda(A)$ possui infinitas bases, como ilustrado na Figura 1. A caracterização de bases distintas é feita a partir de matrizes em $Gl_n(\mathbb{Z})$.

**Proposição 1.1.** *$\Lambda(A) = \Lambda(B)$ se, e somente se, $A = BU$, em que $U \in Gl_n(\mathbb{Z}^n)$.*

*Demonstração.* Sejam $\boldsymbol{b}_1, \ldots, b_n$ e $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ as colunas de $A$ e $B$. Como $\Lambda(A) \subset \Lambda(B)$, então $\boldsymbol{a}_i = B\boldsymbol{u}_i$, $\boldsymbol{u}_i \in \mathbb{Z}^n$, o que implica $A = BU$, $U \in \mathbb{Z}^{n\times n}$. Analogamente, temos $B = AV$, $V \in \mathbb{Z}^{n\times n}$, o que implica $\det B = \det B \det U \det V \Rightarrow \det U \det V = 1$. Assim $U$ e $V$ são unimodulares e, de fato, não é difícil ver que $V = U^{-1}$. $\square$

**Exemplo 1.** *Na Figura 1 estão ilustrados dois reticulados contidos no plano e duas bases distintas para cada um deles. As matrizes geradoras associadas às diferentes bases do reticulado $\mathbb{Z}^2 = \{(u_1, u_2) : u_1, u_2 \in \mathbb{Z}\}$ em 1a são*

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ e } \overline{B} = \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix}.$$

*No caso do reticulado hexagonal,1b, temos*

$$A = \begin{pmatrix} 1 & 1/2 \\ 0 & \sqrt{3}/2 \end{pmatrix} \text{ e } \overline{B} = \begin{pmatrix} 3/2 & 7/2 \\ \sqrt{3}/2 & 3\sqrt{3}/2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1/2 & \sqrt{3}/2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix}.$$

*Em ambos os casos, a matriz mudança de base unimodular $U$ é dada por*

$$U = \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix}.$$

Um corolário do teorema acima é que qualquer matriz geradora para o mesmo reticulado possui o mesmo determinante, em módulo. Assim, definimos $\det \Lambda := |\det B|$ em que $B$ é qualquer matriz geradora. O determinante $\det \Lambda$ é um importante invariante de um reticulado.

## 1.1 Sub-reticulados

Sejam $\Lambda, \Lambda' \subset \mathbb{R}^n$ dois reticulados de mesmo posto. Se $\Lambda' \subseteq \Lambda$, dizemos que $\Lambda'$ é um *sub-reticulado* de $\Lambda$. O *índice* de $\Lambda'$ em $\Lambda$ definido como a $\det \Lambda' / \det \Lambda$. Como qualquer ponto de $\Lambda'$ é também um ponto de $\Lambda$, se $\Lambda = \Lambda(A)$ e $\Lambda' = \Lambda(B)$, então as colunas de $B$ podem ser escrita como combinações inteiras das colunas de $A$. Assim $B = AM$, $M \in \mathbb{Z}^n$, mostrando que o índice de $\Lambda'$ em $\Lambda$ é sempre um número inteiro.

Utilizando a caracterização de $\Lambda'$ e $\Lambda$ como grupos abelianos, é possível definir o quociente $\Lambda/\Lambda'$ como

$$\frac{\Lambda}{\Lambda'} = \{\Lambda' + \boldsymbol{x} : \boldsymbol{x} \in \Lambda\}.$$

Dizemos que $\boldsymbol{x}, \boldsymbol{y} \in \Lambda$ estão na mesma classe de equivalência se $\boldsymbol{x}+\Lambda = \boldsymbol{y}+\Lambda$, o que por sua vez, ocorre se, e somente se, $\boldsymbol{x} - \boldsymbol{y} \in \Lambda'$. A cardinalidade do grupo quociente $|\Lambda/\Lambda'|$ é igual ao número de classes de equivalências distintas em $\Lambda$ com respeito a $\Lambda'$. Temos o seguinte resultado:

**Proposição 1.2.** *A cardinalidade do grupo quociente $\Lambda/\Lambda'$ é igual ao índice de $\Lambda'$ em $\Lambda$.*

*Demonstração.* Forma Normal de Smith. Sejam $A$ e $B$ matrizes geradoras para $\Lambda$ e $\Lambda'$, com $A = BM$, $M \in \mathbb{Z}^{n\times n}$. A Forma Normal de Smith de $M$ é dada por $M = UDV$, $U, V \in \mathrm{Gl}_n(\mathbb{Z})$. Temos, assim

$$A = BUDV \Rightarrow AV^{-1} = BUD \Rightarrow A' = B'D$$

em que $A' = AV^{-1}$ e $B' = BU$ são matrizes geradoras para $\Lambda$ e $\Lambda'$, pela Proposição 1.1. As bases $A'$ e $B'$ satisfazem $\boldsymbol{a}'_i = d_i \boldsymbol{b}_i$. Tome um vetor $\boldsymbol{x} = u_1\boldsymbol{a}'_1 + \ldots + u_n\boldsymbol{a}'_n \in \Lambda$. Provaremos que $\boldsymbol{x}$ está na mesma classe de equivalência de $r_1\boldsymbol{a}'_1 + \ldots + r_n\boldsymbol{a}'_n$, em que $r_i$ é o resto da divisão de $u_i$ por $d_i$ (isto é, $u_i = q_i d_i + r_i$, $0 \le r_i < d_i$). Com efeito,

$$\begin{aligned}\boldsymbol{x} - (r_1\boldsymbol{a}'_1 + \ldots + r_n\boldsymbol{a}'_n) &= q_1 d_1 \boldsymbol{a}'_1 + \ldots + q_n d_n \boldsymbol{a}'_n \\ &= q_1\boldsymbol{b}'_1 + \ldots + q_n\boldsymbol{b}'_n \in \Lambda'.\end{aligned}$$

Assim, as únicas classes de equivalências são $r_1\boldsymbol{a}'_1 + \ldots + r_n\boldsymbol{a}'_n + \Lambda$, o que nos dá $d_1 d_2 \ldots d_n = |\det B|$ possibilidades, todas elas distintas. $\square$

A consequência geométrica é dada a seguir:

**Corolário 1.** *A cardinalidade do quociente $\Lambda/\Lambda'$ é igual à quantidade de pontos de $\Lambda$ no paralelotopo aberto*

$$\mathcal{P}(A) = \{\alpha_1 \boldsymbol{a}_1 + \ldots + \alpha_n \boldsymbol{a}_n : \alpha_i \in [0,1)\},$$

*isto é $\Lambda/\Lambda' = \#(\mathcal{P}(A) \cap \Lambda)$.*

*Demonstração.* Uma consequência imediata da Seção 5.2, da segunda aula, generalizada para qualquer reticulado $\Lambda$. □

Seja $m \in \mathbb{N}$. A quantidade de números de sub-reticulados de $\Lambda$ com um dado índice $m$ é denotada por $L_N(m)$. Pode-se mostrar que $L_N(m)$ é finita e é uma função multiplicativa (isto é $L_N(m_1 m_2) = L_N(m_1) L_N(m_2)$ sempre que $\gcd(m_1, m_2) = 1$). Fórmulas para $L_N(m)$ podem ser encontradas em [New72, Cap. 2].

## 1.2 Teoremas de Minkowski e Blichfeldt

Como $\Lambda(A) = A\mathbb{Z}^n$, as versões gerais dos Teoremas de Minkowski podem ser facilmente enunciadas na linguagem de reticulados. Recapitulando a aula anterior:

**Teorema 2.** *Se $K \subset \mathbb{R}^n$ é um conjunto limitado tal que $0 < \operatorname{vol} K < \infty$, então*

$$\lim_{r \to \infty} \frac{\#(K \cap \Lambda)}{\operatorname{vol} rK} = \frac{1}{\det \Lambda}.$$

**Teorema 3.** *Se $K$ é um conjunto fechado, limitado, e $\operatorname{vol} K \geq \det \Lambda$, então existem $\boldsymbol{x}, \boldsymbol{y} \in K$, $\boldsymbol{x} \neq \boldsymbol{y}$, tais que $\boldsymbol{x} - \boldsymbol{y} \in \Lambda$.*

**Teorema 4.** *Se $K$ é um corpo convexo fechado, centralmente simétrico, e $\operatorname{vol} K \geq \det A$, então existem $\boldsymbol{x}, \boldsymbol{y} \in K$, $\boldsymbol{x} \neq \boldsymbol{y}$, tais que $\boldsymbol{x} - \boldsymbol{y} \in \Lambda$.*

# 2 Primeiro Mínimo

Seja $K$ um corpo convexo fechado, centralmente simétrico, e $F_K(\boldsymbol{x})$ a sua função de *gauge*. Definimos o primeiro mínimo de $\Lambda$ com relação a $K$ como:

$$\lambda_{1,K}(\Lambda) = \min_{\boldsymbol{x} \in \Lambda \setminus \{\boldsymbol{0}\}} F_K(\boldsymbol{x}). \tag{3}$$

Encontrar $\lambda_{1,K}(\Lambda)$ possui interesse tanto teórico como prático, por exemplo na proposição e análise de esquemas criptográficos (falaremos sobre isso mais

para frente no curso, e nos trabalhos finais). Um caso bastante especial que será estudado mais para frente é quando $K = B_2(1)$ é a esfera euclidiana em $\mathbb{R}^n$ com raio 1. O Teorema de Minkowski para Corpos Convexos 4 nos dá uma estimativa para o primeiro mínimo de $\Lambda$:

**Teorema 5.** *Seja $K$ um corpo convexo fechado centralmente simétrico e $\Lambda \subset \mathbb{R}^n$ um reticulado.*

$$\lambda_{1,K}(\Lambda) \leq 2 \left( \frac{\det \Lambda}{\text{vol } K} \right)^{1/n}. \tag{4}$$

*Demonstração.* Se $r = 2 \left( \frac{\det \Lambda}{\text{vol } K} \right)^{1/n}$, então vol $rK = 2^n \det \Lambda$. Pelo Teorema 4, existe $\boldsymbol{x} \in rK \cap \Lambda$. Isso significa que existe $\boldsymbol{x} \in \Lambda$ com $F_K(\boldsymbol{x}) \leq r$, de onde segue o limitante. □

Quando $K = B_p(1) = \{\boldsymbol{x} \in \mathbb{R}^n : |x_1|^p + \ldots + |x_n|^p \leq 1\}$ é a bola unitária na norma $\ell_p$ um limitante sutilmente mais fraco que (4), porém bastante útil, pode ser derivado:

**Teorema 6** (Minkowski para norma $l_p$)**.** *Seja $\Lambda \subset \mathbb{R}^n$ um reticulado de posto $n$, e $1 \leq p < \infty$. Existe um ponto não-nulo $\boldsymbol{x} \in \Lambda$ tal que*

$$\|\boldsymbol{x}\|_p \leq n^{1/p} (\sqrt{\det \Lambda})^{1/n} \tag{5}$$

*Demonstração.* Sabemos que $\|\boldsymbol{x}\|_p \leq n^{1/p} \|\boldsymbol{x}\|_\infty$, e portanto vale a inclusão $B_\infty(r) \subseteq B_p(n^{1/p} r)$. Tome $r = \sqrt{\det \Lambda}^{1/n}$. O volume de $B_\infty(r)$ é o volume do cubo de lado $2R$ centrado em $\boldsymbol{x}$, dado por

$$\text{vol } B_\infty(r) = 2^n r^n = 2^n \sqrt{\det \Lambda}.$$

Assim vol $B_p(n^{1/p} r) \geq 2^n \sqrt{\det \Lambda}$ e pelo Corolário 1, existe um ponto $\boldsymbol{x} \in \Lambda \cap B_p(n^{1/p} r)$, de onde vem que

$$\|\boldsymbol{x}\|_p \leq n^{1/p} (\sqrt{\det \Lambda})^{1/n}.$$

□

**Observação 1.** *De fato vale a desigualdade estrita* vol $B_p(1) < n^{n/p} 2^n =$ vol $B_\infty(n^{1/p})$. *Assim a desigualdade* (5) *pode ser substituída pela desigualdade estrita (veja também Exercício 1).*

# 3 Somas de Quadrados

Os teoremas acima parecem, à primeira vista, versar apenas sobre propriedades extremamente específicas e geométricas de reticulados euclidianos. Entretanto, já mostramos na terceira aula uma aplicação do Teorema de Minkowski para Corpos Convexos a aproximações diofantinas simultâneas (ou produtos de formas lineares). Apresentaremos aqui uma aplicações à Teoria dos Números, em particular aos teoremas dos dois e quatro quadrados.

## 3.1 Teorema dos Dois Quadrados

**Teorema 7** (dos Dois Quadrados)**.** *Seja $p \in \mathbb{N}$ um número primo. Então $p = a^2 + b^2$, para $a, b \in \mathbb{N}$ se, e somente se, $p = 2$ ou $p \equiv 1 \bmod 4$.*

A condição necessária é simples. Com efeito, um inteiro $a^2$ só pode ser congruente a 0 ou 1 módulo 4. Então se $p$ pode ser representado como soma de 2 quadrados, $p = 2$ ou $p$ é um primo ímpar congruente a 1 módulo 4. Para uma demonstração "clássica" da condição suficiente veja [IN91]. Aqui mostraremos como o teorema segue como uma aplicação do Teorema de Minkowski. Precisamos antes de um simples fato da Teoria dos Números, que é uma consequência de resultados mais gerais acerca de resíduos quadráticos.

**Lema 1.** *Se $p$ é um primo tal que $p \equiv 1 \bmod 4$, então existe $x$ tal que $x^2 \equiv -1 \bmod p$.*

*Demonstração.* Para qualquer $i \in \{1, 2, \ldots, p-1\}$, existe $a_i \neq i$ tal que $ia_i \equiv -1 \bmod p$. Além disso, para $i \neq j$, $a_i \neq a_j$. Assim, agrupando os termos, temos

$$1a_1 \times 2a_2 \times \ldots \times \left(\frac{p-1}{2}\right) a_{\frac{p-1}{2}} \equiv \underbrace{(-1) \times (-1) \ldots \times (-1)}_{(p-1)/2 \text{ vezes}} \equiv (-1)^{\frac{p-1}{2}}.$$

Mas o lado esquerdo da igualdade acima é igual a $(p-1)! \equiv -1 \bmod q$ (por quê?). Assim, temos $(-1)^{\frac{p-1}{2}} \equiv -1 \bmod p$, o que é absurdo. Logo, existe $x$ tal que $x^2 \equiv -1 \bmod p$. $\square$

*Demonstração do Teorema 3:* Seja $x$ tal que $x^2 \equiv -1 \bmod p$. Seja $\Lambda$ o reticulado gerado pela matrix

$$A = \begin{pmatrix} p & x \\ 0 & 1 \end{pmatrix}$$

Tome agora qualquer elemento em $(pu_1 + u_2x, u_2) \in \Lambda$, $u_1, u_2 \in \mathbb{Z}$. Temos:

$$\|(pu_1 + u_2x, u_2q)\|_2^2 = (pu_1 + u_2x)^2 + (u_2)^2 \equiv 0 \bmod q,$$

ou seja, a norma ao quadrado de todos os elementos de $\Lambda$ é um múltiplo de $p$. Pelo Teorema 4, existe um elemento não-nulo $\boldsymbol{y} = (y_1, y_2) \in \Lambda$ cujo quadrado da norma satisfaz

$$\|\boldsymbol{y}\|_2^2 \leq 2^2 \frac{\det \Lambda}{\text{vol } B_2(1)} \leq \frac{4p}{\pi} < 2p$$

Como a norma de $\boldsymbol{y}$ é múltipla de $p$, temos temos que ter necessariamente $y_1^2 + y_2^2 = p$, finalizando a prova do teorema. □

Utilizando a identidade

$$(a_1^2 + b_1^2)(a_2^2 + b_2^2) = (a_1b_1 + a_2b_2)^2 + (a_1b_2 - a_2b_1)^2$$

vemos que se dois números são representados como soma de dois quadrados, então o seu produto também pode ser representado de tal maneira[1]. Assim, pode-se demonstrar a versão completa do Teorema dos Dois quadrados

**Teorema 8** (dos Dois Quadrados Completo)**.** *Dado um número inteiro $m$, existem $a, b$ tais que $m = a^2 + b^2$ se, e somente se, $m = ck^2$, em que $c \in \mathbb{N}$ não possui nenhum fator primo congruente a 3 módulo 4.*

## 3.2 Teorema dos Quatro Quadrados

O Teorema dos Quatro Quadrados (de Langrage) afirma que todo número inteiro positivo pode ser escrito como a soma de quatro quadrados. O Teorema 5 para o primeiro mínimo de $\Lambda$ nos auxilia a demonstrar a versão do teorema quando $p$ é um número primo. Primeiramente, precisamos de um lema auxiliar com o mesmo "sabor" do Lema 1.

**Lema 2.** *Seja $p$ um número primo maior que 2. Existem $w, z$ tais que $w^2 + z^2 \equiv -1 \bmod p$.*

*Demonstração.* Seja o conjunto

$$S_w = \left\{ w^2 \bmod p : w = 0, \ldots, \frac{p-1}{2} \right\}.$$

[1]Uma maneira esclaredora de demonstrar a identidade sem "abrir os dois lados" é considerar o conjunto de inteiros de Gauss $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$, em que $i^2 = -1$. A norma de um ponto em $\mathbb{Z}[i]$ é dada por $a^2 + b^2 = (a+bi)(a-bi)$. A identidade é equivalente à multiplicatividade da norma, i.e., $N(a_1 + ib_1).N(a_2 + ib_2) = N((a_1 + ib_1)(a_2 + ib_2))$.

Afirmamos que $\#S_w = p + 1/2$. De fato, tomando dois pontos $0 \leq w_1, w_2 \leq (p-1)/2$ com $w_1 > w_2$ temos $w_1^2 \not\equiv w_2^2 \bmod p$, caso contário,

$$w_1^2 - w_2^2 = (w_1 + w_2)(w_1 - w_2) \equiv 0 \bmod p,$$

e portanto $p$ deveria dividir $w_1 + w_2$ ou $w_1 - w_2$, o que não pode ocorrer pois ambos os termos estão entre 0 e $p-1$. Assim, $0^2, 1^2, 2^2, \ldots (p-1)/2^2$ estão em classes distintas módulo $p$ e portanto $\#S_w = (p+1)/2$. De maneira bastante análoga, mostramos que o conjunto

$$S_z = \left\{ -1 - z^2 \bmod p : w = 0, \ldots, \frac{p-1}{2} \right\}$$

possui cardinalidade $(p+1)/2$. Como $\#S_w + \#S_z = p + 1$, deve existir um elemento em $\#S_w \cap \#S_z$, dando-nos os números $w$ e $z$ desejados. □

**Teorema 9.** *Seja $p$ um número primo. Existe $a, b, c, d$ tais que $a^2 + b^2 + c^2 + d^2 = p$.*

*Demonstração.* Se $p = 2$ o teorema é trivial. Se $p > 2$, sejam $w$ e $z$ dados pelo lema acima. Como é esperado, construímos um reticulado 4-dimensional e aplicamos o teorema de Minkowski. O reticulado considerado é o dado pela matriz

$$A = \begin{pmatrix} p & 0 & w & -z \\ 0 & p & z & w \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

A norma ao quadrado de um vetor $A\boldsymbol{u}$, $\boldsymbol{u} \in \mathbb{Z}^4$ é dada por

$$\|A\boldsymbol{u}\|^2 = u_3^2 + u_4^2 + (pu_2 + zu_3 + wu_4)^2 + (pu_1 + wu_3 - zu_4)^2.$$

Com a restrição de que $w^2 + y^2 \equiv -1 \bmod p$ não é difícil ver que $\|A\boldsymbol{u}\|^2 \equiv 0 \bmod p$. Aplicando o Teorema 5, existe um vetor não nulo $\boldsymbol{y}$ com norma

$$\|\boldsymbol{y}\|^2 \overset{(a)}{\leq} 4 \left( \frac{\det \Lambda}{(\pi^2/2)} \right)^{1/2} = \frac{4\sqrt{2}p}{\pi} < 2p,$$

em que $\pi^2/2$ é o volume da bola unitária em $\mathbb{R}^4$. Assim $\|\boldsymbol{y}\|^2 = p$, provando o teorema. □

Para enunciar a versão completa do Teorema dos Quatro Quadrados, precisamos da Identidade de Euler

$$\begin{aligned} &(a_1^2 + b_1^2 + c_1^2 + d_1^2)(a_2^2 + b_2^2 + c_2^2 + d_2^2) = \\ &(a_1a_2 + b_1b_2 + c_1c_2 + d_1d_2)^2 + (a_1b_2 - b_1a_2 + c_1d_2 - d_1c_2)^2 + \\ &(a_1c_2 - b_1d_2 - c_1a_2 + d_1b_2)^2 + (a_1d_2 + b_1c_2 - c_1b_2 - d_1a_2)^2. \end{aligned}$$

Novamente, é muito simples demonstrar a identidade acima simplesmente expandindo os dois lados. Uma demonstração mais esclarecedora é à partir dos inteiros de Lipschitz

$$\mathcal{L}(i,j,k) = \{a + bi + cj + dk : a,b,c,d \in \mathbb{Z}\},$$

em que $i,j,k$ são as unidades quaternionicas $i^2 = j^2 = k^2 = ijk = -1$. A norma de um elemento em $\mathcal{L}(i,j,k)$ é dada por

$$N(a+bi+cj+dk) = a^2+b^2+c^2+d^2 = (a+bi+ci+di)(a-bi-ci-di).$$

A identidade de Euler é equivalente à multiplicativadade da norma, $N(z_1z_2) = N(z_1)N(z_2)$, para $z_1, z_2 \in \mathcal{L}(i,j,k)$.

A Identidade de Euler implica que se dois números são representados como somas de dois quadrados, então o produto deles também é, de onde deduzimos imediatamente

**Teorema 10.** *Seja $m$ um número inteiro. Existem $a,b,c,d$ tais que*

$$a^2+b^2+c^2+d^2 = m.$$

Outros teoremas considerando somas de quadrados e formas quadráticas são possíveis. Por exemplo, o seguinte teorema generaliza o dos dois quadrados, versando sobre primos escritos na forma $a^2+mb^2$.

**Teorema 11.** *Seja $p$ um primo $m \in \mathbb{Z}^n$ tal que $m$ é um resíduo quadrático módulo $p$ (isto é, existe $x$ tal que $x^2 \equiv -m \bmod p$). Existem $a,b,k$ tais que $a^2+mb^2 = kp$, com $1 \le k \le \lfloor 4\sqrt{m}/\pi \rfloor$.*

A demonstração, como esperado, utiliza um reticulado 2-dimensional conveniente.

**Exercício 1.** Aprimore o limitante do Teorema 2, utilizando a fórmula de volume para a bola na norma $l_p$:

$$\text{vol } B_p(r) = 2^n r^n \frac{\Gamma\left(1+\frac{1}{p}\right)^n}{\Gamma\left(1+\frac{n}{p}\right)}.$$

Compare com o Teorema 2 em termos assintóticos.
Dica: Utilize a aproximação de Stirling $\Gamma(s) \approx \sqrt{2\pi}e^{-s}s^{s-1/2}$.

**Exercício 2.** Seja $p$ um primo e $2n+1$ um número ímpar. Prove que existe $0 < m < p^{2n}$ tal que

$$mp = a^{2n+1} + b^{2n+1},$$

com $a$ e $b$ naturais.

**Exercício 3.** Utilizando a nossa demonstração do Teorema 3, encontre $a$ e $b$ tais que $a^2 + b^2 = p$ para $p = 29$, $p = 252097800629$ e $p = 2760727302649$.
Dica: utilize rotinas computacionais para encontrar vetores curtos em um reticulado.

**Exercício 4.** Demonstre o Teorema 8.

**Exercício 5.** Demonstre o Teorema 11. É possível melhorar o limitante para o múltiplo $k$?

# Referências


[IN91] H. L. Montgomery I. Niven, H. S. Zuckerman. *An Introduction to The Theory of Numbers.* Wiley, 5 edition, 1991.

[New72] M. Newmman. *Integral Matrices.* Academic Press, 1972.