Classificação dos Sub-Reticulados Não Equivalentes do Reticulado Hexagonal

Classification of the Sub-Reticulated Not Equivalent of the Hexagonal Reticulated

João Bosco Batista Lacerda
Departamento de Matemática
Universidade Federal da Paraíba - UFPB, João Pessoa, PB
boscolacerda@mat.ufpb.br

Antonio de Andrade e Silva
Departamento de Matemática
Universidade Federal da Paraíba - UFPB, João Pessoa, PB
andrade@mat.ufpb.br

Resumo: Neste trabalho apresentamos, de forma sucinta, um método para classificar todos os sub-reticulados de índice N, não equivalentes, do reticulado hexagonal no plano A_2.

Palavras-chave: código; reticulado ideal; reticulado primitivo.

Abstract: In this paper we present, in a succinctly way, a method to classify every sub- reticulated of nonequivalent index N, of hexagonal reticulated in the plan A_2.

Key words: code, ideal reticulated, primitive reticulated.

1 Introdução

A busca de melhores códigos sobre $\mathbb{Z}_2^n$ corresponde em $\mathbb{R}^n$ ao problema clássico do empacotamento esférico, ainda sem solução até hoje, de descobrir como juntar o maior número de esferas idênticas em uma grande região vazia. No ambiente de

Recebido em 05/01/2013 - Aceito em 28/04/2013.

$\mathbb{Z}_2^n$, o problema fica um pouco menos complicado quando se tem alguma estrutura algébrica no código. No caso do empacotamento de esferas em $\mathbb{R}^n$, a estrutura algébrica é a de reticulado, isto é, quando os centros das esferas formam um subgrupo discreto do $\mathbb{R}^n$. Um arranjo familiar é aquele em que os centros das esferas formam o reticulado cúbico de face centrada (usualmente encontrado em bancas de frutas), onde o espaço ocupado pelas esferas em um hangar é

$$\frac{\pi}{\sqrt{18}} = 0,7405\ldots$$

do espaço total, isto é, o número de esferas é $0,7405\ldots$ do volume do hangar, dividido pelo volume de uma esfera. Por isso, dizemos que esse empacotamento tem densidade $0,7405\ldots$ Gauss mostrou, em 1831, que dentre os empacotamentos reticulados em $\mathbb{R}^3$, esse é o mais denso. Em uma dimensão, o empacotamento mais denso é obviamente o reticulado $\mathbb{Z}$ e em duas dimensões é o reticulado hexagonal A_2, que é gerado pela base

$$\beta = \left\{(1,0), \left(-\frac{1}{2}, \frac{\sqrt{3}}{2}\right)\right\}$$

e cuja densidade é

$$\frac{\pi}{\sqrt{12}} = 0,9069\ldots$$

Mas esse problema não se reduz a 2 ou 3 dimensões e tem considerável importância prática em dimensões maiores que 3, e isso o torna um dos mais famosos problemas em aberto da matemática. A resposta para quais desses sub-reticulados apresenta a melhor densidade de empacotamento é totalmente respondida em Conway e Sloane[2]. Do ponto de vista da comunicação digital, especialmente celular e rádio, a busca de sub-reticulados de índice N tem como objetivo responder às seguintes questões: Quais sub-reticulados de índice N tem a maior norma mínima? Quais desses sub-reticulados tem a maior relação SNR (*signal noise ratio*)? Quais sub-reticulados possui uma região fundamental de energia mínima? O leitor interessado em mais detalhes pode consultar Bersntein et al[1].

2 Resultados básicos

Nesta seção apresentamos alguns resultados básicos sobre reticulados e teoria dos números que serão necessários ao desenvolvimento deste trabalho. O leitor interessado em mais detalhes pode consultar Cassels [3], Conway e Sloane [2] e Ribenboim [4].

Seja $\mathbb{R}^n$ o espaço Euclidiano n-dimensional. A norma quadrática $\mathbf{N}(\mathbf{v}) = ||\mathbf{v}||^2$ de um vetor $\mathbf{v} \in \mathbb{R}^n$ é a soma dos quadrados de suas componentes, isto é, $\mathbf{N}(\mathbf{v}) = (\mathbf{v},\mathbf{v}) = \mathbf{v}\mathbf{v}^t$, em que $(\mathbf{v},\mathbf{v})$ é o produto interno de $\mathbf{v}$ por $\mathbf{v}$. A distância Euclidiana quadrática entre dois vetores $\mathbf{u},\mathbf{v} \in \mathbb{R}^n$ é a norma quadrática de sua diferença, isto é,

$$d^2(\mathbf{u},\mathbf{v}) = \mathbf{N}(\mathbf{u}-\mathbf{v}) = ||\mathbf{u}-\mathbf{v}||^2 .$$

Uma esfera em $\mathbb{R}^n$, com centro $\mathbf{c}$ e raio ρ, consiste de todos os pontos $\mathbf{v} \in \mathbb{R}^n$ tais que $\mathbf{N}(\mathbf{v}-\mathbf{c}) = \rho^2$, isto é,

$$E_\rho(\mathbf{c}) = \{\mathbf{v} \in \mathbb{R}^n : \mathbf{N}(\mathbf{v}-\mathbf{c}) = \rho^2\}.$$

Um empacotamento esférico Λ em $\mathbb{R}^n$ de raio ρ consiste de uma sequência infinita de pontos $\mathbf{c}_1, \mathbf{c}_2, \ldots$ em $\mathbb{R}^n$, os centros das esferas, tais que

$$\mathbf{N}(\mathbf{c}_i - \mathbf{c}_j) \geq 4\rho^2, \quad \forall \ \ i \neq j.$$

O raio ρ é chamado de raio de empacotamento e, neste caso, $d^2_{\min}(\Lambda) = 4\rho^2$, em que $d^2_{\min}(\Lambda)$ é a distância Euclidiana quadrática mínima entre os elementos de Λ.

Um subgrupo aditivo de $\mathbb{R}^n$ é discreto se sua interseção com qualquer subconjunto limitado em $\mathbb{R}^n$ é finita. Um reticulado Λ é um subgrupo aditivo discreto de $\mathbb{R}^n$, ou, equivalentemente, os centros do empacotamento esférico formam um grupo aditivo finitamente gerado por um conjunto de vetores linearmente independentes do $\mathbb{R}^n$, denominado de base ou $\mathbb{Z}$-base. Um sub-reticulado Γ de um reticulado Λ é um subconjunto de elementos de Λ, que é também um reticulado. Restrigiremos os nossos estudos, sem perda de generalidade, aos reticulados do $\mathbb{R}^n$ cuja dimensão sejam igual a n. Assim, dada uma base $\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ do reticulado Λ a

matriz

$$\mathbf{M} = \left(\mathbf{u}_i : 1 \leq i \leq n\right),$$

cujas linhas são os vetores $\mathbf{u}_i$ chama-se uma matriz geradora do reticulado Λ e os elementos do reticulado Λ consistem de todos os vetores $\mathbf{vM}$, onde $\mathbf{v} \in \mathbb{Z}^n$. Em outras palavras, todo reticulado é um módulo sobre $\mathbb{Z}$. A matriz $G = \mathbf{M}^t\mathbf{M}$ chama-se de matriz de Gram.

Sejam Λ e Γ reticulados em $\mathbb{R}^n$. Diremos que Λ é similar a Γ se existir uma transformação ortogonal $T : \mathbb{R}^n \to \mathbb{R}^n$ e $r \in \mathbb{R} - \{0\}$ tal que $\Gamma = rT(\Lambda)$. Nesse caso, se Λ e Γ possuem matrizes geradoras $\mathbf{M}$ e $\mathbf{N}$, respectivamente, então

$$\mathbf{N} = r\mathbf{RMU},$$

em que $\mathbf{U}$ é uma matriz unimodular e $\mathbf{R}$ é uma matriz ortogonal. Quando $r = 1$, diremos que Λ é equivalente a Γ. Em particular, $\Gamma = \Lambda$ se, e somente se, $\mathbf{N} = \mathbf{UM}$.

Uma região em $\mathbb{R}^n$, que contém um e somente um ponto de cada classe lateral à direita (à esquerda) de Λ em $\mathbb{R}^n$, chama-se de região fundamental. Note que região fundamental não é única, mas toda região fundamental possui o mesmo volume, pois o volume é invariante por translação. O volume fundamental de um reticulado Λ é o volume de uma região fundamental, o qual será denotado por $V(\Lambda)$. Seja $\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ uma base do reticulado Λ. Então o conjunto

$$P = P(\mathbf{u}_1, \ldots, \mathbf{u}_n) = \left\{ \sum_{i=1}^{n} a_i \mathbf{u}_i : 0 \leq a_i < 1 \right\}$$

é uma região fundamental de Λ. A região fundamental P chama-se região fundamental básica de Λ. De forma análoga aos reticulados do plano, o volume deste sólido n-dimensional é dado por

$$V(P) = |\det \mathbf{M}|.$$

O determinante do reticulado Λ é definido como sendo o determinante da matriz

G, isto é,

$$\det \Lambda = \det G.$$

Apesar de um reticulado possuir várias matrizes de Gram diferentes, o determinante de cada uma delas é o mesmo e só depende do reticulado, ou seja, o determinante do reticulado Λ independe da base $\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ de Λ.

Sejam Λ um reticulado em $\mathbb{R}^n$ e Γ um sub-reticulado de Λ. Então

$$N = \frac{\det \Gamma}{\det \Lambda}$$

chama-se de índice de Γ em Λ. Agora, vamos nos restringir ao reticulado hexagonal A_2. Sejam Γ um sub-reticulado de A_2, $\{\mathbf{u}_1, \mathbf{u}_2\}$uma base de A_2 e $\{\mathbf{v}_1, \mathbf{v}_2\}$ uma base de Γ. Então existem únicos $b_{ij} \in \mathbb{Z}$ tais que

$$\begin{aligned} \mathbf{v}_1 &= b_{11}\mathbf{u}_1 + b_{21}\mathbf{u}_2 \\ \mathbf{v}_2 &= b_{12}\mathbf{u}_1 + b_{22}\mathbf{u}_2 \end{aligned}$$

Se $\mathbf{B} = \left[b_{ij} \right]$, então

$$N = \det \mathbf{B} \neq 0$$

é o índice de Γ em A_2. Pela Regra de Cramer, obtemos

$$\begin{aligned} N\mathbf{u}_1 &= c_{11}\mathbf{v}_1 + c_{21}\mathbf{v}_2 \\ N\mathbf{u}_2 &= c_{12}\mathbf{v}_1 + c_{22}\mathbf{v}_2 \end{aligned}$$

onde $c_{ij} \in \mathbb{Z}$. Portanto

$$NA_2 \subseteq \Gamma \subseteq A_2$$

em que

$$NA_2 = \{N\mathbf{u} : \mathbf{u} \in A_2\}$$

é um reticulado. Dessa forma, temos que $\{N\mathbf{u}_1, N\mathbf{u}_2\}$ é uma base de NA_2.

Vamos provar que se $\{\mathbf{u}_1, \mathbf{u}_2\}$ é uma base qualquer de A_2, então existe uma base

$\{\mathbf{v}_1, \mathbf{v}_2\}$ de Γ tal que

$$\begin{aligned} \mathbf{v}_1 &= a\mathbf{u}_1 \\ \mathbf{v}_2 &= b\mathbf{u}_1 + c\mathbf{u}_2 \end{aligned}$$

onde a, b, $c \in \mathbb{Z}$, $c > 0$ e $0 \leq b < a$. O leitor interessado no caso geral pode consultar [3][*Corollary* 1, página 13]. De fato, como $N\mathbf{u}_1, N\mathbf{u}_2 \in \Gamma$ temos que existem vetores $\mathbf{w}_1$ (por exemplo, $\mathbf{w}_1 = N\mathbf{u}_1$) e $\mathbf{w}_2$ em Γ tais que

$$\begin{aligned} \mathbf{w}_1 &= d_{11}\mathbf{u}_1 + d_{21}\mathbf{u}_2 \\ \mathbf{w}_2 &= d_{12}\mathbf{u}_1 + d_{22}\mathbf{u}_2 \end{aligned}$$

onde $d_{ij} \in \mathbb{Z}$, $d_{11} \neq 0$ e $d_{22} \neq 0$. Sendo assim, o conjunto

$$\Gamma_2 = \{b_2 \in \mathbb{Z} : v = b_1\mathbf{u}_1 + b_2\mathbf{u}_2, \ \forall \ \mathbf{v} \in \Gamma\}$$

é um sub-reticulado não nulo de $\mathbb{Z}$. Então existe um menor inteiro positivo $a_{22} \in \mathbb{Z}$ tal que $\Gamma_2 = \langle a_{22} \rangle$. Escolha $\mathbf{w}_2 \in \Gamma$ da forma

$$\mathbf{w}_2 = a_{21}\mathbf{u}_1 + a_{22}\mathbf{u}_2.$$

Analogamente, o conjunto

$$\Gamma_1 = \{b_1 \in \mathbb{Z} : \mathbf{v} = b_1\mathbf{u}_1 + b_2\mathbf{u}_2, \ \ b_2 = 0, \ \forall \ \mathbf{v} \in \Gamma\}$$

é um sub-reticulado não nulo de $\mathbb{Z}$. Então existe um menor inteiro positivo $a_{11} \in \mathbb{Z}$ tal que $\Gamma_1 = \langle a_{11} \rangle$. Escolha $\mathbf{w}_1 \in \Gamma$ da forma

$$\mathbf{w}_1 = a_{11}\mathbf{u}_1 \tag{2.1}$$

é fácil verificar que $\{\mathbf{w}_1, \mathbf{w}_2\}$ é uma base de Γ. Finalmente, pelo Algoritmo da Divi-

são, existem únicos q_1 e r_{21} tais que

$$a_{12} = q_1 a_{11} + r_{21}, \text{ com } 0 \leq r_{21} < a_{11}$$

e, assim,

$$\mathbf{w}_2 = q_1 a_{11}\mathbf{u}_1 + r_{21}\mathbf{u}_1 + a_{22}\mathbf{u}_2 \tag{2.2}$$

multiplicando (2.1) por $-q_1$ e somando com (2.2), obtemos a base desejada

$$\begin{aligned} \mathbf{v}_1 &= a_{11}\mathbf{u}_1 \\ \mathbf{v}_2 &= r_{21}\mathbf{u}_1 + a_{22}\mathbf{u}_2 \end{aligned}$$

onde $a_{11}, r_{21}, a_{22} \in \mathbb{Z}$, $a_{22} > 0$ e $0 \leq r_{21} < a_{11}$. A matriz triangular

$$\begin{pmatrix} a_{11} & 0 \\ r_{21} & a_{22} \end{pmatrix}$$

chama-se de forma normal de Hermite ou matriz particionadora.

Seja p um número primo. Diremos que um número $a \in \mathbb{N}$ é um resíduo quadrático módulo p quando a equação $x^2 \equiv a \pmod{p}$ possui solução, onde $x \in \{1, 2, \ldots, p-1\}$. Uma condição necessária e suficiente para que a seja um resíduo quadrático módulo p, $p > 2$ e mdc $(a, p) = 1$, é dada pelo teste de Euler, ou seja,

$$a^{\frac{p-1}{2}} \equiv 1 (\text{mod } p).$$

Sejam p um número primo ímpar e $a \in \mathbb{N}$ tal que mdc$(a, p) = 1$. O símbolo de Legendre é definido por

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{se } a \text{ é resíduo quadrado módulo p} \\ -1, & \text{caso contrário} \end{cases}$$

O símbolo de Legendre goza das seguintes propriedades:

(i) Se $a \equiv b \pmod{p}$, então $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(ii) $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$.

(iii) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

A propriedade (i) é uma consequência imediata da definição e (ii) decorre do teste de Euler. Podemos provar que 2 é um resíduo quadrado módulo p se, e somente se, $p \equiv \pm 1 \pmod 8$, ou seja,

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{2}}$$

e, pela propriedade (ii), concluímos que

$$2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} \pmod{p},$$

sendo assim, temos que

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{se } p \equiv 1,7 \pmod 8 \\ -1, & \text{se } p \equiv 3,5 \pmod 8 \end{cases}.$$

Portanto,

$$\left(\frac{4}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{2}{p}\right) = 1, \text{ se } p \equiv 1,3,5 \text{ ou } 7 \pmod 8.$$

Proposição 1 (Lagrange) Seja $f(x) = ax^2 + bx + c \in \mathbb{Z}[x]$ tal que $\text{mdc}(a, p) = 1$. Então

$$f(x) \equiv 0 \pmod{p}$$

possui no máximo duas raízes. Em particular, a congruência

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

possui soluções se, e somente se,

$$\Delta = b^2 - 4ac$$

é um resíduo quadrático módulo p, isto é,

$$\left(\frac{\Delta}{p}\right) \equiv \Delta^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Prova. Suponhamos, por absurdo, que a congruência

$$f(x) \equiv 0 \pmod{p}$$

tenha três soluções não congruentes módulo p, digamos x_1, x_2 e x_3. Então

$$\begin{aligned} f(x) - f(x_1) &= a(x^2 - x_1^2) + b(x - x_1) \\ &= (x - x_1)[a(x + x_1) + b]. \end{aligned}$$

Como

$$f(x_j) \equiv f(x_1) \pmod{p}, \quad j = 2, 3,$$

temos que

$$f(x_j) - f(x_1) = (x_j - x_1)[a(x_j + x_1) + b] \equiv 0 \pmod{p}.$$

Logo, a congruência linear

$$[ax + (b + ax_1)] \equiv 0 \pmod{p}$$

possui duas soluções não congruentes módulo p, o que é uma contradição.

Finalmente, como mdc $(a, p) = 1$ temos que

$$ax^2 + bx + c \equiv 0 \pmod{p} \Leftrightarrow x^2 + a^{-1}bx + a^{-1}c \equiv 0 \pmod{p}.$$

Logo,

$$\begin{aligned} x^2 + a^{-1}bx + a^{-1}c &\equiv x^2 + a^{-1}bx + \left[2^{-1}a^{-1}b\right]^2 - \left[2^{-1}a^{-1}b\right]^2 + a^{-1}c \\ &\equiv (x + 2^{-1}a^{-1}b)^2 - 2^{-2}a^{-2}(b^2 - 4ac). \end{aligned}$$

Portanto, a congruência

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

possuem soluções se, e somente se,

$$\Delta = b^2 - 4ac$$

é um resíduo quadrático módulo p, isto é,

$$\left(\frac{\Delta}{p}\right) \equiv \Delta^{\frac{p-1}{2}} \equiv 1 \pmod{p},$$

que é o resultado desejado.

Note que se

$$N = p_1^{k_1} \cdots p_n^{k_n} = \prod_{i=1}^{n} p_i^{k_i},$$

em que os p_i são números primos distintos, então resolver a congruência

$$f(x) \equiv 0 \pmod{N}$$

é equivalente, via Teorema Chinês dos Restos, resolver o sistema de congruências

$$f(x) \equiv 0 \pmod{p_i^{k_i}}, \quad i = 1, \ldots, n.$$

O leitor interessado em mais detalhes sobre o Teorema de Lagrange as observações a seguir pode consultar Sierpinski[6, página 239].

Observação 1: Note, pela Proposição 1, que o número de soluções da congruência

$$x^2 + x + 1 \equiv 0 \pmod{p}$$

pode ser escrito na forma

$$\left(1 + \left(\frac{p}{3}\right)\right)$$

se $p > 3$, pois $\Delta = -3$. Por exemplo, se $p = 7$, então $2^2 \equiv -3 \pmod 7$ e $x_1 = 2$, $x_2 = 4$ são as soluções não congruentes. Portanto, se

$$N = \prod_{i=1}^{n} p_i^{k_i},$$

então o número de soluções da congruência

$$x^2 + x + 1 \equiv 0 \pmod{N}$$

é dado por

$$\nu_1 = \begin{cases} 0, & \text{se } 2 \mid N \text{ ou } 9 \mid N \\ \prod\limits_{i=1, p_i > 3}^{n} \left(1 + \left(\frac{p_i}{3}\right)\right), & \text{casocontrário} \end{cases} . \tag{2.3}$$

Observação 2: Note, pela Proposição 1, que o número de soluções da congruência

$$x^2 - 1 \equiv 0 \pmod{p}$$

pode ser escrito na forma

$$\left(1 + \left(\frac{4}{p}\right)\right),$$

se $p \geq 3$, pois $\Delta = 4$. Por exemplo, se $p = 7$, então $2^2 \equiv 4 \pmod 7$ e $x_1 = -1$, $x_2 = 1$ são as soluções não congruentes. Portanto, se

$$N = \prod_{i=1}^{n} p_i^{k_i},$$

então o número de soluções da congruência

$$x^2 - 1 \equiv 0 \pmod{N}$$

é dado por $\mu = 2^{n-1+v_2}$, onde

$$v_2 = \begin{cases} 2, & \text{se } N \equiv 0 \pmod 8 \\ 1, & \text{se } N \equiv 1,3,4,5 \text{ ou } 7 \pmod 8 \\ 0, & \text{se } N \equiv 2 \text{ ou } 6 \pmod 8 \end{cases}, \tag{2.4}$$

pois na fatoração de N pode ocorrer primo par.

3 O reticulado hexagonal

Nesta seção apresentamos um método para classificar todos os sub-reticulados de índice N não equivalentes do reticulado hexagonal A_2.

Sejam F um corpo de número e $\sigma_i : F \to \mathbb{C}$, $i = 1, \ldots, n$, as F-imersões. Não é difícil verificar que os conjugados $\sigma_i(\alpha) = \alpha_i$ de α não necessitam ser elemento de F. Assim, dizemos que σ_i é real se $\sigma_i(F) \subseteq \mathbb{R}$, caso contrário, é complexo. É claro que se σ_i é complexo, então $\overline{\sigma}_i : F \to \mathbb{C}$ definida por $\overline{\sigma}_i(\beta) = \overline{\sigma_i(\beta)}$ é um homomorfismo injetivo tal que $\overline{\sigma}_i \neq \sigma_i$ e $\overline{\sigma}_i^2 = \sigma_i$. Assim, denotamos os homomorfismos reais por $\sigma_1, \ldots, \sigma_k$, os complexos por $\sigma_{k+1}, \overline{\sigma}_{k+1}, \ldots, \sigma_{k+l}, \overline{\sigma}_{k+l}$ e $n = k + 2l$.

Seja $\varphi : F \to \mathbb{R}^n$ definida por

$$\varphi(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_k(\alpha), \sigma_{k+1}(\alpha), \overline{\sigma}_{k+1}(\alpha), \ldots, \sigma_{k+l}(\alpha), \overline{\sigma}_{k+l}(\alpha)).$$

Então φ é um homomorfismo injetor e $\varphi(r\beta) = r\varphi(\beta)$, para todo $r \in \mathbb{Q}$ e $\beta \in F$. Em particular, se $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ é uma $\mathbb{Q}$-base para F, então $\{\varphi(\mathbf{v}_1), \ldots, \varphi(\mathbf{v}_n)\}$ é um conjunto linearmente independente sobre $\mathbb{R}$.

Seja $\mathbb{Z}[\omega]$ o anel dos inteiros de Eisenstein-Jacobi de $\mathbb{Q}[\omega]$, em que ω é a raiz cúbica da unidade. Como $\mathbb{Z}[\omega]$ é um domínio de ideais principais temos que todo

ideal de $\mathbb{Z}[\omega]$ é da forma

$$I = \langle a + b\omega \rangle = \{z(a + b\omega) : z \in \mathbb{Z}[\omega]\}.$$

Logo, se $z \in I$, então existe $c + d\omega \in \mathbb{Z}[\omega]$ tal que

$$\begin{aligned} z &= (a + b\omega)(c + d\omega) = c(a + b\omega) + d\omega(a + b\omega) \\ &= c(a + b\omega) + d(-b + (a - b)\omega) = c\mathbf{v}_1 + d\mathbf{v}_2, \end{aligned}$$

em que $\mathbf{v}_1 = a + b\omega$ e $\mathbf{v}_2 = -b + (a - b)\omega$. Assim,

$$\varphi(\mathbf{v}_1) = (a, b) \text{ e } \varphi(\mathbf{v}_2) = (-b, a - b).$$

Consequentemente, $\{\mathbf{v}_1, \mathbf{v}_2\}$ é uma base para I e

$$\Lambda = \varphi(I) = \{c\varphi(\mathbf{v}_1) + d\varphi(\mathbf{v}_2) : c, d \in \mathbb{Z}\}$$

é um reticulado em $\mathbb{R}^2$. Portanto, para cada ideal I de $\mathbb{Z}[\omega]$ o conjunto $\varphi(I)$ é um reticulado de $\mathbb{R}^2$. Mas a recíproca é, em geral, falsa. Não obstante, temos o seguinte resultado:

Proposição 2: Seja Λ um reticulado qualquer de $\mathbb{R}^2$. Se $\omega\beta \in I$, para todo $\beta \in I = \varphi^{-1}(\Lambda)$, então I é um ideal de $\mathbb{Z}[\omega]$. Neste caso, diremos que Λ é um reticulado ideal de $\mathbb{R}^2$.

Prova. Dados $\alpha, \beta \in I$, existem $\mathbf{x}, \mathbf{y} \in \Lambda$ tais que $\mathbf{x} = \varphi(\alpha)$ e $\mathbf{y} = \varphi(\beta)$. Logo,

$$\mathbf{x} - \mathbf{y} = \varphi(\alpha) - \varphi(\beta) = \varphi(\alpha - \beta) \Rightarrow \alpha - \beta \in \varphi^{-1}(\Lambda),$$

isto é, $\alpha - \beta \in I$. Como $\omega\alpha \in I$, para todo $\alpha \in I$, temos que $(a + b\omega)\alpha \in I$, para todos $a, b \in \mathbb{Z}$. Portanto, I é um ideal de $\mathbb{Z}[\omega]$.

O reticulado hexagonal A_2 em $\mathbb{R}^2$ é definido como

$$\Lambda = \varphi(\mathbb{Z}[\omega]) = \{c\varphi(1) + d\varphi(\omega) : c, d \in \mathbb{Z}\},$$

em que

$$\varphi(1)=(1,0) \text{ e } \varphi(\omega)=\left(-\frac{1}{2},\frac{\sqrt{3}}{2}\right)$$

(confira Figura 1). Assim, podemos identificar

$$(1,0)\leftrightarrow 1,\ (-\frac{1}{2},\frac{\sqrt{3}}{2})\leftrightarrow \omega \text{ e } (-\frac{1}{2},-\frac{\sqrt{3}}{2})\leftrightarrow \omega^2.$$

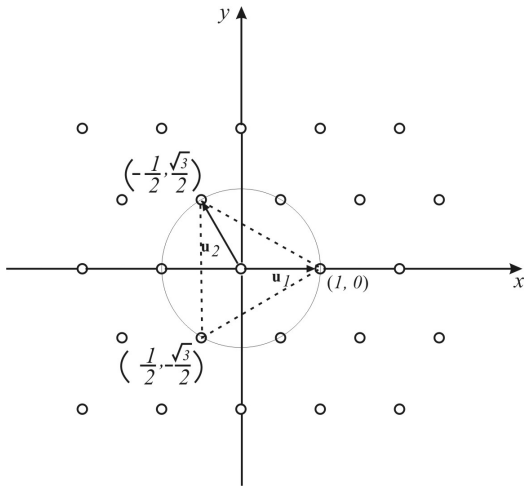

Figura 1. Reticulado hexagonal

Seja Γ um sub-reticulado de A_2 tal que $[A_2:\Gamma]=N$. Então existe uma matriz particionadora

$$\mathbf{B}=\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}$$

tal que $\det\mathbf{B}=ac=N$. Se

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

é a matriz geradora de A_2 e $\mathbf{N}$ é a matriz geradora de Γ, então

$$\mathbf{N} = \mathbf{BM} = \begin{pmatrix} a & 0 \\ b - \frac{1}{2}c & \frac{\sqrt{3}}{2}c \end{pmatrix},$$

isto é, Γ é gerado pelos vetores

$$\mathbf{v}_1 = (a, 0) \text{ e } \mathbf{v}_2 = \left(b - \frac{1}{2}c, \frac{\sqrt{3}}{2}c \right).$$

Como $\frac{A_2}{\Gamma}$ é um grupo abeliano, finitamente gerado, temos que $\frac{A_2}{\Gamma}$ é um grupo cíclico de ordem N ou $\frac{A_2}{\Gamma}$ é isomorfo a um produto direto $\mathbb{Z}_{\frac{N}{m}} \times \mathbb{Z}_m$ de grupos cíclicos, com m um fator de $\frac{N}{m}$. Neste caso, $m^2 \mid N$. Realmente, se $N = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$, $\alpha_i \geq 0$, então, pelo Algoritmo da Divisão, cada α_i pode ser escrito sob a forma:

$$\alpha_i = 2q_i + r_i, \text{ com } 0 \leq r_i < 2.$$

Sendo assim, teremos:

$$N = \left(p_1^{q_1} p_2^{q_2} \cdots p_n^{q_n} \right)^2 p_1^{r_1} p_2^{r_2} \cdots p_n^{r_n}.$$

Colocando $m = p_1^{q_1} p_2^{q_2} \cdots p_n^{q_n}$, obtemos o resultado. Diremos que Γ é um sub-reticulado primitivo de A_2 se $\frac{A_2}{\Gamma}$ for um grupo cíclico.

Teorema 1: Seja $N = \prod_{i=1}^{n} p_i^{k_i}$, com os p_i números primos distintos. Então o número de sub-reticulados primitivos não equivalentes de A_2 de índice N é

$$f_1(N) = \frac{1}{6} N \prod_{i=1}^{n} \left(1 + \frac{1}{p_i} \right) + \frac{\nu_1}{3} + 2^{n-2+\nu_2},$$

em que ν_1 é dado por (2.3) e ν_2 é dado por (2.4).

Prova. Nosso problema é equivalente a determinar todos os homomorfismos de $\mathbb{Z}$-módulos

$$\phi : A_2 \to \frac{\mathbb{Z}}{N\mathbb{Z}} = \mathbb{Z}_N,$$

pois $\ker\phi = \Gamma$ é um sub-reticulado de A_2. Como A_2 é gerado por 1 e ω temos que ϕ é completamente determinado por $\phi(1)$ e $\phi(\omega)$. Note que

$$\ker(r\phi) = \ker\phi, \quad \forall \quad r \in \mathscr{U}(\mathbb{Z}_N).$$

O número de sub-reticulados primitivos de índice N em um reticulado qualquer de $\mathbb{R}^2$ é dado pela função ψ [5][Theorem 8, p. 134]

$$\psi(N) = N\prod_{p|N}\left(1+\frac{1}{p}\right). \tag{3.5}$$

Como sub-reticulados equivalentes são invariantes por rotação e reflexão, temos que dividir a expressão (3.5) por 6. Além disso, devemos adicionar os sub-reticulados de A_2 que já tenham sido rotacionados ou reflexionados, nesse caso, devemos dividir somente por 2 ou 3, respectivamente. Assim, há dois casos a serem considerados:

1^o. **Caso**. Suponhamos que Γ tenha somente rotação. Então, sem perda de generalidade, podemos supor que:

$$\phi(1) = 1, \quad \phi(\omega) = x \quad \text{e} \quad \phi(\omega^2) = x^2,$$

em que

$$x^2 + x + 1 \equiv 0 \pmod{N},$$

pois

$$\phi(\omega^2 + \omega + 1) = \phi(0) = 0.$$

O número de soluções desta congruência, pela Observação 1, é dada por ν_1. Assim, o termo adicional é dado por

$$\left(\frac{1}{2} - \frac{1}{6}\right)\nu_1 = \frac{1}{3}\nu_1.$$

2^o. **Caso**. Suponhamos que Γ tenha somente reflexão. Então, sem perda de

generalidade, temos as seguintes possibilidades:

$$\begin{aligned}
\phi(1) &= 1,\ \phi(\omega)=x \text{ e } \phi(\omega^2)=-x-1,\\
\phi(1) &= -x-1,\ \phi(\omega)=1 \text{ e } \phi(\omega^2)=x,\\
\phi(1) &= x,\ \phi(\omega)=-x-1 \text{ e } \phi(\omega^2)=1,
\end{aligned}$$

em que

$$x^2-1\equiv 0 \pmod{N}.$$

Assim, pela Observação 2, o número de sub-reticulados não equivalentes é dado por

$$3\cdot 2^{n-1+\nu_2}.$$

Logo, o termo adicional é dado por

$$\left(\frac{1}{3}-\frac{1}{6}\right)3\cdot 2^{n-1+\nu_2}=2^{n-2+\nu_2}.$$

Portanto,

$$f_1(N)=\frac{1}{6}N\prod_{i=1}^{n}(1+\frac{1}{p_i})+\frac{\nu_1}{3}+2^{n-2+\nu_2}$$

é o número de sub-reticulados primitivos não equivalentes de A_2 de índice N.

Teorema 2: O número de sub-reticulados não equivalentes de A_2 com índice N é

$$f(N)=\sum_{m^2|N} f_1\left(\frac{N}{m^2}\right).$$

Prova. Seja Γ um sub-reticulado qualquer de A_2 com índice N. Então Γ pode ser escrito de modo único como

$$\Gamma = m\Gamma',$$

em que Γ' é um sub-reticulado primitivo de A_2 com índice $\frac{N}{m^2}$ em A_2, pois

$$[A_2:\Gamma]=N=m^2\cdot\frac{N}{m^2}$$

e, se

$$\mathbf{M} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

é a matriz geradora de Γ, então

$$\mathbf{M}' = \begin{pmatrix} \frac{a}{m} & \frac{b}{m} \\ \frac{c}{m} & \frac{d}{m} \end{pmatrix},$$

com $\mathbf{M} = m\mathbf{M}'$, é a matriz geradora de Γ'. Portanto,

$$f(N) = \sum_{m^2|N} f_1\left(\frac{N}{m^2}\right)$$

é o número de sub-reticulados não equivalentes de A_2 com índice N.

Teorema 3: Seja Γ um reticulado em $\mathbb{R}^2$ com matriz geradora

$$\mathbf{N} = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}, \quad a, b, c \in \mathbb{Z}.$$

Então:

1. O reticulado hexagonal A_2 contém uma cópia similar de Γ se, e somente se,

$$4ac - b^2 = 3m^2, \quad m \in \mathbb{Z}.$$

2. O reticulado hexagonal A_2 contém uma cópia de Γ se, e somente se,

$$4ac - b^2 = 3m^2, \quad m \in \mathbb{Z} \ \ e \ \ a = 3^k \prod_{p_i \equiv 1 \pmod 3} p_i^{l_i} \prod_{q_i \equiv -1 \pmod 3} q_i^{2m_i}.$$

Prova. (1) Seja $\Gamma' = \varphi^{-1}(\Gamma)$ uma cópia similar de Γ em A_2. Então existe $r \in \mathbb{Q}\ (\mathbb{Z})$ tal que

$$ac - \frac{b^2}{4} = r^2 \det \Gamma' = r^2 \frac{3}{4} N^2 \Leftrightarrow 4ac - b^2 = 3m^2, \quad m \in \mathbb{Z}.$$

(2) Como

$$4a\begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} = \begin{pmatrix} 2a & 0 \\ b & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 3m^2 \end{pmatrix}\begin{pmatrix} 2a & b \\ 0 & 1 \end{pmatrix},$$

temos que $4a\Gamma \subseteq A_2$. Portanto, $\Gamma \subseteq A_2$.

Teorema 4: Seja Γ um sub-reticulado qualquer de A_2 com índice N. Então $d^2_{\min}(\Gamma) \leq N$. Além disso, $d^2_{\min}(\Gamma) = N$ se, e somente se, Γ é um reticulado ideal.

Prova. Como A_2 é o reticulado mais denso em $\mathbb{R}^2$ temos que $d^2_{\min}(\Gamma) \leq N$, para todo sub-reticulado Γ de A_2.

4 Conclusão

Neste trabalho apresentamos um método para classificar todos os sub-reticulados de índice N não equivalentes do reticulado hexagonal A_2.

5 Referências

[1] BERNSTEIN, M.; SLOANE, N. J. A.; WRIGHT, P. E. On sublattices of the hexagonal lattice, *Discrete Math*, v.170, p. 29–39, 1997.

[2] CONWAY, J. H.; SLOANE, N. J. A. Sphere Packing, Lattices and groups. Springer-Verlag, 1993.

[3] CASSELS, J. W. S. An introdution to the geometry of number. Springer-Verlag, 1959.

[4] RIBENBOIM, P. Algebraic numbers, pure and applied mathematics, Queen's University Kingston, Ontario, Canadá. 1972.

[5] SCHOENEBERG, B. Elliptic modular functions. Springer-Verlag, 1974.

[6] SIERPINSKI, W. Elementary theory of numbers, North Holland, 1988.