UNIVERSIDADE FEDERAL DE SANTA CATARINA
CAMPUS TRINDADE
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA EM REDE NACIONAL

João Figueiredo Penaforte

Teorema de Minkowski: e suas aplicações

Florianópolis
2024

João Figueiredo Penaforte

Teorema de Minkowski: e suas aplicações

Dissertação submetida ao Programa de Pós-Graduação em Matemática em Rede Nacional da Universidade Federal de Santa Catarina para a obtenção do título de Mestre em Matemática.
Orientador: Prof. Sérgio Tadao Martins, Dr.

Florianópolis
2024

Ficha catalográfica gerada por meio de sistema automatizado gerenciado pela BU/UFSC.
Dados inseridos pelo próprio autor.

Penaforte, João Figueiredo
Teorema de Minkowski: e suas aplicações / João Figueiredo Penaforte ; orientador, Sérgio Tadao Martins, 2024.
80 p.

Dissertação (mestrado profissional) - Universidade Federal de Santa Catarina, Centro de Ciências Físicas e Matemáticas, Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT, Florianópolis, 2024.

Inclui referências.

1. Matemática. 2. Teoria dos Números. 3. Soma de Quadrados. 4. Reticulados. 5. Ensino de Matemática. I. Martins, Sérgio Tadao. II. Universidade Federal de Santa Catarina. Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT. III. Título.

João Figueiredo Penaforte

Teorema de Minkowski: e suas aplicações

O presente trabalho em nível de mestrado foi avaliado e aprovado por banca examinadora composta pelos seguintes membros:

Profª Marianna Ravara Vago, Drª.
Instituição Universidade Federal de Santa Catarina

Prof. Eliezer Batista, Dr.
Instituição Universidade Federal de Santa Catarina

Prof. Leonardo Koller Sacht, Dr.
Instituição Universidade Federal de Santa Catarina

Certificamos que esta é a **versão original e final** do trabalho de conclusão que foi julgado adequado para obtenção do título de Mestre em Matemática.

Documento assinado digitalmente
Maria Inez Cardoso Goncalves
Data: 19/07/2024 10:03:02-0300
CPF: ***.897.119-**
Verifique as assinaturas em https://v.ufsc.br

Coordenação do Programa de
Pós-Graduação

Documento assinado digitalmente
Sergio Tadao Martins
Data: 18/07/2024 21:42:35-0300
CPF: ***.598.118-**
Verifique as assinaturas em https://v.ufsc.br

Prof. Sérgio Tadao Martins, Dr.
Orientador

Florianópolis, 2024.

Dedico essa dissertação ao meu pai e aos meus
sobrinhos Benício e Otávio.

AGRADECIMENTOS

Agradeço ao Departamento de Matemática pelo acolhimento e todo suporte oferecido em toda minha carreira de estudante. Aos meus colegas Tiago e Karina pelos compartilhamentos tão valiosos ao longo desses dois anos de estudos e dedicação. Ao meu orientador Sérgio Tadao, por me impulsionar a buscar novas perspectivas e conhecimentos dentro da Matemática e por toda sua nobre contribuição neste trabalho. Aos professores do Corpo Docente do Profmat UFSC, em especial ao prof. Eliezer Batista que sempre se apresentou de forma solícita e profissional à todas demandas acadêmicas. À minha irmã Mariana, pelo apoio e incentivo a continuar buscando meus objetivos.

Agradeço minha companheira Nani que, em todos os momentos, esteve ao meu lado me empoderando e me incentivando a concluir o mestrado.

oṃ tryambakam yajāmahe sugandhiṃ puṣṭivardhanam |
urvārukamiva bandhanān mṛtyor mukṣīya mā 'mṛtāt ||.
(mahāmṛyuṃjaya mantra - ṛg veda, Mandala 7, poema 59, verso 12)

RESUMO

Nesta dissertação está apresentado o Teorema de Minkowski e suas aplicações na Teoria dos Números. Os resultados são mostrados no caso geral e também em casos particulares. São apresentadas suas aplicações para o caso da soma de dois quadrados e também para a soma de quatro quadrados. Ao final, apresenta-se também uma abordagem da utilização de tais resultados aplicados no Ensino Médio como forma de estimular a pesquisa em Matemática e Teoria dos Números no Sistema Básico de Ensino.

Palavras-chave: Teoria dos Números . Soma de Quadrados. Reticulados. Ensino de Matemática.

ABSTRACT

This dissertation presents Minkowski's Theorem and its applications in Number Theory. The results are shown in the general case and also in particular cases. Its applications are presented for the case of the sum of two squares and also for the sum of four squares. At the end, an approach to the use of such results applied in High School is also presented as a way of stimulating research in Mathematics and Number Theory in the Basic Education System.

Keywords: Number Theory. Sum of Squares. Lattices. Mathematics Teaching.

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

O matemático Hermann Minkowski (1864-1909) foi pioneiro nos estudos da Geometria dos Números, uma área dentro da Teoria dos Números. Sua grande contribuição está relacionada à consideração de figuras no espaço euclidiano n-dimensinal que produzem resultados relevantes sobre diversos temas da Teoria dos Números, incluindo os resultados sobre somas de quadrados.

À primeira vista, o assunto Soma de Quadrados é acessível e de simples entendimento para estudantes de Matemática e Aritmética em geral. Porém as demonstrações relacionadas ao tema clamam certo estudo algébrico. Nesta dissertação serão demonstradas algumas maneiras de representar números inteiros como soma de quadrados baseado no resultado central do Teorema de Minkowski. Este tema possui grande importância no estudo de Teoria dos Números e Aritmética, conteúdos importantes na Matemática do Ensino Médio e também para as Olímpiadas de Matemática.

1.1 OBJETIVOS

Segundo Fan [5] (2012), um problema interessante em Teoria dos Números se refere às representações de um determinado inteiro positivo como a soma de um número fixo de quadrados de números inteiros. Rigorosamente falando, fixado um inteiro positivo k, queremos determinar para quais inteiros positivos n existem $x_1, \cdots, x_k$ inteiros tais que

$$n = \sum_{i=1}^{k} x_i^2$$

O caso $k = 1$ é trivial. O matemático Pierre de Fermat (1607-1665) considerou o caso $k = 2$ para primos $n = p$. Ele provou que um primo congruente a 3 módulo 4 não pode ser escrito como soma de dois quadrados. Observou ainda que todo primo congruente a 1 módulo 4 pode ser representado como a soma de dois quadrados. A generalização para todos inteiros positivos n já tinha sido abordada por Albert Girard (1595-1632), antes de Fermat. Entretanto, nem Girard nem Fermat, fizeram as demonstrações matemáticas de seus resultados. A primeira demonstração foi feita por Leonhard Euler (1707-1783) no século XVIII. O caso $k = 4$ foi solucionado por Joseph-Louis Lagrange (1736-1813) em 1770. Ele demonstrou que qualquer inteiro pode ser escrito como soma de quatro quadrados. Entre os anos 1797 e 1798, Adrien-Marie Legendre (1752-1833) demonstrou que todo inteiro positivo n pode ser escrito como soma de três quadrados, especificamente quando n não é da forma $4^a(8b + 7)$ para quaisquer inteiros não negativos a e b.

Atualmente existem muitas demonstrações diferentes dos resultados desenvolvidos por Fermat, Lagrange e Legendre em diversas áreas da Matemática. Abordaremos

as demonstrações deste presente trabalho utilizando as ideias da Geometria dos Números de Minkowski.

Para abordagem do tema, é necessário levantar conceitos sobre tópicos de Álgebra Linear, Álgebra Pura e também Aritmética, de onde surgiu a ideia inicial para realização deste trabalho. Essa revisão será feita nos capítulos que antecedem o Teorema de Minkowski e suas aplicações.

No capítulo onde é apresentado o Teorema de Minkowski apresenta-se a demonstração do teorema principal bem como suas aplicações nos casos dos números primos que podem ser escritos como soma de dois quadrados e o resultado que todo inteiro positivo n pode ser escrito como soma de quatro quadrados. Por fim é apresentada uma Proposta de Atividade para o Ensino Médio abordando o tema central da soma de quadrados.

2 DIVISIBILIDADE E CONGRUÊNCIA

Com a finalidade de contemplar resultados importantes que serão utilizados nas aplicações do Teorema de Minkowski, precisa-se explorar conceitos sobre divisibilidade e congruência. É importante que seja definido o Critério de Euler, o Símbolo de Legendre, o Teorema Chinês dos restos, entre outros conceitos sobre resíduos quadráticos e Aritmética em geral.

É importante mencionar que muitos resultados contidos neste capítulo são frutos do estudo da disciplina Aritmética no Mestrado Profissional em Matemática e a principal referência bibliográfica utilizada foi o livro *Introdução à Teoria dos Números* de SANTOS, J.P.O. [1] (2004).

Para o entendimento desse capítulo, a menos de menção contrária, todos os números serão inteiros.

2.1 O PRINCÍPIO DA BOA ORDEM

Um elemento $a_0 \in A$ diz-se **elemento mínimo** de A se, para todo $a \in A$ tem-se que $a_0 \leq a$. Usaremos o símbolo $min\ A$ para indicar o mínimo de um conjunto A, quando existir.

Definição 1. *(Princípio da Boa Ordem) Todo conjunto não vazio de inteiros não negativos contém um elemento mínimo.*

2.2 O MÁXIMO DIVISOR COMUM

O *máximo divisor comum* de dois inteiros a e b (a ou b diferente de zero), denotado por (a,b), é o maior inteiro que divide a e b.

Teorema 2.2.1. *Considere a um inteiro não nulo. Se $a \mid b$ e $a \mid c$, então, para todos inteiros m, n, tem-se que $a \mid (mb + nc)$.*

Demonstração:

Se $a \mid b$, existe um inteiro t tal que $at = b$. Multiplicando m dos dois lados da equação, temos $a(tm) = bm$. Logo $a \mid mb$.

Se $a \mid c$, existe um inteiro r tal que $ar = c$. Multiplicando n dos dois lados da equação, temos $a(rn) = cn$. Logo $a \mid nc$.

Somando os dois resultados acima, temos que

$$a(tm) + a(rn) = bm + cn$$

$$a(tm + rn) = (bm + cn).$$

Com isso, temos que $a \mid (mb + nc)$. ■

Teorema 2.2.2. *(Identidade de Bézout) Sejam a e b inteiros e $d = (a,b)$. Então existem inteiros r e s tal que $d = a \cdot r + b \cdot s$.*

Demonstração:

Inicialmente considere o conjunto $S = \{ax + by \mid x,y \in \mathbb{Z},\ \ ax + by \geq 0\}$.
O conjunto S não é vazio, pois se $x = a$ e $y = b$ temos

$$a \cdot a + b \cdot b = a^2 + b^2 \geq 0$$

Sabemos, pelo Princípio da Boa Ordem, que todo conjunto não vazio de inteiros não negativos contém um elemento mínimo. Sendo assim, existe elemento mínimo em S, seja $t = min\ S$. Como $t \in S$ temos

$$t = a \cdot r + b \cdot s,$$

com r e s inteiros.

Com a finalidade de mostrar que $t = (a,b)$, é importante verificar que

1. t é divisor de a e b, ou seja, $t \mid a$ e $t \mid b$.
2. Se c é um divisor comum de a e b, então $c \mid t$.

Se ambas afirmações forem mostradas, teremos t o maior inteiro que divide a e b. Para mostrar a primeira afirmação, utilizando o algoritmo da divisão de a por t, temos que

$$a = t \cdot q + r_1,$$

com $0 \leq r_1 < t$. Se t não for divisor de a, podemos concluir que $r_1 > 0$ e então

$$r_1 = a - t \cdot q = a - (a \cdot r + b \cdot s) \cdot q = a(1 - r \cdot q) + b(-s \cdot q).$$

Ou seja, $r_1 \in S$, pois é da forma $r_1 = a \cdot x + b \cdot y$, com $x = (1 - r \cdot q)$ e $y = (-s \cdot q)$. Entretanto $r_1 < t = min\ S$, contradição! Então, temos que t é divisor de a, $t \mid a$. De forma análoga podemos mostrar que t também é divisor de b, $t \mid b$. Desta forma, a primeira afirmação foi satisfeita.

Para mostrar a segunda afirmação, se $c \mid a$ e $c \mid b$, pelo Teorema 2.2.1 temos que $c \mid an + bm$ para todos inteiros n e m. Em particular para $c \mid ar + bs = t$. Logo, a segunda afirmação também foi satisfeita. Então conclui-se que $t = d = (a,b)$.

■

2.3 O TEOREMA FUNDAMENTAL DA ARITMÉTICA

Lema 2.3.1. *(Lema de Euclides) Se $a \mid bc$ e $(a,b) = 1$ então $a \mid c$.*

Demonstração: Pela Identidade de Bézout, temos que $am + bn = 1$, para alguns inteiros m e n. Multiplicando ambos lados desta equação por c temos que

$$c(am + bn) = c$$

$$amc + bnc = c \tag{1}$$

Por hipótese, temos que $a \mid bc$, ou seja, existe $k \in \mathbb{Z}$ tal que $a \cdot k = bc$. Da equação (1) temos

$$amc + bnc = c$$

$$amc + n(ak) = c$$

$$a(mc + nk) = c$$

Assim, podemos concluir que $a \mid c$. ■

Definição 2. ***Números Primos****. Um inteiro positivo p é chamado* ***primo*** *se tem exatamente dois divisores positivos: 1 e p.*

Definição 3. ***Números Compostos****. Um inteiro $m > 1$ é chamado* ***composto*** *quando não é primo.*

Teorema 2.3.1. *(**Teorema Fundamental da Aritmética**) Todo inteiro maior do que 1 pode ser representado de maneira única (a menos da ordem) como um produto de fatores primos.*

Demonstração:

Sabemos que um número $p > 1$ é primo se possui exatamente dois divisores positivos, ou seja, $1 \mid p$ e $p \mid p$. Se n for primo está encerrada a demonstração. Se n não for primo, seja n seja um número composto. Considere p_1 ($p_1 > 1$) o menor dos divisores positivos de n e que p_1 é primo. De fato, p_1 necessariamente é primo, senão teríamos $p \mid p_1 \Rightarrow 1 < p < p_1$. Mas sabemos que $p \mid n$, o que contradiria a escolha de p_1. Desta forma, podemos concluir que $n = p_1 n_1$.

Se n_1 for primo, a prova da existência do produto de fatores primos está completa. Senão, tomamos p_2 como o menor divisor de n_1. Pela constatação anterior, p_2 deve ser primo e temos que $n = p_1 p_2 n_2$.

Repetindo este procedimento de forma sucessiva, obtemos uma sequência decrescente de inteiros positivos n_1. $n_2, \cdots, n_r$. Como todos são números inteiros maiores do que 1, este procedimento certamente finalizará. Como os primos na sequência p_1, $p_2, \cdots, p_k$ não são, necessariamente, distintos, n terá sua representação na forma:

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

Para garantirmos a unicidade, vamos fazer a indução matemática em n. Considere que para $n = 2$ a afirmação é verdadeira. Assumimos, desta maneira, que ela é válida para todos números inteiros maiores do que 1 e menores do que n. Vamos mostrar que ela é verdadeira para n. Se n for primo, está concluída a demonstração.

Vamos supor, então, que n é um número composto e que possua duas fatorações distintas em primos, ou seja,

$$n = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_r$$

Mostraremos que $s = r$ e que cada p_i é igual a algum q_j.

De fato, se dado p primo é tal que $p \mid ab$ e $p \nmid a$, então $(a,p) = 1$, pois os únicos divisores positivos de p são 1 e p. Pelo Lema de Euclides, concluímos que $p \mid b$.

Como p_1 divide o produto $q_1 q_2 \cdots q_r$ ele divide pelo menos um dos fatores q_j. Sem perda de generalidade podemos considerar que $p_1 \mid q_1$. Mas, como são ambos números primos, isto implica que $p_1 = q_1$. Desta forma $n/p_1 = p_2 \cdots p_s = q_2 \cdots q_r$. Como $1 < n/p_1 < n$, a hipótese de indução nos mostra que ambas fatorações são idênticas, isto é, $s = r$ e, a menos da ordem, as fatorações $p_1 p_2 \cdots p_s$ e $q_1 q_2 \cdots q_s$ são iguais.

■

2.4 CONGRUÊNCIA

Assumiremos a definição 4 e o lema 2.4.1 de [2] MARTINS, S.T. e TENGAN, E. (2020, p. 597)

Definição 4. *Escrevemos $a \equiv b(mod\ m)$ (lê-se a **é congruente a** b **módulo** m) se, e somente se, $m \mid (a - b)$*

Por exemplo, temos $27 \equiv 3(mod\ 12)$ e $3 \equiv -33(mod\ 12)$ pois $27 - 3 = 24$ e $3 - (-33) = 36$ são múltiplos de 12. As propriedades a seguir mostram que a relação de congruência é uma relação de equivalência: a ideia é que quando escrevemos $a \equiv b(mod\ m)$, em termos de questões de divisibilidade por m, os inteiros a e b são por assim dizer "iguais".

Lema 2.4.1. *Para m fixado, a relação de congruência módulo m é de equivalência:*

- *(i) Reflexividade $a \equiv a(mod\ m)$ para todo a*
- *(ii) Simetria $a \equiv b(mod\ m) \Leftrightarrow b \equiv a(mod\ m)$*
- *(iii) Transitividade Se $a \equiv b(mod\ m)$ e $b \equiv c(mod\ m)$ então $a \equiv c(mod\ m)$*

Lema 2.4.2. *Se a, b, c e m são números inteiros e $ac \equiv bc(mod\ m)$, então $a \equiv b(mod\ \frac{m}{d})$, onde $d = (c,m)$.*

Demonstração: Da hipótese que $ac \equiv bc(mod\ m)$ temos que $m \mid (ac - bc)$, ou seja, $c(a - b) = km$, onde k é um inteiro. Dividindo ambos lados desta equação por d, chegaremos a $\frac{c}{d}(a - b) = k(\frac{m}{d})$. Desta forma, podemos concluir que $(\frac{m}{d}) \mid (\frac{c}{d})(a - b)$. Como $d = (c,m)$, podemos verificar que $(\frac{m}{d},\frac{c}{d}) = 1$. Então, pelo Lema de Euclides, segue que $(\frac{m}{d}) \mid (a - b)$ o que implica $a \equiv b(mod\ \frac{m}{d})$. ■

Definição 5. *Chama-se **sistema completo de resíduos** módulo m todo conjunto de números inteiros cujos restos pela divisão por m são os números $0, 1, \cdots, m-1$, sem repetições e em alguma ordem qualquer.*

Por exemplo, o conjunto $\{3,4,5\}$ é um sistema completo de resíduos módulo 3. Pode-se observar que $3 \equiv 0(mod\ 3)$, $4 \equiv 1(mod\ 3)$ e $5 \equiv 2(mod\ 3)$, ou seja, os números 3, 4 e 5 deixam resto 0, 1 e 2 pela divisão por 3, respectivamente.

Pela definição 5, conclui-se que um sistema completo de resíduos módulo m possui exatamente m elementos.

Definição 6. *Chama-se **sistema reduzido de resíduos** módulo m todo conjunto de números inteiros $\{r_1, r_2, \cdots, r_t\}$ que satisfaça as condições:*

1. $(r_i,m) = 1$*, para todos* $i = 1, \cdots, t$*;*
2. $r_i \not\equiv r_j(mod\ m)$*, para todo* $i \neq j$*;*
3. *para todo* $a \in \mathbb{Z}$ *tal que* $(a,m) = 1$*, existe* i *tal que* $a \equiv r_i(mod\ m)$*.*

´

Por exemplo, o conjunto $\{9,11\}$ é um sistema reduzido módulo 4. Verifica-se, inicialmente que $(9,4) = 1$ e $(11,4) = 1$. Tem-se também que $9 \not\equiv 11(mod\ 4)$. Para satisfazer a terceira condição, devemos considerar $a \in \mathbb{Z}$ ímpar, caso contrário não teríamos $(a,m) = 1$. Logo, pelo algoritmo da divisão, considera-se que $a = 4k + 1$ ou $a = 4k+3$. Temos que se $a = 4k+1$, então $a \equiv 1 \equiv 9(mod\ 4)$ e que se $a = 4k+3$, então $a \equiv 3 \equiv 11(mod\ 4)$. Desta forma, todas as condições da definição 6 foram satisfeitas.

2.5 TEOREMA DE FERMAT

Teorema 2.5.1. *(Pequeno Teorema de Fermat): Seja p primo. Se $p \nmid a$ então*
$a^{p-1} \equiv 1(mod\ p)$

Demonstração:

Sabemos que o conjunto formado pelos p números 0, 1, 2, $\cdots$, $p-1$ constitui um sistema completo de resíduos módulo p. Isto significa que qualquer conjunto contendo no máximo p elementos incongruentes módulo p pode ser colocado em bijeção com algum subconjunto de $\{0,1,2,\cdots,p-1\}$. Desta forma, vamos considerar os números a, $2a$, $3a$, $\cdots$, $(p-1)a$. Como $(a,p) = 1$, nenhum destes ia, $1 \leqslant i \leqslant p-1$ é divisível por p, ou seja, nenhum é congruente a zero módulo p. Quaisquer dois deles serão necessariamente incongruentes módulo p, pois se existisse $aj \equiv ak(mod\ p)$, teríamos que $j \equiv k(mod\ p)$ e isto só seria possível se $j = k$, já que ambos j e k são positivos e menores do que p. Temos, então, um conjunto de $p-1$ elementos incongruentes módulo p e não-divisíveis por p. Então, cada um deles é congruente a exatamente um

resíduo módulo p dentre $1, 2, 3, \cdots, p-1$. Se multiplicarmos todas essas congruências, membro a membro, vamos encontrar:

$$a(2a)(3a)\cdots(p-1)a \equiv 1.2.3\cdots(p-1)(mod\ p)$$

ou seja $a^{p-1}(p-1)! \equiv (p-1)!(mod\ p)$. Mas, como $((p-1)!,p) = 1$, podemos cancelar o fator $(p-1)!$ em ambos os lados, obtendo

$$a^{p-1} \equiv 1(mod\ p),$$

o que conclui a demostração.

■

2.6 TEOREMA CHINÊS DO RESTO

O resutado deste teorema é utilizado numa parte da demonstração da aplicação do Teorema de Minkoski para a Soma de Quatro Quadrados, um dos resultados mais importantes deste trabalho.

O nome dado ao teorema seguinte se deve ao fato de que este resultado já era conhecido pelos matemáticos chineses na antiguidade (SANTOS,J.P.O [1], 2004).

Teorema 2.6.1. *(O Teorema Chinês do Resto) Sejam $n_1, n_2, \cdots, n_k$ números naturais tais que $(n_i,n_j) = 1$ para $i \neq j$ e c_i inteiros. Então o sistema*

$$x \equiv c_1(mod\ n_1)$$

$$x \equiv c_2(mod\ n_2)$$

$$x \equiv c_3(mod\ n_3)$$

$$\vdots$$

$$x \equiv c_k(mod\ n_k)$$

possui solução e a solução é única módulo n, onde $n = n_1.n_2\cdots n_k$.

Demonstração:

Sejam $n = n_1.n_2\cdots n_k$ e $N_i = \frac{n}{n_i} = n_1.n_2\cdots(n_i-1)(n_i+1)\cdots n_k$, isto é, N_i é o produto de todos os inteiros $n_1n_2\cdots n_k$ excluindo n_i. Como $(n_i,n_j) = 1$ para $i \neq j$, então $(N_i,n_i) = 1$. Assim pela Identidade de Bézout, existem inteiros r_i e s_i tais que $r_iN_i + s_in_i = 1$, para cada $i = 1, \cdots, k$. Vamos provar que o inteiro $x_0 = c_1r_1N_1 + c_2r_2N_2 + \cdots + c_kr_kN_k$ é uma solução do sistema dado. Inicialmente, se $i \neq j$ então $N_j \equiv 0(mod\ n_i)$ já que $n_i \mid N_j$.

Logo, $c_jr_jN_j \equiv 0(mod\ n_i)$, de modo que

$$x_0 = c_1r_1N_1 + c_2r_2N_2 + \cdots + c_kr_kN_k \equiv c_ir_iN_i(mod\ n_i)$$

Por outro lado, de $r_iN_i + s_in_i = 1$, temos que $r_iN_i \equiv 1(mod\ n_i)$ para cada $i = 1, \cdots, k$.

Daí, $c_ir_iN_i \equiv c_i(mod\ n_i)$ e, por transitividade, $x_0 \equiv c_i(mod\ n_i)$ para todo i. Isso mostra que x_0 é uma solução do sistema. Por fim, se y_0 é outra solução do sistema então $y_0 \equiv c_i(mod\ n_i)$ para cada $i = 1, \cdots, k$. Desse modo, $x_0 \equiv y_0(mod\ n_i)$, isto é, $n_i \mid (x_0 - y_0)$. Como $(n_i,n_j) = 1$, com $i \neq j$, segue do Lema de Euclides que $n = n_1n_2 \cdots n_k$ divide $x_0 - y_0$, ou seja, $x_0 \equiv y_0(mod\ n)$, o que prova a unicidade da solução módulo n. Por isso, a solução geral do sistema é $x = x_0 + kn$, $k \in \mathbb{Z}$. ■

2.7 RESÍDUOS QUADRÁTICOS

Resíduos quadráticos é um pré-requisito para o entendimento das aplicações do Teorema de Minkowski, tema central desta dissertação. Será apresentada sua definição, bem como os conceitos relacionados ao Símbolo de Lengendre e Critério de Euler, fundamentais para este trabalho.

Portanto, nesta seção estaremos interessados no estudo de soluções para a congruência $x^2 \equiv a(mod\ m)$. No caso que m é primo ímpar e $(a,m) = 1$ esta congruência, caso tenha solução, tem exatamente duas soluções incongruentes módulo m.

Teorema 2.7.1. *Para p um primo ímpar e a um inteiro não divisível por p, a congruência*

$$x^2 \equiv a(mod\ p),$$

caso tenha solução, tem exatamente duas soluções incongruentes módulo p.

Demonstração:

Caso essa congruência tenha uma solução x_1, claramente $-x_1$ também será solução, uma vez que $(-x_1)^2 = x_1^2 \equiv a(mod\ p)$. Devemos mostrar que estas soluções x_1 e $-x_1$ são incongruentes módulo p. Se $x_1 \equiv -x_1(mod\ p)$, então teríamos $2x_1 \equiv 0(mod\ p)$ e, como p é ímpar e $p \nmid x_1$ (pois $p \mid (x_1^2 - a)$ e $p \nmid a$), isto é impossível. Precisamos mostrar que só existem duas soluções incongruentes. Seja y uma solução de $x^2 \equiv a(mod\ p)$, isto é, $y^2 \equiv a(mod\ p)$. Como x_1 é solução temos $x_1^2 \equiv y^2 \equiv a(mod\ p)$ e, portanto, $(x_1^2 - y^2) = (x_1 + y)(x_1 - y) \equiv 0(mod\ p)$. Logo, $p \mid (x_1 + y)$ ou $p \mid (x_1 - y)$, o que implica $y \equiv -x_1(mod\ p)$ ou $y \equiv x_1(mod\ p)$. Com isso mostramos que, caso exista uma solução, existem exatamente duas soluções incongruentes. ■

Definição 7. *Dizemos que a é um resíduo quadrático módulo m se a congruência $x^2 \equiv a(mod\ m)$ tiver solução. Caso $x^2 \equiv a(mod\ m)$ não tenha nenhuma solução, dizemos que a não é um resíduo quadrático módulo m ou que a é um resíduo não-quadrático. Se m for primo, sempre considere que a não divide m.*

Por exemplo, como $4^2 \equiv 1(mod\ 5)$, 1 é um resíduo quadrático módulo 5. Vamos considerar o primo 7 e achar todos os números que são resíduos quadráticos módulo 7. Para isso é suficiente considerarmos os quadrados dos números $1, 2, \cdots, 6$. Observe que estes números formam um sistema reduzido de resíduos módulo 7.

$1^2 \equiv 1(mod\ 7)$
$2^2 \equiv 4(mod\ 7)$
$3^2 \equiv 2(mod\ 7)$
$4^2 \equiv 2(mod\ 7)$
$5^2 \equiv 4(mod\ 7)$
$6^2 \equiv 1(mod\ 7)$

Na coluna da esquerda temos os quadrados dos números de 1 a 6 e na coluna da direita apenas os números 1, 4 e 2. Estes são todos os resíduos quadráticos módulo 7. Observe que estes números aparecem na metade superior da lista acima e que eles estão repetidos na metade inferior. O fato de haver repetição a partir do 4^2 vem da congruência $(7-k)^2 \equiv k^2(mod\ 7)$ que pode ser verificado no desenvolvimento de $7^2 - 14k + k^2 \equiv k^2(mod\ 7)$. No caso de um primo ímpar qualquer, pode-se mostrar que, dentre os elementos, $1, 2, \cdots, p-1$, que constituem um sistema reduzido de resíduos módulo p, metade deles, ou seja, $(p-1)/2$ são resíduos quadráticos e os restantes $(p-1)/2$, não são. Este é o resultado provado no teorema seguinte.

Teorema 2.7.2. *Seja p um primo ímpar. Dentre os números $1, 2, \cdots, p-1$, exatamente $(p-1)/2$ são resíduos quadráticos e $(p-1)/2$ não são.*

Demonstração: Vamos considerar, como fizemos no caso $p = 7$, os quadrados dos números de 1 a $p-1$. Como $1^2 \equiv 1(mod\ p)$ sabemos pelo Teorema 2.5.1, que -1 também é solução de $x^2 \equiv 1(mod\ p)$, mas $-1 \equiv p-1(mod\ p)$. Logo, 1 e $p-1$ são as únicas soluções de $x^2 \equiv 1(mod\ p)$. Tomamos, agora, 2^2 que será congruente a algum número k diferente de 1. Como $-2 \equiv p-2(mod\ p)$, 2 e $p-2$ são as únicas soluções incongruentes de $x^2 \equiv k(mod\ p)$. É claro que se $p > 3$, k será igual a 4. Veja o caso de $p = 7$ descrito acima. Já temos portanto dois pares, $(1,p-1)$ e $(2,p-2)$, cada par sendo as duas únicas soluções de uma congruência do tipo $x^2 \equiv a(mod)$. Procedendo dessa maneira teremos, ao final $(p-1)/2$ pares, cada um solução para uma dentre $(p-1)/2$ congruências $x^2 \equiv a_i(mod)$ associados a exatamente $(p-1)/2$ dos números $1, 2, 3, \cdots, p-1$. Os restantes $(p-1)/2$ não são resíduos quadráticos. ■

2.7.1 Símbolo de Legendre e o Critério de Euler

Definição 8. *Para p um primo ímpar e a um inteiro não-divisível por p, definimos o Símbolo de Legendre $\left(\frac{a}{p}\right)$ por*

$$\left(\frac{a}{p}\right) = \begin{cases} 1, \textit{ se a é um resíduo quadrático de p} \\ -1, \textit{ se a não é um resíduo quadrático de p} \end{cases}$$

Como vimos no exemplo acima, temos que que as congruências $x^2 \equiv 1(mod\ 7)$, $x^2 \equiv 2(mod\ 7)$ e $x^2 \equiv 4(mod\ 7)$ possuem solução, ou seja

$$\left(\frac{1}{7}\right) = \left(\frac{2}{7}\right) = \left(\frac{4}{7}\right) = 1.$$

Por outro lado,

$$\left(\frac{3}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{6}{7}\right) = -1$$

uma vez que as congruências $x^2 \equiv 3(mod\ 7)$, $x^2 \equiv 5(mod\ 7)$ e $x^2 \equiv 6(mod\ 7)$ não possuem soluções.

Teorema 2.7.3. *(Lagrange) Seja $f(x) = c_n x^n + c_{n-1}x^{n-1} + \cdots + c_2 x^2 + c_1 x + c_0$ um polinômio com coeficientes inteiros tal que $(c_n, p) = 1$, onde p é primo. Nestas condições a congruência*

$$f(x) \equiv 0(mod\ p)$$

tem no máximo n soluções. É claro que quando $n > p$ a congruência acima não tem mais do que p soluções distintas módulo p.

Demonstração:

A demonstração será feita por indução em n, o grau do polinômio $f(x)$. Para $n = 1$ temos a congruência linear

$$f(x) = c_1 x + c_0 \equiv 0(mod\ p).$$

Como por hipótese, $(c_1, p) = 1$, podemos concluir que $c_1 x \equiv -c_0(mod\ p)$ tem exatamente uma solução. De fato, existe $y \in \mathbb{Z}$ tal que $c_1 x = -c_0 + py$. Sendo assim, pela Identidade de Bézout, existe solução para equação $c_1 x - py = 1$. Multiplicando ambos lados da equação por $(-c_0)$ concluímos o resultado enunciado acima. Logo, o resultado é válido para $n = 1$. Assumimos o resultado verdadeiro para todo polinômio de grau $n-1$. A prova que apresentamos é por contradição. Vamos supor que a congruência $f(x) \equiv 0(mod\ p)$ tenham $n+1$ soluções incongruentes módulo p. Sejam $x_0, x_1, x_2, \cdots, x_n$ estas $n+1$ soluções. Podemos verificar que

$$f(x) - f(x_0) = c_n(x^n - x_0^n) + c_{n-1}(x^{n-1} - x_0^{n-1}) + \cdots + c_1(x - x_0) = (x - x_0)h(x),$$

uma vez que $(x^i - x_0^i)$ é divisível por $(x - x_0)$ para todo inteiro i, $i = 1, 2, 3, \cdots, n$ e que $h(x)$ é um polinômio de grau $n-1$ contendo c_n como coeficiente de x^{n-1}. Como $f(x_k) \equiv f(x_0)(mod\ p)$, temos

$$f(x_k) - f(x_0) = (x_k - x_0)h(x_k) \equiv 0(mod\ p)$$

Isto implica que, para $k \neq 0$, $h(x_k) \equiv 0(mod\ p)$ pois $x_k \not\equiv x_0(mod\ p)$ se $x_k \neq x_0$. Portanto a congruência $h(x) \equiv 0(mod\ p)$ possui n soluções incongruentes módulo p, o que contradiz a hipótese de indução, uma vez que $(c_n, p) = 1$ e $h(x)$ tem grau $n-1$. Logo, $f(x)$ não pode ter mais do que n soluções incongruentes módulo p, o que conclui a demonstração.

■

Teorema 2.7.4. *(Critério de Euler) Se p for um primo ímpar e a um inteiro não divisível por p, então*

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2}(mod\ p)$$

Demonstração:

Vamos supor, primeiramente, que $\left(\frac{a}{p}\right) = 1$. Isto significa que a congruência $x^2 \equiv a(mod\ p)$ tem solução. Seja y uma solução. Do fato de que $(a,p) = 1$ e $p \mid (y^2 - a)$ concluímos que $(y,p) = 1$. Logo, pelo Pequeno Teorema de Fermat, $y^{p-1} \equiv 1(mod\ p)$ e, portanto,

$$a^{\frac{(p-1)}{2}} \equiv (y^2)^{\frac{(p-1)}{2}} = y^{p-1} \equiv 1(mod\ p)$$

Isto prova o teorema no caso em que $\left(\frac{a}{p}\right) = 1$.

Consideremos, agora, o caso $\left(\frac{a}{p}\right) = -1$. Como vimos na seção inicial deste capítulo, se a for um resíduo quadrático, $a^{(p-1)/2} \equiv 1(mod\ p)$. Sabemos que a congruência $f(x) = x^{(p-1)/2} - 1 \equiv 0(mod\ p)$ possui no máximo $(p-1)/2$ soluções incongruentes módulo p (Teorema 2.7.3). Mas do fato de existirem $(p-1)/2$ resíduos quadráticos, e de termos $a^{(p-1)/2} \equiv 1(mod\ p)$ para todo resíduo quadrático, concluímos que todos eles são soluções de $f(x) \equiv 0(mod\ p)$. Isto nos garante que a congruência $f(x) \equiv 0(mod\ p)$ possui exatamente $(p-1)/2$ raízes e que, portanto, se a não for resíduo quadrático, isto é, $\left(\frac{a}{p}\right) = -1$, então $a^{(p-1)/2} \not\equiv 1(mod\ p)$. Mas, como

$$a^{p-1} - 1 = \left(a^{(p-1)/2} - 1\right)\left(a^{(p-1)/2} + 1\right)$$

e $a^{p-1} - 1 \equiv 0(mod\ p)$, para $(p,a) = 1$, concluímos que $a^{(p-1)/2} \equiv \pm 1(mod\ p)$.

Logo, caso $\left(\frac{a}{p}\right) = -1$ deveremos ter $a^{(p-1)/2} \equiv -1(mod\ p)$, ou seja,

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2}(mod\ p)$$

o que conclui a demonstração.

■

3 BASE DE UM ESPAÇO VETORIAL

Um dos conceitos mais importantes no estudo da Geometria dos Números, está relacionado com a determinação de um reticulado. Este, por sua vez, é definido a partir de uma base de vetores linearmente independentes de um espaço euclidiano n-dimensional. Neste capítulo serão definidos conceitos importantes sobre Álgebra Linear, com o objetivo de justificar o uso de reticulados no Teorema de Minkowski e suas aplicações.

3.1 ESPAÇOS VETORIAIS

Assumiremos a definição a seguir de STEINBRUCH,A. e WINTERLE,P. [3] (2012, p.18) de seu livro *Álgebra Linear*.

Seja um conjunto V, não vazio, sobre o qual estão definidas as operações soma vetorial e multiplicação escalar, isto é:

$$\forall u, v \in V, u + v \in V$$

$$\forall a \in \mathbb{R}, \forall u \in V, au \in V$$

O conjunto V com essas duas operações é chamado de *espaço vetorial real* (ou espaço vetorial sobre $\mathbb{R}$) se forem verificados os seguintes axiomas:

1. Em relação à soma vetorial:

   $(u + v) + w = u + (v + w),\ \forall u, v, w \in V$

   $u + v = v + u,\ \forall u,v \in V$

   $\exists\, 0 \in V,\ \forall u \in V, u + 0 = 0 + u = u$

   $\forall u \in V,\ \exists(-u) \in V,\ u + (-u) = 0$

2. Em relação à multiplicação escalar, para $\forall u, v \in V$ e $\forall a, \beta \in \mathbb{R}$:

   $(a\beta)u = a(\beta u)$

   $(a + \beta)u = au + \beta u$

   $a(u + v) = au + av$

   $1u = u$

No contexto de espaços vetoriais, os elementos de V são chamados de **vetores**, independentemente de sua natureza.

3.1.1 Propriedades dos Espaços Vetoriais

Da definição de Espaço Vetorial V decorrem as seguintes propriedades:

1. Existe um único vetor nulo em V (elemento neutro da soma vetorial).

2. Cada vetor $u \in V$ admite apenas um simétrico $(-u) \in V$.
3. Para quaisquer $u, v, w \in V$, se $u + w = v + w$ então $u = v$.
4. Qualquer que seja $v \in V$, tem-se que $-(-v) = v$. Isto é, o oposto de $-v$ é v.
5. Quaisquer que sejam u,$v \in V$, existe um e somente um $x \in V$ tal que $u + x = v$. Esse vetor x será representado por $x = v - u$.
6. Qualquer que seja $v \in V$, tem-se $0v = 0$. Naturalmente, o primeiro zero é o número real zero, e o segundo é o vetor $0 \in V$.
7. Qualquer que seja $\lambda \in \mathbb{R}$, tem-se $\lambda 0 = 0$.
8. $\lambda v = 0$ implica $\lambda = 0$ ou $v = 0$.
9. Qualquer que seja $v \in V$, tem-se que $(-1)v = -v$
10. Quaisquer que sejam $v \in V$ e $\lambda \in \mathbb{R}$, tem-se que $(-\lambda)v = \lambda(-v) = -(\lambda v)$.

3.2 DEPENDÊNCIA E INDEPENDÊNCIA LINEAR

3.2.1 Combinação Linear

Definição 9. *Considere os vetores $v_1, v_2, \cdots, v_n$ do espaço Vetorial V e os escalares, $a_1, a_2, \cdots, a_n$. Qualquer vetor $v \in V$ da forma:*

$$v = a_1 v_1 + a_2 v_2 + \cdots + a_n v_n$$

*é uma **combinação linear** dos vetores $v_1, v_2, \cdots, v_n$.*

Definição 10. *Seja V um espaço vetorial e $A = \{v_1, \cdots, v_n\} \subset V$. Consideremos a equação*

$$a_1 v_1 + \cdots + a_n v_n = 0$$

Sabemos que essa equação admite pelo menos uma solução:

$$a_1 = a_2 = \cdots = a_n = 0$$

chamada de solução trivial.

*O conjunto A diz-se **linearmente independente** (LI), ou os vetores $v_1, \cdots, v_n$ são LI, caso a equação acima admita apenas a solução trivial.*

*Se existem soluções com algum $a_i \neq 0$, diz-se que o conjunto A é **linearmente dependente** (LD), ou que os vetores $v_1, \cdots, v_n$ são LD.*

3.2.2 Subespaços Vetoriais e Subespaços Gerados

Sejam V um espaço vetorial e S um subconjunto não vazio de V. O subconjunto S é um *subespaço vetorial* de V se S é um espaço vetorial em relação à adição e à multiplicação por escalar definidas em V.

Seja V um espaço vetorial. Consideremos o subconjunto

$$A = \{v_1, v_2, \cdots, v_n\} \subset V, A \neq \varnothing.$$

O subconjunto S de todos os vetores de V que são combinações lineares dos vetores de A é um subespaço de de V.

De fato, se:

$$u = a_1 v_1 + a_2 v_2 + \cdots + a_n v_n$$

e

$$v = b_1 v_1 + b_2 v_2 + \cdots + b_n v_n$$

são dois vetores quaisquer de S, pode-se escrever:

$$u + v = (a_1 + b_1)v_1 + (a_2 + b_2)v_2 + \cdots + (a_n + b_n)v_n$$

$$au = (aa_1)v_1 + (aa_2)v_2 + \cdots + (aa_n)v_n$$

Tendo em vista que $u + v \in S$ e que $au \in S$, por serem combinações lineares de $v_1, v_2, \cdots, v_n$, conclui-se que S é um subespaço vetorial de V.

Simbolicamente, o subespaço S é:

$$S = \{v \in V \mid v = a_1 v_1 + \cdots + a_n v_n,\ a_1, \cdots, a_n \in \mathbb{R}\}$$

Observações

1. O subespaço S diz-se gerado pelos vetores $v_1, \cdots, v_n$, ou gerado pelo conjunto A, e representa-se por:

   $$S = [v_1, v_2, \cdots, v_n] \ \ ou\ S = G(A)$$

   Os vetores $v_1, v_2, \cdots, v_n$ são chamados de geradores do subespaço S, enquanto A é o conjunto gerador de S.

2. Para o caso particular $A = \varnothing$, define-se: $[\varnothing] = \{0\}$.

3. $A \subset G(A)$, ou seja, $\{v_1, \cdots, v_n\} \subset [v_1, \cdots, v_n]$

4. Todo conjunto $A \subset V$ gera um subespaço vetorial de V, podendo ocorrer $G(A) = V$. Neste caso, A é um conjunto gerador de V.

3.2.3 Base de um Espaço Vetorial

Um conjunto $B = \{v_1, \cdots, v_n\} \subset V$ é uma base do espaço vetorial V se:

1. B é LI;
2. B gera V.

Exemplo:

1. $B = \{(1,1), (-1,0)\}$ é base de $\mathbb{R}^2$. De fato

a) B é LI, pois $a(1,1) + b(-1,0) = (0,0)$ implica:

$$\begin{cases} a - b = 0 \\ a = 0 \end{cases}$$

e daí $a = b = 0$.

b) B gera $\mathbb{R}^2$, pois para todo $(x,y) \in \mathbb{R}^2$, tem-se:

$$(x,y) = y(1,1) + (y - x)(-1,0)$$

Realmente, a igualdade

$$(x,y) = a(1,1) + b(-1,1)$$

implica

$$\begin{cases} a - b = x \\ a = y \end{cases}$$

de onde $a = y$ e $b = y - x$.

Como mostrado acima, os vetores da base B são LI. Sendo eles do $\mathbb{R}^2$, irão gerar o próprio $\mathbb{R}^2$. Na verdade, quaisquer dois vetores não-colineares do $\mathbb{R}^2$ formam uma base desse espaço.

2. (Base Canônica) Consideremos os vetores

$$e_1 = (1, 0, 0, \cdots, 0), e_2 = (0, 1, 0, \cdots, 0), \cdots, e_n = (0, 0, 0, \cdots, 1)$$

Temos que o conjunto $B = \{e_1, e_2, \cdots, e_n\}$ é LI em $\mathbb{R}^n$. Tendo em vista que todo vetor $v = (x_1, x_2, \cdots, x_n) \in \mathbb{R}^n$ pode ser escrito como combinação linear de $e_1, e_2, \cdots, e_n$, isto é:

$$v = x_1 e_1 + x_2 e_2 + \cdots + x_n e_n$$

conclui-se que B gera o $\mathbb{R}^n$. Portanto, B é uma base de $\mathbb{R}^n$. Essa base é conhecida como *base canônica* do $\mathbb{R}^n$.

3.3 RELAÇÃO ENTRE CÁLCULO DE VOLUME E DETERMINANTES

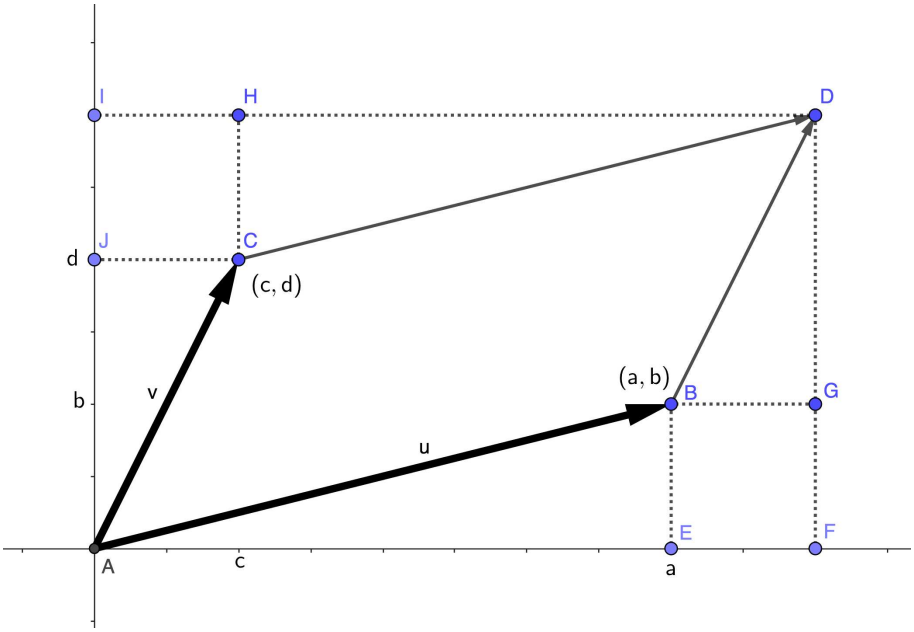
Ainda sobre o estudo dos reticulados em Geometria dos Números, se faz necessário o cálculo do volume do sólido formado pelos vetores de sua base, que será definido posteriormente como volume do paralelogramo fundamental de um reticulado no Teorema de Minkowski.

Toda base B é um conjunto de vetores LI. Nessa seção vamos mostrar que podemos calcular o volume do sólido gerado pelos vetores de uma base B qualquer. Para bases de espaços vetoriais euclidianos, temos que o cálculo desse volume é igual ao módulo do determinante dos vetores da base.

Desta forma, vamos apresentar resultados para bases de $\mathbb{R}^2$ e $\mathbb{R}^3$.

Para o $\mathbb{R}^2$ vamos fazer o cálculo da área deste paralelogramo a partir dos conceitos de geometria plana. Considere os vetores $\vec{u}$ e $\vec{v}$ na figura abaixo, sendo $\{u, v\}$ uma base de $\mathbb{R}^2$.

Figura 1 – Paralelogramo entre vetores LI.



Para fazer o cálculo da área do Paralelogramo $ABDC$ vamos fazer o cálculo da área do retângulo maior $AFDI$ e subtrair as áreas dos retângulos $EFGB$, $CHIJ$, como também subtrair as áreas dos triângulos AEB, CDH, BDG e ACJ. Observem que, por semelhança, os triângulos AEB e CDH são congruentes, como também são congruentes os triângulos BDG e ACJ. Sendo o vetor $\vec{u} = (a,b)$ e $\vec{v} = (c,d)$ temos:

$$\text{Área}(ABDC) = \text{Área}(AFDI) - 2.\text{Área}(EFGB) - 2.\text{Área}(AEB) - 2.\text{Área}(BDG)$$

Logo:

$$\text{Área}(ABDC) = (a+c)(b+d) - 2.(c.b) - 2.\left(\frac{a.b}{2}\right) - 2.\left(\frac{c.d}{2}\right)$$

$$\text{Área}(ABDC) = ab + ad + bc + cd - 2.bc - ab - cd$$

$$\text{Área}(ABDC) = ad - bc = Det(\vec{u},\vec{v})$$

Sem perda de generalidade, sabendo os vetores $\vec{u}$ e $\vec{v}$ podem ser inseridos em filas distintas na matriz que usamos para calcular o determinante e que a área do paralegramo $ABDC$ é sempre positiva, conluímos que Área$(ABDC) = |Det(\vec{u},\vec{v})|$.

Para o espaço tridimensional $\mathbb{R}^3$, Vamos utilizar a ideia de produto vetorial e produto misto. Assumiremos as definições de STEINBRUCH,A. e WINTERLE,P. [4] do livro *Geometria Analítica* (2012).

Definição 11. *Chama-se **produto interno** (ou produto escalar) de dois vetores $\vec{u} = x_1\vec{i} + y_1\vec{j} + z_1\vec{k}$ e $\vec{v} = x_2\vec{i} + y_2\vec{j} + z_2\vec{k}$, e representa por $\langle\vec{u},\vec{v}\rangle$ ao número real*

$$\langle\vec{u},\vec{v}\rangle = x_1x_2 + y_1y_2 + z_1z_2$$

Definição 12. *O **Módulo de um vetor** $\vec{v} = x\vec{i} + y\vec{j} + z\vec{k}$, representado por $|\vec{v}|$, é o número real não negativo*

$$|\vec{v}| = \sqrt{\langle\vec{v},\vec{v}\rangle} = \sqrt{x^2 + y^2 + z^2}$$

Definição 13. *Dados os vetores $\vec{u} = x_1\vec{i} + y_1\vec{j} + z_1\vec{k}$ e $\vec{v} = x_2\vec{i} + y_2\vec{j} + z_2\vec{k}$ tomados nesta ordem, chama-se **produto vetorial** dos vetores $\vec{u}$ e $\vec{v}$, e se representa por $\vec{u} \times \vec{v}$, ao vetor:*

$$\vec{u} \times \vec{v} = (y_1z_2 - z_1y_2)\vec{i} - (x_1z_2 - z_1x_2)\vec{j} + (x_1y_2 - y_1x_2)\vec{k}$$

Cada componente deste vetor pode ainda ser expresso na forma de um determinante de 2ª ordem:

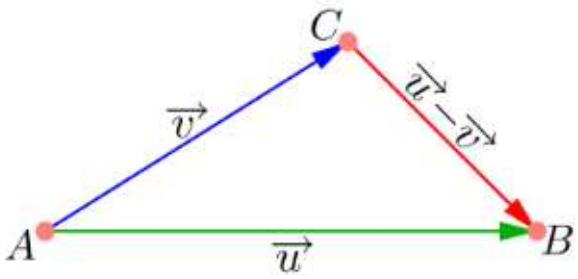
$$\vec{u} \times \vec{v} = \begin{vmatrix} y_1 & z_1 \\ y_2 & z_2 \end{vmatrix}\vec{i} - \begin{vmatrix} x_1 & z_1 \\ x_2 & z_2 \end{vmatrix}\vec{j} + \begin{vmatrix} x_1 & y_1 \\ x_2 & y_2 \end{vmatrix}\vec{k} = \begin{vmatrix} \vec{i} & \vec{j} & \vec{k} \\ x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \end{vmatrix}$$

Vamos mostrar que o produto interno de dois vetores está relacionado com o ângulo por eles formado. Se $\vec{u} \neq \vec{0}$ e se ϑ é o ângulo entre os vetores $\vec{u}$ e $\vec{v}$, então:

$$\langle\vec{u},\vec{v}\rangle = |\vec{u}||\vec{v}|cos\vartheta$$

Aplicando a lei dos cossenos ao triângulo ABC da figura 2, temos:

Figura 2 – Ângulo entre Vetores.



$$|\vec{u}-\vec{v}|^2 = |\vec{u}|^2 + |\vec{v}|^2 - 2|\vec{u}||\vec{v}|cos\vartheta \tag{2}$$

Pela definição de módulo de um vetor, temos que

$$|\vec{u}-\vec{v}|^2 = \left(\sqrt{\langle \vec{u}-\vec{v},\vec{u}-\vec{v}\rangle}\right)^2 = \langle \vec{u}-\vec{v},\vec{u}-\vec{v}\rangle$$

$$|\vec{u}-\vec{v}|^2 = \langle \vec{u},\vec{u}\rangle - \langle \vec{u},\vec{v}\rangle - \langle \vec{v},\vec{u}\rangle + \langle \vec{v},\vec{u}\rangle$$

$$|\vec{u}-\vec{v}|^2 = \langle \vec{u},\vec{u}\rangle + \langle \vec{v},\vec{u}\rangle - 2\langle \vec{u},\vec{v}\rangle$$

$$|\vec{u}-\vec{v}|^2 = |\vec{u}|^2 + |\vec{v}|^2 - 2\langle \vec{u},\vec{v}\rangle \tag{3}$$

logo, de (2) e (3) conlui-se que:

$$\langle \vec{u},\vec{v}\rangle = |\vec{u}||\vec{v}|cos\vartheta.$$

Considere $\vec{u} = (x_1,y_1,z_1)$ e $\vec{v} = (x_2,y_2,z_2)$. Queremos mostrar a propriedade a seguir:

$$|\vec{u}\times\vec{v}|^2 = |\vec{u}|^2|\vec{v}|^2 - (\langle \vec{u},\vec{v}\rangle)^2 \tag{4}$$

Pela definição de produto vetorial temos que:

$$\vec{u}\times\vec{v} = \begin{vmatrix} y_1 & z_1 \\ y_2 & z_2 \end{vmatrix}\vec{i} - \begin{vmatrix} x_1 & z_1 \\ x_2 & z_2 \end{vmatrix}\vec{j} + \begin{vmatrix} x_1 & y_1 \\ x_2 & y_2 \end{vmatrix}\vec{k}$$

então:

$$|\vec{u}\times\vec{v}|^2 = (y_1z_2 - z_1y_2)^2 + (-x_1z_2 + z_1x_2)^2 + (x_1y_2 - y_1x_2)^2$$

Desenvolvendo o outro lado da equação:

$$|\vec{u}|^2|\vec{v}|^2 = (x_1^2 + y_1^2 + z_1^2)(x_2^2 + y_2^2 + z_2^2)$$

e também:

$$(\langle \vec{u},\vec{v}\rangle)^2 = (x_1x_2 + y_1y_2 + z_1z_2)^2$$

Realizando as operações indicadas acima, conclui-se que

$$|\vec{u} \times \vec{v}|^2 = |\vec{u}|^2|\vec{v}|^2 - \left(\langle \vec{u}, \vec{v} \rangle\right)^2 .$$

Da equação (4), temos que:

$$|\vec{u} \times \vec{v}|^2 = |\vec{u}|^2|\vec{v}|^2 - \left(\langle \vec{u}, \vec{v} \rangle\right)^2$$

$$|\vec{u} \times \vec{v}|^2 = |\vec{u}|^2|\vec{v}|^2 - \left(|\vec{u}||\vec{v}| cos\vartheta\right)^2$$

$$|\vec{u} \times \vec{v}|^2 = |\vec{u}|^2|\vec{v}|^2 - |\vec{u}|^2|\vec{v}|^2 (cos\vartheta)^2$$

$$|\vec{u} \times \vec{v}|^2 = |\vec{u}|^2|\vec{v}|^2 (1 - (cos\vartheta)^2)$$

então:

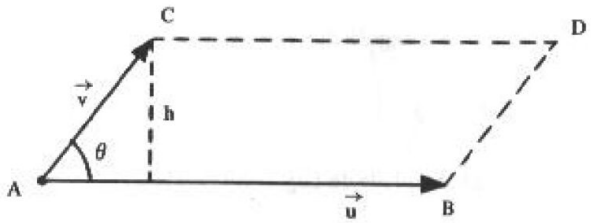
$$|\vec{u} \times \vec{v}|^2 = |\vec{u}|^2|\vec{v}|^2 (sen\vartheta)^2$$

e alcança-se o seguinte resultado

$$|\vec{u} \times \vec{v}| = |\vec{u}||\vec{v}| sen\vartheta$$

Sendo assim, o módulo do produto vetorial dos vetores $\vec{u}$ e $\vec{v}$ calcula a área do paralelogramo $ABCD$ determinado pelo vetores $\vec{u} = \vec{AB}$ e $\vec{v} = \vec{AC}$.

Figura 3 – Interpretação Geométrica do Produto Vetorial.



Geometricamente temos que:

Área ABCD $= |\vec{u}|\, h$ e ainda $h = |\vec{v}|\, sen\vartheta$

Área ABCD $= |\vec{u}|\, |\vec{v}|\, sen\vartheta$

Que coincide com o resultado que obtemos quando fazemos o produto vetorial entre dois vetores, $|\vec{u} \times \vec{v}| = |\vec{u}|\, |\vec{v}|\, sen\vartheta$

Desta forma,

$$|\vec{u} \times \vec{v}| = \text{Área ABCD}$$

Para espaços euclidianos de dimensão 3, vamos fazer a interpretação do produto misto de vetores. Para mostrar o resultado abaixo considere que o vetor $(\vec{v} \times \vec{w})$ é simultaneamente ortogonal aos vetores $\vec{v}$ e $\vec{w}$. A demostração desta propriedade está disponível no Livro *Geometria Analítica* de STEINBRUCH,A. e WINTERLE,P. [4] (2012, p.66)

Definição 14. *Dados os vetores* $\vec{u} = x_1\vec{i}+y_1\vec{j}+z_1\vec{k}$, $\vec{v} = x_2\vec{i}+y_2\vec{j}+z_2\vec{k}$ *e* $\vec{w} = x_3\vec{i}+y_3\vec{j}+z_3\vec{k}$, *tomados nesta ordem, o* ***produto misto*** *dos vetores* $\vec{u}$, $\vec{v}$ *e* $\vec{w}$ *é o numero real obtido a partir do produto interno* $\langle\vec{u},(\vec{v}\times\vec{w})\rangle$. *Indica-se o produto misto por* $(\vec{u},\vec{v},\vec{w})$. *Tendo em vista que:*

$$\vec{v}\times\vec{w} = \begin{vmatrix} \vec{i} & \vec{j} & \vec{k} \\ x_2 & y_2 & z_2 \\ x_3 & y_3 & z_3 \end{vmatrix} = \begin{vmatrix} y_2 & z_2 \\ y_3 & z_3 \end{vmatrix}\vec{i} - \begin{vmatrix} x_2 & z_2 \\ x_3 & z_3 \end{vmatrix}\vec{j} + \begin{vmatrix} x_2 & y_2 \\ x_3 & y_3 \end{vmatrix}\vec{k}$$

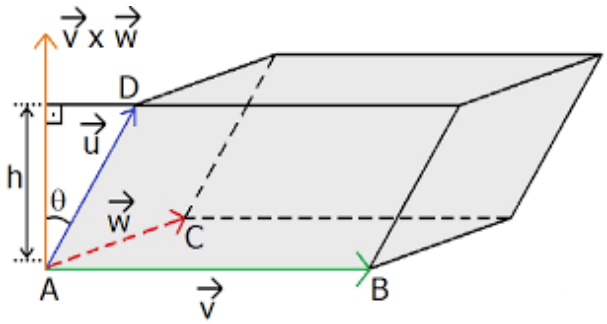
e levando em consideração a definição de produto interno de dois vetores, o valor de $\langle\vec{u},(\vec{v}\times\vec{w})\rangle$ *é dado por:*

$$(\vec{u},\vec{v},\vec{w}) = x_1\begin{vmatrix} y_2 & z_2 \\ y_3 & z_3 \end{vmatrix} - y_1\begin{vmatrix} x_2 & z_2 \\ x_3 & z_3 \end{vmatrix} + z_1\begin{vmatrix} x_2 & y_2 \\ x_3 & y_3 \end{vmatrix} = \begin{vmatrix} x_1 & x_2 & x_3 \\ x_2 & y_2 & z_2 \\ x_3 & y_3 & z_3 \end{vmatrix} = Det\,(\vec{u},\vec{v},\vec{w})$$

.

O produto misto $\langle\vec{u},(\vec{v}\times\vec{w})\rangle$ é igual, em módulo, ao volume do paralelepípedo de arestas determinadas pelos vetores $\vec{u} = \vec{AD}$, $\vec{v} = \vec{AB}$ e $\vec{w} = \vec{AC}$.

Figura 4 – Interpretação Geométrica do Produto Misto.



Sabe-se que o volume V de um paralelepípedo é:

$$V = \text{Área da Base} \times \text{altura}$$

ou seja, $V = A_b \times h$. Da interepretação geométrica do produto vetorial temos que $A_b = |\vec{v}\times\vec{w}|$. E sendo ϑ o ângulo entre os vetores $\vec{u}$ e $\vec{v}\times\vec{w}$, lembrando que o vetor $\vec{v}\times\vec{w}$ é perpendicular à base, a altura do paralelepípedo é dada por:

$$h = |\vec{u}|\,|cos\vartheta|$$

(É importante considerar o valor absoluto de $|cos\vartheta|$, pois ϑ pode ser um ângulo obtuso.)

Então, o volume do paralelepípedo é:

$$V = |\vec{v}\times\vec{w}|\,|\vec{u}|\,|cos\vartheta| = |\vec{u}|\,|\vec{v}\times\vec{w}|\,|cos\vartheta|$$

Fazendo $\vec{v} \times \vec{w} = \vec{a}$, obtemos:

$$V = |\vec{u}|\,|\vec{a}|\,|cos\vartheta| = |\langle \vec{u}, \vec{a} \rangle|$$

(Como sabemos que $\langle \vec{u}, \vec{a} \rangle = |\vec{u}|\,|\vec{a}|\,cos\vartheta \Rightarrow |\langle \vec{u}, \vec{a} \rangle| = |\vec{u}|\,|\vec{a}|\,|cos\vartheta|$).

Segue que:

$$V = |\langle \vec{u}, \vec{a} \rangle| = |\langle \vec{u}, (\vec{v} \times \vec{w}) \rangle| = |(\vec{u}, \vec{v}, \vec{w})| = |Det(\vec{u}, \vec{v}, \vec{w})|\,.$$

4 O TEOREMA DE MINKOWSKI

4.1 BIOGRAFIA

Segundo Strobl [12] (1985), Hermann Minkowski foi um matemático alemão, que desenvolveu estudos em diversas áreas da Matemática. Na época da escola mostrara seu talento e interesse pela Matemática lendo obras de Dedekind, Dirichlet e Gauss.

Era amigo íntimo do matemático David Hilbert (1862-1943). Ambos fizeram suas graduações na mesma época, na Universidade de Königsberg.

Minkowski desenvolveu a maioria de seus estudos na matemática pura e passou muito de seu tempo investigando sobre formas quadráticas e frações contínuas. Recebeu alguns prêmios por alguns de de seus trabalho. Um desses prêmios, dividido com o matemático Henry Smith, foi a solução do número de representações de um inteiro como soma de cinco quadrados.

Sua contribuição mais original foi a criação da Teoria Geométrica dos Números, também conhecida como Geometria dos Números. Este foi um dos temas que abordou em algumas de suas pesquisas enquanto trabalhava como professor nas Universidades de Bonn, Königsberg, Zurique, Berlim e Göttingen. No final de sua carreira, se interessou por física matemática, especificamente pelas teorias eletrônica e eletrodinâmica.

O famoso físico teórico Albert Einstein (1879-1955) foi seu aluno em diversos cursos, motivo pelo qual ambos cientistas interessaram-se por problemas semelhantes na teoria da relatividade.

De acordo com Corry [13] (1998), Minkowski havia desenvolvido uma nova visão de espaço e tempo e lançou as bases matemáticas da Teoria da Relatividade. Ele percebeu que o trabalho de Lorentz e Einstein poderia ser melhor compreendido em um espaço não euclidiano. Espaço e tempo que antes eram considerados independentes, foram acoplados em um *continuum espaço-tempo* de quatro dimensões.

Seu trabalho de Geometria dos Números permitiu desenvolvimentos futuros sobre corpos convexos e as questões sobre problemas de empacotamento, as formas pelas quais figuras de uma determinada forma podem ser colocadas dentro de outra figura.

No registro de sua morte, o amigo Hilbert deixou a seguinte mensagem, traduzida ao português: "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."

Figura 5 – Minkowski - Perfil.

4.2 O RETICULADO E O PARALELOGRAMO FUNDAMENTAL

As definições de reticulado e o volume associado ao seu respectivo paralelogramo fundamental são essenciais para o entendimento do Teorema de Minkowski e suas aplicações.

Como mencionado anteriormente, estes são conceitos fundamentais dentro da Geometria dos Números.

Neste capítulo, além de suas definições, serão apresentados alguns exemplos.

Assumiremos a definição a seguir de SOUZA, P.H.C [8] (2018, p.22)

Definição 15. *Um reticulado no $\mathbb{R}^n$ é um conjunto $\Lambda \subset \mathbb{R}^n$ gerado por todas as suas combinações $\mathbb{Z}$-lineares de n vetores linearmente independentes, isto é,*

$$\Lambda = \{a_1 w_1 + a_2 w_2 + \cdots + a_n w_n \mid a_i \in \mathbb{Z}\}$$

para alguma base $\omega = \{w_1, w_2, \cdots, w_n\}$ de $\mathbb{R}^n$.

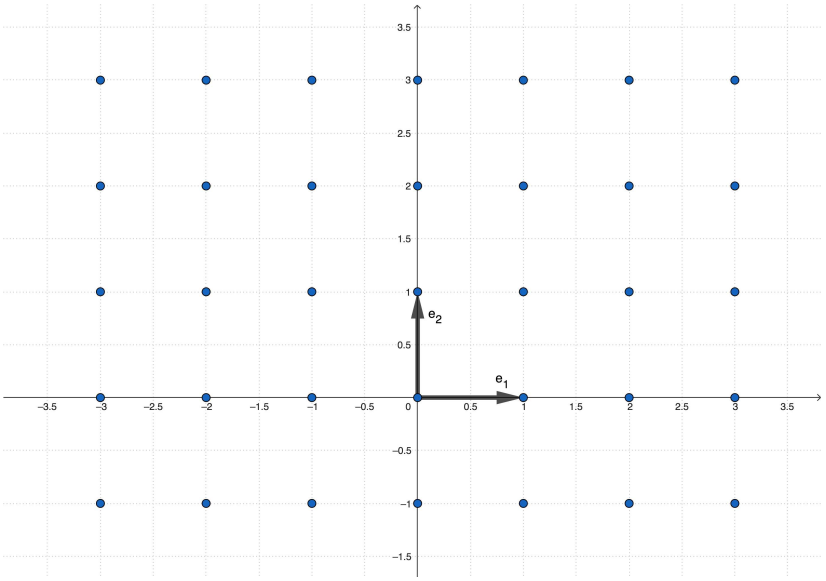
Ou seja, dada uma base ω de $\mathbb{R}^n$, o reticulado associado a essa base é o conjunto dos pontos obtidos pelas combinações lineares de coeficientes inteiros dos vetores $w_i \in \omega$.

Exemplo 4.2.1. *Dada a base canônica $\mathcal{C} = \{(1,0),(0,1)\}$, o reticulado Λ_1 associado é dado por:*

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

Na figura 6 é possível verificar os pontos que pertencem ao reticulado $\mathbb{Z}^2$. Todos estes podem ser escritos como combinação $\mathbb{Z}$-linear dos vetores da base $\mathcal{C}$.

Figura 6 – Reticulado dos Inteiros - $\mathbb{Z}^2$.

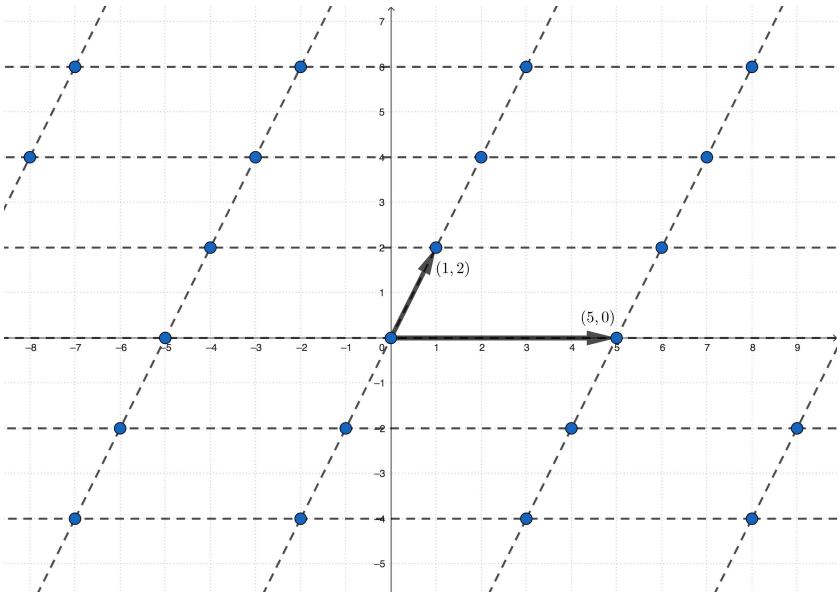


Exemplo 4.2.2. *Dada a base* $B = \{(1,2),(5,0)\}$*, o reticulado* Λ_2 *associado é dado por:*

$$\Lambda_2 = \{i \cdot (1,2) + j \cdot (5,0) \in \mathbb{R}^2 \mid i,j \in \mathbb{Z}\} = \{(i+5j, 2i) \in \mathbb{R}^2 \mid i,j \in \mathbb{Z}\}$$

Na figura 7 estão determinados os pontos que pertencem ao reticulado Λ_2, que podem ser expressos como combinações $\mathbb{Z}$-lineares dos vetores da base Λ_2.

Figura 7 – Reticulado Λ_2.



Definição 16. *Dada uma base* $\omega = \{w_1, w_2, \cdots, w_n\}$ *de um reticulado* $\Lambda \subset \mathbb{R}^n$*, o* ***paralelogramo fundamental*** $P(\omega)$ *é definido por*

$$P(\omega) = \{\beta_1 w_1 + \beta_2 w_2 + \cdots + \beta_n w_n \mid 0 \leq \beta_i < 1\}$$

Definição 17. *Seja* Λ *um reticulado no* $\mathbb{R}^n$*. Definimos como* $vol(\Lambda) = |det(w_1, w_2, \cdots, w_n)|$*, o* ***volume*** *do paralelogramo fundamental associado à base* $\{w_1, w_2, \cdots, w_n\}$*.*

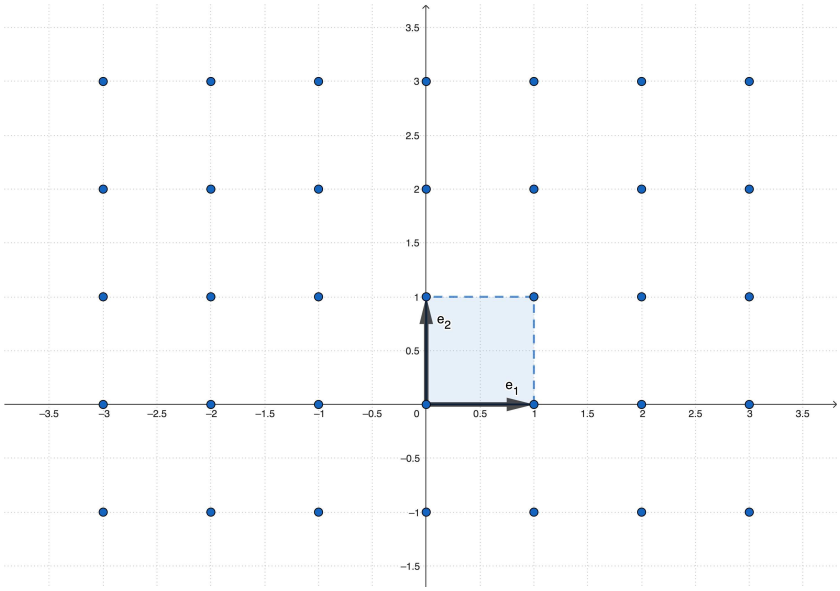
No $\mathbb{R}^2$, este $vol(\Lambda)$ será chamado de **elemento de área do reticulado** e seu cálculo permanecerá associado ao valor do determinante da matriz que possui como linhas os elementos da base (SOUZA, P.H.C [8], 2018).

No caso específico do $\mathbb{Z}^2$, citado no exemplo 4.2.1, temos que

$$vol(\mathbb{Z}^2) = \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix} = 1$$

e seu paralelogramo fundamental pode ser observado na figura 8.

Figura 8 – Paralelogramo Fundamental de $\mathbb{Z}^2$.



4.3 RELAÇÃO DE EQUIVALÊNCIA

Definição 18. *Dizemos que uma relação R sobre um conjunto A é uma relação de equivalência se R for simultaneamenta reflexiva, simétrica e transitiva.*

Definição 19. *Sejam A um conjunto não vazio, $R \subset A \times A$ uma relação de equivalência de A em A e $a \in A$. Definimos a classe de equivalência do elemento $a \in A$, denotada por $\bar{a}$, por:*

$$\bar{a} \stackrel{def}{=} \{x \in A \mid (x,a) \in R\}$$

Definição 20. *Sejam A um conjunto não vazio e $R \subset A \times A$ uma relação de equivalência em A. Definimos o* ***conjunto quociente*** *de A por R, denotado A/R, por:*

$$A/R \stackrel{def}{=} \{\bar{x}, \forall x \in A\}$$

Definição 21. *Dado o reticulado $\Lambda \subset \mathbb{R}^n$, escrevemos*

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

Verifica-se que a relação definida acima é uma relação de equivalência em $\mathbb{R}^n$. O paralelogramo fundamental do reticulado Λ contém exatamente um elemento de cada classe de equivalência, e portanto pode ser visto como o quociente $\mathbb{R}^n/\Lambda$.

Exemplo 4.3.1. *Dado o reticulado $\mathbb{Z}^2$, escrevemos*

$$a \equiv b(mod\ \mathbb{Z}^2) \Leftrightarrow a - b \in \mathbb{Z}^2, (a,b \in \mathbb{R}^2)$$

Verifica-se que a relação definida acima é uma relação de equivalência em $\mathbb{R}^2$. O paralelogramo fundamental do reticulado $\mathbb{Z}^2$ contém exatamente um elemento de cada classe de equivalência, e portanto pode ser visto como o quociente $\mathbb{R}^2/\mathbb{Z}^2$.

4.4 O TEOREMA DE MINKOWSKI

Para a apresentação do Teorema de Minkowski é importante conhecer a definição de conjuntos convexos.

Definição 22. *Um conjunto $V \subset \mathbb{R}^n$ é dito **convexo** quando dados $x,y \in V$, o segmento*

$$[x,y] = \{(1-t)x + ty \mid t \in [0,1]\}$$

estiver inteiramente contido em V.

Teorema 4.4.1. *(Teorema de Minkowski) Considere o reticulado $\Lambda \subset \mathbb{R}^n$ e seja $V \subset \mathbb{R}^n$ um conjunto tal que:*

1. *V é simétrico em relação à origem. Ou seja, $v \in V \Leftrightarrow -v \in V$*
2. *V é convexo.*
3. *$vol(V) > 2^n.vol(\Lambda)$*

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

Demonstração:

Vamos considerar P o paralelogramo fundamental determinado a partir dos vetores LI da base do reticulado Λ e considere o seguinte conjunto $\frac{1}{2}V = \left\{\frac{v}{2} \mid v \in V\right\}$.

Determinado o quociente $\frac{1}{2}V/\Lambda$, iremos particionar o conjunto $\frac{1}{2}V$ em uma quantidade enumerável de subconjuntos U_i com o objetivo de transladar cada um destes subconjuntos para dentro do paralelogramo fundamental a partir de translações τ_i do reticulado Λ.

De fato, como

$$vol\left(\frac{1}{2}V\right) = \frac{1}{2^n}vol(V) > \frac{1}{2^n}2^n.vol(\Lambda) = vol(\Lambda) = vol(P),$$

podemos concluir que existem $i \neq j$ tais que $(\tau_i + U_i) \cap (\tau_j + U_j) \neq \varnothing$. Ou seja, uma vez que a união de todas partições somam um volume maior que volume do paralelogramo fundamental, certamente haverá sobreposição de pelo menos 2 desses subconjuntos após suas respectivas translações para o interior do paralelogramo fundamental.

Considerando os pontos $\frac{v}{2} \in (\tau_i + U_i)$ e $\frac{w}{2} \in (\tau_j + U_j)$ dois pontos sobrepostos dessas translações, com $v \in V$, $w \in V$ e $v - w \neq 0$, temos

$$\frac{v}{2} \equiv \frac{w}{2}(mod\ \Lambda) \Leftrightarrow \frac{v}{2} - \frac{w}{2} = \frac{v-w}{2} \in \Lambda$$

.

Uma vez que V é simétrico em relação à origem, temos que $w \in V \Rightarrow -w \in V$. Entretanto, V é também um conjunto convexo, logo $v \in V, -w \in V \Rightarrow \frac{v-w}{2} \in V$. Portanto, $\frac{v-w}{2} \neq 0$, pertence ao reticulado Λ e também ao conjunto V. ■

Exemplo 4.4.1. *Para ilustrar a demonstração do Teorema de Minkowski vamos considerar o reticulado $\mathbb{Z}^2 \subset \mathbb{R}^2$ e seja V um conjunto convexo e simétrico em relação à origem. Note que para o reticulado $\mathbb{Z}^2$, o volume seu paralelogramo fundamental é*

$$vol(\mathbb{Z}^2) = det((1,0),(0,1)) = 1$$

Para satisfazer todas as condições do Teorema de Minkowski, seja V um conjunto convexo e simétrico em relação à origem no qual

$$vol(V) > 2^2.vol(\mathbb{Z}^2) = 4$$

Inicialmente considere o conjunto $\frac{1}{2}V = \left\{\frac{v}{2} \mid v \in V\right\}$. Pode-se concluir que se

$$vol(V) > 4 \Rightarrow vol\left(\frac{1}{2}V\right) > \frac{1}{2^2}vol(V) = \frac{1}{4} \cdot 4 = 1$$

Na figura 9 está representado o conjunto $\frac{1}{2}V$ e o reticulado $\mathbb{Z}^2$.

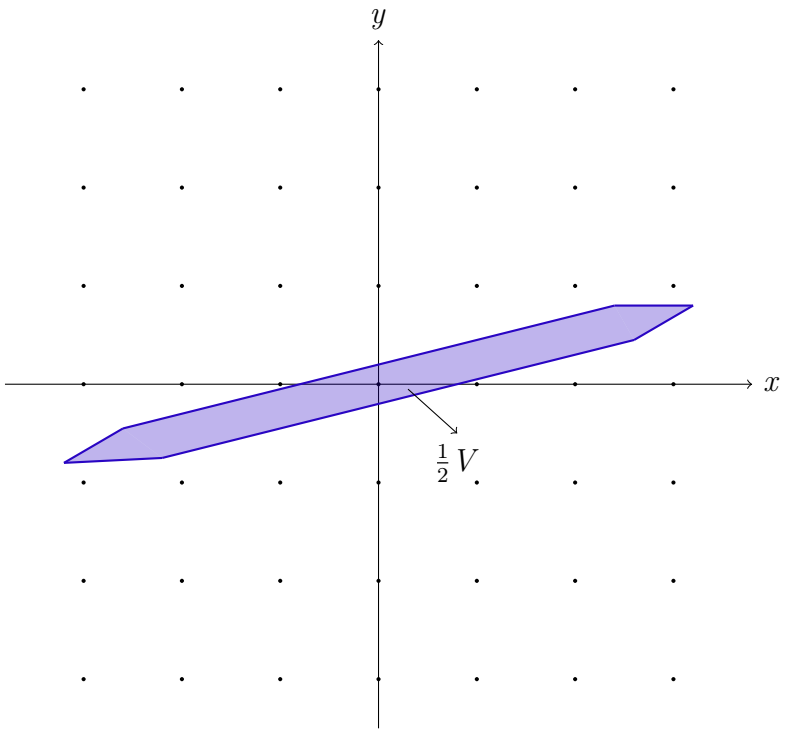


Figura 9 – Conjunto $\frac{1}{2}V$ e o Reticulado $\mathbb{Z}^2$.

Seguindo com a ideia apresentada no Teorema de Minkowski, dado o quociente $\frac{1}{2}V/\mathbb{Z}^2$, podemos particionar $\frac{1}{2}V$ em uma quantidade enumerável de subconjuntos U_i conforme a figura 10.

Assim, como $vol(\frac{1}{2}V) > vol(\mathbb{Z}^2) = 1$, transladando os subconjuntos U_i para dentro do paralelogramo fundamental a partir translações inteiras, existirão pelo menos dois subconjuntos sobrepostos. Ou seja, existem $i \neq j$ tais que $(\tau_i + U_i) \cap (\tau_j + U_j) \neq \varnothing$. Pode-se constatar este fato na figura 11 e 12.

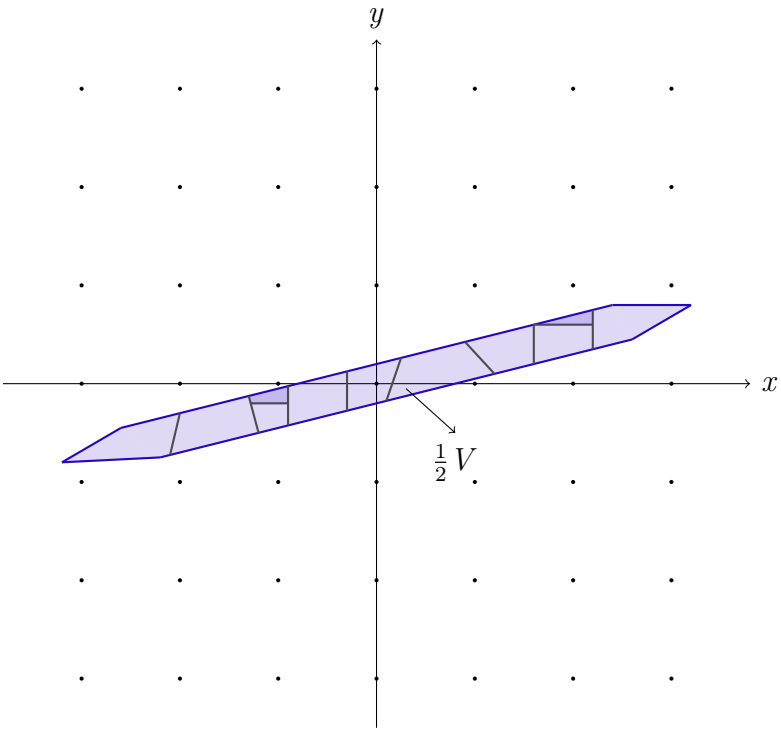


Figura 10 – Conjunto $\frac{1}{2}V$ particionado em subconjuntos.

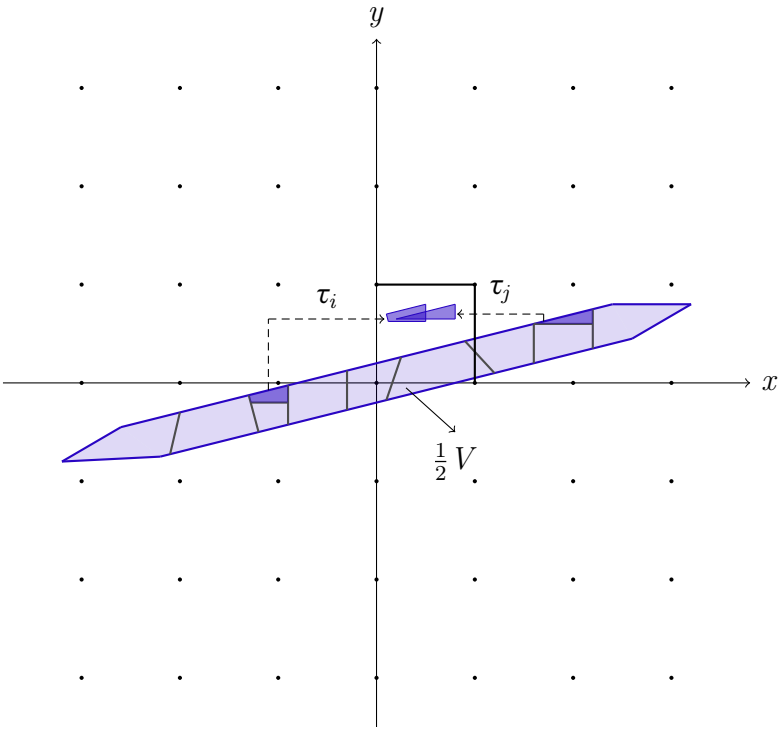


Figura 11 – Translações τ_i para o paralelogramo fundamental.

Para concluir o exemplo, dados os pontos sobrepostos $\frac{v}{2} \in (\tau_i + U_i)$ *e* $\frac{w}{2} \in (\tau_j + U_j)$*, com* $v \in V$*,* $w \in V$ *e* $v - w \neq 0$*, temos*

$$\frac{v}{2} \equiv \frac{w}{2}(mod\ \mathbb{Z}^2) \Leftrightarrow \frac{v}{2} - \frac{w}{2} = \frac{v-w}{2} \in \mathbb{Z}^2$$

.

Ou seja, encontramos dois pontos não nulos de subconjuntos distintos que são equivalentes pela relação de equivalência que usamos neste teorema.

Sendo V simétrico em relação à origem, temos que $w \in V \Rightarrow -w \in V$*. Assim, sabemos que V é também um conjunto convexo, logo* $v \in V, -w \in V \Rightarrow \frac{v-w}{2} \in V$*. Portanto,* $\frac{v-w}{2} \neq 0$ *, pertence ao reticulado* $\mathbb{Z}^2$ *e também ao conjunto* V*.*

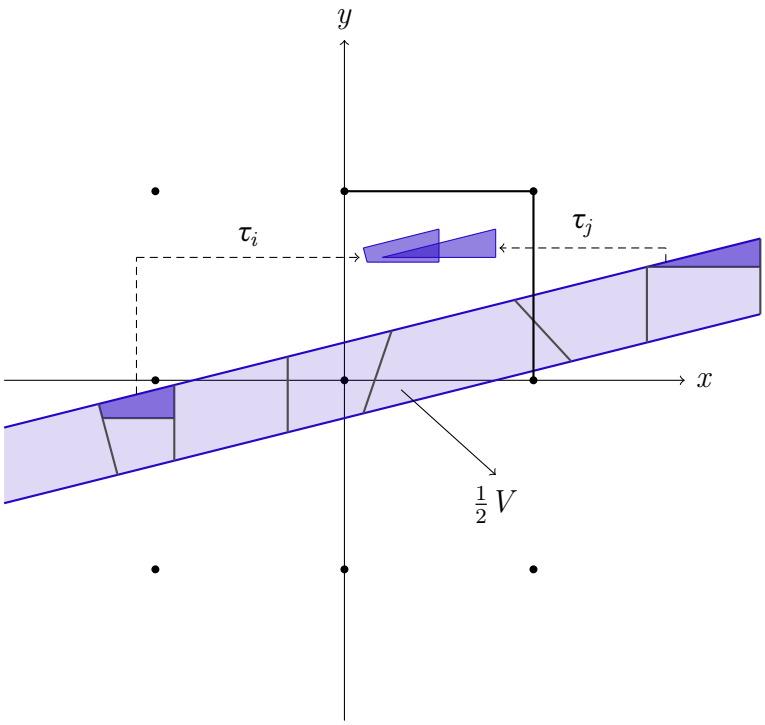


Figura 12 – Intersecção não vazia de $(U_i + _i)$ e $(U_j + _j)$.

4.5 APLICAÇÕES DO TEOREMA DE MINKOWSKI

Nesta sessão serão apresentados algumas aplicações do Teorema de Minkowski relacionadas a representação de inteiros como soma de quadrados, resultados conhecidos da Teoria dos Números.

A seguir caracterizamos os números primos que possuem representação como soma de dois quadrados e demonstraremos o teorema de Lagrange sobre a representação de inteiros como soma de quatro quadrados.

4.5.1 Soma de dois quadrados

O livro *Introdução à Teoria dos Números* (SANTOS, J.P.O. [1], 2003) apresenta os seguintes resultados que caracterizam números primos através de soma de quadrados.

Teorema 4.5.1. *Sendo p um primo a equação $x^2 + y^2 = p$ possui solução inteira se, e somente se, $p = 2$ ou $p \equiv 1(mod\ 4)$*

4.5.1.1 Demonstração

Observamos, inicialmente, que para $p = 2$ o resultado do enunciado do teorema é imediato, pois $2 = 1^2 + 1^2$.

Nos resta mostrar que todo primo p satisfazendo $p \equiv 1(mod\ 4)$ pode ser expresso como soma de dois quadrados.

Para tal demonstração, precisamos mostrar que -1 é resíduo quadrático de p satisfazendo $p \equiv 1(mod\ 4)$, ou seja, $p = 4k + 1$ com $k \in \mathbb{Z}$. Aplicando o Critério de Euler para o resíduo -1 e o primo $p = 4k + 1$, temos

$$\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2}(mod\ p)$$

$$\left(\frac{-1}{4k+1}\right) \equiv (-1)^{(4k+1-1)/2}(mod\ p)$$

$$\left(\frac{-1}{4k+1}\right) \equiv (-1)^{(4k)/2} \equiv (-1)^{2k}(mod\ p)$$

Como $k \in \mathbb{Z}$ chegamos a -1 elevado a um número par, portanto $(-1)^{2k} = 1$.

Assim, temos que $\left(\frac{-1}{p}\right) = 1$ para todo primo p ímpar tal que $p \equiv 1(mod\ 4)$. Ou seja, -1 é um resíduo quadrático de p.

Então temos $q \in \mathbb{Z}$ que é solução de $q^2 \equiv -1(mod\ p)$. Tome $z_1 = (1,q)$, $z_2 = (0,p)$ os dois vetores do reticulado $\Lambda = \Lambda(z_1,z_2)$.

Logo, $det(\Lambda) = \begin{vmatrix} 1 & q \\ 0 & p \end{vmatrix} = p$.

Considere $C = \{(x,y) : x^2 + y^2 < 2p\}$ em $\mathbb{R}^2$, então temos que

$$vol(C) = 2\pi p > 4p = 2^2.det(\Lambda)$$

De acordo com o Teorema de Minkowski, temos que C contém um ponto $(a,b) \in \Lambda \setminus 0$. Logo $(a,b) = iz_1 + jz_2 = (i, iq + jp) \in \mathbb{R}^2$, com $i,j \in \mathbb{Z}$, que implica

$$a^2 + b^2 = i^2 + (iq + jp)^2 \equiv i^2(q^2 + 1) \equiv 0 \ (mod\ p)$$

De fato, temos também que $0 < a^2 + b^2 < 2p$, o que garante que $a^2 + b^2 = p$. ■

4.5.2 Soma de quatro quadrados

Teorema 4.5.2. *(Teorema dos quatro quadrados de Lagrange)*

Para $n \in \mathbb{N}$, sempre podemos encontrar $a, b, c, d \in \mathbb{Z}$ tais que $n = a^2+b^2+c^2+d^2$. Ou seja, todo inteiro positivo possui representação como soma de quatro quadrados.

Demonstração:

Suponha que a fatoração em primos de de n seja $n = p_1^{a_1}.p_2^{a_2}.\cdots.p_k^{a_k}$. Para provar o teorema, precisamos apenas nos preocupar com o caso no qual $a_1, a_2, \cdots, a_k \in \{0,1\}$. Por exemplo, o número $216 = 2^3 \cdot 3^3$. Uma vez que podemos escrever $216 = 2^2 \cdot 3^2(2 \cdot 3)$, basta provar que se podemos escrever o fator $(2 \cdot 3)$ como soma de quatro quadrados, o número 216 também será escrito como soma de quatro quadrados. Ou seja,

$$216 = 2^2 \cdot 3^2(2 \cdot 3)$$

$$216 = 2^2 \cdot 3^2(a^2 + b^2 + c^2 + d^2)$$

$$216 = 2^2 \cdot 3^2 \cdot a^2 + 2^2 \cdot 3^2 \cdot b^2 + 2^2 \cdot 3^2 \cdot c^2 + 2^2 \cdot 3^2 \cdot d^2$$

$$216 = (2 \cdot 3 \cdot a)^2 + (2 \cdot 3 \cdot b)^2 + (2 \cdot 3 \cdot c)^2 + (2 \cdot 3 \cdot d)^2$$

Isto se deve ao fato que todo quadrado multiplicado por uma potência de expoente par sempre poderá ser escrito como o quadrado de um número.

Afirmamos que existem $x,y \in \mathbb{Z}$ tais que $x^2 + y^2 \equiv -1(mod\ n)$. Inicialmente vamos considerar $n = p$ primo. Se $p = 2$ a solução é trivial. Vamos considerar os casos que p é ímpar. Sendo p um primo ímpar, se $\left(\frac{-1}{p}\right) = 1$, ou seja, um primo da forma $p \equiv 1(mod\ 4)$, então temos $a^2 \equiv -1(mod\ p)$ para algum a. Tomando $x = a$ e $y = 0$ está satisfeita a equivalência proposta.

Vamos considerar agora os primos da forma $p \equiv 3(mod\ 4)$, tais que $\left(\frac{-1}{p}\right) = -1$. Assim, sejam os pares residuais $(0,p-1),(1,p-2),...,(\frac{p-1}{2},\frac{p-1}{2})$, que totalizam $\frac{p+1}{2}$ pares. Destes, temos que 0 e $p-1$ não serão resíduos quadráticos de p. Dos $\frac{p-1}{2}$ pares restantes, o último sempre aparecerá com resíduos quadráticos iguais. Se este par de resíduos iguais satisfizer a afirmação $x^2 + y^2 \equiv -1(mod\ n)$, encontramos uma solução. Senão, restam $\frac{p-3}{2}$ pares de resíduos quadrático. Podemos concluir que dois dos $\frac{p-1}{2}$

resíduos aparecerão juntos em um dos $\frac{p-3}{2}$ pares restantes, pelo princípio das casas dos pombos. Note que isto equivale a preencher $p-3$ espaços com $p-3$ restos da divisão de p, mas desses, $\frac{p-1}{2}$ sendo resíduos quadráticos. Ou seja $\frac{p-1}{2} = \frac{p-3}{2}+1$. Então podemos concluir que a afirmação $x^2+y^2 \equiv -1(mod\ n)$ terá solução também para um primo da forma $p \equiv 3(mod\ 4)$.

Resta agora mostrar que a afirmação $x^2+y^2 \equiv -1(mod\ n)$ vale também para n sendo um produto de primos, ou seja, para qualquer número natural. Vamos considerar n um produtos de primos do tipo $n = p_1p_2\cdots p_k$, sendo p_i números primos. Para cada primo p_i da fatoração de n, podemos dizer que existem $a_i^2+b_i^2 \equiv -1(mod\ p_i)$. Este resultado foi mostrado acima para $p=2$ e também para todo p primo ímpar. De fato, para cada p_i encontraremos uma solução do tipo $a_i \equiv c_i(mod\ p_i)$ e também um $b_i \equiv d_i(mod\ p_i)$.

Obtidos esses resultados, vamos buscar por uma solução que atenda simultaneamente todas as equações $a_i \equiv c_i(mod\ p_i)$ e também para todas equações $b_i \equiv d_i(mod\ p_i)$, para cada p_i da fatoração de n.

$$\begin{cases} x \equiv a_1(mod\ p_1) \\ x \equiv a_2(mod\ p_2) \\ \quad\vdots \\ x \equiv a_k(mod\ p_k) \end{cases} \qquad \begin{cases} y \equiv b_1(mod\ p_1) \\ y \equiv b_2(mod\ p_2) \\ \quad\vdots \\ y \equiv b_k(mod\ p_k) \end{cases}$$

Perceba que se houver solução para cada sistema acima, esta deverá ser a mesma solução para x e y da congruêcia que queremos provar,

$$x^2+y^2 \equiv -1(mod\ p_1p_2\cdots p_k).$$

Pelo Teorema Chinês do Resto, a condição que $(p_i,p_j)=1$ para $i \neq j$ é satisfeita, por serem todos primos. Sendo assim, ambos os sistemas possuem solução única módulo $n = p_1p_2\cdots p_k$ e o resultado $x^2+y^2 \equiv -1(mod\ n)$ está provado para todo $n \in \mathbb{N}$.

Desta forma, seja $a^2+b^2 \equiv -1(mod\ n)$ a solução desta congruência e considere o seguinte reticulado:

$$\Lambda := \{(nx_1+ax_3+bx_4, nx_2+bx_3-ax_4, x_3, x_4) : x_1,x_2,x_3,x_4 \in \mathbb{Z}\}$$

com a base $v_1 = (n,0,0,0)$, $v_2 = (0,n,0,0)$, $v_3 = (a,b,1,0)$ e $v_4 = (b,-a,0,1)$.

Uma vez que

$$vol(\Lambda) = |Det(\vec{v_1},\vec{v_2},\vec{v_3},\vec{v_4})| = \begin{vmatrix} n & 0 & 0 & 0 \\ 0 & n & 0 & 0 \\ a & b & 1 & 0 \\ b & -a & 0 & 1 \end{vmatrix} = n^2$$

O volume de uma esfera no $\mathbb{R}^4$ é calculado por uma integral e não será demonstrado neste trabalho. Deste modo, usaremos o resultado a seguir para calcular o volume de

uma esfera de raio R no espaço n-dimensional: $V_n = \frac{\pi^{\frac{n}{2}}}{\frac{n}{2}\Gamma\left(\frac{n}{2}\right)}R^n$, com $\Gamma(\frac{1}{2}) = \pi^{\frac{1}{2}}$ e $\Gamma(z) = (z-1)!$ para um inteiro positivo z.

Seja $B \subseteq \mathbb{R}^4$ uma bola aberta de raio $\sqrt{2n}$ centrada na origem. Temos que

$$Vol(B) = \frac{\sqrt{\pi^4}}{\frac{4}{2}\Gamma\left(\frac{4}{2}\right)}(\sqrt{2n})^4 = 2n^2\pi^2 > 2^4n^2 = 2^4Det(\Lambda)$$

De acordo com o Teorema de Minkowski, o conjunto B possui um ponto do reticulado Λ diferente da origem. Uma vez que

$$(nx_1 + ax_3 + bx_4)^2 + (nx_2 + bx_3 - ax_4)^2 + x_3^2 + x_4^2 \equiv a^2x_3^2 + b^2x_4^2 + b^2x_3^2 + a^2x_4^2 + x_3^2 + x_4^2 \equiv$$

$$\equiv x_3^2(a^2 + b^2 + 1) + x_4^2(a^2 + b^2 + 1) \equiv (a^2 + b^2 + 1)(x_3^2 + x_4^2) \equiv 0(mod\ n)$$

e que o raio desta bola em $\mathbb{R}^4$ é menor que $\sqrt{2n}$, segue:

$$0 < (nx_1 + ax_3 + bx_4)^2 + (nx_2 + bx_3 - ax_4)^2 + x_3^2 + x_4^2 < 2n$$

e podemos concluir que

$$(nx_1 + ax_3 + bx_4)^2 + (nx_2 + bx_3 - ax_4)^2 + x_3^2 + x_4^2 = n$$

Isto prova o teorema quando n é ímpar.

Suponha agora que n é um número par. Escrevendo $n = 2^v m$, onde m e v são inteiros positivos e admitindo o fato que $2 \nmid m$, podemos encontrar $x_1, x_2, x_3, x_4 \in \mathbb{Z}$ tais que $m = x_1^2 + x_2^2 + x_3^2 + x_4^2$.

Se v é par, então

$$n = (2^{v/2}x_1)^2 + (2^{v/2}x_2)^2 + (2^{v/2}x_3)^2 + (2^{v/2}x_4)^2$$

Se v é ímpar, então

$$n = \left[2^{(v-1)/2}(x_1 + x_2)\right]^2 + \left[2^{(v-1)/2}(x_1 - x_2)\right]^2 + \left[2^{(v-1)/2}(x_3 + x_4)\right]^2 + \left[2^{(v-1)/2}(x_3 - x_4)\right]^2$$

Isto completa a prova do teorema.

■

5 UMA PROPOSTA DE ATIVIDADE PARA O ENSINO MÉDIO

No anexo A deste trabalho propõe-se uma atividade para o Ensino Médio, a cerca dos resultados encontrados no Capítulo 4 deste trabalho. Inicialmente, esta atividade será apresentada e logo após trataremos de suas respectivas análises e respostas. Após a realização desta atividade, propõe-se a análise e resolução de um problema da Olímpiada Brasileira de Matemática sobre o assunto soma de quadrados.

Esta atividade tem como objetivo propor que o estudante do Ensino Médio compreenda os resultados dos teoremas que caracterizam a representação de números inteiros como soma de dois ou quatro quadrados.

A partir de estimativas será possível observar que, por mais que o assunto possa ser considerado aprofundado em Matemática, é possível que esses estudantes possam compreender e aplicar os resultados dos teoremas, inclusive com certa facilidade em alguns casos.

A partir desta motivação, estes estudantes podem perceber que mesmo teorias matemáticas avançadas para o nível escolar básico, podem gerar resultados simples e de fácil entendimento.

6 CONCLUSÃO

Este trabalho compilou diversos assuntos estudados no mestrado profissional Profmat, tais como bases de espaços vetoriais, volume de sólidos formados por vetores linearmente independentes, o conjunto dos números inteiros, a divisibilidade, os números primos, relação de equivalência, a congruência módulo n e resíduos quadráticos. Teve como motivação o Teorema de Minkowski, que é base para o desenvolvimento da Geometria dos Números.

Os principais resultados apresentados nesta dissertação são as aplicações do Teorema de Minkowski para a soma de quadrados. Uma das caracterísiticas mais marcantes deste trabalho é como a Geometria dos Números integra muitas outras áreas da Matemática como Álgebra Pura, Álgebra Linear, Aritmética, Geometria e Cálculo.

A partir de ampla pesquisa bibliográfica, foi possível redigir um texto acessível para o entendimento dos conceitos e resultados fundamentais deste trabalho.

Por fim, podemos concluir que existem muitas possibilidades para aplicações de conceitos algébricos no Ensino Médio e no treinamento para Olimpíadas com a finalidade de estimular o desenvolvimento da Matemática também dentro do âmbito escolar.

REFERÊNCIAS

[1] SANTOS, J.P.O. *Introdução à Teoria dos Números*. Coleção Matemática Universitária, IMPA, RJ 2004.

[2] MARTINS, Sérgio Tadao. TENGAN, Eduardo. *Álgebra Exemplar*. Projeto Euclides, IMPA, RJ 2020.

[3] STEINBRUCH, A. WINTERLE, P. *Álgebra Linear*. Pearson, SP 2012.

[4] STEINBRUCH, A. WINTERLE, P. *Geometria Analítica*. Pearson, SP 2012.

[5] FAN, Esteve. *On Geometric Proofs of Theorems on Sums of Squares*. Department of Mathematics, Dartmouth College, Hanover USA 2012 - Disponível em `https://math.dartmouth.edu/~stevefan/papers/OnGeometricProofsofTheoremsonSumsofSquares.pdf`.

[6] DONG, Zichao. *Minkowski's Theorem and Its Applications*. Department of Mathematical Sciences - Carnegie Mellon University, Pittsburgh USA 2019 - Disponível em `https://www.math.cmu.edu/~ttkocz/teaching/1819/read-sem-notes.pdf`.

[7] IUSENKO, Kostiantyn (USP). *Álgebra I para Licenciatura*. Notas de aula - USP 2021 - Disponível em `https://www.ime.usp.br/~iusenko/ensino_2021_1/`.

[8] SOUZA, P.H.C. *Teorema de Minkowski e Aplicações*. Trabalho de Conclusão de Curso - UFSJ - Juiz de Fora MG - 2018.

[9] BARROS, F.V.D.C. *O método de Minkowski e a representação de um inteiro como soma de quadrados*. Dissertação de Mestrado - URCA - Juazeiro do Norte CE - 2020.

[10] *Hermann Minkowski Biography* Mac Tutor Site - School of Mathematics and Statistics - University of St. Andrews - Escócia . Disponível em `https://mathshistory.st-andrews.ac.uk/Biographies/Minkowski/`.

[11] CASSELS, J.W.S *An Introduction to the Geometry Numbers*. Editora Springer, Nova Iorque - 1971.

[12] STROBL, W. *Aus den wissenschaftlichen Anfängen Hermann Minkowskis*. Historia Mathematica 12 (2), 142-156, 1985.

[13] CORRY, L., *The influence of David Hilbert and Hermann Minkowski on Einstein's views over the interrelation between physics and mathematics*, Endeavor 22 (3), 95-97, 1988.

Anexos

ANEXO A – PRODUTO EDUCACIONAL

Produto Educacional

Teorema de Minkowski e suas aplicações

João Figueiredo Penaforte

Universidade Federal de Santa Catarina

Campus Florianópolis

Programa de Pós Graduação Mestrado Profissional em Matemática em Rede Nacional - PROFMAT

Coordenação Dra. Maria Inez Cardoso Gonçalves

Dissertação do Profmat Este ebook é um produto oriundo da dissertação do PROFMAT intitulada "Teorema de Minkowski e suas aplicações" defendida em 2024

Autor João Figueiredo Penaforte

Orientador Dr. Sérgio Tadao Martins

”A matemática é a única linguagem
que temos em comum com a natureza.”
(Stephen Hawking)

Carta ao leitor

Prezado Leitor,

Compartilho com você este material criado a partir da minha dissertação feita para o Programa de Mestrado Profissional em Matemática (Profmat). Neste material estão compilados alguns problemas sobre a natureza de números que podem ser escritos como somas de quadrados.

Busquei elencar problemas que trazem características diversas sobre as possibilidades de um número ser escrito como soma de alguns quadrados e formas de desenvolver demonstrações matemáticas a partir de alguns resultados conhecidos.

Desejo que este conteúdo seja de grande valor para você, que seja fonte de inspiração para o desenvolvimento de seus estudos e aprofundamento na Matemática. Agradeço antecipadamente pela sua atenção e interesse pelo meu trabalho.

Atenciosamente,

João Penaforte.

Sumário

Capítulo 1

Introdução

O assunto de soma de quadrados de números inteiros é conhecido pelos estudantes do Ensino Médio especialmente quando se trata do Teorema de Pitágoras.

De fato, a partir do Teorema de Pitágoras, é possível chegar a diversos números que podem ser escritos como soma de dois números inteiros elevados ao quadrado. Sabe-se que, num triângulo retângulo, o quadrado do comprimento de sua hipotenusa é sempre igual a soma dos quadrados dos comprimentos dos catetos.

Com o objetivo de desenvolver uma percepção um pouco mais investigativa a cerca da natureza dos números, quais seriam os números que podem ser escritos como soma de dois quadrados? Existem números que podem ser escritos como soma de quatro quadrados? Quais são as justificativas para essas perguntas?

Nesta atividade será proposta uma abordagem investigativa a cerca dessas características citadas acima sobre números inteiros. Através de um investigação minunciosa é possível criar estratégias para resolução dos problemas propostos e também desenvolver algumas demonstrações matemáticas em nível do Ensino Médio.

Este assunto é, por vezes, abordado em questões de Olimpíadas de Matemática. Por este motivo, mostraremos a resolução de um problema olímpico utilizando os resultados encontrados nesta atividade.

1.1 Plano de aula

1.1.1 Conteúdo

Soma de quadrados

1.1.2 Objetivos

1. Estimar e caracterizar números que podem ser escritos como soma de quadrados
2. Desenvolver um demonstração matemática

1.1.3 Base Nacional Comum Curricular

1. **Unidade Temática**: Números e Álgebra
2. **Objetos do Conhecimento**: Propriedades algébricas sobre números que podem ser escritos como soma de quadrados.
3. **Habilidades**:

   (EM13MAT302) Construir modelos empregando as funções polinomiais de 1º ou 2º graus, para resolver problemas em contextos diversos, com ou sem apoio de tecnologias digitais.

   (EM13MAT510) Investigar conjuntos de dados relativos ao comportamento de duas variáveis numéricas, usando ou não tecnologias da informação, e, quando apropriado, levar em conta a variação e utilizar uma reta para descrever a relação observada.

(EM13MAT315) Investigar e registrar, por meio de um fluxograma, quando possível, um algoritmo que resolve um problema.

1.1.4 Linhas de Ação

1. **Tempo de Aula**: 50 minutos.

2. Apresentação dos Resultados importantes sobre Teoria de Números e desenvolvimento metodológico.

Capítulo 2

Soma de Quadrados

2.1 Soma de Quadrados

Neste capítulo serão apresentados resultados da Teoria dos Números que dizem respeito sobre números que podem ou não ser escritos como somas de quadrados.

Os teoremas terão seus resultados principais enunciados, mas não serão demonstrados matematicamente neste Produto Educacional. Isto pelo fato de tais resultados necessitarem de embasamento mais aprofundado em Álgebra.

2.1.1 Conceitos e Resultados importantes sobre somas de quadrados

Para esta atividade, todos os números são inteiros.

Definição 2.1. Para dado n inteiro positivo, dizemos que este poderá ser escrito como soma de quadrados se existirem x e y inteiros, tais que $n = x^2 + y^2$

1. (Identidade de Brahmagupta-Fibonacci)

Se r e s são somas de dois quadrados então $r \cdot s$ também é soma de dois quadrados.

2. Se n for um número inteiro, tal que n é da forma $4k + 3$, então n não pode ser representado como soma de dois quadrados.

3. Para todo número primo $p > 2$ temos que p pode ser escrito como soma de dois quadrados se, e somente se, $p = 4k + 1$.

4. Para todo inteiro não negativo n, existem a e b tais que $a^2 + b^2 + 1 = k \cdot n$, com k inteiro.

SOMA DE QUATRO QUADRADOS

5. Teorema de Lagrange: Todo inteiro n, não negativo, pode ser escrito como soma de quatro quadrados. Ou seja, existem inteiros a, b, c e d, tais que $n = a^2 + b^2 + c^2 + d^2$.

Capítulo 3

Exercícios

3.1 Problemas

Nesta capítulo propomos uma atividade para o Ensino Médio, a cerca dos resultados obtidos da dissertação Teorema de Minkowski e suas aplicações. Inicialmente, esta atividade será apresentada e logo após trataremos de suas respectivas análises e respostas.

Esta atividade tem como objetivo propor que o estudante do Ensino Médio compreenda os resultados dos teoremas que caracterizam a representação de números inteiros como soma de dois ou quatro quadrados.

A partir de estimativas será possível observar que, por mais que o assunto possa ser considerado aprofundado em Matemática, é possível que esses estudantes possam compreender e aplicar os resultados dos teoremas, inclusive com certa facilidade em alguns casos.

A partir desta motivação, estes estudantes podem perceber que mesmo teorias matemáticas avançadas para o nível escolar básico podem gerar resultados simples e de fácil entendimento.

3.2 Apresentação da Atividade Proposta

Segue abaixo a apresentação da atividade proposta, baseada nos resultados demonstrados a partir do Teorema de Minkowski. Os exercícios foram adaptados nos propósitos desta sequência didática com a finalidade de desenvolver a habilidade de identificação de números como soma de quadrados.

3.2.1 Atividade - Ensino Médio

Exercício 3.1

Sejam os números primos 7, 11, 19, 23, 29, 31 e 37. É possível escrever estes números como soma de dois quadrados? É possível escrever 13 como soma de dois quadrados, pois $13 = 3^2 + 2^2$.

Exercício 3.2

A partir da resposta anterior, verifique os restos das divisões deste números primos pelo número 4. É possível concluir alguma relação sobre a possibilidade de um número primo ser escrito como soma de dois quadrados?

Exercício 3.3

Ambos números 13 e 29 podem ser escritos como soma de dois quadrados. Se considerarmos o produto entre 13 e 29 poderíamos escrever tal resultado como soma de dois quadrados? Escreva $13 \cdot 29$ como soma de dois quadrados.

Exercício 3.4

É possível escrever o número 216 como soma de quatro quadrados? Escreva 216 como soma de quatro quadrados.

Exercício 3.5

Considere o divisor 54 do número 216. Pode-se perceber que 54 é o número consecutivo do número primo 53, que deixa resto 1 na divisão por 4. Existe alguma relação da soma de quatro quadrados com esse fato? Explique.

Exercício 3.6

Como forma de motivar o desenvolvimento de habilidades matemáticas no Ensino Médio, propõe-se a demonstração do Lema de Euler (1748):
Se m e n são somas de quatro quadrados, então o produto $m \cdot n$ também é uma soma de quatro quadrados.

Dica: Análogo ao resultado encontrado no exercício 3.3 que

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$$

sugere-se verificar se

$$(a^2+b^2+c^2+d^2)(r^2+s^2+t^2+v^2) = (ar+bs+ct+dv)^2+(as-br-cv+dt)^2+$$

$$+(at+bv-cr-ds)^2+(av-bt+cs-dr)^2$$

3.3 Problema da Olimpíada Brasileira de Matemática

Os temas relacionados com Teoria dos Números são frequentemente abordados em exames de Olimpíadas de Matemática. Neste capítulo mostraremos uma solução de um problema olímpico utilizando os conceitos desenvolvidos na Atividade da Seção anterio.

Exercício 3.7

(XXV OBM 2003 - Segunda Fase - Níveis 2 e 3) Dizemos que um número n de quatro algarismos é biquadrado quando é igual à soma dos quadrados de dois números: um é formado pelos dois primeiros algarismos de n, na ordem em que aparecem em n e o outro, pelos dois últimos algarismos de n, também na ordem em que aparecem em n.

Por exemplo, 1233 é biquadrado pois $1233 = 12^2 + 33^2$. Encontre um outro número biquadrado.

(**Observação:** Lembre-se que um número de quatro algarismos não pode começar com zero.)

APÊNDICE A

Soluções

Solução 3.1

Deste números, os que podem ser escritos como soma de dois quadrados são $17 = 4^2 + 1^2$, $29 = 5^2 + 2^2$ e $37 = 6^2 + 1^2$, os outros não podem. Esta primeira atividade, por meio de estimativas empíricas, oferece a oportunidade dos estudantes terem o primeiro contato com a ideia de poder representar um número como uma soma de dois quadrados. Assim, podem se preparar para a introdução do resultado geral.

Solução 3.2

A partir da divisão destes números por 4, pode-se observar que aqueles que deixam resto 1 são exatamente os que conseguimos escrever como soma de dois quadrados. Por outro lado, os primos que deixam resto 3 na divisão por 4 não podem ser escritos como soma de dois quadrados. Conclusão: os primos que deixam resto 1 na divisão por 4 e o número 2 podem ser escritos como soma de dois quadrados.

Solução 3.3

Esta demonstração está em nível de Ensino Médio e é uma maneira de estimular demonstrações matemáticas no âmbito escolar. Uma vez que $13 = 3^2 + 2^2$ e $29 = 5^2 + 2^2$, podemos verificar que

$$13 \cdot 29 = (3^2 + 2^2)(5^2 + 2^2) = 3^2 \cdot 5^2 + 3^2 \cdot 2^2 + 2^2 \cdot 5^2 + 2^2 \cdot 2^2 =$$

$$= (3^2 \cdot 5^2 + 2^2 \cdot 2^2) + (3^2 \cdot 2^2 + 2^2 \cdot 5^2)$$

Somando $2(3 \cdot 5)(2 \cdot 2)$ e subtraindo $2(3 \cdot 2)(2 \cdot 5)$ obtemos.

$$13 \cdot 29 = (3^2 \cdot 5^2 + 2(3 \cdot 5)(2 \cdot 2) + 2^2 \cdot 2^2) + (3^2 \cdot 2^2 - 2(3 \cdot 2)(2 \cdot 5) + 2^2 \cdot 5^2) =$$

$$= (5 \cdot 3 + 2 \cdot 2)^2 + (5 \cdot 2 - 2 \cdot 3)^2 = 19^2 + 4^2$$

Fica como sugestão apresentar a Identidade de Brahmagupta-Fibonacci que é uma outra maneira de encontrar números que podem ser escrito como soma de dois quadrados a partir da técnica algébrica apresentada acima.

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2 = (ac + bd)^2 + (ad - bc)^2$$

Solução 3.4

Sim, é possível. Observe que $216 = 10^2 + 10^2 + 4^2 + 0^2$.

Solução 3.5

Todo número, além de poder ser representado como soma de quatro quadrados, pode também ser escrito como múltiplo de um número resultante da soma de dois quadrados mais um. Como temos que o 53 é um primo que tem resto 1 na divisão por 4, sabemos que ele pode ser escrito como soma de dois quadrados, então:

$$216 = (53 + 1)(4) = (7^2 + 2^2 + 1)(2^2 + 0^2) =$$

$$= (7^2 2^2 + 7^2 0^2) + (2^2 2^2 + 2^2 0^2) + (2^2 + 0^2) =$$

$$= (7^2 2^2) + (2^2 2^2) + (2^2) + (0^2) = 14^2 + 4^2 + 2^2 + 0^2$$

Este resultado acima foi importante para verificar que não é única a forma de escrever um número como soma de 4 quadrados, pois

$$216 = 10^2 + 10^2 + 4^2 + 0^2 = 14^2 + 4^2 + 2^2 + 0^2$$

Solução 3.6

De fato, se $m = a^2 + b^2 + c^2 + d^2$ e $n = r^2 + s^2 + t^2 + v^2$, temos que

$$(a^2 + b^2 + c^2 + d^2)(r^2 + s^2 + t^2 + v^2) = (ar + bs + ct + dv)^2 + (as - br - cv + dt)^2 +$$

$$+(at + bv - cr - ds)^2 + (av - bt + cs - dr)^2$$

Vamos desenvolver ambos os lados da igualdade e assim obter o resultado desejado. Desenvolvendo o lado esquerdo da igualdade acima, temos:

$$(a^2 + b^2 + c^2 + d^2)(r^2 + s^2 + t^2 + v^2) =$$

$$= a^2r^2 + a^2s^2 + a^2t^2 + a^2v^2 + b^2r^2 + b^2s^2 + b^2t^2 + b^2v^2 +$$

$$+c^2r^2 + c^2s^2 + c^2t^2 + c^2v^2 + d^2r^2 + d^2s^2 + d^2t^2 + d^2v^2$$

Vamos agora desenvolver o lado direito da igualdade e comparar com o resultado obtido no lado esquerdo. Para isso, será desenvolvido cada quadrado separadamente. Então.

$$(ar + bs + ct + dv)^2 = (ar + bs)^2 + 2(ar + bs)(ct + dv) + (ct + dv)^2 =$$

$$= a^2r^2 + b^2s^2 + c^2t^2 + d^2v^2 + 2arct + 2ardv + 2bsct + 2bsdv + 2arbs + 2ctdv$$

Da mesma forma,

$$(as - br - cv + dt)^2 = (as - br)^2 + 2(as - br)(-cv + dt) + (-cv + dt)^2 =$$

$$= a^2s^2 + b^2r^2 + c^2v^2 + d^2t^2 - 2ascv + 2asdt + 2brcv - 2brdt - 2asbr - 2cvdt$$

Analogamente,

$$(at + bv - cr - ds)^2 = (at + bv)^2 + 2(at + bv)(-cr - ds) + (-cr - ds)^2 =$$

$$= a^2t^2 + b^2v^2 + c^2r^2 + d^2s^2 - 2atcr - 2atds - 2bvcr - 2bvds + 2atbv + 2crds$$

Por fim,

$$(av - bt + cs - dr)^2 = (av - bt)^2 + 2(av - bt)(cs - dr) + (cs - dr)^2 =$$

$$= a^2v^2 + b^2t^2 + c^2s^2 + d^2r^2 + 2avcs - 2avdr - 2btcs + 2btdr - 2avbt - 2csdr$$

Agora, somando (2), (3), (4) e (5), obtemos

$$(ar+bs+ct+dv)^2+(as-br-cv+dt)^2+(at+bv-cr-ds)^2+(av-bt+cs-dr)^2 =$$

$$= a^2r^2 + b^2s^2 + c^2t^2 + d^2v^2 + a^2s^2 + b^2r^2 + c^2v^2 + d^2t^2 +$$

$$+a^2t^2 + b^2v^2 + c^2r^2 + d^2s^2 + a^2v^2 + b^2t^2 + c^2s^2 + d^2r^2$$

Como ambos lados da igualdade em (1) e (6) dão o mesmo resultado, podemos concluir que

$$(a^2 + b^2 + c^2 + d^2)(r^2 + s^2 + t^2 + v^2) = (ar + bs + ct + dv)^2 + (as - br - cv + dt)^2 +$$

$$+(at + bv - cr - ds)^2 + (av - bt + cs - dr)^2$$

Solução 3.7

A ideia é separar o número de quatro dígitos em duas partes: os dois primeiros dígitos, da esquerda para a direita, formam o número x e os dois últimos formam o número y. Para verificar a condição do número ser biquadrado, chegamos em $100x + y = x^2 + y^2$. Desta forma, podemos considerar a equação $x^2 - 100x + y^2 - y = 0$. Com o objetivo se escrever as expressões em função de x e y como quadrados, utilizaremos a técnica de completamento de quadrados. Logo,

$$x^2 - 100x + y^2 - y = 0 \Leftrightarrow$$

$$4x^2 - 400x + 4y^2 - 4y = 0 \Leftrightarrow$$

$$4x^2 - 400x + 10000 + 4y^2 - 4y + 1 = 10000 + 1 \Leftrightarrow$$

$$(2x - 100)^2 + (2y - 1)^2 = 10001$$

Assim, pretendemos encontrar m e n tais que $m^2 + n^2 = 10001$, com m par e n ímpar.

Da fatoração em primos de 10001 temos que $10001 = 73 \cdot 137$. E observe que ambos 73 e 137 são primos do tipo $4k+1$, ou seja, podem ser escritos como soma de dois quadrados. Ou seja, $10001 = 73 \cdot 137 = (8^2 + 3^2)(11^2 + 4^2)$.

Sabe-se que se dois números podem ser escritos como somas de dois quadrados, então o produto dos mesmos também pode. Da Identidade de Brahmagupta-Fibonacci apresentada no exercício 3.3 temos que

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2 = (ac - bd)^2 + (ad + bc)^2$$

Aplicando o resultado da Identidade mencionada acima obtemos

$$(8^2 + 3^2)(11^2 + 4^2) = (8 \cdot 11 + 3 \cdot 4)^2 + (8 \cdot 4 - 3 \cdot 11)^2 = 100^2 + 1^2$$

$$(8^2+3^2)(11^2+4^2) = (8\cdot 4+3\cdot 11)^2+(8\cdot 11-3\cdot 4)^2 = 65^2+76^2$$

As duas maneiras de escrever 10001 como soma de dois quadrados são do tipo $(m,n) = (\pm 100, \pm 1)$ ou $(m,n) = (\pm 65, \pm 76)$ e suas permutações.

A partir da primeira solução encontra-se $2x - 100 = \pm 100$ que resulta em $x = 0$ ou $x = 100$, que não geram um número biquadrado, conforme enunciado no problema.

A partir da segunda solução encontra-se $2y - 1 = 65$ e $2x - 100 = \pm 76$ que resultam nos pares ordenados $(x,y) = (88, 33)$ ou $(x,y) = (12, 33)$.

Logo o outro número biquadrado é o 8833.

Referências Bibliográficas

MEC. *Base Nacional Comum Curricular*. Disponível em <http://basenacionalcomum.mec.gov.br/images/BNCC_EI_EF_110518_versaofinal_site.pdf>: Ministério da Educação, 2024.

NETO, A. P. *Mini Curso Soma de Quadrados*. Disponível em <https://im.ufal.br/evento/bsbm/download/minicurso/quadrados.pdf>: UFAL, 2014.

OBM. *Provas e Gabaritos*. Disponível em: <https://www.obm.org.br/como-se-preparar/provas-e-gabaritos/>.: Olimpíada Brasileira de Matemática, 2024.

SANTOS, J. E. C. dos. *Números Inteiros como Soma de Quadrados*. João Pessoa, PB: Dissertação de Mestrado Profmat, 2013.