UNIVERSIDADE DE BRASÍLIA
INSTITUTO DE CIÊNCIAS EXATAS
DEPARTAMENTO DE MATEMÁTICA

Algoritmo LLL e Magma na Resolução de Inequações Diofantinas Exponenciais e Somas de Potências de Fibonacci

por

Victor Carvalho Cardoso

Brasília
2024

Victor Carvalho Cardoso

Algoritmo LLL e Magma na Resolução de desigualdades Diofantinas Exponenciais e Somas de Potências de Fibonacci

Dissertação apresentada ao Programa de Pós-Graduação em Matemática da Universidade de Brasília, como requisito parcial para obtenção do titulo de Mestre em Matemática.

Orientador: Prof. Dr. Hemar Godinho.

Brasília
2024

Agradecimentos

Quero expressar minha profunda gratidão a Deus e a todas as pessoas que contribuíram para a realização deste trabalho.

Primeiramente agradeço ao Senhor pela vida e tempo dedicado a esse estudo. Agradeço sinceramente ao meu orientador, Hemar, pela orientação sábia, apoio constante, e por acreditar em mim desde o início. Sua paciência, dedicação e valiosos conselhos foram fundamentais para o sucesso desta dissertação.

Também gostaria de agradecer aos membros da banca examinadora pela avaliação cuidadosa deste trabalho e pelas sugestões construtivas que contribuíram significativamente para o aprimoramento do mesmo.

Sou grato à minha família, em especial á minha noiva Maria pelo apoio incondicional, encorajamento e compreensão ao longo desta jornada acadêmica. Seu amor e apoio foram o alicerce que me permitiu alcançar meus objetivos.

Por fim, quero expressar minha gratidão aos meus amigos e colegas de trabalho que estiveram ao meu lado durante este período. Seus estímulos, trocas de experiências e momentos de descontração foram essenciais para manter minha motivação e determinação.

"Penso, logo existo."

René Descartes

Resumo

Nos meandros da matemática, encontra-se um fascinante desafio que tem intrigado mentes brilhantes há séculos: as desigualdades e equações exponenciais Diofantinas. Estas representam uma esfera de estudo rica e complexa, onde as propriedades intrínsecas das potências lançam enigmas profundos para serem decifrados. O que torna estas equações tão cativantes é sua capacidade de se entrelaçarem com os princípios fundamentais da teoria dos números, abrindo portas para novos horizontes de compreensão matemática. Motivados pela curiosidade incessante que caracteriza este campo, lançamo-nos na jornada para explorar as soluções por trás dessas desigualdades e equações exponenciais. Nosso foco repousa sobre as desigualdades exponenciais Diofantinas do tipo $|p^x - q^y| < p^{\gamma x}$, bem como na intrigante equação exponencial Diofantina $T_n^s + T_{n+1}^s = F_m$, construída sobre as sequências de Fibonacci. Para tal investigação, empregamos o poderoso algoritmo LLL, uma ferramenta concebida por Lenstra, Lenstra e Lovász, que desvela padrões ocultos e revela estruturas subjacentes em espaços vetoriais, contamos também com a assistência do sofisticado software de álgebra computacional Magma, uma ferramenta que potencializa nossa capacidade de análise.

Palavras Chaves: desigualdades Diofantinas, Algoritmo LLL, Equação com sequencias de Fibonacci.

Abtract

In the intricacies of mathematics lies a fascinating challenge that has intrigued brilliant minds for centuries: Diophantine exponential inequalities and equations. These represent a rich and complex sphere of study, where the intrinsic properties of powers pose deep enigmas to be deciphered. What makes these equations so captivating is their ability to intertwine with the fundamental principles of number theory, opening doors to new horizons of mathematical understanding. Motivated by the relentless curiosity that characterizes this field, we embark on a journey to explore the solutions behind these exponential inequalities and equations. Our focus rests on Diophantine exponential inequalities of the form $|p^x - q^y| < p^{\gamma x}$, as well as the intriguing Diophantine exponential equation $T_n^s + T_{n+1}^s = F_m$, constructed upon the Fibonacci sequences. For such investigation, we employ the powerful LLL algorithm, a tool conceived by Lenstra, Lenstra, and Lovász, which unveils hidden patterns and reveals underlying structures in vector spaces. We also rely on the assistance of the sophisticated computational algebra software, Magma, a tool that enhances our analytical capabilities.

Keywords: Diophantine Inequalities, LLL Algorithm, Equation with Fibonacci Sequences.

Conteúdo

Introdução

Na área da matemática, uma equação Diofantina é uma expressão na qual várias variáveis são restritas a assumir apenas valores inteiros. O termo "Diofantina" é uma homenagem ao matemático helenístico Diofanto de Alexandria, que viveu no século III e se dedicou ao estudo dessas equações, sendo um dos pioneiros no uso de símbolos na álgebra.

Diofanto desempenhou um papel significativo no desenvolvimento da álgebra e influenciou muitos matemáticos posteriores a explorarem a teoria dos números. Ele foi reconhecido por sua contribuição ao introduzir a notação abreviada na álgebra grega, simplificando a representação de quantidades e operações.

Embora a maioria dos historiadores situe Diofanto no século III d.C., há evidências que sugerem que ele pode ter vivido na mesma época que Herão. Poucos detalhes sobre sua vida são conhecidos, exceto que ele trabalhou em Alexandria. Algumas informações sobre sua vida podem ser encontradas em um epigrama na Antologia Grega.

Entre as obras de Diofanto, como "Aritmética", "Sobre Números Poligonais" e "Porisma", destaca-se "Aritmética", que é a obra mais extensamente preservada do autor, consistindo em seis dos treze livros que ele escreveu. Nesta obra, ele apresenta uma abordagem analítica da teoria dos números e resolve 130 problemas diversos, incluindo equações de primeiro e segundo graus, além de uma equação cúbica peculiar. Os problemas algébricos indeterminados que possuem apenas soluções racionais são conhecidos como "problemas diofantinos", e o termo hoje em dia refere-se a problemas nos quais as soluções estão restritas a números inteiros.

O estudo matemático dos problemas propostos por Diofanto é conhecido como análise Diofantina. De acordo com Smart [11] questões comuns abordadas em uma análise Diofantina típica incluem:

I. Existe alguma solução?

II. Há outras soluções além das facilmente identificadas?

III. O número de soluções é finito ou infinito?

IV. Todas as soluções são teoricamente determináveis?

V. É possível calcular todas as soluções?

Um exemplo de problema Diofantino é: um pai tem 1 ano a menos que o dobro da idade do filho, e os dígitos AB que formam a idade do pai são invertidos na idade do filho, ou seja, BA, o que nos leva à equação $19B - 8A = 1$.

Esses tipos de problemas tradicionais muitas vezes permanecem sem solução por séculos até que alguns matemáticos comecem a entender sua profundidade, em vez de tratá-los apenas como quebra-cabeças.

Apesar de equações individuais apresentarem um certo nível de desafio e terem sido consideradas ao longo da história como meros problemas, a formulação de teorias gerais para as equações Diofantinas foram realizadas apenas no século XX.

Um campo bastante estudado e investigado atualmente pela Análise Diofantina é o das equações e desigualdades Diofantinas exponenciais. Uma inequação Diofantina exponencial é uma inequação na forma

$$f(x_1, x_2, \ldots, x_n) > 0 \quad \text{ou} \quad f(x_1, x_2, \ldots, x_n) < 0,$$

onde f é uma função exponencial das variáveis $x_1, x_2, \ldots, x_n$ e os coeficientes de f são inteiros. Em nosso estudo investigaremos as soluções da inequação

$$|a^{x_1} - b^{x_2}| < a^{\delta x_1},$$

onde $0 < \delta < 1$ é um número real fixo e a, b são inteiro positivos.

As desigualdades Diofantinas exponenciais tem aplicações em diversas áreas, incluindo criptografia, teoria dos grafos, teoria dos números computacionais e teoria dos jogos.

O estudo dessas desigualdades remonta a trabalhos de importantes matemáticos como Fermat, Euler e Legendre. No entanto, foi somente no século XX que a teoria das desigualdades Diofantinas exponenciais começou a se desenvolver de forma mais sistemática, com contribuições significativas de pesquisadores como Baker, Matiyasevich e Schlickewei.

Detalhando um pouco mais sobre as aplicações dessas desigualdades, uma das áreas mais importantes é na criptografia de chave pública, onde são utilizadas na construção de algoritmos de criptografia de base matemática, como o RSA e o Diffie-Hellman, sua importância se dá pois a segurança desses algoritmos depende da dificuldade em resolver certos tipos de desigualdades Diofantinas exponenciais.

As desigualdades também são frequentemente usadas na análise de complexidade de algoritmos e na teoria dos números computacionais. No que tange a teoria dos grafos elas são usadas para analisar propriedades de grafos exponenciais e em árvores de busca em largura.

Já uma equação Diofantina exponencial é uma equação onde uma ou mais variáveis ocorrem como expoentes. Em termos gerais, uma equação Diofantina exponencial tem a forma:

$$a_1^{x_1} + a_2^{x_2} + \ldots + a_n^{x_n} = b,$$

onde a_1, a_2, ..., a_n, e b são constantes inteiras, e x_1, x_2, ..., x_n são variáveis inteiras desconhecidas.

Uma das aplicações mais notáveis para equações Diofantinas exponenciais é na teoria dos números, onde são utilizadas para investigar propriedades dos números inteiros e dos números primos, além de, também, desempenharem um papel importante na criptografia.

Uma fato bem interessante é que essas equações têm sido estudadas em contextos geométricos e analíticos, fornecendo insights sobre a distribuição de pontos em curvas elípticas e superfícies abelianas. Elas também têm aplicações em física teórica, particularmente na teoria das cordas e na teoria dos números em sistemas físicos quânticos.

Um exemplo muito interessante dessas equações é o problema da soma de potências de Fibonacci estudado por Chaves e Marques [2] onde mostraram que

$$(F_n^{(k)})^s + (F_{n+1}^{(k)})^s = F_m^{(k)},$$

não tem solução em inteiros positivos com a condição $n \geq 2$ e $3 \leq k \leq \min\{n, \log s\}$. Outros resultados interessantes a cerca destas equações serão apresentados no capitulo 4. Em nosso estudo abordaremos as soluções do seguinte caso particular de equação:

$$T_n^s + T_{n+1}^s = F_m$$

para inteiros positivos $s \geq 2$ e $n \geq 2$, onde F_n é o n-ésimo número de Fibonacci e $T_n = F_n^{(3)}$ é o n-ésimo número de Tribonacci. Alguns outros exemplos de equações Diofantinas exponenciais são:

I. Equação de Fermat: $x^n + y^n = z^n$ para $n > 2$.

II. Equação de Ramanujan-Nagell: $2^n - 7 = x^2$ para $n > 2$.

III. Equação de Thue-Mahler: $f(x, y) = c$ onde f é uma forma polinomial com coeficientes inteiros e c é uma constante inteira.

IV. Equação de Pell: $x^2 - Dy^2 = 1$, onde D é livre de quadrados.

Em resumo, as equações e desigualdades Diofantinas exponenciais desempenham um papel significativo em várias áreas da matemática e da ciência, desafiando os matemáticos a desenvolverem novas técnicas e métodos para resolver problemas complexos.

De modo geral, mas nem tão geral, problemas Diofantinos possuem menos equações que variáveis desconhecidas e se resumem a achar inteiros que deverão

funcionar corretamente para todas as equações. Numa linguagem um pouco mais técnica, elas definem uma curva algébrica, uma superfície algébrica ou um objeto mais genérico e então é pedido para se achar os reticulados.

Nesse contexto surge o algoritmo LLL, sigla para Lenstra-Lenstra-Lovász. Esse algoritmo busca a redução de bases para reticulados. Ele foi proposto por Arjen K. Lenstra, Hendrik W. Lenstra Jr. e László Lovász em 1982.

A história do algoritmo LLL remonta aos esforços para resolver problemas fundamentais na teoria dos números e na criptografia. Inicialmente desenvolvido como uma técnica para resolver o problema de vetor mais curto (CVP) em reticulados, o algoritmo LLL logo se tornou uma ferramenta essencial em várias áreas da matemática aplicada e da ciência da computação.

As aplicações do algoritmo LLL são vastas e abrangem várias disciplinas. Na criptografia, é utilizado para resolver problemas relacionados com sistemas de chave pública, como criptoanálise de criptossistemas baseados em reticulados. Na teoria dos números, é empregado em problemas relacionados à decomposição de inteiros e fatoração de números.

Além disso, o algoritmo LLL encontra aplicação em áreas como processamento de sinais, design de códigos, aprendizado de máquina e otimização combinatória. Sua eficácia em reduzir bases de reticulados de forma polinomial o torna uma ferramenta valiosa em problemas de otimização linear e não linear.

Em nosso objetivo o LLL tem papel fundamental na redução dos limites superiores para soluções de equações e desigualdades Diofantinas, no entanto devido a grandeza e complexidade de aplicação desses limites superiores no algoritmo, faz-se necessário o auxilio de uma ferramenta que será nossa aliada, o Magma.

O Magma é um software de álgebra computacional desenvolvido pela Universidade de Sydney na década de 1980. Desde então, tornou-se uma ferramenta essencial para resolver uma variedade de problemas em matemática e ciências afins. Sua história remonta a John Cannon e outros pesquisadores que buscavam uma plataforma eficiente para realizar cálculos complexos em álgebra, teoria dos números, geometria algébrica e outras áreas da matemática.

O Magma é amplamente utilizado em diversas aplicações importantes, como a resolução de sistemas de equações algébricas, fatoração de inteiros, criptografia, análise de curvas e superfícies algébricas, entre outras. Sua flexibilidade e eficiência o tornam uma escolha popular entre pesquisadores, educadores e profissionais que lidam com problemas matemáticos complexos. Sua capacidade de lidar com cálculos complexos e realizar análises detalhadas o torna uma ferramenta valiosa em muitos campos da matemática e ciências relacionadas.

Sua comunidade de usuários e desenvolvedores é ativa e colaborativa, contribuindo para a melhoria contínua do software. Atualizações regulares e novos recursos são adicionados para atender às necessidades em constante evolução dos

usuários.

Neste trabalho usaremos o LLL em conjunto com o Magma e outros resultados para reduzir e encontrar com efetividade as soluções das desigualdades e equações Diofantinas exponenciais, esta ultima em particular dada por soma de potencias de sequencias de Fibonacci.

Iniciaremos a próximo capítulo falando com detalhes sobre o fabuloso algoritmo LLL, no capítulo seguinte, daremos uma breve introdução sobre o software Magma apontando os comandos de fundamental importância para compreender o desenrolar dos exemplos e demonstrações, no capítulo subsequente apresentaremos breves resultados sobre a teoria de limites para formas lineares em logaritmo e usaremos estes em conjunto com o conhecimentos dos capítulos anteriores para solucionar desigualdades Diofantinas exponenciais. Por fim, no ultimo capítulo apresentaremos um conjunto de resultado preliminares e com estes solucionaremos uma equação com soma de potenciais de sequencias de Fibonacci.

Capítulo 1

Algoritmo LLL

O objetivo principal do algoritmo LLL é a redução de bases de reticulados definidos no $\mathbb{R}^n$. Esse algoritmo representa um avanço significativo no estudo dos reticulados, permitindo a tradução de problemas matemáticos para o contexto dos reticulados.

O algoritmo LLL, cujos autores são Arjen K. Lenstra, Hendrik W. Lenstra e László Lovász, foi proposto no artigo intitulado "Factoring Polynomials with Rational Coefficients", publicado em 1982.

Uma possível origem para o algoritmo LLL, conforme Nguyen [9], remonta a maio de 1980, quando Peter van Emde Boas estava visitando Roma. Durante sua estadia, ele discutiu um problema específico com Alberto Marchetti-Spaccamela.

O problema em questão era determinar se era possível, em tempo polinomial, verificar se existe um ponto com coeficientes inteiros dentro do triângulo formado por três pontos com coordenadas racionais em um plano. A princípio, a resposta parecia simples: para triângulos grandes, a resposta seria afirmativa, e para triângulos pequenos, seria razoável esperar apenas um pequeno número de pontos inteiros próximos para verificação. No entanto, esse raciocínio não se aplicava a triângulos extremamente longos e finos.

Embora fosse possível transformar um triângulo tão delgado em um com uma forma mais "arredondada", essa transformação afetava o reticulado associado. Van Emde Boas e Marchetti-Spaccamela encontraram dificuldades ao lidar com esses reticulados inclinados. Ao retornar a Amsterdã, Van Emde Boas consultou Hendrik Lenstra sobre o problema. Lenstra prontamente sugeriu que a redução de reticulado desenvolvida por Gauss quase duzentos anos antes poderia resolver esse problema.

1.1 Espaço Euclidiano $\mathbb{R}^n$

Inicialmente vamos definir o espaço onde iremos trabalhar e suas ferramentas fundamentais.

Consideramos n-uplas dos elementos de um campo $\mathbb{R}$ como sendo os vetores colunas ou vetores linhas

$$\mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \in \mathbb{R}^n, \qquad \mathbf{x} = \begin{bmatrix} x_1 & x_2 & \dots & x_n \end{bmatrix} \in \mathbb{R}^n.$$

Usaremos ambas as notações ao longo deste escrito, e quando for necessário deixarei claro qual delas deve ser considerada para que não haja erro de interpretação. Antes de tudo, vamos primeiro definir algumas operações e lemas básicos sem apresentar as demonstrações, mais o leitor pode encontra-las em Bremner [1].

Definição 1. *Dados dois vetores* $\mathbf{x}$, $\mathbf{y}$ *de* n*-uplas do campo* $\mathbb{R}^n$ *definimos a soma, multiplicação por escalar e produto interno respectivamente por*

$$\mathbf{x} + \mathbf{y} = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} + \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} x_1 + y_1 \\ x_2 + y_2 \\ \vdots \\ x_n + y_3 \end{bmatrix}$$

$$a\mathbf{x} = a \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} ax_1 \\ ax_2 \\ \vdots \\ ax_n \end{bmatrix} \qquad a \in \mathbb{R}$$

$$\mathbf{x} \cdot \mathbf{y} = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \cdot \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix} = \sum_{i=1}^{n} x_i y_i.$$

Além disso a norma de um vetor $\mathbf{x} \in \mathbb{R}^n$ *fica definida como*

$$|\mathbf{x}| = \sqrt{\mathbf{x} \cdot \mathbf{x}} = \sqrt{\sum_{i=1}^{n} x_i^2}.$$

Com isso apresentados os seguinte lemas,

Lema 1. *Dois vetores* $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$ *são ditos* **ortogonais** *se é somente se* $\mathbf{x} \cdot \mathbf{y} = 0$.

Lema 2 (Desigualdade de Cauchy-Schwarz)**.** *Para quaisquer vetores* $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$ *vale a seguinte desigualdade,*

$$|\mathbf{x} \cdot \mathbf{y}| \leq |\mathbf{x}| \cdot |\mathbf{y}|.$$

Definição 2. *Dados vetores* $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$ *com* $\mathbf{y} \neq 0$*, definimos* $\mathbf{u}$ *e* $\mathbf{v}$ *como sendo respectivamente os componentes paralelo a* $\mathbf{x}$ *e ortogonal a* $\mathbf{y}$ *dados por*

$$\mathbf{u} = \left(\frac{\mathbf{x} \cdot \mathbf{y}}{\mathbf{y} \cdot \mathbf{y}}\right) \cdot \mathbf{y}, \qquad \mathbf{v} = \mathbf{x} - \left(\frac{\mathbf{x} \cdot \mathbf{y}}{\mathbf{y} \cdot \mathbf{y}}\right) \cdot \mathbf{y}.$$

Definição 3. *Os vetores* $\mathbf{x_1}, \mathbf{x_2}, ..., \mathbf{x_n} \in \mathbb{R}^n$ *são ditos* **lineramente independentes** *se a combinação linear desses vetores*

$$a_1\mathbf{x_1} + a_2\mathbf{x_2} + \ldots + a_k\mathbf{x_k} = 0 \quad (a_1, a_2, \ldots, a_k \in \mathbb{R})$$

possui somente a solução trivial $a_k = 0$, $\forall k \in \mathbb{N}$*. Caso contrario os vetores são ditos* **lineramente dependentes***.*

Além disso, denotaremos os vetores canônicos do $\mathbb{R}^n$ por $e_1, e_2, ..., e_n$, que por definição possuem a i-ésima coordenada igual a 1 e as demais iguais a zero.

1.2 Reticulados

Nessa subseção será apresentado a definição formal dos reticulado e algumas de suas propriedades.

Definição 4. *Seja* $\mathbf{x_1}, \mathbf{x_2}, ..., \mathbf{x_n}$ *uma base do* $\mathbb{R}^n$ *para* $n \geq 1$*. O* **Reticulado** *com base* $\mathbf{x_1}, \mathbf{x_2}, ..., \mathbf{x_n}$ *e dimensão* n *é o conjunto* $\mathbb{L}$ *de todas as combinações lineares dos vetores bases com coeficientes inteiros, ou seja*

$$\mathbb{L} = \mathbb{Z}\mathbf{x_1} + \mathbb{Z}\mathbf{x_2} + ... + \mathbb{Z}\mathbf{x_n} = \left\{ \sum_{i=1}^{n} a_i\mathbf{x_i} | a_1, a_2, ..., a_n \in \mathbb{Z} \right\}.$$

As bases $\mathbf{x_1}, \mathbf{x_2}, ..., \mathbf{x_n}$ são ditas geradoras do reticulado. Além disso, para $i = 1, 2, ..., n$, escrevemos $\mathbf{x_i} = (x_{i1}, ..., x_{in})$ e formamos a matrix $X = (\mathbf{x}_{ij})$ de ordem $n \times n$ cujo vetores bases de $\mathbb{L}$ são as linhas da matriz X. Assim,

$$|\det(X)| = \det(\mathbb{L}), \tag{1.1}$$

onde $det(\mathbb{L})$ é dito determinante do reticulado.

É fácil nota que, quando o reticulado possui dimensão maior ou igual a dois existem vetores $\mathbf{y_1}, \mathbf{y_2}, ..., \mathbf{y_n}$ diferentes de $\mathbf{x_1}, \mathbf{x_2}, ..., \mathbf{x_n}$ que também são base de $\mathbb{L}$. Para ver isso considere uma base X e uma matriz $C = (c_{ij})$, $n \times n$ com entradas inteiras e determinante igual a ± 1 (Matriz Unimodular), definindo então

$$Y = CX$$

e usando a equação 1 temos,

$$|\det(Y)| = ||\det(CX)| = |\det(X)| = |\det(\mathbb{L})|.$$

Portanto Y é um outra base para $\mathbb{L}$. Assim temos o seguinte corolário

Corolário 3. *O determinante do reticulado não depende da base.*

Vejamos um exemplo contendo tudo que foi exposto até aqui.

Exemplo 1. *Seja $\mathbb{L}$ um reticulado com base definida pelos vetores $\mathbf{x_1} = (4, 5, 1)$, $\mathbf{x_2} = (4, 8, 2)$ e $\mathbf{x_3} = (6, 2, 6)$ pertencentes ao $\mathbb{R}^3$. A matriz base de $\mathbb{L}$ é dada então por*

$$X = \begin{bmatrix} 4 & 5 & 1 \\ 4 & 8 & 2 \\ 6 & 2 & 6 \end{bmatrix} \qquad \det(\mathbb{L}) = |\det(X)| = 76$$

Escolhendo uma matriz unimodular qualquer C, por exemplo

$$C = \begin{bmatrix} 2 & 1 & 4 \\ -2 & 1 & -1 \\ -1 & 2 & 2 \end{bmatrix} \qquad \det(C) = 1$$

conseguimos calcular uma nova base Y para $\mathbb{L}$,

$$Y = CX \Rightarrow Y = \begin{bmatrix} 2 & 1 & 4 \\ -2 & 1 & -1 \\ -1 & 2 & 2 \end{bmatrix} \cdot \begin{bmatrix} 4 & 5 & 1 \\ 4 & 8 & 2 \\ 6 & 2 & 6 \end{bmatrix}$$

$$Y = \begin{bmatrix} 36 & 26 & 28 \\ -10 & -4 & -6 \\ 16 & 15 & 15 \end{bmatrix} \qquad \det(\mathbb{L}) = |\det(Y)| = 76$$

Com esse exemplo podemos ver o quão fácil é começar com uma base composta por vetores curtos e, em seguida, produzir outras bases compostas por vetores muito mais longos. Em nosso contexto, é muito mais interessante e importante fazer exatamente o oposto: Dada uma base para um reticulado, que em geral é composta por vetores longos, queremos encontrar outra base "reduzida"para o mesmo reticulado, ou seja, uma base composta por vetores curtos. Este é o problema fundamental da redução de base de reticulados. Para entender como podemos encontrar essa base reduzida, precisamos primeiramente compreender a ortogonalização de Gram-Schmidt.

1.3 Ortogonalização de Gram-Schmidt

O Processo de ortogonalização de Gram-Schmidt é um método para ortogonalização de um conjunto de vetores linearmente independentes em um espaço definido com produto interno euclidiano, normalmente o espaço euclidiano $\mathbb{R}^n$.

O nome do processo é uma homenagem a Jorge Pedersen Gram e Erhard Schmidt, que apesar de não o terem descoberto foi utilizado por Gram em sua tese de doutorado e por Schmidt em seus estudos sobre espaços vetoriais.

O método fixa um dos vetores e sequencialmente projeta os outros de maneira ortogonal ao anterior, ortogonalizando entre si todos os vetores. Vejamos com mais detalhes: Considere uma base qualquer do $\mathbb{R}^n$ dada por $\mathbf{x_1}, ..., \mathbf{x_n}$, o objetivo é construir uma base ortogonal $x_1^*, ..., x_n^*$ para $\mathbb{R}^n$, de inicio tomemos o primeiro vetor $x_1^* = \mathbf{x_1}$, agora necessitamos de um vetor x_2^* que seja ortogonal a x_1^*, isto é, $x_2^* \cdot x_1^* = 0$, podemos olhar par x_2^* como sendo $\mathbf{x_2}$ menos a projeção ortogonal de $\mathbf{x_2}$ sobre $\mathbf{x_1}$, isto é,

$$x_2^* = \mathbf{x_2} - \mu x_1^*$$

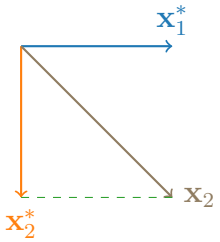

Figura 1.1: Representação

μ é escolhido de tal maneira que

$$x_2^* \cdot x_1^* = 0$$

$$(\mathbf{x_2} - \mu x_1^*) \cdot x_1^* = 0$$

resolvendo esta equação, temos

$$\mathbf{x_2} \cdot x_1^* - \mu x_1^* \cdot x_1^* = 0$$

$$\mu x_1^* \cdot x_1^* = \mathbf{x_2} \cdot x_1^*$$

$$\mu = \frac{\mathbf{x_2} \cdot x_1^*}{x_1^* \cdot x_1^*}$$

logo o segundo vetor ortogonal é dado por

$$x_2^* = \mathbf{x_2} - \frac{\mathbf{x_2} \cdot x_1^*}{x_1^* \cdot x_1^*} x_1^*.$$

O terceiro vetor tem deve ser ortogonal a x_1^* e x_2^* simultaneamente, assim deve satisfazer

$$x_3^* \cdot x_2^* = 0$$
$$(\mathbf{x_3} - \gamma x_2^* - \eta x_1^*) \cdot x_1^* = 0$$
$$x_3^* \cdot x_1^* = 0$$
$$(\mathbf{x_3} - \gamma x_2^* - \eta x_1^*) \cdot x_2^* = 0$$

desse modo

$$x_3^* = \mathbf{x^3} - \gamma x_2^* - \eta x_1^*$$

resolvendo as equações temos

$$\gamma = \frac{\mathbf{x_3} \cdot x_2^*}{x_2^* \cdot x_2^*}$$
$$\eta = \frac{\mathbf{x_3} \cdot x_1^*}{x_1^* \cdot x_1^*}$$

portanto o terceiro vetor é calculado por

$$x_3^* = \mathbf{x^3} - \frac{\mathbf{x_3} \cdot x_2^*}{x_2^* \cdot x_2^*} x_2^* - \frac{\mathbf{x_3} \cdot x_1^*}{x_1^* \cdot x_1^*} x_1^*.$$

Repetindo esse processo de maneira sucessiva conseguimos encontra todos o vetores ortogonais $x_1^*, x_2^*, ..., x_n^*$. Estabelecemos então a seguinte definição,

Definição 5. *Seja* $\mathbf{x_1}, ..., \mathbf{x_n}$ *uma base do* $\mathbb{R}^n$. *A* **ortogonalização de Gram-Schmidt (OGS)** *de* $\mathbf{x_1}, ..., \mathbf{x_n}$ *é a base* $x_1^*, ..., x_n^*$ *dada por:*

$$x_1^* = \mathbf{x_1},$$

$$x_i^* = \mathbf{x_i} - \sum_{j=1}^{i-1} \mu_{ij} x_j^*, \quad \mu_{ij} = \frac{\mathbf{x_i} \cdot x_j^*}{x_j^* \cdot x_j^*} \quad (1 \leq j < i \leq n),$$

onde os μ_{ij} *serão chamados de* **coeficientes da OGS** .

Observe que não estamos exigindo a normalização do vetores. Escrevendo $x_i^* = (x_{i1}, ..., x_{in})$ definimos a matriz $X^* = (x_{ij}^*)$, onde suas linhas são os vetores da OGS, de maneira similar temos $X = (\mathbf{x}_{ij})$. Vejamos então alguns exemplos

Exemplo 2. *Sejam os vetores* $\mathbf{x_1} = (6, 9, -5)$, $\mathbf{x_2} = (4, -2, 4)$, $\mathbf{x_3} = (2, 8, 4)$ *geradores do espaço* $\mathbb{R}^3$, *vamos aplicar o processo de ortogonalização de Gram-Schmidt para obter uma base ortogonal do* $\mathbb{R}^3$. *Primeiramente definimos*

$$x_1^* = \mathbf{x_1} = (6, 9, -5)$$

agora temos que,

$$x_2^* = \mathbf{x_2} - \mu_{21} x_1^*$$

calculando o coeficiente μ_{21} *temos*

$$\mu_{21} = \frac{\mathbf{x_2} \cdot x_1^*}{x_1^* \cdot x_1^*} = \frac{(4,-2,4)\cdot(6,9,-5)}{(6,9,-5)\cdot(6,9,-5)} = -\frac{7}{71}$$

segue então que

$$x_2^* = (4,-2,4) + \frac{7}{71}(6,9,-5)$$

$$x_2^* = \left(\frac{326}{71}, -\frac{79}{71}, \frac{249}{71}\right).$$

Agora vamos encontrar x_3^**, temos*

$$x_3^* = \mathbf{x_3} - \mu_{31} x_1^* - \mu_{32} x_2^*$$

calculando os coeficientes

$$\mu_{31} = \frac{\mathbf{x_3} \cdot x_1^*}{x_1^* \cdot x_1^*} = \frac{(2,8,4)\cdot(6,9,-5)}{(6,9,-5)\cdot(6,9,-5)} = \frac{32}{71}$$

$$\mu_{32} = \frac{\mathbf{x_3} \cdot x_2^*}{x_2^* \cdot x_2^*} = \frac{(2,8,4)\cdot\left(\frac{326}{71}, -\frac{79}{71}, \frac{249}{71}\right)}{\left(\frac{326}{71}, -\frac{79}{71}, \frac{249}{71}\right)\cdot\left(\frac{326}{71}, -\frac{79}{71}, \frac{249}{71}\right)} = \frac{508}{1229}$$

dai,

$$x_3^* = (2,8,4) - \frac{32}{71}(6,9,-5) - \frac{508}{1229}\left(\frac{326}{71}, -\frac{79}{71}, \frac{249}{71}\right)$$

$$x_3^* = \left(-\frac{3198}{1229}, \frac{5412}{1229}, \frac{5904}{1229}\right)$$

portanto a nova base ortogonal é

$$x_1^* = (6,9,-5) \quad x_2^* = \left(\frac{326}{71}, -\frac{79}{71}, \frac{249}{71}\right) \quad x_3^* = \left(-\frac{3198}{1229}, \frac{5412}{1229}, \frac{5904}{1229}\right).$$

Exemplo 3. *Agora vamos aplicar o processo de ortogonalização de Gram-Schmidt para obter uma base ortogonal do espaço* $\mathbb{R}^4$ *com os vetores* $\mathbf{x_1} = (-1,5,7,2)$*,* $\mathbf{x_2} = (4,0,-3,8)$*,* $\mathbf{x_3} = (2,-8,0,1)$ *e* $\mathbf{x_4} = (9,-8,0,1)$*. Primeiramente, definimos:*

$$x_1^* = x_1 = (-1,5,7,2)$$

Agora, para x_2^*, temos:

$$x_2^* = x_2 - \mu_{21} x_1^*$$

Calculando o coeficiente μ_{21}:

$$\mu_{21} = \frac{x_2 \cdot x_1^*}{x_1^* \cdot x_1^*} = \frac{(4,0,-3,8)\cdot(-1,5,7,2)}{(-1,5,7,2)\cdot(-1,5,7,2)} = -\frac{9}{79}$$

Agora, substituímos x_1^* e μ_{21} para encontrar x_2^*:

$$x_2^* = (4,0,-3,8) + \frac{9}{79}(-1,5,7,2) = \left(\frac{307}{79}, \frac{45}{79}, -\frac{174}{79}, \frac{650}{79}\right)$$

Para x_3^*, temos:

$$x_3^* = x_3 - \mu_{31} x_1^* - \mu_{32} x_2^*$$

Calculando os coeficientes μ_{31} e μ_{32}:

$$\mu_{31} = \frac{x_3 \cdot x_1^*}{x_1^* \cdot x_1^*} = \frac{(2,-8,0,1)\cdot(-1,5,7,2)}{(-1,5,7,2)\cdot(-1,5,7,2)} = -\frac{40}{79}$$

$$\mu_{32} = \frac{x_3 \cdot x_2^*}{x_2^* \cdot x_2^*} = \frac{(2,-8,0,1)\cdot\left(\frac{307}{79}, \frac{45}{79}, -\frac{174}{79}, \frac{650}{79}\right)}{\left(\frac{307}{79}, \frac{45}{79}, -\frac{174}{79}, \frac{650}{79}\right)\cdot\left(\frac{307}{79}, \frac{45}{79}, -\frac{174}{79}, \frac{650}{79}\right)} = \frac{452}{3475}$$

Agora, substituímos x_1^*, x_2^*, μ_{31} e μ_{32} para encontrar x_3^*:

$$x_3^* = (2,-8,0,1) - \left(-\frac{40}{79}\right)(-1,5,7,2) - \frac{452}{3475}\left(\frac{307}{79}, \frac{45}{79}, -\frac{174}{79}, \frac{650}{79}\right)$$

$$x_3^* = \left(\frac{3434}{3475}, -\frac{3852}{695}, \frac{13312}{3475}, \frac{131}{139}\right)$$

Finalmente, para x_4^*, temos:

$$x_4^* = x_4 - \mu_{41} x_1^* - \mu_{42} x_2^* - \mu_{43} x_3^*$$

Calculando os coeficientes μ_{41}, μ_{42} e μ_{43}:

$$\mu_{41} = \frac{x_4 \cdot x_1^*}{x_1^* \cdot x_1^*} = \frac{(9,-8,0,1)\cdot(-1,5,7,2)}{(-1,5,7,2)\cdot(-1,5,7,2)} = -\frac{47}{79}$$

$$\mu_{42} = \frac{x_4 \cdot x_2^*}{x_2^* \cdot x_2^*} = \frac{(9,-8,0,1) \cdot \left(\frac{307}{79}, \frac{45}{79}, -\frac{174}{79}, \frac{650}{79}\right)}{\left(\frac{307}{79}, \frac{45}{79}, -\frac{174}{79}, \frac{650}{79}\right) \cdot \left(\frac{307}{79}, \frac{45}{79}, -\frac{174}{79}, \frac{650}{79}\right)} = \frac{3053}{6950}$$

$$\mu_{43} = \frac{x_4 \cdot x_3^*}{x_3^* \cdot x_3^*} = \frac{(9,-8,0,1) \cdot \left(\frac{3434}{3475}, -\frac{3852}{695}, \frac{13312}{3475}, \frac{131}{139}\right)}{\left(\frac{3434}{3475}, -\frac{3852}{695}, \frac{13312}{3475}, \frac{131}{139}\right) \cdot \left(\frac{3434}{3475}, -\frac{3852}{695}, \frac{13312}{3475}, \frac{131}{139}\right)}$$

$$\mu_{43} = \frac{188261}{164223}$$

Agora, substituímos x_1^*, x_2^*, x_3^*, μ_{41}, μ_{42} *e* μ_{43} *para encontrar* x_4^**:*

$$x_4^* = (9,-8,0,1) + \frac{47}{79}(-1,5,7,2) - \frac{3053}{6950}\left(\frac{307}{79}, \frac{45}{79}, -\frac{174}{79}, \frac{650}{79}\right) =$$

$$\frac{188261}{164223}\left(\frac{3434}{3475}, -\frac{3852}{695}, \frac{13312}{3475}, \frac{131}{139}\right)$$

$$x_4^* = \left(\frac{662812007}{109261850}, -\frac{1064929681}{218523700}, \frac{3323071291}{109261850}, -\frac{5114081}{109261850}\right)$$

Portanto, a nova base ortogonal é:

$$x_1^* = (-1,5,7,2)$$

$$x_2^* = \left(\frac{307}{79}, \frac{45}{79}, -\frac{174}{79}, \frac{650}{79}\right)$$

$$x_3^* = \left(\frac{3434}{3475}, -\frac{3852}{695}, \frac{13312}{3475}, \frac{131}{139}\right)$$

$$x_4^* = \left(\frac{2154810}{2053177}, -\frac{302180}{2053177}, \frac{2698045}{2053177}, -\frac{65655}{2053177}\right).$$

Definição 6. *Sejam os coeficientes da ortogonalização de Gram-Schmidt* (μ_{ij})*, definimos* M *como a matriz triangular inferior:*

$$M = \begin{bmatrix} 1 & 0 & \dots & 0 \\ \mu_{21} & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \mu_{n1} & \mu_{n2} & \dots & 1 \end{bmatrix}.$$

É fácil ver que se todos os coeficientes da OGS são nulos então vale

$$X = MX^*.$$

A OGS traz diversas propriedades, dentre elas temos o seguinte teorema

Teorema 4 (Teorema de Gram-Shmidt)**.** *Seja* $\mathbf{x_1}, \mathbf{x_2}, ..., \mathbf{x_n}$ *uma base do* $\mathbb{R}^n$ *e seja* $x_1^*, x_2^*, ..., x_n^*$ *sua ortogonalização de Gram-Shmidt. Seja* X *(respectivamente* X^**) uma matriz* $n \times n$ *em que suas* i *linhas são os vetores* $\mathbf{x_i}$ *(respectivamente* x_i^**) para* $1 \leq i \leq n$*. Então,*

(i) $x_i^* \cdot x_j^* = 0$ *para* $1 \leq i < j \leq n$*.*

(ii) O espaço gerado por $(x_1^*, x_2^*, ..., x_k^*)$ *é igual ao espaço gerado por* $(\mathbf{x_1}, \mathbf{x_2}, ..., \mathbf{x_k})$ *para* $1 \leq k \leq n$*.*

(iii) O vetor x_k^* *é a projeção de* $\mathbf{x_k}$ *no complemento ortogonal de espaço gerado por* $(\mathbf{x_1}, \mathbf{x_2}, ..., \mathbf{x_{k-1}})$ *para* $1 \leq k \leq n$*.*

(iv) $|x_k^*| \leq |\mathbf{x_k}|$ *para* $1 \leq k \leq n$*.*

(v) $\det(X^*) = \det(X)$*.*

Demonstração. (i) Vamos aplicar indução em j. Para $j = 1$, não há nada a provar. Suponha que a afirmação seja verdadeira para algum $j \geq 1$. Para $1 \leq i < j + 1$ temos por definição

$$x_i^* \cdot x_{j+1}^* = x_i^* \cdot \left(\mathbf{x_{j+1}} - \sum_{k=1}^{j} \mu_{j+1,k} x_k^* \right)$$

usando a bilinearidade do produto escalar

$$= x_i^* \cdot \mathbf{x_{j+1}} - \sum_{k=1}^{j} \mu_{j+1,k} x_i^* \cdot x_k^*$$

pela hipótese de indução

$$= x_i^* \cdot \mathbf{x_{j+1}} - \mu_{j+1,i}(x_i^* \cdot x_i^*)$$

$$= x_i^* \cdot \mathbf{x_{j+1}} - \frac{\mathbf{x_{j+1}} \cdot x_i^*}{x_i^* \cdot x_i^*}(x_i^* \cdot x_i^*) = 0.$$

Portanto, $x_i^* \cdot x_j^* = 0$ para $1 \leq i < j \leq n$.
(ii) Se $\mu_{ii} = 1$ temos que $\mathbf{x_i}$ pertence ao espaço gerado por $(x_1^*, \ldots, x_k^*)$ para $1 \leq i \leq k$, e, portanto,

$$\text{span}(\mathbf{x_1}, \ldots, \mathbf{x_k}) \subseteq \text{span}(x_1^*, \ldots, x_k^*).$$

Para a inclusão reversa, usamos indução em k. Para $k = 1$ temos $x_1^* = \mathbf{x_1}$ e, portanto, a afirmação é óbvia. Suponha que a afirmação seja verdadeira para algum $k \geq 1$. Usando a Definição 5, obtemos

$$x_{k+1}^* = \mathbf{x_{k+1}} - \sum_{j=1}^{k} \mu_{k+1,j} x_j^* = \mathbf{x_{k+1}} + y, \quad y \in \text{span}(x_1^*, \ldots, x_k^*).$$

A hipótese de indução dá $\text{span}(x_1^*, \ldots, x_k^*) \subseteq \text{span}(\mathbf{x_1}, \ldots, \mathbf{x_k})$, e assim a última equação implica $x_{k+1}^* \in \text{span}(\mathbf{x_1}, \ldots, \mathbf{x_{k+1}})$. Portanto,

$$\text{span}(x_1^*, \ldots, x_{k+1}^*) \subseteq \text{span}(\mathbf{x_1}, \ldots, \mathbf{x_{k+1}}).$$

(iii) Para simplificar a notação, escrevemos $U = \text{span}(x_1, \ldots, x_{k-1})$; então $U^\perp$ é o subespaço de $\mathbb{R}^n$ consistindo de todos os vetores y tais que $y \cdot x = 0$ para todo vetor $x \in U$. Existe uma decomposição única $\mathbf{x_k} = x_k' + y$ onde $x_k' \in U^\perp$ e $y \in U$; aqui, x_k' é a projeção de $\mathbf{x_k}$ sobre o complemento ortogonal de U. Assim, sendo $\mu_{ii} = 1$ temos

$$\mathbf{x_k} = x_k^* + \sum_{j=1}^{k-1} \mu_{kj} x_j^*.$$

Pela parte (b), temos $U = \text{span}(x_1^*, \ldots, x_{k-1}^*)$, e portanto $x_k^* = x_k'$.

(iv) Usando a parte (a), vemos que

$$\mathbf{x_k} = x_k^* + \sum_{j=1}^{k-1} \mu_{kj} x_j^*$$

implica

$$|\mathbf{x_k}|^2 = |x_k^*|^2 + \sum_{j=1}^{k-1} \mu_{kj}^2 |x_j^*|^2.$$

Como cada termo na soma é não-negativo, isso prova a afirmação.

(v) Da definição 6, $X = MX^*$, onde $M = (\mu_{ij})$ é uma matriz triangular inferior com $\mu_{ii} = 1$ para $1 \leq i \leq n$. Logo, $\det(M) = 1$, e portanto

$$\det(X) = \det(M) \det(X^*) = \det(X^*).$$

□

Com o processo de ortogonalização de Gram-Schmidt em mãos estamos prontos para o tópico especial.

1.4 Redução de base LLL

Neste capitulo mostraremos como reduzir a base de um reticulado de maneira a conseguir uma base mais curta e próxima da ortogonalidade.

Da definição 4 lembramos que um reticulado $\mathbb{L}$ de dimensão n é um conjunto formado por todas as combinações lineares de vetores $\mathbf{x_1}, \mathbf{x_2}, ..., \mathbf{x_n} \in \mathbb{R}^n$, e estes por sua vez são chamados de base do reticulado. Além disso, a forma matricial para o reticulado é dada pela matriz X cujas linhas são os vetores $\mathbf{x_1}, \mathbf{x_2}, ..., \mathbf{x_n}$,

$$X = \begin{bmatrix} x_{11} & x_{12} & \dots & x_{1n} \\ x_{21} & x_{22} & \dots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n1} & x_{n2} & \dots & x_{nn} \end{bmatrix}.$$

O objetivo é, dado um reticulado $\mathbb{L}$, como podemos reduzir sua base de tal maneira que ela seja mais curta e próxima da ortogonalidade?, bem primeiramente vejamos algumas definições e teoremas.

Definição 7. *Uma* **operação unimodular de linhas** *em uma matriz é uma das seguintes operações elementares*

- *Multiplicar qualquer linha por* -1.
- *Permuta quaisquer duas linhas.*
- *Soma um múltiplo inteiro de uma linha a qualquer outra linha.*

Definição 8 (Redução LLL)**.** *O parâmetro de redução, denotado por* α*, é um número real tal que* $1/4 < \alpha < 1$*. O valor padrão para este parâmetro é* $\alpha = 3/4$*.*

Sejam $x_1, x_2, \dots, x_n$ *uma base ordenada do reticulado* $\mathbb{L}$ *em* $\mathbb{R}^n$*, e* $x_1^*, x_2^*, \dots, x_n^*$ *a sua ortogonalização de Gram-Schmidt. A base* $x_1, x_2, \dots, x_n$ *é considerada* α*-reduzida* **(ou LLL-reduzida com parâmetro** α**)** *se satisfizer as seguintes condições:*

1. $|\mu_{ij}| \leq \frac{1}{2}$ *para* $1 \leq j < i \leq n$,
2. $|x_i^* + \mu_{i,i-1} x_{i-1}^*|^2 \geq \alpha |x_{i-1}^*|^2$ *para* $2 \leq i \leq n$.

A condição (1) afirma que cada vetor de base x_i é "quase ortogonal"ao espaço gerado pelos vetores anteriores, já que, pelo Teorema 0.4, temos $\text{span}(x_1, \dots, x_{i-1}) = \text{span}(x_1^*, \dots, x_{i-1}^*)$.

A condição (2) indica que a troca entre x_{i-1} e x_i, seguida pelo recálculo do GSO, pode gerar um novo vetor mais curto $\bar{\mathbf{x}}_i^* = \mathbf{x}_i^* + \mu_{i,i-1}\mathbf{x}_{i-1}^*$, mas não consideravelmente mais curto.

A condição (2) é conhecida como condição de troca. Observe que

$$|x_i^* + \mu_{i,i-1}x_{i-1}^*|^2 \geq \alpha|x_{i-1}^*|^2 \Rightarrow \left(|x_i^*| + \mu_{i,i-1}|x_{i-1}^*|\right)^2 \geq \alpha|x_{i-1}^*|^2$$

$$\Rightarrow |x_i^*|^2 + 2\mu_{i,i-1}|x_{i-1}^*||x_i^*| + (\mu_{i,i-1})^2|x_{i-1}^*|^2 \geq \alpha|x_{i-1}^*|^2$$

Dado que $x_1^*, x_2^*, \ldots, x_n^*$ são ortogonais, podemos reescreve-la como:

$$|x_i^*|^2 + (\mu_{i,i-1})^2|x_{i-1}^*|^2 \geq \alpha|x_{i-1}^*|^2$$

$$|x_i^*|^2 \geq (\alpha - \mu_{i,i-1}^2)|x_{i-1}^*|^2 \quad \text{para } 2 \leq i \leq n.$$

Definição 9. *Definimos o parâmetro auxiliar β da seguinte forma:*

$$\beta = \frac{4}{4\alpha - 1}$$

de modo que $\beta > \frac{4}{3}$ e $\frac{1}{\beta} = \alpha - \frac{1}{4}$. Para o valor padrão $\alpha = \frac{3}{4}$, obtemos $\beta = 2$.

Proposição 5. *Se $x_1, x_2, \ldots, x_n$ formam uma base α-reduzida da reticulado $\mathbb{L}$ em $\mathbb{R}^n$, e $x_1^*, x_2^*, \ldots, x_n^*$ é a sua ortogonalização de Gram-Schmidt, então:*

(a) $|x_j|^2 \leq \beta^{i-j}|x_i^*|^2$ *para* $1 \leq j \leq i \leq n$,

(b) $\det(\mathbb{L}) \leq |x_1||x_2|\ldots|x_n| \leq \beta^{\frac{n(n-1)}{4}} \det(\mathbb{L})$,

(c) $|x_1| \leq \beta^{\frac{n-1}{4}}(\det(\mathbb{L}))^{1/n}$,

onde β e o parâmetro auxiliar definido anteriormente.

Demonstração. As condições 1 e 2 para uma α -redução implicam que, para $1 < i \leq n$ tenhamos

$$|x_i^*|^2 \geq (\alpha - \mu_{i,i-1}^2)|x_{i-1}^*|^2 \geq (\alpha - \frac{1}{4})|x_{i-1}^*|^2 = \frac{1}{\beta}|x_{i-1}^*|^2.$$

Logo $|x_{i-1}^*|^2 < \beta|x_i^*|^2$, e por indução conseguimos

$$|x_{i-1}^*|^2 < \beta^{i-j}|x_i^*|^2 \quad (1 \leq j \leq i \leq n). \tag{1.2}$$

Tomando a definição dos vetores da OGS

$$x_i = x_i^* + \sum_{j=1}^{i-1} \mu_{ij}x_j^*,$$

e sendo estes ortogonais temos

$$|x_i|^2 = |x_i^*|^2 + \sum_{j=1}^{i-1} \mu_{ij}^2 |x_i^*|^2.$$

considerando a definição 8 junto a desigualdade (2) temos,

$$|x_i|^2 \leq |x_i^*|^2 + \sum_{j=1}^{i-1} \frac{1}{4}\beta^{i-j}|x_i^*|^2 = \left(1 + \frac{1}{4}\sum_{j=1}^{i-1}\frac{1}{4}\beta^{i-j}\right)|x_i^*|^2$$

usando a formula para soma de sequencia geométrica no obtemos,

$$|x_i|^2 \leq \left(1 + \frac{1}{4}\cdot\frac{\beta^i - \beta}{\beta - 1}\right)|x_i^*|^2$$

aplicando indução chegamos a

$$1 + \frac{1}{4}\cdot\frac{\beta^i - \beta}{\beta - 1} \leq \beta^{i-1}.$$

O caso $i = 1$ é trivial. Para os outros casos é suficiente mostrar que

$$1 + \frac{1}{4}\cdot\frac{\beta^i - \beta}{\beta - 1} \leq \beta\left(1 + \frac{\beta^i - \beta}{4(\beta - 1)}\right).$$

Uma vez que $\beta > 4/3$, multiplicando por $4(\beta-1)$ temos uma inequação equivalente, simplificando então

$$(\beta - 1)(3\beta - 4) \geq 0,$$

o que é obvio uma vez que $\beta > 4/3$. Temos agora que

$$|x_i|^2 \leq \beta^{i-1}|x_i^*|^2.$$

usando (2)

$$|x_j|^2 \leq \beta^{j-1}|x_j^*|^2 \leq \beta^{i-1}|x_i^*|^2 \quad 1 \leq j \leq i \leq n$$

o que demonstra a afirmação (a). Do teorema de Gram-Schmidt nos sabemos que

$$\det(\mathbb{L}) = |\mathbf{x}_1^*||\mathbf{x}_2^*|\cdots|\mathbf{x}_n^*| \leq |\mathbf{x}_1||\mathbf{x}_2|\cdots|\mathbf{x}_n|,$$

o que prova o lado esquerdo da desigualdade em (b), de $|x_i|^2 \leq \beta^{i-1}|x_i^*|^2$ temos

$$|\mathbf{x}_1|^2|\mathbf{x}_2|^2\cdots|\mathbf{x}_n|^2 \leq \beta^{0+1+2+\ldots+(n-1)}|\mathbf{x}_1^*|^2|\mathbf{x}_2^*|^2\cdots|\mathbf{x}_n^*|^2,$$

e portanto

$$|\mathbf{x}_1||\mathbf{x}_2|\cdots|\mathbf{x}_n| \leq \beta^{n(n-1)/4}|\mathbf{x}_1^*||\mathbf{x}_2^*|\cdots|\mathbf{x}_n^*| = \beta^{n(n-1)/4}\det(\mathbb{L}),$$

o que mostra a desigualdade da direita em (b). Colocando $j = 1$ em (a) temos

$$|x_1|^2 \leq \beta^{i-1}|x_i^*|^2 \quad (1 \leq i \leq n),$$

e aplicando o produto sobre $i = 1, 2, ..., n$ temos

$$|\mathbf{x}_1|^{2n} \leq \beta^{0+1+2+...+(n-1)}|\mathbf{x}_1^*|^2|\mathbf{x}_2^*|^2\cdots|\mathbf{x}_n^*|^2 = \beta^{n(n-1)/2}\det(\mathbb{L})^2,$$

aplicando agora para a $2n - ezima$ raiz provamos (c). □

Proposição 6. *Sejam $x_1, x_2, \ldots, x_n$ uma base de $\mathbb{R}^n$ e $x_1^*, x_2^*, \ldots, x_n^*$ sua ortogonalização de Gram-Schmidt. Seja $\mathbb{L}$ o reticulado gerado por $x_1, x_2, \ldots, x_n$. Para qualquer vetor não nulo $y \in \mathbb{L}$, temos*

$$|y| \geq \min\{|x_1^*|, |x_2^*|, \ldots, |x_n^*|\}.$$

Isso é, qualquer vetor não nulo do reticulado é pelo menos tão longo quanto o vetor mais curto na ortogonalização de Gram-Schmidt.

Demonstração. Seja y qualquer elemento não nulo de $\mathbb{L}$:

$$y = \sum_{i=1}^{n} r_i x_i,$$

onde $r_i \in \mathbb{Z}$ para $1 \leq i \leq n$. Como $y \neq 0$, temos $r_i \neq 0$ para algum i; seja k o maior índice tal que $r_k \neq 0$. Usando a Definição 5, podemos expressar $x_1, x_2, \ldots, x_n$ em termos de $x_1^*, x_2^*, \ldots, x_n^*$:

$$y = \sum_{i=1}^{k} r_i \sum_{j=1}^{n} \mu_{ij} x_j^* = \sum_{i=1}^{k}\sum_{j=1}^{n} r_i \mu_{ij} x_j^*.$$

Invertendo a ordem da soma, e usando $\mu_{kk} = 1$, obtemos

$$y = \sum_{j=1}^{k} \left(\sum_{i=j}^{k} r_i \mu_{ij} \right) x_j^* = r_k x_k^* + \sum_{j=1}^{k-1} \nu_j x_j^*,$$

para alguns $\nu_1, \ldots, \nu_{k-1} \in \mathbb{R}$. Como $x_1^*, x_2^*, \ldots, x_n^*$ são ortogonais, obtemos

$$|y|^2 = r_k^2|x_k^*|^2 + \sum_{j=1}^{k-1} \nu_j^2 |x_j^*|^2.$$

Como r_k é um inteiro não nulo, temos $r_k^2 \geq 1$, e então

$$|y|^2 \geq |x_k^*|^2 + \sum_{j=1}^{k-1} \nu_j^2 |x_j^*|^2.$$

Todos os termos na soma são não negativos, e portanto

$$|y|^2 \geq |x_k^*|^2 \geq \min\{|x_1^*|^2, \ldots, |x_n^*|^2\}.$$

Tomando a raiz quadrada completamos a prova. □

Teorema 7 (Teorema LLL)**.** *Se $x_1, x_2, ..., x_n$ é uma α-redução de base de um reticulado $\mathbb{L} \subseteq \mathbb{R}^n$ e $\mathbf{y} \in \mathbb{L}$ qualquer vetor não nulo, então*

$$|x_1| \leq \beta^{(n-1)/2} |\mathbf{y}|.$$

Em particular, o primeiro vetor da α-redução de base não é maior que $\beta^{(n-1)/2}$ vezes o menor vetor não nulo de $\mathbb{L}$.

Demonstração. Sejam $x_1^*, x_2^*, \ldots, x_n^*$ a ortogonalização de Gram-Schmidt de $x_1, x_2, \ldots, x_n \in \mathbb{L}$. Pela definição de uma base α-reduzida, para $2 \leq i \leq n$ temos

$$|x_i^*|^2 \geq (\alpha - \mu_{i,i-1}^2)|x_{i-1}^*|^2 \geq (\alpha - 1/4)|x_{i-1}^*|^2 = \frac{1}{\beta}|x_{i-1}^*|^2.$$

Uma vez que $x_1^* = x_1$, isso resulta em

$$|x_1|^2 = |x_1^*|^2 \leq \beta |x_2^*|^2 \leq \beta^2 |x_3^*|^2 \leq \cdots \leq \beta^{n-1} |x_n^*|^2,$$

e, portanto, para $1 \leq i \leq n$ temos

$$|x_i^*|^2 \geq \beta^{-(i-1)} |x_1|^2.$$

A Proposição 6 agora mostra que para qualquer vetor não nulo $y \in \mathbb{L}$ temos

$$|y| \geq \min\{|x_1^*|, \ldots, |x_n^*|\} \geq \beta^{-(n-1)/2} |x_1|,$$

e isso completa a prova. □

Vejamos agora como funciona na prática

Exemplo 4. *Considere um reticulado $\mathbb{L}$ de dimensão 3 gerado pelos vetores $\mathbf{x_1} = (4, 5, 1)$, $\mathbf{x_2} = (4, 8, 2)$ e $\mathbf{x_3} = (6, 2, 6)$. A matriz base desse reticulado, os coeficientes e o quadrado do modulo dos vetores da OGS será denotado respectivamente pelas matrizes X, (μ_{ij}) e $(|x_i^*|^2)$. Assim para o reticulado $\mathbb{L}$ temos:*

$$X = \begin{bmatrix} 4 & 5 & 1 \\ 4 & 8 & 2 \\ 6 & 2 & 6 \end{bmatrix}, \quad (\mu_{ij}) = \begin{bmatrix} 1 & 0 & 0 \\ 29/21 & 1 & 0 \\ 20/21 & -34/41 & 1 \end{bmatrix}, \quad (|x_i^*|^2) = \begin{bmatrix} 42 \\ 82/21 \\ 1444/41 \end{bmatrix}.$$

Consideremos o parâmetro de redução $\alpha = 3/4$. Nosso objetivo é reduzir a base do reticulado de maneira a satisfazer as condições (1) e (2) da Definição 8. Vamos reduzir os coeficientes da OGS dá direita para a esquerda linha por linha, veja que $|\mu_{21}| = 29/21 > 1/2$, tomamos $\lceil \mu_{21} \rfloor = 1$ então fazemos $x_2 = x_2 - 1 \cdot x_1$, dai

$$X_1 = \begin{bmatrix} 4 & 5 & 1 \\ 0 & 3 & 1 \\ 6 & 2 & 6 \end{bmatrix}, \quad (\mu_{ij}) = \begin{bmatrix} 1 & 0 & 0 \\ 8/21 & 1 & 0 \\ 20/21 & -34/41 & 1 \end{bmatrix}, \quad (|x_i^*|^2) = \begin{bmatrix} 42 \\ 82/21 \\ 1444/41 \end{bmatrix}$$

observe que agora temos $|\mu_{21}| = 8/21 < 1/2$, testamos agora a condição de troca para o parâmetro padrão $\alpha = 3/4$,

$$\frac{82}{21} \geq \left(\frac{3}{4} - \frac{64}{441}\right) \cdot 42 \Rightarrow \frac{82}{21} \geq \frac{1067}{42}.\textit{(Falso)}$$

devemos então permutar então as linhas 2 e 1, dai

$$X_2 = \begin{bmatrix} 0 & 3 & 1 \\ 4 & 5 & 1 \\ 6 & 2 & 6 \end{bmatrix}, \quad (\mu_{ij}) = \begin{bmatrix} 1 & 0 & 0 \\ 8/5 & 1 & 0 \\ 20/21 & -34/41 & 1 \end{bmatrix}, \quad (|x_i^*|^2) = \begin{bmatrix} 10 \\ 82/21 \\ 1444/41 \end{bmatrix}$$

veja que $|\mu_{21}| = 8/5 > 1/2$. Observe que $|\mu_{21}| = 8/5 > 1/2$, tomamos $\lceil \mu_{21} \rfloor = 2$ então fazemos $x_2 = x_2 - 2 \cdot x_1$, dai

$$X_3 = \begin{bmatrix} 0 & 3 & 1 \\ 4 & -1 & -1 \\ 6 & 2 & 6 \end{bmatrix}, \quad (\mu_{ij}) = \begin{bmatrix} 1 & 0 & 0 \\ -2/5 & 1 & 0 \\ 6/5 & 52/41 & 1 \end{bmatrix}, \quad (|x_i^*|^2) = \begin{bmatrix} 10 \\ 82/5 \\ 1444/41 \end{bmatrix}$$

testamos agora a condição de troca

$$\frac{82}{5} \geq \left(\frac{3}{4} - \frac{4}{25}\right) \cdot 10 \Rightarrow \frac{82}{5} \geq \frac{59}{10}.\textit{(Verdadeiro)}$$

Seguimos o processo agora para μ_{32}, observe que $|\mu_{32}| = 52/41 > 1/2$ tomamos $\lceil \mu_{32} \rfloor = 1$ então fazemos $x_3 = x_3 - 1 \cdot x_2$, dai

$$X_4 = \begin{bmatrix} 0 & 3 & 1 \\ 4 & -1 & -1 \\ 2 & 3 & 7 \end{bmatrix}, \quad (\mu_{ij}) = \begin{bmatrix} 1 & 0 & 0 \\ -2/5 & 1 & 0 \\ 8/5 & 11/41 & 1 \end{bmatrix}, \quad (|x_i^*|^2) = \begin{bmatrix} 10 \\ 82/5 \\ 1444/41 \end{bmatrix}$$

temos então $|\mu_{32}| = 11/41 < 1/2$. testamos agora a condição de troca para o parâmetro padrão $\alpha = 3/4$,

$$\frac{1444}{41} \geq \left(\frac{3}{4} - \frac{121}{1681}\right) \cdot \frac{82}{5} \Rightarrow \frac{1444}{41} \geq \frac{4559}{410}.\textit{(Verdadeiro)}$$

seguimos o processo para μ_{31}, *observe* $|\mu_{31}| = 8/5 > 1/2$, *então fazemos* $x_3 = x_3 - 2 \cdot x_1$, *dai*

$$X_5 = \begin{bmatrix} 0 & 3 & 1 \\ 4 & -1 & -1 \\ 2 & -3 & 5 \end{bmatrix}, \quad (\mu_{ij}) = \begin{bmatrix} 1 & 0 & 0 \\ -2/5 & 1 & 0 \\ -2/5 & 11/41 & 1 \end{bmatrix}, \quad (|x_i^*|^2) = \begin{bmatrix} 10 \\ 82/5 \\ 1444/41 \end{bmatrix}$$

temos então $|\mu_{32}| = 2/5 < 1/2$. *testamos agora a condição de troca para o parâmetro padrão* $\alpha = 3/4$,

$$\frac{1444}{41} \geq \left(\frac{3}{4} - \frac{121}{1681}\right) \cdot \frac{82}{5} \Rightarrow \frac{1444}{41} \geq \frac{4559}{410}.\textit{(Verdadeiro)}$$

$$X_5 = \begin{bmatrix} 0 & 3 & 1 \\ 4 & -1 & -1 \\ 2 & -3 & 5 \end{bmatrix}, \quad (\mu_{ij}) = \begin{bmatrix} 1 & 0 & 0 \\ -2/5 & 1 & 0 \\ -2/5 & 11/41 & 1 \end{bmatrix}, \quad (|x_i^*|^2) = \begin{bmatrix} 10 \\ 82/5 \\ 1444/41 \end{bmatrix}$$

logo, vemos que as condições

1. $|\mu_{ij}| \leq \dfrac{1}{2}$, *para* $1 \leq j < i \leq n$.

2. $|x_i^*|^2 \geq (\alpha - \mu_{i,i-1}^2)|x_{i-1}^*|^2$, *para* $2 \leq i \leq n$.

são satisfeitas, portanto a base $3/4$*-reduzida do reticulado é representada pela matriz* X_5. *Considerando agora a nova base* $3/4 - reduzida$ $x_1 = (0,3,1), x_2 = (4,-1,-1), x_3 = (2,-3,5)$ *e o parâmetro auxiliar* $\beta = 2$, *temos*

$$|(0,3,1)| \leq 2^{(3-1)/2}|\mathbf{y}| = 2|\mathbf{y}|$$
$$\sqrt{10} \leq 2|\mathbf{y}|$$

para qualquer vetor não nulo $\mathbf{y} \in L$. *O que de fato acontece pois considerando a nova base, qualquer vetor* $\mathbf{y}$ *é da forma* $\mathbf{y} = a(0,3,1) + b(4,-1,-1) + c(2,-3,5)$, *substituindo temos*

$$\sqrt{10} \leq 2|a(0,3,1) + b(4,-1,-1) + c(2,-3,5)|$$
$$\leq 2\left(|a(0,3,1)| + |b(4,-1,-1)| + |c(2,-3,5)|\right).$$

assim e fácil ver que

$$\sqrt{10} \leq 2\left(|a|\sqrt{10} + |b|\sqrt{18} + |c|\sqrt{38}\right) \quad \textit{para qualquer} \quad a,b,c \in \mathbb{Z}$$

exceto $a = b = c = 0$ *e portanto vale o teorema LLL. Além disso vamos testar a condição (c) da proposição 20. Do Exemplo 0.1.1 temos* $\det(\mathbb{L}) = 76$ *e sendo* β *como acima temos*

$$\sqrt{10} \leq 2^{1/2}(76)^{1/3} \Rightarrow \sqrt{10} \leq \sqrt{2} \cdot \sqrt[3]{76} \Rightarrow 3,16 \leq 5,99.$$

Observe que para o nosso exemplo usamos um total de 5 passo para encontra a base 3/4-reduzida, no entanto é perceptível naturalmente que dependendo da dimensão do reticulado e dos parâmetros escolhidos a quantidade de passos pode aumentar bastante, e nos deparamos com a pergunta: Existe um limite de passos?. Em vista disto temos o seguinte teorema,

Teorema 8. *O número total de passos no loop do algoritmo LLL é no máximo*

$$-\frac{2\log B}{\log \alpha}\cdot n(n-1)+(n-1),$$

onde $B \leq \sqrt{n\cdot\lambda^2}$, n *é a ordem da matriz e* λ *é tal que* $|x_{ij}| \leq \lambda$ *para* $1 \leq i,j \leq n$.

Demonstração. Devido a grande quantidade de lemas e teoremas necessários para a prova desse teorema, optamos por omitir sua demonstração, mas caso o leitor tenha interesse pode consultar Bremner [1, teorema 4.19].

□

Aplicando-o ao nosso exemplo anterior com parâmetro de redução $\alpha = 3/4$ o número máximo de passos é

$$-\frac{12\log\sqrt{3\cdot 9^2}}{\log\frac{3}{4}}+2=116.$$

Neste ponto, o leitor pode questionar por que escolhemos o valor $\alpha = 3/4$ como parâmetro de redução em vez de outro valor, considerando que esse parâmetro pode variar dentro do intervalo $0 < \alpha < 1$. É importante observar que no limite superior do parâmetro, o teorema 8 indica que seria necessário um número infinito de passos para realizar a redução, o que não é viável, apesar deste garantir a melhor redução. Por outro lado, no limite inferior do parâmetro, apenas alguns poucos passos seriam necessários, mas a redução resultante seria "fraca". Portanto, o valor de 3/4 é aquele com o qual alcançamos o resultado mais significativo e viável para a redução, e é por isso que o utilizaremos em todas as reduções futuras.

Vejamos mais um exemplo de redução, no entanto dessa vez, devido a dimensão do reticulado usaremos o software Magma para calcular essa redução. No capitulo 2 especificaremos com detalhes os comandos utilizados para essa aplicação do LLL via software Magma.

Exemplo 5. *Consideremos o reticulado*$\mathbb{L}$*de dimensão 8 gerado pela matriz*

$$X = \begin{bmatrix} 8 & -3 & -3 & -9 & 1 & 9 & -3 & -9 \\ -7 & 5 & 1 & 1 & 9 & -3 & -4 & -2 \\ -5 & 2 & 1 & -3 & -4 & 5 & 5 & 4 \\ -4 & 9 & -6 & -5 & -7 & 2 & -1 & 5 \\ -5 & 0 & 2 & 2 & 0 & 5 & 6 & -5 \\ -8 & -2 & 3 & 5 & -1 & 7 & 7 & 4 \\ 3 & -9 & 3 & -7 & 3 & 2 & -3 & 2 \\ -4 & -2 & -8 & 6 & 0 & 4 & -9 & 7 \end{bmatrix} \quad \det(X) = -1067148$$

aplicando a redução LLL conseguimos, com parâmetro $\alpha = 3/4$*, a seguinte base* $3/4$*-reduzida:*

$$C = \begin{bmatrix} 2 & -1 & -2 & 4 & 1 & -1 & -3 & -1 \\ -3 & 1 & -1 & 1 & -3 & 4 & 2 & 3 \\ -3 & 4 & 0 & -3 & 1 & -3 & 0 & 0 \\ -3 & -1 & 0 & 2 & -1 & -4 & -1 & -2 \\ 0 & -3 & 1 & 0 & 1 & 1 & -4 & -3 \\ 1 & 4 & 3 & 2 & 3 & -2 & 0 & 1 \\ -1 & -4 & 0 & 0 & 5 & 1 & 1 & -2 \\ -4 & -3 & -1 & -3 & 0 & -3 & -1 & 5 \end{bmatrix} \quad \det(C) = 1067148.$$

O número de passos feito pelo algoritmo é no máximo

$$-\frac{112 \log \sqrt{8 \cdot 9^2}}{\log \frac{3}{4}} + 7 = 1267.$$

Afim de obter um limite inferior para o comprimento dos vetores diferentes de zero de um reticulado Γ considere a seguinte definição:

Definição 10. *Seja* Γ *um reticulado de dimensão* n *e* $|\cdot|$ *a norma euclidiana no* $\mathbb{R}^n$*. Definimos*

$$l(\Gamma) = \min_{0 \neq x \in \Gamma} |x|.$$

Em palavras, $l(\Gamma)$ *é a menor norma de um vetor não nulo dentre todos os vetores de um reticulado.*

Assim, temos o seguinte lema:

Lema 9. *Sejam* $x_1, x_2, ..., x_n$ *uma base reduzida de um reticulado* Γ*. Então*

$$l(\Gamma) \geq 2^{-(n-1)/2} |x_1|.$$

Demonstração. Suponha que $x_1, x_2, ..., x_n$ seja uma base 3/4-reduzida de um reticulado Γ e $x_1^*, x_2^*, ..., x_n^*$ sua OGS. Pela proposição 5 (a) de uma base reduzida, sabemos que $|x_i^*|^2 \geq \beta^{-(i-1)}|x_1|^2$ para $1 \leq i \leq n$, como a base é 3/4-reduzida, temos $\beta = 2$. Assim,

$$|x_n^*|^2 \geq \beta^{-(n-1)}|x_1|^2$$
$$|x_n^*| \geq 2^{-(n-1)/2}|x_1|$$

Agora, sendo $l(\Gamma)$ a menor norma de um vetor não nulo em Γ pelas propriedades de OGS temos $l(\Gamma) \geq |x_n^*|$ o que completa a prova do lema. □

Como mencionado antes, para nosso objetivo, devido a grandiosidade dos números e operações envolvidas, faz-se necessário a presença de um software que forneça velocidade nos cálculos, e é isto que veremos agora.

Capítulo 2

Aplicação do LLL via software Magma

Para a aplicação do algoritmo de redução de base LLL devido a complexidade dos cálculos envolvidos usaremos o software Magma. O Magma é um software de álgebra computacional utilizado em pesquisas matemáticas de ensino superior. De acordo com Steel [12], ele fornece uma ampla variedade de funcionalidades para realizar cálculos simbólicos e manipulações algébricas em diversas áreas matemáticas, incluindo álgebra, teoria dos números, geometria algébrica, teoria dos grupos e muito mais.

O software possui uma linguagem de programação própria, que permite aos usuários criar scripts e programas para automatizar cálculos complexos. Essa linguagem é reconhecida por sua sintaxe clara e é acessível até mesmo para aqueles sem experiência extensiva em programação.

O Magma é conhecido por sua facilidade de uso e integração com outros softwares de álgebra computacional, como GAP e SageMath, que para o nosso caso, não será necessário. Além disso, sua comunidade ativa de usuários e desenvolvedores garante suporte contínuo, atualizações e o desenvolvimento de recursos adicionais.

o Magma é licenciado para uso em ambientes acadêmicos e de pesquisa, tornando-se uma ferramenta valiosa para estudantes, pesquisadores e matemáticos que buscam explorar e aplicar conceitos matemáticos em várias disciplinas.

Os comandos que serão utilizados para aplicação do LLL dada uma matriz B estão na Figura 2.1. Nela, o comando

$$B := RMatrixSpace(IntegerRing(), n, n)![...]$$

define uma matriz de ordem $n \times n$ com entradas definidas em $\mathbb{R}$. O comando

$$L1 := Lattice(B);$$
$$L1;$$

define a matriz B como como base de um reticulado. Já o comando

$$C := LLL(B : Proof := false);$$
$$C;$$

aplica a redução de base LLL com parâmetro de redução padrão ($\alpha = 3/4$) ao reticulado $L1$ gerando assim a base reduzida C. Por fim, o comando

$$C[1];$$
$$NQ := Norm(C[1]);$$
$$NQ;$$
$$R := SquareRoot(NQ);$$
$$R;$$

define um vetor linha da matriz C (no exemplo é o primeiro vetor) e calcula a norma euclidiana apresentando o resultado na ultima linha do código.

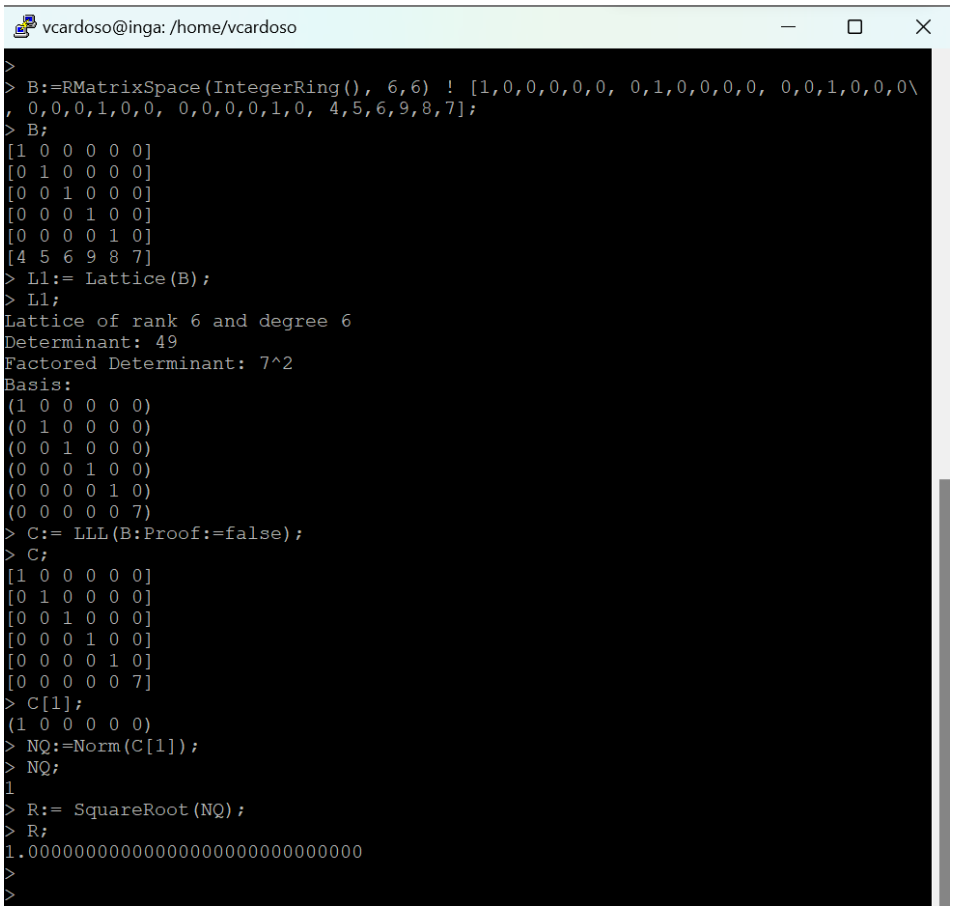

Figura 2.1: Exemplo De Aplicação.

Agora, com todas as ferramentas necessárias podemos dá inicio a nosso objetivo. Começaremos primeiramente com as desigualdades Diofantinas exponenciais, e no capítulo seguinte finalizaremos com uma equação envolvendo soma de potências de sequencias de Fibonacci.

Capítulo 3

Inequações Diofantinas Exponenciais

As desigualdades Diofantinas exponenciais representam um domínio crucial na teoria dos números, instigando a curiosidade e o fascínio de matemáticos na busca por soluções inteiras (ou, de forma mais ampla, racionais) para expressões exponenciais que envolvem variáveis inteiras. Especificamente, essas desigualdades são expressas pela forma $|a^{x_1} - b^{x_2}| < a^{\delta x_1}$, onde a e b são inteiros positivos predefinidos, e x_1 e x_2 são variáveis inteiras. A resolução dessas desigualdades frequentemente apresenta desafios consideráveis dado à natureza exponencial das expressões envolvidas.

Essas desigualdades possuem amplas aplicações em diversas áreas da matemática, abrangendo desde a teoria dos números até a criptografia e a otimização combinatória. Na teoria dos números, por exemplo, a resolução de desigualdades Diofantinas exponenciais desempenha um papel essencial na compreensão da distribuição de números inteiros em sequências exponenciais. Por outro lado, na criptografia, essas desigualdades são fundamentais para garantir a segurança de sistemas criptográficos baseados em reticulados.

Motivados pelo interesse gerado por essas desigualdades, este capítulo é dedicado exclusivamente à investigação e abordagem das soluções para este tipo específico de inequação por meio do poderoso algoritmo LLL, com o apoio valioso do software Magma. Assim, adentramos em uma jornada acadêmica que busca não apenas compreender, mas também contribuir para o avanço do conhecimento matemático nesta área desafiadora e estimulante.

Antes de qualquer coisa vejamos inicialmente alguns breves resultados sobre limites para formas lineares em logaritmo que nos serão essenciais.

3.1 Limites para Formas Lineares em Logaritmo

A teoria das formas lineares em logaritmos é um campo fascinante da matemática que tem suas raízes na teoria dos números e na análise Diofantina. Esta área concentra-se no estudo das soluções inteiras de equações lineares em logaritmos, ou seja, equações da forma $a \log x + b \log y = c$, onde a, b, e c são constantes e x e y são variáveis inteiras.

O interesse por essas equações surge de sua importância em várias áreas da matemática aplicada, como a teoria da criptografia, a teoria dos números computacionais e a teoria da informação.

Ao longo do tempo, matemáticos como Lagrange, Legendre, Gauss, Baker e Birch desenvolveram técnicas poderosas para lidar com estas equações e resolveram vários problemas importantes nesta área. No entanto, ainda existem muitas questões em aberto e desafios a serem enfrentados, o que torna a teoria das formas lineares em logaritmos um campo de pesquisa ativo e em constante evolução.

Nesta subseção apresentaremos alguns lemas essenciais para nosso estudo. Optamos por não citar estes lemas em sua totalidade, uma vez que os aplicamos exclusivamente a logaritmos de inteiros racionais e coeficientes racionais. Esses resultados estabelecem limites para formas lineares em logaritmos no cenário real.

Selecionamos resultados que fornecem constantes completamente explícitas, resultando em limites superiores convenientes para as soluções dos problemas diofantinos que buscamos resolver. É importante ressaltar que, em princípio, nossos métodos para reduzir esses limites são independentes do tamanho dos próprios limites.

Para começar seja $p_1, p_2, ..., p_n$ inteiros racionais tal que $2 \leq p_1 < p_2 < ... < p_n$. Seja também $b_1, ..., b_n \in \mathbb{Z}$ e $B = \max_{1 \leq i \leq n} |b_i|$. No caso real temos o seguinte resultado.

Lema 10 (Waldschmidt)**.** *Seja o valor não nulo*

$$\Lambda = b_1 \cdot \log(p_1) + \cdots + b_n \cdot \log(p_n).$$

Ponha

$$V_i = max(1, \log p_i) \quad i = 1, ..., n;$$

$$\Omega = V_1 \cdots V_n;$$

$$C_1 = 2^{9n+26} \cdot n^{n+4} \cdot \Omega \cdot \log(eV_{n-1});$$

$$C_2 = C_1 \cdot \log(eV_n).$$

Então

$$|\Lambda| > e^{-(C_1 \cdot \log B + C_2)}.$$

Demonstração. Demonstração desse lema foi feita por Waldschmidt [12]. □

Lema 11. *Seja* $a \geq 0, h \geq 1, b > (e^2/h)^h$, *e seja* $x \in \mathbb{R}$ *satisfazendo* $x \leq a + b(\log x)^h$. *Então*

$$x < (2a^{1/h} + 2b^{1/h} \log(h^h b))^h.$$

Demonstração. Por $(z_1 + z_2)^{1/h} \leq z_1^{1/h} + z_2^{1/h}$, inferimos que

$$x^{1/h} \leq a^{1/h} + c \log\left(x^{1/h}\right)$$

onde $c = hb^{1/h} > e^2$. Definindo $x^{1/h} = (1 + y)c \log c$; então $y > 0$. Agora,

$$(1 + y)c \log c = x^{1/h} \leq a^{1/h} + c \log(1 + y) + c \log c + c \log \log c$$

$$< a^{1/h} + cy + c \log c + c \log \log c,$$

logo,

$$yc(\log c - 1) < a^{1/h} + c \log \log c.$$

Segue-se, pelo fato de $c > e^2$, que

$$x^{1/h} = c \log c + yc \log c < c \log c + \frac{\log c}{\log c - 1}(a^{1/h} + c \log \log c) < 2(a^{1/h} + c \log c).$$

□

3.2 Solucionando desigualdades Diofantinas

Sejam então $p, < ... < p_t$ números primos, onde $t > 2$. Seja S o conjunto de todos os números inteiros positivos compostos apenas por esses primos, assim

$$S = \{p_1^{x_1} ... p_t^{x_t} : x_i \in \mathbb{Z}, x_i \geq 0\} \quad \text{para } i = 1, ..., t.$$

Seja $0 < \delta < 1$ um número real fixo. Nesta dissertação, estudaremos a seguinte inequação Diofantina:

$$|a^{x_1} - b^{x_2}| < a^{\delta x_1}$$

que, para simplificação, será generalizada como:

$$0 < x - y < y^{\delta} \tag{3.1}$$

onde $x, y \in S$. Para uma solução x, y da equação (3.1), os finitos $z \in \mathbb{N}$ para os quais zx, zy também são soluções da equação (3.1) podem ser facilmente encontrados. Portanto, podemos assumir que $(x, y) = 1$. Definimos

$$X = \max_{1 \leq i \leq t} \text{ord}_{p_i}(xy).$$

Em outras palavras, a função X define a maior potência inteira entre os fatores primos da inequação. Tijdeman demonstrou que existe um número computável c, dependente apenas de p_t, tal que para todos $x, y \in S$ com $x > y \geq 3$,

$$x - y > \frac{y}{(\log y)^c}.$$

Ao considerarmos as soluções da desigualdade (3.1), surge a dúvida inicial sobre a existência de soluções muito grandes. No entanto, o teorema a seguir nos esclarece que há um limite superior para as soluções de (3.1) que pode ser encontrado calculando as constantes C_4 e C_5.

Teorema 12 (Limites Superiores)**.** *Com a notação acima ponhamos,*

$$C_4 = 2^{9t+26} \cdot t^{t+4} \cdot \max\left(1, \frac{1}{\log p_1}\right) \cdot \log p_2 \cdots \log p_t \cdot \frac{\log(e \cdot \log p_{t-1})}{1-\delta}$$

$$C_5 = \frac{2\log 2}{\log p_1} + 2C_4 \log(eC_4 \log p_t).$$

Então as soluções de (3.1) satisfazem $X < C_5$.

Demonstração. Se $y \leq x/2$, então

$$2y \leq x \Rightarrow y \leq x - y \Rightarrow y < y^{\delta},$$

como $0 < \delta < 1$ temos

$$y^{1-\delta} < 1,$$

o que contradiz $y \geq 1$, logo $y > x/2$. Coloquemos $\Lambda = \log\left(\frac{x}{y}\right)$, então dividindo toda a inequação (3.1) por y

$$0 < \Lambda < \frac{x}{y} - 1 < y^{-(1-\delta)}$$

e sendo $y > x/2$

$$0 < \Lambda < \frac{x}{y} - 1 < y^{-(1-\delta)} < \left(\frac{x}{2}\right)^{-(1-\delta)}$$

$$\Rightarrow 0 < \Lambda < \left(\frac{x}{2}\right)^{-(1-\delta)}$$

como $x = \max(x, y) \geq p_1^X$ no obtemos

$$0 < \Lambda < 2^{1-\delta} p_1^{-(1-\delta)X}. \tag{3.2}$$

Tomemos agora o Lema 10 de formas lineares em logaritmo, com $n = t, q = 2$. Sendo $B = X$ e $p_i \geq 3$ temos $V_i = \log p_i$ para $i \geq 2$ e o lema nos permite escreve a seguinte desigualdade

$$\Lambda > e^{-(\log X + \log(e \log p_t))C_4(1-\delta)\log p_1}.$$

Combinando com a inequação (3.2) temos

$$\begin{aligned}
0 < e^{-(\log X+\log(e\log p_t))C_4(1-\delta)\log p_1} < \Lambda < 2^{1-\delta} p_1^{-(1-\delta)X} \\
e^{-(\log X+\log(e\log p_t))C_4(1-\delta)\log p_1} < 2^{1-\delta} p_1^{-(1-\delta)X} \\
\log\left(e^{-(\log X+\log(e\log p_t))C_4(1-\delta)\log p_1}\right) < \log\left(2^{1-\delta} p_1^{-(1-\delta)X}\right) \\
-(\log X + \log(e\log p_t))C_4(1-\delta)\log p_1 < (1-\delta)\log 2 - (1-\delta)X\log p_1 \\
(1-\delta)X\log p_1 < (1-\delta)\log 2 + (\log X + \log(e\log p_t))C_4(1-\delta)\log p_1 \\
X < \frac{(1-\delta)\log 2 + (\log X + \log(e\log p_t))C_4(1-\delta)\log p_1}{(1-\delta)\log p_1}
\end{aligned}$$

o que implica

$$X < C_4 \log(e \log p_t) + \frac{\log 2}{\log p_1} + C_4 \log X.$$

Usando agora o resultado do Lema 11 com $b = C_4$, $h = 1$, $a = C_4 \log(e \log p_t) + \frac{\log 2}{\log p_1}$ e como $C_4 > e^2$ temos

$$X < 2C_4 \log(e \log p_t) + \frac{2\log 2}{\log p_1} + 2C_4 \log(C_4)$$

$$X < 2C_4 \left(\log(e \log p_t) + \log(C_4)\right) + \frac{2\log 2}{\log p_1}$$

portanto,

$$X < \frac{2\log 2}{\log p_1} + 2C_4 \log(eC_4 \log p_t).$$

□

Exemplo 6. *Consideremos a seguinte inequação*

$$|2^{x_1} - 3^{x_2}| < 2^{\delta x_1} \tag{3.3}$$

queremos encontrar um limite superior para suas soluções. Com a notação generalizada temos $y = 2^{x_1}$ *e* $x = 3^{x_2}$, *assim* $t = 2, p_1 = 2, p_2 = 3$, *escolhemos agora* $\delta = 9/10$ *temos*

$$C_4 = 2^{50} \cdot \max\left(1, \frac{1}{\log 2}\right) \cdot \log 3 \cdot \frac{\log(e \cdot \log 2)}{1 - 9/10}$$

$$C_4 = 2^{50} \cdot 1,44 \cdot 1,09 \cdot 6,3 = 1,11 \cdot 10^{16}$$
$$C_5 = \frac{2\log 2}{\log 2} + 2 \cdot 1,11 \cdot 10^{16} \log(e1,11 \cdot 10^{16} \log 3)$$
$$C_5 = 8,44 \cdot 10^{17}$$

assim as soluções da inequação (5) satisfazem $X < 8,44 \cdot 10^{17}$.

Exemplo 7. *Considere agora uma inequação tal que* $t = 6$ *e* $p_i = 2,3,5,7,11,13$ *para* $i = \{1,...,6\}$*, escolhemos* $\delta = 1/2$ *então*

$$C_4 = 2^{80} \cdot \max\left(1, \frac{1}{\log 2}\right) \cdot \log 3 \cdot \log 5 \cdot \log 7 \cdot \log 11 \cdot \log 13 \cdot \frac{\log(e \cdot \log 11)}{1 - 1/2}$$
$$C_4 = 2^{80} \cdot 1,44 \cdot 21,16 \cdot 3,74 = 1,37 \cdot 10^{26}$$
$$C_5 = \frac{2\log 2}{\log 13} + 2 \cdot 1,37 \cdot 10^{26} \log(e1,37 \cdot 10^{26} \log 13)$$
$$C_5 = 1,7 \cdot 10^{28}$$

logo, as soluções da inequação são menores que $1,7 \cdot 10^{28}$.

Agora que obtivemos um limite superior para as soluções da Equação (3.1), abordaremos como reduzir esse limite. Para o caso em que $t = 2$, Gauss demonstrou que é possível resolver de maneira simples usando apenas frações contínuas. Portanto, concentraremos nossa atenção nos casos em que $t \geq 3$.

Para esses cenários, empregaremos o algoritmo de redução de base LLL para diminuir o limite superior e encontrar todas as soluções da inequação (3.1). Suponha que x, y seja uma solução de (3.1). Definiremos $x_i = \text{ord}_i(x/y)$ para $i = 1,...,t$, e $X = \max_{1 \leq i \leq t} |x_i|$. Seja C um limite superior para X, por exemplo, $C = C_5$. Escolheremos constantes positivas $\gamma \in \mathbb{Z}$, $C_0 \in \mathbb{R}$, e definiremos

$$\theta_i = [\gamma C_0 \log p_i] \quad i = 1,...,t$$

Considere agora o reticulado $\Gamma \subseteq \mathbb{Z}^t$, gerado pelos vetores coluna da matriz

$$A = \begin{bmatrix} \gamma & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & \gamma & 0 \\ \theta_1 & \dots & \theta_{t-1} & \theta_t \end{bmatrix}$$

Defina $\lambda = x_1\theta_1 + \cdots + x_t\theta_t$. Então,

$$y = \begin{bmatrix} \gamma & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & \gamma & 0 \\ \theta_1 & \dots & \theta_{t-1} & \theta_t \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ \vdots \\ \vdots \\ x_t \end{bmatrix} = \begin{bmatrix} x_1\gamma \\ \vdots \\ x_{t-1}\gamma \\ \lambda \end{bmatrix} \in \Gamma$$

com essa notação, temos o seguinte lema útil.

Lema 13. *Suponha que, para uma solução de (3.1)*

$$|\lambda| > \sum_{i=1}^{t} |x_i| \tag{3.4}$$

então, para $i = 1, ..., t$ *temos*

$$|x_i| < \frac{\log(2^{1-\delta}\gamma C_0) - \log\left(|\lambda| - \sum_{i=1}^{t} |x_i|\right)}{(1-\delta)\log p_i} \tag{3.5}$$

Demonstração. Seja

$$\Lambda = \log\left(\frac{x}{y}\right) = \sum_{i=1}^{t} x_i \log p_i$$

então

$$|\lambda - \gamma C_0 \Lambda| = \left|\sum_{i=1}^{t} x_i([\gamma C_0 \log p_i] - \gamma C_0 \log p_i)\right| \leq \sum_{i=1}^{t} |x_i|,$$

sendo $|\lambda| > \sum_{i=1}^{t} |x_i|$ temos

$$|\lambda - \gamma C_0 \Lambda| \leq \sum_{i=1}^{t} |x_i|$$

como $|\lambda| - |\gamma C_0 \Lambda| \leq |\lambda - \gamma C_0 \Lambda|$ temos

$$|\lambda| - |\gamma C_0 \Lambda| \leq \sum_{i=1}^{t} |x_i|$$

logo,

$$|\Lambda| \geq \frac{|\lambda| - \sum_{i=1}^{t} |x_i|}{\gamma C_0} > 0.$$

Da demonstração do teorema 12 de limites superiores sabemos que

$$\Lambda < \left(\frac{x}{2}\right)^{-(1-\delta)}$$

então

$$\frac{|\lambda| - \sum_{i=1}^{t} |x_i|}{\gamma C_0} < \left(\frac{x}{2}\right)^{-(1-\delta)}$$

logo,

$$x < 2|\Lambda|^{-1/(1-\delta)} \leq \left(\frac{2^{1-\delta}\gamma C_0}{|\lambda| - \sum_{i=1}^{t} |x_i|}\right)^{1/(1-\delta)}$$

dai desde que $p_i^{|x_i|} \leq \max(x, y) = x$ concluímos

$$|x_i| < \frac{\log(2^{1-\delta}\gamma C_0) - \log\left(|\lambda| - \sum_{i=1}^{t} |x_i|\right)}{(1-\delta)\log p_i} \tag{3.6}$$

□

Corolário 14. *Seja X_0 um número positivo tal que*

$$l(\Gamma) \geq (4t^2 + (t-1)\gamma^2)^{1/2} X_0. \tag{3.7}$$

então a inequação (3.1) não tem soluções para $i = 1, ..., t$,

$$\frac{\log\left(\dfrac{2^{1-\delta}\gamma C_0}{tX_0}\right)}{(1-\delta)\log p_i} \leq |x_i| \leq X_0. \tag{3.8}$$

Demonstração. Como $x \neq y$ temos $y \neq 0$. Suponha agora que para todo i tenhamos $|x_i| \leq X_0$, então

$$l(\Gamma)^2 \leq |y|^2 = \gamma^2 \sum_{i=1}^{t-1} x_i^2 + \lambda^2 \leq (t-1)\gamma^2 X_0^2 + \lambda^2$$

$$\Rightarrow l(\Gamma)^2 \leq (t-1)\gamma^2 X_0^2 + \lambda^2.$$

segue agora da demonstração do teorema 12 que

$$\lambda^2 \geq l(\Gamma)^2 - (t-1)\gamma^2 X_0^2 \geq 4t^2 X_0^2,$$

o que nos infere

$$|\lambda| - \sum_{i=1}^{t} |x_i| \geq 2tX_0 - tX_0 = tX_0.$$

aplicando agora o lema 13 o resultado segue. □

Para encontra um campo viável de busca de soluções da equação (3.1) usamos o corolário 14 para ajusta o limite superior C_5 e consequentemente reduzir X da seguinte maneira: Selecionamos C_0, ligeiramente maior que $(tC_5)^t$. Se C_0 for substancialmente grande, o erro de arredondamento será insignificante em comparação com C_i, tornando seguro assumir $\gamma = 1$. O parâmetro γ é empregado para manter o "erro de arredondamento"$|\gamma C_0 \log p_i - \theta_i|$ relativamente reduzido. Calculamos os valores dos inteiros θ_i com precisão e montamos a matriz base do reticulado Γ gerado pelo vetores colunas. Aplicamos a redução LLL nesta matriz para conseguimos obter um limite inferior para $l(\Gamma)$ usando o lema 9. Podemos

antecipar que esse limite será da ordem de $(\det(\Gamma))^{\frac{1}{t}}$ e aproximadamente $\gamma t C_0$. Consequentemente, podemos prever que

$$l(\Gamma) \geq (4t^2 + (t-1)\gamma^2)^{1/2} X_0$$

será válido com $X_0 = C_5$, caso contrário, devemos tentar um C_0 mais elevado. Se a desigualdade acima for confirmada, então pelo corolário 14,

$$|x_i| \leq \frac{\log\left(\dfrac{2^{1-\delta}\gamma C_0}{tX_0}\right)}{(1-\delta)\log p_i}$$

oferece limites para $|x_i|$ e, por conseguinte, para X, na ordem de $\log(C_0/C_5)$, que é da ordem de $\log C_5$. Assim a redução do limite superior é, de fato, substancial. Observe que lema 13 é mais preciso do que o seu corolário e, portanto, mais apropriado para reduzir á um limite pequeno de C_5.

Agora, procedemos com detalhes.

Exemplo 8. *Considere a seguinte inequação*

$$0 < x - y < y^{1/2} \tag{3.9}$$

para $t = 3$, $p_1 = 2, p_2 = 3, p_3 = 5$ e $\delta = 1/2$, de outra maneira, iremos encontrar todas as soluções de todas as desigualdades do tipo (3.9) formadas por $x, y \in S = \{2^{x_1} \cdot 3^{x_2} \cdot 5^{x_3} : x_i \in \mathbb{Z}, x_i \geq 0 \quad para \quad i = (1,2,3)\}$. Inicialmente usando o Teorema 12 temos,

$$C_4 = 2^{53} \cdot 3^7 \cdot \max\left(1, \frac{1}{\log 2}\right) \cdot \log 3 \cdot \log 5 \cdot \frac{\log(e \cdot \log 3)}{1 - 1/2}$$

$$C_4 = 1,09 \cdot 10^{20}$$

$$C_5 = \frac{2\log 2}{\log 2} + 2 \cdot 1,09 \cdot 10^{20} \log(e \cdot 1,09 \cdot 10^{20} \log 5)$$

$$C_5 = 1,04 \cdot 10^{22},$$

ou seja, as soluções de (3.9) satisfazem $X < 1,04 \cdot 10^{22}$. Nosso objetivo agora e reduzir esse limite para encontrar todas as soluções. Começamos fazendo $C_0 = 10^{400}$ e como este valor é grande podemos tomar $\gamma = 1$, calculamos então os coeficientes θ_i,

$$\theta_1 = 10^{400} \cdot \log 2$$
$$\theta_2 = 10^{400} \cdot \log 3$$
$$\theta_3 = 10^{400} \cdot \log 5$$

assim a matriz base do reticulado Γ *é*

$$B' = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 10^{400} \cdot \log 2 & 10^{400} \cdot \log 3 & 10^{400} \cdot \log 5 \end{bmatrix}.$$

Para aplicar o LLL via software Magma escrevemos a matriz da seguinte maneira

$$B = \begin{bmatrix} 1 & 0 & 10^{400} \cdot \log 2 \\ 0 & 1 & 10^{400} \cdot \log 3 \\ 0 & 0 & 10^{400} \cdot \log 5 \end{bmatrix}.$$

Aplicamos agora o LLL em B *usando o software Magma temos os seguintes resultados*

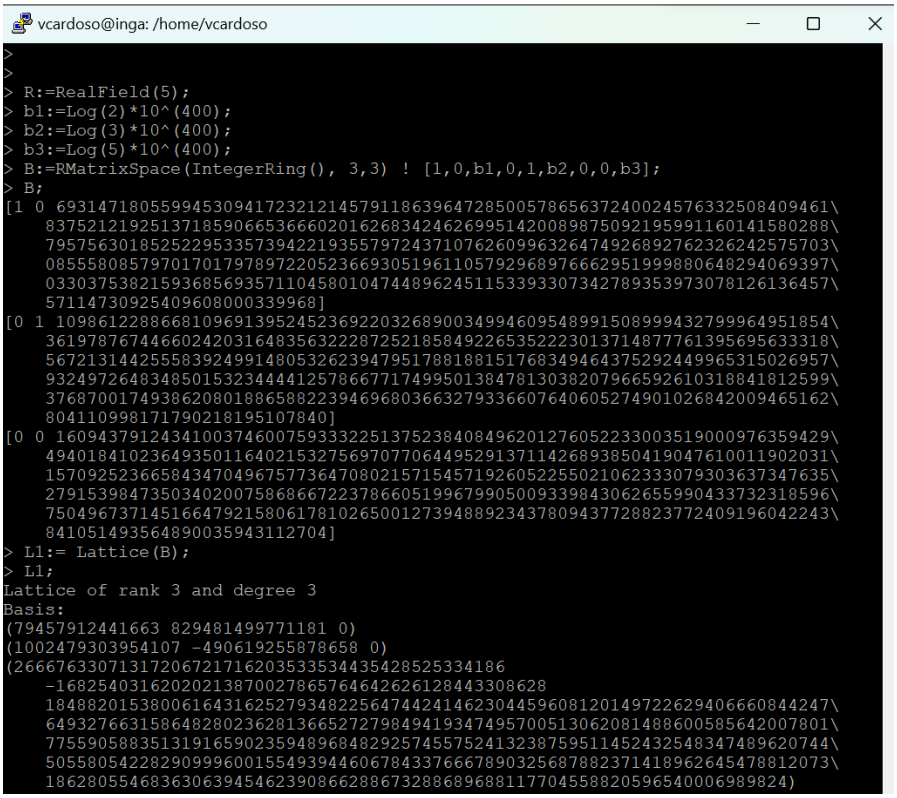

Figura 3.1: Definição da matriz e do reticulado.

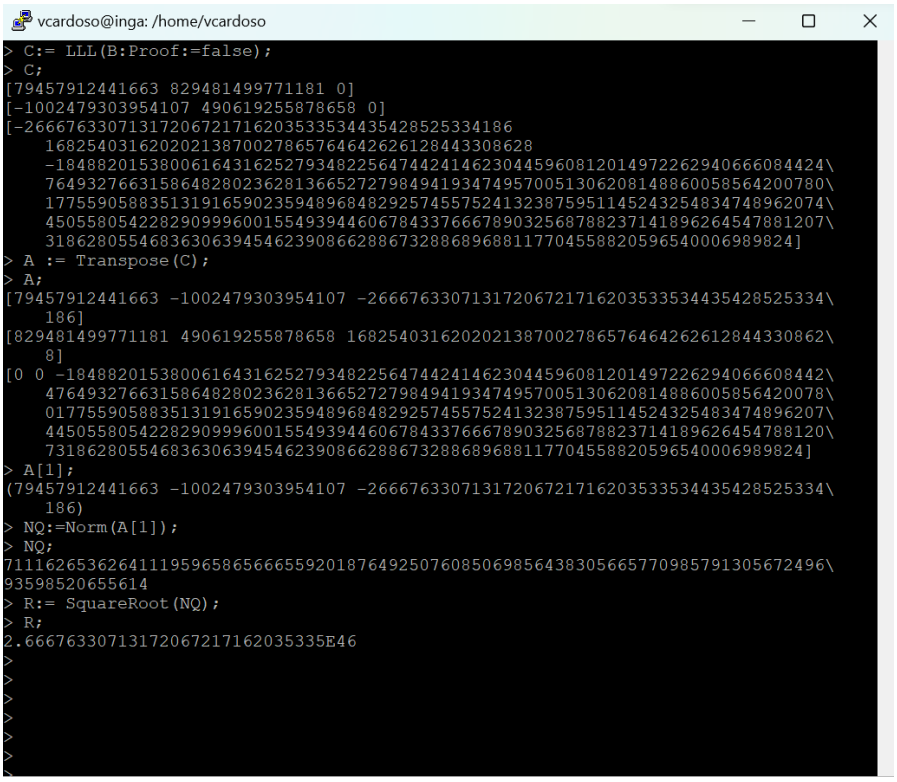

Figura 3.2: Aplicação do LLL, retransposição da matriz e calculo da norma do 1º vetor.

Temos assim, que a norma do primeiro vetor satisfaz

$$|c_1| \geq 2,66 \cdot 10^{46}.$$

Usando o lema 9 obtemos a seguinte estimativa para a menor norma de um vetor não nulo do reticulado Γ

$$l(\Gamma) \geq 2^{-1} \cdot 2,66 \cdot 10^{46},$$

verificamos agora se a desigualdade (3.7) é válida para $X_0 = C_5 = 1,04 \cdot 10^{22}$

$$l(\Gamma) \geq \sqrt{38} \cdot 1,04 \cdot 10^{22},$$

o que de fato acontece pois

$$l(\Gamma) \geq 2^{-1} \cdot 2,66 \cdot 10^{46} \geq \sqrt{38} \cdot 1,04 \cdot 10^{22}.$$

Assim usando o corolário 14 obtemos o seguinte limite para as soluções de (3.9) (Lembrando que $\gamma = 1, \delta = 1/2, X_0 = C_5$*)*

$$|x_i| \leq \frac{\log\left(\dfrac{2^{1/2}10^{400}}{3 \cdot 1,04 \cdot 10^{22}}\right)}{(1/2)\log 2}$$

$$|x_i| \leq 2509.$$

Veja que conseguimos reduzir bastante o campo para as soluções de (3.9) isso é possível pois o corolário 14 garante que se o comprimento do menor vetor do reticulado Γ *satisfaz (3.7) então as soluções da nossa desigualdade satisfazem (3.8). Vamos repetir este processo. Fazemos agora* $C_5 = 2509$ *e tomemos* $C_0 = 10^{50}$ *ainda com* $\gamma = 1$*. Então temos*

$$B = \begin{bmatrix} 1 & 0 & 10^{50} \cdot \log 2 \\ 0 & 1 & 10^{50} \cdot \log 3 \\ 0 & 0 & 10^{50} \cdot \log 5 \end{bmatrix}.$$

aplicando o LLL no Magma

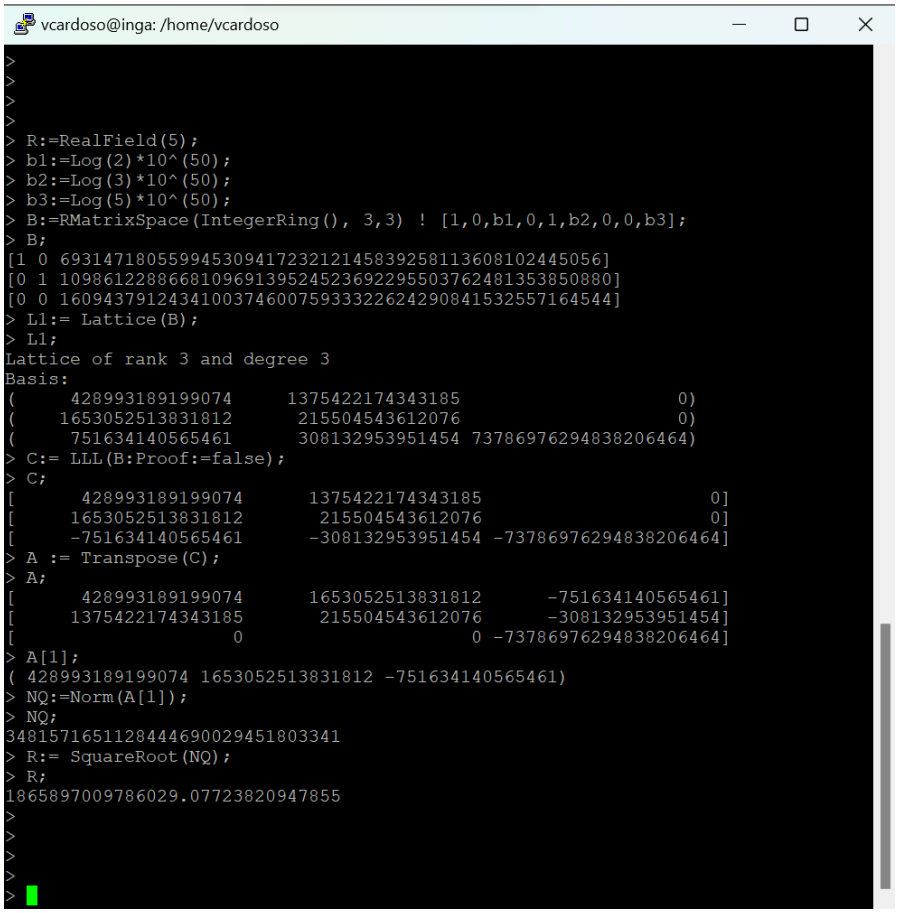

Figura 3.3: Definição do reticulado, aplicação do LLL e Norma do primeiro vetor.

conseguimos obter que

$$|c_1| \geq 1,86 \cdot 10^{15}$$

assim pelo lema 9 temos a seguinte estimativa para o comprimento do menor vetor do reticulado

$$l(\Gamma) \geq 2^{-1} \cdot 1,86 \cdot 10^{15}.$$

Pela desigualdade (3.7) devemos ter $l(\Gamma) \geq \sqrt{38} \cdot 2509$, *o que se dá de fato. Assim, conseguimos reduzir o limite das soluções de (3.9) para*

$$|x_i| \leq \frac{\log\left(\dfrac{2^{1/2}10^{50}}{3 \cdot 2509}\right)}{(1/2)\log 2} \Rightarrow |x_i| \leq 307$$

em particular temos

$$|x_1| \leq 307, \quad |x_2| \leq 193, \quad |x_3| \leq 132.$$

Vamos escolher agora $C_0 = 10^{30}$ *e tomemos* $\gamma = 10^5$, *lembremos que agora* $C_5 = 307$, *dai*

$$B = \begin{bmatrix} 1 & 0 & 10^5 \cdot 10^{30} \cdot \log 2 \\ 0 & 1 & 10^5 \cdot 10^{30} \cdot \log 3 \\ 0 & 0 & 10^5 \cdot 10^{30} \cdot \log 5 \end{bmatrix}.$$

então

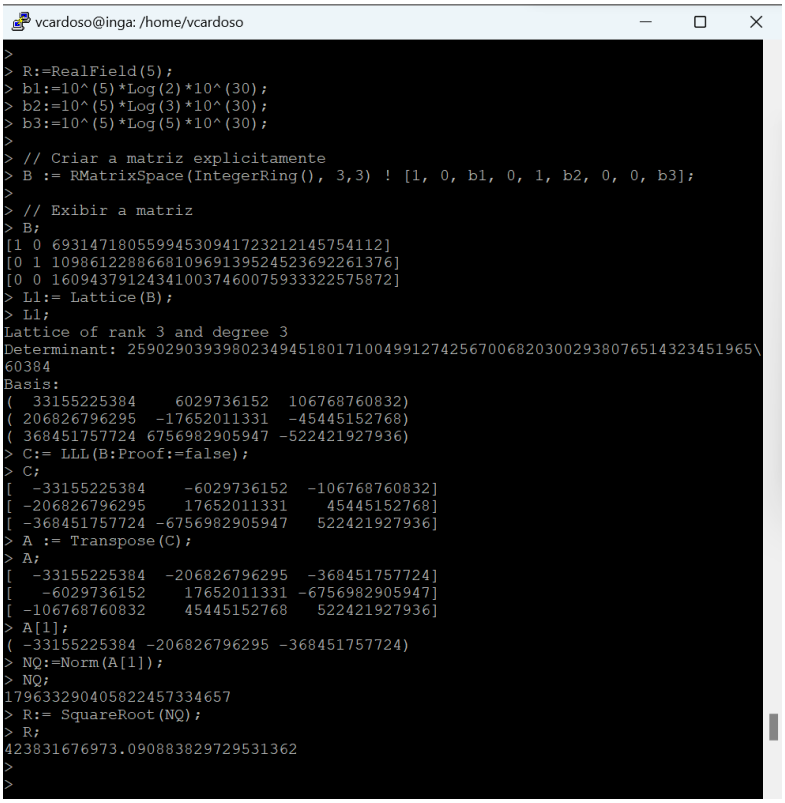

Figura 3.4: Definição do reticulado, aplicação do LLL e Norma do primeiro vetor.

assim temos

$$|c_1| \geq 4,23 \cdot 10^{11}$$

pela estimativa

$$l(\Gamma) \geq 2,11 \cdot 10^{11}.$$

Pela desigualdade (3.7) devemos ter $l(\Gamma) \geq 4,34 \cdot 10^7$, *e vemos que esta é satisfeita. Assim, com o corolário 14 conseguimos reduzir o limite das soluções de (3.9) para*

$$|x_i| \leq \frac{\log\left(\dfrac{2^{1/2} \cdot 10^5 \cdot 10^{30}}{3 \cdot 307}\right)}{(1/2)\log 2} \Rightarrow |x_i| \leq 213$$

em particular,

$$|x_1| \leq 213, \quad |x_2| \leq 134, \quad |x_3| \leq 92.$$

Façamos mais uma tentativa, dessa vez reduzimos C_0 *para* $C_0 = 10^{20}$ *e tomemos* $\gamma = 10^5$, *lembremos que agora* $C_5 = 213$, *dai*

$$B = \begin{bmatrix} 1 & 0 & 10^5 \cdot 10^{20} \cdot \log 2 \\ 0 & 1 & 10^5 \cdot 10^{20} \cdot \log 3 \\ 0 & 0 & 10^5 \cdot 10^{20} \cdot \log 5 \end{bmatrix}.$$

então (Observe que na figura 3.5 mudei a estrutura de contrução da matriz, usei a função Round para arredondar os resultados para o inteiro mais próximo.)

```
> B := RMatrixSpace(IntegerRing(), 3, 3) ! [1, 0, Round(Log(2)*10^(25)), 0, 1,\
 Round(Log(3)*10^(25)), 0, 0, Round(Log(5)*10^(25))];
> B;
[1 0 693147180559453094172321]
[0 1 1098612288668109691395 2452]
[0 0 1609437912434100374600 7593]
> L1:= Lattice(B);
> L1;
Lattice of rank 3 and degree 3
Determinant: 259029039398023494518017089804168274998886813653649
Basis:
(  25864335   66032104 -162371455)
( 204174417 -194497365 -136421320)
( 299784785  113810061   29976481)
> C:= LLL(B:Proof:=false);
> C;
[  25864335   66032104 -162371455]
[ 204174417 -194497365 -136421320]
[ 299784785  113810061   29976481]
> A := Transpose(C);
> A;
[  25864335  204174417  299784785]
[  66032104 -194497365  113810061]
[-162371455 -136421320   29976481]
> A[1];
( 25864335 204174417 299784785)
> NQ:=Norm(A[1]);
> NQ;
132227073699778339
> R:= SquareRoot(NQ);
> R;
363630408.106608074136410944116
>
```

Figura 3.5: Definição do reticulado, aplicação do LLL e Norma do primeiro vetor.

segue então que

$$|c_1| \geq 3,63 \cdot 10^8$$

e assim a estimativa satisfaz

$$1,81 \cdot 10^8 \geq 3,01 \cdot 10^7,$$

portanto os novos limites para as soluções de (3.9) são dados por

$$|x_i| \leq \frac{\log\left(\dfrac{2^{1/2} \cdot 10^5 \cdot 10^{20}}{3 \cdot 213}\right)}{(1/2)\log 2}$$

$$|x_1| \leq 148, \quad |x_2| \leq 93, \quad |x_3| \leq 63.$$

A partir de agora poderíamos diminuir mais o valor de C_0, no entanto, precisaríamos de um γ maior para garantir o erro de arredondamento continue sob controle, mas assim a condição de redução (3.7) não seria satisfeita. Por outro lado se deixássemos γ com o mesmo valor, para garantir que (3.7) seja satisfeita, a diminuição em C_0 seria insignificante e fútil diante do trabalho, tornando o processo inviável.

Nossa melhor alternativa para refinar o campo de soluções da nossa desigualdade é usar o lema 13 que é mais forte que seu corolário 14. Primeiramente observe que o campo de soluções e tal que $|x_i| < 148$, então é razoável estimar que para alguma solução de (3.9) tenhamos

$$5 \cdot 10^{20} > \sum_{i=1}^{3} |x_i|$$

dai $|\lambda| > 5 \cdot 10^{20}$, e por (3.6)

$$|x_i| < \frac{\log(2^{1/2}10^5 10^{20}) - \log\left(5 \cdot 10^{20} - 304\right)}{(1/2)\log p_i}$$

$$\Rightarrow |x_1| < 29, \quad |x_2| < 18, \quad |x_3| < 12.$$

Com esse resultado, estabelecemos um limite superior para as variáveis que são soluções da Equação (3.9), o que reduz significativamente nosso trabalho. Agora, vamos detalhar cada possibilidade de inequação e suas soluções por meio do Magma. Informamos que as possibilidades que resultarem em um conjunto de soluções vazio não serão apresentadas. Além disso, devido à praticidade do Magma, aumentaremos o escopo de busca por soluções.

Aqui, a critério de simplicidade, denotaremos as variáveis x_1, x_2, x_3 por x, y, z respectivamente. As possibilidades de desigualdades são:

1. $0 < 2^x 3^y - 5^z < 5^{z/2}$.
2. $0 < 2^x 3^y - 2^x 5^z < 2^{x/2} 5^{z/2}$.
3. $0 < 2^x 3^y - 3^y 5^z < 3^{y/2} 5^{z/2}$.
4. $0 < 2^x 5^z - 3^y < 3^{y/2}$.
5. $0 < 2^x 5^z - 3^y 5^z < 3^{y/2} 5^{z/2}$.
6. $0 < 3^y 5^z - 2^x < 2^{x/2}$.
7. $0 < 3^y 5^z - 2^x 5^z < 2^{x/2} 5^{z/2}$.
8. $0 < 3^y 5^z - 2^x 3^y < 2^{x/2} 3^{y/2}$.
9. $0 < 2^x - 3^y 5^z < 3^{y/2} 5^{z/2}$.
10. $0 < 3^y - 2^x 5^z < 2^{x/2} 5^{z/2}$.
11. $0 < 5^z - 2^x 3^y < 2^{x/2} 3^{y/2}$.

Suas respectivas soluções são,

```
> // Defina a inequao
> inequacao := function(x, y, z)
function>     return 0 lt 2^x * 3^y - 5^z and 2^x * 3^y - 5^z lt 5^(z/2);
function> end function;
>
> // Encontre as solues no conjunto de inteiros dentro das restries
> solutions := [];
> for x in [0..113] do
for>     for y in [0..71] do
for|for>         for z in [0..49] do
for|for|for>             if inequacao(x, y, z) then
for|for|for|if>                 Append(~solutions, [x, y, z]);
for|for|for|if>             end if;
for|for|for>         end for;
for|for>     end for;
for> end for;
> solutions;
[
    [ 0, 3, 2 ],
    [ 1, 1, 1 ],
    [ 3, 4, 4 ],
    [ 7, 0, 3 ]
]
> // Exiba o nmero de solues
> NumberOfSolutions := #solutions;
> NumberOfSolutions;
4
>
```

Figura 3.6: Soluções de 1

```
> // Defina a inequao
> inequacao := function(x, y, z)
function>     return 0 lt 2^x * 3^y - 2^x * 5^z and 2^x * 3^y - 2^x * 5^z lt 2\
^(x/2) * 5^(z/2);
function> end function;
>
> // Encontre as solues no conjunto de inteiros dentro das restries
> solutions := [];
> for x in [0..113] do
for>     for y in [0..71] do
for|for>         for z in [0..49] do
for|for|for>             if inequacao(x, y, z) then
for|for|for|if>                 Append(~solutions, [x, y, z]);
for|for|for|if>             end if;
for|for|for>         end for;
for|for>     end for;
for> end for;
>
> // Exiba as solues
> solutions;
[
    [ 0, 3, 2 ],
    [ 1, 3, 2 ],
    [ 2, 3, 2 ]
]
>
> // Exiba o nmero de solues
> NumberOfSolutions := #solutions;
> NumberOfSolutions;
3
```

Figura 3.7: Soluções de 2

```
> // Defina a inequao
> inequacao := function(x, y, z)
function>     return 0 lt 2^x * 3^y - 3^y * 5^z and 2^x * 3^y - 3^y * 5^z lt 3\
^(y/2) * 5^(z/2);
function> end function;
>
> // Encontre as solues no conjunto de inteiros dentro das restries
> solutions := [];
> for x in [0..113] do
for>     for y in [0..71] do
for|for>         for z in [0..49] do
for|for|for>             if inequacao(x, y, z) then
for|for|for|if>                 Append(~solutions, [x, y, z]);
for|for|for|if>             end if;
for|for|for>         end for;
for|for>     end for;
for> end for;
>
> // Exiba as solues
> solutions;
[
    [ 7, 0, 3 ],
    [ 7, 1, 3 ],
    [ 7, 2, 3 ]
]
>
> // Exiba o nmero de solues
> NumberOfSolutions := #solutions;
> NumberOfSolutions;
3
```

Figura 3.8: Soluções de 3

```
> // Defina a inequao
> inequacao := function(x, y, z)
function>     return 0 lt 2^x * 5^z - 3^y and 2^x * 5^z - 3^y lt 3^(y/2);
function> end function;
>
> // Encontre as solues no conjunto de inteiros dentro das restries
> solutions := [];
> for x in [0..113] do
for>     for y in [0..71] do
for|for>         for z in [0..49] do
for|for|for>             if inequacao(x, y, z) then
for|for|for|if>                 Append(~solutions, [x, y, z]);
for|for|for|if>             end if;
for|for|for>         end for;
for|for>     end for;
for> end for;
>
> // Exiba as solues
> solutions;
[
    [ 1, 2, 1 ],
    [ 1, 5, 3 ],
    [ 2, 1, 0 ],
    [ 5, 3, 0 ],
    [ 8, 5, 0 ]
]
>
> // Exiba o nmero de solues
> NumberOfSolutions := #solutions;
> NumberOfSolutions;
5
```

Figura 3.9: Soluções de 4

```
> // Defina a inequao
> inequacao := function(x, y, z)
function>     return 0 lt 2^x * 5^z - 5^z * 3^y and 2^x * 5^z - 5^z * 3^y lt 5^(\
z/2) * 3^(y/2);
function> end function;
>
> // Encontre as solues no conjunto de inteiros dentro das restries
> solutions := [];
> for x in [0..113] do
for>     for y in [0..71] do
for|for>         for z in [0..49] do
for|for|for>             if inequacao(x, y, z) then
for|for|for|if>                 Append(~solutions, [x, y, z]);
for|for|for|if>             end if;
for|for|for>         end for;
for|for>     end for;
for> end for;
>
> // Exiba as solues
> solutions;
[
    [ 2, 1, 0 ],
    [ 5, 3, 0 ],
    [ 8, 5, 0 ]
]
>
> // Exiba o nmero de solues
> NumberOfSolutions := #solutions;
> NumberOfSolutions;
3
```

Figura 3.10: Soluções de 5

```
> // Defina a inequao
> inequacao := function(x, y, z)
function>     return 0 lt 3^y * 5^z - 2^x and 3^y * 5^z - 2^x lt 2^(x/2);
function> end function;
>
> // Encontre as solues no conjunto de inteiros dentro das restries
> solutions := [];
> for x in [0..113] do
for>     for y in [0..71] do
for|for>         for z in [0..49] do
for|for|for>             if inequacao(x, y, z) then
for|for|for|if>                 Append(~solutions, [x, y, z]);
for|for|for|if>             end if;
for|for|for>         end for;
for|for>     end for;
for> end for;
>
> // Exiba as solues
> solutions;
[
    [ 1, 1, 0 ],
    [ 2, 0, 1 ],
    [ 3, 2, 0 ],
    [ 7, 3, 1 ],
    [ 15, 8, 1 ]
]
>
> // Exiba o nmero de solues
> NumberOfSolutions := #solutions;
> NumberOfSolutions;
5
```

Figura 3.11: Soluções de 6

```
> // Defina a inequao
> inequacao := function(x, y, z)
function>     return 0 lt 3^y * 5^z - 2^x * 5^z and 3^y * 5^z - 2^x * 5^z lt 5^(\
z/2) * 2^(x/2);
function> end function;
>
> // Encontre as solues no conjunto de inteiros dentro das restries
> solutions := [];
> for x in [0..113] do
for>     for y in [0..71] do
for|for>         for z in [0..49] do
for|for|for>             if inequacao(x, y, z) then
for|for|for|if>                 Append(~solutions, [x, y, z]);
for|for|for|if>             end if;
for|for|for>         end for;
for|for>     end for;
for> end for;
>
> // Exiba as solues
> solutions;
[
    [ 1, 1, 0 ],
    [ 3, 2, 0 ],
    [ 3, 2, 1 ]
]
>
> // Exiba o nmero de solues
> NumberOfSolutions := #solutions;
> NumberOfSolutions;
3
```

Figura 3.12: Soluções de 7

```
> // Defina a inequao
> inequacao := function(x, y, z)
function>     return 0 lt 3^y * 5^z - 2^x * 3^y and 3^y * 5^z - 2^x * 3^y lt 2^(\
x/2) * 3^(y/2);
function> end function;
>
> // Encontre as solues no conjunto de inteiros dentro das restries
> solutions := [];
> for x in [0..113] do
for>     for y in [0..71] do
for|for>         for z in [0..49] do
for|for|for>             if inequacao(x, y, z) then
for|for|for|if>                 Append(~solutions, [x, y, z]);
for|for|for|if>             end if;
for|for|for>         end for;
for|for>     end for;
for> end for;
>
> // Exiba as solues
> solutions;
[
    [ 2, 0, 1 ],
    [ 2, 1, 1 ]
]
>
> // Exiba o nmero de solues
> NumberOfSolutions := #solutions;
> NumberOfSolutions;
2
```

Figura 3.13: Soluções de 8

```
> // Defina a inequao
> inequacao := function(x, y, z)
function>     return 0 lt 2^x - 3^y * 5^z and 2^x - 3^y * 5^z lt 3^(y/2) * 5^(z/\
2);
function> end function;
>
> // Encontre as solues no conjunto de inteiros dentro das restries
> solutions := [];
> for x in [0..113] do
for>     for y in [0..71] do
for|for>         for z in [0..49] do
for|for|for>             if inequacao(x, y, z) then
for|for|for|if>                 Append(~solutions, [x, y, z]);
for|for|for|if>             end if;
for|for|for>         end for;
for|for>     end for;
for> end for;
>
> // Exiba as solues
> solutions;
[
    [ 2, 1, 0 ],
    [ 4, 1, 1 ],
    [ 5, 3, 0 ],
    [ 7, 0, 3 ],
    [ 8, 5, 0 ],
    [ 11, 4, 2 ]
]
>
> // Exiba o nmero de solues
> NumberOfSolutions := #solutions;
> NumberOfSolutions;
6
```

Figura 3.14: Soluções de 9

```
> // Defina a inequao
> inequacao := function(x, y, z)
function>     return 0 lt 3^y - 2^x * 5^z and 3^y - 2^x * 5^z lt 2^(x/2) * 5^(z/\
2);
function> end function;
>
> // Encontre as solues no conjunto de inteiros dentro das restries
> solutions := [];
> for x in [0..113] do
for>     for y in [0..71] do
for|for>         for z in [0..49] do
for|for|for>             if inequacao(x, y, z) then
for|for|for|if>                 Append(~solutions, [x, y, z]);
for|for|for|if>             end if;
for|for|for>         end for;
for|for>     end for;
for> end for;
>
> // Exiba as solues
> solutions;
[
    [ 0, 3, 2 ],
    [ 1, 1, 0 ],
    [ 3, 2, 0 ],
    [ 4, 4, 1 ]
]
>
> // Exiba o nmero de solues
> NumberOfSolutions := #solutions;
> NumberOfSolutions;
4
```

Figura 3.15: Soluções de 10

```
> // Defina a inequao
> inequacao := function(x, y, z)
function>     return 0 lt 5^z - 2^x * 3^y and 5^z - 2^x * 3^y lt 2^(x/2) * 3^(y/\
2);
function> end function;
>
> // Encontre as solues no conjunto de inteiros dentro das restries
> solutions := [];
> for x in [0..113] do
for>     for y in [0..71] do
for|for>         for z in [0..49] do
for|for|for>             if inequacao(x, y, z) then
for|for|for|if>                 Append(~solutions, [x, y, z]);
for|for|for|if>             end if;
for|for|for>         end for;
for|for>     end for;
for> end for;
>
> // Exiba as solues
> solutions;
[
    [ 2, 0, 1 ],
    [ 3, 1, 2 ],
    [ 6, 5, 6 ],
    [ 10, 1, 5 ]
]
>
> // Exiba o nmero de solues
> NumberOfSolutions := #solutions;
> NumberOfSolutions;
4
```

Figura 3.16: Soluções de 11

Portanto, concluímos que a seguinte inequação

$$0 < x - y < y^{1/2} \tag{3.10}$$

para $t = 3$, $p_1 = 2, p_2 = 3, p_3 = 5$ *e* $\delta = 1/2$, *onde* $x, y \in S = \{2^{x_1} \cdot 3^{x_2} \cdot 5^{x_3} : x_i \in \mathbb{Z}, x_i \geq 0, i = (1,2,3)\}$ *com* $(x,y) = 1$ *possui um total de 42 soluções. As quais satisfazem*

$$ord_2(xy) \leq 15, \quad ord_3(xy) \leq 8, \quad ord_5(xy) \leq 6.$$

Outro caso interessante foi o apresentado por Weger com o seguinte teorema:

Teorema 15 (Weger)**.** *A inequação Diofantina*

$$0 < x - y < y^{1/2}$$

com $x, y \in S = \{2^{x_1} \cdots 13^{x_6} : x_i \in \mathbb{Z}, x_i \geq 0, i = (1,2,3)\}$ *com* $(x,y) = 1$ *tem exatamente 605 soluções. Dentre elas, 517 satisfazem*

$$ord_2(xy) \leq 19, \quad ord_3(xy) \leq 12, \quad ord_5(xy) \leq 8,$$

$$ord_7(xy) \leq 7, \quad ord_{11}(xy) \leq 5, \quad ord_{13}(xy) \leq 5.$$

Capítulo 4

Equações com Soma de Potências de Números Consecutivos de Fibonacci

As equações cujas soluções pertencem ao conjunto dos números inteiros são conhecidas como equações Diofantinas. Ao longo da história, muitos estudiosos da Teoria dos Números têm se dedicado a essa área de pesquisa. Entre as equações mais notáveis estão as equações de Pell, as equações pitagóricas e, possivelmente a mais famosa delas, a equação do Último Teorema de Fermat.

Este capítulo se concentra em uma situação particular de equações Diofantinas: Uma equação Diofantina exponencial relacionada a renomada sequência de Fibonacci e suas generalizações. Para realizar esta análise, faremos uso de métodos baseados em formas lineares em logaritmos para restringir as variáveis na equação, o Algoritmo LLL para diminuir o limite destas variáveis, juntamente com uma série de lemas e teoremas apresentados, e o software Magma para automatizar os cálculos extensos.

Vamos entender nosso problema. A sequência de Fibonacci constituí uma série de números comumente encontrada em diversas áreas da matemática e ciências aplicadas. Ela é definida por uma relação de recorrência simples, que pode ser expressa da seguinte forma:

$$F(n) = \begin{cases} 0 & \text{se } n = 0 \\ 1 & \text{se } n = 1 \\ F(n-1) + F(n-2) & \text{se } n > 1 \end{cases}$$

Essa definição resulta em uma sequência de números denominada sequência de Fibonacci, denotada como $\{0, 1, 1, 2, 3, 5, 8, 13, 21, \dots\}$, em que cada termo subsequente é a soma dos dois termos anteriores. De maneira mais simples, vamos definir a sequência de Fibonacci $(F_n)_{n\geq 0}$, por

$$F_n = F_{n-1} + F_{n-2}, \text{ onde } n \geq 2,$$

com $F_0 = 0$ e $F_1 = 1$. Assim, considere agora um número inteiro $k \geq 2$. Definimos a sequência de Fibonacci de ordem k-generalizada pela seguinte relação de recorrência:

$$F_n^{(k)} = F_{n-1}^{(k)} + \ldots + F_{n-k}^{(k)}, \quad \forall n \geq 2,$$

onde os k termos iniciais são determinados por $F_{-(k-2)}^{(k)} = F_{-(k-3)}^{(k)} = \ldots = F_0^{(k)} = 0$ e $F_1^{(k)} = 1$.

Observa-se que quando $k = 2$, obtemos a sequência de Fibonacci, cujos primeiros termos são:

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \ldots$$

Se $k = 3$, os termos são chamados de números de Tribonacci, denotados por $F_n^{(3.1)} = T_n$. Veja alguns dos primeiros termos:

$$0, 1, 1, 2, 4, 7, 13, 24, 44, 81, 149, 274, \ldots$$

Uma das relações intrigantes elaborada com essas sequencias é a seguinte: ao somarmos os quadrados de números consecutivos da sequência de Fibonacci, obtemos novamente um número de Fibonacci, expresso pela identidade

$$F_n^2 + F_{n+1}^2 = F_{2n+1}.$$

Inicialmente, os matemáticos Chaves e Marques exploraram equações do tipo para sequências de Fibonacci k-generalizadas, concluindo que a equação quadrática

$$(F_n^{(k)})^2 + (F_{n+1}^{(k)})^2 = F_m^{(k)}$$

não possui solução em inteiros (n, m, k) com $n \geq 2$ e $k \geq 3$. Em seguida, eles alcançaram um resultado parcial para a equação mais geral

$$(F_n^{(k)})^s + (F_{n+1}^{(k)})^s = F_m^{(k)}$$

sob a condição $3 \leq k \leq \min\{n, \log s\}$ para garantir a inexistência de soluções. Luca e Ruiz determinaram que esta última equação não tem solução em inteiros (n, m, k, s) com $k \geq 3$, $n \geq 2$ e $s \geq 2$. Em um estudo adicional, Freitas e colaboradores provaram a inexistência de solução para a equação

$$(F_n^{(k)})^2 + (F_{n+1}^{(k)})^2 = F_m^{(l)}$$

em inteiros (n, m, k, l) com $2 \leq k < l$ e $n \geq 2$.

O objetivo deste capítulo é apresentar o resultado da equação investigada por Kreutz [6] via Algoritmo LLL e Software Magma,

$$T_n^s + T_{n+1}^s = F_m$$

para inteiros positivos $s \geq 2$ e $n \geq 2$.

Antes de enunciar o teorema vamos apresenta alguns resultados preliminares, como teoremas e lemas, que serão fundamentais para as demonstrações subsequentes. Optamos por limitar o conteúdo desta subseção, omitindo algumas das demonstrações dos resultados aqui apresentados, a fim de manter o foco em nosso objetivo principal. Estes resultados veem da tese de doutorado de Kreutz [6], onde o leitor pode encontrar as demonstrações.

4.1 Preliminares

Teorema 16 (Kreutz). *Seja (n, m, k, l, s) solução da equação Diofantina*

$$(F_n^{(k)})^s + (F_{n+1}^{(k)})^s = F_m^{(l)}$$

como $n, m \geq 2$, $k > l \geq 2$, $s \geq 3$ inteiros. Então,

$$s < 8,11 \cdot 10^{210} k^{100} (\log k)^{43},$$

$$n < 1,49 \cdot 10^{39} k^2 (\log k)^8,$$

$$s < 1,97 \cdot 10^{230} k^{110} (\log k)^{47}.$$

Teorema 17 (Matveev). *Seja K um corpo de números de grau D sobre $\mathbb{Q}$, sejam $\gamma_1, \ldots, \gamma_t$ números reais positivos de K, e sejam $b_1, \ldots, b_t$ números inteiros. Suponha $B \geq \max\{|b_1|, \ldots, |b_t|\}$, e considere $\Lambda := \gamma_1^{b_1} \cdot \ldots \cdot \gamma_t^{b_t} - 1$. Sejam $A_1, \ldots, A_t$ números reais tais que*

$$A_i \geq \max\{Dh(\gamma_i), |\log \gamma_i|, (0.16)\}, \quad i = 1, \ldots, t.$$

Então, assumindo que $\Lambda \neq 0$, temos

$$|\Lambda| > \exp\left(-1.4 \cdot 30^{t+3} \cdot t^{4.5} \cdot D^2 (1 + \log D)(1 + \log B) \cdot A_1 \cdots A_t\right).$$

Lema 18. *Para todo $k \geq 2$ temos*

$$\alpha^{n-2} \leq F_n^{(k)} \leq \alpha^{n-1},$$

para todo $n \geq 1$.

Demonstração. Para $n = 1$ temos $\frac{1}{\alpha} \leq F_1^{(k)} = 1 \leq \alpha^0 = 1$. Vamos provar por indução em $n \geq 2$ para um $k \geq 2$ dado. Observe que para $2 \leq n \leq k + 1$ temos por Kreutz [6, lema 1.3],

$$F_n^{(k)} = 2^{n-2}$$

. Como $\alpha < 2$, a desigualdade $\alpha^{n-2} \leq F_n^{(k)}$ segue diretamente. Para a outra desigualdade, observe que como $\alpha > 2(1-2^{-k})$, é suficiente provar que $2^{n-1}(1-2^{-k})^{n-1} \geq 2^{n-2}$, ou seja, $(1-2^{-k})^{n-1} > \frac{1}{2}$. No entanto, vale que $(1-x)^n > 1-nx$, para todo $n > 1$ e $x > 0$, daí

$$(1-2^{-k})^{n-1} > 1-(n-1)\cdot 2^{-k} \geq 1-\frac{k}{2^k} \geq 1-\frac{1}{2} = \frac{1}{2},$$

onde usamos os fatos que $n \leq k+1$ e $2^{k-1} \geq k$. Suponha então que o resultado seja verdadeiro para todo inteiro menor que $n \geq k+2$, logo

$$\alpha^{n-3} \leq F_{n-1}^{(k)} \leq \alpha^{n-2}$$

$$\alpha^{n-4} \leq F_{n-2}^{(k)} \leq \alpha^{n-3}$$

...

$$\alpha^{n-k-2} \leq F_{n-k}^{(k)} \leq \alpha^{n-k-1}$$

Somando as desigualdades da hipótese de indução acima temos

$$\alpha^{n-3}+\alpha^{n-4}+\cdots+\alpha^{n-k-2} \leq F_n^{(k)} \leq \alpha^{n-2}+\alpha^{n-3}+\cdots+\alpha^{n-k-1}$$

$$\alpha^{n-k-2}(\alpha^{k-1}+\alpha^{k-2}+\cdots+\alpha+1) \leq F_n^{(k)} \leq \alpha^{n-k-1}(\alpha^{k-1}+\alpha^{k-2}+\cdots+\alpha+1)$$

$$\alpha^{n-k-2}\alpha^k \leq F_n^{(k)} \leq \alpha^{n-k-1}\alpha^k$$

$$\alpha^{n-2} \leq F_n^{(k)} \leq \alpha^{n-1},$$

pois $\alpha^k = \alpha^{k-1}+\alpha^{k-2}+\cdots+\alpha+1$, o que completa a demonstração. □

Lema 19. *Se $A \geq 3$ e $\frac{y}{\log y} < A$, então $y < 2A\log A$.*

Demonstração. Como a função $f(y) = \frac{y}{\log y}$ é crescente para $y > e$, suponha, por absurdo, que $y \geq 2A\log A$. Daí,

$$\frac{y}{\log y} \geq \frac{2A\log A}{\log(2A\log A)} > \frac{2A\log A}{2\log A} = A,$$

onde usamos o fato de que para $A \geq 3$, $2\log A < A$ e, portanto, $\log(2A\log A) < \log A^2 = 2\log A$. Mas isso contradiz a hipótese $y/\log y < A$. □

Proposição 20. *Sejam $X_1, X_2, \ldots, X_n$ inteiros positivos. Sejam*

$$Q = \sum_{i=1}^{n-1} X_i^2$$

e

$$T = \frac{1 + \sum_{i=1}^{n} X_i}{2}.$$

e assuma que $d(\Lambda, y)^2 \geq T^2 + Q$. *Se* $x_i \in \mathbb{Z}$ *são tais que* $|x_i| \leq X_i$ *para todo* $1 \leq i \leq n$, *então*

$$\left| \alpha_0 + \sum_{i=1}^{n} x_i \alpha_i \right| \geq \frac{\sqrt{d(\Lambda, y)^2 - Q} - T}{C},$$

ou $x_1 = \ldots = x_{n-1} = 0$ *e* $x_n = -\left\lceil \frac{C\alpha_0}{C\alpha_n} \right\rfloor$, *onde* $d(\Lambda, y)$ *é a distância de* y *à rede:*

$$d(\Lambda, y) = \min_{x \in \Lambda} |x - y|.$$

Lema 21. *(a) Para qualquer vetor não nulo* $x \in \Lambda$, *temos* $d(\Lambda) \geq \frac{|b_1|}{c_1}$, *onde* $c_1 = \max_{1 \leq i \leq n} \frac{|b_1|}{|b_i^*|}$.

(b) Considere $y \notin \Lambda$ *e escreva* $y = \sum_{i=1}^{n} y_i b_i$, *onde* $\{b_1, \ldots, b_n\}$ *é a base reduzida de* Λ, *e seja* i_0 *o maior índice tal que* $||y_i|| \neq 0$. *Então, para todo* $x \in \Lambda$ *temos* $|x - y| \geq ||y_{i_0}|| \frac{|b_1|}{c_1}$, *onde* $||\cdot||$ *é a distância para o inteiro mais próximo.*

Lema 22 (Dujella e Petho). *Seja* M *um inteiro positivo e* $\frac{p}{q}$ *um convergente da fração continua do irracional* γ *tal que* $q > 6M$ *e seja* μ *um número real. Seja* $\epsilon = k\mu|q - Mk\gamma|$, *onde* $|\cdot|$ *´e a distância até o inteiro mais próximo. Se* $\epsilon > 0$, *então não existe solução para* $0 < m\gamma - n + \mu < A \cdot B^{-k}$ *em inteiros positivos* m, n *e* k *com* $m \leq M$ *e* $k \geq \frac{\log(Aq/\epsilon)}{\log B}$.

Lema 23 (Kreutz). *Seja* α *a raiz dominante do polinômio característico associado a* $F_n^{(k)}$ *e* β *a raiz associada a* $F_m^{(l)}$. *Considere* $\beta < \alpha$ *e a seguinte forma linear* $\Lambda = f_l(\beta)\beta^{m-1} f_k(\alpha)^{-s} \alpha^{-ns} - 1$, *então*

$$|\Lambda| =< \frac{4}{1,32^n} + \frac{1}{1,32^s} < \frac{5}{1,32^t}$$

onde $t = \min\{n, s\}$.

Lema 24. *Se* $A \geq 3$ *e* $\frac{y}{\log^2 y} < A$, *então* $y < 16A \log^2 A$.

Demonstração. Como a função $f(y) = \frac{y}{\log^2 y}$ é crescente para $y > e^2$, suponha, por absurdo, que $y \geq 16A \log^2 A$. Daí,

$$\frac{y}{\log^2 y} \geq \frac{16A \log^2 A}{\log^2(16A \log^2 A)} > \frac{16A \log^2 A}{\log^2(A^4)} = A,$$

onde usamos o fato de que para $A \geq 3$, $16 \log^2 A < A^3$ e portanto $\log^2(16A \log^2 A) < \log^2(A^4) = 4 \log^2 A$. Mas isso contradiz a hipótese $\frac{y}{\log^2 y} < A$. □

4.2 Equação com potências de Fibonacci

Considere o n-ésimo número de Fibonacci F_n e o n-ésimo número de Tribonacci $F_n^{(3)} = T_n$. Nesse contexto, apresentamos o seguinte teorema:

Teorema 25. *Se (s, n, m) é solução para a equação*

$$T_n^s + T_{n+1}^s = F_m$$

com $s \geq 2$ e $n \geq 2$, então $(s, n, m) = (2, 2, 5)$.

A estratégia da demonstração deste teorema é a seguinte: Faremos uso de formas lineares em logaritmo em conjunto com o teorema 17 para estabelecer limites superiores e, em seguida, aplicaremos o algoritmo LLL em conjunto com o lema 21 para reduzir esses limites e encontra um campo viável de busca de soluções.

Demonstração. Usando diretamente o teorema 16 temos

$$s < 2,39 \cdot 10^{260},$$

$$n < 9,93 \cdot 10^{49},$$

$$m < 4,99 \cdot 10^{284}.$$

Considere α a raiz dominante do polinômio característico associado a T_n e β a raiz associada a F_m. Naturalmente sabemos que $\alpha > \beta$. Usando o lema 18 temos

$$\begin{aligned} \beta^{m-1} &\geq F_m = (T_n)^s + (T_{n+1})^s && (4.1)\\ &\geq \alpha^{(n-2)s} + \alpha^{(n-1)s} = \alpha^{(n-2)s}(1 + \alpha^s) && (4.2)\\ &> \alpha^{(n-2)s+s} = \alpha^{(n-1)s} > \beta^{(n-1)s} && (4.3) \end{aligned}$$

assim conseguimos $m - 1 > (n - 1)s$. Por outro lado, como $\sqrt{2} < \beta < \alpha < 2$,

$$\begin{aligned} (\sqrt{2})^{m-2} < \beta^{m-2} &\leq F_m = (T_n)^s + (F_{n+1})^s && (4.4)\\ &\leq \alpha\alpha^{(n-1)s} + \alpha^{ns} = \alpha\alpha^{ns}(\alpha^{-s} + 1) && (4.5)\\ &< \alpha^{ns} \cdot \alpha = \alpha^{ns+1} < 2^{ns+1} && (4.6) \end{aligned}$$

Obtendo assim $\frac{m-2}{2} < ns + 1$. Como resultado, chegamos à seguinte inequação envolvendo m, n e s:

$$(n - 1)s + 1 < m < 2(ns + 2). \tag{4.7}$$

Agora, pela fórmula de Binet para sequência de Fibonacci K-generalizada escrevemos

$$T_n = f_3(\alpha)\alpha^{n-1} + E_3(n)$$

$$F_m = f_2(\beta)\beta^{m-1} + E_2(m),$$

ainda, obtemos do lema 23,

$$|\Lambda_1| = |f_2(\beta)\beta^{m-1} f_3(\alpha)^{-s}\alpha^{-ns} - 1| < \frac{4}{1,32^n} + \frac{1}{1,32^s}$$

$$|\Lambda_1| = |f_2(\beta)\beta^{m-1} f_3(\alpha)^{-s}\alpha^{-ns} - 1| < \frac{5}{1,32^t} \tag{4.8}$$

com $t = min\{n, s\}$. Temos $\Lambda_1 \neq 0$, e para $\gamma_1 = f_2(\beta)$, $\gamma_2 = \beta$, $\gamma_3 = f_3(\alpha)$, $\gamma_4 = \alpha$, $b_1 = 1$, $b_2 = m-1$, $b_3 = -s$, e $b_4 = -ns$, de acordo com o Teorema 17, temos que

$$|\Lambda_1| > \exp(-1.02 \times 10^{19} \log(ns)).$$

Portanto,

$$t < 3.68 \times 10^{19} \log(ns).$$

Vamos dividir em dois casos: quando n é o mínimo e quando s é o mínimo.
Se $n \leq s$, então temos:

$$n < 3.68 \times 10^{19} \log(ns). \tag{4.9}$$

Considere agora a expressão linear em logaritmos dada por:

$$|\Lambda_2| = |f_2(\beta)\beta^{m-1} T_{n+1}^{-s} - 1| < \frac{2}{1.65^s}. \tag{4.10}$$

Pelo mesmo raciocínio utilizado anteriormente, concluímos que $\Lambda_1 \neq 0$, e portanto podemos aplicar o Teorema 17, com:

$$\begin{aligned}
&\gamma_1 = f_2(\beta),\\
&\gamma_2 = \beta,\\
&\gamma_3 = T_{n+1},\\
&b_1 = 1,\\
&b_2 = m-1,\\
&b_3 = -s.
\end{aligned}$$

Portanto,

$$|\Lambda_2| > \exp(-1.04 \times 10^{16} n \log(ns)).$$

Segue que,

$$s < 2.08 \times 10^{16} n \log(ns).$$

Usando o fato de que $n \leq s$, segue que

$$s < 4.16 \times 10^{16} n \log s.$$

Assim, pelo lema 19

$$s < 3.33 \times 10^{18} n \log n. \tag{4.11}$$

Utilizando esta inequação em (4.9), segue que

$$n < 3.68 \times 10^{19} \log\left(3.33 \times 10^{18} n^2 \log n\right),$$

e pelo lema 19 , temos

$$n < 5.4 \times 10^{21}.$$

Retornando à inequação (4.11), temos $s < 9 \times 10^{41}$ e $m < 2(ns+2) < 9.73 \times 10^{63}$.

Agora nosso objetivo é diminuir esses limites utilizando o algoritmo LLL. Primeiramente, vamos examinar a expressão linear:

$$\Gamma = \log f_2(\beta) + (m-1)\log\beta - s\log f_3(\alpha) - ns\log\alpha.$$

Se $\Gamma > 0$, então temos $0 < \Gamma < e^{\Gamma} - 1 < \frac{5}{(1,32)^n}$. Se $\Gamma < 0$, então temos que $|e^{\Gamma} - 1| < \frac{1}{2}$ para $n \geq 9$ (observe que o caso $n < 9$ pode ser tratado separadamente). Assim, para $\Gamma < 0$, temos $1 - e^{\Gamma} \leq |e^{\Gamma} - 1| < \frac{1}{2}$ e, portanto, $e^{|\Gamma|} = \frac{1}{e^{\Gamma}} < 2$. Logo,

$$0 < |\Gamma| < e^{|\Gamma|}|e^{\Gamma} - 1| < \frac{10}{(1,32)^t}.$$

Para evitar redundâncias desnecessárias, é aconselhável ponderar $\Gamma > 0$.

Com a notação na proposição 20, considere:

$$|x_1| = |m-1| \leq 9,73 \cdot 10^{63} = X_1$$

$$|x_2| = |s| \leq 9 \cdot 10^{41} = X_2$$

$$|x_3| = |ns| \leq 4.,86 \cdot 10^{63} = X_3$$

Agora escolhemos uma constante $C \geq X_3$, tal que $X = \max\{|X_1|, |X_2|, |X_3|\}$. Tomemos $C := 10^{200}$. Sendo $\lceil x \rfloor$ o inteiro mais próximo de x e α, β, respectivamente, as raizes dominantes dos polinômios característicos associados a T_n, F_m considere agora a matriz

$$B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \lceil 10^{200}\log\beta \rfloor & \lceil 10^{200}\log f_3(\alpha) \rfloor & \lceil 10^{200}\log\alpha \rfloor \end{pmatrix}$$

Com a ajuda do software Magma, computamos a base reduzida pelo LLL:

```
> R:=RealField(5);
> b1:=Log((1 + Sqrt(5))/2)*10^(200);
> b2:=Log(E)*10^(200);
> b3:=Log(A)*10^(200);
> B := RMatrixSpace(IntegerRing(), 3,3) ! [1, 0, b1, 0, 1, b2, 0, 0, b3];
> B;
[1 0 4812118250596034474977589134245315693609408376950596915935302956253492029\
4
    6487987132894412574749180482274935354696776488123379854413934549358748293\
71
    2664590348549953990640301700037124532854828648366081
[0 1 -4805875663167974071894948319644662077667216746621181692102669442575484123\
\
    8754157848611287365696548274994163073259934160304047079902813824679854668\
34
    4292480626070095888658210331182056677176125341827072]
[0 0 6093778634360062315368033711690339097303827879207347714727631205682810177\
4
    7255926686496058285980642652278361889651150117849202350433193472997247254\
89
    1219832242466783721610016907307003847406378937221121
> L1:= Lattice(B);
> L1;
Lattice of rank 3 and degree 3
Basis:
(1017472676151958 -184065038991413 0)
(598901865829974 883506998289615 0)
(265156058547131 180152308445814 -6038339879714466163586487329581230225467073\
95
    2666304685401930080392998659827438163337802760284254028066349400049222151\
83
    9632935407879668212098294802292313669839032523161 6)
> C:= LLL(B:Proof:=false);
> C;
[-598901865829974 -883506998289615 0]
[1017472676151958 -184065038991413 0]
[-265156058547131 -180152308445814 6038339879714466163586487329581230225467073\
9
    5266630468540193008039299865982743816333780276028425402806634940004922215\
18
    3963293540787966821209829480229231366983903252316 16]
>
```

Figura 4.1

Com o vetores $\{v_1, v_2, v_3\}$ encontrados da base LLL-reduzida, buscamos os vetores $\{b_1^*, b_2^*, b_3^*\}$ da base Gram-Schmidt associados:

```
> GramSchmidt3Vectors := function(v1, v2, v3)
function>     // Inicializa os vetores da base ortogonal
function>     v1_star := Vector(v1);
function>     mu_21 := InnerProduct(Vector(v2), v1_star) / InnerProduct(v1_sta\
r, v1_star);
function>     v2_star := Vector(v2) - Vector([ mu_21 * v1_star[i] : i in [1..3\
] ]);
function>
function>     mu_31 := InnerProduct(Vector(v3), v1_star) / InnerProduct(v1_sta\
r, v1_star);
function>     mu_32 := InnerProduct(Vector(v3), v2_star) / InnerProduct(v2_sta\
r, v2_star);
function>     v3_star := Vector(v3) - Vector([ mu_31 * v1_star[i] + mu_32 * v2\
_star[i] : i in [1..3] ]);
function>
function>     // Retorna a base de Gram-Schmidt
function>     return v1_star, v2_star, v3_star;
function> end function;
>
> // Exemplo de uso com trs vetores
> v1 := C[1];
> v2 := C[2];
> v3 := C[3];
> GramSchmidt3Vectors(v1, v2, v3);
(-598901865829974 -883506998289615                0)
(20218108541648141559899881609628865301574 80/2583374287803514605957582061
    -13705225824568700921111955510571331921496 48/2583374287803514605957582061 0)
(0 0 6038339879714466163586487329581230225467073952666304685401930080392998659\
8
    2743816333780276028425402806634940004922215183963293540787966821209829480\
22
    92313669839032523161 6)
```

Figura 4.2

E assim calculamos

$$\frac{|v_1|}{|b_1^*|} = 1, \quad \frac{|v_1|}{|b_2^*|} \leq 0.37, \quad \frac{|v_1|}{|b_3^*|} \leq 0.08$$

Seguindo o lema 21, podemos escolher $c_1 := 1$.

Agora considere $y = (0, 0, -\lceil 10^{200} \log f_2(\beta) \rfloor)$. Para utilizarmos o lema 21, precisamos escrever y na base $\{v_1, v_2, v_3\}$, por exemplo,

$$y = y_1 v_1 + y_2 v_2 + y_3 v_3$$

e encontrar o maior índice i, com $i \in \{1, 2, 3\}$, tal que $y_i \notin \mathbb{Z}$, e então calculamos a distância até o inteiro mais próximo, denotado por $|y_i|$, obtendo $|y_3| > 0.062$. Assim, pelo lema 21, temos

$$d(\Lambda, y) \geq 0.062 \cdot \frac{|v_1|}{1} > 7.316 \times 10^{64}.$$

Por fim, verificamos a condição $d(\Lambda, y)^2 > T^2 + Q$, para T e Q como definidos na proposição 20 e obtemos

$$|\Gamma| \geq \frac{\sqrt{d(\Lambda, y)^2 - Q} - T}{C} > 6.5 \times 10^{-136}.$$

Comparando com (4.8), e usando que $n \leq s$, obtemos $n \leq 1126$. Daí, $s < 2.64 \times 10^{22}$ e $m < 5.95 \times 10^{25}$.

Repetindo o processo por mais duas vezes (na primeira vez com $C := 10^{85}$ e na segunda com $C := 10^{80}$) obtemos

$$n \leq 456, \quad s < 9.3 \times 10^{21} \quad \text{e} \quad m < 8.5 \times 10^{24}.$$

Usar esse argumento mais vezes não nos dará melhores limitantes, por isso, agora atacaremos a forma linear dada em (4.10).

Neste caso, temos $\Lambda_2 = e^{\Gamma_2 - 1} > 0$, e portanto

$$0 < \Gamma_2 < e^{\Gamma_2} - 1 < \frac{2}{1.65^s},$$

com

$$\Gamma_2 = (m-1) \log \beta - s \log T_{n+1} + \log f_2(\beta).$$

Dividindo por $\log T_{n+1}$, segue que

$$0 < \frac{(m-1) \log \beta}{\log T_{n+1}} - s + \frac{\log f_2(\beta)}{\log T_{n+1}} < \frac{2}{\log 2} \cdot 1.65^{-s}.$$

Usaremos o método de redução dado pelo lema 22, onde

$$\gamma_n = \frac{\log \beta}{\log T_{n+1}}$$

é irracional,

$$\mu_n = \frac{\log f_2(\beta)}{\log T_{n+1}}, \quad A = \frac{2}{\log 2} \quad \text{e} \quad B = 1.65.$$

Também, com os limitantes obtidos anteriormente, temos $M := 8.5 \times 10^{24}$.

Agora considere $q_{n,r}$ o denominador do r-ésimo convergente da fração contínua associada a γ_n, obtemos:

$$\min_{2 \le n \le 456} q_{n,80} > 6M \quad \text{e} \quad q = \max_{2 \le n \le 456} q_{n,80} < 9.2 \times 10^{54}.$$

Ainda, com $\epsilon_n := \|\mu_n q_{n,80}\| - M\|\gamma_n q_{n,80}\|$, temos

$$\epsilon = \min_{2 \le n \le 456} \epsilon_n > 0.0067.$$

Pelo lema 22, segue que

$$s < \frac{\log(Aq/\epsilon)}{\log B} < 265.$$

Portanto, como estamos com $n \le s$, segue que $n < 265$ e $m < 2(ns + 2) < 140454$.

Seja agora $s < n$

Neste caso, $s < 3.68 \times 10^{19} \log(ns)$, e usando que $s < n$ temos

$$s < 7.36 \times 10^{19} \log n. \tag{4.12}$$

Considere agora a forma linear

$$|\Lambda_3| = |f_2(\beta)\beta^{m-1} f_3(\alpha)^{-s} \alpha^{-(n-1)s}(1 + \alpha^s)^{-1} - 1| < \frac{3}{1.32^n}. \tag{4.13}$$

Podemos escolher então $A_5 := 11s$. Dai, obtemos pelo Teorema 17:

$$|\Lambda_3| > \exp(-1.52 \times 10^{21} s \log(ns)),$$

assim,

$$n < 5.48 \times 10^{21} s \log(ns) \tag{4.14}$$

e portanto, utilizando $s < n$ em conjunto com (4.12), segue que

$$n < 8.07 \times 10^{41} \log^2 n.$$

Logo, pelo lema 24 , $n < 1.21 \times 10^{47}$ e, de (4.12), $s < 7.98 \times 10^{21}$. Assim, obtemos de (4.7) $m < 1.94 \times 10^{69}$. Como feito anteriormente, usaremos agora o algoritmo LLL com a forma linear:

$$0 < \log f_2(\beta) + (m-1)\log\beta - s\log f_3(\alpha) - ns\log\alpha < \frac{5}{1.32^s}.$$

Considere

$$|X1| = 1.94 \times 10^{69}$$

$$|X2| = 7.98 \times 10^{21}$$

$$|X3| = 9.66 \times 10^{68}$$

Escolha $C := 10^{220}$. Então, após os cálculos do Magma:

$$|\Gamma| \geq \frac{\sqrt{6.95 \times 10^{143} - 3.77 \times 10^{138}} - 1.46 \times 10^{69}}{10^{220}} > 8.3 \times 10^{-149}.$$

Obtendo assim, $s < 1233$. Como $n < 5.48 \times 10^{21} s\log(ns)$, temos $n < 4.63 \times 10^{26}$ e $m < 1.15 \times 10^{30}$. Repetindo o processo, obtemos $s \leq 567$ e daí $n < 2.08 \times 10^{26}$ e $m < 2.36 \times 10^{29}$.

Considere agora a forma linear dada por

$$\Gamma = \log f_2(\beta) - \log(1+\alpha^s) + (m-1)\log\beta - s\log f_3(\alpha) - (n-1)s\log\alpha.$$

Podemos considerar $\Gamma > 0$, pois o caso $\Gamma < 0$ é análogo. Assim, pela desigualdade (4.13), temos

$$0 < \Gamma < e^{\Gamma} - 1 = \Lambda_3 < \frac{3}{1.32^n}. \tag{4.15}$$

Assim, considere:

$$|x_1| = |m-1| \leq 2.36 \times 10^{29} = X_1$$

$$|x_2| = |s| \leq 567 = X_2$$

$$|x_3| = |(n-1)s| \leq 1.18 \times 10^{29} = X_3.$$

Devemos escolher uma constante $C \geq X^3$, onde $X = \max\{|X_1|, |X_2|, |X_3|\}$. Seja, $C := 10^{100}$.

Considere agora a matriz

$$B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \lceil (10^{100}\log\beta)\rfloor & \lceil (10^{100}\log f_3(\alpha))\rfloor & \lceil (10^{100}\log\alpha)\rfloor \end{pmatrix}$$

onde $\lceil x \rceil$ é o inteiro mais próximo de x. Agora aplicamos o algoritmo LLL a matriz acima e atravez do software Magma computamos a base LLL-reduzida:

```
> R:=RealField(5);
> b1:=Log((1 + Sqrt(5))/2)*10^(100);
> b2:=Log(E)*10^(100);
> b3:=Log(A)*10^(100);
> B := RMatrixSpace(IntegerRing(), 3,3) ! [1, 0, b1, 0, 1, b2, 0, 0, b3];
> B;
[1 0 4812118250596034474977589134249521031403695290152694448264723367422144794\
    1
92565413411500637525377024]
[0 1 -4805875663167974071894948319642420534589691062413959159097112584576251008\
    41107590479132021587810713 6]
[0 0 6093778634360062315368033711691899828479299560896207908187876455737166249\
    7
44831312034010940932358144]
> L1:= Lattice(B);
> L1;
Lattice of rank 3 and degree 3
Basis:
(687745227729566 299578434348834 0)
(774657687477584 -946370975223863 0)
(255002867364697 -162303631651794 -690174634679056378743475586227702545245110\
    89
72170386555162524223799296)
> C:= LLL(B:Proof:=false);
> C;
[687745227729566 299578434348834 0]
[774657687477584 -946370975223863 0]
[255002867364697 -162303631651794 -690174634679056378743475586227702545245110\
    89
72170386555162524223799296]
```

Figura 4.3

Para os vetores encontrados $\{v_1, v_2, v_3\}$ da base LLL-reduzida, encontramos os vetores da base de Gram-Schmidt associados $\{b_1^*, b_2^*, b_3^*\}$

```
> // Funo para calcular a base de Gram-Schmidt para trs vetores no R^3
> GramSchmidt3Vectors := function(v1, v2, v3)
function>     // Inicializa os vetores da base ortogonal
function>     v1_star := Vector(v1);
function>     mu_21 := InnerProduct(Vector(v2), v1_star) / InnerProduct(v1_sta\
r, v1_star);
function>     v2_star := Vector(v2) - Vector([ mu_21 * v1_star[i] : i in [1..3\
] ]);
function>
function>     mu_31 := InnerProduct(Vector(v3), v1_star) / InnerProduct(v1_sta\
r, v1_star);
function>     mu_32 := InnerProduct(Vector(v3), v2_star) / InnerProduct(v2_sta\
r, v2_star);
function>     v3_star := Vector(v3) - Vector([ mu_31 * v1_star[i] + mu_32 * v2\
_star[i] : i in [1..3] ]);
function>
function>     // Retorna a base de Gram-Schmidt
function>     return v1_star, v2_star, v3_star;
function> end function;
>
> // Exemplo de uso com trs vetores
> v1 := C[1];
> v2 := C[2];
> v3 := C[3];
> GramSchmidt3Vectors(v1, v2, v3);
(687745227729566 299578434348834                0)
(66126910886796196386562439628504750303470169/14068518414792281027720692697\
8
    -151808215053078554929704031948408648525604231/14068518414792281027720692\
69
    78 0)
(0 0 -690174634679056378743475586227702545245110897217038655516252422379929\
6)
```

Figura 4.4

e então obtemos

$$\frac{|v_1|}{|b_2^*|} < 0,61, \quad \frac{|v_1|}{|b_3^*|} < 0,01.$$

Pelo lema 21, podemos escolher $c_1 := 1$. Considere agora $y(s) = (0, 0, \lceil 10^{100}(\log f_2(\beta) - \log(1 + \alpha^s))\rfloor)$. Para aplicarmos o lema 21, precisamos expressar $y(s)$ na base $\{v_1, v_2, v_3\}$, por exemplo,

$$y(s) = y_1(s)v_1 + y_2(s)v_2 + y_3(s)v_3,$$

para todo $2 \leq s \leq 567$, e encontrar o maior índice i, $i \in \{1, 2, 3\}$ tal que $y_i(s) \notin \mathbb{Z}$, e então, calcular a distância até o inteiro mais próximo, denotado por $\|y_i(s)\|$. Ao fazer isso, obtemos

$$\min_{2 \leq s \leq 567} \|y_i(s)\| > 0.0011926103.$$

Assim, pelo lema 21, temos

$$d(\Lambda, y) \geq \|y_i(s)\| \cdot \frac{|v_1|}{c_1} > 0.0011926103 \cdot 1.31 \times 10^{33} > 1.56 \times 10^{30}.$$

Por fim, verificamos a condição $d(\Lambda, y)^2 > T^2 + Q$, para T e Q conforme definidos na proposição 20, e obtemos

$$|\Gamma| \geq \frac{\sqrt{d(\Lambda, y)^2 - Q} - T}{C} > 1.36 \times 10^{-70}.$$

Ao comparar com (4.15), temos $n \leq 583$, resultando em $m < 658794$.

Repetindo o processo para a mesma forma linear Γ, com

$$|x_1| = |m - 1| \leq 658794 = X_1$$

$$|x_2| = |s| \leq 567 = X_2$$

$$|x_3| = |(n - 1)s| \leq 329395 = X_3$$

e considerando $C := 10^{30}$, obtemos

$$|\Gamma| > 4.1 \times 10^{-23}.$$

Comparando com (4.15), temos $n < 189$, e portanto $m < 213574$. Podemos repetir o processo mais uma vez e obter $n < 174$. Repetir o processo outras vezes não nos dará limitantes melhores. Concluindo neste caso, como $s < n$, temos também $s < 174$, resultando em $m < 60556$. .

Portanto, em qualquer caso, resta usar o Magma para procurar as soluções com

$$2 \leq s \leq 265, \quad 2 \leq n \leq 265 \quad \text{e} \quad (n - 1)s + 1 < m < 2(ns + 2).$$

Após alguns dias de cálculo computacional, o Magma retorna como única solução $(s, n, m) = (2, 2, 5)$.

□

Referências

1. BREMNER, M. R., *Lattice Basis Reduction: An introduction to the LLL Algorithm and Its Applications*, Saskatoon, Canadá: CRC Press, 2012.

2. CHAVES, A. P., MARQUES, D., A Diophantine equation related to the sum of squares of consecutive k-generalized Fibonacci numbers, *The Fibonacci Quarterly*, v. 52, n. 1, p. 70-74, 2014.

3. CHAVES, A. P.; MARQUES, D., A Diophantine equation related to the sum of powers of two consecutive generalized Fibonacci numbers. *Journal of Number Theory*, v. 156, p. 1-14, 2015.

4. COHEN, H., *Number Theory: Analytic and Modern Tools*, Graduate Texts in Mathematics, France: Springer, v. 2, 2007.

5. COHEN, H., *Number Theory: Tools and Diophantine Equations*, Graduate Texts in Mathematics, France: Springer v. 1, 2007.

6. KREUTZ, Alessandra., *Soma de Potências de Números Consecutivos de Fibonacci k-Generalizados*. Tese de Doutorado - Programa de Pós-Graduação em Matemática, Universidade de Brasília, Brasília, 2019.

7. LUCA, F., RUIZ, C. A. G., An exponential Diophantine equation related to the sum of powers of two consecutive k-generalized Fibonacci numbers, *Colloquium Mathematicum*, v. 137, p. 171-188, 2014.

8. MILLER, M. D., On generalized Fibonacci numbers, *Amer. Math. Monthly*, v. 78, p. 1108-1109, 1971.

9. NGUYEN, P. Q.; VALLÉE, B., *The LLL Algorithm: Survey and Applications*, Paris, France: Springer, v. 1, 2010. ISSN 1619-7100.

10. SHOREY, T. N.; TIJDEMAN, R., *Exponential Diophantine Equations*, Cambridge Tracts in Mathematics, UK: Cambridge University Press, 2008.

11. SMART, N. P. The algorithmic resolution of Diophantine equations. Col: London Mathematical Society Student Texts. 41. [S.l.]: Cambridge University Press. 1998. ISBN 0-521-64156-X

12. STEEL, A.; CANNON, J.; BOSMA, W.; FIEKER, C., *Language and Data Structures*, Handbook of Magma Functions, 1nd ed. Sydney: 2013.

13. TIJDEMAN, Rob., *Linear Forms in Logarithms and Exponential Diophantine Equations*, Hardy-Ramanujan Journal 42, p. 32-34, jul. 2019. ISSN 9512-2300.

14. WALDSCHMIDT, M., *A lower bound for linear forms in logarithms*, Acta Arith. **37** (1980), 257-283.

15. WEGER, B. M. M., *Solving Exponential Diophantine Equations Using Lattice Basis Reduction Algorithms*, Journal of Number Theory, 26, p. 325-367, 1987.

16. WEGER, B. M. M.; PETHOR, A., *Products of prime powers in binary recurrence sequences, Part I: the hyperbolic case, with an application to the generalized Ramanujan-Nagell equation*, Math. Comput. **47** (1986), 713-727.

17. WOLFRAM, A., Solving generalized Fibonacci recurrences, *Fibonacci Quarterly*, v. 36, n. 2, p. 129-145, 1998.