Universidade Federal
de São João del-Rei

Pedro Henrique Cardoso de Sousa

TEOREMA DE MINKOWSKI E APLICAÇÕES

São João del-Rei

Dezembro de 2018

Pedro Henrique Cardoso de Sousa

TEOREMA DE MINKOWSKI E APLICAÇÕES

Trabalho de Conclusão de Curso apresentado à Coordenadoria do Curso de Matemática, da Universidade Federal de São João del-Rei, como requisito parcial à obtenção do título de Licenciado em Matemática.

Orientador: Prof. Dr. Fábio Alexandre de Matos

São João del-Rei, _____ de _____ de _____

Banca Examinadora

_____

Orientador: Prof. Dr. Fábio Alexandre de Matos

_____

Prof. Dr. Arnulfo Miguel Rodríguez Peña

_____

Prof. Dr. Waliston Luiz Lopes Rodrigues Silva

São João del-Rei

Dezembro de 2018

Agradecimentos

A sensação é de imensa gratidão, primeiramente agradeço a minha família: minha irmã Emily, companheira de idas e vindas pra aula nesses três últimos anos e que esteve ali sempre quando precisei; meu irmão Sidney, que assim como minha irmã sempre esteve presente quando precisei; minha mãe Emília que todos os dias faz de tudo por mim, mesmo que as vezes do seu jeito, mas sei que acredita ser sempre o correto e agradeço por isso; meu pai José Narciso, meu maior incentivador e com quem pude contar durante toda minha vida; agradeço também aos meus tios Nilton e Nivaldo e tias Fátima, Lia e Luci, minha vó Eni e meu avô Dedé, por toda a liberdade e torcida nesse tempo todo.

Agradeço também a todos professores que passaram pela minha formação, em especial a Carlos e Fábio por toda a amizade e apoio. Agradeço a banca examinadora pela boa vontade e disponibilidade.

Sozinho não chegaria a lugar nenhum, e nesses quatro anos tive o prazer de conviver com pessoas como Elton, Júlio César, Hamilton, Mariana, Marcelo, Nívio, Paloma, Rafael, Rafaela, Utan, Vitor e tantos outros, onde cada um de sua maneira fazem parte disso.

Por fim, agradeço a aqueles que contribuíram estando presente no meu dia a dia, todos meus amigos do "Fut dos Mano", Carlinhos, Dener, José Fabiano, Kellynho e Sarita principalmente, por todo companheirismo, todas as gargalhadas e pelo simples fato de estarem no meu dia a dia, foram importantíssimos.

Agradeço a todos pela torcida!

Dedicatória

Dedico este trabalho ao meu pai José Narciso de Sousa pois, esse também é um sonho seu e só estou podendo desfrutar deste momento pelo seu empenho, desde a época da escola básica, em me propiciar todas as condições necessárias para estar preparado para momentos assim. Obrigado pai!

"Só se pode alcançar um grande êxito quando nos mantemos fiéis a nós mesmos."

Friedrich Nietzsche

Resumo

Este presente trabalho tem como objetivo estudar uma técnica geométrica que pode ser utilizada para a soma de quadrados. Passaremos por definições importantes dentro da Teoria dos Números como por exemplo as definições dos conjuntos de números naturais e inteiros, de divisibilidade, de números primos e de congruência módulo n, chegando, por fim, no Teorema de Minkowski, matemático alemão que iniciou a ideia da Geometria dos Números; resultado que será utilizado para o estudo de tal técnica.

Palavras-chave: Números Naturais, Números Inteiros, Divisibilidade, Números Primos, Congruência, Reticulado, Minkowski, Soma de Quadrados.

Sumário

Introdução

A Teoria dos Números pode ser considerada uma das mais antigas áreas da Matemática e, dentro dessa, existem algumas outras subáreas, como por exemplo a Aritmética, a Teoria Analitica dos Números, a Teoria Algébrica dos Números e também Teoria Geométrica dos Números, criada pelo matemático alemão Hermann Minkowski.

A Teoria dos Números desperta grande interesse para diversos pesquisadores e também para alunos de graduação, uma vez que através de seus problemas e de seu caráter intrigante nos trás a motivação na busca de padrões e generalizações. Um exemplo é o problema relacionado a soma de quadrados, será que existe algum padrão ou ainda algum resultado que nos remeta a escrita de determinados números como soma de quadrados? Seja esse número inteiro ou, ainda mais restrito, um número primo, buscar o conhecimento sobre algum resultado dentro da Teoria dos Números ou em uma de suas subáreas torna-se uma tarefa bastante interessante.

Neste contexto algumas técnicas geométricas surgem como ferramentas que podem ser utilizadas para o estudo de soma de quadrados, é o caso do Teorema de Minkowski, que nos permitirá provar teoremas que garantem que

Todo primo p da forma $4k+1$ é soma de dois quadrados, mais ainda, que *todo primo p é soma de quatro quadrados* e ainda que *todo inteiro não negativo* também *pode ser escrito como soma de quatro quadrados*,

resultados interessantíssimos que a partir deste teorema podem ser demonstrados.

No primeiro capítulo deste trabalho apresentaremos alguns conceitos iniciais da Teoria dos Números que são necessários nas construções subsequentes, começando com os números naturais $\mathbb{N}$, com sua definição axiomática, definindo os números inteiros $\mathbb{Z}$ e a divisibilidade. Será apresentado um pouco sobre o conjunto dos números primos, passando pelo Teorema Fundamental da Aritmética, pelo Crivo de Erastótenes e pela infinidade dos mesmos, por fim, dentro dos conceitos iniciais, falaremos sobre congruência módulo

n, uma relação que virá a exercer papel fundamental nas demonstrações de soma de quadrados.

No capitulo 2 a grande motivação é o Teorema de Minkowski. Começaremos contando um pouco sobre tal matemático e de sua importância e influência dentro da matemática e da física, na sequência será definido o reticulado e posteriormente o Teorema de Minkowski. Por fim, no último capítulo, retornaremos as aplicações citadas anteriormente e, fazendo uso do Teorema, buscaremos validar cada um dos três resultados.

Existem várias outras técnicas para o estudo de soma de quadrados, contudo, este trabalho limitar-se ao Teorema de Minkowski e aplicações.

Capítulo 1

Conceitos Iniciais

Neste primeiro capítulo serão apresentados alguns conceitos sobre o conjunto dos números inteiros, divisibilidade, números primos e também congruências módulo n. Essas ideias serão essenciais para o desenvolvimento do trabalho e das aplicações apresentadas no capítulo 3.

1.1 Os Números Inteiros

Primeiramente, vale destacar um subconjunto dos números inteiros, o conjunto dos números naturais

$$\mathbb{N} = (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, ...)$$

o conjunto dos números naturais pode ser caracterizado pelos *axiomas de Peano*:

1. Existe uma função injetiva $S : \mathbb{N} \longrightarrow \mathbb{N}$ onde a imagem $S(n)$ de cada número natural n chama-se *sucessor de* n; ou seja, todo número natural tem um sucessor, que ainda é um número natural; números diferentes têm sucessores diferentes.

2. Existe um único natural $1 \in \mathbb{N}$ tal que $1 \neq S(n)$ para todo $n \in \mathbb{N}$; ou seja, existe um único número natural 1 que ão é sucessor de nenhum outro.

3. Se um conjunto $X \subset \mathbb{N}$ é tal que $1 \in \mathbb{N}$ e $S(X) \subset X$ (isto é, $n \in \mathbb{N} \Rightarrow S(n) \in X$) então $X = \mathbb{N}$; ou seja, temos o que chamamos de Princípio da Indução Finita:
   Seja $P(n)$ uma propriedade sobre um número natural n maior ou igual a um número natural n_0 fixado. Se pudermos provar que valem as condições

Condição 1: $P(n_0)$ é verdadeira; ou seja, vale a propriedade para n_0;

Condição 2: É verdadeira a implicação $P(n) \longrightarrow P(n+1)$ para todo $n \geq n_0$

então, podemos afirmar que a propriedade $P(n)$ é verdadeira para todo $n \geq n_0$.

Exemplo 1.1.1. Demonstre que, para todo $n \in \mathbb{N}^* 1+2+3+4+...+n = \dfrac{n(n+1)}{2}$.

$$P(n) : 1 + 2 + 3 + 4 + ... + n = \frac{n(n+1)}{2}$$

$$P(1) : 1 = \frac{1 \cdot 2}{2} \checkmark$$

Seja $n \geq 1$ tal que $P(n)$ é verdade (*hipótese de indução*)

$$1 + 2 + 3 + ... + (n+1) = (1 + 2 + 3 + ... + n) + (n+1) =$$

$$= \frac{n(n+1)}{2} + (n+1) = \frac{n^2 + 3n + 2}{2} = \frac{(n+1)(n+2)}{2} = \frac{(n+1)((n+1)+1)}{2}$$

Logo, $P(n+1)$ é verdade e, pelo Princípio da Indução Finita, $P(n)$ é verdade para todo n diferente de zero.

Em $\mathbb{N}$, são definidas duas operações:

$$\text{(Soma)} + : \mathbb{N} \text{ x } \mathbb{N} \longrightarrow \mathbb{N}$$

$$(m, n) \longmapsto m + n$$

$$\text{(Multiplicação)} \cdot : \mathbb{N} \text{ x } \mathbb{N} \longrightarrow \mathbb{N}$$

$$(m, n) \longmapsto m \cdot n$$

para todo $m, n \in \mathbb{N}$ e, considerando o conjunto $\mathbb{N}^*$ o conjunto $\mathbb{N}$ retirando o zero, temos também, as seguintes propriedades:

1. (Boa definição) Para todo $a, b, a', b' \in \mathbb{N}$ com $a = a'$ e $b = b' \Longrightarrow a + b = a' + b'$;
2. (Comutatividade) Para todo $a, b \in \mathbb{N}, a + b = b + aea \cdot b = b \cdot a$;
3. (Associatividade) Para todo $a, b, c \in \mathbb{N}, (a+b)+c = a+(b+c)e(a \cdot b) \cdot c = azcdot(b \cdot c)$;
4. (Existência do elemento neutro) $\exists 0, 1 \in \mathbb{N}$ tais que para todo $a \in \mathbb{N} a + 0 = a$ e $a \cdot 1 = a$;
5. (Distributiva) Para todo $a, b, c \in \mathbb{N}, a \cdot (b + c) = a \cdot b + a \cdot c$;
6. (Soma e adição são fechadas) Para todo $a, b \in \mathbb{N}, a + b \in \mathbb{N}$ e $a \cdot b \in \mathbb{N}$;
7. (Tricotomia) Dados $a, b \in \mathbb{N}$, uma, e somente uma, das seguintes possibilidades é verificada

- $a = b$;
- $\exists c \in \mathbb{N}^*, b = a + c$, ou seja, $a < b$;
- $\exists c \in \mathbb{N}^*, a = b + c$, ou seja, $b < a$.

Nos números naturais vale também os seguintes princípios:

1. (Princípio da Boa Ordenação) Todo subconjunto não vazio do conjunto dos números naturais possui um *menor elemento*; ou seja, dado um subconjunto P de $\mathbb{N}$, não vazio, vai existir um elemento $p \in P$ tal que $p \leq a$, para todo $a \in P$.

   Exemplo 1.1.2. No conjunto $[7, 1)$ o menor elemento é o 7.

2. (Princípio da Casa dos Pombos Contínuo) O chamado princípio da casa dos pombos afirma que, se temos $wn + 1$ pombos e n casinhas, então existirá uma casinha que possuirá pelo menos $w + 1$ pombos. Além disso, é notório que se em todas as casas houvessem, no máximo, w pombos, então o número de pombos não poderia ultrapassar wn.

Porém, sejam a e b números naturais temos que a operação $b - a$ apenas é definida quando $b \geq a$ e, para que seja sempre definida essa operação, a solução encontrada foi ampliar o conjunto dos números naturais e, assim, criar um novo conjunto

$$\mathbb{Z} = (..., -4, -3, -2, -1, 0, 1, 2, 3, 4, ...)$$

chamado de *Conjunto dos Números Inteiros*. Em HEFEZ (2009), no conjunto $\mathbb{Z}$

> Os números à esquerda do zero são chamados de *números negativos* e os à direita são chamados de *números positivos*. Os pares de números 1 e -1, 2 e -2, 3 e -3 etc, são chamados de *números simétricos*. O elemento 0, que não é nem positivo, nem negativo, é o seu próprio simétrico.
>
> Em $\mathbb{Z}$ temos uma relação de ordem que estende a relação de ordem de $\mathbb{N}$, onde declaramos $a < b$ quando a se encontra à esquerda de b. Esta relação continua transitiva e total (i.e., satisfazendo à tricotomia). Os intervalos em $\mathbb{Z}$ são definidos de modo análogo aos intervalos de $\mathbb{N}$.
>
> Representamos por $-a$ o dimétrico de a, seja ele positivo, negativo ou nulo, temos sempre que

$$-(-a) = a$$

Temos também, em $\mathbb{Z}$, as operações de adição e multiplicação tais como foram definidas no conjunto dos números naturais.

1.2 Divisibilidade

Para quaisquer $d, a \in \mathbb{Z}$, dizemos que d é um divisor de a ou a é um múltiplo de d ou ainda que d divide a e representamos por

$$\mathrm{d|a}$$

se existir um número inteiro c com $a = cd$. Caso aconteça o contrário, escrevemos $d \nmid a$.

Exemplo 1.2.1. Seguem exemplos de números que são divisíveis, ou não:

1. $-7|14$
2. $14 \nmid -7$
3. $1|100$
4. $2|48$
5. $21 \nmid 3$
6. $0 \nmid n$, para todo $n \in \mathbb{Z}$

Vale destacar nesse momento algumas propriedades importantes da divisibilidade. Sejam $a, b, c, d \in \mathbb{Z}$, temos:

1. ("d divide") Se $d|a$ e $d|b$, então $d|ax + by$ para qualquer combinação linear $ax + by$ de a e b com coeficientes $x, y \in \mathbb{Z}$.
2. (Limitação) Se $d|a$, então $a = 0$ ou $|d| \leq |a|$.
3. (Transitividade) Se $a|b$ e $b|c$, então $a|c$.

Demonstração 1.2.1. (1) Se $d|a$ e $d|b$, então podemos escrever $a = dq_1$ e $b = dq_2$ com $q_1, q_2 \in \mathbb{Z}$, logo $ax + by = d(q_1x + q_2y)$. Como $q_1x + q_2y \in \mathbb{Z}$, temos $d|ax + by$.
(2) Suponha $d|a$ e $a \neq 0$. Neste caso, $a = dq$ com $q \neq 0$, assim $|q| \geq 1$ e $|a| = |d||q| \geq |d|$.
(3) Se $a|b$ e $b|c$, então existem $q_1, q_2 \in \mathbb{Z}$ tais que $b = aq_1$ e $c = bq_2$, logo $c = aq_1q_2$ e portanto $a|c$. $\square$

Uma das propriedades mais importantes dos números inteiros é o algoritmo da divisão; ou seja, a possibilidade de dividir um número por outro com resto pequeno.

Lema 1.2.1. *Dados $a, b \in \mathbb{Z}, a \geq 0 e\ b > 0$, existem q e r tais que $a = bq + r$ e $0 \leq r < b$.*

Demonstração 1.2.2. Seja o conjunto $S = \{a - (bx) : x \in \mathbb{Z} \text{ e } a - (bx) \geq 0\}$. Se $x = 0$ então $a - (bx) = a \geq 0$. Como $a|0$ e $a \in S$ temos que $S \neq \emptyset$. Pelo Princípio da Boa Ordem existe $r = minS$. Como $r \in S, r = a - (bq) \geq 0$, para algum $q \in \mathbb{Z}$ Temos que mostrar que $r < b$. Se $r \geq b$ teríamos

$$a - b \cdot (q + 1) = a - b \cdot q - b = (a - (b \cdot q)) - b = r - b \geq 0$$

Logo, $a - b \cdot (q + 1) \in S$. Mas $a - b \cdot (q + 1) = r - b < r = minS$, que é um absurdo. Assim, $r < b$. $\square$

Teorema 1.2.2 (Divisão Euclidiana)**.** *Para quaisquer inteiros a e b inteiros, com $b \neq 0$, existe um único par (q, r) de inteiros tais que $a = b \cdot q + r$ onde $0 \leq r < |b|$. Os números q e r são chamados, respectivamente, de quociente e resto da divisão de a por b.*

Demonstração 1.2.3. Separando em casos:
Caso 1: $b > 0$.
Quando $a \geq 0$ o Lema 1.2.1 garante a ocorrência do Teorema.
Quando $a < 0$ podemos determinar, pelo Lema 1.2.1, q_1 e r_1, tais que

$$|a| = b \cdot q_1 + r_1, 0 \leq r_1 < b.$$

Se $r_1 = 0$ temos

$$-|a| = a = b \cdot (-q_1) + 0,$$

logo, $q = -q_1$ e $r = 0$ satisfazem as condições do Teorema. Se $r > 0$, temos

$$a = -|a| = b \cdot (-q_1) - r_1 = b \cdot (-q_1) - b + b - r_1 = b \cdot (-q_1 - 1) + (b - r_1).$$

Como $0 < b - r_1 < b$ então $q = -q_1$ e $r = b - r_1$, satisfazem as condições do Teorema.

Caso 2: $b < 0$.
Qualquer que seja a podemos determinar q_1 e r_1 tais que

$$a = |b| \cdot q_1 + r_1 \leq r_1 < |b|.$$

Se $b > 0$ então $|b| = -b$. Dessa forma,

$$a = |b| \cdot q_1 + r_1 = (-b) \cdot q_1 + r_1 = b \cdot (-q_1) + r_1.$$

Então $q = -q_1$ e $r = r_1$ satisfazem as condições do Teorema.

Agora, provando a unicidade, de fato $qb+r = a = q_1b+r_1$. Suponha que $r_1 \geq r$, dessa forma

$$(q - q_1) \cdot b = r_1 - r.$$

Como $|b| > r_1$ temos $r_1 - r < |b|$. Por outro lado,

$$(q - q_1)\cdot = r_1 - r < |b| \Rightarrow 0 \leq |q - q_1| \cdot |b| < |b|.$$

Como $|b| > 0$ temos que $0 \leq |q - q_1| < 1$. Entre 0 e 1 não há números inteiros, logo,

$$|q - q_1| = 0 \Rightarrow q = q_1$$

Assim,

$$q \cdot b + r = q_1 \cdot b + r_1 \Rightarrow r = r_1.$$

□

Exemplo 1.2.2. $a = b \cdot q + r, 0 \leq r < |b|$

1. $10 = 3 \cdot 3 + 1$
2. $11 = 3 \cdot 3 + 2$
3. $12 = 3 \cdot 4 + 0$
4. $13 = 3 \cdot 4 + 1$
5. $14 = 3 \cdot 4 + 2$
6. $15 = 3 \cdot 5 + 0$
7. $-6 = 2 \cdot (-3)$
8. $-7 = 2 \cdot (-4) + 1$

Quando $r = 0$, diremos que o b é divisível por a, ou que a é um divisor de b e a definição que segue é extremamente importante em vários campos da matemática e também em construções futuras nesse trabalho.

Definição 1.2.1 (Máximo Divisor Comum)**.** Se $u_1, u_2, ..., u_n$ são números naturais não todos nulos, então os elementos do conjunto $D(u_1) \cap D(u_2) \cap ... \cap D(u_n)$ são os divisores comuns de $u_1, u_2, ..., u_n$. Em particular

$$mdc(u_1, u_2, ..., u_n) = max(D(u_1) \cap D(u_2) \cap ... \cap D(u_n)),$$

onde $max(D(u_1) \cap D(u_2) \cap ... \cap D(u_n))$ denta o maior elemento de $D(u_1) \cap D(u_2) \cap ... \cap D(u_n)$; ou seja, o maior divisor comum de $u_1, u_2, ..., u_n$.

1.3 Números primos

O conjunto dos números primos é uma reunião de números especiais que desempenham papel fundamental em diversas teorias matemáticas, veremos nessa seção o que são números primos, uma maneira prática de verificar a primalidade de um número, a sua infinidade e o Teorema Fundamental da Aritmética.

Definição 1.3.1. Um número inteiro não negativo, diferente de 0 e de 1, que é múltiplo apenas de 1 e de sí próprio é chamado de *número primo.*

Definição 1.3.2. Um número inteiro não negativo e diferente de 0 e 1 que não é primo é chamado de *número composto.*

Teorema 1.3.1 (Teorema Fundamental da Aritmética)**.** *Seja $n \geq 2$ um número natural. Podemos escrever n de uma única forma como um produto*

$$n = p_1 \cdot ... \cdot p_m$$

onde $m \geq 1$ é um natural e $p_1 \leq ... \leq p_m$ são primos.

Segue a demonstração apresentada na referência 11 deste trabalho:

Demonstração 1.3.1. O autor mostrou a existência da fatoração de n em primos por indução. S e n é primo não há o que provar (escrevemos $m = 1, p_1 = n$). Se n é composto podemos escrever $n = ab, a, b \in \mathbb{N}, 1 < a < n, 1 < b < n$. Por hipótese de indução,a e b de decompõem como produto de primos. Juntando as fatorações de a e b (e reordenando os fatores) obtemos uma fatoração de n. Mostrando agora a unicidade. Suponha por absurdo que n possui duas fatorações diferentes

$$n = p_1 \cdot ... \cdot p_m = q_1 \cdot ... \cdot q_{m'}$$

com $p_1 \leq ... \leq p_m, q_1 \leq ... \leq q_{m'}$ e que n é mínimo com tal propriedade. Como $p_1 | q_1 \cdot ... \cdot q_{m'}$ temos $p_1 | q_i$ para algum valor de i pelo seguinte corolário:

Corolário 1.3.2. *Seja p um número primo e sejam $a_1, ..., a_m \in \mathbb{Z}. Sep | a_1 \cdot ... \cdot a_m$ então $p | a_i$ para algum $i, 1 \leq i \leq m$.*

Logo, como q_1 é primo, $p_1 = q_i$ e $p_1 \geq q_1$. Analogamente temos $q_1 \leq p_1$, donde $p_1 = q_1$. Mas

$$n/p_1 = p_2 \cdot ... \cdot p_m = q_2 \cdot ... \cdot q_{m'}$$

admite uma única fatoração, pela minimalidade de n, donde $m = m'$ e $p_i = q_i$ para todo i, o que contradiz o fato de n ter duas fatorações. □

Exemplo 1.3.1. Os números $2, 3, 5, 7, 53$ são primos, enquanto os números $4, 10, 40, 52$ são compostos, pois são múltiplos de 2. Geralmente, todos os números pares, exceto o 2 são compostos, uma vez que são múltiplos de 2.

Neste sentido, os números 0 e 1 não se encaixam em nenhuma das duas definições anteriores, assim, não são primos e nem compostos, classificação que vale aos demais inteiros não negativos.

Um método bastante antigo para definir a primalidade de um número é o Crivo de Erastótenes (matemático grego 276 a.C. - 194 a.C.). A palavra *crivo* significa peneira e o método consiste em peneirar os números naturais (ou inteiros não negativos) em um intervalo fechado, começando no primeiro número primo, 2, até um número n, incluindo ambos, retirando deste intervalo os números que não são primos; ou seja, retirando os números compostos.

Lema 1.3.3 (Crivo de Erastótenes)**.** *Se um número natural $a > 1$ é composto, então ele é múltiplo de algum primo p tal que $p^2 \leq a$. Equivalentemente, é primo todo número a que não é múltiplo de nenhum número primo p tal que $p^2 \leq a$.*

O livro de Abramo Hefez, Iniciação a Aritmética (2009), apresenta a seguinte prova para o lema anterior:

> De fato, se a é composto e p é o menor número primo do qual a é múltiplo, então $a = p \cdot b$, onde p e b são menores do que a. De todo modo, sendo b primo ou composto, ele será múltiplo de um número primo q. Como a é múltiplo de b e b é múltiplo de q, temos que a também é múltiplo de q e sendo p o menor primo do qual a é múltiplo, temos $p \leq q$. Logo, $p^2 \leq p \cdot q \leq a$.

Exemplo 1.3.2. Para mostrar que o número $385 (= 5 \cdot 7 \cdot 11)$ é composto, precisamos testar se o mesmo é múltiplo de algum dos primos $p = 2, 3, 5, 7, 11, 13$ ou 19, já que o próximo primo 23 é tal que $23^2 = 529 > 385$.

Outra questão relativa aos números primos que é interessante ressaltar é a sua infinidade.

Teorema 1.3.4 (Euclides)**.** *Existem infinitos primos.*

Será apresentada uma demonstração baseada no que foi atribuído a Euclides (século III a.C.), uma ideia com mais de 2000 anos e que ainda é base para muitas outras provas.

Demonstração 1.3.2. Suponha por absurdo que $p_1, p_2, ..., p_m$ fossem todos primos. O número $A = p_1p_2...p_m + 1 > 1$ não seria divisível por nenhum primo p_i, o que contradiz o Teorema Fundamental da Aritmética. □

1.4 Congruência módulo n

Definição 1.4.1. Seja dado um número inteiro $n > 1$. Dois números inteiros a e b são *congruentes módulo* n se a e b possuírem o mesmo resto quando divididos por n. Simbolizaremos por

$$a \equiv b \text{ (mod n)}.$$

Se a e b não forem congruentes módulo n representaremos por

$$a \not\equiv b \text{ (mod n)}.$$

Segue algumas propriedades das congruências e suas demonstrações, presentes na referência 11 deste trabalho.

Proposição 1.4.1. *Para quaisquer $a, b, c, d, n \in \mathbb{Z}$ temos:*

1. *(Reflexividade) $a \equiv a$ (mod n);*
2. *(Simetria) se $a \equiv b$ (mod n), então $b \equiv a$ (mod n);*
3. *(Transitividade) se $a \equiv b$ (mod n) e $b \equiv c$ (mod n), então $a \equiv c$ (mod n);*
4. *(Compatibilidade com a soma e diferença) Podemos somar e subtrair "membro a membro":*

$$\begin{cases} a \equiv b(modn) \\ c \equiv d(modn) \end{cases} \Rightarrow \begin{cases} a + c \equiv b + d(modn) \\ a - c \equiv b - d(modn) \end{cases}$$

   Em particular, se $a \equiv b$ (mod n), então $ka \equiv kb$ (mod n) para todo $k \in \mathbb{Z}$;

5. *(Compatibilidade com o produto) Podemos multiplicar "membro a membro":*

$$\begin{cases} a \equiv b(modn) \\ c \equiv d(modn) \end{cases} \Rightarrow ac \equiv bd(modn)$$

Em particular, se $a \equiv b$ *(mod n), então* $a^k \equiv b^k$ *(mod n) para todo* $k \in \mathbb{N}$*;*

6. *(Cancelamento) Se* $mdc(c, n) = 1$ *então*

$$ac \equiv bc \text{ (mod } n) \Leftrightarrow a \equiv b \text{ (mod } n).$$

Demonstração 1.4.1. Para o item (1) basta observar que $n|a-a = 0$. Em (2), se $n|a-b$, então $n|-(a-b) \Leftrightarrow n|b-a$. Em (3), se $n|a-b$ e $n|b-c$, então $n|(a-b)+(b-c) \Leftrightarrow n|a-c$. Em (4) e (5), se $n|a-b$ e $n|c-d$, então $n|(a-b)+(c-d) \Leftrightarrow n|(a+c)-(b+d)$, $n|(a-b)-(c-d) \Leftrightarrow n|(a-c)-(b-d)$ e $n|(a-b)c+(c-d)b \Leftrightarrow n|ac-bd$. Finalmente, como $mdc(c, n) = 1$ temos que $n|ac-bc \Leftrightarrow n|(a-b)c \Leftrightarrow n|a-b$ pela proposição a seguir. □

Proposição 1.4.2. *Se* $mdc(a, b) = 1$ *e* $a|bc$*, então* $a|c$*.*

Demonstração 1.4.2. Como $mdc(a, b) = 1$, existem $x, y \in \mathbb{Z}$ tais que $ax + by = 1 \Rightarrow a \cdot cx + (bc) \cdot y = c$. Do fato de a dividir cada termo do lado esquerdo, temos que $a|c$. □

Exemplo 1.4.1. Congruências módulo n:

1. $10 \equiv 7$ (mod 3), pois os restos da divisão de 10 e de 7 por 3 são iguais a 1;
2. $12 \equiv 17$ (mod 5), pois os restos da divisão de 12 e de 17 por 5 são iguais a 2;
3. $1 \equiv 11$ (mod 10), pois os restos da divisão de 1 e de 11 por 10 são iguais a 1;
4. $27 \not\equiv 15$ (mod 4), pois os restos da divisão de 27 por 4 é 3 e o da divisão de 15 por 4 é igual a 1;

Uma maneira mais prática de verificar a congruência sem necessariamente efetuar a divisão é o seguinte resultado:

Proposição 1.4.3. *Tem-se que* $a \equiv b$ *(mod n) se e somente se n divide* $b - a$*.*

Demonstração 1.4.3. Pelo algorítimo da divisão, temos que

$$a = nq_1 + r_1 \text{ e } b = nq_2 + r_2$$

onde $0 \leq r_1 < m$ e $0 \leq r_2 < m$. Supondo que $r_1 \leq r_2$, podemos escrever

$$b - a = n(q_2 - q_1) + r_2 - r_1.$$

Logo, n divide $b - a$ se, e somente se, n divide $r_2 - r_1$. Pelo fato de $0 \leq r_2 - r_1 < n$, segue que n divide $b - a$ se e somente se $r_2 - r_1 = 0$, ou seja, se e somente se $r_2 = r_1$. $\square$

Capítulo 2

Teorema de Minkowski

2.1 História

Hermann Minkowski (1864 − 1909) foi um matemático alemão que inicialmente estudou as formas quádricas, que são polinômios quadráticos homogêneos de n variáveis. Um de seus colegas de graduação foi o também matemático alemão David Hilbert (1862 − 1943) que, em seu registro de morte, deixou a seguinte mensagem

> Seit meiner Studienzeit war mir Minkowski der beste und zuverlässigste Freund, der an mir hing mit der ganzen ihm eigenen Tiefe und Treue. Unsere Wissenschaft, die uns das liebste war, hatte uns zusammengeführt; sie erschien uns wie ein blühender Garten. Gern suchten wir dort auch verborgene Pfade auf und entdeckten manche neue, uns schön dünkende Aussicht, und wenn der eine dem andern sie zeigte und wir sie gemeinsam bewunderten, war unsere Freude vollkommen. Er war mir ein Geschenk des Himmels, wie es nur selten jemand zuteil wird, und ich muss dankbar sein, dass ich es so lange besaß. Jäh hat ihn der Tod von unserer Seite gerissen. Was uns aber der Tod nicht nehmen kann, das ist sein edles Bild in unserem Herzen und das Bewusstsein, dass sein Geist in uns fortwirkt.

que traduzida ao portugês diz: "Desde minha época de estudante Minkowski foi meu melhor e mais confiável amigo que me apoiou com toda a profundidade e lealdade que era

tão característica dele. Nossa ciência, que ele amava acima de tudo, nos uniu, e que nos parecia um jardim cheio de flores. Nele, nos divertimos procurando caminhos escondidos e descobrimos muitas vezes uma nova perspectiva que recorria ao nosso senso de beleza, e quando um de nós mostrava para o outro e nos maravilhávamos sobre isso juntos, nossa alegria era completa. Ele foi para mim um dom raro dos céus e eu devo ser grato por ter possuído esse dom por tanto tempo. Agora, a morte, de repente, rasgou-o do nosso meio. No entanto, o que a morte não pode levar é a sua imagem nobre em nossos corações, além dos conhecimentos que seu espírito, dentro de nós, continua ser ativo."

Outra curiosidade sobre a vida de Minkowski é que ele foi professor universitário bastante influente na carreira do físico teórico Albert Einstein $(1879-1955)$ e que também se interessou pela teoria da relatividade, vindo a formular o Espaço de Minkowski, que é a configuração matemática na qual a teoria da relatividade restrita de Einstein é mais comumente formulada.

A *Geometria dos Números* também é uma criação deste matemático.

2.2 Reticulados e Elemento de Área

Nesta seção definiremos o que é um reticulado e o elemento de área associado ao mesmo, além de exemplos.

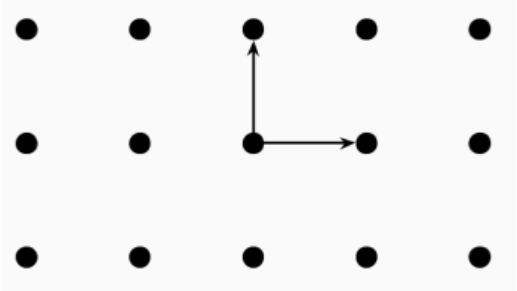
Definição 2.2.1. Um reticulado no $\mathbb{R}^n$ é um conjunto $\Lambda \subset \mathbb{R}^n$ gerado por todas as combinações $\mathbb{Z}$-lineares de n vetores linearmente independentes, isto é,

$$\Lambda = \mathbb{Z}w_1 + w_2 + ... + \mathbb{Z}w_n = \{\alpha_1 w_1 + \alpha_2 w_2 + ... + \alpha_n w_n; \alpha_i \in \mathbb{Z}\}$$

para alguma base $\omega = w_1, w_2, ..., w_n$ de $\mathbb{R}^n$.; ou seja, dada uma base ω do $\mathbb{R}^n$ o reticulado associado a essa base é o conjunto dos pontos obtidos pelas combinações lineares de coeficientes inteiros dos vetores $w_i \in \omega$.

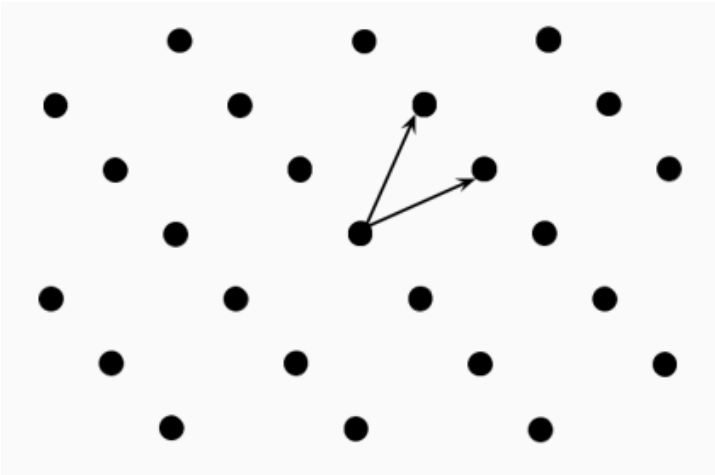
Exemplo 2.2.1. Se $\beta_1 = (1,0),(0,1)$ então o reticulado Λ_1 associado é dado por:

$$\Lambda_1 = \{(x,y) \in \mathbb{R}^2; x,y \in \mathbb{Z}\} = \mathbb{Z}^2$$



Exemplo 2.2.2. Se $\beta_2 = (\frac{1}{2},1),(1,\frac{1}{2})$ então o reticulado Λ_2 associado é dado por:

$$\Lambda_2 = \{x(\tfrac{1}{2},1) + y(1,\tfrac{1}{2}) \in \mathbb{R}^2; x,y \in \mathbb{Z}\}$$

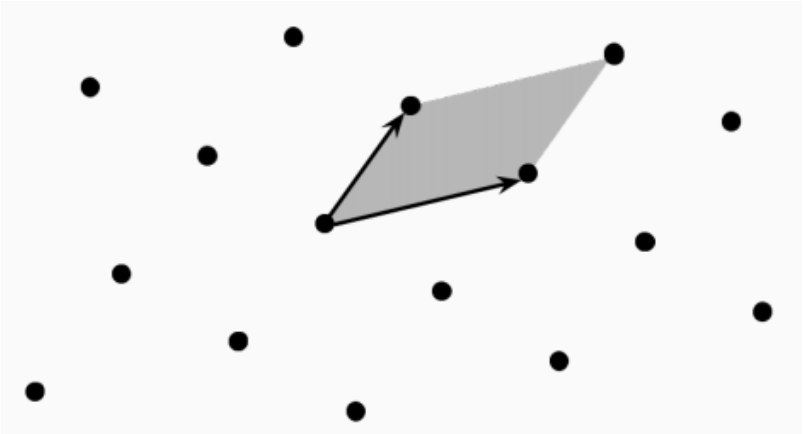


Definição 2.2.2. Seja Λ um reticulado no $\mathbb{R}^n$, definiremos o volume deste como $vol(\Lambda) = |det(w_1, w_2, ..., w_n)|$. chamado de *paralelogramo fundamental* associado à base $w_1, w_2, ..., w_n$.

No $\mathbb{R}^2$, este $vol(\Lambda)$ será chamado de *elemento de área do reticulado* e seu cálculo permanecerá associado ao valor do determinante da matriz que possui como linhas os elementos da base.

Exemplo 2.2.3. Seja a base $\beta = (a, b), (c, d)$, então, o elemento de área do reticulado Λ associado é dado por:

$$\triangle = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = |ad - bc|$$



O cálculo do $vol(\Lambda)$ pode ser entendido como uma generalização do produto misto.

Definição 2.2.3. Dados os vetores $w_1, w_2 e w_3 \in \mathbb{R}^3$, definiremos o produto misto como o número real dado por $w_1 \bullet (w_2 \times w_3)$. Onde $\bullet$ representa o produto interno ou escalar e $\times$ é o produto vetorial. Seja $w_1 = (x_1, y_1, z_1), w_2 = (x_2, y_2, z_2)$ e $w_3 = (x_3, y_{3,3})$, temos que:

$$w_1 \bullet (w_2 \times w_3) = \begin{vmatrix} x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \\ x_3 & y_3 & z_3 \end{vmatrix}$$

O que se deve pelo fato de que:

$$w_1 \bullet (w_2 \times w_3) = (x_1, y_1, z_1) \bullet (y_2 z_3 - y_3 z_2, -x_2 z_3 + x_3 z_2, x_2 y_3 - x_3 y_2) =$$

$$x_1 y_2 z_3 - x_1 y_3 z_2 - x_2 y_1 z_3 + x_3 y_1 z_2 + x_2 y_3 z_1 - x_3 y_2 z_1 = \begin{vmatrix} x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \\ x_3 & y_3 & z_3 \end{vmatrix}$$

O significado do $vol(\Lambda)$ é ainda mais interessante quando pensamos na interpretação geométrica do produto misto pois, podemos pensar no mesmo sendo igual ao módulo do volume de um paralelepípedo de arestas determinadas pelos vetores w_1, w_2 e w_3.

Definição 2.2.4. Dado um reticulado $\Lambda \subset \mathbb{R}^n$, escrevemos

$$a \equiv b \pmod{\Lambda} \Leftrightarrow a - b \in \Lambda \ (a, b \in \mathbb{R}^n)$$

O que define uma relação de equivalência de $\mathbb{R}^n$ e um conjunto dos representantes do quociente $\mathbb{R}^n/\Lambda$ é dado justamente pelo paralelogramo fundamental.

2.3 Teorema de Minkovski

Em 1889, o matemático alemão Hermann Minkowski provou o teorema que leva seu sobrenome, o que é o marco da formulação de um ramo da Teoria dos Números, a Geometria dos Números.

Antes do Teorema de Minkowski, vamos à algumas definições que se fazem importantes nesse momento. As seguintes definições sobre conjunto mensuráveis são apresentadas no sentido de Camille Jordan (1838 - 1922), matemático francês com trabalhos conhecidos nas áreas de teoria dos grupos e de análise.

Definição 2.3.1. Chama-se retângulo n-dimensional, n-retângulo ou simplesmente retângulo qualquer subconjunto de $\mathbb{R}^n$ que se possa representar sob a forma de um produto cartesiano de n intervalos fechados e limitados. Dados dois pontos, $a = (a_1, a_2, ..., a_n), b = (b_1, b_2, ..., b_n) \in \mathbb{R}^n$ que verifiquem $-\infty < a_i \leq b_i < +\infty, i = 1, 2, ..., n$, indica-se por $E(a, b)$ o retângulo

$$E(a, b) = \{(x_1, x_2, ..., x_n) \in \mathbb{R}^n : a_i \leq x_i \leq b_i, i = 1, 2, ..., n\}$$

Um 1-retângulo é um intervalo limitado e fechado. Um 2-retângulo é um retângulo no sentido comum do termo, isto é, a sua fronteira é um polígono de quatro lados paralelos dois a dois e lados adjacentes que formam ângulos retos. Um 3-retângulo é um paralelipípedo retângulo, e assim por diante.

Definição 2.3.2. Dois n-retângulos, $E_1, E_2 \subset \mathbb{R}^n$, são não sobrepostos se

$$int(E_1) \cap int(E_2) = \emptyset.$$

Definição 2.3.3 (Conjunto mensurável)**.** Um conjunto $A \subset \mathbb{R}^n$ diz-se *mensurável no sentido de Jordan* se para cada $\varepsilon > 0$ existirem famílias de retângulos não sobrepostos, $\{\underline{E}_i, i = 1, 2, 3, ..., k\}, \{\overline{E}_i, i = 1, 2, 3, .., m\}$ tais que

$$\bigcup_{i=1}^{k} \underline{E}_i \subset A \subset \bigcup_{i=1}^{m} \overline{E}_i$$

Definição 2.3.4 (Conjunto convexo)**.** Um conjunto C é dito convexo se dados dois pontos quaisquer do conjunto, o segmento de reta entre esses dois pontos estiver em C, ou seja, para quaisquer $x_1, x_2 \in C$ e um escalar $\alpha \in [0, 1]$,

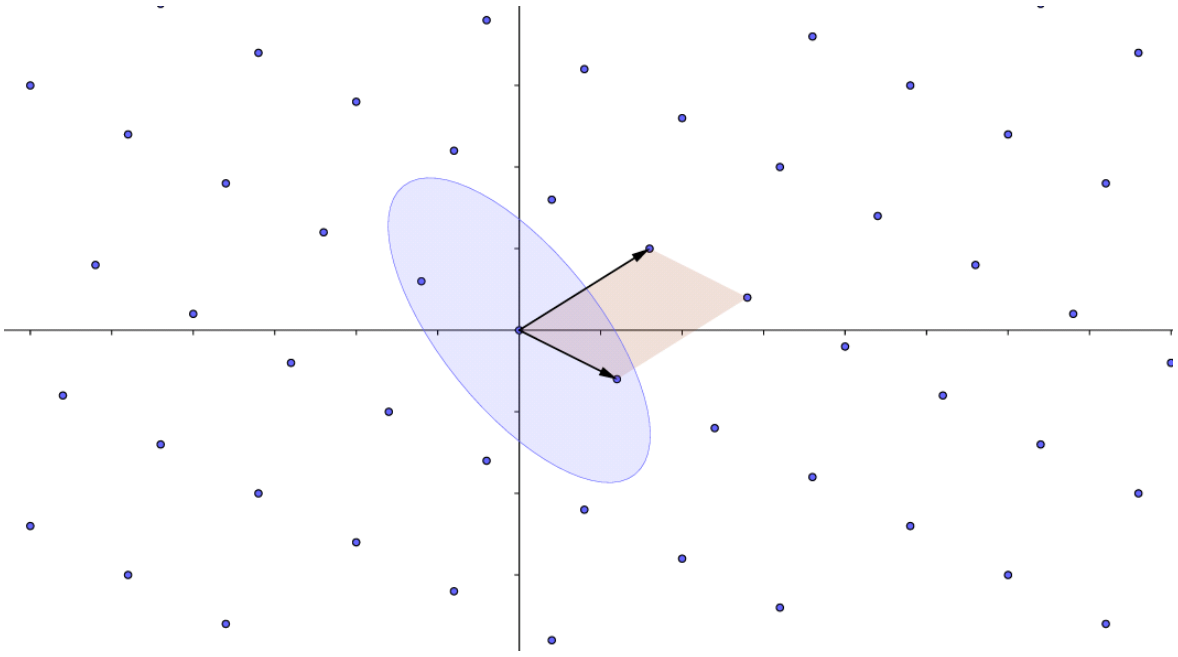
$$\alpha x_1 + (1 - \alpha)x_2 \in C.$$

Teorema 2.3.1 (Teorema de Minkowski)**.** *Seja $\Lambda \subset \mathbb{R}^n$ um reticulado e $V \subset \mathbb{R}^n$ é um subconjunto mensurável tal que*

1. *V e simétrico com relação à origem (i.e. $v \in V \Longrightarrow -v \in V$);*
2. *V é convexo;*
3. *$vol(V) > 2^n vol(\Lambda)$.*

Então existe um ponto em $\vee \cap \Lambda$ diferente da origem.

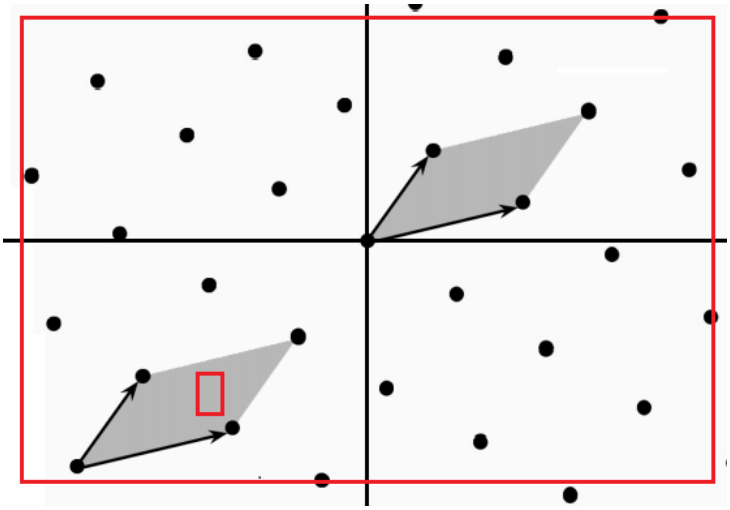
Geometricamente temos o seguinte exemplos, onde o subconjunto convexo V é a parte representada em azul e o $vol(\Lambda)$ é a parte laranja.



Demonstração 2.3.1. Seja P o paralelogramo fundamental determinado por uma base $w_1, w_2, ..., w_n$ do reticulado Λ e seja $\frac{1}{2}V = \left\{\frac{v}{2} | v \in V\right\}$, onde V um subconjunto mensurável.

Considerando o quociente $\frac{1}{2}V/\Lambda$, podemos particionar $\frac{1}{2}V$ em uma quantidade *enumerável* de subconjuntos mensuráveis U_i de maneira a existir τ_i do reticulado Λ com $\tau_i + U_i$ dentro do paralelogramo fundamental P.

Ilustrando o que foi descrito acima, temos na seguinte imagem um reticulado genérico e em vermelho a borda de um subconjunto mensurável que pode ser dividido em retângulos (um representante U_i é o retângulo pequeno desenhado) de maneira que, dado um ponto τ_i no reticulado, transladando esse Λ, temos U_i de maneira que $\tau_i + U_1 \in vol(\Lambda)$



Como

$$vol(\tfrac{1}{2}V) = \tfrac{1}{2^n} vol(V) > \tfrac{1}{2^n} \cdot 2^n vol(\Lambda) = vol(\Lambda) = vol(P),$$

pelo princípio da casa dos pombos existem $i \neq j$ tais que $(\tau_i + \frac{1}{2}U_i) \cap (\tau_j + \frac{1}{2}U_j)$ é diferente do vazio, isto é, existem dois pontos distintos v e $w \in V$ tais que

$$\tfrac{v}{2} \equiv \tfrac{w}{2} (mod \Lambda) \iff \tfrac{v}{2} - \tfrac{w}{2} = \frac{v-w}{2} \in \Lambda \text{ com } v - w \neq 0.$$

Mas $\frac{v-w}{2}$ também pertence ao subconjunto mensurável V, pois, como V é simétrico em relação a origem, $w \in V \implies -w \in V$ e, como V é convexo $v, -w \in V \implies \frac{v-w}{2} \in V$. Portanto, $\frac{v-w}{2} \neq 0$ e pertence ao reticulado Λ e também ao subconjunto mensurável V.

□

Capítulo 3

Aplicações

Neste capítulo serão apresentadas algumas aplicações do Teorema de Minkowski relativas à algumas técnicas geométricas para o estudo de soma de quadrados.

3.1 Soma de Quadrados

O livro *Teoria dos Números: um passeio com primos e outros números familiares pelo mundo inteiro* (referência [11]) apresenta os seguintes resultados que caracterizam números primos através de soma de quadrados.

Teorema 3.1.1. *Todo primo p da forma $4k+1$ é soma de dois quadrados.*

Demonstração 3.1.1. Temos que existe um inteiro x tal que $x^2 \equiv -1 \pmod{p}$ pois $(\frac{-1}{p}) = (-1)^{(p-1)/2} = 1$. Considere o reticulado em $\mathbb{R}^2$

$$\Lambda := \{(a,b) \in \mathbb{Z}^2 | a \equiv bx \pmod{p}\}.$$

Temos que o volume de Λ é p (fixado b, a é determinado módulo p, logo Λ contém um em cada p pontos de $\mathbb{Z}^2$). Portanto, pelo Teorema de Minkowski, existe um ponto $(a,b) \neq (0,0)$ em Λ que pertence ao círculo com centro na origem e cujo raio é $\sqrt{3p/2}$ pois a área deste círculo é $3p\pi/2 > 2^2 p = 2^2 vol(\Lambda)$. Assim, $0 < a^2 + b^2 < 3p/2$ e

$$a^2 + b^2 \equiv b^2(x^2+1) \pmod{p} \iff a^2 + b^2 \equiv 0 \pmod{p}$$

Ou seja, $a^2 + b^2 = p$.

Outro resultado importante nos diz que todo número primo pode ser escrito como soma de quatro quadrados.

Lema 3.1.2. *Para todo primo existem inteiros a, b tais que $a^2 + b^2 + 1 = mk$, para algum $k \in \mathbb{Z}$.*

De fato, seja m um número primo p e considere s conjuntos

$$A = \{a^2 | a = 0, 1, 2, ..., \frac{p-1}{2}\}$$
$$B = \{-b^2 - 1 | b = 0, 1, 2, ..., \frac{p-1}{2}\}$$

Desta forma, nenhum elemento de A é côngruo a outro elemento de A, valendo o mesmo para o conjunto B. Então, pelo princípio da casa dos pombos, como $|A| + |B| = p + 1$ e só existem p classes em $\mathbb{Z}_p$ temos ue um elemento de A é côngruo a um de B.

Teorema 3.1.3. *Todo primo p é soma de quatro quadrados.*

Demonstração 3.1.2. Pelo lema anterior, temos que existem inteiros u, v tais que $u^2 + v^2 + 1 = 0$ (mod p). Considere o reticulado em $\mathbb{R}^4$ dado por

$$\Lambda := \{(a, b, c, d) \in \mathbb{Z}^4 | a \equiv cu + dv \text{ (mod p) e } b \equiv cv - du \text{ (mod p)}\}$$

Temos que Λ tem volume p^2 (fixados c e d, a e b ficam determinados módulo p, logo Λ contém uma a cada p^2 pontos em $\mathbb{Z}^4$). A esfera de raio r em $\mathbb{R}^4$ tem volume $\pi^2 r^4/2$. Tomando $r = \sqrt{19p/10}$, como $\pi^2(\frac{19p}{10})^2/2 > 2^4 vol(\Lambda) = 16p^2$ pelo Teorema de Minkowski existe um ponto $(a, b, c, d) \in \Lambda$ tal que $0 < a^2 + b^2 + c^2 + d^2 \leq 19p/10 < 2p$. Porém

$$a^2 + b^2 + c^2 + d^2 \equiv (c^2 + d^2)(u^2 + v^2 + 1) \text{ (mod p)}$$
$$\iff a^2 + b^2 + c^2 + d^2 \equiv 0 \text{ (mod p)}$$

Logo $a^2 + b^2 + c^2 + d^2 = p$.

3.2 Teorema de Lagrange da Soma de Quadrados

Teorema 3.2.1. *Todo inteiro m não negativo pode ser escrito como a soma de quatro quadrados.*

Demonstração 3.2.1. Dividiremos em dois casos, m ímpar ou par.

Se m é ímpar:

Pelo Lema 3.1.2, encontramos $a, b \in \mathbb{Z}$ tais que $a^2 + b^2 + 1 = mk$ para algum $k \in \mathbb{Z}$. Montaremos então o seguinte reticulado:

$$\Lambda := \begin{cases} X = mx + az + bw \\ Y = my + bz - aw \\ Z = z \\ W = w \end{cases} , x, y, z \in \mathbb{Z}$$

Que tem elemento de área $\triangle = m^2$.

Vamos tentar obter no reticulado Λ um ponto $p = (X, Y, Z, W)$ tal que $X^2 + Y^2 + Z^2 + W^2 = m$ usando Minkowski. Primeiro calculamos $X^2 + Y^2 + Z^2 + W^2$ e obtemos:

$$m(mx^2 + my^2 - 2axy - 2ayw + 2bxy + 2byz) + (a^2 + b^2 + 1)(w^2 + y^2),$$

logo, $X^2 + Y^2 + Z^2 + W^2 = mk$ para algum $k \in \mathbb{Z}$. Podemos buscar um ponto do reticulado tal que $X^2 + Y^2 + Z^2 + W^2 < 2m$, encontraríamos então um ponto que satisfaz $X^2 + Y^2 + Z^2 + W^2 < m$. Note que $X^2 + Y^2 + Z^2 + W^2 < 2m$ define uma esfera em $\mathbb{R}^4$ de raio $\sqrt{2m}$, seu volume, que é calculado através de um processo que envolve integrais e que não foi abordado neste trabalho, é dado por:

$$V = \frac{1}{2}\pi^2 r^4 = \frac{1}{2}\pi^2 (2m)^4$$

Por Minkowski precisamos que $V \geq 2^4 \triangle = 2^4 m^2$, que é uma informação válida. Logo existe um ponto inteiro na "casca"sa esfera 4D de raio $\sqrt{m}$. Se m é par basta observar que $m = 2m'$, então se

$$m' = X^2 + Y^2 + Z^2 + W^2 \text{ com } X, Y, Z, W \in \mathbb{Z}$$

podemos escrever

$$m = (X + Y)^2 + (X - Y)^2 + (Z + W)^2 + (Z - W)^2$$

Considerações Finais

Neste trabalho foram estudados alguns tópicos vistos durante a graduação, como os conjuntos de números naturais e inteiros, a divisibilidade, os números primos e a congruência modulo n, e teve como motivação o Teorema de Minkowski, um fato novo e um passo a mais dentro da Teoria dos Números.

De modo geral, apresentamos neste trabalho um estudo sobre as implicações do Teorema de Minkowski para soma de quadrados buscando, através das bibliografias, reunir de uma maneira mais acessível os conceitos e definições necessárias para a compreensão dos resultados.

Por fim, o que foi abordado no presente trabalho pode vir a servir como motivação para um estudo mais aprofundado e detalhado da Teoria dos Números e mais especificamente da Geometria dos Números, dando subsídio para o pensamento relativo a padrões e generalizações nesta área da Matemática, principalmente dentro de uma graduação.

Referências Bibliográficas

[1] C. D. Olds, Anneli Lax and Giuliana P. Davidoff, **The Geometry of Numbers**, volume 41 of Annelli Lax New Mathematical Library, Mathematical Association of America, Washington, DC, 2000.

[2] G. H. Hardy and E. M. Wright, **An introduction to the theory of numbers**, The Clarendon Press Oxford University Press, New York, fifth edition, 1979.

[3] J. W. S. Cassels, **An introduction to the geometry of numbers**, Classics in Mathematics, Springer-Verlag, Berlin, 1997.

[4] F. Martinez, C. G. Moreira, N. Saldanha e E. Tengan, **Teoria dos Números: um passeio com primos e outros números familiares pelo mundo**, 4º edição, IMPA, 2015.

[5] A. Hefez, **Elementos de aritmética**, Sociedade Brasileira de Matemática, 2006.

[6] A. A. Giola, **The theory of numbers: an introduction**, Courier Corporation, 2001

[7] A. J. Ferrari, **Reticulados algébricos via corpos abelianos**, Unesp, 2008.

[8] F. T. Orihuela, **O Teorema de Minkowski**, IMECC, 2016.

[9] A. C. Ribeiro, **Reticulados sobre Corpos de Números**. Dissertação de Mestrado, Ibilce-Unesp, São José do Rio Preto-SP, 2003.

[10] H. Minkowski, **Geometrie der Zahlen**. Leipzig: Teubner, 1896.

[11] Martinez, F. B., Moreira, C. G., Saldanha, N., Tengan, E.. **Teoria dos Números: um passeio com primos e outros números familiares pelo mundo inteiro.** Coleção Projeto Euclides, IMPA, 2013.

[12] Manuel Guerra, **Integração em** $\mathbb{R}^n$. Análise Matemática III, 2004.

[13] Caixeta, S. B., **Algoritmo da Divisão de Euclides**. Dissertação de Mestrado, Universidade de Brasília - PROFMAT, Brasília 2016.

[14] Hefez, Abramo. **Iniciação à aritmética**. Sociedade Brasileira de Matemática, 2009.

[15] Hefez, Abramo. **Elementos de Aritmética**, Coleçao Textos Universitários. Editora da SBM, Rio de Janeiro-RJ, v. 2.