UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
Faculdade de Ciências e Tecnologia
Câmpus de Presidente Prudente

Criptografia: uma aplicação via Reticulados

Fernanda Postigo Adami

Orientador: Prof. Dr. Agnaldo José Ferrari

Programa: Matemática Aplicada e Computacional

Presidente Prudente, dezembro de 2024

UNIVERSIDADE ESTADUAL PAULISTA

Faculdade de Ciências e Tecnologia de Presidente Prudente

Programa de Pós-Graduação em Matemática Aplicada e Computacional

Criptografia: uma aplicação via Reticulados

Fernanda Postigo Adami

Orientador: Prof. Dr. Agnaldo José Ferrari

Dissertação apresentada ao Programa de Pós-Graduação em Matemática Aplicada e Computacional da Faculdade de Ciências e Tecnologia da UNESP para obtenção do título de Mestre em Matemática Aplicada e Computacional.

Presidente Prudente, dezembro de 2024

A198c

Adami, Fernanda Postigo
Criptografia: uma aplicação via Reticulados / Fernanda Postigo Adami. -- Presidente Prudente, 2024
90 p. : il., tabs.

Dissertação (mestrado) - Universidade Estadual Paulista (UNESP), Faculdade de Ciências e Tecnologia, Presidente Prudente
Orientador: Agnaldo José Ferrari

1. Criptografia. 2. Reticulados. 3. Criptossistemas. 4. Pós-quântica. 5. Matemática. I. Título.

Sistema de geração automática de fichas catalográficas da Unesp. Dados fornecidos pelo autor(a).

UNIVERSIDADE ESTADUAL PAULISTA

Câmpus de Presidente Prudente

CERTIFICADO DE APROVAÇÃO

TÍTULO DA DISSERTAÇÃO: Criptografia: uma aplicação via Reticulados

AUTORA: FERNANDA POSTIGO ADAMI
ORIENTADOR: AGNALDO JOSÉ FERRARI

Aprovada como parte das exigências para obtenção do Título de Mestra em Matemática Aplicada e Computacional, pela Comissão Examinadora:

Prof. Dr. AGNALDO JOSÉ FERRARI (Participação Presencial)
Departamento de Matemática / Faculdade de Ciências de Bauru

Profa. Dra. CRISTIANE ALEXANDRA LÁZARO (Participação Presencial)
Departamento de Matemática / Faculdade de Ciências de Bauru

Profa. Dra. MAIARA FRANCINE BOLLAUF (Participação Virtual)
Departamento de Teoria da Informação / Simula UiB, Bergen, Noruega

Presidente Prudente, 04 de dezembro de 2024

À minha irmã Caroline, dedico.

Agradecimentos

Agradeço à Deus por iluminar meu caminho e me dar forças para concluir mais esta etapa tão importante.

Aos meus pais, Suzana e Ivander, por todo amor, apoio e compreensão incondicional ao longo da minha jornada acadêmica. Vocês são a base para todas as conquistas.

À minha irmã Caroline e aos meus sobrinhos Leonardo e Maria, por sempre me darem motivos para seguir em frente, mesmo nos momentos de dificuldade.

Ao meu namorado, Thiago, que esteve ao meu lado na parte mais importante desse desafio, oferecendo apoio, carinho e paciência. O seu amor é minha fonte de motivação diária, obrigada por acreditar no meu potencial.

Às minhas amigas Larissa e Karen, e aos meus primos Geninho e Pérola, pelo carinho, incentivo e pelos momentos de alegria compartilhados. Obrigada por sempre estarem presentes, dividindo angústias, desafios e comemorando comigo as vitórias.

Ao meu orientador, Professor Agnaldo, pela orientação precisa, paciência e comprometimento durante todo o processo. Sua dedicação e conhecimento foram fundamentais para a realização deste trabalho.

À UNESP, à CAPES e a banca examinadora, essenciais para a execução e concretização desta pesquisa.

"O mundo está cheio de coisas óbvias
que ninguém, por acaso,
jamais observa.".
Arthur Conan Doyle

Resumo

A criação da criptografia de chave pública por Diffie e Hellman em 1976, seguida pelo desenvolvimento do sistema de criptografia de chave pública RSA por Rivest, Shamir e Adleman em 1978, são momentos fundamentais para o desenvolvimento das telecomunicações. Neste contexto, este trabalho se concentra na exploração de problemas complexos que emergem na Teoria dos Reticulados e que serve como fundamento para a criação de novos criptossistemas de chave pública. Apresentamos um estudo aprofundado do capítulo "Lattices and Cryptography", da segunda edição do livro "An Introduction to Mathematical Cryptography" de Jefrey Hoffstein, Jill Pipher e Joseph H. Silverman, publicado em 2014 e buscamos investigar "problemas difíceis" que surgem na Teoria dos Reticulados que podem ser utilizados como base para criptossistemas de chave pública tais como o GGH e o NTRU.

Palavras-Chave: *reticulados algébricos, criptografia, chave pública, criptossistemas.*

Abstract

The creation of public key cryptography by Diffie and Hellman in 1976, followed by the development of the RSA public key cryptography system by Rivest, Shamir and Adleman in 1978, are fundamental moments in the development of telecommunications. In this context, this work focuses on exploring complex problems that emerge in Lattice Theory and that serve as a foundation for the creation of new public key cryptosystems. We present an in-depth study of the chapter "Lattices and Cryptography", from the second edition of the book "An Introduction to Mathematical Cryptography" by Jefrey Hoffstein, Jill Pipher and Joseph H. Silverman, published in 2014 and seek to investigate "hard problems" that arise in Lattice Theory that can be used as a basis for public key cryptosystems such as GGH and NTRU.

Keywords: *algebraic lattices, cryptography, public key, cryptosystems.*

Lista de Figuras

Lista de Tabelas

Conteúdo

Introdução

Entre as muitas facetas da Criptografia moderna, este trabalho se concentra em investigar um tipo de problema complexo que surge na Teoria dos Reticulados que pode ser usado como base para um criptossistema de chave pública e visa apresentar um estudo detalhado do capítulo 7, *"Lattices and Cryptography"*, da segunda edição do livro *"An Introduction to Mathematical Cryptography"*, de Jeffrey Hoffstein, Jill Pipher e Joseph H. Silverman, publicado em 2014. Os problemas associados a reticulados, como o problema do Vetor Mais Curto (*Shortest Vector Problem* - SVP) e o problema do Vetor Mais Próximo (*Closest Vector Problem* - CVP), oferecem uma base sólida para a construção de criptossistemas que exploram sua alta complexidade computacional, sendo, portanto, resistentes a ataques quânticos (PEIKERT, 2016).

Dez anos após a publicação do livro que fundamentou este estudo, a Criptografia baseada em reticulados evoluiu significativamente, sendo reconhecida como uma das mais promissoras para resistir à computação quântica. Embora este trabalho não tenha como objetivo explorar o estado atual dessa área de pesquisa, apresenta um estudo dos pilares que consolidaram essa área. Um exemplo é o GGH, um sistema que já foi quebrado, mas que desempenhou um papel fundamental no desenvolvimento inicial da criptografia de reticulados. Já o NTRU, que continua relevante, destacou-se na competição promovida pelo NIST para selecionar algoritmos pós-quânticos (SPECTRUM, 2024). Além disso, criptossistemas como LWE e Ring-LWE, que serão mencionados no último capítulo, tornaram-se pilares da criptografia moderna (LINDNER; PEIKERT, 2011).

No primeiro capítulo, veremos conceitos fundamentais de álgebra, como grupo, anel, corpo, ideal, anéis de polinômios, anéis polinomiais de convolução e espaço vetorial, que são indispensáveis para a compreensão dos tópicos subsequentes. O segundo capítulo aborda a Teoria dos Reticulados, com uma explicação detalhada de conceitos como base, região fundamental, empacotamento esférico, densidade de empacotamento, problemas de norma mínima, os principais reticulados conhecidos na literatura, o teorema de Hermite, o Raio de Hadamard, a base reduzida de reticulado e algoritmos fundamentais como o LLL, BKZ e o algoritmo de Babai.

Além disso, o capítulo inclui uma análise detalhada do comportamento do algoritmo de Babai sob diferentes configurações geométricas de bases, realizada por meio de implementações no software *Mathematica Wolfram*. Nessa análise, foram avaliadas situações em que o algoritmo funciona ou falha, considerando fatores como ângulos entre vetores, proporções de normas e o impacto do Raio de Hadamard, tanto no espaço bidimensional ($\mathbb{R}^2$) quanto tridimensional ($\mathbb{R}^3$). Os resultados obtidos destacam as condições necessárias para a eficiência do algoritmo, com implicações práticas significativas para aplicações em criptografia.

No terceiro capítulo, exploramos o fascinante universo da criptografia, desde suas raízes históricas até os conceitos fundamentais que moldaram sua evolução. Apresentamos um panorama sobre a trajetória da criptografia, com exemplos notáveis, como a cifra de César e a máquina Enigma, destacando como cada avanço refletiu as demandas de segurança de sua época. Ademais, abordamos a transição para a era moderna com a introdução dos computadores e a distinção entre criptografia de chave simétrica e assimétrica, culminando no estudo detalhado de dois criptossistemas clássicos: RSA e o da mochila. O capítulo ainda traça perspectivas sobre os desafios impostos pela computação quântica, destacando os esforços globais, como a competição do NIST, para identificar algoritmos capazes de resistir às ameaças futuras.

O quarto capítulo foca em criptossistemas baseados em problemas difíceis em reticulados, detalhando os fundamentos e aplicações de dois criptossistemas emblemáticos, o GGH e o NTRU, analisando suas estruturas matemáticas e os problemas que garantem sua segurança. Além disso, são explorados os avanços recentes na padronização de algoritmos resistentes a ataques quânticos, com uma análise comparativa entre o NTRU e sistemas mais tradicionais, como o RSA, evidenciando suas vantagens e desafios no contexto atual. Por fim, o capítulo apresenta brevemente o criptossistema LWE (Learning With Errors) e o Ring-LWE, sendo estes promissores e relevantes no desenvolvimento de criptografia pós-quântica.

Capítulo

1

Conceitos básicos

Neste capítulo, apresentamos alguns conceitos iniciais de Álgebra que são fundamentais para o embasamento da pesquisa, fundamentados com base em (HERSTEIN, 1970) e (IEZZI; DOMINGUES, 1970) .

1.1 Álgebra Linear

1.1.1 Independência e dependência linear

Definição 1.1.1. *Um conjunto de vetores é considerado linearmente independente se nenhum dos vetores puder ser expresso como uma combinação linear dos outros vetores de maneira não trivial. Em outras palavras, um conjunto de vetores é linearmente independente se a única maneira de obter o vetor nulo como uma combinação linear dos vetores do conjunto é atribuindo coeficientes iguais a zero para todos os vetores.*
Matematicamente, um conjunto de vetores $v_1, v_2, ..., v_n$ *é linearmente independente se a única solução da equação:*

$$c_1v_1 + c_2v_2 + ... + c_nv_n = 0$$

é $c_1 = c_2 = ... = c_n = 0$ *com* $c_1, c_2, ..., c_n \in \mathbb{R}$

Definição 1.1.2. *Um conjunto de vetores* $v_1, v_2, ..., v_n$ *é* ***linearmente dependente*** *se existirem coeficientes* $c_1, c_2, ..., c_n$*, não todos iguais a zero, tais que:*

$$c_1v_1 + c_2v_2 + ... + c_nv_n = 0$$

Nesse caso, os vetores são linearmente dependentes pois, pelo menos um vetor pode ser expresso como uma combinação linear dos outros.

1.1.2 Espaço vetorial

Definição 1.1.3. *Seja V um conjunto não vazio, munido das operações de soma e multiplicação por escalar. Dizemos que V é um* ***espaço vetorial*** *se atender às seguintes propriedades, para quaisquer $u, v, w \in V$ e $\alpha, \beta \in \mathbb{R}$:*

- *(A_1) Associatividade: $(u + v) + w = u + (v + w)$.*
- *(A_2) Comutatividade: $u + v = v + u$.*
- *(A_3) Existência do elemento neutro: Existe um $0 \in V$ tal que $u + 0 = u$, para todo $u \in V$.*
- *(A_4) Existência do inverso aditivo: Para cada $u \in V$, existe um $(-u) \in V$ tal que $u + (-u) = 0$.*
- *(M_1) Distributividade em relação à soma de vetores: $\alpha(u + v) = \alpha u + \alpha v$.*
- *(M_2) Distributividade em relação à soma de escalares: $(\alpha + \beta)u = \alpha u + \beta u$.*
- *(M_3) Associatividade da multiplicação escalar: $(\alpha\beta)u = \alpha(\beta u)$.*
- *(M_4) Existência do elemento neutro: Existe $1 \in \mathbb{R}$ tal que $1 \cdot u = u$, para todo $u \in V$.*

Exemplo 1.1.4. *O conjunto $\mathbb{R}^n$, formado por todos os vetores com n componentes reais, junto com as operações usuais de soma de vetores e multiplicação por escalares é um exemplo de espaço vetorial. Para $n = 2$, temos:*

$$\mathbf{u} = (u_1, u_2), \quad \mathbf{v} = (v_1, v_2), \quad e\ \alpha \in \mathbb{R}.$$

As operações são definidas como: $\mathbf{u} + \mathbf{v} = (u_1 + v_1, u_2 + v_2)$, $\alpha \cdot \mathbf{u} = (\alpha u_1, \alpha u_2)$. Pode-se verificar que todas as propriedades de um espaço vetorial são satisfeitas para $\mathbb{R}^2$.

Definição 1.1.5. *Um subconjunto S de um espaço vetorial V é um subespaço vetorial de V, se forem satisfeitas as seguintes condições.*

(i) 0 vetor nulo está em S, isto é, $0 \in S$.

(ii) Se $u, v \in S$, então $u + v \in S$.

(iii) Se $u \in S$, então $\alpha u \in S$ para todo $\alpha \in \mathbb{R}$.

Definição 1.1.6. *Sejam a, b números inteiros quaisquer e m um inteiro estritamente positivo. Diz-se que a* ***é côngruo a*** *b* ***módulo*** *m se $m|(a-b)$, isto é $a-b=mq$, para um conveniente inteiro q. Para indicar que a é côngruo a b, módulo m, usa-se a notação*

$$a \equiv b \,(mod\, m)$$

Seguem as propriedades básicas da congruência de inteiros:

1. $a \equiv a \,(mod\, m)$.
2. Se $a \equiv b \,(mod\, m)$, então $b \equiv a \,(mod\, m)$.
3. Se $a \equiv b \,(mod\, m)$ e $b \equiv c \,(mod\, m)$, então $a \equiv c \,(mod\, m)$.
4. Se $a \equiv b \,(mod\, m)$ e $0 \leq b < m$, então b é o resto da divisão euclidiana de a por m. Reciprocamente, se r é o resto da divisão de a por m, então $a \equiv r \,(mod\, m)$.
5. $a \equiv b \,(mod\, m)$ se, e somente se, a e b dão o mesmo resto na divisão euclidiana por m.
6. $a \equiv b \,(mod\, m)$ se, e somente se, $a \pm c \equiv b \pm c \,(mod\, m)$.
7. $a \equiv b \,(mod\, m)$ e $c \equiv d \,(mod\, m)$, então $a + c \equiv b + d \,(mod\, m)$.
8. Se $a \equiv b \,(mod\, m)$, então $ac \equiv bc \,(mod\, m)$.
9. Se $a \equiv b \,(mod\, m)$ e $c \equiv d \,(mod\, m)$, então $ac \equiv bd \,(mod\, m)$.
10. Se $ca \equiv cb \,(mod\, m)$ e mdc $(c, m) = d > 0$, então $a \equiv b \,(mod\, m/d)$.

Definição 1.1.7. *Seja A um conjunto não vazio. Dizemos que uma relação $\mathbb{R} \subset A \times A$ é uma relação de equivalência sobre A se R satisfaz as seguintes condições:*

(i) $(a, a) \in R$ *para todo* $a \in A$.

(ii) Se $(a, b) \in R$ *então* $(b, a) \in R$.

(iii) Se $(a, b) \in R$ *e* $(b, c) \in R$, *então* $(a, c) \in R$.

Em outras palavras, dizemos que uma relação R sobre um conjunto A é uma relação de equivalência se R for: reflexiva, simétrica e transitiva. Por exemplo, a relação de congruência módulo m sobre $\mathbb{Z}$ é uma relação de equivalência, visto que as três condições (reflexiva, simétrica e transitiva) são satisfeitas.

Definição 1.1.8. *Dado um número inteiro $m \geq 2$, a **classe modular** de um número inteiro a módulo m, denotada por $\overline{a}$, é o conjunto de todos os números inteiros x tais que $a \equiv x \pmod{m}$.*

$$\overline{a} = \{x \in \mathbb{Z} \mid x \equiv a \pmod{m}\}.$$

O conjunto de todas as classes modulares módulo m é representado por $\mathbb{Z}_m$ e definido como:

$$\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\}.$$

Se m for um número primo, o conjunto $\mathbb{Z}_m$, com as operações de adição e multiplicação módulo m, forma um corpo.

Uma classe modular de um número inteiro módulo m também é chamada de "classe de restos módulo m". Denotaremos $\overline{a}$ qualquer número natural a, para representar o resto de divisão por n. Os possíveis restos de uma divisão por n são $\overline{0}, \overline{1}, \overline{2}, ..., \overline{n-1}$. Se $n = 3$, então os possíveis restos serão $\overline{0}, \overline{1}$ e $\overline{2}$. Note que, $\overline{a} = \overline{b}$ se, e somente se, os restos da divisão de a e de b por n são iguais.

1.1.2.1 Base de um espaço vetorial

Uma *base* de um espaço vetorial V sobre um corpo $\mathbb{K}$ é um conjunto de vetores $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$ em V que satisfaz duas propriedades:

1. Os vetores no conjunto são linearmente independentes, ou seja, nenhum vetor pode ser expresso como uma combinação linear dos outros vetores.

2. Os vetores no conjunto geram todo o espaço vetorial V, o que significa que qualquer vetor em V pode ser representado como uma combinação linear dos vetores na base.

Exemplo 1.1.9. *Suponha que temos um espaço vetorial tridimensional V sobre os números reais $\mathbb{R}$. Neste espaço vetorial, podemos considerar os vetores que representam coordenadas tridimensionais. Um vetor tridimensional típico é da forma $\mathbf{v} = \begin{bmatrix} x \\ y \\ z \end{bmatrix}$, onde x, y e z são números reais.*

Uma base comum para esse espaço vetorial tridimensional é a seguinte:

$$\mathbf{e}_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \quad \mathbf{e}_2 = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \quad \mathbf{e}_3 = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$$

Esses vetores são chamados de vetores de base canônica e representam os vetores unitários nos eixos x, y e z. Eles formam uma base para o espaço vetorial tridimensional $\mathbb{R}^3$ sobre os números reais $\mathbb{R}$, chamada ***base canônica****.*

1.2 Álgebra

Esta sessão não tem a intenção de fazer uma revisão ampla a respeito da teoria da Álgebra, mas sim oferecer uma introdução dos conceitos que serão necessários para o entendimento dos procedimentos realizados nos criptossistemas que sucedem.

1.2.1 Grupo

Definição 1.2.1. *Seja G um conjunto não vazio e $*$ uma operação $(x, y) \to x * y$ sobre G. G é chamado Grupo se as seguintes propriedades forem satisfeitas:*

(i) Associatividade:

$(a * b) * c = a * (b * c)$, *quaisquer que sejam* $a, b, c \in G$.

(ii) Existência de elemento neutro:

$a * e = e * a = a$, *qualquer que seja* $a \in G$.

(iii) Existência de simétricos:

$\forall a \in G$, *existe um elemento* a' *tal que* $a * a' = a' * a = e$.

Definição 1.2.2. *Um grupo é chamado de* ***abeliano*** *ou* ***comutativo*** *se satisfaz também a propriedade de comutatividade, ou seja, $a * b = b * a$, quaisquer que sejam $a, b \in G$.*

Usaremos a notação $(G, *)$ para indicar a operação * sobre o grupo G.

Outros exemplos de Grupos são: $(\mathbb{Z}, +), (\mathbb{Q}, +)$ e $(\mathbb{C} - \{0\}, \cdot)$. Note que todos eles são grupos abelianos, já que a propriedade comutativa é válida.

Definição 1.2.3. *Seja $(G, \cdot)$ um grupo e H um subconjunto não vazio de G. Dizemos que H é um subgrupo de G se, com a operação $\cdot$ de G, o conjunto H também for um grupo, ou seja, $(H, \cdot)$ forma um grupo.*

Definição 1.2.4. *Dado um grupo $(G, *)$, um subgrupo H de G e um elemento $x \in G$, o conjunto*

$$H * x = \{h * x \mid h \in H\}$$

é chamado de classe lateral à direita de H em G.

De maneira análoga, o conjunto

$$x * H = \{x * h \mid h \in H\}$$

é chamado de classe lateral à esquerda de H em G.

Definição 1.2.5. *Dizemos que um grupo multiplicativo G é cíclico se, para algum $a \in G$, temos $G = \{a^m;\ m \in \mathbb{Z}\}$. Se G é um grupo aditivo, então será cíclico se, dado $a \in G$, temos $G = \{ma;\ m \in \mathbb{Z}\}$. Em ambos os casos, o elemento a é chamado gerador do grupo G.*

.

1.2.2 Anel

Definição 1.2.6. *Seja A um conjunto não vazio munido de duas operações $\cdot : A \times A \to A$ e $+ : A \times A \to A$, as operações de multiplicação e adição, respectivamente. A é dito um **anel**, denotado por $(A, +, \cdot)$ se são satisfeitas as seguintes condições:*

(i) $(A, +)$ é um grupo abeliano;

(ii) A multiplicação é associativa, ou seja, para quaisquer $a, b, c \in A$ vale que $(ab)c = a(bc)$;

(iii) A multiplicação é distributiva em relação a adição, ou seja, para quaisquer $a, b, c \in A$, vale $a(b + c) = ab + ac$ e $(b + c)a = ba + ca$.

Os conjuntos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ são anéis, por exemplo.

Se além disso, valer que $ab = ba$, dizemos que A é um **anel comutativo**. Se existe o elemento neutro para a multiplicação, ou seja, se existe $1 \in A$ tal que $1a = a1 = a, \forall a \in A$, dizemos que A **é um anel com unidade 1**.

Definição 1.2.7. *Um subconjunto $S \subseteq A$ de um anel A é um subanel de A se S é fechado para as operações que definem A e é também um anel em relação a estas operações.*

Proposição 1.2.8. *Um subconjunto $S \neq \emptyset$ será um subanel de A se, e somente se, dados $x, y \in S$, valer que $x - y \in S$ e $xy \in S$.*

Um elemento $x \in A$ é dito invertível no anel A se existe $y \in A$ tal que $xy = 1$. O conjunto dos elementos invertíveis de um anel A, denotado por U_A, é um grupo comutativo em relação à multiplicação.

Definição 1.2.9. *Se A é um anel comutativo, então $a \in A$, com $a \neq 0$ é um* ***divisor de zero*** *se existe $0 \neq b \in A$ tal que $ab = 0$.*

Definição 1.2.10. *Um anel A que não possui divisores de zero é chamado de domínio, ou anel de integridade. Ou seja, A é um domínio se, para todos $x, y \in A$ vale que se $xy = 0$, então $x = 0_A$ ou $y = 0_A$.*

Um conceito fundamental em Álgebra é o de homomorfismo, que se refere a uma aplicação entre duas estruturas algébricas semelhantes, a qual preserva as operações definidas nessas estruturas e, consequentemente, mantém suas propriedades, utilizamos esse conceito para a seguinte definição:

Definição 1.2.11. *Uma aplicação ϕ de um anel A em um anel R será um homomorfismo de anéis se forem satisfeitas, para quaisquer $a, b \in A$,*

1. $\phi(a + b) = \phi(a) + \phi(b)$,
2. $\phi(ab) = \phi(a)\phi(b)$.

1.2.3 Corpo

Definição 1.2.12. *Seja $(\mathbb{K}, +, \cdot)$ um anel comutativo com unidade. Dizemos que $\mathbb{K}$ é um* ***corpo*** *se, $\forall a \in \mathbb{K} - \{0\}$, existe $a^{-1} \in \mathbb{K}$ tal que $aa^{-1} = 1$, onde 0 é o elemento neutro da adição e 1 é a unidade, elemento neutro da multiplicação. Ou seja, um anel comutativo com unidade $\mathbb{K}$ é corpo se todos seus elementos, com exceção do 0, possuem inverso multiplicativo.*

Exemplo 1.2.13. *O conjunto dos números racionais munido das operações usuais de soma e multiplicação é um anel com unidade que, no caso, é o número* 1.

Além disso, todo número racional não nulo tem um inverso multiplicativo, o qual é um número racional. Dessa forma, o conjunto dos números racionais é um corpo. O mesmo raciocínio se aplica ao conjunto dos números reais.

1.2.4 Ideal

O conceito de ideal de um anel nos fornece resultados importantes para o estudo de anéis e corpos.

Definição 1.2.14. *Sejam A um anel e $I \subseteq A$, não vazio. Dizemos que I é um* ***Ideal*** *de A, denotando por $I \trianglelefteq A$, se $(I, +)$ é subgrupo de $(A, +)$ e, dado qualquer $a \in A$ e $r \in I$, temos $ar \in I$. Uma condição necessária e suficiente para I ser um ideal de A é, dados quaisquer $a, b \in I$ e $r \in A$, valer que $ra + b \in I$.*

Definição 1.2.15. *Dado um anel A, para todo $x \in A$ o conjunto $xA = \{xa;\ a \in A\}$, denotado por $\langle x \rangle$ ou (x), é um ideal de A, denominado o* ***ideal principal gerado por*** *x.*

Proposição 1.2.16. *Se A é um anel comutativo com unidade, cujos únicos ideais são os triviais $\langle 0 \rangle$ e o próprio A, então A é um corpo.*

Faremos agora a construção de modo à obter um conjunto quociente que seja um anel. Para isso, dado um ideal I de um anel A, denotemos por A/I o conjunto de todas as classes laterais distintas de I em A. Podemos considerar este conjunto, pois vimos que $(I, +)$ é subgrupo de $(A, +)$. Ou seja, A/I é o conjunto das classes laterais do tipo $a + I$, com $a \in A$.

A/I é um grupo quociente, com relação à adição dada por $(a + I) + (b + I) = (a + b) + I$. Então, para que A/I tenha uma estrutura de anel, devemos definir uma multiplicação sobre este conjunto de modo que sejam satisfeitas as propriedades que definem um anel. O mais natural é definir $(a + I)(b + I) = ab + I$.

Proposição 1.2.17. *Se A é um anel e I é um ideal de A, então o conjunto A/I adquirido na construção acima é um anel, chamado anel quociente de A sobre I.*

Se A é um anel comutativo, então A/I também o é, pois $(a + I)(b + I) = ab + I = ba + I = (b + I)(a + I)$. Por outro lado, se A possui unidade 1, então A/I possui unidade $1 + I$.

As operações de adição e multiplicação no anel quociente A/I são definidas da seguinte forma:

(i) Adição: A soma de duas classes de equivalência $\overline{a}$ e $\overline{b}$ em A/I é definida como a classe de equivalência $\overline{a + b}$ em A/I.

(ii) Multiplicação: O produto de duas classes de equivalência $\overline{a}$ e $\overline{b}$ em A/I é definido como a classe de equivalência $\overline{ab}$ em A/I.

O anel quociente A/I herda propriedades e estruturas do anel A, mas possui algumas características específicas relacionadas ao ideal I em questão. Os elementos do anel quociente são representados por classes de equivalência, onde elementos equivalentes produzem a mesma classe de equivalência.

1.3 Anéis de Polinômios

Alguns conceitos e propriedades importantes sobre o anel dos polinômios serão vistos agora. Inicialmente, definimos quem são seus elementos e as operações de adição e multiplicação.

Definição 1.3.1. *Se $\mathbb{K}$ é um corpo, um polinômio com variável x e coeficientes sobre $\mathbb{K}$ é dado por uma expressão $p(x) = a_n x^n + \cdots + a_1 x + a_0$, com $a_0, \cdots, a_n \in \mathbb{K}$ e n um inteiro positivo. Denotamos o conjunto destes polinômios por $\mathbb{K}[x]$.*

As operações sobre o conjunto dos polinômios são as usuais, dadas pela adição e multiplicação definidas. Dados $p(x) = a_n x^n + \cdots + a_0$ e $q(x) = b_m x^m + \cdots + b_0$ ambos em $\mathbb{K}[x]$, considerando $m \geq n$. Então

$$p(x) + q(x) = c_m x^m + \cdots c_0, \quad \textit{onde} \;\; c_i = a_i + b_i, \quad 0 \leq i \leq m$$

e

$$p(x)q(x) = c_{m+n} x^{m+n} + \cdots + c_0, \quad \textit{onde} \;\; c_i = \sum_{j=0}^{i} a_j b_{i-j}, \quad 0 \leq i \leq m+n.$$

Logo, $\mathbb{K}[x]$ munido destas operações, é um anel, denominado **anel dos polinômios sobre um corpo $\mathbb{K}$.** O zero deste anel é dado pelo polinômio constante $p(x) = 0$.

Dado um corpo $\mathbb{K}$, denotamos por $\mathbb{K}(x)$ o corpo quociente do anel dos polinômios $\mathbb{K}[x]$ e chamamos este de *corpo de funções racionais*. Desse modo, $\mathbb{K}(x)$ é formado por todos os quocientes $f(x)/g(x)$, com $g(x) \neq 0$. Podemos pensar nas frações $f(x)/g(x)$ como funções de $\mathbb{K}$ em si mesmo, por isso recebem o nome de *funções racionais* ou *expressões racionais*.

Proposição 1.3.2. *Todo ideal do anel $\mathbb{K}[x]$ é principal, ou seja, se F é um ideal de $\mathbb{K}[x]$, existe $f \in F$ tal que $F = \langle f \rangle$.*

Definição 1.3.3. *Se p é um polinômio sobre um corpo $\mathbb{K}$, $p \neq 0$, então definimos o grau de p pela maior potência da variável x, com coeficiente não-nulo, que ocorre em p.*

Portanto, o grau de um polinômio é definido pela função

$$gr : \mathbb{K}[x] \setminus \{0\} \longrightarrow \mathbb{N} \quad \textit{dada por} \quad \sum_{i=0}^{n} a_i x^i \longmapsto n,$$

onde n é o maior inteiro positivo tal que $a_n \neq 0$. Denotaremos o grau de um polinômio p por $gr(p)$. Segue das definições de adição e multiplicação do anel que $gr(p+q) \leq max(gr(p), gr(q))$ e $gr(pq) = gr(p) + gr(q)$. O grau do polinômio zero é, por convenção, igual à $-\infty$.

Teorema 1.3.1. *Sejam $f, p \in \mathbb{K}[x]$ polinômios, com $f \neq 0$. Então existem polinômios únicos $q, r \in \mathbb{K}[x]$ tais que $p = fq + r$, onde $gr(r) < gr(f)$.*

Neste caso, o polinômio q é chamado *quociente* e r é dito *resto* da divisão. O processo para determinar p e q é o chamado algoritmo da divisão. Com isso, podemos definir a divisibilidade entre polinômios.

Definição 1.3.4. *Dados $f, g \in \mathbb{K}[x]$, dizemos que f **divide** g, ou que g é múltiplo de f, se existe um polinômio $h \in \mathbb{K}[x]$ tal que $g = fh$.*

Quando f divide g, denotamos por $f|g$. Caso contrário, denotamos como $f \nmid g$ para dizer que f não divide g. Note que, pelo algoritmo da divisão, f divide g se temos o polinômio resto $r = 0$. Com isto, podemos definir o conceito de máximo divisor comum para polinômios.

Definição 1.3.5. *Um polinômio $m \in \mathbb{K}[x]$ é definido como o máximo divisor comum (mdc) de polinômios $p, q \in \mathbb{K}[x]$ se $m|p$, $m|q$ e, além disso, sempre que $f|p$ e $f|q$, tivermos $f|m$.*

Quando $m \in \mathbb{K}[x]$ é o máximo divisor comum dos polinômios p e q sobre $\mathbb{K}$, então existem polinômios $a, b \in \mathbb{K}[x]$ tais que $m = ap + bq$.

Definição 1.3.6. *Se p e q são polinômios sobre um corpo $\mathbb{K}$ com $mdc(p, q) = 1$, então p e q são ditos coprimos.*

Definição 1.3.7. *Dizemos que um polinômio sobre um subanel $\mathbb{K}$ de $\mathbb{C}$ é redutível se for produto de dois polinômios de menor grau sobre $\mathbb{K}$. Caso contrário, o polinômio é dito irredutível.*

Ou seja, $p \in \mathbb{K}[x]$ é irredutível se não existem $f, g \in \mathbb{K}[x]$ tais que $0 < gr(f), gr(g) < gr(p)$ e $p = fg$. Pela definição acima, qualquer polinômio redutível pode ser escrito como produto de dois polinômios de menor grau. Se estes forem redutíveis podem ser, cada um, reescritos como um produto de polinômios de menor grau, e assim por diante. Por indução, este processo continua até certo ponto, ou seja, o ponto em que os polinômios fatores deste produto são todos irredutíveis.

Teorema 1.3.2. *Qualquer polinômio sobre um corpo $\mathbb{K}$ é produto de polinômios irredutíveis sobre $\mathbb{K}$.*

1.3.1 Anéis polinomiais de convolução

Um tipo especial de anéis polinomiais são os de convolução. Este se torna importante para nosso trabalho, visto que é utilizado no sistema criptográfico de chave pública NTRU, abordado nas seções seguintes.

Definição 1.3.8. *Dado um inteiro positivo N. O anel de polinômios de convolução de posto N é o anel quociente:*

$$R = \frac{\mathbb{Z}[x]}{(x^N - 1)}$$

Da mesma forma, o anel de polinômios de convolução (modulo q) é o anel quociente

$$R_q = \frac{(\mathbb{Z}/q\mathbb{Z})[x]}{(x^N - 1)}$$

onde os elementos desse anel são da forma:

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_{N-1} x^{N-1}$$

com os coeficientes em $\mathbb{Z}$ ou $\mathbb{Z}/q\mathbb{Z}$.

É importante destacar que é mais fácil fazer cálculos nos anéis R e R_q do que em polinômios gerais de anéis quocientes, porque o polinômio $x^N - 1$ tem uma forma mais simples. A questão é que quando trabalhamos em anéis quocientes com denominadores $x^N - 1$, vale a identidade $x^N \equiv 1$. Por exemplo, se temos um termo x^k, o reescrevemos como $k = iN + j$ com $0 \leq j < N$ e definimos

$$x^k = x^{iN+j} = \left(x^N\right)^i \cdot x^j = 1^i \cdot x^j = x^j.$$

Em resumo, os expoentes das potências de x podem ser reduzidos módulo N. Muitas vezes é conveniente identificar um polinômio

$$\boldsymbol{a}(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{N-1} x^{N-1} \in R$$

com seu vetor de coeficientes

$$(a_0, a_1, a_2, \ldots, a_{N-1}) \in \mathbb{Z}^N,$$

e da mesma forma com polinômios em R_q.

A adição de polinômios corresponde à adição usual de vetores,

$$\boldsymbol{a}(x) + \boldsymbol{b}(x) \longleftrightarrow (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots, a_{N-1} + b_{N-1})$$

Já a regra para multiplicação é um pouco mais complicada, visto que precisamos reduzir o coeficiente e o grau dos polinômios.

Proposição 1.3.9. *O produto de dois polinômios $\boldsymbol{a}(x), \boldsymbol{b}(x) \in R$ é dado por:*

$$\boldsymbol{a}(x) \star \boldsymbol{b}(x) = \boldsymbol{c}(x) \quad com \quad c_k = \sum_{i+j \equiv k(\bmod N)} a_i b_{k-i},$$

onde o somatório que define c_k é para todo i e j entre 0 e $N-1$ satisfazendo a condição $i + j \equiv k(mod\ N)$. O produto de dois polinômios $\boldsymbol{a}(x), \boldsymbol{b}(x) \in R_q$ é dado da mesma maneira, exceto que para o valor de c_k, que será reduzido módulo q.

Demonstração. Primeiro calculamos o produto polinomial usual de $\boldsymbol{a}(x), \boldsymbol{b}(x)$ e o utilizamos que $x^N = 1$ para combinar os termos. Assim:

$$\begin{aligned}
\boldsymbol{a}(x) \star \boldsymbol{b}(x) &= \left(\sum_{i=0}^{N-1} a_i x^i\right) \star \left(\sum_{j=0}^{N-1} b_j x^j\right) \\
&= \sum_{k=0}^{2N-2} \left(\sum_{i+j=k} a_i b_j\right) x^k \\
&= \sum_{k=0}^{N-1} \left(\sum_{i+j=k} a_i b_j\right) x^k + \sum_{k=N}^{2N-2} \left(\sum_{i+j=k} a_i b_j\right) x^{k-N} \\
&= \sum_{k=0}^{N-1} \left(\sum_{i+j=k} a_i b_j\right) x^k + \sum_{k=0}^{N-2} \left(\sum_{i+j=k+N} a_i b_j\right) x^k \\
&= \sum_{k=0}^{N-1} \left(\sum_{i+j \equiv k(\bmod N)} a_i b_j\right) x^k.
\end{aligned}$$

Exemplo 1.3.10. *Seja $N = 5$ e $\boldsymbol{a}(x), \boldsymbol{b}(x) \in R$ os polinômios*

$$\boldsymbol{a}(x) = 1 - 2x + 4x^3 - x^4 \quad e \quad \boldsymbol{b}(x) = 3 + 4x - 2x^2 + 5x^3 + 2x^4.$$

Então

$$\begin{aligned}
\boldsymbol{a}(x) \star \boldsymbol{b}(x) &= 3 - 2x - 10x^2 + 21x^3 + 5x^4 - 16x^5 + 22x^6 + 3x^7 - 2x^8 \\
&= 3 - 2x - 10x^2 + 21x^3 + 5x^4 - 16 + 22x + 3x^2 - 2x^3 \\
&= -13 + 20x - 7x^2 + 19x^3 + 5x^4 \quad em\ R = \mathbb{Z}[x]/\left(x^5 - 1\right).
\end{aligned}$$

Se trabalharmos em R_{11}, reduziremos os coeficientes dos polinômios módulo 11 para obtermos

$$\boldsymbol{a}(x) \star \boldsymbol{b}(x) = 9 + 9x + 4x^2 + 8x^3 + 5x^4 \quad em\ R_{11} = (\mathbb{Z}/11\mathbb{Z})[x]/\left(x^5 - 1\right).$$

Observação 1.3.10.1. *O produto de convolução de dois vetores é dado por*

$$(a_0, a_1, a_2, ..., a_{N-1}) \star (b_0, b_1, b_2, ..., b_{N-1}) = (c_0, c_1, c_2, ..., c_{N-1}),$$

onde os c_k são definidos pela operação da Proposição 1.2.9. Usamos $\star$ para denotar a multiplicação de convolução nos anéis R e R_q e o produto de convolução dos vetores.

Existe uma função de R para R_q no qual reduzimos os coeficientes de um polinômio módulo q. Esta função reduzida módulo q satisfaz

$$(\boldsymbol{a}(x) + \boldsymbol{b}(x)) \bmod q = (\boldsymbol{a}(x) \bmod q) + (\boldsymbol{b}(x) \bmod q),$$
$$(\boldsymbol{a}(x) \star \boldsymbol{b}(x)) \bmod q = (\boldsymbol{a}(x) \bmod q) \star (\boldsymbol{b}(x) \bmod q).$$

Na terminologia matemática, a função $R \to R_q$ é um homomorfismo de anel. Para realizar essa redução utilizamos do conceito a seguir.

Definição 1.3.11. *Dada uma função $f : R \to R_q$, onde R é um anel e R_q é o anel reduzido módulo q, a operação de* levantamento central (center-lift) cl(f)*, é um homomorfismo de anel que ajusta os coeficientes de um elemento de R_q para pertencer ao anel R e centraliza os valores dos coeficientes em torno de zero.*

Formalmente, para um elemento $\boldsymbol{a}(x) \in R_q$ na forma $\boldsymbol{a}(x) = \sum_{i=0}^{n} \boldsymbol{a}_i x^i$, onde $\boldsymbol{a}_i \in \mathbb{Z}_q$, a operação de center-lift *é definida como:*

$$cl(\boldsymbol{a}(x)) = \sum_{i=0}^{n} cl\ _q(\boldsymbol{a}_i)x^i,$$

onde $cl_q(\boldsymbol{a}_i)$ é uma função que ajusta o coeficiente $\boldsymbol{a}_i$ para pertencer ao intervalo $[\frac{-q}{2}, \frac{q}{2}]$ e centraliza seu valor em relação a zero, de modo que $cl_q(\boldsymbol{a}_i) \in \{\frac{-q}{2}, \frac{-q}{2} + 1, \ldots, \frac{q}{2} - 1, \frac{q}{2}\}$.

A operação de *center-lift* é usada para garantir que os coeficientes do elemento $\boldsymbol{a}(x) \in R_q$ pertençam ao anel R e estejam dentro do intervalo $[\frac{-q}{2}, \frac{q}{2}]$, preservando as propriedades de adição e multiplicação de convolução em R e R_q. Por exemplo, se $q = 2$, então o center-lift de $\boldsymbol{a}(x)$ é um polinômio binário.

Muitos polinômios possuem inversos multiplicativos em R, mas isso nem sempre ocorre em R_q, dessa forma, é importante a consideração abaixo.

Proposição 1.3.12. *Seja q primo. Então $\boldsymbol{a}(x) \in R_q$ tem inverso multiplicativo se, e somente se*

$$mdc(\boldsymbol{a}(x), x^N - 1) = 1 \text{ em } (\mathbb{Z}/q\mathbb{Z})[x]$$

Disso, concluímos os próximos resultados.

Proposição 1.3.13. *Seja $\boldsymbol{a}(x) \in \mathbb{Z}/q\mathbb{Z}[x]$, onde q é um número primo, temos que,*

(i) $\boldsymbol{a}(1) \equiv 0$ *(mod q), se e somente se* $(x-1)|\boldsymbol{a}(x)$ *em* $\mathbb{Z}/q\mathbb{Z}[x]$

(ii) Se $\boldsymbol{a}(1) \equiv 0$ *(mod q), então* $\boldsymbol{a}(x)$ *não é invertível em* R_q.

Demonstração. (i) Em $(\mathbb{Z}/q\mathbb{Z})[x]$, usamos divisão com resto para dividir $\mathbf{a}(x)$ por $x-1$. O resultado é

$$\mathbf{a}(x) = (x-1)\mathbf{b}(x) + \mathbf{r}(x) \quad \text{com } \operatorname{gr}(\mathbf{r}(\mathbf{x})) < \operatorname{gr}(x-1) = 1.$$

Assim, ou $\mathbf{r}(x) = 0$ ou $\operatorname{gr}(\mathbf{r}(x)) = 0$, e portanto, em ambos os casos $\mathbf{r}(x)$ é constante. Logo,

$$\mathbf{a}(x) = (x-1)\mathbf{b}(x) + c \quad \text{para algum } c \in \mathbb{Z}/q\mathbb{Z}.$$

Podemos determinar c substituindo $x = 1$, que nos leva a $c = \mathbf{a}(1)$. Portanto

$$\mathbf{a}(x) = (x-1)\mathbf{b}(x) + \mathbf{a}(1).$$

Assim (i) se torna de fácil entendimento, já que a equação acima nos mostra que $\mathbf{a}(x)$ é múltiplo de (ou divisível por) $x-1$ se e somente se $\mathbf{a}(1) = 0$.

(ii) Suponha que $\mathbf{a}(x)$ é invertível em R_q, dizemos $\mathbf{a}(x)\mathbf{b}(x) = 1$ em R_q. Temos uma função bem definida $R_q \equiv \mathbb{Z}/q\mathbb{Z}$ em $x = 1$. Essa função é bem definida porque a relação $x^N \models 1$ é verdadeira quando $x \models 1$. Além disso, a função respeita a adição e a multiplicação. Portanto, a relação $\mathbf{a}(x)\mathbf{b}(x) = 1$ em R_q leva a relação $\mathbf{a}(1)\mathbf{b}(1) = 1$ em $\mathbb{Z}/q\mathbb{Z}$. Em particular, não podemos ter $\mathbf{a}(1) = 0$. Isso prova que

$$\mathbf{a}(x) \text{ invertível } \implies \mathbf{a}(1) \neq 0,$$

que é equivalente a dizer

$$\mathbf{a}(1) = 0 \quad \implies \quad \mathbf{a}(x) \text{ não é invertível}$$

Capítulo

2

Reticulados

Neste capítulo será apresentado o conceito de reticulados e tópicos fundamentais para o entendimento dos criptossistemas baseados em reticulados. Para isto, foram utilizadas as referências (CONWAY; SLOANE, 1999), (FERRARI, 2012) e (GRUBER; LEKKERKERKER, 1987).

2.1 Conceitos básicos

Definição 2.1.1. *Seja* $\{v_1, v_2, \cdots, v_m\}$ *um conjunto de vetores linearmente independentes do espaço vetorial* $\mathbb{R}^n$*, com* $m \leq n$*. O conjunto*

$$\Lambda = \left\{ \sum_{i=1}^{m} \alpha_i v_i ; \alpha_i \in \mathbb{Z} \right\}$$

é chamado um reticulado de posto m*, e* $\{v_1, v_2, \cdots, v_m\}$ *é chamado uma base do reticulado* Λ*.*

Então, de acordo com a definição, ao variar os coeficientes α_i no conjunto dos inteiros, vemos que um reticulado no $\mathbb{R}^n$ é um conjunto infinito de pontos dispostos de maneira regular no espaço.

Proposição 2.1.2. *Um reticulado* $\Lambda \subset \mathbb{R}^n$ *é um subgrupo do grupo aditivo abeliano* $(\mathbb{R}^n, +)$*.*

Demonstração. De fato, tomando os vetores $u, w \in \Lambda$, temos que

$$u = \sum_{i=1}^{m} \alpha_i v_i ; \alpha_i \in \mathbb{Z}$$

e

$$w = \sum_{i=1}^{m} \beta_i v_i; \beta_i \in \mathbb{Z}$$

Então temos que $u + (-w)$ é igual à

$$\sum_{i=1}^{m} \alpha_i v_i + \sum_{i=1}^{m} -\beta_i v_i = \sum_{i=1}^{m} (\alpha_i - \beta_i) v_i$$

Como $(\alpha_i - \beta_i) \in \mathbb{Z}$, segue que $(u + (-w)) \in \Lambda$, o que mostra que Λ é subgrupo de $(\mathbb{R}^n, +)$. Assim, um reticulado Λ é um grupo aditivo abeliano.

A seguir, é definida uma região relacionada aos pontos do reticulado, compreendida entre os vetores da base desse.

Definição 2.1.3. *Sendo $\Lambda \subset \mathbb{R}^n$ um reticulado com base $\mathrm{B} = \{v_1, v_2, \cdots, v_m\}$, é definida a região fundamental ou paralelotopo fundamental de Λ em relação à base B o conjunto*

$$P_B = \left\{ x \in \mathbb{R}^n; x = \sum_{i=1}^{n} \alpha_i v_i; 0 \leq \alpha < 1 \right\}$$

Geometricamente, a região fundamental é a região compreendida entre os vetores da base do reticulado, formando um paralelotopo com esses vetores. Desse modo, a região fundamental depende da base do reticulado escolhida. Bases diferentes determinam regiões diferentes.

Quando transladamos a região fundamental através de todos os pontos do reticulado, a união das cópias da região cobre todo o espaço euclidiano, de modo que cada cópia contenha um único ponto do reticulado. Dessa forma, dizemos que a região fundamental "ladrilha"o espaço.

Exemplo 2.1.4. *O reticulado com base $\{v_1, v_2\}$, onde $v_1 = (1, 0)$ e $v_2 = (0, 1)$ é um reticulado de posto 2 no $\mathbb{R}^2$, chamado de reticulado $\mathbb{Z}^2$. O reticulado e a região fundamental são descritos na Figura 2.1.*

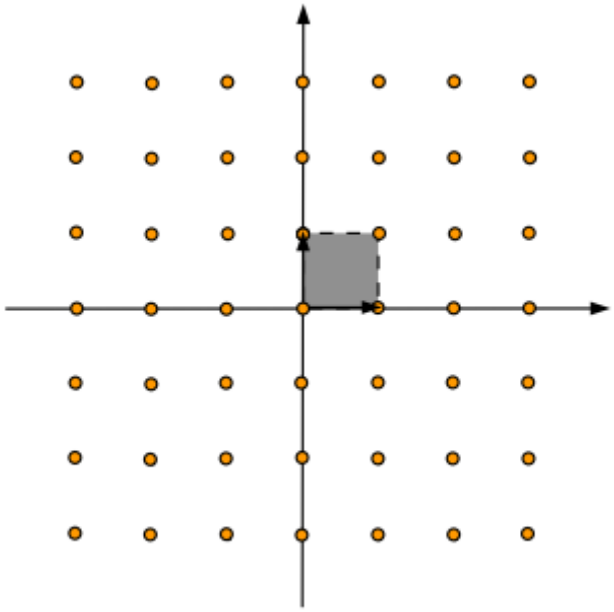

Figura 2.1: Reticulado $\mathbb{Z}^2$ com uma região fundamental.

Definição 2.1.5. *Seja* $\{v_1, v_2, \cdots, v_m\}$ *uma base para o reticulado* Λ *tal que* $v_i = (v_{i1}, \cdots, v_{in})$, *para* $i = 1, \cdots, m$. *A matriz* $M = (v_{ij})$ *é chamada uma matriz geradora para o reticulado* Λ. *Desse modo, a matriz geradora é formada pelos vetores da base do reticulado, dispostos em linha ou coluna. Em nosso trabalho, convencionamos a disposição dos vetores em linhas na matriz.*

Se M é uma matriz geradora para o reticulado Λ, então Λ pode ser escrito na forma matricial como

$$\Lambda = \{xM; x \in \mathbb{Z}^n\}$$

Exemplo 2.1.6. *A matriz* $M = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ *é uma matriz geradora para o reticulado* $\mathbb{Z}^2$.

A matriz $N = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ *é a matriz geradora para o reticulado* $\mathbb{Z}^3$.

A matriz geradora de um reticulado não é única. Isto decorre do fato da matriz geradora ter como entradas os elementos dos vetores da base do reticulado, dispostos em linha ou coluna. Como o reticulado não possui uma única base, segue que sua matriz geradora também não é única. A seguir, é apresentada a condição necessária e suficiente para que duas matrizes sejam geradoras de um mesmo reticulado.

Proposição 2.1.7. *Duas matrizes M_1 e M_2 geram o mesmo reticulado se, e somente se, $M_1 = AM_2$, onde A é uma matriz com elementos inteiros e determinante ± 1. A matriz A é chamada mudança de base.*

Definição 2.1.8. *Seja M uma matriz geradora para o reticulado Λ. A matriz $G = MM^t$, onde t denota uma transposição, é chamada de matriz de Gram para o reticulado Λ.*

Como a matriz geradora M contém os vetores $\{v_1, v_2, \cdots, v_m\}$, vetores da base do reticulado, então a (i, j)-ésima entrada da matriz G é o produto interno $\langle v_i, v_j \rangle$. Então, as entradas da matriz de Gram G guardam informações métricas importantes, pois referem-se às posições relativas dos vetores da base do reticulado. Nessas informações podemos identificar, por exemplo, ortogonalidade entre vetores da base, bem como o comprimento desses vetores. O próximo resultado garante que o determinante de um reticulado independe da matriz geradora escolhida.

Proposição 2.1.9. *Sendo M uma matriz geradora de Λ, com matriz de Gram $G = MM^t$ e M' outra matriz geradora de Λ com matriz de Gram $G' = M'M'^t$. Então,* $\det(G) = \det(G')$.

Definição 2.1.10. *O determinante de um reticulado Λ é definido como o determinante da matriz de Gram de Λ, ou* seja, $\det(\Lambda) = \det(\mathrm{G})$.

Como $G = MM^t$, se a matriz geradora M for quadrada, ou seja, $m = n$, então $\det(\Lambda) = \det(G) = \det(M)^2$. Nesse caso, o reticulado é dito de posto completo.

Definição 2.1.11. *O volume do reticulado Λ é definido por* $\mathrm{Vol}(\Lambda) = \sqrt{\det(\Lambda)}$. *Esse é o volume da região fundamental do reticulado Λ.*

Bases diferentes do reticulado determinam o mesmo volume. Isso decorre da Proposição 2.1.6, pois, como mostrado, duas matrizes geram o mesmo reticulado quando diferem por um produto de uma matriz inversível com entradas inteiras e determinante da matriz ± 1. Além disso, pela Proposição 2.1.8, vimos que o determinante do reticulado independe da matriz geradora escolhida. Assim, o volume independe da base do reticulado escolhida.

Definição 2.1.12. *Sendo B uma matriz de ordem n com entradas inteiras, um sub-reticulado de Λ é definido por*

$$\Lambda' = \{\alpha BM; \alpha \in \mathbb{Z}^n\}$$

onde M *é a matriz geradora do reticulado Λ.*

Como foi mostrado no início da seção, um reticulado Λ é um grupo aditivo abeliano. Um sub-reticulado Λ' é um subgrupo de Λ. A demonstração desse resultado é idêntica àquela utilizada para mostrar que Λ é subgrupo de $(\mathbb{R}^n, +)$.

Definição 2.1.13. *Seja Λ um reticulado no $\mathbb{R}^n$. O **reticulado dual** de Λ, denotado por Λ^*, é definido por*

$$\Lambda^* = \{x \in \mathbb{R}^n; \langle x, v\rangle \in \mathbb{Z}, \forall v \in \Lambda\}$$

Ou seja, o reticulado dual de um reticulado $\Lambda \subset \mathbb{R}^n$ é o reticulado composto pelo conjunto de todos os vetores do espaço n-dimensional tais que o produto interno desses vetores com todos os elementos de Λ resulta em um número inteiro.

Definição 2.1.14. *Um reticulado é denominado isodual quando ele é geometricamente congruente ao seu dual. Em outras palavras, um reticulado é isodual se ele difere de seu dual somente, possivelmente, por uma rotação ou reflexão.*

Definição 2.1.15. *Dois reticulados são equivalentes na métrica euclidiana se um deles pode ser obtido do outro através de uma composição de uma rotação ou reflexão com multiplicação por um fator de escala. Ou seja, os dois reticulados Λ_1e Λ_2, com matrizes geradoras M_1 e M_2, respectivamente, são equivalentes se, e só se,*

$$M_1 = \sqrt{c}M_2RA$$

onde A é a matriz mudança de base, com entradas inteiras e determinante ± 1, R é uma matriz ortogonal e $\sqrt{c}$ é o fator de escala, com $c \in \mathbb{R}$.

2.2 Empacotamento esférico

Nesta subseção são apresentados os principais conceitos e propriedades envolvendo empacotamentos esféricos, em especial o empacotamento reticulado, dando continuidade ao estudo dos reticulados. Dessa forma, são apresentados os conceitos de empacotamento esférico, seguido de empacotamento reticulado, raio e densidade de empacotamento, raio de cobertura e o número de vizinhos "Kissing Number". As referências utilizadas nesta seção foram [1], [2] e [3].

Definição 2.2.1. *Um empacotamento esférico é uma distribuição de esferas de mesmo raio no espaço $\mathbb{R}^n$ de modo que a interseção de quaisquer duas dessas esferas tenha no máximo um ponto. Podemos nos referir ao empacotamento esférico simplesmente como empacotamento no*

$\mathbb{R}^n$. *Dessa forma, um empacotamento no* $\mathbb{R}^n$ *é uma distribuição de esferas idênticas no espaço n-dimensional de modo que essas esferas não se sobreponham e tenham, no máximo, um ponto de intersecção tomando-se duas delas.*

De acordo com Conway and Sloane [1], o problema clássico do empacotamento esférico consiste em encontrar um arranjo de esferas idênticas no $\mathbb{R}^n$ de modo que a fração do espaço coberta pelas esferas seja a maior possível.

Definição 2.2.2. *Um empacotamento reticulado é um empacotamento no* $\mathbb{R}^n$ *tal que o conjunto dos centros das esferas formam um reticulado* $\Lambda \subset \mathbb{R}^n$. *Dizemos também, nesse caso, que o empacotamento é associado ao reticulado* Λ.

Ao estudarmos os empacotamentos reticulados, o interesse está em determinar o empacotamento associado a um reticulado Λ em que as esferas tenham raio máximo. Esse raio é conhecido como raio de empacotamento e definido a seguir.

Definição 2.2.3. *O raio de empacotamento de um reticulado* Λ *é o maior raio* ρ *tal que* $B_\rho(u) \cap B_\rho(v) = \emptyset, \forall u, v \in \Lambda$, *com* $u \neq v$. *Ou seja, o raio de empacotamento é o maior raio tal que, para quaisquer dois pontos do reticulado* Λ, *as bolas abertas com raio* ρ *centradas nesses pontos não tenham elementos em comum.*

Podemos determinar o valor do raio de empacotamento através da norma mínima de um vetor não nulo do reticulado, que é definida a seguir.

Definição 2.2.4. *A norma mínima* η *de um reticulado* Λ *é definida por*

$$\eta = \min\left\{\|x\|^2, x \in \Lambda, x \neq 0\right\}$$

Dessa forma, a norma mínima tem o mesmo valor do quadrado da distância mínima entre dois pontos do reticulado. Assim, fica definido valor do raio de empacotamento como metade do quadrado da distância mínima entre os pontos do reticulado, ou seja, $\rho = \sqrt{\eta}/2$.

Outro conceito importante relacionado aos empacotamentos, em particular o empacotamento reticulado, é sua densidade, definida a seguir.

Definição 2.2.5. *Dado um empacotamento no* $\mathbb{R}^n$ *associado a um reticulado* Λ, *é definida sua* ***densidade de empacotamento*** *como sendo a proporção do espaço euclidiano n-dimensional coberta pela união das esferas do empacotamento.*

A seguir, é definida a expressão que determina o valor da densidade de empacotamento.

Definição 2.2.6. *Dado um empacotamento no $\mathbb{R}^n$ associado ao reticulado Λ, com base $B = \{v_1, v_2, \cdots, v_m\}$ e raio de empacotamento ρ, a densidade de empacotamento de Λ é dada por*

$$\Delta(\Lambda) = \frac{\text{Vol}(B(\rho))}{\text{Vol}(\Lambda)}$$

onde $B(\rho)$ denota a esfera de centro na origem e raio ρ na dimensão n. Assim, a densidade de empacotamento é definida como a razão entre o volume da esfera de raio ρ e o volume do reticulado Λ.

Podemos simplificar $\text{Vol}(B(\rho)) = \text{Vol}(B(1))\rho^n$, onde $B(1)$ denota a esfera de raio 1 centrada na origem. Assim, a densidade de empacotamento é dada por

$$\Delta(\Lambda) = \frac{\text{Vol}(B(1))\rho^n}{\text{Vol}(\Lambda)}$$

Desse modo, podemos reduzir o problema ao estudo de um outro parâmetro, chamado **densidade de centro**, dado por

$$\delta(\Lambda) = \frac{\rho^n}{\text{Vol}(\Lambda)}$$

e, portanto, a **densidade de empacotamento** de Λ é

$$\Delta(\Lambda) = \text{Vol}(B(1))\delta(\Lambda)$$

ou seja, o produto entre o volume da esfera unitária de dimensão n e a densidade de centro de Λ.

Exemplo 2.2.7. *O reticulado de base $\{v_1, v_2\}$, em que $v_1 = (1, 0)$ e $v_2 = \left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$ é o reticulado mais denso na dimensão 2 , chamado de reticulado hexagonal, cuja densidade de centro é aproximadamente 0, 28868.*

Até aqui, estudamos somente o caso em que as esferas se interceptam em, no máximo, um ponto, tomadas duas a duas, como é definido o empacotamento no $\mathbb{R}^n$. Agora, ao aumentarmos o raio das esferas de um empacotamento no $\mathbb{R}^n$ associado a um reticulado Λ, além do raio de empacotamento, as esferas se sobrepõem. Desse modo, podemos cobrir todo o espaço gerado pelo reticulado Λ, desde que esse novo raio seja suficientemente grande. Definimos esse raio, como se segue.

Definição 2.2.8. *O **raio de cobertura**, denotado por R, de um empacotamento no $\mathbb{R}^n$ associado a um reticulado Λ, é o menor raio associado às esferas que resulta em uma cobertura total do espaço gerado pelo reticulado Λ.*

Em outras palavras, o raio de cobertura é o menor raio, aumentado além do raio de empacotamento, que faz com que as esferas sobrepostas "cubram" todo o espaço gerado pelo reticulado.

O interesse agora nessa etapa dos estudos, sobre os empacotamentos no $\mathbb{R}^n$ associados a um reticulado Λ, está em determinar a melhor cobertura do espaço por esferas sobrepostas. Para mensurar qual seria essa melhor cobertura, utilizamos uma taxa análoga à densidade de empacotamento, definida a seguir.

Definição 2.2.9. *Considerando um arranjo de esferas de raio R (raio de cobertura) centradas nos pontos do reticulado Λ que cobrem todo o $\mathbb{R}^n$, é definida a densidade de cobertura como sendo*

$$\Theta = \frac{\mathrm{Vol}(B(R))}{\mathrm{Vol}(\Lambda)} = \frac{\mathrm{Vol}(B(1))R^n}{\mathrm{Vol}(\Lambda)}$$

As densidades de empacotamento e cobertura satisfazem a seguinte relação:

$$\Delta \leq 1 \leq \Theta$$

ou seja, pelas definições dessas densidades, vemos que o volume de uma esfera com raio de empacotamento ρ é sempre menor ou igual ao volume do reticulado, enquanto que o volume da esfera com raio de cobertura R é sempre maior ou igual ao volume do reticulado.

Enquanto o problema do empacotamento esférico consiste em determinar os empacotamentos mais densos, aqueles que cobrem a maior proporção do espaço, por esferas que se tangenciam, o problema da cobertura reside em determinar os empacotamentos menos densos por esferas que cobrem todo o espaço, de modo que a região de esferas sobrepostas seja a menor possível. Desse modo, vemos que quanto mais próximas de 1, melhor são as densidades, tanto de empacotamento quanto de cobertura.

A seguir, é definido outro parâmetro importante no estudo dos empacotamentos no $\mathbb{R}^n$.

Definição 2.2.10. *O **"kissing number"** τ, ou número de vizinhos, de um empacotamento esférico é o número de esferas idênticas que tocam uma outra esfera idêntica central. Em outras palavras, fixada uma esfera do empacotamento, o kissing number é o número de esferas que tem um ponto de intersecção com essa esfera central.*

No Exemplo 2.2.1, temos que o *kissing number* do reticulado hexagonal é $\tau = 6$.

Em um empacotamento reticulado, o *kissing number* é sempre o mesmo para todas as esferas, mas em um empacotamento qualquer isso não é necessariamente válido. Quanto maior é o valor de τ, mais denso é o empacotamento, uma vez que um número maior de esferas se

tangenciam, cobrindo maior proporção do espaço. Desse modo, o estudo desse parâmetro busca determinar qual o número máximo de esferas idênticas que tangenciam uma outra esfera idêntica central.

Na próxima subseção, são apresentados alguns reticulados já conhecidos na literatura e suas principais propriedades, que foram objeto de estudo.

2.3 Exemplos de reticulados

Após estudarmos os reticulados, seus principais conceitos e propriedades, os empacotamentos no $\mathbb{R}^n$, com suas principais propriedades, com foco nos empacotamentos reticulados, se torna interessante apresentar alguns dos principais reticulados conhecidos na literatura, que serão apresentados nessa seção. Utilizamos nesta subseção as referências [2] e [3].

Desse modo, são apresentados nessa seção os reticulado $A_n, D_n, \mathbb{Z}^n, E_8, E_7, E_6, K_{12}, \Lambda_{16}, \Lambda_{24}$. Foram estudadas as principais propriedades já conhecidas desses reticulados.

2.3.1 Reticulado A_n

É conhecido como o reticulado no hiperplano. É definido por, para $n \geq 1$,

$$A_n = \left\{(x_0, x_1, \ldots, x_n) \in \mathbb{Z}^{n+1}; x_0 + x_1 + \ldots + x_n = 0\right\}$$

Desse modo, A_n é um reticulado n-dimensional no espaço euclidiano $\mathbb{R}^{n+1}$.

Por essa definição, temos que A_n está contido no hiperplano $\sum_{i=0}^{n} x_i = 0$, e uma de suas matrizes geradoras é dada por:

$$M = \begin{pmatrix} -1 & 1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & -1 & 1 & 0 & \ldots & 0 & 0 \\ . & . & . & . & \ldots & . & . \\ 0 & 0 & 0 & 0 & \ldots & -1 & 1 \end{pmatrix}$$

Colocando as principais propriedades estudadas para o reticulado, temos $\det(A_n) = n + 1$, norma mínima $\eta = 2$, raio de empacotamento $\rho = \sqrt{2}/2$, com kissing number $\tau = n(n + 1)$,

densidade de centro $\delta = \frac{2^{-n/2}}{\sqrt{n+1}}$ e densidade de empacotamento

$$\Delta = \begin{cases} \frac{\pi^{n/2}2^{-n/2}}{(n/2)!\sqrt{n+1}}, & \text{se } n \text{ é par} \\ \frac{2^n\pi^{(n-1)/2}((n-1)/2)!2^{-n/2}}{n!\sqrt{n+1}}, & \text{se } n \text{ é ímpar} \end{cases}$$

2.3.2 Reticulado D_n

O reticulado D_n, onde $n \geq 3$, é definido por

$$D_n = \{(x_1, x_2, \ldots, x_n) \in \mathbb{Z}^n; x_1 + x_2 + \ldots + x_n \text{ é par } \}$$

Uma matriz geradora é dada por

$$M = \begin{pmatrix} -1 & -1 & 0 & 0 & \ldots & 0 & 0 \\ 1 & -1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & 1 & -1 & 0 & \ldots & 0 & 0 \\ . & . & . & . & \ldots & . & . \\ 0 & 0 & 0 & 0 & \ldots & 1 & -1 \end{pmatrix}$$

Além disso, temos $\det(D_n) = 4, \eta = 2, \rho = \sqrt{2}/2, \tau = 2n(n-1)$, densidade de centro $\delta = 2^{-(n+2)/2}$ e densidade de empacotamento

$$\Delta = \begin{cases} \frac{\pi^{n/2}2^{-(n+2)/2}}{(n/2)!}, & \text{se } n \text{ é par} \\ \frac{2^n\pi^{(n-1)/2}((n-1)/2)!2^{-(n+2)/2}}{n!}, & \text{se } n \text{ é ímpar} \end{cases}$$

O reticulado D_n é o mais denso nas dimensões $n = 3, 4$ e 5 .

2.3.3 Reticulado $\mathbb{Z}^n$

O reticulado $\mathbb{Z}^n$, para $n \geq 2$, é definido por

$$\mathbb{Z}_n = \{(x_1, x_2, \ldots, x_n); x_i \in \mathbb{Z}\}$$

Possui uma matriz geradora $M = I_n$ (matriz identidade de ordem n). Além disso, $\eta = 1$, $\rho = 1/2, \tau = 2n$, densidade de centro $\delta = 2^{-n}$ e densidade de empacotamento

$$\Delta = \begin{cases} \frac{\pi^{n/2}}{(n/2)!2^n}, & \text{se } n \text{ é par} \\ \frac{2^n \pi^{(n-1)/2}((n-1)/2)!}{n!2^n}, & \text{se } n \text{ é ímpar} \end{cases}$$

No exemplo 2.1.3 temos o reticulado $\mathbb{Z}^n$, para a dimensão $n = 2$.

2.3.4 Reticulado E_8

O reticulado E_8 é um reticulado de dimensão 8, que é dado por

$$E_8 = \left\{(x_1, x_2, \ldots, x_8) \in \mathbb{R}^8; \forall x_i, x_i \in \mathbb{Z} \text{ ou } x_i \in \mathbb{Z} + 1/2, \sum x_i \equiv 0 \pmod 2\right\}$$

Assim, os elementos do reticulado E_8 são vetores de dimensão 8 tal que as coordenadas dos vetores são números inteiros ou inteiros acrescidos de 1/2, além de a soma das coordenadas dos vetores ser um número inteiro par.

Uma de suas matrizes geradoras é dada por

$$M = \begin{pmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 \\ 1/2 & 1/2 & 1/2 & 1/2 & 1/2 & 1/2 & 1/2 & 1/2 \end{pmatrix}$$

Além disso, temos $\det(E_8) = 1, \eta = 2, \rho = \sqrt{2}/2, \tau = 240, \delta(E_8) = 1/16$e $\Delta(E_8) = \pi^4/384$. Esse é o reticulado de maior densidade conhecida no espaço euclidiano $\mathbb{R}^8$.

2.3.5 Reticulado E_7

O reticulado E_7 é um reticulado 7-dimensional, definido por

$$E_7 = \{(x_1, x_2, \ldots, x_8) \in E_8; x_1 + x_2 + \ldots + x_8 = 0\},$$

ou seja, E_7 é um reticulado de dimensão 7 no espaço 8-dimensional e, além disso, é um sub-reticulado de E_8.

Uma das matrizes geradoras de E_7 é dada por

$$M = \begin{pmatrix} -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 \\ 1/2 & 1/2 & 1/2 & 1/2 & -1/2 & -1/2 & -1/2 & -1/2 \end{pmatrix}$$

Além disso, temos $\det(E_7) = 2, \eta = 2, \rho = \sqrt{2}/2, \tau = 126, \delta(E_7) = 1/16$e $\Delta(E_7) = \pi^3/105$. Esse é o reticulado com maior densidade conhecida na dimensão 7.

2.3.6 Reticulado E_6

O reticulado E_6, também sub-reticulado de E_8, é um reticulado de dimensão 6 no espaço 8-dimensional definido por

$$E_6 = \{(x_1, x_2, \ldots, x_8) \in E_8; x_1 + x_8 = x_2 + x_3 + x_4 + x_5 + x_6 + x_7 = 0\}$$

Uma matriz geradora de E_6 é dada por

$$M = \begin{pmatrix} 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 \\ 1/2 & 1/2 & 1/2 & 1/2 & -1/2 & -1/2 & -1/2 & -1/2 \end{pmatrix}$$

Para esse reticulado, temos $\det(E_6) = 3, \eta = 2, \rho = \sqrt{2}/2, \tau = 72, \delta(E_6) = 1/8\sqrt{3}$ e $\Delta(E_6) = \pi^3/48\sqrt{3}$. Esse é o reticulado com maior densidade conhecida no espaço 6-dimensional.

2.3.7 Reticulado K_{12}

O reticulado K_{12}, também conhecido como reticulado de Coxeter-Todd, pois foi descrito por esses em 1954, é um reticulado 12-dimensional. Uma de suas matrizes geradoras é dada por

$$M = \begin{pmatrix}
2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & -\frac{1}{2} & -\frac{1}{2} & 1 & 0 & 0 & 0 & \frac{\sqrt{3}}{2} & \frac{\sqrt{3}}{2} & 0 & 0 & 0 \\
-\frac{1}{2} & 1 & -\frac{1}{2} & 0 & 1 & 0 & \frac{\sqrt{3}}{2} & 0 & \frac{\sqrt{3}}{2} & 0 & 0 & 0 \\
-\frac{1}{2} & -\frac{1}{2} & 1 & 0 & 0 & 1 & \frac{\sqrt{3}}{2} & \frac{\sqrt{3}}{2} & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & -\sqrt{3} & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & -\sqrt{3} & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & -\sqrt{3} & 0 & 0 & 0 \\
\frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & 0 & 0 & -\frac{\sqrt{3}}{2} & \frac{\sqrt{3}}{2} & \frac{\sqrt{3}}{2} & -\frac{\sqrt{3}}{2} & 0 & 0 \\
\frac{1}{2} & \frac{1}{2} & \frac{1}{2} & 0 & \frac{1}{2} & 0 & \frac{\sqrt{3}}{2} & -\frac{\sqrt{3}}{2} & \frac{\sqrt{3}}{2} & 0 & -\frac{\sqrt{3}}{2} & 0 \\
\frac{1}{2} & \frac{1}{2} & \frac{1}{2} & 0 & 0 & \frac{1}{2} & \frac{\sqrt{3}}{2} & \frac{\sqrt{3}}{2} & -\frac{\sqrt{3}}{2} & 0 & 0 & -\frac{\sqrt{3}}{2}
\end{pmatrix}.$$

Temos que $\det(K_{12}) = 729, \eta = 4, \rho = 1, \tau = 756, \delta(K_{12}) = 1/27$ e $\Delta(K_{12}) = \pi^6/19440$. O reticulado K_{12} é o reticulado com maior densidade conhecida na dimensão 12 .

2.3.8 Reticulado Λ_{16}

O reticulado Λ_{16}, também conhecido como reticulado de Barnes-Wall, descrito por esses em 1959, é um reticulado no espaço 16-dimensional. Uma matriz geradora é dada por

$$M = \frac{1}{\sqrt{2}} \begin{pmatrix} 4 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 1 & 0 & 0 & 0 & 1 \\ 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Além disso, temos $\det(\Lambda_{16}) = 256, \eta = 4, \rho = 1, \tau = 4320, \delta(\Lambda_{16}) = 1/16$ e $\Delta(\Lambda_{16}) = \pi^8/16$ (8 !). O reticulado Λ_{16} é o reticulado mais denso conhecido em dimensão 16 .

2.3.9 ReticuladoΛ_{24}

O reticulado Λ_{24} é um reticulado no espaço 24-dimensional e foi descrito por Leech em 1965. Uma de suas matrizes geradoras é dada por

$$M = \frac{1}{\sqrt{8}} \begin{pmatrix}
8 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
4 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
4 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
4 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
4 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
4 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
4 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 2 & 2 & 2 & 0 & 0 & 0 & 0 & 2 & 2 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 0 & 2 & 0 & 2 & 0 & 0 & 2 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 0 & 0 & 2 & 2 & 2 & 0 & 0 & 2 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\
2 & 2 & 0 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\
0 & 2 & 2 & 2 & 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 \\
-3 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1
\end{pmatrix}.$$

Além disso, temos que $\det(\Lambda_{24}) = 1, \eta = 4, \rho = 1, \tau 196560, \delta(\Lambda_{24}) = 1\text{e}\ \Delta(\Lambda_{24}) = \pi^{12}/12$!. O reticulado Λ_{24} é o reticulado de maior densidade conhecida em dimensão 24.

2.4 Vetor de norma mínima em reticulados

Nesta subseção é explicado o que são os problemas existentes no estudo de reticulados, consistindo no problema do vetor mais curto (SVP - *shortest vector problem*) e no problema

do vetor mais próximo (CVP - *closest vector problem*), embasado em (SILVERMAN; PIPHER; HOFFSTEIN, 2014). Tanto o SVP quanto o CVP se tornam computacionalmente difíceis à medida que a dimensão n do reticulado cresce.

2.4.1 Problema do vetor mais curto (SVP - *shortest vector problem*)

Consiste em encontrar o vetor não nulo mais curto em um reticulado Λ, isto é, encontrar um vetor não nulo $v \in \Lambda$ que minimiza a norma euclidiana $\|\nu\|$.

É importante observar que pode existir mais de um vetor não nulo que satisfaça o SVP em um reticulado. Por exemplo, em $\mathbb{Z}^2$, todos os vetores na forma $(0, \pm 1)$ e $(\pm 1, 0)$ são soluções para o SVP. Esse é o motivo pelo qual o problema SVP exige "um" vetor mais curto e não "o" vetor mais curto.

2.4.2 Problema do vetor mais próximo (CVP - *closest vector problem*)

Dado um vetor $w \in \mathbb{R}^n$, busca-se encontrar o vetor $v \in \Lambda$ que é mais próximo a w, isto é, encontrar um vetor $v \in \Lambda$ que minimiza a norma euclidiana $\|w - v\|$.

2.4.3 Problemas variados de SVP e CVP

Existem algumas variações dos problemas SVP e CVP que são aplicados tanto na Teoria dos Reticulados, de acordo com (BOLLAUF, 2014), a saber:

2.4.3.1 Problema da base mais curta (SBP)

Consiste em encontrar uma base $v_1, \ldots, v_n$ para um reticulado tal que ela seja a mais curta em algum parâmetro. Por exemplo, podemos querer que

$$\max_{1 \leq i \leq n} \|v_i\| \text{ ou } \sum_{i=1}^{n} \|v_i\|^2$$

sejam mínimos. Existem diferentes versões desse problema, dependendo dos parâmetros usados para medir o tamanho da base.

2.4.3.2 Problema do vetor mais curto aproximado (ApprSVP)

Seja $\psi(n)$ uma função de n. Em um reticulado Λ de dimensão n, buscamos encontrar um vetor não nulo que não seja maior do que $\psi(n)$ vezes maior do que qualquer outro vetor não nulo mais curto. Em outras palavras, se v_s é o vetor mais curto em Λ, queremos encontrar um vetor não nulo $v \in \Lambda$ que satisfaz:

$$\|v\| \leq \psi(n) \|v_s\|$$

E cada escolha distinta para $\psi(n)$ define um problema APPRSVP distinto. Por exemplo, considere um algoritmo que queira encontrar $v \in \Lambda$ satisfazendo

$$\|v\| \leq 3\sqrt{n} \|v_s\| \text{ ou } \|v\| \leq 2^{n/2} \|v_s\| .$$

Claramente um algoritmo que resolve o primeiro dos problemas é mais forte do que um algoritmo que resolve o segundo.

2.4.3.3 Problema do vetor mais próximo aproximado (ApprCVP)

É igual ao ApprSVP, mas agora estamos procurando um vetor que aproxime a solução do CVP, ao invés de aproximar a solução do SVP.

2.4.4 Teorema de Hermite

Teorema 2.4.1. *(Teorema de Hermite) Todo reticulado L de dimensão n contém um vetor v diferente de zero satisfazendo*

$$||v||^2 \leq \sqrt{n} \det(L)^{1/n}$$

Para uma dada dimensão n, a **constante de Hermite** γ_n é o menor valor tal que todo reticulado L de dimensão n contém um vetor diferente de zero $v \in L$ satisfazendo

$$||v||^2 \leq \gamma_n \det(L)^{2/n}$$

Para fins criptográficos, estamos principalmente interessados no valor de γ_n quando n é grande.

Observação 2.4.0.1. *Uma das versões do Teorema de Hermite é o Teorema de Gram-Schmidt. Ele descreve um procedimento para transformar uma base linearmente independente de um espaço vetorial em uma base ortogonal desse espaço. O processo consiste em construir uma nova base de vetores ortogonais a partir da base original.*

2.4.4.1 Raio de Hadamard

O raio de Hadamard é outra versão da constante de Hermite, ele serve para medir a qualidade de uma base $\mathcal{B}$ de um reticulado Λ em termos de ortogonalidade e eficiência. Ele é denotado como $\mathcal{H}(\mathcal{B})$ e está relacionado ao volume do paralelepípedo gerado pela base do reticulado. O seu valor está limitado entre 0 e 1 e quanto maior for o Raio de Hadamard, melhor a base é em termos de ortogonalidade e eficiência.

Definição 2.4.1. *O **Raio de Hadamard** de uma base $\mathcal{B} = \{v_1, ..., v_n\} \in \Lambda$ é definido como o raio da menor esfera centrada na origem que contém a região fundamental associada à base $\mathcal{B}$ e pode ser calculado por:*

$$\mathcal{H}(\mathcal{B}) = \left(\frac{\det(\Lambda)}{\|\boldsymbol{v}_1\| \, \|\boldsymbol{v}_2\| \cdots \|\boldsymbol{v}_n\|} \right)^{1/n}, \tag{2.4.4.1}$$

onde $\det \Lambda$ *é o determinante da matriz de Gram.*

2.5 Base reduzida de reticulado

Uma base reduzida de um reticulado é um conjunto especial de vetores que formam uma base para o reticulado e têm certas propriedades que tornam sua representação mais eficiente e única. Grosso modo, os coeficientes dos vetores da base reduzida são reduzidos ao máximo possível. Isso significa que os vetores da base reduzida possuem as menores normas possíveis.

A obtenção de uma base reduzida envolve técnicas algorítmicas, como o algoritmo de redução de base de LLL (Lenstra-Lenstra-Lovász), o qual será explicado na próxima seção. Além disso, o teorema de Hermite e o raio de Hadamard também auxiliam no processo de reduzir uma base.

Quando falamos de "base" de reticulado, podemos defini-las como: base boa ou base ruim. Uma base boa para um reticulado, é uma base que consiste em vetores curtos e que, dois a dois, sejam o mais ortogonal possível e uma base ruim para um reticulado, por sua vez, é a formada por vetores de normas bem distintas e que geralmente possuem o ângulo entre eles muito pequenos ou muito grandes.

Geometricamente:

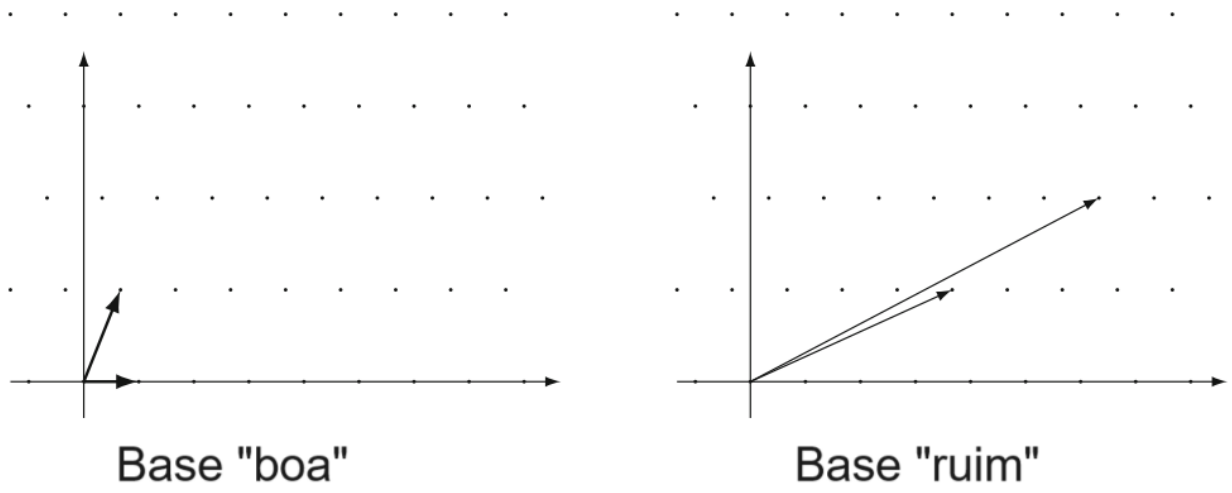

Figura 2.2: Uma base boa e uma base ruim do mesmo reticulado. (Hoffstein, J. et al., 2014, p. 405.)

A seguir apresentamos um exemplo onde vamos alterando a base do reticulado e acompanhando o que acontece com o raio de Hadamard.

Exemplo 2.5.1. *Considere o reticulado bidimensional* $\mathbb{Z}^2$.

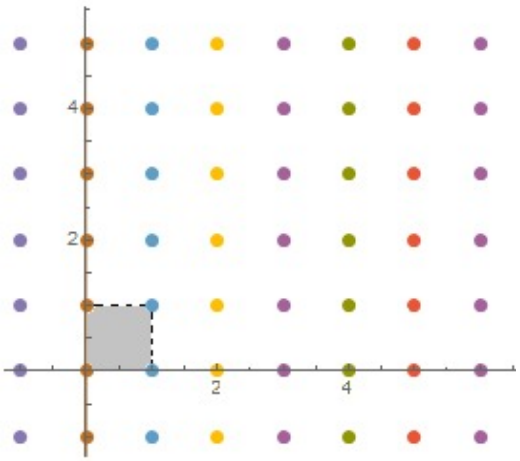

Figura 2.3: Base (1,0),(0,1) para $\mathbb{Z}^2$

Claramente, esta é uma base "boa", visto que seus vetores são ortogonais. Quando calculamos o raio de Hadamard para esta base obtemos o valor 1*, pelo fato do ângulo entre os vetores ser exatamente* 90 *graus. Mais tarde, implementaremos o algoritmo de Babai para esta e as próximas bases.*

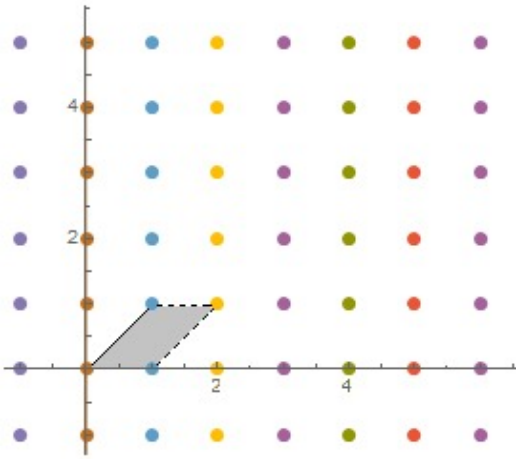

Figura 2.4: Base (1,0),(1,1) para $\mathbb{Z}^2$

Neste caso, temos uma base "levemente" ortogonal, com o ângulo entre os vetores de $45°$*, o raio de Hadamard tem o valor aproximado de* $0,840896$*, próximo a* 1*, o que podemos considerar como um bom sinal de eficiência e ortogonalidade.*

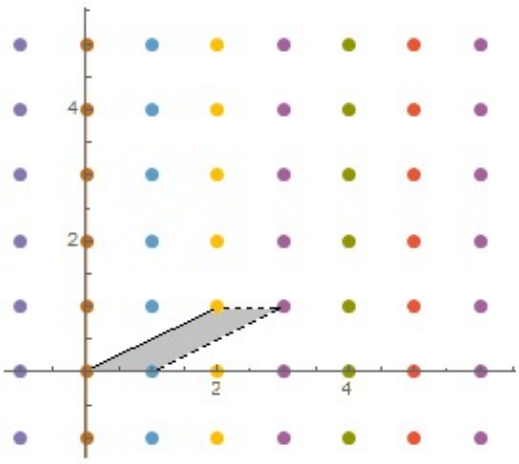

Figura 2.5: Base (1,0),(2,1) para $\mathbb{Z}^2$

No caso acima o ângulo entre os vetores é aproximadamente $26.5°$*. Ao calcularmos o raio de Hadamard obtemos aproximadamente* $0,66874$*, um valor mais próximo de* 1*, porém, a sua funcionalidade é questionada. Analisaremos está questão na subseção a seguir.*

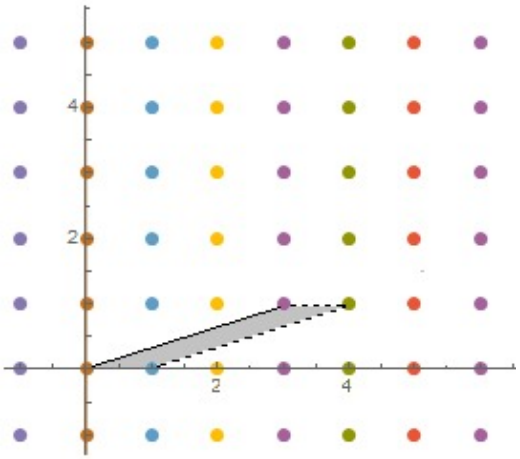

Figura 2.6: Base (1,0),(3,1) para $\mathbb{Z}^2$

Neste caso, temos o ângulo entre os vetores de $18.4°$*, o raio de Hadamard aproximado de* $0,562341$ *e nada podemos afirmar sobre sua funcionalidade algebricamente. Porém, geometricamente, percebemos sua não-ortogonalidade.*

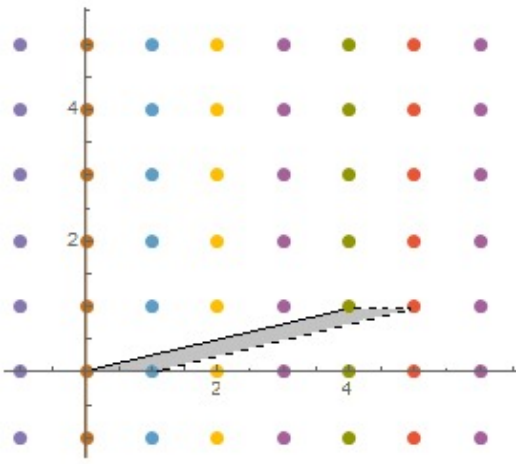

Figura 2.7: Base (1,0),(4,1) para $\mathbb{Z}^2$

Para esta base, o raio de Hadamard mede aproximadamente $0,492479$ *e o ângulo entre os vetores é de* $14°$*. Já geometricamente, vemos o quão não-ortogonal é esta base, já que os ângulos entre os vetores é pequeno, assim sendo, podemos considerá-la uma "base ruim".*

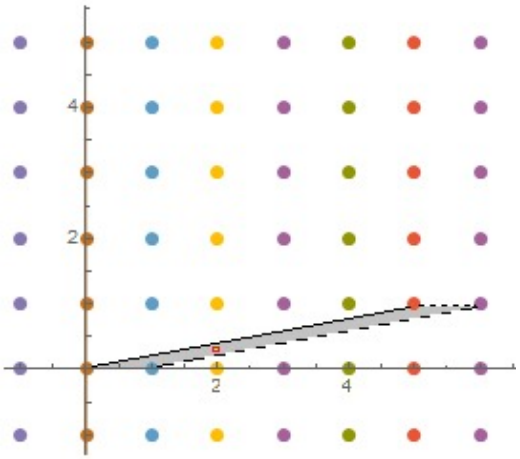

Figura 2.8: Base (1,0),(5,1) para $\mathbb{Z}^2$

Por fim, neste último caso, geometricamente notamos um ângulo pequeno entre os vetores, algebricamente, o ângulo mede aproximadamente $12°$*, temos o raio de Hadamard medindo* $0,44285$.

Nota-se que nesse exemplo, podemos exibir uma base tão "ruim" quanto se queira, uma vez que exibimos 6 bases da forma $B_n = \{(1,0),(n,1)\}$ para $0 \leq n \leq 5$, mas para qualquer $n \in \mathbb{N}$, temos que B_n é base de $\mathbb{Z}^2$, e sendo θ o ângulo entre os vetores $(1,0)$ e $(n,1)$, temos:

$$(1,0).(n,1) = ||(1,0)||.||(n,1)|| \cos\theta$$
$$n = \sqrt{n^2+1}\cos\theta$$
$$\cos\theta = \frac{n}{\sqrt{n^2+1}}$$

Agora, vejamos o que acontece com o ângulo θ se n cresce indefinidamente:

$$\lim_{n\to\infty} \frac{n}{\sqrt{n^2+1}} = \lim_{n\to\infty} \frac{1}{\sqrt{1+\frac{1}{n^2}}} = 1.$$

Logo, para $n \in \mathbb{N}$ suficientemente grande, $\cos\theta$ se aproxima do valor 1, portanto, θ se aproxima de zero e consequentemente o raio de Hadamard

$$\mathcal{H}(B) = \left(\frac{1}{\sqrt{n^2+1}}\right)^{1/2}$$

também se aproxima de zero quando n cresce indefinidamente.

2.5.1 Algoritmo de Lattice Reduction - LLL

Em geral, os criptossistemas que serão vistos tem suas seguranças dependendo da dificuldade de resolver apprSVP e/ou apprCVP em vários tipos de reticulados. Nesta seção descrevemos o algoritmo LLL que resolve esses problemas dentro de um fator de C^n, onde C é uma pequena constante e n é a dimensão do reticulado.

Assim, em pequenas dimensões, o algoritmo LLL chega perto de resolver SVP e CVP, mas em grandes dimensões não o faz tão bem. Em última análise, a segurança de criptossistemas baseados em reticulados depende da incapacidade do LLL e outros algoritmos de redução de reticulados para resolver eficientemente o apprSVP e o apprCVP dentro de uma dimensão alta.

Teorema 2.5.1. *Seja $v_1, ..., v_n$ uma base para um reticulado $\Lambda \in \mathbb{Z}^n$. O algoritmo descrito na figura abaixo termina em um número finito de etapas e retorna uma base reduzida LLL para Λ.*

Mais precisamente, seja $B = \max ||v_i||$. Então o algoritmo executa o k loop principal (Passos [4–14]) não mais que $O(n^2 \log n + n^2 \log B)$ vezes. Em particular, o algoritmo LLL é um algoritmo de tempo polinomial.

Algoritmo 1: Algoritmo LLL

Entrada: Uma base $(b_1, \cdots, b_n)$ para L

Saída: Uma base LLL reduzida $(b'_1, \cdots, b'_n)$

Calcule $(b^*_1, \cdots, b^*_n)$ usando o método de ortogonalização de Gram-Schmidt;

$k = 2$;

enquanto $i \leq n$

$b_i = b_i - \sum_{j=1}^{i-1} \lfloor \mu_{i,j} \rceil b_j$;

se $||b^*_i||^2 \geq \left(\frac{3}{4} - \mu^2_{i,i-1}\right) ||b^*_{i-1}||^2$ **então**

$i = i + 1$;

se não

Troque b_i e b_{i-1};

$i = \max\{2, i-1\}$;

imprima$[i]$

O algoritmo LLL procura uma base ortogonal, ou a mais ortogonal possível, já que as coloca em ordem e o primeiro vetor que aparece é o de norma mínima. O algoritmo LLL tem muitas aplicações na criptoanálise, desde ataques a criptossistemas de chave pública de mochila e ao sistema RSA, até para atacar criptossistemas baseados em reticulados, como o GGH e o NTRU. Todos esses criptossistemas serão abordados neste trabalho. É importante enfatizar que

o algoritmo LLL e suas generalizações têm uma ampla variedade de aplicações em Matemática Pura e Aplicada fora de seus usos em criptografia.

Entretanto, para uso em sistemas criptográficos o algoritmo LLL não tem problemas para atacar e quebrar códigos quando estamos em dimensões regulares, não tão grandes Na prática, instâncias seguras desses criptossistemas requerem reticulados de dimensão entre 500 e 1000, que, exceto para NTRUEncrypt, levam a comprimentos de chave impraticáveis.

2.5.2 Algoritmo de Babai

Antes de apresentar os criptossistemas, é necessário estudar o Algoritmo de Babai, uma vez que este é utilizado para decriptar mensagens em tais criptossistemas, já que ajuda a resolver os SVP e CVP.

Seja um reticulado Λ com uma base $v_1, v_2, \ldots, v_n$ formada por vetores dois a dois ortogonais, ou seja,

$$< v_i v_j >= 0, \forall i \neq j.$$

Resolvemos os problemas SVP e CVP utilizando o algoritmo de Babai.

Quando resolvemos o SVP, devemos lembrar que o comprimento de qualquer vetor no reticulado Λ é dado pela fórmula:

$$\|a_1 v_1 + a_2 v_2 + \cdots + a_n v_n\|^2 = a_1^2 \|v_1\|^2 + a_2^2 \|v_2\|^2 + \cdots + a_n^2 \|v_n\|^2 .$$

Como $a_1, \ldots, a_n \in \mathbb{Z}$, é fácil ver que os vetores mais curtos não nulos em Λ são os vetores mais curtos no conjunto $\{\pm v_1, \pm v_2, \ldots, \pm v_n\}$.

Quando falamos do CVP, precisamos encontrar o vetor em Λ que está mais próximo a um dado vetor $w \in \mathbb{R}^n$. Escrevemos, primeiramente:

$$w = t_1 v_1 + t_2 v_2 + \cdots + t_n v_n, \text{ com } t_1, \ldots, t_n \in \mathbb{R}.$$

Então, para $v = a_1 v_1 + a_2 v_2 + \cdots + a_n v_n \in \Lambda$, temos:

$$\|v - w\| = (a_1 - t_1)^2 \|\nu_1\|^2 + (a_2 - t_2)^2 \|v_2\|^2 + \cdots + (a_n - t_n)^2 \|v_n\|^2 . \tag{2.5.2.1}$$

Como a_i deve ser inteiro, a Equação 2.5.2.1 será minimizada se tomarmos cada a_i como sendo o inteiro mais próximo ao correspondente t_i.

Vemos que o algoritmo apresentado, só funciona perfeitamente com bases ortogonais, ou as mais ortogonais possíveis. Caso a base não seja ortogonal, o algoritmo não irá funcionar corretamente.

A base $\{v_1, v_2, \ldots, v_n\}$ para o reticulado Λ determina uma região fundamental F. Sabemos que as translações de F por elementos de Λ preenchem todo o espaço $\mathbb{R}^n$, logo, cada $w \in \mathbb{R}^n$ está em uma única translação $F + v$ de F por um elemento $v \in \Lambda$. Consideramos o vértice do paralelogramo $\Lambda + v$ que está mais próximo a w, nosso vetor alvo, como sendo nossa solução hipotética para o problema CVP. Encontramos o vértice mais próximo, já que:

$$w = v + \varepsilon_1\nu_1 + \varepsilon_2 v_2 + \cdots + \varepsilon_n v_n, \text{ para algum } 0 \leq \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n < 1$$

e então, somente substituímos ε_i por 0 se ele for menor do que $\frac{1}{2}$ e substituímos por 1 se ele for maior ou igual a $\frac{1}{2}$.

Algoritmo de Babai para o Vértice mais Próximo: *Seja $\Lambda \subset \mathbb{R}^n$ um reticulado com base $v_1, v_2, \ldots, v_n$ e seja $w \in \mathbb{R}^n$ um vetor arbitrário. Se os vetores da base forem suficientemente ortogonais um ao outro, então resolvemos o CVP conforme o algoritmo abaixo:*

Algoritmo 2: Algoritmo de Babai

Entrada $w = t_1v_1 + t_2v_2 + \cdots + t_nv_n$, com $t_1, \ldots, t_n \in \mathbb{R}$.

Defina $a_i = \lfloor t_i \rceil$ para $i = 1, 2, \ldots, n$.

$v = a_1v_1 + a_2v_2 + \cdots + a_nv_n$

Imprima$[v]$.

Exemplo 2.5.2. *Considere a seguinte base para um reticulado 2-dimensional:*

Base Boa:

$$\mathbf{v}_1 = (2, 1); \mathbf{v}_2 = (1, 2)$$

Agora, suponha que temos o seguinte vetor alvo w:

$$w = (7, 4)$$

Vamos aplicar o Algoritmo de Babai para encontrar o vetor mais próximo v no reticulado gerado pela Base Boa para w:

Escreva w como uma combinação linear dos vetores da base:

$$w = t_1\mathbf{v}_1 + t_2\mathbf{v}_2$$

Neste caso:

$$(7,4) = t_1(2,1) + t_2(1,2)$$

Isso nos dá as equações: $\begin{cases} 7 = 2t_1 + t_2 \\ 4 = t_1 + 2t_2 \end{cases}$

Resolvendo este sistema encontramos que $t_1 = 3$ *e* $t_2 = 1$.

Agora, podemos calcular o vetor v *usando* t_1 *e* t_2*:* $v = t_1\mathbf{v}_1 + t_2\mathbf{v}_2$ *Substituindo os valores:* $v = 3(2,1) + 1(1,2) = (6,3) + (1,2) = (7,5)$

Portanto, o vetor mais próximo v *do reticulado gerado pela base boa para o vetor* $w = (7,4)$ *é* $v = (7,5)$.

Voltaremos ao Exemplo 2.5.1, utilizando o reticulado $\mathbb{Z}^2$ e diferentes bases, para analisarmos a funcionalidade das bases para determinar em quais delas o Algoritmo de Babai funciona.

- **Base {(1,0),(0,1)}** - Figura 2.4

  Quando tomamos um vetor alvo $w = (0.8, 0.8)$ vemos que o vetor mais próximo que pertence ao reticulado é o vértice da região fundamental $(1,1)$. O algoritmo de Babai entrega exatamente este vetor, funcionando perfeitamente, já que temos uma base ortogonal e o raio de Hadamard igual a 1.

- **Base {(1,0),(1,1)}** - Figura 2.5

  Neste caso, pensamos no vetor alvo $w = (1.92, 0.96)$. Geometricamente, analisamos que o vetor do reticulado mais próximo de w é o vértice da região fundamental, ou seja, o algoritmo de Babai funciona. O raio de Hadamard dessa base é $0,840896$.

- **Base {(1,0),(2,1)}** - Figura 2.6

  É nesta base em que não podemos confiar no algoritmo de Babai, vemos que o raio de Hadamard pode ser um indicador, já que ele reduz para $0,66874$. Tomando um veto alvo $w = (1.19, 0.55)$, o vetor mais próximo do reticulado é o $(1,1)$ que não pertence a região fundamental. O algoritmo de Babai não funciona, pois este percorre apenas os vértices da região, dessa forma entregando o vetor $(2,1)$ como o mais próximo de w ao invés do $(1,1)$.

- **Base {(1,0),(3,1)}** - Figura 2.7

  Análago ao exemplo anterior, com raio de Hadamard igual a $0,562341$, podemos tomar um vetor alvo em que o vetor mais próximo não é o mesmo entregue pelo algoritmo de Babai. Se $w = (2.1, 0.67)$, o vetor $(2,1) \in \mathbb{Z}^2$ é o mais próximo de w, e não o vetor $(3,1)$ conforme entregue pelo algoritmo.

- **Base {(1,0),(4,1)}** - Figura 2.8

  Se $w = (2, 0.28)$ é o vetor alvo, o algoritmo de Babai nos entrega o vetor $(1, 0)$ como o mais próximo, porém, a verdade é que o vetor mais próximo é $(2, 0)$, que não é um vértice da região fundamental. O raio de Hadamard para esse caso é igual a $0, 492479$.

- **Base {(1,0),(5,1)}** - Figura 2.9

  Por fim, fica evidente que nesta base não ortogonal, com raio de Hadamard $0, 44285$, dado um vetor alvo qualquer na região fundamental, não teremos o algoritmo de Babai funcionando com eficiência. Seja $w = (4.2, 0.84)$, o vetor mais próximo de w é $(4, 1)$. Como $(4, 1)$ não é um dos vértices da região fundamental, o algoritmo não funciona, pois entrega o vetor $(5, 1)$.

2.5.3 Testes utilizando o Wolfram Mathematica

2.5.3.1 Análise no $\mathbf{R}^2$

Na presente análise, realizamos uma série de testes no Mathematica Wolfram, com o objetivo de examinar o comportamento do algoritmo de Babai no espaço $\mathbb{R}^2$ e identificar condições sob as quais ele falha. Observamos, inicialmente, que, quando os vetores de entrada possuem tamanhos iguais, o ângulo entre eles não parece interferir no desempenho do algoritmo, isto é, o algoritmo de Babai executa o procedimento sem aparentes erros. Contudo, ao multiplicar um dos vetores da base por um escalar, alterações foram percebidas. Notamos que, em alguns ângulos específicos entre os vetores, o algoritmo falhava.

Um exemplo notável ocorreu ao triplicarmos o valor de um dos vetores e reduzirmos o ângulo entre eles. Nessa configuração, o algoritmo de Babai falhou, indicando que, em determinadas condições, especialmente quando um vetor é ampliado em escala e o ângulo entre os vetores é muito pequeno, o desempenho do algoritmo se torna comprometido. Por outro lado, mantendo os vetores da base de mesmo tamanho e variando o ângulo entre eles livremente, nota-se que o algoritmo permanece funcional.

Essas observações constituem uma conjectura baseada nos experimentos realizados, sugerindo que a relação entre o tamanho e o ângulo dos vetores exerce influência direta na eficácia do algoritmo de Babai em certas configurações geométricas.

A tabela a seguir apresenta uma síntese dos resultados observados nos testes realizados para identificar as condições de falha do algoritmo de Babai. Nela, estão dispostos os valores

dos escalares α aplicados a um dos vetores da base e os ângulos θ máximos entre os vetores que levaram à ocorrência de falhas.

Esses valores de θ correspondem aos ângulos críticos, abaixo dos quais o algoritmo deixou de funcionar corretamente. Quando $\alpha = 1$, ou seja, quando ambos os vetores possuem o mesmo tamanho, nenhuma falha foi observada independentemente do ângulo entre eles. Nos demais casos, conforme α aumentava, observamos que ângulos maiores intensificavam a possibilidade de falha, não necessitando que o ângulo fosse muito pequeno, uma vez que os vetores já tinham proporções muito diferentes, conforme indicado na tabela. Essa análise permite identificar a sensibilidade do algoritmo de Babai a variações de tamanho e ângulo entre os vetores da base no espaço $\mathbb{R}^2$.

Tabela 2.1: Ângulo θ com falha no algoritmo de Babai a partir da multiplicação de um escalar α

α	Agudos $\theta \leq$	Obtusos $\theta \geq$
1	-	-
2	$45°$	$135°$
3	$61,875°$	$118,125°$
4	$67,5°$	$112,5°$
5	$73,125°$	$106,875°$
8	$78,75°$	$101,25°$

Descrição do Algoritmo

O algoritmo implementado procura por bases $B = \{u, v\}$ em que o Algoritmo de Babai não funcione no espaço bidimensional:

1. **Definição dos vetores da base e ângulos associados**: Fixamos o primeiro vetor base como sendo $u = (1, 0)$, o algoritmo define ângulos em múltiplos de θ, cobrindo até π radianos com aumentos em divisões de $\pi/32$ radianos. Esses ângulos determinam as direções nas quais novos vetores serão calculados. Para cada etapa $j\theta$, com $j = 1, 2, \ldots, 31$, obtemos o vetor $v = (v_1, v_2)$ rotacionando o vetor u, no sentido anti-horário, por um ângulo $j\theta$, ou seja,

$$v = \alpha(\cos(j\theta), \text{sen}(j\theta)).$$

O escalar α servirá para o estudo do algoritmo de Babai quando os vetores tiverem normas distintas. Se $\alpha = 1$, então os vetores u e v possuem a mesma norma,

2. **Subdivisão da Região Fundamental**: Após estabelecer os vetores, a região fundamental formada por dois vetores do reticulado é subdividida em s regiões menores, com um vetor alvo posicionado no centro de cada sub-região, conforme a imagem abaixo. O objetivo é verificar se existe um vetor do reticulado mais próximo ao vetor alvo, sem que esse vetor do reticulado seja um dos vértices da região fundamental.

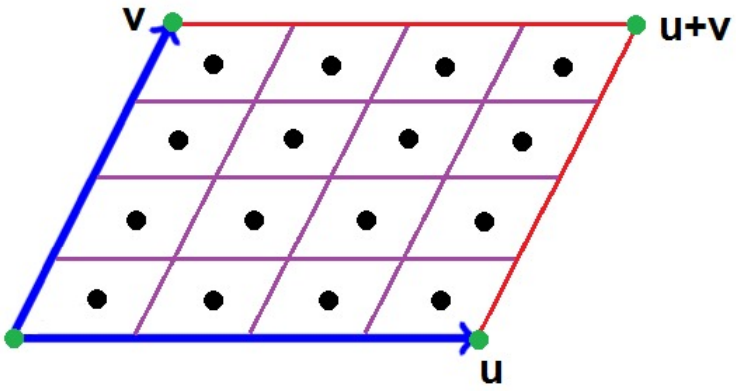

Figura 2.9: Região fundamental dividida em 16 subregiões.

3. **Verificação da Falha do Algoritmo de Babai**: Para cada vetor alvo no centro das sub-regiões, o algoritmo verifica a presença de vetores do reticulado que estejam mais próximos do alvo que os vértices da região fundamental. Caso um vetor seja encontrado, isso indica uma falha do algoritmo de Babai na aproximação do vetor alvo. A imagem a seguir ilustra um exemplo onde o Algoritmo de Babai funcionou.

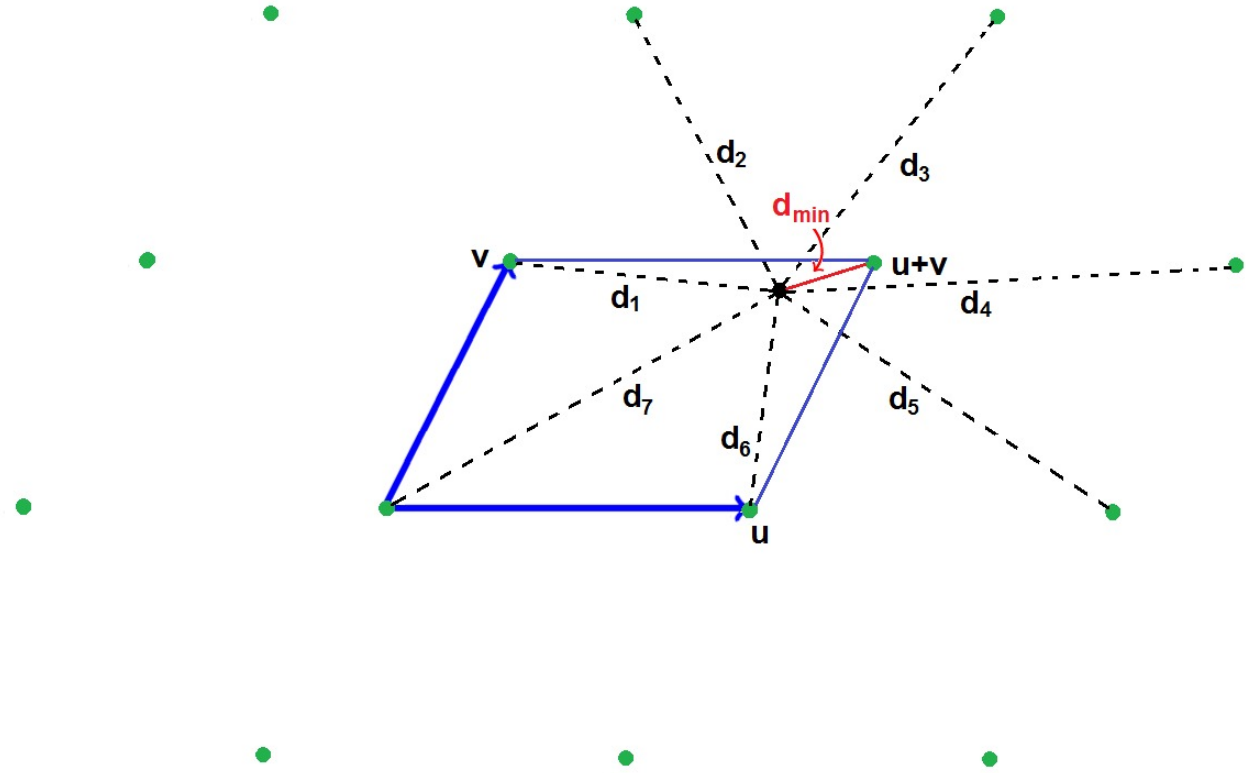

Figura 2.10: Verificação da Falha do Algoritmo de Babai

4. **Identificação do vetor alvo e os vetores mais próximos a ele**: O algoritmo finaliza registrando os vetores que estão mais próximos do vetor alvo de cada sub-região do que qualquer um dos vértices, evidenciando onde ocorre a falha do algoritmo de Babai.

2.5.3.2 Análise no $\mathbf{R}^3$

Analogamente, foram realizados testes para avaliar o desempenho do algoritmo de Babai em reticulados no espaço tridimensional $\mathbb{R}^3$. A análise focou-se em duas configurações de vetores: uma em que todos os vetores têm a mesma norma e outra em que as normas dos vetores diferem significativamente.

Configuração 1: Vetores de Base com Normas Iguais

Na primeira série de experimentos, os vetores da base tinham a mesma norma. Observou-se que, conforme o menor ângulo entre os vetores da base aumentava, aproximando-se de 90°, a eficácia do algoritmo de Babai aumentava. De forma mais específica, quando dois dos ângulos entre os três vetores eram iguais e maiores, o algoritmo não apresentou falhas. No entanto,

Algoritmo 3: Falha do Babai no R2

Entrada: $\theta_j = \frac{\pi_j}{32}$, $j = 1, 2, ..., 31$; α
$j = 1$;
Enquanto $j \leq 31$
$u = (1, 0)$;
$v = \alpha(\cos(\theta_j), \text{sen}(\theta_j))$
Entrada: q q: total de subregiões (quadrado perfeito);
$s = \sqrt{q}$;
$i_1 = 1$;
Enquanto $i_1 \leq s$
$j_1 = 1$;
Enquanto $j_1 \leq s$
$w_1 = \frac{2i_1-1}{2s}v + \frac{2j_1-1}{2s}u$;
Var = 10;
$i = -\text{Var}$;
Enquanto $i \leq \text{Var}$
$j = -\text{Var}$;
Enquanto $j \leq \text{Var}$
$w = iu + jv$;
$eq_1 = ||w_1 - w|| - ||w_1||$;
$eq_2 = ||w_1 - w|| - ||w_1 - u||$;
$eq_3 = ||w_1 - w|| - ||w_1 - v||$;
$eq_4 = ||w_1 - w|| - ||w_1 - u - v||$;
Se $eq_1 < 0$ e $eq_2 < 0$ e $eq_3 < 0$ e $eq_4 < 0$, **então**
vet= $(v_1, w, R[i, 1])$; v_1: vetor mais próximo, w: alvo, $R[i, j]$: sub-região
$Rd = (\frac{Abs[Det[u,v]]}{Norm[u]Norm[v]})^{\frac{1}{2}}$ cálculo do Raio de Hadamard
Imprima[vet];
Imprima[Rd];

quando os três ângulos eram distintos, a ocorrência de falhas variava, indicando uma dependência do algoritmo em ângulos simétricos ou próximos de 90°.

Foram realizados 578 testes nesta configuração, dos quais 505 indicaram que o algoritmo funcionou, e 73 indicaram falha. Isso representa uma taxa de sucesso de aproximadamente 87,37%, sugerindo que a simetria entre ângulos favorece o funcionamento correto do algoritmo. Outro aspecto investigado foi o raio de Hadamard da base, mas concluiu-se que este não é um indicador confiável da eficiência do algoritmo, já que em alguns casos o raio chegou a ultrapassar o valor de 0,9, e o algoritmo ainda assim falhou.

Configuração 2: Vetores de Base com Normas Diferentes

Na segunda configuração, os vetores de base possuíam normas desiguais: um vetor de norma unitária, outro com norma dobrada e um terceiro com norma quadruplicada. Nessa configuração, o algoritmo de Babai mostrou-se funcional apenas quando os ângulos entre os

vetores se aproximavam de 90°. Diferentemente do caso anterior, não foi observada uma correlação clara entre a falha do algoritmo e a relação entre os dois maiores ângulos.

Um total de 435 testes foram realizados nessa configuração, com apenas 13 resultando na funcionalidade do algoritmo (aproximadamente 2,99% de sucesso), enquanto 422 resultaram em falha. A análise adicional indicou que, com aumentos significativos de normas (como, por exemplo, um vetor quadruplicado e outro aumentado em 10 vezes), o algoritmo de Babai foi bem-sucedido apenas quando todos os ângulos entre os vetores eram exatamente 90°, evidenciando que tanto a variação de norma quanto a falta de ortogonalidade influenciam fortemente a eficácia do algoritmo na dimensão 3.

Descrição do Algoritmo no $\mathbb{R}^3$

O algoritmo percorre as seguintes etapas para verificar as configurações de base em que o algoritmo de Babai falha ou funciona em $\mathbb{R}^3$.

Entrada de Parâmetros: Definimos a quantidade de subdivisões q da região fundamental e os valores dos escalares m_1 e m_2. Esses escalares serão necessários para que os vetores fiquem de tamanhos diferentes, assim como o α no $\mathbb{R}^2$.

Sobre os Ângulos: Variamos os ângulos entre os vetores da base, iterando sobre β_1, β_2, e β_3 em incrementos de 10°:

$$\beta_1 = \frac{10\pi i}{180}, \quad \beta_2 = \frac{10\pi j}{180}, \quad \beta_3 = \frac{10\pi k}{180}$$

para $i, j, k \in \{1, 2, \ldots, 17\}$.

Definimos t_{11} para calcular os vetores da base: Para cada configuração de ângulos, calculamos t_{11} usando:

$$t_{11} = 1 - \frac{\cos\beta_3 - \cos\beta_1 \cos\beta_2}{(\text{sen}\beta_1 \text{sen}\beta_2)^2}$$

Se $t_{11} > 0$, prosseguimos para o próximo passo. Caso contrário, iremos ignorar esta configuração de ângulos. Calculamos $t_1 = \sqrt{t_{11}}$ e $t_2 = t_1 \text{sen}\beta_2$. Se $t_2 > 10^{-5}$, definimos os vetores da base em coordenadas esféricas:

$$\begin{aligned} u &= m_1(0, 0, 1) \\ v &= m_2(\text{sen}\beta_1, 0, \cos\beta_1) \\ w &= \left(\frac{\cos\beta_3 - \cos\beta_1 \cos\beta_2}{\text{sen}\beta_1}, t_2, \cos\beta_2\right) \end{aligned}$$

Construção do reticulado e região fundamental: Assim como no $\mathbb{R}^2$, iremos subdividir a região fundamental em q partes (onde q é um cubo perfeito) e pegar um vetor alvo a no centro de cada sub-caixa gerada, conforme a imagem abaixo.

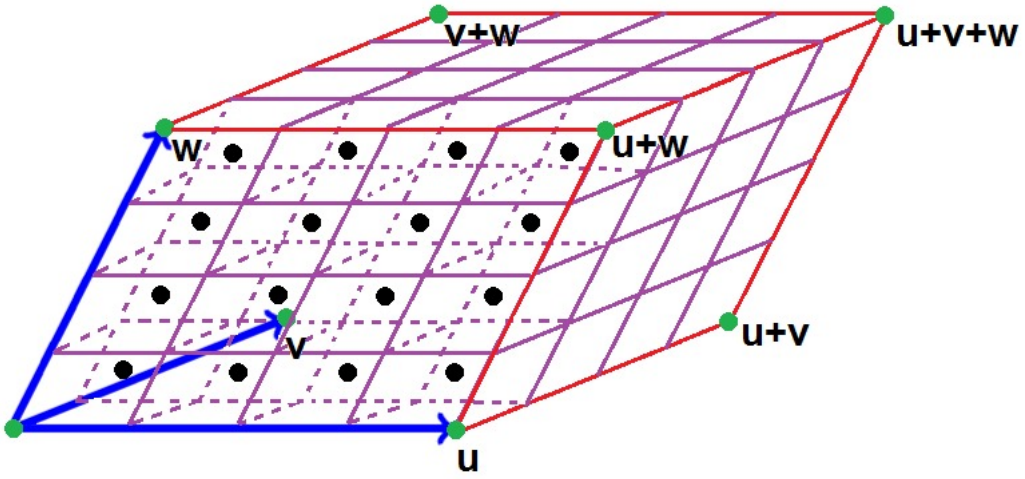

Figura 2.11: Região fundamental do reticulado subdividido em q sub-caixas

Para isso, escolhemos variar i_2, j_2, e k_2 de -6 a 6 para localizar vetores r_1 no reticulado, que estão mais próximos do alvo do que os vértices da caixa formada pela região fundamental. Determinamos:

$$r_1 = i_2 u + j_2 v + k_2 w$$

$$a = \frac{2i_1 - 1}{2s} u + \frac{2j_1 - 1}{2s} v + \frac{2k_1 - 1}{2s} w$$

para $i_1, i_2, i_3 \in \{1, 2, ..., s\}$, em que $s =$ raiz cúbica de q.

Verificação das Condições para o Algoritmo de Babai: Para cada vetor alvo a, verificamos se existe um vetor r_1 mais próximo a a do que os vértices da região fundamental. Isso implica verificar as desigualdades de distância, por exemplo:

$$\text{Norm}[a - r_1] < \text{Norm}[a], \quad \text{Norm}[a - r_1] < \text{Norm}[a - u], ..., \text{ e assim por diante, para } v \text{ e } w.$$

Se essas desigualdades forem satisfeitas para algum r_1 que não seja um dos vértices, então o algoritmo de Babai **falha** para esta configuração.

Em todos os casos, calculamos o Raio de Hadamard

$$Rd_1 = \sqrt[3]{\frac{|\det(u,v,w)|}{\|u\|\|v\|\|w\|}}$$

e indicamos os ângulos (em graus) entre os vetores da base a partir das seguintes equações

$$n_1 = \frac{\arccos\left(\frac{u\cdot v}{\|u\|\|v\|}\right)\cdot 180}{\pi}, \quad n_2 = \frac{\arccos\left(\frac{u\cdot w}{\|u\|\|w\|}\right)\cdot 180}{\pi}, \quad n_3 = \frac{\arccos\left(\frac{v\cdot w}{\|v\|\|w\|}\right)\cdot 180}{\pi}$$

Exibição dos Resultados: Ao final da execução, o algoritmo exibe todas as configurações de ângulos e raio de Hadamard calculados, indicando se o algoritmo de Babai funciona ou não para cada caso.

Algoritmo 4: Falha do Babai no R3

Entrada: $q = 16$; q: cubo perfeito

$m_1 = 1$ escalar que mudará o tamanho do vetor u

$m_2 = 1$; escalar que mudará o tamanho do vetor v

Saída: Conjunto $\{(n_1, n_2, n_3)$, Raio Hadamard, Babai OK / NÃO$\}$

$i = 1; j - i; k = j$

enquanto $i \leq 17$

enquanto $j \leq 17$

enquanto $k \leq 17$

$\beta_1 = \frac{10\pi i}{180}$;

$\beta_2 = \frac{10\pi j}{180}$;

$\beta_3 = \frac{10\pi k}{180}$;

$\text{cont}_1 = 1$;

$t_{11} = 1 - \frac{Cos\beta_3 - Cos\beta_1 Cos\beta_2}{Sen\beta_1 {Sen\beta_2}^2}$;

Se $t_{11} > 0$, **faça**

$t_1 = \sqrt{t_{11}}$;

$t_2 = t_1 Sen\beta_2$

Se $t_2 > 10^{-5}$, **faça** vetores da base

$u = m_1(0, 0, 1)$;

$v = m_2(Sen\beta_1, 0, Cos\beta_1)$

$w = (\frac{Cos\beta_3 - Cos\beta_1 Cos\beta_2}{Sen\beta_1}, t_2, Cos\beta_2)$

Var = 6; r={ };

$i_2, j_2, k_2 = -\text{Var}$;

enquanto $i_2 \leq \text{Var}$ **enquanto** $j_2 \leq \text{Var}$ **enquanto** $k_2 \leq \text{Var}$ $r_1 = i_2u + j_2v + k_2w$;

$r \cup r_1 \to r$;

$s = Sqrt[3][q]$;

$a = \{\}$;

$i_1 = 1; j_1 = 1; k_1 = 1$;

enquanto $i_1 \leq s$

enquanto $j_1 \leq s$

enquanto $k_1 \leq s$

$a_1 = \frac{2i_1-1}{2s}u_1 + \frac{2j_1-1}{2s}v_1 + \frac{2k_1-1}{2s}w_1$

$a \cup a_1 \to a$;

$cont_1 = 1$, então

$y_1 = \text{Card}(a); y_2 = \text{Card}(r)$

$x_1 = 1; x_2 = 1$

enquanto $x_1 \leq y_1$

enquanto $x_2 \leq y_2$

$eq_1 = ||a[x_1]] - r[[x_2]]|| - ||a[[x_1]]||$

...

$eq_8 = ||a[[x_1]] - r[[x_2]] - ||a[[x_1]] - u_1 - v_1 - w_1||$

Se $eq_1, eq_2, \ \ldots\ , eq_8 < 0$ e $r[[x_2]] \neq u, v, w, u+v, u+w, v+w, u+v+w, -u, -v, -w, -u-w, -v-w, -u-v-w$ e $cont1 = 1$ então

Calcule $Rd = \frac{|Det[u,v,w]|}{||u||||v||||w||}^{1/3}$

Calcule $n_1 = \frac{\text{ArcCos}\left[\frac{\text{u.v}}{||\text{u1}||||\text{v}||}\right]180}{\pi}$

$n_2 = \frac{\text{ArcCos}\left[\frac{\text{u.w}}{||\text{u}||||\text{w}||}\right]180}{\pi}$

$n_3 = \frac{\text{ArcCos}\left[\frac{\text{v.w}}{||\text{v}||||\text{w}||}\right]180}{\pi}$

vet=$[(\beta_1, \beta_2, \beta_3), (n_1, n_2, n_3), Rd, \text{ NÃO}]$

Imprima[vet]

cont1= 0; Vá para [END];

Rótulo [END]

Se cont1= 1 então

$vet_2 = [(\beta_1, \beta_2, \beta_3), (n_1, n_2, n_3), Rd, \text{ Babai OK}]$

Imprima[vet2]

Capítulo

3

Criptografia

Criptografia é uma palavra de origem grega, proveniente de Kryptós, que significa oculto, e de Graphé, que significa escrita. Desse modo, criptografia é uma forma de escrita oculta ou secreta, e tem por objetivo esconder o significado de uma mensagem. A criptografia é a arte dos “códigos secretos” e estuda os métodos para codificar uma mensagem de modo que só seu destinatário legítimo consiga interpretá-la.

Nesta seção apresentamos alguns marcos históricos à respeito da criptografia, visando estimular o interesse do leitor.

3.1 Histórico

Em “O Livro dos Códigos”, Simon Singh (SINGH, 2004) escreveu: “A história dos códigos e de suas chaves é a história de uma batalha secular entre os criadores de código e os decifradores, uma corrida armamentista intelectual que teve um forte impacto na história humana”.

A interessante história "secular", até onde se sabe, iniciou-se em 1900 a.C. Naquela época, os escribas utilizavam hieróglifos para substituir palavras de documentos importantes do Império Egípcio, a fim de evitar que alguém não confiável soubesse do que se tratava tais documentos.

Posteriormente, de acordo com Singh, a prática de ocultar o significado de uma mensagem era utilizada pelo exército espartano no século V a.C. Foi nessa época que a Grécia, diante da constante ameaça de ser conquistada pela Pérsia, percebeu que era essencial haver uma comunicação segura. O resultado dessa percepção foi a criptografia propriamente dita, que desenvolveu simultaneamente dois ramos distintos: a transposição e a substituição.

Na transposição, as letras de uma palavra ou frase são reorganizadas, formando um anagrama. Um exemplo de transposição é o chamado citale espartano, mostrado na Figura 3.1, composto por um bastão de madeira e uma tira de couro ou papiro. A técnica utilizada era a de enrolar a tira em forma de espiral ao redor do bastão com um diâmetro pré-determinado e a mensagem era escrita de forma longitudinal. Feito isso, a tira era desenrolada e enviada pelo mensageiro, que a transportava como se fosse um cinto.

Para ler a mensagem, era preciso que o receptor tivesse um bastão de mesmo diâmetro para enrolar novamente a tira e, dessa forma, compreender sua mensagem. Pode-se associar um algoritmo a esse método de criptografar a mensagem, sendo este o ato de enrolar a tira; pode-se também associar a chave para decifrar a mensagem como sendo a largura do bastão.

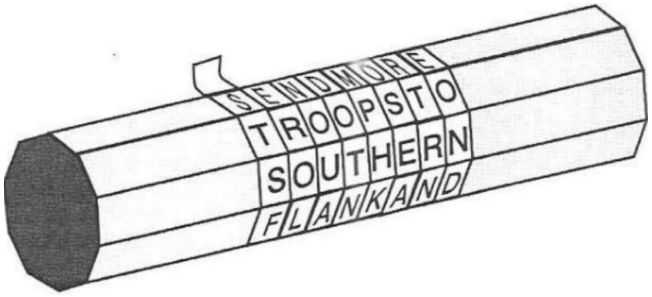

Figura 3.1: Citale Espartano

Já na substituição, tem-se um sistema em que uma letra é representada por outra. Por exemplo, a letra A é substituída pela letra V (A:=V), a letra B, substituída pela letra X (B:=X) e assim por diante, até que cada letra do alfabeto tenha uma outra que a substitua, formando um alfabeto cifrado.

Esse método que transforma o alfabeto convencional em outro é denominado como cifra monoalfabética. Júlio César, general romano, foi um dos que utilizou o método de substituição monoalfabética para codificar informações de seu império, ele utilizava tanto a cifra de substituição, que seu método ficou conhecido como Cifra de César. A cifra consiste em deslocar o alfabeto três casas para frente, como mostra a Figura 3.1.

Alfabeto Original	a	b	c	d	e	...	v	w	x	y	z
Alfabeto Cifrado	D	E	F	G	H	...	Y	Z	A	B	C

Figura 3.2: Método da Cifra de César

Apesar de ter sido utilizada por muito tempo, a cifra por substituição monoalfabética era de fácil decifração. O primeiro relato de quebra dessas cifras se deu no Oriente, de acordo com Singh, estudiosos árabes decifravam mensagens através da análise de frequência de cada letra, no texto cifrado. Após ser utilizado pelos árabes, tal método da Criptoanálise chegou na Europa, colocando a segurança das comunicações em risco.

Dessa forma, as cifras de substituição monoalfabéticas se tornaram obsoletas, surgindo a necessidade de criar novas cifras, mais difíceis de serem quebradas, a fim de proteger o sigilo das comunicações. A solução então, fora criar chaves enormes e sem padrões.

Utilizar uma chave enorme e sem um padrão que pudesse ser reconhecido, foi o que os alemães conseguiram fazer durante a Segunda Guerra Mundial, com a Enigma. A Enigma é uma máquina criptográfica criada por Arthur Scherbius, em 1918, essa invenção, de acordo com Singh (2004, p. 164) "se tornaria o mais terrível sistema de cifragem da história".

A princípio, ela era formada por três elementos: um teclado para a entrada das letras da mensagem original; um misturador, que cifrava as letras; e um mostrador, formado por lâmpadas (uma para cada letra), que servia para identificar as letras cifradas. A fim de deixar sua invenção cada vez mais complexa, Scherbius acrescentou mais características à sua máquina.

Primeiramente, inseriu mais dois misturadores e um refletor na máquina, para aumentar seu potencial; depois, possibilitou que os misturadores fossem removidos para trocar de posição; e, por fim, acrescentou um painel de tomadas que ficava entre o teclado e o primeiro misturador. A Figura 3.3 mostra todo o esquema da máquina, depois das alterações realizadas por seu criador.

Figura 3.3: Máquina Enigma

A Enigma passou a ser muito utilizada pelos militares, e, ao todo, os alemães compraram 30 mil peças da máquina. Segundo Singh (2004, p. 161) "a invenção de Scherbius deu aos alemães o sistema mais seguro de criptografia do mundo", funcionando da seguinte forma: Uma letra do texto é pressionada no teclado, uma corrente elétrica passa pelos diversos componentes de cifragem da máquina, acendendo uma luz no painel de lâmpadas, a letra acendida é a codificação da letra digitada. E cada vez que uma letra é pressionada, as peças móveis da máquina mudam de posição e, se numa próxima vez que a mesma letra for teclada, provavelmente será cifrada como algo diferente.

De acordo com Singh, pesar de parecer ser a peça chave para a vitória nazista durante a guerra, a máquina acabou sendo um dos principais motivos da queda alemã. O serviço secreto francês obteve uma réplica da máquina Enigma, graças a traição do alemão Hans-Thilo. A partir disso, houve uma imensa movimentação entre os aliados, com o objetivo de tentar quebrar os códigos da Enigma e, assim, obter informações fundamentais capazes de levar à vitória da guerra.

Os britânicos também controlavam de perto as comunicações alemãs e começaram a interceptar algumas cifras estranhas, que eram provenientes da Enigma, acabando por confundir os criptoanalistas aliados. Porém, ironicamente, foi um método que os alemães criaram para aumentar a segurança que acabou por expor a fraqueza da Enigma. Esse método fazia com que as comunicações alemãs dependessem de duas chaves para o envio de mensagens, dessa forma, toda correspondência usaria uma chave diária, mas cada mensagem começaria com uma nova chave exclusivamente para descriptografar essa mensagem. Para evitar erros, o remetente repetia a chave da mensagem duas vezes - uma frase simples de três letras que dava instruções sobre como definir os discos codificadores.

Diante disso, o criptoanalista e matemático polonês Marian Rejewski aproveitou essa repetição, estudando as chaves de três letras de cada mensagem interceptada. Em um ano, ele reuniu um catálogo de todas as configurações possíveis do misturador que a Enigma poderia gerar, ou seja, 105456 configurações no total. Assim, as chaves de mensagem tornaram-se impressões digitais que revelaram a chave do dia e as configurações da Enigma.

No entanto, se não fosse por Alan Turing e a equipe de criptoanálise em Bletchley Park, a guerra poderia ter durado ainda mais. Como os Aliados sabiam que os alemães poderiam reconhecer o método de repetir uma chave de mensagem e Alan Turing foi designado para encontrar outra maneira de quebrar a cifra da Enigma. Turing, como Rejewski, começou a trabalhar em mensagens antigas, identificando padrões.

Em 1943, ele e sua equipe projetaram o *Colossus*, primeiro computador operacional, utilizado durante a Segunda Guerra Mundial para decifrar os códigos criados pela Enigma. O trabalho de Turing e sua equipe deu aos Aliados um conhecimento prévio dos ataques de bombardeio e até mesmo detalhes sobre as forças alemãs que os Aliados enfrentariam na Normandia. A quebra da Enigma, graças à criação do *Colossus*, foi essencial para se ter uma guerra mais curta e com menos vítimas.

Tal criação foi o que deu início a uma era moderna da criptografia, já que ele era programado a partir de uma codificação bem mais complexa que a da Enigma. O Colossus era de uso exclusivo do governo e de militares e, após o fim da Segunda Guerra Mundial, ele foi destruído e seu protótipo foi queimado. Isso ocorreu porque o governo tinha o intuito de utilizar de comunicação sigilosa e não queria deixar uma tecnologia tão poderosa existindo e assim, todas as informações para o desenvolvimento do primeiro computador moderno foram perdidas e restou a outros cientistas, alguns anos depois, recriarem o computador.

3.2 Criptografia de chave simétrica e assimétrica

Com o surgimento dos computadores programáveis, os criptoanalistas conseguiram desenvolver e quebrar os mais variados tipos de cifras, pois utilizavam da velocidade desses computadores para pesquisar todas as chaves possíveis até que encontrassem a certa. Em contrapartida, os criptógrafos também exploravam esses computadores para a criação de cifras mais eficientes, dessa forma, os métodos criptográficos até aqui citados, se tornaram obsoletos.

A criptografia que foi apresentada até o momento, é identificada como **criptografia simétrica**, ou criptografia de chave simétrica, o que significa que o mesmo método utilizado para cifrar as mensagens, também é usado para decifrar, como mostra a Figura 3.4. A partir da década de 70, as empresas estavam dotadas de computadores e a cifragem entre elas se alastrou, com isso, surgiu a necessidade de padronizar um tipo de cifragem para que as ações de negociações e transferências entre elas, pudessem ser totalmente seguras e eficientes. É neste momento que surge o **DES (Data Encryption Standard)**, um algoritmo de criptografia simétrica. O maior problema dos métodos de criptografia simétrica é a distribuição da chave secreta, que precisa ser transmitida através de um canal de comunicação inseguro.

Figura 3.4: Algoritmo de criptossistema com chave simétrica

É a partir desse problema que surge a **criptografia assimétrica**. Na criptografia assimétrica, cada parte da comunicação possui duas chaves, uma pública e a outra privada. Uma chave é utilizada para encriptar uma mensagem enquanto a outra para decriptar e essas duas chaves são relacionadas matematicamente. A chave pública é utilizada para encriptar a mensagem, ou seja, essa chave é divulgada para o remetente; já a chave para decriptar a mensagem é privada, isto é, ela é um segredo pertencente ao destinatário (Figura 3.5). Dessa forma, não existe mais o problema que era manter o segredo da chave do método de criptografia simétrica.

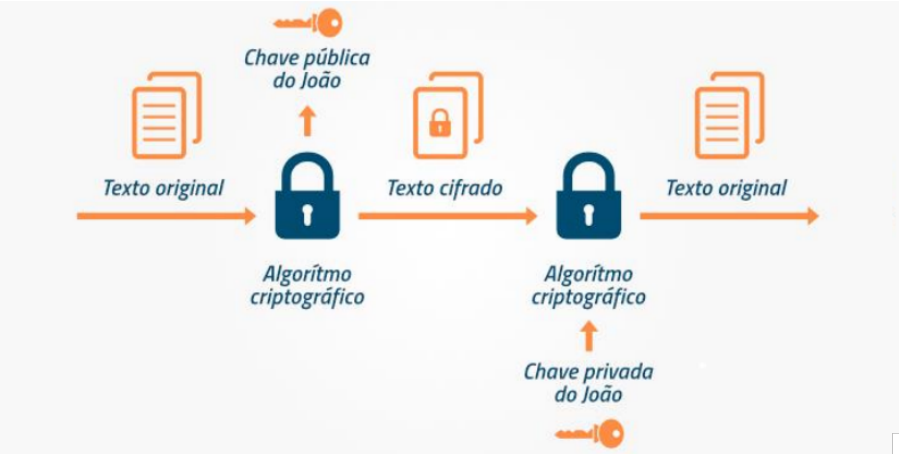

Figura 3.5: Algoritmo de criptossistema com chaves assimétricas

3.3 Criptossistemas de chaves públicas

Na criptografia assimétrica é onde temos os chamados “Criptossistemas de chaves públicas”. A ideia é que existisse uma chave pública em que todos pudessem ter acesso, mas que ao mesmo tempo oferecesse a possibilidade de privacidade para a outra chave, que seria usada no processo de descriptografar.

3.3.1 Criptossistema RSA

Um dos principais criptossistemas de chave pública conhecido é o RSA, criado pelos cientistas Ron Rivest, Adi Shamir e Leonard Adleman, do MIT (Massachusetts Institute of Technology).O RSA é um sistema cuja utilização exige o uso de computadores, fatoração de números que são resultado da multiplicação de dois números primos de grande valor e no uso de funções modulares. O algoritmo, apresentado a seguir, envolve a geração de duas chaves, uma pública e outra privada. A chave pública é usada para criptografar dados, enquanto a chave privada é usada para descriptografá-los.

Inicialmente devem ser escolhidos dois números primos de grande valor p e q; quanto maior o número escolhido, mais seguro será o algoritmo. O produto $N = pq$ faz parte da chave pública de codificação, enquanto os primos p e q fazem parte da chave privada. Logo, a segurança do sistema está na dificuldade em fatorar N; dependendo do tamanho da chave, a procura da fatoração que gera a chave utilizada no sistema RSA, quando feita por computadores de última geração, leva anos ou décadas.

Por ser um sistema muito seguro, o RSA é o algoritmo usado para segurança de informações, como por exemplo, na confidencialidade de dados, usado para criptografar informações sensíveis, como comunicações online, senhas e dados de cartões de crédito, para proteger a confidencialidade dos dados contra acesso não autorizado. Também é utilizado em sistemas de autenticação de usuários e em protocolos de autenticação de servidores, ajudando a garantir que os usuários ou servidores sejam quem afirmam ser.

Outro exemplo é na criação de assinaturas digitais, que são usadas para verificar a autenticidade e a integridade de documentos eletrônicos, além de ser usado para proteger dados armazenados, como arquivos criptografados em discos rígidos e backups. As chaves usadas em bancos, operadas pelo RSA são compostas por números da ordem de 10308 algarismos. Quando usada com essa quantidade de algarismos a chave é tão segura, que mesmo juntando cem milhões de computadores a chave só poderia ser quebrada depois de mil anos.

Algoritmo 5: Algoritmo RSA

Entrada: Dois números primos p e q
Saída: Chave pública (N, e) e chave privada (N, d)
$N \leftarrow pq$;
$\phi(N) \leftarrow (p-1)(q-1)$;
$e \leftarrow$ escolha de e relativamente primo a $\phi(N)$;
$d \leftarrow$ calcule d tal que $de \equiv 1 \pmod{\phi(N)}$;
Chave pública: (N, e) ;
Chave privada: (N, d) ;

3.3.2 Criptossistema da mochila

Nesta seção descrevemos um modelo de sistema criptográfico de chave pública diferente do RSA. Esta versão é apresentada em (SILVERMAN; PIPHER; HOFFSTEIN, 2014), referência que embasa nosso trabalho, como um exemplo de introdução e instrutivo para o conhecimento de criptossistemas de chave públicas. O chamado criptossistema da mochila, também conhecido como criptossistema de Knapsack, foi proposto por Merkle e Hellman em 1978 e utiliza de problemas de soma de subconjunto e de sequências supercrescentes, então, para entendermos melhor seu funcionamento, algumas definições serão apresentadas.

O Problema da Soma do Subconjunto: Suponha que você tenha uma lista de números inteiros positivos $(M_1, M_2, ..., M_n)$ e outro número inteiro S. Encontre um subconjunto dos elementos da lista cuja soma seja igual a S. (Você pode assumir que existe pelo menos um subconjunto que satisfaz essa condição).

Proposição 3.3.1. *Seja $M = (M_1, M_2, ..., M_n)$ e seja (M, S) um problema de soma de subconjuntos. Para todos os conjuntos $\boldsymbol{I}$ e $\boldsymbol{J}$ satisfazendo*

$$\boldsymbol{I} \subset \left\{ i : 1 \leq i \leq \frac{1}{2}n \right\} \quad e \quad \boldsymbol{J} \subset \left\{ j : \frac{1}{2}n < j \leq n \right\}$$

calcule e faça uma lista de valores

$$A_{\boldsymbol{I}} = \sum_{i \in \boldsymbol{I}} M_i \quad e \quad B_{\boldsymbol{J}} = S - \sum_{j \in \boldsymbol{J}} M_j.$$

Então essas listas incluem um par de conjuntos $\boldsymbol{I}_0$ e $\boldsymbol{J}_0$ satisfazendo $A_{\boldsymbol{I}_0} = B_{\boldsymbol{J}_0}$, e os conjuntos $\boldsymbol{I}_0$ e $\boldsymbol{J}_0$ fornecem uma solução para o problema da soma do subconjunto

$$S = \sum_{i \in \boldsymbol{I}_0} M_i + \sum_{j \in \boldsymbol{J}_0} M_j.$$

Definição 3.3.2. *Uma sequência supercrescente de inteiros é uma lista de inteiros positivos $\boldsymbol{r} = (r_1, r_2, \ldots, r_n)$ com a propriedade que*

$$r_{i+1} \geq 2r_i \quad \text{para todo } 1 \leq i \leq n-1.$$

Lema 3.3.1. *Seja $\boldsymbol{r} = (r_1, r_2, \ldots, r_n)$ uma sequência supercrescente. Então*

$$r_k > r_{k-1} + \cdots + r_2 + r_1 \quad \text{para todo } 2 \leq k \leq n.$$

Essas considerações são importantes, pois a utilizamos no criptossistema da mochila, já que, um problema de soma de subconjuntos no qual os inteiros em M formam uma sequência supercrescente é muito simples de resolver. Abaixo, é apresentado um exemplo a fim de entendermos como são esses conceitos na prática:

Exemplo 3.3.3. *A sequência* $M = (3, 11, 24, 50, 115)$ *é supercrescente. Escrevemos* $S = 142$ *como uma soma de elementos em* M*: Primeiro* $S \geq 115$*, o último elemento da sequência, então* $x_5 = 1$ *e sustituímos* S *por* $S - 115 = 27$*. Como* $27 < 50$*, então* $x_4 = 0$*. Continuando,* $27 \geq 24$*, então* $x_3 = 1$ *e* S *se torna* $27 - 24 = 3$*. Como* $3 < 11$*, então* $x_2 = 0$*, e finalmente* $3 \geq 3$*, então* $x_1 = 1$*. Observe que* S *é reduzido a* $3 - 3 = 0$*, o que significa que* $x = (1, 0, 1, 0, 1)$ *é a solução. Para checarmos vemos se quando substituímos os valores, chegamos ao valor inicial de S.*

$$1 \cdot 3 + 0 \cdot 11 + 1 \cdot 24 + 0 \cdot 50 + 1 \cdot 115 = 142$$

Merkle e Hellman propuseram um sistema criptográfico de chave pública baseado em um problema de soma de subconjuntos super crescente que é disfarçado usando congruências. Utilizaremos dos nomes conhecidos como Alice e Bob, que trocam mensagens, e Eve, que tentará interceptá-las. A tabela abaixo explica como funciona o criptossistema.

Alice	Bob
Criação da chave	
Escolha uma sequência supercrescente $r = (r_1, \ldots, r_n)$ Escolha A e B com $B > 2r_n$ e $\text{mdc}(A, B) = 1$ Calcule $M_i \equiv Ar_i \pmod{B}$ para $1 \leq i \leq n$. Publique a chave pública $\boldsymbol{M} = (M_1, \ldots, M_n)$.	
Criptografia	
	Escolha uma mensagem binária $\boldsymbol{x}$. Use a chave pública de Alice $\boldsymbol{M}$ para computar $\boldsymbol{S} = \boldsymbol{x} \cdot \boldsymbol{M}$ Envie a mensagem cifrada $\boldsymbol{S}$ para Alice.
Descriptografia	
Calcule $S' \equiv A^{-1}S \pmod{B}$. Resolva o problema da soma do subconjunto S' usando a sequência supercrescente r. A mensagem $\boldsymbol{x}$ satisfaz $\boldsymbol{x} \cdot \boldsymbol{r} \equiv S'$.	

Tabela 3.1: O criptossistema da mochila de Merkle–Hellman

Vemos que a ideia geral é começar com uma sequência secreta supercrescente, disfarçá-la usando operações lineares modulares secretas e publicar a sequência disfarçada como a chave

pública. Uma questão importante que deve ser considerada em relação aos sistemas de mochila é o tamanho dos diversos parâmetros necessários para obter um nível de segurança desejado. A chave deve ser muito grande para garantir o mínimo de segurança e, mesmo assim, existem maneiras de quebrá-lo.

De acordo com (SILVERMAN; PIPHER; HOFFSTEIN, 2014), após a criação do algoritmo de redução de reticulados LLL em 1985, já apresentado neste trabalho, ficou claro que o criptossistema da mochila tem uma fraqueza fundamental. Agora, veremos como Eve é capaz de invadir este criptossistema e também de que maneira conseguimos o relacioná-lo com a teoria de reticulados.

Para interceptar a mensagem, Eve reformula o problema da soma do subconjunto usando vetores. Suponha que ela queira escrever S como uma soma de subconjuntos do conjunto $M = (M_1, ..., M_n)$, seu primeiro passo é formar a matriz

$$\begin{pmatrix} 2 & 0 & 0 & \cdots & 0 & m_1 \\ 0 & 2 & 0 & \cdots & 0 & m_2 \\ 0 & 0 & 2 & \cdots & 0 & m_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 2 & m_n \\ 1 & 1 & 1 & \cdots & 1 & S \end{pmatrix}$$

Em vetores, teremos:

$$\begin{aligned} \boldsymbol{v}_1 &= (2, 0, 0, \ldots, 0, m_1), \\ \boldsymbol{v}_2 &= (0, 2, 0, \ldots, 0, m_2), \\ &\vdots \qquad\qquad \vdots \\ \boldsymbol{v}_n &= (0, 0, 0, \ldots, 2, m_n), \\ \boldsymbol{v}_{n+1} &= (1, 1, 1, \ldots, 1, S). \end{aligned}$$

Eve então olhará para todas as combinações lineares de $v_1, ..., v_{n+1}$,

$$L = \{a_1\boldsymbol{v}_1 + a_2\boldsymbol{v}_2 + \cdots + a_n\boldsymbol{v}_n + a_{n+1}\boldsymbol{v}_{n+1} : a_1, a_2, \ldots, a_{n+1} \in \mathbb{Z}\}$$

Como já definimos, vemos que L é um reticulado em $\mathbb{R}^{n+1}$.

Suponha agora que $x = (x_1, ..., x_n)$ é a solução para o problema da soma do subconjunto dado. Então, o reticulado L contém o vetor:

$$\boldsymbol{t} = \sum_{i=1}^{n} x_i\boldsymbol{v}_i - \boldsymbol{v}_{n+1} = (2x_1 - 1, 2x_2 - 1, \ldots, 2x_n - 1, 0) \tag{3.3.2.1}$$

onde a última coordenada de $\boldsymbol{t}$ é 0 porque $S = x_1m_1 + \cdots + x_nm_n$. Chegamos agora ao cerne da questão. Como os x_i são todos 0 ou 1, todos os valores de $2x_i - 1$ são ± 1, então o vetor $\boldsymbol{t}$ é bem curto, dessa forma, Eve pode usar o algoritmo LLL para encontrar vetores curtos diferentes de zero, logo ela será capaz de encontrar $\boldsymbol{t}$ e, portanto, recuperar a mensagem $\boldsymbol{x}$ sem saber a chave privada, fazendo com que a segurança deste criptossistema fique comprometida.

Exemplo 3.3.4. *Seja* $r = (2, 5, 13, 29, 60, 122, 257, 500)$ *a sequência supercrescente secreta de Alice, e suponha que ela escolha* $A = 491$ *e* $B = 1021$*; A sua sequência disfarçada é*

$$M \equiv (2 \cdot 491, 5 \cdot 491, 13 \cdot 491, 29 \cdot 491, 60 \cdot 491, 122 \cdot 491, 257 \cdot 491, 500 \cdot 491) \text{ (mod 1021)}$$

$$M = (982, 413, 257, 966, 872, 684, 604, 460).$$

Observe que M *não está nem perto de ser supercrescente. Bob decide enviar a Alice a mensagem secreta* $x = (1, 0, 1, 1, 0, 1, 0, 0)$*. Ele criptografa* x *computando*

$$S = x \cdot M = 1 \cdot 982 + 0 \cdot 413 + 1 \cdot 257 + 1 \cdot 966 + 0 \cdot 872 + 1 \cdot 684 + 0 \cdot 604 + 0 \cdot 460 = 2899$$

Ao receber S, Alice multiplica por 440, o inverso de 491 módulo 1021

$$S' \equiv 440 \cdot 2899 = 99 \text{ (mod 1021)}$$

Então Alice usa o algoritmo como foi exemplificado acima para resolver $S' = x \cdot r$*, como ela conhece* r *consegue encontrar a mensagem binária* x*.*

Utilizando o LLL, Eve conseguiria interceptar a mensagem, uma vez que este fornece o vetor de norma mínima $(-1, 1, -1, -1, 1, -1, 1, 1, 0)$, quando a norma é $\sqrt{8}$ como no caso do exemplo. Substituindo os valores encontrados na Equação 3.3.2.1, Eve encontra o vetor de mensagem x.

3.4 Perspectivas na Era Pós-Quântica

A história por trás do desenvolvimento da criptografia se relaciona com toda a história de desenvolvimento da civilização humana, já que, desde os primeiros escritos, ela corrobora com a humanidade, sendo uma ferramenta muito útil para comunicações simples ou até mesmo para troca de informações de guerra e informações bancárias e de segurança. Diante disso, não é possível estudar sistemas criptográficos sem o interesse de realizar um resgate histórico; conhecer a história da criptografia acaba sendo um pré-requisito para compreender os criptossistemas e os desdobramentos que ela apresenta.

Atualmente, a criptografia é amplamente utilizada na internet e na segurança, para oferecer aos usuários a proteção de suas transações bancárias e o sigilo de suas informações e

comunicações. Essa necessidade de manter uma informação sigilosa, em oposição a ânsia de descobri-las, foi fundamental para o estudo mais profundo de algumas áreas da Matemática, auxiliando assim seu desenvolvimento, bem como o desenvolvimento de tecnologias, como no caso dos computadores.

Um fato importante e fundamental para o surgimento deste trabalho é que a criptografia utilizada atualmente só é considerada segura porque, até o momento, não existem tecnologias de computadores quânticos amplamente disponíveis. Com o possível advento dessas tecnologias, toda a criptografia baseada em métodos tradicionais poderá se tornar obsoleta. Bernstein, Buchmann e Dahmen, em 2009, introduzem o conceito de criptografia pós-quântica, destacando sua importância para mitigar o impacto da computação quântica em sistemas tradicionais (BERNSTEIN; BUCHMANN; DAHMEN, 2009).

Esse cenário impulsionou diversas iniciativas para o desenvolvimento de novos sistemas criptográficos resistentes a ataques quânticos, como a competição organizada pelo NIST (National Institute of Standards and Technology). A competição tem por objetivo selecionar algoritmos de criptografia pós-quântica que possam garantir a segurança dos dados mesmo na presença de computadores quânticos, e os criptossistemas baseados na teoria de reticulados, detalhados nos capítulos seguintes, são vistos como promissores, devido ao seu potencial para suportar esse tipo de ameaça.

3.4.1 Competição NIST

Em 2016, o NIST lançou um concurso público para a seleção dos melhores algoritmos de criptografia pós-quântica (PQC). Este concurso visava encontrar algoritmos que fossem seguros contra os ataques de computadores quânticos, uma nova ameaça potencial para a criptografia tradicional. O concurso atraiu uma participação global significativa, com 82 inscrições provenientes de 25 países diferentes.

O processo de seleção para os algoritmos PQC foi extenso e rigoroso, dividido em quatro rodadas de avaliação. Cada rodada teve como objetivo reduzir o número de algoritmos candidatos, avaliando sua segurança, desempenho e viabilidade para padronização. Após o encerramento da quarta rodada em 2022, o NIST selecionou quatro algoritmos finalistas para avançar à fase de padronização.

Os quatro algoritmos escolhidos pelo NIST são: **CRYSTALS-Kyber**, **CRYSTALS-Dilithium**, **Sphincs+** e **FALCON**. No entanto, para fins de padronização, esses algoritmos foram designados com novos nomes, agora são conhecidos como Federal Information Processing

Standards (FIPS) 203, 204, 205 e 206. O FIPS 203, 204 e 205 foram oficialmente anunciados, enquanto o FIPS 206, anteriormente conhecido como FALCON, deve ser padronizado até o final de 2024.

Os algoritmos selecionados pelo NIST se dividem em duas categorias principais, que são de **criptografia geral**, usada para proteger informações transmitidas por redes públicas, e de **assinatura digital**: utilizada para autenticar indivíduos e prevenir ataques de malware. Os algoritmos de criptografia geral visam garantir a confidencialidade das informações, enquanto os algoritmos de assinatura digital são críticos para a integridade e autenticidade dos dados.

Cada protocolo de criptografia é baseado em problemas matemáticos complexos que são fáceis de verificar, mas difíceis de resolver sem a chave correta. No caso dos algoritmos selecionados, o **FIPS 203** e **FIPS 204** utilizam a criptografia de reticulado, baseada em problemas difíceis deste tópico. O problema matemático central é encontrar o menor múltiplo comum entre um conjunto de números, geralmente representado em múltiplas dimensões ou em um reticulado. Enquanto o **FIPS 205** é baseado em funções hash, convertendo mensagens em sequências criptografadas que são difíceis de reverter.

A comunidade de criptografia demonstrou grande interesse e preocupação com a segurança dos novos algoritmos. Em abril de 2024, foi publicado o artigo *"Quantum Algorithms for Lattice Problems"* de Yilei Chen (CHEN, 2024), da Universidade Tsinghua, que sugeriu possíveis vulnerabilidades na criptografia baseada em reticulados. A descoberta rápida da falha no argumento evidenciou uma comunidade ativa e vigilante de especialistas em criptografia, aumentando a confiança na robustez dos algoritmos selecionados (ROUSSEAU, 2024).

Richard Marty, do departamento de Serviços Financeiros da *LGT Private Bank*, mencionou que o processo de transição para criptografia pós-quântica levou 18 meses e exigiu um investimento de aproximadamente meio milhão de dólares. Ele destacou a complexidade dessa mudança, que envolve uma atualização significativa dos sistemas de segurança para proteger dados contra ameaças de computadores quânticos, e enfatizou a necessidade de agir rapidamente, já que a tecnologia quântica pode surgir a qualquer momento (SPECTRUM, 2024).

Capítulo

4

Criptossistemas baseados em problemas difíceis em reticulados

A criptografia desempenha um papel fundamental na segurança da informação na era da informação. Desde os primórdios da comunicação, a humanidade tem procurado maneiras de proteger suas mensagens e dados sensíveis contra olhares "maldosos" e perigosos. Um avanço notável nesse campo foi a introdução de criptossistemas de chave pública, que revolucionaram a maneira como compartilhamos informações provisórias e garantimos a segurança dos dados.

Durante meados da década de 1990, foram introduzidos vários criptossistemas baseados em reticulados, os mais importantes deles, em ordem alfabética, foram os Criptossistema Ajtai-Dwork (AJTAI, 1996), o criptossistema GGH de Goldreich, Goldwasser e Halevi, e o criptossistema NTRU proposto por Hoffstein Pipher e Silverman.

A motivação para a introdução desses criptossistemas foi dupla. Primeiro, por que é interessante ter criptossistemas que se baseia em problemas dificeis de se resolver matematicamente e segundo, os criptossistemas baseados em reticulados são frequentemente muito mais rápidos do que a fatoração ou sistemas baseados em logaritmos discretos, como Elgamal, RSA e ECC. Informalmente, para alcançar k bits de segurança, a criptação e decriptação dos sistemas de Elgamal, RSA e ECC requerem operações $\mathcal{O}(k^3)$, enquanto para sistemas baseados em reticulados requerem apenas operações $\mathcal{O}(k^2)$. Além disso, operações simples de álgebra linear usadas em sistemas baseados em reticulados são muito fáceis de implementar em hardware e software.

No entanto, a análise segurança de criptossistemas baseados em reticulados não é tão bem compreendida quanto para sistemas baseados em fatoração e logaritmo discreto e, portanto, embora os sistemas baseados em reticulados sejam objeto de muitas pesquisas atuais, suas implementações no mundo real são poucas em comparação com sistemas mais antigos.

Neste capítulo, será abordado o estudo do tópico "criptossistemas de chave pública baseados em problemas difíceis em reticulados". Estes sistemas são importantes, não apenas pela segurança que oferecem, mas também pelos conceitos matemáticos que os fundamentam.

4.1 O Criptossistema de Chave Pública GGH

O sistema GGH (Gentry, Halevi e Gertner) é um criptossistema de chave pública baseado em reticulados. O problema difícil por trás dele é o problema do vetor mais próximo (CVP).

Para explicar esse sistema adicionaremos sujeitos, sendo eles: Alice, Bob e Eve. A chave privada de Alice é uma base boa β_{boa} para um reticulado Λ e sua chave pública é uma base ruim β_{ruim} para o mesmo reticulado. A mensagem de Bob é um vetor binário m, que ele utiliza para formar uma combinação linear $\Sigma m_i v_i$ dos vetores $v_i \in \beta_{\text{ruim}}$. Bob então perturba essa soma adicionando à ela um pequeno vetor r aleatório. O resultado é um vetor w que difere de um vetor v do reticulado por um vetor r.

Como Alice conhece uma base boa para Λ, ela pode utilizar o algoritmo de Babai para encontrar v e expressá-lo em termos da base ruim β_{ruim} e recuperar m. Se uma atacante, Eve, conhece somente a base β_{ruim} , ela é incapaz de resolver o problema CVP em Λ.

Assim, a segurança do criptossistema está na dificuldade em resolver o CVP usando uma base não ortogonal. Uma forma de atacá-lo é tentar melhorar a base ruim, que é a chave pública, afim de tornar seus vetores menores e mais ortogonais, usando um algoritmo chamado LLL.

Além disso, como a chave pública do sistema GGH é uma base de um reticulado Λ, seu tamanho acaba se tornando muito grande, tornando o uso desse criptossistema ineficiente em termos práticos. O algoritmo 6 detalha esse criptossistema.

Algoritmo 6: Algoritmo do criptossistema GGH

Escolha um reticulado Λ.

Chave privada: $\{v_1, \ldots, v_n\}$ como sendo uma base boa para o reticulado Λ.

Chave pública: $\{w_1, \ldots, w_n\}$ como sendo uma base ruim para o reticulado Λ.

Encriptação de uma mensagem $m \in \mathbb{F}_2^n$: Escolha um vetor de perturbação r. A mensagem cifrada, por sua vez, é dada por: $e = m_1w_1 + m_2w_2 + \cdots + m_nw_n + r$. Note que a mensagem cifrada $e \notin \Lambda$.

Decriptação: Encontre um vetor $u \in \mathcal{L}$ que é próximo a e. Se r for pequeno o suficiente, menor que a norma mínima do reticulado, então

$u = m_1w_1 + m_2w_2 + \cdots + m_nw_n$, com isso, basta resolver o CVP para e em Λ para recuperar m.

A chave privada, que é a base boa para o reticulado Λ, pode ser usada para encontrar u.

Escreva, primeiramente, $e = \mu_1v_1 + \mu_2v_2 + \cdots + \mu_nv_n$, com $\mu_1, \mu_2, \ldots, \mu_n \in \mathbb{R}$. A aproximação

$\mu_1, \mu_2, \ldots, \mu_n$ para o menor inteiro: $\lfloor \mu_1 \rceil v_1 + \cdots + \lfloor \mu_n \rceil v_n$ será igual a u.

4.2 O Criptossistema de Chave Pública NTRU

O sistema NTRU é baseado originalmente em estruturas algébricas, construído em torno de anéis polinomiais, mais especificamente, anéis polinomiais em $R = \frac{\mathbb{Z}[x]}{(x^N-1)}$, onde N é um inteiro maior do que 1 e os elementos desse anel são polinômios da forma: $a(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{N-1}x^{N-1}$. Entretanto, este sistema pode ser descrito de maneira equivalente usando reticulados, uma vez que a chave pública no NTRU consiste em polinômios invertíveis em um anel polinomial, que pode ser definido em um reticulado. Os coeficientes dos polinômios envolvidos no NTRU podem ser considerados pontos no espaço euclidiano N-dimensional, onde N é o grau do polinômio, dessa forma, esses coeficientes podem ser vistos como vetores em um reticulado.

Com base em Bollauf 2014 (BOLLAUF, 2014), para compreender a relação entre o anel convolucional de polinômios e reticulados, precisamos da definição a seguir.

Definição 4.2.1. *Dizemos que um polinômio* $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{N-1}x^{N-1}$ *com coeficientes em* $\mathbb{Z}_q$ *é* ***curto*** *se existir um valor* c *tal que* $1 \leq c \leq \frac{q}{2}$ *e, para cada* i*, a condição* $|a_i| \leq c$ *seja satisfeita.*

O problema considerado difícil na teoria de anéis convolucionais de polinômios é:

Dado um valor $1 < t < N$ e duas sequências de valores módulo q, denotadas por $\{\alpha_1, \alpha_2, \ldots, \alpha_t\}$ e $\{\beta_1, \beta_2, \ldots, \beta_t\}$, precisamos encontrar um polinômio f de grau inferior a N tal que f seja curto e satisfaça a condição

$$f(\alpha_i) = \beta_i, \qquad \text{para todo } 1 \leq i \leq t.$$

Esse problema também pode ser interpretado como uma variante do problema do vetor mais próximo (CVP). Para essa abordagem, consideramos um polinômio p tal que $\deg(p) \leq N-1$ e associamos $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{N-1}x^{(N-1)}$ ao vetor $(a_0, a_1, a_2, \ldots, a_{N-1}) \in \mathbb{Z}^N$. Denotamos por $\mathcal{L}$ o reticulado formado pelos vetores p que satisfazem

$$p(\alpha_i) \equiv 0 \pmod{q}, \qquad \text{para cada } 1 \leq i \leq t.$$

Dessa forma, fica entendido que, se F é um polinômio, não necessariamente curto, que satisfaz $F(\alpha_i) \equiv \beta_i \pmod{q}$, para todo $1 \leq i \leq t$, então, F_0 é o ponto do reticulado $\mathcal{L}$ mais próximo a F, com uma grande possibilidade de $F - F_0$ ser um polinômio curto, considerando as avaliações adequadas.

O algoritmo LLL, já mencionado neste trabalho, é utilizado para resolver de forma aproximada o problema do vetor mais curto e do vetor mais próximo, apresentando bons resultados para dimensões menores que 100. Em reticulados de alta dimensão, ele nem sempre oferece uma base com a redução ideal, ou seja, não gera os vetores mais curtos possíveis.

Outro algoritmo capaz de resolver esses problemas é o BKZ (Block Korkin-Zolotarev), que é mais moderno e uma extensão do algoritmo LLL. Ele funciona realizando uma redução de base em blocos, onde aplica o SVP em sub-reticulados de dimensões menores. Esse processo em blocos oferece uma base de qualidade melhor e, embora seja mais custoso em termos de tempo de execução, fornece uma redução mais forte do que o LLL. Assim, o BKZ é mais adequado para problemas complexos de reticulados e é mais eficaz em contextos onde a resistência contra ataques precisa ser maior (SILVERMAN; PIPHER; HOFFSTEIN, 2014).

O algoritmo do sistema NTRU é robusto, e envolve reduzir a função polinomial módulo p e q , onde p e q são primos escolhidos observando algumas restrições. Além disso, este algoritmo utiliza de uma operação $\circledast$ para denotar um produto de convolução cíclica em R.

Para a encriptação desse sistema, precisamos de mais uma definição:

Definição 4.2.2. *Para quaisquer inteiros positivos d_1 e d_2, teremos:*

$$\mathcal{T}(d_1, d_2) = \boldsymbol{a}(x) \in R : \left\{ \begin{array}{l} \boldsymbol{a}(x) \text{ tem } d_1 \text{ coeficientes iguais a } 1, \\ \boldsymbol{a}(x) \text{ tem } d_2 \text{ coeficientes iguais a } -1, \\ \boldsymbol{a}(x) \text{ tem todos os outros coeficientes iguais a } 0 \end{array} \right\}$$

Polinômios em $\mathcal{T}(d_1, d_2)$ são chamados de polinômios ternários e são análogos aos binários.

Alice escolhe parâmetros públicos (N, p, q, d) com N um inteiro maior do que $1, p$ e q sendo primos com $mdc(p, q) = mdc(N, q) = 1$ e $q > (6d + 1)p$. Posteriormente, ela escolhe um polinômio $f \in T(d+1, d)$ e um $g \in T(d, d)$, que são suas chaves privadas. Alice calcula a inversa de f, que será a F_q, pois é reduzida módulo q e a inversa F_p, que é reduzida módulo p e utiliza da operação $\circledast$ (produto de convolução cíclica) para determinar sua chave pública h, sendo esta $h = F_q \circledast g$.

Na encriptação, Bob escolhe um polinômio m reduzido módulo p, este polinômio representa sua mensagem, além disso, ele escolhe um polinômio $r \in T(d, d)$ e utiliza a h (chave pública de Alice) para computar $e \equiv pr \circledast h + m (\mathrm{mod} q)$, sendo essa sua mensagem criptografada.

Para Alice decriptar e, ela utiliza suas chaves privadas (f, g), e computa $f \circledast e \equiv pg \circledast r + f \circledast m (\mathrm{mod} q)$. Nesta etapa, Alice começa com $f \circledast e$, que é uma combinação linear dos polinômios f, e, g, r e m e a operação é realizada módulo q, ou seja, todos os coeficientes são reduzidos a um intervalo entre $\frac{-q}{2}$ e $\frac{q}{2}$.

Depois, ela ajusta o resultado de $f \circledast e$ para que este pertença ao anel dos polinômios em módulo p. Isso é feito encontrando um polinômio que é congruente a $f \circledast e$ módulo p, ou seja, $a \equiv f \circledast e (\mathrm{mod}\, p)$. Após encontrar o valor ajustado de a, Alice o multiplica por F_P, para calcular $m\, (m \equiv F_p \circledast a (\mathrm{mod} p))$, o resultado m é o polinômio que representa a mensagem original.

Alice	Bob
Criação da chave	
Escolhe o polinômio privado $\boldsymbol{f} \in \mathcal{T}(d+1, d)$ que é invertível em R_q e R_p. Escolhe o polinômio privado $\boldsymbol{g} \in \mathcal{T}(d, d)$. Calcula $\boldsymbol{F}_q$, a inversa de$\boldsymbol{f}$ em R_q. Calcula $\boldsymbol{F}_p$, a inversa de $\boldsymbol{f}$ em R_p.	
Criptografia	
	Escolhe uma mensagem $\boldsymbol{m} \in R_p$ Escolhe um polinômio aleatório $\boldsymbol{r} \in \mathcal{T}(d, d)$. Usa a chave pública de Alice $\boldsymbol{h}$ para calcular $\boldsymbol{e} \equiv p\boldsymbol{r} \star \boldsymbol{h} + \boldsymbol{m} (\mathrm{mod} q)$. Envia a mensagem cifrada $\boldsymbol{e}$ para Alice.
Descriptografia	
Calcula $\boldsymbol{f} \star \boldsymbol{e} \equiv p\boldsymbol{g} \star \boldsymbol{r} + \boldsymbol{f} \star \boldsymbol{m} (\mathrm{mod} q)$. Utiliza a operação "Center-lift" para $\boldsymbol{a} \in R$ e calcula $\boldsymbol{m} \equiv \boldsymbol{F}_p \star \boldsymbol{a} (\mathrm{mod} p)$.	

Tabela 4.1: O Criptossistema NTRU

De acordo com Zanon (2020) (ZANON, 2020), um erro pode ocorrer durante a decifragem ao fazer a convolução entre uma mensagem cifrada c e a chave privada f. Se os parâmetros não forem escolhidos corretamente, um dos coeficientes de $f \circledast c = f \circledast m + g \circledast r$ pode ser maior que q em módulo. Como estamos no anel $R_{N,q}$, esse coeficiente será reduzido módulo q, o que leva à perda de informação, portanto, é necessário garantir que $|f \circledast m + g \circledast r|_\infty < q$.

Zanon (2020) faz uma análise dos parâmetros para o NTRU não homomórfico – uma aplicação homomórfica permite operar diretamente sobre dados cifrados sem a necessidade de decifrá-los – como em Silverman et. al (2014) (SILVERMAN; PIPHER; HOFFSTEIN, 2014), onde é observada uma correlação entre os parâmetros p e q. Contudo, ainda não há critérios específicos para definir automaticamente parâmetros N, p e q em aplicações homomórficas, considerando segurança, número de produtos, e termos por expressão aritmética.

Sabe-se que, uma das principais vantagens dos sistemas criptográficos baseados em reticulados, como o NTRU, é sua alta velocidade em comparação com sistemas baseados em logaritmos discretos e fatoração. No caso do NTRU, o aspecto que mais consome tempo no processo de cifragem e decifragem é o cálculo do produto de convolução. Esses produtos, podem ser computados sem a necessidade de multiplicações e exigem apenas cerca de $\frac{2}{3}N^2$ operações de soma e subtração e ainda, quando d é menor que $N/3$, as duas primeiras operações requerem aproximadamente $\frac{2}{3}dN$ somas e subtrações.

Dessa forma, o processo de cifragem e decifragem no NTRU ocorre em $O(N^2)$[1] etapas, sendo cada uma delas executada de maneira extremamente rápida, pois, embora $O(N^2)$ não seja associada a rapidez para algoritmos em geral, no caso específico do NTRU, é considerado rápido devido à natureza leve das operações e ao fato de que outros sistemas de criptografia podem ter uma complexidade muito maior.

4.2.0.1 Relação entre o NTRU e Reticulados

Embora o NTRU tenha sido originalmente descrito em termos de anéis polinomiais de convolução, ele pode ser analisado e descrito de forma equivalente utilizando reticulados, que oferecem uma perspectiva geométrica sobre sua segurança (MICCIANCIO; GOLDWASSER, 2002).

Os polinômios utilizados no NTRU, como as chaves pública e privada, podem ser representados como vetores em um espaço euclidiano $\mathbb{R}^N$. Por exemplo, um polinômio

[1] O termo $O(N^2)$ é uma notação chamada "notação Big-O", que descreve o comportamento assintótico de algoritmos em termos de eficiência e desempenho conforme o tamanho do problema cresce.

$f(x) = a_0 + a_1x + \cdots + a_{N-1}x^{N-1}$ é associado ao vetor $(a_0, a_1, \ldots, a_{N-1}) \in \mathbb{Z}^N$. Assim, o espaço dos polinômios em R corresponde a um reticulado em $\mathbb{R}^N$.

A segurança do NTRU está intimamente relacionada à dificuldade de resolver problemas computacionais em reticulados, como o problema do vetor mais curto e o problema do vetor mais próximo (NGUYEN; STERN, 2001), que foram discutidos no capítulo 2. O reticulado associado ao NTRU é definido pela matriz geradora:

$$H = \begin{bmatrix} qI & 0 \\ h & I \end{bmatrix},$$

onde q é o parâmetro modular, I é a matriz identidade, e h é o vetor que representa a chave pública. O reticulado gerado por H contém todos os vetores $\mathbf{v} = (r, m - r \circledast h)$, onde r e m são os polinômios utilizados na cifragem.

A partir dessa matriz, o problema de recuperar a chave privada f a partir da chave pública h pode ser interpretado como a resolução do problema do vetor mais curto ou do vetor mais próximo no reticulado $\mathcal{L}$ gerado por H. A escolha dos parâmetros N, p e q é feita para garantir que reduzir a base de $\mathcal{L}$ utilizando algoritmos como LLL ou BKZ seja computacionalmente inviável.

Além disso, o uso de polinômios "curtos" no NTRU está diretamente relacionado ao problema de encontrar vetores curtos no reticulado. Durante o processo de cifragem e decifragem, o algoritmo depende de propriedades geométricas do reticulado para garantir que os coeficientes resultantes permaneçam dentro de intervalos específicos, evitando perdas de informação.

Essa perspectiva baseada em reticulados não apenas fornece uma justificativa matemática adicional para a segurança do NTRU, mas também conecta o sistema a problemas clássicos da teoria de reticulados..

4.2.0.2 Comparação entre RSA e NTRU

A segurança de sistemas criptográficos baseados em diferentes fundamentos matemáticos é um tema de relevância crescente, especialmente no contexto da ascensão dos computadores quânticos. Os algoritmos RSA e NTRU são dois exemplos proeminentes de abordagens distintas para garantir a confidencialidade e a autenticidade das informações. Enquanto o RSA, é amplamente utilizado e se baseia na fatoração de números grandes, o NTRU, fundamenta-se em problemas de reticulados, o que lhe confere uma potencial resistência a ataques quânticos.

Dada a diferença nos fundamentos matemáticos, nos níveis de segurança oferecidos e na eficiência de implementação, é relevante comparar os aspectos principais desses dois sistemas.

A tabela a seguir foi elaborada com base nos trabalhos de Stallings (2016), Hoffstein (1998) e Gentry (2001) (GENTRY; SZYDLO, 2001; HOFFSTEIN; PIPHER; SILVERMAN, 1998; STALLINGS, 2016) com o objetivo de apresentar uma visão geral dessas diferenças, permitindo uma análise clara de cada ponto de distinção entre os sistemas RSA e NTRU, incluindo aspectos como a velocidade de criptografia e descriptografia, os requisitos de chaves e a viabilidade prática.

Aspecto	**RSA**	**NTRU**
Fundamento Matemático	Fatoração de números grandes	Reticulados
Segurança	Alta para chaves grandes, mas vulnerável a ataques quânticos	Alta para reticulados adequados, resistente a ataques quânticos
Velocidade de Criptografia	Lenta (operações com números grandes)	Rápida (menor tempo de computação)
Velocidade de Descriptografia	Lenta	Muito rápida
Tamanho da Chave	Grande para segurança adequada (2.048+ bits)	Pequena (relativamente compacta em comparação)
Resistência a Computadores Quânticos	Vulnerável (devido à fatoração)	Alta resistência
Implementação Prática	Ampla, bem estudada, padrão em muitos sistemas	Comum em algumas aplicações devido à eficiência
Aplicação Comum	Transações financeiras, certificados digitais	Autenticação, sistemas de baixa latência
Requisitos Computacionais	Alto (devido a operações aritméticas intensas)	Menor, adequado para dispositivos com menos potência

Tabela 4.2: Comparação entre os sistemas criptográficos RSA e NTRU

É importante ressaltar que, embora o NTRU se mostre uma alternativa eficiente ao RSA em termos de velocidade de operação e resistência a ataques de computação quântica, ele ainda não conta com uma prova formal de segurança. Essa ausência limita sua adoção em algumas aplicações, uma vez que a segurança de um criptossistema ideal deve ser sustentada tanto pela prática quanto pela teoria. Por outro lado, o RSA, apesar de sua popularidade e segurança comprovada para chaves grandes, permanece vulnerável frente aos avanços dos computadores quânticos.

Na próxima seção, exploraremos o criptossistema baseado no problema do *Learning with Errors* (LWE), que combina segurança eficiente com demonstrações formais, oferecendo uma abordagem promissora para aplicações seguras no cenário pós-quântico.

4.3 O criptossistema LWE (Learning with Errors)

Outro sistema criptográfico bastante conhecido é *o Learning with Errors* (LWE), nesta seção não teremos um estudo detalhado dele, e sim forneceremos ao leitor uma compreensão geral sobre tal criptossistema.

Em 2005, Regev em (REGEV, 2005b) e (REGEV, 2005a), propôs o LWE (Learning With Errors), que foi aprimorado em 2010 por Lyubashevsky, Peikert e Regev (LYUBASHEVSKY; PEIKERT; REGEV, 2010) para uma versão algébrica Ring-LWE. É importante frisar que outras versões algébricas mais práticas e mais seguras vieram depois: Poly-LWE e Twisted Ring-LWE. Um maior aprofundamento sobre essas versões é encontrado nas referências (ORTIZ et al., 2021) e (ELIAS et al., 2020) deste trabalho.

Definição 4.3.1. *O problema de LWE é definido como a busca do vetor $s \in \mathbb{Z}_q^n$ a partir de um conjunto de equações da forma $\langle s, a_i \rangle + e_i = b_i \pmod q$, onde $1 \leq i \leq n$. Onde onde a_i é um vetor de entrada público, escolhido uniformemente em $\mathbb{Z}_q^n$, os valores e_i são erros pequenos adicionados conforme uma distribuição $\mathcal{D}$, geralmente escolhida como uma distribuição normal, e b_i são os resultados correspondentes das equações.*

Em 2010, Lyubashevsky, Peikert e Regev introduziram o uso de anéis polinomiais para definir o esquema de LWE em anel (Ring-LWE),

Definição 4.3.2. *Dado um polinômio $f(x) = x^d + 1$, onde d é uma potência de 2, um inteiro q, e um elemento $s \in R_q = \mathbb{Z}_q[x]/f(x)$, o problema Ring-LWE consiste em encontrar s que satisfaça as equações $s \cdot a_i + e_i = b_i \pmod{R_q}$, onde $1 \leq i \leq n$. Sendo, a_i e b_i são elementos de R_q, e a redução modular em R_q implica a redução dos coeficientes do polinômio resultante módulo $f(x)$ e módulo q.*

Com base no problema Ring-LWE, podemos construir um criptossistema da seguinte forma:

- **Geração de Chaves**: Escolhe-se aleatoriamente um elemento $a \in R_q$ e utiliza-se a distribuição $\mathcal{D}$ para gerar os elementos s e e em R. A chave privada é dada por s, e a chave pública por $(a, b = a \cdot s + e)$.
- **Encriptação**: Para encriptar d bits, os bits podem ser interpretados como coeficientes de um polinômio em R. O algoritmo de encriptação escolhe valores $r, e_1, e_2 \in R$ de acordo

com a distribuição $\mathcal{D}$ e calcula o par (u, v) da seguinte forma:

$$\begin{aligned} u &= a \cdot r + e_1 \pmod{q}, \\ v &= b \cdot r + e_2 + \left\lfloor \frac{q}{2} \right\rfloor \cdot z \pmod{q}, \end{aligned} \tag{4.3.0.1}$$

onde z representa o valor binário dos bits a serem encriptados.

- **Decriptação**: O algoritmo de decriptação realiza o cálculo

$$v - u \cdot s = (r \cdot e - s \cdot e_1 + e_2) + \left\lfloor \frac{q}{2} \right\rfloor \cdot z \pmod{q}. \tag{4.3.0.2}$$

Recentemente, o uso do polinômio ciclotômico $f(x)$ e a distribuição gaussiana $\mathcal{D}$, foram integrados ao esquema NTRU, o que permitiu alcançar uma criptografia semântica segura e eficiente baseada em reticulados. Esse novo criptossistema foi submetido à competição do NIST e selecionado como finalista para a categoria de "Key Encapsulation Mechanisms". Essa escolha pelo NIST reflete a confiabilidade e eficiência do NTRU para proteção contra ataques quânticos e sua adequação para futuros padrões de criptografia.

Conclusões e perspectivas

Conclui-se que a Teoria dos Reticulados desempenha um papel fundamental em sistemas criptográficos modernos, proporcionando uma base matemática sólida para garantir a segurança da comunicação. Sistemas como NTRU aproveitam a complexidade dos problemas difíceis em reticulados para criar algoritmos de criptografia robustos, podendo ser resistentes a ataques quânticos. Dessa forma, inserir os conceitos de reticulados em criptossistemas representa uma abordagem promissora para a segurança dos dados. Em relação ao NTRU, pudemos observar que, apesar de ter uma interpretação polinomial, é construído sobre reticulados convolucionais modulares e exibe uma notável resistência a ataques quânticos devido à dificuldade de encontrar vetores curtos, um problema de alta complexidade em teoria dos reticulados.

No caso do GGH, o qual utilizamos o algoritmo de Babai, tivemos importantes conclusões sobre a influência das propriedades geométricas da base, como o ângulo e norma entre vetores, na eficácia do algoritmo. Percebemos que no espaço $\mathbb{R}^2$, o algoritmo de Babai é estável para vetores da base que possuem mesma norma, independentemente do ângulo, e identificamos circunstâncias específicas em que ele pode falhar com vetores de normas diferentes. Essa análise pode contribuir para o entendimento e aprimoramento de métodos de redução de bases em criptografia.

A partir disso, apresentamos as perspectivas futuras em ralação ao nosso trabalho.

- **Identificação de Famílias de Reticulados no NTRU**: Analisar sobre famílias de reticulados no NTRU, especialmente em dimensões baixas. A identificação de boas famílias de reticulados pode ajudar a verificar a segurança dessas estruturas, permitindo otimizações e potencializando a aplicabilidade do NTRU.

- **Validação da Conjectura no Algoritmo de Babai**: Estudar mais detalhadamente a conjectura de que o algoritmo de Babai sempre é eficaz em $\mathbb{R}^2$ quando os vetores da base possuem mesma norma, independentemente do ângulo entre eles. Isso poderá ampliar o uso de técnicas de redução de bases em dimensões superiores.

Bibliografia

AJTAI, M. Generating hard instances of lattice problems. *Proceedings of the 28th Annual ACM Symposium on Theory of Computing*, ACM, p. 99–108, 1996.

BERNSTEIN, D.; BUCHMANN, J.; DAHMEN, E. *Introduction to Post-Quantum Cryptography*. [S.l.]: Springer, 2009. 1–14 p.

BOLLAUF, M. Criptografia baseada em reticulados. 2014. Trabalho acadêmico.

CHEN, Y. Quantum algorithms for lattice problems. *arXiv preprint*, 2024. Disponível em: <https://arxiv.org/abs/2404.11232>. Acesso em: 20 de ago. 2024.

CONWAY, J.; SLOANE, N. *Sphere Packings, Lattices and Groups*. New York: Springer-Verlag, 1999.

ELIAS, Y. et al. Provably weak instances of ring-lwe. *arXiv preprint*, 2020. Disponível em: <https://arxiv.org/abs/1502.03708>. Acesso em: 13 dez. 2023.

FERRARI, A. *Reticulados algébricos: Abordagem matricial e simulações*. Campinas: Imecc-Unicamp, 2012. (Tese de doutorado).

GENTRY, C.; SZYDLO, M. Cryptanalysis of the ntru public key cryptosystem. In: SPRINGER. *Advances in Cryptology – EUROCRYPT 2001*. [S.l.], 2001. p. 182–200.

GRUBER, P. M.; LEKKERKERKER, C. G. *Geometry of Numbers*. Amsterdam: North-Holland, 1987. v. 37. (North-Holland Mathematical Library, v. 37). ISBN 978-0444869663.

HERSTEIN, I. *Tópicos de Álgebra*. São Paulo: Editora Polígono S.A., 1970.

HOFFSTEIN, J.; PIPHER, J.; SILVERMAN, J. Ntru: A ring-based public key cryptosystem. *Algorithmic Number Theory Symposium (ANTS)*, Springer, p. 267–288, 1998.

IEZZI, G.; DOMINGUES, H. *Álgebra Moderna*. [S.l.]: Saraiva Educação SA, 1970.

LINDNER, R.; PEIKERT, C. Better key sizes (and attacks) for lwe-based encryption. *Cryptology ePrint Archive*, 2011. Disponível em: <https://eprint.iacr.org/2011/473>. Acesso em: 13 jul. 2023.

LYUBASHEVSKY, V.; PEIKERT, C.; REGEV, O. On ideal lattices and learning with errors over rings. *Proceedings of the 43rd Annual ACM Symposium on Theory of Computing*, p. 1–10, 2010. DOI: 10.1145/1806689.1806725.

MICCIANCIO, D.; GOLDWASSER, S. *Complexity of Lattice Problems: A Cryptographic Perspective*. [S.l.]: Springer, 2002.

NGUYEN, P. Q.; STERN, J. The two faces of lattices in cryptology. *Proc. of Cryptography and Lattices*, p. 146–180, 2001.

ORTIZ, J. et al. The ring-lwe problem in lattice-based cryptography: The case of twisted embeddings. *Entropy*, v. 23, n. 9, p. 1108, 2021. Disponível em: <https://doi.org/10.3390/e23091108>. Acesso em: 13 dez. 2023.

PEIKERT, C. A decade of lattice cryptography. *Foundations and Trends in Theoretical Computer Science*, v. 10, n. 4, p. 283–424, 2016.

REGEV, O. On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM*, v. 56, n. 6, p. 1–40, 2005. DOI: 10.1145/1067159.1067162.

REGEV, O. On the hardness of lattice problems. *Proceedings of the 37th Annual ACM Symposium on Theory of Computing*, p. 473–482, 2005. DOI: 10.1145/1060590.1060664.

ROUSSEAU, S. Quantum algorithms for lattice problems. *Quantum Science and Technology*, v. 5, n. 2, p. 123–130, 2024. DOI: 10.1088/2058-9565/abcde.

SILVERMAN, J.; PIPHER, J.; HOFFSTEIN, J. *An Introduction to Mathematical Cryptography*. [S.l.]: Springer, 2014. v. 3.

SINGH, S. *O Livro dos Códigos*. [S.l.]: Editora Record, 2004.

SPECTRUM, I. Nist announces post-quantum cryptography standards. *IEEE Spectrum*, 2024. Disponível em: <https://spectrum.ieee.org/post-quantum-cryptography-2668949802>. Acesso em: 10 set. 2024.

STALLINGS, W. *Cryptography and Network Security: Principles and Practice*. 7th. ed. [S.l.]: Pearson Education, 2016. ISBN 978-0134444284.

ZANON, G. M. *Criptografia Homomórfica*. 2020. Trabalho acadêmico.