UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
Câmpus de São José do Rio Preto

Gabriel Severino

Classificação de anéis quadráticos

São José do Rio Preto
2024

Gabriel Severino

Classificação de anéis quadráticos

Dissertação de Mestrado apresentada como parte dos requisitos para obtenção do título de Mestre em Matemática, junto ao Programa de Pós-Graduação em Matemática, do Instituto de Biociências, Letras e Ciências Exatas da Universidade Estadual Paulista “Júlio de Mesquita Filho”, Câmpus de São José do Rio Preto.

Orientador: Prof. Dr. Parham Salehyan

Financiadora: CAPES

São José do Rio Preto
2024

S498c

Severino, Gabriel
Classificação de anéis quadráticos / Gabriel Severino. -- São José do Rio Preto, 2024
147 p. : tabs.

Dissertação (mestrado) - Universidade Estadual Paulista (Unesp), Instituto de Biociências Letras e Ciências Exatas, São José do Rio Preto
Orientador: Parham Salehyan

1. Álgebra. 2. Teoria dos números. 3. Anéis quadráticos. 4. Domínios euclidianos. 5. Formas quadráticas. I. Título.

Sistema de geração automática de fichas catalográficas da Unesp. Biblioteca do Instituto de Biociências Letras e Ciências Exatas, São José do Rio Preto. Dados fornecidos pelo autor(a).

Essa ficha não pode ser modificada.

Gabriel Severino

Classificação de anéis quadráticos

Dissertação de Mestrado apresentada como parte dos requisitos para obtenção do título de Mestre em Matemática, junto ao Programa de Pós-Graduação em Matemática, do Instituto de Biociências, Letras e Ciências Exatas da Universidade Estadual Paulista “Júlio de Mesquita Filho”, Câmpus de São José do Rio Preto.

Financiadora: CAPES

Comissão Examinadora

Prof. Dr. Parham Salehyan
Orientador

Prof. Dr. Jéfferson Luiz Rocha Bastos
UNESP – Câmpus de São José do Rio Preto

Prof. Dr. Jaime Edmundo Apaza Rodriguez
UNESP – Câmpus de Ilha Solteira

São José do Rio Preto
06 de março de 2024

Aos meus país, minha irmã e aos meus amigos,
dedico

AGRADECIMENTOS

Terminado a dissertação, sinto que não poderia ter chegado aqui sozinho, por isso gostaria agradecer a todos que fizeram parte dessa jornada.

Agradeço aos meus pais, Luiz e Lourdes, e a minha irmã, Nayara, que sempre me proporcionaram apoio incondicional em todos os aspectos. É sem dúvidas devido a eles pude chegar aqui.

Agradeço a todos os professores, com os quais tanto aprendi, e aos servidores do IBILCE. Em especial agradeço ao meu orientador, Prof. Dr. Parham Salehyan.

Agradeço aos membros da Banca, Prof. Dr. Jaime Edmundo Apaza Rodriguez e Prof. Dr. Jéfferson Luiz Rocha Bastos, por terem aceitado fazer parte deste momento tão importante para mim.

Agradeço aos meus amigos: Lucas, Juninho, Arthur, Carlos, Vinícius e José Eduardo.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001, à qual agradeço pelo financiamento que possibilitou a realização deste trabalho.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

Matemática é a arte de dar o mesmo nome a coisas diferentes.
Henri Poincaré

RESUMO

O objetivo deste estudo é classificar todos os anéis quadráticos norma euclidianos, isto é, classificar quais anéis quadráticos são um domínio euclidiano cuja função euclidiana seja o valor absoluto da função norma padrão definidas sobre anéis quadráticos.

Palavras-chave: Álgebra. Teoria dos números. Anéis quadráticos norma euclidianos.

ABSTRACT

The objective of this study is to classify all Norm-Euclidean quadratic rings, that is, to classify which quadratic rings are Euclidean domains whose Euclidean function is the absolute value of the standard norm defined on quadratic rings.

Keywords: Algebra. Number theory. Norm-Euclidean quadratic rings.

Lista de Tabelas

Sumário

1 Introdução

Diante da perspectiva atual, o algoritmo de Euclides é a base da teoria elementar dos números. Hoje sabemos que a propriedade euclidiana em um domínio implica em uma série de outras propriedades como, por exemplo, a fatoração única. Apesar de sabermos que Algoritmo de Euclides já era utilizado por Euclides para calcular o maior divisor comum entre dois números, quão perto Euclides chegou de compreender a propriedade da fatoração única dos inteiros é motivo de debate entre historiadores da matemática.

Durante a Idade Média, matemáticos árabes e europeus estudaram os fatores primos de número inteiros e perceberam que uma lista de todos os fatores de um número n poderia ser produzida a partir de sua fatoração prima. Como por exemplo o matemático suíço Leonhard Euler que apesar de não declarar propriamente o teorema da fatoração única, apresenta um método para decompor qualquer número em seus fatores primos. O método era simplesmente dividir pelo diferentes primos até encontrar todos os fatores primos (COLLISON, 1980). No entanto, a hipótese mais aceita de quem deu a primeira declaração clara de fatoração única como conhecemos hoje foi devida a Gauss, em 1801, apresentado no artigo 16 de Disquisitiones Arithmeticae.

Mesmo atualmente dizer se um domínio possui fatoração única é ainda uma tarefa desafiadora, como por exemplo, dizer quando um anel quadrático é um domínio de fatoração única. A classificação de anéis quadráticos que possuem fatoração única ainda é um problema em aberto, mas parcialmente resolvido. Para anéis quadráticos imaginários $\mathcal{O}_d$, Gauss demonstrou quando $d = -1, -2, -3, -7, -11, -19, -43, -67$ ou -167, $\mathcal{O}_d$ forma um domínio de fatoração única. Gauss também conjecturou que esses são os únicos anéis quadráticos complexos com essa propriedade, posteriormente provada verdadeira por H. Stark em [27]. No entanto, para corpos quadráticos reais, ou seja, para $d > 0$, a questão permanece sem solução. Atualmente, não se sabe se existem infinitos anéis quadráticos que apresentam fatoração única, apesar de Gauss ter conjecturado que sim. Com isso em mente, neste trabalho abordaremos um caso mais simples do problema, a classificação de anéis quadráticos norma euclidianos, isto é, anéis quadráticos que possuem o algoritmo euclidiano, onde a função euclidiana é o valor absoluto da norma.

O Capítulo 2 tem por objetivo introduzir os conceitos relacionados a corpos quadráticos e corpos quadráticos euclidianos bem como notação relacionados a eles.

O objetivo principal do Capítulo 3 é classificar todos os anéis quadráticos complexos euclidianos, não apenas norma euclidianos. Iniciamos demonstrando que $\mathcal{O}_d$ é euclidiano para os valores $d = -1, -2, -3, -7, -11$. Em seguida demonstraremos que eles são os únicos anéis quadráticos complexos que são domínios euclidianos. Por fim, daremos uma demonstração elementar da existência de anéis quadráticos não euclidiano que são domínios de fatoração única.

A partir do Capítulo 4 iniciaremos a classificação dos anéis quadráticos reais norma

euclidianos. No capítulo exploraremos um pouco a teoria das formas quadráticas binárias, mostraremos que dado um corpo quadrático $\mathbb{Q}(\sqrt{d})$ sempre podemos associá-lo a uma forma quadrática binária $N_d(x, y)$. Daremos condições sobre $N_d(x, y)$ a fim de que $\mathcal{O}_d$ seja euclidiano e desenvolveremos resultados sobre as formas associadas com a finalidade de demonstrar que $\mathcal{O}_d$ é euclidiano para $d \in \{2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\}$.

No Capítulo 5, desenvolveremos mais resultados sobre formas binárias quadráticas, inicialmente, demonstraremos que dado uma forma quadrática binária $f(x, y)$, com discriminante positivo diferente de um quadrado perfeito, existem números reais x_0 e y_0 tais que para todos x e y inteiros $|f(x+x_0, y+y_0)| > \frac{1}{128}\sqrt{\delta}$, onde δ é o discriminante de $f(x, y)$. Posteriormente, diante da suposição de que os coeficientes de $f(x, y)$ são inteiros, mostraremos que x_0 e y_0 podem ser considerados números racionais e a partir daí concluiremos que para todo inteiro d livres de quadrados tais que $d \geq 128^2$, $|N_d(x + x_0, y + y_0)| > 1$, o que é uma condição suficiente para que o anel quadrático $\mathcal{O}_d$ não seja euclidiano, assim, demonstraremos que somente há anéis quadráticos norma euclidianos $\mathcal{O}_d$ para valores abaixo d abaixo de 128^2.

No capítulo seguinte classificaremos os anéis quadráticos reais, este será dividido em três seções. Na Seção 6.1 classificaremos os anéis quadráticos com discriminante 2 ou 3 módulo 4. Daremos uma demonstração elementar sobre a finitude de anéis quadráticos euclidianos $\mathcal{O}_d$ com discriminante $d \equiv 2, 3 \pmod 4$, com uma cota superior muito melhor que a desenvolvida no Capítulo 5 e finalizaremos demonstrando que os únicos valores para o qual $\mathcal{O}_d$ é um anel quadrático norma euclidiano, com $d \equiv 2, 3 \pmod 4$, são $d = 2, 3, 6, 7, 11, 19$.

Na Seção 6.2 lidaremos com anéis quadráticos com discriminante composto congruente a 1 módulo 4. Demonstraremos que os únicos anéis quadráticos norma euclidiano $\mathcal{O}_d$ com d composto são 21, 33 e 57. Esta seção será dividida em três partes. Na primeira subseção demonstraremos que um anel quadrático $\mathcal{O}_d$, com $d \equiv 1 \pmod 4$, só pode ser euclidiano quando d é um primo ou quando d é o produto de primos p e q satisfazendo $p \equiv q \equiv 3 \pmod 4$. Na segunda subseção demonstraremos que não há corpos quadráticos quando $d = pq$ com $3 < p < q$. Por fim, na terceira subseção lidaremos com os casos $d = 3p$.

Por fim, na Seção 6.3 lidaremos com a classificação de anéis quadráticos $\mathcal{O}_p$ com discriminante primo congruente a 1 módulo 4. Dividiremos sua análise em quatro casos $p \equiv 1,\ 5,\ 13,\ 17 \pmod{24}$. Na primeira subseção, lidaremos com o caso $p \equiv 5 \pmod{24}$. Posteriormente, na segunda subseção, lidaremos com o casos $p \equiv 13 \pmod{24}$, com exceção dos casos 61 e 109, será utilizada uma abordagem computacional. Para os anéis $\mathcal{O}_{61}$ e $\mathcal{O}_{109}$ será possível demonstrar a existência de um módulo não euclidiano em cada um dos casos. Na terceira subseção, trabalharemos com o caso $p \equiv 17 \pmod{24}$, as bordagens que serão utilizadas serão semelhante à utilizada na seção anterior. Por fim, na última subseção, lidaremos com o caso $p \equiv 1 \pmod{24}$. Com exceção dos casos 97, 193, 241, 313, 337, 457 e 601, podemos será utilizado uma abordagem computacional. Para o caso $p = 97$, mostraremos a existência de um elemento que contradiz a existência do algoritmo euclidiano em $\mathcal{O}_d$. Os casos 193, 241, 313, 337, 457 e 601 serão tratados através da utilização da teoria desenvolvida no Capítulo 5 com devidas adaptações.

2 Conceitos iniciais

Neste capítulo introduziremos os conceitos básicos que serão utilizados ao longo do texto. Na primeira seção definiremos o que é um resíduos quadrático e o símbolos de Legendre. Posteriormente estenderemos o símbolo de Legendre aos chamados símbolos de Jacobi e Kronecker. Na segunda seção definiremos algumas terminologias e notações sobre anéis comutativos. Na seção seguinte definiremos o que é o conjunto dos inteiros algébricos de um anel e mostraremos que esse conjunto também possui uma estrutura de anel. O restante do capítulo será focado nos corpos quadráticos e anéis quadráticos (anel dos inteiros algébrico de um corpo quadrático). O objetivo principal será caracterizar os anéis quadráticos e definir o que é um anel quadrático euclidiano norma euclidiano.

2.1 Símbolo de Legendre, Símbolo de Jacobi e Símbolo de Kronecker

Nesta seção introduziremos conceitos sobre os símbolos de Legendre, Jacobi e Kronecker.

Definição 2.1. Sejam a, d inteiros. Dizemos que d é um resíduo quadrático módulo a se a equação

$$X^2 \equiv d \ (mod\ a)$$

admite solução, em outras palavra $\bar{d}$ é um quadrado perfeito módulo a.

Definição 2.2. Seja $p > 2$ um número primo e a um inteiro qualquer. Definimos o chamado símbolo de Legendre:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 \text{ se } p \nmid a \text{ e } a \text{ é um resíduo quadrático módulo } p \\ 0 \text{ se } p \mid a \\ -1 \text{ caso contrário.} \end{cases}$$

Proposição 2.3. *Seja $p > 2$ um primo e a um inteiro qualquer. Então*

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

Demonstração: Veja [4], Proposição 2.8. ■

Proposição 2.4. *O símbolo de Legendre possui as seguintes propriedades:*

1. *se $a \equiv b \pmod{p}$ então $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.*

2. $\left(\frac{a^2}{p}\right) = 1$ *se* $p \nmid a$.

3. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, *ou seja, -1 é um resíduo quadrático módulo p se, e somente se,* $p \equiv 1 \pmod 4$.

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

Demonstração: Veja [4], Corolário 2.9. ■

Teorema 2.5 (Reciprocidade quadrática)**.**

1. *Sejam p e q primos ímpares distintos. Então*

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

2. *Seja p um primo ímpar. Então*

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

Demonstração: Veja [4], Teorema 2.11. ■

O símbolo de Legendre $\left(\frac{a}{p}\right)$ pode ser estendido para o símbolo de Jacobi $\left(\frac{a}{n}\right)$, que está definido para todo inteiro arbitrário a e todo inteiro positivo ímpar por

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1}\left(\frac{a}{p_2}\right)^{\alpha_2}\ldots\left(\frac{a}{p_k}\right)^{\alpha_k}$$

se $n = p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_k}$ é a fatoração prima de n (onde $\left(\frac{a}{p_j}\right)$ são dados pelos símbolos de Legendre usual), além disso, definimos $\left(\frac{a}{1}\right) = 1$, para todo inteiro a.

Proposição 2.6. *O símbolo de Jacobi possui as seguintes propriedades*

1. *Se* $a \equiv b \pmod n$ *então* $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.

2. $\left(\frac{a}{n}\right) = 0$ *se* $mdc(a,n) \neq 1$ *e* $\left(\frac{a}{n}\right) \in \{-1,1\}$ *se* $mdc(a,n) = 1$.

3. $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$; *em particular,* $\left(\frac{a^2}{n}\right) \in \{0,1\}$.

4. $\left(\frac{a}{nm}\right) = \left(\frac{a}{n}\right)\left(\frac{a}{m}\right)$, *em particular* $\left(\frac{a}{n^2}\right) \in \{0,1\}$.

5. *Se m e n são positivos e ímpares, então* $\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}\left(\frac{n}{m}\right)$.

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

7. $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$.

Ainda podemos generalizar o símbolo de Jacobi ao chamado símbolo de Kronecker. Defina

$$\left(\frac{a}{2}\right) = \begin{cases} 1 \text{ se } a \equiv \pm 1 \pmod 8 \\ 0 \text{ se } 2 \mid a \\ -1 \text{ se } a \equiv \pm 3 \pmod 8 \end{cases}$$

e

$$\left(\frac{a}{-1}\right) = \begin{cases} 1 \text{ se } a > 0 \\ 0 \text{ se } a = 0 \\ -1 \text{ se } a < 0 \end{cases}$$

e se $n = u \cdot p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, onde $u = \pm 1$, então símbolo de Kronecker é dado por

$$\left(\frac{a}{n}\right) = \left(\frac{a}{u}\right)\left(\frac{a}{p_1}\right)^{\alpha_1}\left(\frac{a}{p_2}\right)^{\alpha_2} \dots \left(\frac{a}{p_k}\right)^{\alpha_k}.$$

2.2 Anéis comutativos

Nesta seção introduziremos conceitos básicos sobre anéis comutativos.

Definição 2.7. Seja A um anel comutativo com unidade 1, um subconjunto I de A é chamado um ideal de A se

1. I é um subgrupo aditivo de A;
2. I é fechado por multiplicação por elementos arbitrários de A, isto é, se $a \in I$ e $r \in A$ então $ra \in I$.

Definição 2.8. Se I é um ideal do anel A, dizemos que a é congruente a b módulo I, e denotamos por $a \equiv b \pmod I$, se $a - b \in I$. Quando $I = \langle c \rangle$ utilizaremos a notação $\pmod c$.

Definição 2.9. Se I é um ideal de A, então para toda $a \in A$ definimos a classe de resíduos de a módulo I como $\overline{a} = a + I = \{a + x : \ x \in I\}$.

Teorema 2.10. *Seja I um ideal do anel A. Então o conjunto das classes de resíduos módulo I forma um anel sob as operações $\overline{a} + \overline{b} = \overline{a+b}$ e $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$. Este anel é dito anel quociente de A por I e será denotado por A/I.*

Definição 2.11. Um anel comutativo com unidade D é dito um domínio ou domínio de integridade se ele satisfaz a seguinte condição:

$$\forall x, y \in D \setminus \{0\}, \ x \cdot y \neq 0.$$

Definição 2.12. Seja D um domínio:

1. Dizemos que a divide b, denotado por $b \mid a$, se existe $c \in D$ tal que $a = bc$.
2. Dizemos que u é uma unidade em D se $u \mid 1$. Denotaremos o conjunto das unidade de D por $U(D)$.
3. Dizemos que c é um divisor comum de a e b se $c \mid a$ e $c \mid b$.

4. Dizemos que c um maior divisor comum (mdc) de a e b se $c \neq 0$ e para qualquer outro divisor comum c' de a e b vale $c' \mid c$.

5. Se 1 é um maior divisor comum de a e b dizemos que a e b são relativamente primos.

6. Se $a = ub$ para alguma unidade $u \in D$ dizemos a e b são associados.

7. Se $a \neq 0$ não é uma unidade, dizemos que a é irredutível se para todo $b, c \in D$ tal que $a = bc$ implicar que b ou c é uma unidade.

8. Se $p \neq 0$ não é uma unidade, dizemos que p é primo se para todo $a, b \in D$ tal que $p \mid ab$ implicar que $p \mid a$ ou $p \mid b$.

Proposição 2.13. *Em D elementos primos são sempre irredutíveis.*

Definição 2.14. Seja A um anel. Um ideal I de A é dito um ideal principal se existe $\alpha \in A$ tal que $I = \langle \alpha \rangle$. Um domínio no qual todo ideal é principal é chamado de domínio de ideais principais.

Definição 2.15. Um domínio D é um domínio de fatoração única se todo elemento não-nulo e não-invertível de D se escreve de maneira única como produto de elementos irredutíveis de D, isto é, de maneira mais precisa:

1. Todo elemento não-nulo e não-invertível de D é produto finito de fatores irredutíveis.

2. Se $\{p_i\}_{1 \leq i \leq s}$ e $\{q_j\}_{1 \leq j \leq t}$ são famílias finitas de elementos irredutíveis de D tais que $p_1 \dots p_s = q_1 \dots q_t$, então

   - $s = t$.
   - a menos da ordenação, p_i é associado a q_i, $\forall i = 1, \dots, s$ (isto é, existe uma bijeção σ de $\{1, \dots, s\}$ sobre $\{1, \dots, s\}$ tal que p_i é associado a $q_{\sigma(i)}$, $\forall i = 1, \dots, s$).

Definição 2.16. Um domínio euclidiano (D, ϕ) é um domínio de integridade D com uma função

$$\phi : D \setminus \{0\} \to \mathbb{N} = \{0, 1, 2, \dots\}$$

que satisfaz as seguintes propriedades:

1. $\forall a, b \in D, b \neq 0$, existem $t, r \in D$ tais que

$$a = bt + r \text{ com } \begin{cases} \phi(r) < \phi(b) \\ \text{ou } r = 0. \end{cases}$$

2. $\phi(a) \leq \phi(ab)$, $\forall a, b \in D \setminus \{0\}$.

Chamaremos ϕ de função euclidiana sobre D.

Exemplo 2.17. Seja $|\ | : \mathbb{Z} \to \mathbb{N}$ a função valor absoluto. Então $(\mathbb{Z}, |\ |)$ é um domínio euclidiano.

Exemplo 2.18. Seja K um corpo e seja $K[x]$ o anel de polinômios numa variável sobre K. Seja $\partial : K[x] \setminus \{0\} \to \mathbb{N}$ a função grau do polinômio. Então $(K[x], \partial)$ é um domínio euclidiano.

Proposição 2.19. *Todo domínio euclidiano é um domínio de ideais principais.*

Proposição 2.20. *Todo domínio de ideais principais é um domínio de fatoração única.*

Corolário 2.21. *Todo domínio euclidiano é um domínio de fatoração única.*

2.3 Elementos integrais sobre um anel

Nesta seção mostraremos que o conjunto dos elementos integrais sobre um anel é também um anel. Mas antes introduziremos o conceito de A-módulo, uma generalização do conceito de espaço vetorial sobre um corpo K.

Definição 2.22. Sejam B um anel e A um subanel de B. Diremos que um elemento $\alpha \in B$ é integral sobre A se existir um polinômio mônico $f \in A[x]$ tal que $f(\alpha) = 0$. Em outras palavras, α satisfaz uma equação da seguinte forma:

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0,$$

onde $a_i \in A, \forall i = 0, \ldots, n-1$.

Definição 2.23. Seja A um anel com unidade. Diz-se que um conjunto não vazio M é um A-módulo se M é um grupo abeliano em relação a uma operação $+$ e munido de uma operação externa (escrita como multiplicação) que a cada par $(\alpha, m) \in A \times M$ associa um elemento $\alpha m \in M$ e tal que, para todos $\alpha_1,\ \alpha_2 \in A$ e todos $m_1,\ m_2 \in M$, verifica:

1. $\alpha_1(\alpha_2 m_1) = (\alpha_1\alpha_2)m_1$;
2. $\alpha_1(m_1 m_2) = \alpha_1 m_1 + \alpha_1 m_2$;
3. $(\alpha_1 + \alpha_2)m_1 = \alpha_1 m_1 + \alpha_2 m_1$;
4. $1 \cdot m_1 = m_1$.

Exemplo 2.24.

1. Todo espaço vetorial sobre um corpo K é um K-módulo.
2. Todo anel pode ser considerado como um módulo sobre si mesmo.

Definição 2.25. Seja um A-módulo M.

1. Um elemento $m \in M$ é uma combinação linear dos elementos $m_1, \ldots, m_n \in M$ se existirem elementos $a_1, \ldots, a_n \in A$ tais que
$$m = a_1 m_1 + \cdots + a_n m_n.$$
2. Seja β um subconjunto de M. Diremos que β é um conjunto gerador de M (ou β gera M) se todo elemento de M for uma combinação linear de um número finito de elementos de β. Se β for um conjunto finito diremos que M é um A-módulo finitamente gerado.
3. Seja β um subconjunto de M. Diremos que β é linearmente independente (ou $l.i$) se $a_1 v_1 + \cdots + a_n v_n = 0$, para todos $v_i \in \beta$ e $a_i \in A, i = 1, \ldots, n$, implicar que $a_1 = \cdots = a_n = 0$.
4. Um subconjunto β de elementos de um A-módulo M diz-se uma base de M se é linearmente independente e β gera M.
5. O A-módulo M diz-se livre se ele contém uma base.

Exemplo 2.26. Todo espaço vetorial V sobre um corpo K de dimensão finita é um K-módulo finitamente gerado. Qualquer base de V forma um conjunto gerador.

Definidos os conceitos de A-módulos, o objetivo do teorema seguinte será caracterizar os elementos integrais de um anel B sobre um subanel A.

Teorema 2.27. *Sejam B um anel e A subanel de B. Então para qualquer $\alpha \in B$ as seguintes condições são equivalentes:*

1. *α é integral sobre B.*
2. *O anel $A[\alpha] \coloneqq \{f(\alpha) |\ f \in A[x]\}$ é um A-módulo finitamente gerado.*
3. *Existe um subanel C de B tal que $A[\alpha] \subset C$ e é um A-módulo finitamente gerado.*

Demonstração: (1) $\Rightarrow$ (2) : Como $\alpha \in B$ é integral sobre A, existem $a_1, a_1, \ldots, a_n \in A$, tais que

$$\alpha^n + a_n\alpha^{n-1} + \cdots + a_1\alpha + a_1 = 0.$$

Portanto,

$$\alpha^n = -(a_n\alpha^{n-1} + \cdots + a_1\alpha + a_0) \tag{2.1}$$

e dessa forma α^n pertence ao A-módulo finitamente gerado por $1, \alpha, \ldots, \alpha^n$. Por indução e pela expressão 2.1, segue que toda potência α^m, $m \in \mathbb{N}$, pertence ao A-módulo $A[\alpha, \alpha^2 \ldots, \alpha^{n-1}]$. Donde segue a igualdade $A[\alpha] = A + A(\alpha) + A(\alpha^2) + \cdots + A(\alpha^{n-1})$.
(2) $\Rightarrow$ (3) : Basta tomar $C = A[\alpha]$.
(3) $\Rightarrow$ (1) : Sejam $c_1, \ldots, c_n \in C$ os geradores de C como A-módulo. Como, por hipótese, $\alpha c_i \in C$, para todo $i = 1, \ldots, n$, temos que

$$\alpha c_i = \sum_{j=1}^{n} a_{ij}c_j,$$

assim temos

$$\alpha c_1 = a_{11}c_1 + \cdots + a_{1n}c_n$$

$$\ddots$$

$$\alpha c_n = a_{n1}c_1 + \cdots + a_{nn}c_n.$$

Em particular, podemos observar, que α é raiz do polinômio característico da matriz (a_{ij}) que é mônico e possui coeficientes em A. ■

Por indução, para um número finito de elementos $\alpha_1, \ldots, \alpha_n$, defina

$$A[\alpha_1, \ldots, \alpha_n] \coloneqq A[\alpha_1, \ldots, \alpha_{n-1}][\alpha_n].$$

Em particular, quando $\alpha_1, \ldots, \alpha_n$ são elementos algébricos sobre um anel A, segue uma generalização natural do teorema anterior:

Corolário 2.28. *Sejam B um anel e A subanel de B. Se $\alpha_1, \ldots, \alpha_n \in B$ forem integrais sobre A, então $A[\alpha_1, \ldots, \alpha_n]$ será um A-módulo finitamente gerado.*

Demonstração: Provaremos o resultado por indução sobre n. O caso $n = 1$ é o Teorema 2.27. Suponhamos que o resultado seja válido para $n-1$, ou seja, $A[\alpha, \ldots, \alpha_{n-1}]$ é um A-módulo finitamente gerado. Como α_n é integral sobre A, é também integral sobre $A[\alpha, \ldots, \alpha_{n-1}]$, portanto, por 2.27,

$$A[\alpha, \ldots, \alpha_{n-1}][\alpha_n] = A[\alpha, \ldots, \alpha_n]$$

é finitamente gerado. ■

Corolário 2.29. *Sejam B um anel e A subanel de B. Então o conjunto $I_B(A)$ dos elementos de B que são integrais sobre A é um subanel de B que contém A.*

Demonstração: Basta observar que se x, y são elementos integrais de A, então, pelo Corolário 2.29, $A[x, y]$ é um A-módulo finitamente gerado que contém os elementos $x+y$, $x-y$ e xy e, pelo teorema 2.27, tais elementos são inteiros sobre A. ■

Como consequência temos a seguinte definição:

Definição 2.30. Sejam B um anel e A subanel de B. O anel $I_B(A)$ dos elementos de B que são inteiros sobre A é chamado fecho inteiro de A em B.

2.4 Corpos quadráticos

Definição 2.31. Seja K um corpo de números. Diremos que K é um corpo quadrático se $[K : \mathbb{Q}] = 2$.

Sejam K um corpo quadrático e $\alpha \in K \setminus \mathbb{Q}$. Assim, α é um zero de um polinômio mônico $x^2 + ax + b$, com $a, b \in \mathbb{Q}$. Dessa forma

$$\alpha = \frac{-a \pm \sqrt{a^2 - 4b}}{2}.$$

Logo, segue a igualdade

$$K = \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{a^2 - 4b}).$$

Em outras palavras, K é um corpo quadrático se, e somente se, existe um racional d, diferente de 0 ou 1, tal que $K = \mathbb{Q}(\sqrt{d})$.

Apesar de d, na construção acima, estar definido para qualquer racional diferente de 0 ou 1 podemos nos restringir a um conjunto mais específico.

Definição 2.32. Dizemos que d é um inteiro livre de quadrados se d não é divisível por nenhum $c^2 \neq 1$, com $c \in \mathbb{Z}$. Denotaremos o conjunto dos inteiros livres de quadrados por $\mathcal{L}$.

Teorema 2.33. *A aplicação definida por $d \mapsto \mathbb{Q}(\sqrt{d})$ é uma bijeção de $\mathcal{L}$, conjuntos dos inteiros livre de quadrados, sobre o conjunto de todos os corpos quadráticos.*

Demonstração: Primeiramente, devemos verificar se a aplicação está bem definida. Em outras palavras, dado $d \in \mathcal{L}$, precisamos garantir que o corpo $\mathbb{Q}(\sqrt{d})$ seja de fato um corpo quadrático. Com efeito, Para qualquer $d \in \mathcal{L}$ temos $[\mathbb{Q}(\sqrt{d}) : \mathbb{Q}] \leq 2$. Se o corpo $\mathbb{Q}(\sqrt{d})$ não fosse quadrático teríamos

$$[\mathbb{Q}(\sqrt{d}) : \mathbb{Q}] = 1.$$

Consequentemente, seguiria a igualdade $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}$. No entanto, isso seria um absurdo, uma vez que implicaria $\sqrt{d} \in \mathbb{Q}$. Portanto, a aplicação está bem definida.

Para provarmos a injetividade da aplicação, suponhamos que $\mathbb{Q}(\sqrt{d_1}) = \mathbb{Q}(\sqrt{d_2})$, onde $d_1, d_2 \in \mathcal{L}$. Isso implica que existem $r, s \in \mathbb{Q}$ tais que $\sqrt{d_1} = r + s\sqrt{d_2}$. Elevando ao quadrado ambos os lados da igualdade, obtemos

$$d_1 = r^2 + s^2 d_2 + 2rs\sqrt{d_2}.$$

A partir da igualdade acima, podemos concluir que $rs = 0$, o que implica que $r = 0$ ou $s = 0$. A igualdade $s = 0$ implicaria que $d_1 = r$ que por sua vez implicaria em $d_1 \notin \mathcal{L}$, o que é impossível. Portanto segue que $r = 0$ e $d_1 = s^2 d_2$ e como d_1 é livre de quadrados, $s^2 = 1$. Portanto, $d_1 = d_2$, o que demonstra a injetividade da aplicação.

Já para a sobrejetividade da aplicação, considere o corpo quadrático $K = \mathbb{Q}(\sqrt{q})$, onde q é um número racional conforme observado anteriormente. Podemos escrever $q = \frac{u}{v}$, onde $u, v \in \mathbb{Z}$. Logo

$$K = \mathbb{Q}(\sqrt{q}) = \mathbb{Q}\left(\sqrt{\frac{u}{v}}\right) = \mathbb{Q}\left(\sqrt{\frac{uv}{v^2}}\right) = \mathbb{Q}(\sqrt{uv}).$$

Escrevendo $uv = n^2 d$, onde d é a parte livre de quadrados de uv, temos

$$K = \mathbb{Q}(\sqrt{n^2 d}) = \mathbb{Q}(\sqrt{d})$$

■

Definição 2.34. Seja $\mathbb{Q}(\sqrt{d})$ um corpo quadrático, onde d é o inteiro livre de quadrados univocamente determinado pelo Teorema 2.33. Diremos que d é o discriminante do corpo quadrático $\mathbb{Q}(\sqrt{d})$.

Em geral, sempre que denotarmos um corpo quadrático como $\mathbb{Q}(\sqrt{d})$ fica-se subentendido que d é o discriminante do corpo quadrático.

Sempre que o discriminante de um corpo quadrático é positivo, o corpo estará contido em $\mathbb{R}$. Por outro lado quando seu discriminante for negativo o corpo quadrático estará contido em $\mathbb{C}$ mas não em $\mathbb{R}$. Assim definimos:

Definição 2.35. Dizemos que um corpo quadrático é real quando seu discriminante é positivo. Caso contrário, isto é, quando seu discriminante é negativo, dizemos que o corpo quadrático é complexo.

Definição 2.36. Em um corpo quadrático $\mathbb{Q}(\sqrt{d})$, a norma e o traço de um elemento $r + s\sqrt{d}$ são definidos, respectivamente, por:

$$N(r + s\sqrt{d}) \coloneqq r^2 - ds^2$$

$$T(r + s\sqrt{d}) \coloneqq 2r.$$

Definição 2.37. Para um elemento $\alpha = r + s\sqrt{d} \in \mathbb{Q}(\sqrt{d})$, definimos o seu conjugado como $\alpha' = r - s\sqrt{d}$.

Seja $\alpha = r + s\sqrt{d}$ um elemento do corpo quadrático $\mathbb{Q}(\sqrt{d})$, então

$$N(\alpha) = \alpha\alpha'$$

$$T(\alpha) = \alpha + \alpha'$$

A propriedade fundamental da norma N é a sua multiplicatividade, isto é:

Proposição 2.38. *Seja $\mathbb{Q}(\sqrt{d})$ um corpo quadrático, então a norma goza da propriedade*

$$N(\alpha\beta) = N(\alpha)N(\beta),$$

para todo $\alpha, \beta \in \mathbb{Q}(\sqrt{d})$.

Demonstração: Basta notar a seguinte relação

$$N(\alpha\beta) = \alpha\beta(\alpha\beta)' = \alpha\beta\alpha'\beta' = \alpha\alpha'\beta\beta' = N(\alpha)N(\beta).$$

2.5 Anéis quadráticos

Agora, nosso objetivo será caracterizar o conjunto dos inteiros algébricos de um corpo quadrático $\mathbb{Q}(\sqrt{d})$, que chamaremos de anel quadrático, e introduzir algumas propriedades relativas a esses anéis.

Definição 2.39. Dado um corpo quadrático $\mathbb{Q}(\sqrt{d})$, diremos que seu conjunto de inteiros algébricos é um anel quadrático com discriminante d e o denotaremos por $\mathcal{O}_d$. Também diremos que $\mathcal{O}_d$ é um anel quadrático real se $d > 0$ e um anel quadrático complexo se $d < 0$.

A seguinte observação, que será útil em cálculos posteriores:

Observação 2.40. Quando $d \equiv 1 \pmod 4$ vale a igualdade

$$\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{d}}{2}\right) = \left\{\frac{a}{2} + \frac{b}{2}\sqrt{d} : \ a, b \in \mathbb{Z}, \ a \equiv b \pmod 2\right\}. \tag{2.2}$$

Teorema 2.41. *Seja d um inteiro livre de quadrados. Então o conjunto dos inteiros algébricos do corpo quadrático $\mathbb{Q}(\sqrt{d})$ é*

$$\mathcal{O}_d = \begin{cases} \mathbb{Z} + \mathbb{Z}\sqrt{d}, & \text{se } d \equiv 2, 3 \pmod 4; \\ \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{d}}{2}\right), & \text{se } d \equiv 1 \pmod 4. \end{cases} \tag{2.3}$$

Demonstração: Todo elemento $\alpha \in \mathbb{Q}(\sqrt{d})$ é da forma $r + s\sqrt{d}$, com $r, s \in \mathbb{Q}$. Logo pode ser escrito como

$$\alpha = \frac{a + b\sqrt{d}}{c}$$

onde $a, b, c \in \mathbb{Z}$, com $c > 0$ e $mdc(a, b, c) = 1$. Portanto, α é um inteiro algébrico se, e somente se, os coeficientes de seu polinômio minimal α sobre $\mathbb{Q}$

$$min_{\mathbb{Q}}\alpha(t) = \left(t - \frac{a + b\sqrt{d}}{c}\right)\left(t - \frac{a - b\sqrt{d}}{c}\right) = t^2 - \frac{2a}{c}t + \frac{a^2 - b^2 d}{c^2}$$

são inteiros, isto é,

$$\frac{a^2 - b^2 d}{c^2}, \ \frac{2a}{c} \in \mathbb{Z}.$$

Se a e c possuem um fator primo p em comum, como d é livre de quadrados, p também divide b, o que contradiz o maior divisor comum entre a, b e c ser igual a 1. Donde podemos concluir que c é um divisor de 2, ou seja, $c = 1$ ou $c = 2$. Se $c = 1$, então

$$\alpha = \frac{a + b\sqrt{d}}{c} = a + b\sqrt{d}$$

é um inteiro algébrico tanto para o caso $d \equiv 1$ $(mod\ 4)$, quanto para $d \equiv 2$ ou 3 $(mod\ 4)$. Agora suponhamos que $c = 2$. como $mdc(a, b, c) = 1$, a e b devem ser ímpares. De

$$\frac{a^2 - b^2 d}{c^2} \in \mathbb{Z}$$

segue

$$a^2 - b^2 d \equiv 0 \pmod 4.$$

Como um número ímpar $2k + 1$ possui quadrado $4k^2 + 4k + 1 \equiv 1 \pmod 4$. Temos, $a^2 \equiv 1 \equiv b^2 \pmod 4$ e isso implica $d \equiv 1 \pmod 4$. Dessa forma e pela observação acima, obtemos

$$\mathcal{O}_d \subset \begin{cases} \mathbb{Z} + \mathbb{Z}\sqrt{d}, & \text{se } d \equiv 2, 3 \pmod 4; \\ \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{d}}{2}\right), & \text{se } d \equiv 1 \pmod 4. \end{cases}$$

Para a recíproca basta verificarmos a existência de um polinômio com coeficientes em $\mathbb{Z}$ satisfazendo o elemento da forma descrita em 2.41. Sejam a e b inteiros, então o elemento $a + b\sqrt{d}$ satisfaz o polinômio

$$x^2 - 2ax + a^2 + db^2.$$

Se $d \equiv 1$ $(mod\ 4)$, então o elemento $a + b\left(\frac{1+\sqrt{d}}{2}\right)$ é um zero do polinômio com coeficientes inteiros.

$$x^2 - (2a + b)x + a^2 + ab + \left(\frac{1 - d}{4}\right) b^2$$

Portanto vale a igualdade

$$\mathcal{O}_d = \begin{cases} \mathbb{Z} + \mathbb{Z}\sqrt{d}, & \text{se } d \equiv 2, 3 \pmod 4; \\ \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{d}}{2}\right), & \text{se } d \equiv 1 \pmod 4. \end{cases}$$

■

Observação 2.42. Devido a Observação 2.2, quando $d \equiv 1 \pmod 4$

$$\mathcal{O}_d = \left\{ \frac{a}{2} + \frac{b}{2}\sqrt{d} : \ a, b \in \mathbb{Z}, \ a \equiv b \pmod 2 \right\}.$$

Observação 2.43. Seja $\alpha \in \mathbb{Q}(\sqrt{d})$, então

$$min_{\mathbb{Q}}\alpha(t) = t^2 - T(\alpha)t + N(\alpha).$$

Logo dizer que o elemento α é um inteiro algébrico é equivalente a mostrar que $T(\alpha), N(\alpha) \in \mathbb{Z}$

Observação 2.44. Seja

$$\omega_d = \begin{cases} \sqrt{d}, \text{ se } d \equiv 2,3 \pmod 4; \\ \frac{1+\sqrt{d}}{2}, \text{ se } d \equiv 1 \pmod 4. \end{cases}$$

Observe que $\{1, \omega_d\}$ é uma base integral de $\mathcal{O}_d$.

Definição 2.45. Nos referiremos à base $\{1, \omega_d\}$ como a base integral canônica de $\mathcal{O}_d$.

A seguir, daremos dois exemplos de anéis quadráticos.

Exemplo 2.46. O anel dos inteiros de Gauss

$$\mathbb{Z}[i] \coloneqq \mathbb{Z} + \mathbb{Z}i$$

é o anel dos inteiros de $\mathbb{Q}(\sqrt{-1})$. De fato, já que $-1 \equiv 3 \pmod 4$, então

$$\mathcal{O}_{-1} = \mathbb{Z} + \mathbb{Z}i.$$

Exemplo 2.47. Uma vez que $-3 \equiv 1 \pmod 4$,

$$\mathcal{O}_{-3} = \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{-3}}{2}\right).$$

Este anel é também conhecido como inteiros de Einsenstein.

Ao trabalharmos com anéis quadráticos, torna-se crucial conhecer suas propriedades decorrentes de sua característica de domínio, como, por exemplo, o conjunto da suas unidades e o conjunto de seus elementos irredutíveis. A partir deste ponto, exploraremos alguns resultados que nos permitirão caracterizar o conjunto das unidades em um anel quadrático.

Proposição 2.48 (Caracterização de unidades)**.** *Um elemento $\alpha \in \mathcal{O}_d$ é uma unidade se, e somente se, $N(\alpha) = \pm 1$.*

Demonstração: Seja α uma unidade em $\mathcal{O}_d$, então existe $\beta \in \mathcal{O}_d$ tal que $\alpha\beta = 1$. Assim, como a norma dos elementos de $\mathcal{O}_d$ são números inteiros,

$$N(\alpha\beta) = N(\alpha)N(\beta) = 1,$$

implica que apenas $N(\alpha) = \pm 1$ é possível.

Reciprocamente, suponhamos que a norma de α satisfaça $N(\alpha) = \pm 1$, logo $\alpha\alpha' = \pm 1$, e como $\alpha' \in \mathcal{O}_d$, α é uma unidade em $\mathcal{O}_d$. ■

Podemos utilizar diretamente a última proposição para determinarmos o conjunto das unidades de anéis quadráticos complexos.

Proposição 2.49. *Seja $\mathbb{Q}(\sqrt{d})$ um corpo quadrático, onde $d < 0$ e livre de quadrados. Então o grupos das unidades de $\mathcal{O}_d$, que denotaremos por $\mathcal{O}_d^\times$, é dado por*

1. $\mathcal{O}_d^\times = \{\pm 1, \pm i\}$, *se* $d = -1$;
2. $\mathcal{O}_d^\times = \{\pm 1, \pm\omega, \pm\omega^2\}$, *onde* $\omega = e^{\frac{2\pi i}{3}}$, *se* $d = -3$;
3. $\mathcal{O}_d^\times = \{\pm 1\}$, *se* $d < 0$ *e* $d \neq -1, -3$.

Demonstração: Segundo a Proposição 2.48, para encontrarmos o conjunto das unidade de $\mathcal{O}_d$ precisamos encontrar os elementos $\alpha \in \mathcal{O}_d$ que satisfaça $N(\alpha) = \pm 1$, resultando em equações diofantinas da forma $x^2 + |d|y^2 = \pm 1$, se $d \equiv 2, 3 \pmod 4$, ou $x^2 + |d|y^2 = \pm 4$, se $d \equiv 1 \pmod 4$, que de forma geral possuem soluções simples. ■

Apesar da facilidade de caracterizar o conjunto das unidade em anéis quadráticos complexos, para o caso real é um tarefa muito mais complicada. O seguinte resultado nos mostra a existência de infinitas unidades não triviais em anéis quadráticos reais. Posteriormente mostraremos que em um anel quadrático real existe uma certa unidade que gera todas em certo sentido.

Teorema 2.50. *Seja $d > 0$ um inteiro que não é um quadrado perfeito. Então a equação $x^2 - dy^2 = 1$ possui solução inteira não trivial, ou seja, solução diferente de $(\pm 1, 0)$. Em particular, quando d é um inteiro positivo livres de quadrado o corpo quadrático $\mathbb{Q}(\sqrt{d})$ possui uma unidade diferente de ± 1.*

Para a demonstração do teorema precisaremos dos dois resultados seguintes.

Lema 2.51. *Se ξ_1 e ξ_2 são números reais diferentes de 0 tal que $\frac{\xi_1}{\xi_2}$ é irracional, então para qualquer $N \in \mathbb{N}$, existem inteiros A e B, ambos diferentes de 0 que satisfazem as inequações:*

$$|A\xi_1 + B\xi_2| \leq \frac{1}{N}(|\xi_1| + |\xi_2|),\ |A| \leq N,\ |B| \leq N$$

Demonstração: Assumimos que ξ_1 e ξ_2 são ambos positivos (caso contrário, apenas precisamos trocar os sinais de a e b na prova abaixo). A irracionalidade de $\frac{\xi_1}{\xi_2}$ implica que a função

$$f : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{R} : (a, b) \mapsto a\xi_1 + b\xi_2$$

é injetora.

Existem $(N+1)^2$ pares de inteiros $(a, b) \in [0, N] \times [0, N]$, e para esses pares, temos $0 \leq f(a, b) \leq N(|\xi_1| + |\xi_2|)$. Se dividirmos o intervalo $[0, N(|\xi_1| + |\xi_2|)]$, em N^2 subintervalos de comprimento igual a $\frac{1}{N}(|\xi_1| + |\xi_2|)$, então, como $(N+1)^2 > N^2$, deve existir, de acordo com o princípio da gaveta dos pombos, pelo menos dois pares

$$(a, b) \neq (a', b') \text{ com } |f(a, b) - f(a', b')| \leq N(|\xi_1| + |\xi_2|).$$

Agora, defina $A = a - a'$ e $B = b - b'$, e assim os inteiros A e B terão as propriedades desejadas. ■

Corolário 2.52. *Assuma que $d \in \mathbb{N}$ não seja um quadrado perfeito. Então existe um inteiro c tal que a equação $A^2 - dB^2 = c$ possui infinitas soluções $(A, B) \in \mathbb{Z} \times \mathbb{Z}$.*

Demonstração: Pelo lema anterior, existem números $A, B \in \mathbb{Z}$, com pelo menos um deles diferente de 0, que satisfazem as desigualdades

$$|A - B\sqrt{d}| \leq \frac{1}{N}(1 + \sqrt{d}),\ |A| \leq N,\ |B| \leq N. \tag{2.4}$$

A desigualdade triangular nos mostra que

$$|A + B\sqrt{d}| \leq |A| + |B\sqrt{d}| \leq (1 + \sqrt{d}) \cdot N, \tag{2.5}$$

e multiplicando 2.4 e 2.5 obtemos

$$|A^2 - mB^2| \leq (1 + \sqrt{d})^2.$$

Agora, fazendo $N \to \infty$, haverá infinitos pares distintos (A, B), pois se tivéssemos apenas uma quantidade finita, o conjunto $\{|A - B\sqrt{d}| : A, B \in \mathbb{Z}\}$ possuiria um mínimo, o que é impossível devido a 2.4. Como, por 2.4, $|A^2 - dB^2|$ é limitado superiormente, deve existir um inteiro c com $|c| \leq (1+\sqrt{d})^2$ para o qual $A^2 - dB^2 = c$ tenha infinita soluções inteiras, o que demonstra o corolário. ■

Agora, podemos demonstrar o Teorema 2.50.

Demonstração do Teorema 2.50: De acordo com o Corolário 2.52, existe um inteiro $c \neq 0$ tal que há infinitos pares (A, B) satisfazendo $A^2 - dB^2 = c$. Por conveniência, assumiremos sem perda de generalidade que $A > 0$. Entre estas infinitas soluções, escolhemos $(c + 1)$ soluções e consideramos as classes de resíduos de A e B módulo c. Pelo princípio das gavetas dos pombos, deve haver pelo menos dois pares $(A_1, B_1) \neq (A_2, B_2)$ com $A_1 \equiv A_2 \pmod{c}$ e $B_1 \equiv B_2 \pmod{c}$.

Os elementos $\eta_j = A_j + B_j\sqrt{d}$ possuem as mesmas normas $N(\eta_1) = N(\eta_2) = c$ e satisfazem a congruência $\eta_1 \equiv \eta_2 \pmod{c}$. Da igualdade $N(\eta_1/\eta_2) = 1$, segue que η_1/η_2 será uma unidade se pudermos mostrar que η_1/η_2 é um inteiro algébrico. Para isso, observe que $\eta_1/\eta_2 = 1 + (\eta_1 - \eta_2)/\eta_2 = 1 + (\eta_1 - \eta_2)\sqrt{d}/c$. Uma vez que, pela construção, a diferença $\eta_1 - \eta_2$ é divisível por c, η_1/η_2 é de fato um inteiro algébrico e, portanto, uma unidade.

Ainda precisamos mostrar que $\eta_1/\eta_2 \neq \pm 1$ é uma unidade não trivial. No entanto, $\eta_1/\eta_2 \neq 1$ segue de $\eta_1 \neq \eta_2$, e $\eta_1/\eta_2 \neq -1$ decorre do fato de que A_1 e A_2 são ambos positivos. Isso conclui a prova do Teorema 2.50 ■

Um resultado muito interessante é o da existência de uma unidade ϵ que gera qualquer outra unidade η pela relação $\epsilon = \pm\epsilon^n$, onde $n \in \mathbb{Z}$.

Teorema 2.53. *Se $\mathcal{O}_d$ é um anel quadrático real, então existe uma unidade $\epsilon \in \mathcal{O}_d^\times$ com a propriedade que toda unidade $\eta \in \mathcal{O}_d^\times$ pode ser escrita unicamente na forma $\eta = \pm\epsilon^t$, para algum $t \in \mathbb{Z}$. Em particular,*

$$\mathcal{O}_d^\times \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}.$$

Demonstração: Dentre as unidades satisfazendo $|\eta| > 1$, afirmamos que existe uma com o menor valor absoluto. Suponhamos o contrário, então existiria uma unidade (na verdade, infinitas) com $1 < |\eta| < \frac{5}{4}$ (basta escolher duas unidades suficientemente próximas do ínfimo dos valores absolutos e considerar o quociente delas). Como $|\eta\eta'| = 1$, isso implica $\frac{4}{5} < |\eta'| < 1$. Se expressarmos η como $\eta = a + b\sqrt{d}$ (onde $2a, 2b \in \mathbb{Z}$), então $2|a| = |\eta + \eta'| \leq |\eta| + |\eta'| < \frac{9}{4}$, e, portanto, $|a| \leq 1$. Como $a = 0$ não é possível, devemos ter $a = \pm 1$ ou $a = \pm 1/2$. Se $a = \pm 1$, então, imediatamente, segue de $1 < |\eta| < \frac{5}{4}$ que $b = 0$, e, portanto, $\eta = 1$, chegando a uma contradição. Se $a = \pm 1/2$, então para nenhum d, haverá uma unidade η satisfazendo $1 < |\eta| < \frac{5}{4}$.

Seja ϵ uma unidade com o menor valor absoluto maior do que 1. Afirmamos que ϵ possui as propriedades listadas no enunciado do Teorema 2.53. Caso contrário, existiria uma unidade η com $\epsilon^n < |\eta| < \epsilon^{n+1}$ para algum $n \in \mathbb{N}$. Mas então $\eta\epsilon^{-n}$ seria uma unidade cujo valor absoluto está estritamente entre 1 e $|\epsilon|$, contradizendo a escolha de ϵ.

A unicidade é evidente: $\pm\epsilon = \pm\epsilon$ implica $|\epsilon| = 1$, o que, por sua vez, implica $t = u$ já que ϵ é irracional. Portanto, os sinais também devem coincidir.

Seja ϵ como no teorema anterior e considere as unidades $\pm\epsilon^{\pm 1}$. Entre essas quatro unidades, há exatamente duas positivas, e entre essas há exatamente uma que é maior do que 1. Então sempre haverá uma unidade $\epsilon > 1$ tal que que qualquer outra unidade é

escrita como $\pm\epsilon^t$, onde $t \in \mathbb{Z}$. A partir de ϵ construído na demonstração do Teorema 2.53 ser uma unidade que possui o menor valor absoluto maior que 1 definimos:

Definição 2.54. Seja $\mathcal{O}_d$ um corpo quadrático real. Dizemos que sua unidade fundamental é a menor unidade de $\mathcal{O}_d$ maior do que 1.

Portanto, a unidade fundamental de um corpo quadrático real gera qualquer outra unidade a partir da relação $\pm\epsilon^t$, $t \in \mathbb{Z}$. Cabe comentar que para um inteiro livre de quadrados d um corpo quadrático real nem sempre possui uma unidade com norma -1. Por exemplo, $\mathcal{O}_{-3}$ não possui uma unidade de norma -1. De fato, basta mostramos que a equação

$$x^2 + 3y^2 = -4$$

não possui solução inteira. Caso a equação possua solução inteira, analisando a equação módulo 3 chegamos a expressão

$$x^2 \equiv -4 \equiv -1 \pmod 3$$

e como -1 não é um resíduo quadrático módulo 3 é impossível que a equação tenha solução. No entanto, para valores específicos de d, $\mathcal{O}_d$ possui unidades de norma negativa. O seguinte resultado, que será útil futuramente, nos exemplifica esse fato.

Teorema 2.55. *Se p é um primo com $p \equiv 1 \pmod 4$, então a unidade fundamental ϵ possui norma $N(\epsilon) = -1$.*

Demonstração: Veja [5], Teorema 11.5.4. ■

Observação 2.56. Caso exista uma unidade de norma negativa, como a unidade fundamental gera qualquer outra unidade pela relação $\pm\epsilon^n$, com $n \in \mathbb{Z}$, então será necessário que a unidade fundamental também tenha norma negativa.

Também podemos utilizar a norma para dar uma condição suficiente para que um elemento em $\mathcal{O}_d$ seja irredutível.

Proposição 2.57. *Se $\alpha \in \mathcal{O}_d$ tem norma $N(\alpha) = \pm p$, onde p é um inteiro primo, então α é irredutível em $\mathcal{O}_d$.*

Demonstração: Seja $\alpha \in \mathcal{O}_d$ tal que $N(\alpha) = \pm p$, onde p é um inteiro primo. Suponha que existam $\beta, \gamma \in \mathcal{O}_d$, tais que $\alpha = \beta\gamma$. Então $N(\alpha) = N(\beta)N(\gamma)$. Mas, como $N(\beta)$ e $N(\gamma)$ são inteiros e $N(\alpha)$ é um primo, então um deles deve possuir norma igual a ± 1, o que implica ser uma unidade. Portanto α é irredutível. ■

2.6 Anéis quadráticos norma euclidianos

Definição 2.58. Diremos que um anel quadrático $\mathcal{O}_d$ é norma euclidiano quando é um domínio euclidiano cuja função euclidiana é o valor absoluto da norma. Em outras palavras, $\mathcal{O}_d$ é norma euclidiano quando para quaisquer $\alpha, \beta \in \mathcal{O}_d$, existem $q, r \in \mathcal{O}_d$ tais que

$$\alpha = \beta \cdot q + r \tag{2.6}$$

com $r = 0$ ou $|N(r)| < |N(\beta)|$.

A partir da igualdade 2.6, podemos expressar r como $r = \alpha - \beta \cdot q$. Assim, obtemos a relação

$$N(r) = N(\alpha - q\beta) = N\left(\left(\frac{\alpha}{\beta}\right)\beta\right) = N\left(\frac{\alpha}{\beta}\right)N(\beta).$$

Como o corpo de frações $\mathcal{O}_d$ é um corpo que contém estritamente $\mathbb{Q}$ e está contido em $\mathbb{Q}(\sqrt{d})$, que é uma extensão de grau 2 de $\mathbb{Q}$, então segue que o corpo de frações de $\mathcal{O}_d$ coincide com $\mathbb{Q}(\sqrt{d})$. Além disso, dado que $|N(r)| < |N(\beta)|$, podemos estabelecer um critério para que um anel quadrático seja norma euclidiano.

Proposição 2.59. *Um anel quadrático $\mathcal{O}_d$ é norma euclidiano se, e somente, para todo $\gamma \in \mathbb{Q}(\sqrt{d})$ existe $q \in \mathcal{O}_d$ tal que $|N(\gamma - q)| < 1$*

Demonstração. Suponhamos que $\mathbb{Q}(\sqrt{d})$ seja norma euclidiano. Seja $\gamma \in \mathbb{Q}(\sqrt{d})$, logo, existem $\alpha, \beta \in \mathcal{O}_d$ tais que

$$\gamma = \frac{\alpha}{\beta}.$$

Sejam $q, r \in \mathcal{O}_d$ tais

$$\alpha = \beta q + r,$$

com $r = 0$ ou $|N(r)| < |N(\beta)|$. Dessa forma temos

$$\gamma = \frac{\alpha}{\beta} = q + \frac{r}{\beta}$$

ou, de forma equivalente,

$$\gamma - q = \frac{r}{\beta}.$$

Portanto, como $r = 0$ ou $|N(r)| < |N(\beta)|$,

$$|N(\gamma - q)| < \left|N\left(\frac{r}{\beta}\right)\right| < 1.$$

Para a recíproca, sejam $\alpha, \beta \in \mathcal{O}_d$. Pela hipótese, exite $q \in \mathcal{O}_d$ tal que

$$\left|N\left(\frac{\alpha}{\beta} - q\right)\right| < 1.$$

Então

$$|N(\alpha - \beta q)| < |N(\beta)|.$$

Definindo $r = \alpha - \beta q$ temos o que queríamos. ■

Corolário 2.60. *Um anel quadrático $\mathcal{O}_d$ é norma euclidiano se para todo $a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ existe um $x + y\sqrt{d} \in \mathcal{O}_d$ tal que*

$$|N((a + b\sqrt{d}) - (x + y\sqrt{d}))| = |(a - x)^2 - d(b - y)^2| < 1.$$

Observação 2.61. Pelo resultado acima, podemos concluir que um anel quadrático $\mathbb{Q}(\sqrt{d})$ é norma euclidiano se, e somente, para quaisquer $a, b \in \mathbb{Q}$ a inequação

1. $|(a - x)^2 - d(b - y)^2| < 1$ possui solução $(x, y) \in \mathbb{Z} \times \mathbb{Z}$, se $d \equiv 2, 3 \ (mod\ 4)$;
2. $|(2a - x)^2 - d(2b - y)^2| < 4$ possui solução $(x, y) \in \mathbb{Z} \times \mathbb{Z}$, com $x \equiv y \ (mod\ 2)$, se $d \equiv 1 \ (mod\ 4)$.

Exemplo 2.62. $\mathcal{O}_i = \mathbb{Z}[i] = \mathbb{Z} + \mathbb{Z}i$ é norma euclidiano.

Demonstração: De acordo com a observação, para quaisquer racionais a e b precisamos encontrar inteiros x e y tais que

$$|(a-x)^2 + (b-y)^2| < 1.$$

Para isso basta escolhermos

$$\begin{cases} x \in \mathbb{Z} \text{ tal que } |a-x| \leq \frac{1}{2} \\ y \in \mathbb{Z} \text{ tal que } |b-y| \leq \frac{1}{2}. \end{cases}$$

Dessa forma que temos

$$|(a-x)^2 + (b-y)^2| \leq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2} < 1.$$

■

Vamos computar um exemplo na prática.

Exemplo 2.63. Sejam $\alpha = 3 + 5i, \beta = 1 + i \in \mathbb{Z}[i]$.

Demonstração: Calculando temos

$$\frac{\alpha}{\beta} = -\frac{1}{2} + \frac{7}{2}i.$$

Queremos encontrar x inteiro tal que $|-\frac{1}{2} - x| \leq \frac{1}{2}$. Claramente, as únicas soluções da desigualdade são $x = -1$ ou $x = 0$. Para y, precisamos que satisfaça $|\frac{7}{2} - y| \leq \frac{1}{2}$. neste caso também temos duas soluções $y = 7$ e $y = 8$. Dessa forma temos quatro opções para q:

$$q = -1 + 7i,\ -1 + 8i,\ 7i,\ 8i.$$

Como $\alpha = \beta q + r$, podemos computar r substituindo os valores de q.

Observação 2.64. O exemplo acima nos mostra que, diferentemente do algoritmo de Euclides que conhecemos em $\mathbb{Z}$, o algoritmo $\mathbb{Z}[i]$ não possui a unicidade para q e r.

De $\mathcal{O}_i = \mathbb{Z}[i]$ ser um anel quadrático euclidiano, então, em particular, é um domínio de fatoração única. Agora daremos dois exemplos de como a fatoração única nos ajuda a resolver equações diofantinas. Primeiramente vamos construir o conjunto dos elementos primos de $\mathbb{Z}[i]$.

Lema 2.65. *Qualquer primo $p \equiv 1 \pmod 4$ fatora-se como $p = (a+ib)(a-ib)$ com $a, b \in \mathbb{Z}$. Em particular, p pode ser escrito como soma de dois quadrados perfeitos em $\mathbb{Z}$.*

Demonstração: Como $p \equiv 1 \pmod 4$, temos $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = 1$, ou seja, existe $x \in \mathbb{Z}$ tal que $x^2 + 1 \equiv 0 \pmod p$. Agora, suponha que p seja irredutível em $\mathbb{Z}[i]$. Então, de $p|x^2+1 = (x+i)(x-i)$, temos que $p|x+i$ ou $p|x-i$. Mas isso é impossível, uma vez que um múltiplo de p em $\mathbb{Z}[i]$ é da forma $p(a+ib) = pa + ipb$, com $a, b \in \mathbb{Z}$, isto é, possui parte real e imaginária múltiplas de p, o que não é o caso para $x \pm i$.

Assim, temos que p é irredutível e existem $\beta, \gamma \in Z[i] \setminus \mathbb{Z}[i]^\times$ tais que $p = \beta\gamma$. Tomando normas, temos $p^2 = N(\beta)N(\gamma)$, o que implica em $N(\beta) = N(\alpha) = p$, já que $\beta, \gamma \notin \mathbb{Z}[i]^\times$, ou seja, $N(\beta), N(\gamma) \neq \pm 1$. Escrevendo $\beta = a + ib$ com $a, b \in \mathbb{Z}$, temos portanto que $p = N(\beta) = a^2 + b^2$, donde obtemos a fatoração $p = (a+ib)(a-ib)$ desejada. Note que $a \pm ib$ são ambos elementos primos em $\mathbb{Z}[i]$ pois possuem norma prima. ■

Teorema 2.66. *Os elementos primos de $\mathbb{Z}[i]$ são, a menos de associados,*

- *números primos $p \in \mathbb{Z}$ tais que $p \equiv 3 \pmod 4$;*
- *números da forma $a + ib$ onde $N(a + ib)$ é primo, necessariamente igual a 2 ou congruente a 1 módulo 4.*

Demonstração: Vamos demonstrar que os inteiros p primos em $\mathbb{Z}$ congruentes a 3 módulo 4 são irredutíveis em $\mathbb{Z}[i]$, o que implica em dizer que são também primos em $\mathbb{Z}[i]$. Seja $p \in \mathbb{Z}$ tal que $p \equiv 3 \pmod 4$. Se p pode ser fatorado como $p = \alpha\beta$ com $\alpha, \beta \in \mathbb{Z}[i] \setminus \mathbb{Z}[i]^\times$, temos $p^2 = N(p) = N(\alpha\beta) = N(\alpha)N(\beta)$. Como α e β não são unidades, então $N(\alpha) = N(\beta) = p$. Entretanto, escrevendo $\alpha = a + bi$ com $a, b \in \mathbb{Z}$, temos que $a^2 + b^2 = p \equiv 3 \pmod 4$, o que é impossível, visto que um quadrado perfeito é congruente a 0 ou 1 módulo 4, logo $a^2 + b^2$ é congruente a 0, 1 ou 2 módulo 4, o que nos leva a uma contradição.

De acordo com a Proposição 2.57, $N(\alpha)$ primo implica que α é um elemento primo em $\mathbb{Z}[i]$.

Agora, vamos mostrar que se α não é um primo em $\mathbb{Z}$ congruente a 3 módulo 4 ou se $N(\alpha)$ não é um primo, então α é redutível. Primeiramente, observe que α é irredutível se, e somente se, α' é irredutível. Seja $\alpha = a + ib$ um elemento irredutível em $\mathbb{Z}[i]$, se $N(a + ib)$ não é um primo em $\mathbb{Z}$, então $a^2 + b^2 = mn$ com $m, n \in \mathbb{Z}$ e $m, n \neq 1$, logo

$$(a + ib)(a - ib) = mn.$$

Pela unicidade da fatoração, podemos afirmar que $a + ib = \epsilon n$ (e $a - ib = \epsilon^{-1}m$), onde ϵ é uma unidade $\mathbb{Z}[i]$, isto é, $\epsilon = \pm 1$ ou $\pm i$. Assim, devemos ter $a = 0$ ou $b = 0$, em qualquer caso segue a igualdade $\alpha = \pm n$. Portanto, α é irredutível se, e somente se, m é irredutível, o que é equivalente a dizer que m é um primo congruente a 3 módulo 4. ■

Exemplo 2.67. Resolva a equação diofantina $y^3 = x^2 + 4$

Demonstração: Temos a fatoração $y^3 = (x + 2i)(x - 2i)$ em $\mathbb{Z}[i]$ e queremos concluir a partir dela que $(x + 2i)$ e $(x - 2i)$ são cubos perfeitos em $\mathbb{Z}[i]$. Observe primeiramente que se π é um irredutível que divide $x + 2i$ e $x - 2i$, então π deve dividir a diferença $4i = -i(1 - i)^4$, ou seja, π é associado a $1 - i$. Assim, podemos escrever

$$x + 2i = u \cdot \pi_1^{e_1} \cdot \pi_2^{e_2} \cdot \cdots \cdot \pi_n^{e_n}$$

$$x - 2i = u \cdot \pi'^{e_1}_1 \cdot \pi'^{e_2}_2 \cdot \cdots \cdot \pi'^{e_n}_n$$

onde $u \in \mathbb{Z}[i]^\times$ e os π_j são irredutíveis dois a dois não associados e $\pi_1 = 1 - i$. Note que π'_j são irredutíveis dois a dois não associados e que, com exceção de $j = 1$, π_j não é associado a nenhum π'_k. Como $(x + 2i)(x - 2i) = y^3$, temos pela fatoração única que π_j e π'_j são os irredutíveis que aparecem na fatoração única de y e que portanto $3|e_j$, com a possível exceção de $j = 1$. Mas como π'_1 e π_1 são associados temos que $2e_1$ deve ser divisível por 3, logo $3|e_1$ também. Por outro lado, toda unidade em $\mathbb{Z}[i]$ é um cubo perfeito em $\mathbb{Z}[i]$, assim concluímos que $x + 2i$ e $x - 2i$ são cubos perfeitos em $\mathbb{Z}[i]$.

Agora, escrevendo $x + 2i = (a + ib)^3$ com $a, b \in \mathbb{Z}$ e expandindo, obtemos $x = a^3 - 3ab^2$ e $2 = 3a^2b - b^3$. Da última equação, temos $b|2$, e testando as possibilidades obtemos as soluções $(a, b) = (\pm 1, 2)$ e $(a, b) = (\pm 1, 1)$, ou seja, $(\pm 11, 5)$ ou $(x, y) = (\pm 2, 2)$. ■

Exemplo 2.68. Toda tripla pitagórica de inteiros positivos, isto é, inteiros positivos a, b, c satisfazendo $a^2+b^2 = c^2$ tais que $\text{mdc}(a, b, c) = 1$, é da forma $(a, b, c) = (2st, s^2-t^2, s^2+t^2)$, para algum par de inteiros positivos s, t de paridades opostas e tal que $s > t$.

Demonstração: Seja (a, b, c) uma tripla pitagórica primitiva, logo $c^2 = a^2 + b^2 = (a + ib)(a - ib)$. Vamos mostrar que $a + ib$ e $a - ib$ são relativamente primos em $\mathbb{Z}[i]$, para isto observe que qualquer divisor comum π de $a + ib$ e $a - ib$ também divide $2a$ e $2b$. Se π não divide 2, então π divide simultaneamente a e b, o que implica que $N(\pi)|N(a) = a^2$ e $N(\pi)|N(b) = b^2$, e assim, $N(\pi)|c^2$, assim, $N(\pi)$ deve ser ± 1, já que $\text{mdc}(a, b, c) = 1$, isto é, π é uma unidade em $\mathbb{Z}[i]$. Portanto $\pi \mid 2$, assim $\pi = 1+i$ ou $\pi = 1-i$. Agora, observe que o fato de $1+i$ ou $1-i$ dividir $a+ib$ implica que a e b possuem a mesma paridade, o que é impossível, uma vez que a e b não podem ser simultaneamente pares pois $\text{mdc}(a, b, c) = 1$ e não podem ser simultaneamente impares, pois teríamos $c^2 = a^2+b^2 \equiv 2 \pmod 4$ o que é uma contradição com o fato de quadrados perfeitos serem congruentes a 0 ou 1 módulo 4. Dessa forma podemos concluir que $a + ib$ e $a - ib$ são relativamente primos em $\mathbb{Z}[i]$, além disso, como vimos que a e b devem ter paridades distintas, vamos supor a par e b ímpar. Pela fatoração única de $\mathbb{Z}[i]$, como $a + ib$ e $a - ib$ são relativamente primos e o produto de ambos é um quadrado perfeito, então ambos devem ser um quadrado perfeito em $\mathbb{Z}[i]$, logo deve existir um $s + it \in \mathbb{Z}[i]$ tal que $a + ib = \epsilon(s + it)^2$, onde $\epsilon \in \mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$. Assim, $a + ib = \epsilon((s^2 - t^2) + i(2st))$. Diante da suposição a par e b ímpar, devemos ter $\epsilon = -i$, e assim $a = 2st$ e $b = s^2 - t^2$, com $s > t$. ■

3 Classificação dos anéis quadráticos norma euclidianos complexos

Neste capítulo mostraremos que o anel quadrático complexo $\mathcal{O}_d$ é norma euclidiano quando $d = -1, -2, -3, -7$ e -11. Mostraremos que eles são os únicos discriminantes tais que o anel quadrático $\mathcal{O}_d$ é um domínio euclidiano.

Teorema 3.1. *$\mathcal{O}_d$ é um anel quadrático complexo norma euclidiano quando $d = -1, -2$, -3, -7, -11.*

Demonstração: Para demonstrar o resultado vamos utilizar o Corolário 2.60 e a Observação 2.61.

Quando $d \equiv 2, 3 \pmod 4$, isto é, $d = -1, -2$, se $\gamma = a + b\sqrt{d}$, com $a, b \in \mathbb{Q}$, tomamos $x, y \in \mathbb{Z}$ tais que $|a - x| \leq \frac{1}{2}$ e $|b - y| \leq \frac{1}{2}$. Assim, se $q = x + y\sqrt{d}$,

$$N(\gamma - q) = N(a - x + (b - y)\sqrt{d}) \leq (a - x)^2 - d(b - y)^2 \leq \frac{1}{4} + |d|\frac{1}{4} < 1.$$

Quando $d \equiv 1 \pmod 4$, isto é, $-3, -7, -11$, se, como acima, $\gamma = a + b\sqrt{d}$ com $a, b \in \mathbb{Q}$, tomamos $y = \frac{v}{2}$ com $v \in \mathbb{Z}$ tal que $|b - y| \leq \frac{1}{4}$ e depois $x = \frac{u}{2}$ com $u \in \mathbb{Z}$, $u \equiv v \pmod 2$, tal que $|a - x| \leq \frac{1}{2}$. Assim, se $q = x + y\sqrt{d}$, então

$$N(\gamma - q) = N(a - x + (b - y)\sqrt{d}) \leq (a - x)^2 - d(b - y)^2 \leq \frac{1}{4} + |d|\frac{1}{16} < 1.$$

■

Agora, nosso objetivo será demonstrar que $\mathcal{O}_d$ é um domínio euclidiano apenas para $d = -1, -2, -3, -7$ e -11. No entanto, para isso, ainda será necessário a utilização de um resultado auxiliar. A fim de demonstrarmos o resultado introduziremos o seguinte teorema

Teorema 3.2. *Seja G um $\mathbb{Z}$-módulo livre e H um submódulo de G. Suponha que $\{x_1, \ldots, x_n\}$ seja uma base para G e $\{y_1, \ldots, y_n\}$ uma base para H. Se para cada i, $y_i = \sum_{j=1}^{n} a_{ij}x_j$, onde $a_{ij} \in \mathbb{Z}$. Então*

$$|G/H| = |det([a_{ij}])|.$$

Demonstração: Veja [3], Teorema 1.17.

Agora, vamos ao resultado.

Corolário 3.3. *Seja $\alpha \in \mathcal{O}_d$. Então*

$$|\mathcal{O}_d/\langle\alpha\rangle| = |N(\alpha)|.$$

Demonstração: Faremos a demonstração do caso $d \equiv 2, 3 \pmod 4$. neste caso $\left\{1, \sqrt{d}\right\}$ é uma $\mathbb{Z}$-base de $\mathcal{O}_d$. Seja $\alpha = a + b\sqrt{d} \in \mathcal{O}_d$, então $\left\{\alpha, \alpha\sqrt{d}\right\} = \left\{a + b\sqrt{d}, bd + a\sqrt{d}\right\}$ é uma $\mathbb{Z}$-base para $\langle\alpha\rangle$. Então, pelo Teorema 3.2,

$$|\mathcal{O}_d/\langle\alpha\rangle| = \left\|\begin{matrix} a & b \\ db & a \end{matrix}\right\| = |a^2 - bd^2| = |N(\alpha)|.$$

O caso $d \equiv 1 \pmod 4$ é análogo, com a diferença que devemos tomar $\left\{1, \frac{1+\sqrt{d}}{2}\right\}$ como a $\mathbb{Z}$-base para $\mathcal{O}_d$. ■

A demonstração do próximo teorema segue o método desenvolvido em [28].

Teorema 3.4. *Seja um inteiro livre de quadrados $d < -11$, então $\mathcal{O}_d$ não é um domínio euclidiano. Mais ainda, $\mathcal{O}_d$ é euclidiano apenas nos casos $d = -1, -2, -3, -7, -11$.*

Demonstração: Seja $d < -11$ livre de quadrados e suponhamos que $\mathcal{O}_d$ seja um domínio euclidiano cuja função euclidiana seja $\phi(x)$. Considere

$$S \coloneqq \{\phi(x) : \ x \in \mathcal{O}_d, \ x \neq 0, \ x \notin U(\mathcal{O}_d)\} \subset \mathbb{N}.$$

Seja $\phi(\alpha)$ o menor elemento de S. Agora, seja $\beta \in \mathcal{O}_d$, então, pela propriedade euclidiana, existem $q, r \in \mathcal{O}_d$ tais que

$$\beta = \alpha q + r,$$

com $r = 0$ ou $\phi(r) < \phi(\alpha)$. Mas pela minimalidade de $\phi(\alpha)$, $\phi(r) < \phi(\alpha)$ só pode ocorrer quando r for uma unidade em $\mathcal{O}_d$, isto é, $r = \pm 1$. Portanto, o anel quociente $\mathcal{O}_d/\langle\alpha\rangle$ possui no máximo três elementos, isto é, os elementos cujos representantes são as possibilidades de r como visto anteriormente. Agora, mostraremos a impossibilidade da existência se α, que será dividido em dois casos: $d \equiv 2, 3 \pmod 4$ e $d \equiv 1 \pmod 4$.

Se $d \equiv 2, 3 \pmod 4$, então da existência de α existem inteiros a, b tais que $\alpha = a + b\sqrt{d}$ e do Corolário 3.3 segue

$$|\mathcal{O}_d/\langle\alpha\rangle| = |N(\alpha)| = a^2 + |d|b^2 \leq 3,$$

o que é impossível quando α não é uma unidade.

Se $d \equiv 1 \pmod 4$, então, podemos escrever $\alpha = \frac{a}{2} + \frac{b}{2}\sqrt{d}$, onde $a \equiv b \pmod 2$, e de maneira análoga

$$|\mathcal{O}_d/\langle\alpha\rangle| = |N(\alpha)| = a^2 + |d|b^2 \leq 4 \cdot 3$$

é impossível quando α não é uma unidade.

Assim resta-nos mostrar quando $d > -11$, ou seja, $d = -5, -6, -10$, o anel quadrático $\mathcal{O}_d$ não é euclidianos. Faremos demostrando que $\mathcal{O}_d$ não é domínio de fatoração única para $d = -5, -6, -10$. Em $\mathcal{O}_{-5}$ temos duas fatorações diferentes em fatores irredutíveis para

$$2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{5}).$$

Para $\mathcal{O}_{-6}$, temos

$$-2 \cdot 3 = (\sqrt{-6})(\sqrt{-6}),$$

onde $2, 3$ e $\sqrt{-6}$ são elementos irredutíveis em $\mathcal{O}_{-6}$. Por fim, em $\mathcal{O}_{-10}$, os irredutíveis 2, 7, $2 + \sqrt{-10}$ e $2 - \sqrt{-10}$ se relacionam como

$$2 \cdot 7 = (2 + \sqrt{-10})(2 - \sqrt{-10}).$$

Com isso demonstramos o resultado ■

A partir dos Teoremas 3.4 e 3.1 não só podemos classificar todos os anéis quadráticos complexos euclidianos, mas também, podemos concluir que há uma equivalência entre anéis quadráticos complexos euclidianos e anéis quadráticos complexos norma euclidianos. Portanto enunciamos:

Teorema 3.5. *Um anel quadrático complexo $\mathcal{O}_d$ é um domínio euclidiano se, e somente se, $d = -1, -2, -3, -7$ e -11. Além disso, a classificação de anéis quadráticos complexos euclidianos coincide com a classificação de anéis quadráticos complexos norma euclidiano.*

Ainda em anéis quadráticos podemos dar um exemplo de uma família de domínios de ideais principais (domínios de fatoração única) que não são domínios euclidianos. Para isto seguiremos a referência [26].

No que se segue adotaremos $\alpha \in \mathbb{C}$ como a raiz de um polinômio quadrático $x^2+tx+q \in \mathbb{Z}[x]$. Em particular, $\mathbb{Z}[\alpha]$ é subconjunto de um anel quadrático.

Lema 3.6. *Seja $\pi \in \mathbb{Z}[\alpha]$ tal que $N(\pi)$ é um número primo, então π é um primo em $\mathbb{Z}[\alpha]$*

Demonstração: Defina $p = N(\pi)$. Então,

$$\left|\left(\frac{\mathbb{Z}[\alpha]}{p\mathbb{Z}[\alpha]}\right)\right| = p^2 \text{ e } \left|\left(\frac{\pi\mathbb{Z}[\alpha]}{p\mathbb{Z}[\alpha]}\right)\right| \neq 1. \tag{3.1}$$

Como p é um número primo e

$$\frac{\mathbb{Z}[\alpha]}{\pi\mathbb{Z}[\alpha]} \cong \frac{(\mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha])}{(\pi\mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha])},$$

segue de 3.1 que $\mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha]$ tem p elementos e logo é um corpo. Portanto, π é um primo em $\mathbb{Z}[\alpha]$. ■

Lema 3.7. *Se $\mathbb{Z}[\alpha]$ não é domínio de fatoração única, então existe um número primo p, mas não primo em $\mathbb{Z}[\alpha]$, com a propriedade: Se $p \mid N(\omega)$, então $p^2 \leq |N(\omega)|$, onde $\omega \in \mathbb{Z}[\alpha]$.*

Demonstração: Seja S o conjunto de todos os elementos de $\mathbb{Z}[\alpha]$ que podem ser escritos como o produto de primos em $\mathbb{Z}[\alpha]$. Sejam $S' = U(\mathbb{Z}[\alpha]) \cup S$ e $W = \mathbb{Z}[\alpha] \setminus S'$. Como $\mathbb{Z}[\alpha]$ não é um domínio de fatoração única, seque que W é diferente do vazio. Seja $\beta \in W$ tal que

$$|N(\beta)| = min\left\{|N(\omega)| : \ \omega \in W, \ \omega \neq 0\right\}. \tag{3.2}$$

Como $\beta \in W$, então β não pode ser um elemento primo em $\mathbb{Z}[\alpha]$, além disso, pela propriedade multiplicativa de N, β deve ser um elemento irredutível, então, pelo lema anterior, $N(\beta)$ não é um número primo. Portanto, existe um primo p tal que

$$p \mid N(\beta) \text{ e } p \leq \sqrt{|N(\beta)|}. \tag{3.3}$$

Note que p não pode ser um primo em $\mathbb{Z}[\alpha]$, pois, caso contrário, como $p \mid N(\beta)$, obteríamos que p seria um associado de β ou β', o que é impossível, uma vez que $\beta \in W$.

Vamos mostrar que p satisfaz a propriedade do anunciado. Seja $\omega \in \mathbb{Z}[\alpha]$ tal que $p \mid \omega$, argumentando de maneira similar ao que fizemos anteriormente, podemos mostrar que $\omega \in W$, logo, utilizando 3.2 e 3.3, obtemos

$$p^2 \leq |N(\beta)| \leq |N(\omega)|.$$

O que completa a demonstração. ■

Lema 3.8. *Seja p um número primo. Então p é um primo em $\mathbb{Z}[\alpha]$ se, e somente se, x^2+tx+q é primo em $\mathbb{Z}_p[x]$*

Demonstração: O resultado é consequência da cadeia de isomorfismos

$$\frac{\mathbb{Z}_p[x]}{(x^2+tx+q)\mathbb{Z}_p[x]} \cong \frac{(\mathbb{Z}[x]/p\mathbb{Z}[x])}{((x^2+tx+q,p)\mathbb{Z}[x]/p\mathbb{Z}[x])} \cong \frac{\mathbb{Z}[x]}{(x^2+tx+q,p)\mathbb{Z}[x]}$$

$$\frac{\mathbb{Z}[x]/p(x^2+tx+q)\mathbb{Z}[x]}{(x^2+tx+q,p)\mathbb{Z}[x]/(x^2+tx+q)\mathbb{Z}[x]} \cong \frac{\mathbb{Z}[\alpha]}{p\mathbb{Z}[\alpha]}.$$

■

Teorema 3.9. *Seja $d \in \mathbb{N}$. Suponha que $\mathbb{Z}\left[\frac{1+\sqrt{-d}}{2}\right]$ não seja um domínio de fatoração única. Então, existe um primo p, que não é um primo em $\mathbb{Z}\left[\frac{1+\sqrt{-d}}{2}\right]$, satisfazendo $p \leq \sqrt{\frac{d}{3}}$.*

Demonstração: Denote $\alpha = \frac{1+\sqrt{-d}}{2}$. Então α é uma raiz de $x^2 - x + \frac{1+d}{4}$ e $N(a+b\alpha) = a^2 + ab + \frac{1+d}{4}b^2$. Como $\mathbb{Z}[\alpha]$ não é um domínio de fatoração única, pelo Lema 3.7, existe um primo p tal que

$$\omega \in \mathbb{Z}[\alpha] \text{ e } p \mid N(\omega) \text{ implica que } p^2 \leq N(\omega). \tag{3.4}$$

Agora, como p não é um primo em $\mathbb{Z}[\alpha]$, pelo Lema 3.8, existe $b \in \mathbb{Z}$ tal que

$$0 \leq b \leq \frac{p+1}{2} \text{ e } b^2 - b + \frac{1+d}{4} \equiv 0 \pmod{p}, \tag{3.5}$$

e como $N(b-\alpha) = b^2 - b + \frac{1+d}{4}$, então $p \mid N(b-\alpha)$. Combinando 3.4 e 3.5, obtemos

$$4p^2 \leq 4N(b-\alpha) = (2b-1)^2 + d \leq p^2 + d,$$

o que nos leva a $p \leq \sqrt{\frac{d}{3}}$. ■

No próximo teorema usaremos a notação $\mathbb{Z}\left[\frac{1+\sqrt{-d}}{2}\right]$ para denotar o anel quadrático $\mathcal{O}_d$.

Teorema 3.10. *Os anéis $\mathbb{Z}\left[\frac{1+\sqrt{-d}}{2}\right]$, com $d \in 3, 7, 11, 19, 43, 67, 163$ são domínios de fatoração única.*

Demonstração: Se $d = 19, 43, 67$, então $\sqrt{\frac{d}{3}} < 5$, além disso, pelo Lema 3.8, 2 e 3 são primos em $\mathbb{Z}\left[\frac{1+\sqrt{-d}}{2}\right]$. Pelo Teorema 3.9, obtemos que $\mathbb{Z}\left[\frac{1+\sqrt{-d}}{2}\right]$ é um domínio de fatoração única.

Se $d = 163$, então $\sqrt{\frac{d}{3}} < 11$, além disso, aplicando o Lema 3.8, obtemos que 2, 3, 5 e 7 são primos em $\mathbb{Z}\left[\frac{1+\sqrt{-d}}{2}\right]$. Pelo Teorema 3.9, obtemos que $\mathbb{Z}\left[\frac{1+\sqrt{-d}}{2}\right]$ é um domínio de fatoração única. ■

Gauss conjecturou que os únicos corpos quadráticos complexo $\mathbb{Q}(\sqrt{-d})$ cujo anel dos inteiros algébricos são domínio de fatoração única são $d = 3, 7, 11, 19, 43, 67, 163$. Essa conjectura foi provada verdadeira por H. M. Stark, veja [27].

4 Anéis quadráticos reais norma euclidianos

A classificação dos anéis quadráticos foi um problema em aberto até o ano de 1952, quando Barnes e Swinnerton-Dyer, em [25], demonstraram que $\mathcal{O}_{97}$ não é norma euclidiano, culminando assim na conclusão da existência de apenas vinte e um corpos quadráticos norma euclidianos (cinco corpos quadráticos complexo e dezesseis corpos quadráticos reais). Devido algumas característica distintas entre os diversos corpos quadráticos é muito difícil desenvolver uma teoria aplicável a todos os casos, diante disso surgiram diferentes métodos de abordar o problema ou parte dele, sendo alguns mais simples e outros mais elaborados. Neste capítulo, iremos introduzir alguns conceitos relacionados à teoria das formas quadráticas binárias e mínimo não homogêneo e mostraremos como essas ideias se relacionam com a classificação de corpos quadráticos norma euclidianos reais e posteriormente, a partir dessas noções, demonstraremos que $\mathcal{O}_d$ é norma euclidiano quando $d = 2$, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73. Seguiremos os trabalhos de Varnavides, [8] e [7].

4.1 Formas quadráticas e anéis quadráticos norma euclidianos

Iniciamos esta seção com alguns conceitos fundamentais sobre formas quadráticas binárias.

Definição 4.1. Uma forma quadrática binária f é uma função $f : \mathbb{R}^2 \to \mathbb{R}$,

$$f(x, y) = ax^2 + bxy + cy^2,$$

onde $a, b, c \in \mathbb{R}$.

Definição 4.2. O discriminante da forma quadrática $f(x, y) = ax^2 + bxy + cy^2$ é definido como $\delta = b^2 - 4ac$.

Observação 4.3. Dado uma forma quadrática binária $f : \mathbb{R}^2 \to \mathbb{R}$, $f(x, y) = ax^2 + bxy + cy^2$, podemos encontrar θ e θ' tais que

$$f(x, y) = a(x - \theta y)(x - \theta' y).$$

Em particular, seguem as igualdades $b = -a(\theta + \theta')$, $c = a\theta\theta'$ e $\delta = a^2(\theta - \theta')$.

Um conceito importante sobre formas quadráticas binárias é o conceito de equivalência entre essas formas.

Definição 4.4. Duas formas quadráticas $f(x, y)$ e $g(x, y)$ são ditas equivalentes se existe uma transformação linear

$$T \in GL(2, \mathbb{Z}) = \left\{ \begin{pmatrix} p & q \\ r & s \end{pmatrix} \mid p, q, r, s \in \mathbb{Z},\ ps - qr = \pm 1 \right\}$$

tal que $g \circ T = f$. Diremos que a transformação T é uma transformação unimodular.

Uma observação mais práticas sobre formas quadráticas binárias equivalentes é a seguinte:

Observação 4.5. Duas formas quadráticas $f(x, y)$ e $g(x, y)$ são equivalentes se existem $p, q, r, s \in \mathbb{Z}$ tais que $f(x, y) = g(px + qy, rx + sy)$ e $ps - qr = \pm 1$.

A importância da definição acima está no fato que formas equivalentes possuem muitas propriedades em comuns. Ao longo do texto veremos algumas dessas propriedades, o que nos permite a opção de escolha de uma forma quadrática mais apropriada para trabalharmos sem perda de propriedades requeridas.

A Definição 4.4 origina uma relação entre formas quadráticas binárias. Claramente, ocorre o seguinte:

Proposição 4.6. *Relação resultante da Definição 4.4 é uma relação de equivalência entre formas quadráticas.*

Lema 4.7. *Seja $f(x, y) = ax^2 + bxy + cy^2$ uma forma quadrática e $T(x, y) = (px + qy, rx + sy)$. Então, $f \circ T(x, y) = kx^2 + lxy + my^2$, onde*

1. $k = ap^2 + bpr + cr^2 = f(p, r)$;
2. $l = 2apq + b(ps + qr) + 2crs$;
3. $m = aq^2 + bqs + cs^2 = f(q, s)$.

Proposição 4.8. *Formas quadráticas equivalentes possuem o mesmo determinante a menos de sinal.*

Demonstração: Sejam $f(x, y)$ e $g(x, y)$ formas quadráticas equivalentes. Sejam δ e δ' o discriminante de $f(x, y)$ e $g(x, y)$, respectivamente. Suponhamos

$$f(x, y) = g(px + qy, rx + sy),$$

para $p, q, r, s \in \mathbb{R}$, onde $ps - qr = \pm 1$. Facilmente, podemos calcular $\delta = (ps - qr)\delta' = \pm\delta'$. ■

Portanto, um exemplo de invariante entre formas equivalentes é o módulo de seus discriminantes.

Exemplo 4.9.

1. As formas quadráticas binárias $f(x, y) = x^2 + y^2$ e $g(x, y) = f(x - y, y) = x^2 - 2xy + 2y^2$ são equivalentes e possuem o mesmo determinante.
2. As formas quadráticas binárias $f(x, y) = x^2 + y^2$ e $g(x, y) = 4x^2 + y^2$ não são equivalentes uma vez que possuem determinantes diferentes.

Lema 4.10. *Seja*

$$f(x,y) = ax^2 + bxy + cy^2$$

uma forma quadrática binária. Sejam p, r inteiros relativamente primos, então exite uma forma quadrática g equivalente a f cujo coeficiente do termo x^2 é $f(p,r)$.

Demonstração: Seja $k = f(p,r)$, onde p, r são inteiros relativamente primos. Logo, existem inteiros q, s tais que $ps - qr = 1$. Considere a forma quadrática $g(x,y) = f(px + qy, rx + sy)$, então $g(x,y)$ é equivalente a $f(x,y)$ e, pelo Lema 4.7, o coeficiente do termo x^2 é $f(p,r)$. ■

Dado um corpo quadrático $\mathbb{Q}(\sqrt{d})$, pelo Teorema 2.41, os inteiros algébricos de $\mathbb{Q}(\sqrt{d})$ podem ser expressos como

$$\begin{cases} a + b\sqrt{d}, \text{ se } d \equiv 2,3 \pmod 4; \\ a + b\left(\frac{1+\sqrt{d}}{2}\right), \text{ se } d \equiv 1 \pmod 4, \end{cases}$$

com $a, b \in \mathbb{Z}$. Defina a forma quadrática

$$N_d(x,y) = \begin{cases} x^2 - dy^2, \text{ se } d \equiv 2,3 \pmod 4; \\ x^2 + xy - \frac{1}{4}(d-1)y^2, \text{ se } d \equiv 1 \pmod 4, \end{cases} \tag{4.1}$$

isto é, $N_d(x,y)$ coincide com a norma do $x + \omega y$ escrito na base $\{1, \omega\}$, onde

$$\begin{cases} \omega = \sqrt{d}, \text{ se } d \equiv 2,3 \pmod 4; \\ \omega = \frac{1+\sqrt{d}}{2}, \text{ se } d \equiv 1 \pmod 4. \end{cases}$$

Pelo Lema 2.59, $\mathbb{Q}(\sqrt{d})$ será norma euclidiano se para todo número $\alpha = x + \sqrt{d}y \in \mathbb{Q}(\sqrt{d})$ existir um inteiro algébrico $\beta = x_0 + \omega y_0$ em $\mathbb{Q}(\sqrt{d})$ que satisfaça

$$|N_d(x + x_0, y + y_0)| < 1.$$

Portanto, temos uma relação entre classificação de anéis quadráticos e forma quadráticas binárias. A seguir desenvolveremos conceitos mais apropriados para lidarmos com cotas de $|N_d(x + x_0, y + y_0)|$.

Definição 4.11. Seja $f(x,y) = ax^2 + bxy + cy^2$ uma forma quadrática. Para números reais x_0, y_0, definimos

$$M(f; x_0, y_0) \coloneqq \inf |f(x + x_0, y + y_0)|$$

tomando valores x, y sobre todos os inteiros.

Definição 4.12. Para uma forma quadrática f definimos o mínimo não homogêneo de $f(x,y)$ como

$$M(f) = \sup M(f; x_0, y_0)$$

onde o supremo é tomado sobre todos os valores reais x_0, y_0.

O resultado a seguir nos diz que o mínimo não homogêneo não varia para formas quadrática binária equivalentes. Propriedade que será essencial futuramente.

Proposição 4.13. *Formas quadráticas binárias equivalentes possuem o mesmo valor para o mínimo não homogêneo $M(f)$.*

Demonstração: Sejam f e f' formas equivalentes e $T \in GL(2,\mathbb{Z})$, com $|det(T)| = 1$ e tal que $f' \circ T = f$. Para todo ponto (x_0, y_0) no plano temos

$$\inf |f(x+x_0, y+y_0)| = \inf |(f' \circ T)(x+x_0, y+y_0))|$$

$$= \inf |f'(T(x+x_0, y+y_0))| = \inf |f'(T(x_0,y_0) + T(x,y))|.$$

Como T é uma bijeção que leva pontos inteiros em pontos inteiros e o ínfimo é tomado sobre todos os pontos inteiros x, y, segue a igualdade

$$\inf |f(x+x_0, y+y_0)| = \inf |f'(T(x_0,y_0) + (x,y))|.$$

Já a igualdade $M(f) = M(f')$ ocorre pois T é uma bijeção de $\mathbb{R}^2$ em $\mathbb{R}^2$ e o supremos é tomado sobre todos os reais x_0, y_0.

Observação 4.14. $x_0 \equiv x \pmod 1$ se, e somente se, existe um número inteiro n tal que $x = x_0 + n$.

Agora, daremos um critério que relaciona anéis quadráticos norma euclidianos e mínimo não homogêneo:

Proposição 4.15. *A fim de que o anel quadrático $\mathcal{O}_d$ seja norma euclidiano é suficiente que se verifique a condição*

$$M(N_d) < 1.$$

De modo contrário, quando um anel quadrático $\mathcal{O}_d$ não é norma euclidiano é imediato que $M(N_d) \geq 1$, o que mais uma vez evidencia como esses conceitos estão intrinsecamente relacionados.

4.2 Aplicação da teoria de formas quadráticas

Introduzida a relação entre formas quadráticas e anéis quadráticos norma euclidianos, vamos desenvolver alguns resultados que nos auxiliarão na demonstração de $M(N_d) < 1$ para os valores $d = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73$.

Lema 4.16. *Sejam A e β números reais. Se $A \geq \frac{1}{4}$ e*

$$\beta^2 \leq A + \frac{1}{4}\lfloor 2A \rfloor^2, \tag{4.2}$$

onde $\lfloor 2A \rfloor$ denota a parte inteira de $2A$, então para qualquer X_0, existe $X \equiv X_0 \pmod 1$ satisfazendo

$$|X^2 - \beta^2| \leq A. \tag{4.3}$$

Demonstração: Iremos dividir a demonstração em dois casos: quando $\beta^2 \leq \frac{1}{4}$ e quando $\beta^2 > \frac{1}{4}$. Primeiramente, assumimos $\beta^2 \leq \frac{1}{4}$. Dado X_0 tome $X \equiv X_0 \pmod 1$ satisfazendo $|X| \leq \frac{1}{2}$. É importante observar que a escolha de X é viável, uma vez que o intervalo $[-\frac{1}{2}, \frac{1}{2}]$ forma um sistema completo de classes módulo 1. Dessa forma, temos

$$|X^2 - \beta^2| = \max\left\{X^2 - \beta^2,\ \beta^2 - X^2\right\} \leq \max\left\{\frac{1}{4} - \beta^2, \beta^2\right\} \leq \frac{1}{4} < A.$$

Agora, suponhamos $\beta > \frac{1}{4}$. Tomando $m = \lfloor 2A \rfloor$, seguem as desigualdades

$$\frac{1}{2}m \leq A < \frac{1}{2}(m+1), \quad \beta^2 \leq A + \frac{1}{4}m^2. \tag{4.4}$$

Agora, tome $l \geq 0$ de forma que

$$l^2 \leq 4\beta^2 - 1 < (l+1)^2. \tag{4.5}$$

Note que, para a escolha de l, é suficiente escolher o maior valor de l que satisfaça $l^2 < 4\beta^2 - 1$. A partir das desigualdades 4.4 e 4.5 segue

$$l^2 \leq 4\beta^2 - 1 \leq 4A + m^2 - 1 < 2(m+1) + m^2 - 1 = (m+1)^2$$

e uma vez que m e l são inteiros não negativos,

$$l \leq m. \tag{4.6}$$

Para X_0 dado, tome X tal que $X \equiv X_0 \pmod 1$ e

$$\frac{1}{2}l \leq |X| \leq \frac{1}{2}(l+1).$$

Observamos que a união dos intervalos $[\frac{1}{2}l, \frac{1}{2}(l+1)]$ e $[-\frac{1}{2}(l+1), -\frac{1}{2}l]$ forma um sistema completo de classes módulo 1, logo é bem definida tal escolha de X. Vamos mostrar que essa escolha de X satisfaz 4.3. Na desigualdade acima, elevando ao quadrado e subtraindo β^2 obtemos

$$\frac{1}{4}l^2 - \beta^2 \leq X^2 - \beta^2 \leq \frac{1}{4}(l+1)^2 - \beta^2.$$

A partir das desigualdades em 4.4, 4.5, 4.6 podemos obter

$$\frac{1}{4}(l+1)^2 - \beta^2 \leq \frac{1}{4}(l+1)^2 - \frac{1}{4}(l^2+1) = \frac{1}{2}l \leq \frac{1}{2}m \leq A.$$

Se $l = m$,

$$\beta^2 - \frac{1}{4}l^2 = \beta^2 - \frac{1}{4}m^2 \leq A.$$

Se $l < m$

$$\beta^2 - \frac{1}{4}l^2 \leq \frac{1}{4}(l+1)^2 - \frac{1}{4}l^2 = \frac{1}{2}(l+1) \leq \frac{1}{2}m \leq A.$$

Portanto, X satisfaz 4.3. ■

Teorema 4.17. *Seja $f(x,y)$ uma forma quadrática binária com discriminante $\delta > 0$. Seja f_1, algum valor de $f(p,r)$ para um par de inteiros coprimos p e r, satisfazendo $0 < |f_1| < \sqrt{\delta}$. Escreva*

$$\alpha^2 = \frac{\delta}{16 f_1^2}. \tag{4.7}$$

Então

$$M(f) \leq \begin{cases} \frac{1}{4}|f_1| & \text{se } \alpha^2 \leq \frac{1}{4}; \\ \alpha^2 |f_1| & \text{se } \frac{1}{4} \leq \alpha^2 \leq \frac{1}{2}. \end{cases} \tag{4.8}$$

Demonstração: Seguindo o Lema 4.10, podemos encontrar uma transformação linear de (x, y) para (X, Y), com coeficientes inteiros e determinante ± 1, tal que a expressão $f(x, y)$ seja escrita como

$$f(x, y) = f_1 X^2 + b_1 XY + c_1 Y^2. \tag{4.9}$$

Colocando f_1 em evidência e completando quadrado, podemos reescrever (4.9) como

$$f(x, y) = f_1 \left(\left(X + \frac{b_1}{2f_1} Y \right)^2 - \frac{\delta}{4f_1^2} Y^2 \right). \tag{4.10}$$

Vamos estimar uma cota superior para $M(f)$. Para um dado valor de Y_0, escolhemos $Y \equiv Y_0 \pmod 1$ tal que $|Y| \leq \frac{1}{2}$. Agora, definimos $\beta^2 = \frac{\delta Y^2}{4f_1^2}$, e assim temos

$$\beta^2 = \frac{\delta Y^2}{4f_1^2} \leq \frac{\delta}{16 f_1^2} = \alpha^2.$$

De acordo com o Lema 4.16, para um dado valor de X_0, podemos encontrar um $X \equiv X_0 \pmod 1$ de modo que

$$\left| \left(X + \frac{b_1}{2f_1} Y \right)^2 - \beta^2 \right| \leq A(\beta),$$

onde $A(\beta)$ é o menor número que satisfaz 4.2 com $A(\beta) \geq \frac{1}{4}$. Assim, podemos escrever

$$M(f, x_0, y_0) \leq |f_1| A(\beta),$$

Portanto, seque que

$$M(f) \leq |f_1| \max A(\beta), \tag{4.11}$$

com $0 \leq \beta \leq \alpha$. Agora, vamos analisar cada caso de 4.8 individualmente.

1. Se $\alpha^2 \leq \frac{1}{4}$, então a condição 4.2 é satisfeita para $A = \frac{1}{4}$. Portanto, a condição 4.11 implica no primeiro resultado afirmado em 4.8.

2. Se $\frac{1}{4} \leq \alpha^2 \leq \frac{1}{2}$, então a condição 4.2 é satisfeita para $A = \alpha^2$. Portanto, obtemos o segundo resultado afirmado em 4.8.

Com isso, demonstramos todas as afirmações feitas em 4.8. ■

Aplicando o teorema anterior às formas quadráticas N_d definidas em 4.1, obtemos o seguinte teorema:

Teorema 4.18. *O anel quadrático $\mathcal{O}_d$ é norma euclidiano quando*

$$d = 2, 3, 5, 6, 7, 13, 17, 21, 33, 37.$$

Demonstração. Utilizando o teorema acima podemos demonstrar o resultado.

1. Para $d = 2$, tome $f_1 = |N_d(0, 1)| = 2$, dessa forma temos $\alpha^2 = \frac{1}{8} \leq \frac{1}{4}$. Pelo caso 1 temos $M(N_d) \leq \frac{1}{2}$.

2. Para $d = 3$, tome $f_1 = |N_d(1, 1)| = 2$, dessa forma temos $\alpha^2 = \frac{3}{16} \leq \frac{1}{4}$. Pelo caso 1 temos $M(N_d) \leq \frac{1}{2}$.

3. Para $d = 5$, tome $f_1 = |N_d(1,1)| = 1$, dessa forma temos $\frac{1}{4} \leq \alpha^2 = \frac{5}{16} \leq \frac{1}{2}$. Pelo caso 2 temos $M(N_d) \leq \frac{5}{16}$.

4. Para $d = 6$, tome $f_1 = |N_d(3,1)| = 3$, dessa forma temos $\alpha^2 = \frac{1}{6} \leq \frac{1}{4}$. Pelo caso 1 temos $M(N_d) \leq \frac{3}{4}$.

5. Para $d = 7$, tome $f_1 = |N_d(2,1)| = 3$, dessa forma temos $\alpha^2 = \frac{7}{36} \leq \frac{1}{4}$. Pelo caso 1 temos $M(N_d) \leq \frac{3}{4}$.

6. Para $d = 13$, tome $f_1 = |N_d(2,1)| = 3$, dessa forma temos $\alpha^2 = \frac{13}{144} \leq \frac{1}{4}$. Pelo caso 1 temos $M(N_d) \leq \frac{3}{4}$.

7. Para $d = 17$, tome $f_1 = |N_d(2,1)| = 2$, dessa forma temos $\frac{1}{4} \leq \alpha^2 = \frac{17}{64} \leq \frac{1}{2}$. Pelo caso 2 temos $M(N_d) \leq \frac{17}{32}$.

8. Para $d = 21$, tome $f_1 = |N_d(1,1)| = 3$, dessa forma temos $\alpha^2 = \frac{7}{48} \leq \frac{1}{4}$. Pelo caso 1 temos $M(N_d) \leq \frac{3}{4}$.

9. Para $d = 33$, tome $f_1 = |N_d(5,2)| = 3$, dessa forma temos $\alpha^2 = \frac{33}{144} \leq \frac{1}{4}$. Pelo caso 1 temos $M(N_d) \leq \frac{3}{4}$.

10. Para $d = 37$, tome $f_1 = |N_d(2,1)| = 3$, dessa forma temos $\frac{1}{4} \leq \alpha^2 = \frac{37}{144} \leq \frac{1}{2}$. Pelo caso 2 temos $M(N_d) \leq \frac{37}{48}$. ■

No entanto, tal abordagem não será suficiente para lidarmos com os casos $d = 11$, 19, 29, 41, 57, 73. Para a discussão dos seis casos iniciaremos introduzindo o seguinte lema e posteriormente faremos sua aplicação nos seis casos citados.

Lema 4.19. *Suponha que β seja um número real e m um inteiro não negativo tais que*

$$\beta^2 \leq \frac{1}{4}(m^2 + 1). \tag{4.12}$$

Seja

$$B_m(\beta) = max\left\{\frac{1}{4}, \frac{1}{2}(m-1), \beta^2 - \frac{1}{4}(m-1)^2\right\}. \tag{4.13}$$

Então para qualquer número real X_0 existe um número real X, com $X \equiv X_0 \pmod 1$, tal que

$$|X^2 - \beta^2| \leq B_m(\beta). \tag{4.14}$$

Mais ainda, é possível escolher X, com $X \equiv X_0 \pmod 1$, tal que

$$|X^2 - \beta^2| < B_m(\beta), \tag{4.15}$$

exceto quando

1. $m = 0$, $\beta = 0$ *e* $X_0 \equiv \frac{1}{2} \pmod 1$,

2. $m = 0$, $\beta^2 = \frac{1}{4}$ *e* $X_0 \equiv 0 \pmod 1$,

3. $m \geq 2$, $\beta^2 \geq \frac{1}{4}((m-1)^2 + 1)$ *e* $X_0 \equiv \frac{1}{2}m \pmod 1$

4. $m \geq 1$, $\beta^2 \geq \frac{1}{4}(m-1)^2$ *e* $X_0 \equiv \frac{1}{2}(m-1) \pmod 1$.

Demonstração: Vamos começar provando o resultado quando $\beta \leq \frac{1}{4}$. Tome $X \equiv X_0 \pmod 1$ tal que $0 \leq |X| \leq \frac{1}{2}$, sendo a desigualdade estrita no lado direito exceto quando

$$X_0 \equiv 0 \pmod 1$$

e a desigualdade estrita no lado esquerdo exceto quando

$$X_0 \equiv \frac{1}{2} \pmod 1.$$

Então

$$|X^2 - \beta^2| \leq \frac{1}{4}$$

sendo a desigualdade estrita exceto quando

$$\beta = 0 \text{ e } X_0 \equiv \frac{1}{2} \pmod 1,$$

ou quando

$$\beta^2 = \frac{1}{4} \text{ e } X_0 = 0 \pmod 1.$$

Isso estabelece o resultado quando $\beta \leq \frac{1}{4}$.

Agora, podemos supor $\beta^2 > \frac{1}{4}$. Se l é um inteiro positivo tal que

$$\beta^2 < \frac{1}{4}(l^2+1) < \frac{1}{4}(m^2+1),$$

então

$$\beta^2 - \frac{1}{4}(l-1)^2 < \frac{1}{4}\Big((l^2+1) - (l^2-1)\Big) = \frac{1}{2}l \leq \frac{1}{2}(m-1).$$

Logo, também ocorrem

$$\frac{1}{4} < \frac{1}{2}(m-1) \text{ e } \frac{1}{2}(l-1) < \frac{1}{2}(m-1).$$

Portanto, por 4.13,

$$B_l(\beta) < B_m(\beta).$$

Consequentemente, quando $\beta^2 > \frac{1}{4}$, é suficiente provar o resultado para m escolhido de modo que ocorra

$$\frac{1}{4}\Big((m-1)^2+1\Big) \leq \beta^2 \leq \frac{1}{4}(m^2+1). \tag{4.16}$$

Suponhamos que m seja escolhido de forma que satisfaça 4.16 e tome $X \equiv X_0 \pmod 1$ tal que

$$\frac{1}{2}(m-1) \leq |X| \leq \frac{1}{2}m. \tag{4.17}$$

Observe que essa escolha de X é possível uma vez que os intervalos $(\frac{1}{2}(m-1), \frac{1}{2}m)$ e $(-\frac{1}{2}m, -\frac{1}{2}(m-1))$ contém todas as classe de resíduos módulos 1. Portanto temos a desigualdade estrita no lado esquerdo de 4.17 exceto quando

$$X_0 \equiv \frac{1}{2}(m-1) \pmod 1,$$

e a desigualdade estrita no lado direito exceto quando

$$X_0 \equiv \frac{1}{2}m \pmod 1.$$

Então, pela desigualdade 4.17,

$$\beta^2 - \frac{1}{4}m^2 \leq \beta^2 - X^2 \leq \beta - \frac{1}{4}(m-1)^2,$$

assim, juntamente com a desigualdade 4.16,

$$-\frac{1}{2}(m-1) = \frac{1}{4}((m-1)^2+1) - \frac{1}{4}m^2 \leq -\frac{1}{4}m^2 \leq \beta^2 - X^2 \leq \beta^2 - \frac{1}{4}(m-1)^2, \quad (4.18)$$

com a desigualdade estrita no lado esquerdo exceto quando

$$\beta^2 = \frac{1}{4}((m-1)^2+1) \text{ e } X_0 \equiv \frac{1}{2}m \pmod 1$$

e desigualdade estrita no lado direito exceto quando

$$X_0 \equiv \frac{1}{2}(m-1)^2 \pmod 1.$$

Agora, observe que

$$\beta^2 - \frac{1}{4}(m-1)^2 > \frac{1}{4} \text{ se } m = 1,$$

e

$$\frac{1}{2}(m-1) > \frac{1}{4}, \text{ se } m > 1.$$

Portanto, por 4.13,

$$\max\left\{\frac{1}{2}(m-1),\ \beta^2 - \frac{1}{4}(m-1)^2\right\} = B_m(\beta).$$

Consequentemente, por 4.18,

$$|X^2 - \beta^2| \leq B_m(\beta).$$

Mais ainda, temos

$$|X^2 - \beta^2| < B_m(\beta)$$

exceto quando

$$\beta^2 = \frac{1}{4}((m-1)^2+1) \text{ e } X_0 \equiv \frac{1}{2}m \pmod 1,$$

neste caso $m \geq 2$ pois $\beta^2 > \frac{1}{4}$, ou quando

$$\beta^2 - \frac{1}{4}(m-1)^2 \geq \frac{1}{2}(m-1) \text{ e } X_0 \equiv \frac{1}{2}(m-1) \pmod 1,$$

neste caso

$$\beta^2 \geq \frac{1}{4}(m^2-1),$$

o que completa a prova do lema. ■

Observamos que o lema anterior é um aprimoramento do Lema 4.16, o que possibilita uma aplicação similar àquela utilizada na demonstração do Teorema 4.17. Dessa forma, usaremos o Lema 4.19 para demonstrar que $\mathcal{O}_d$ é um anel quadrático norma euclidiano para $d = 11, 19, 29, 41, 57$ e 73.

Teorema 4.20. *$\mathcal{O}_d$ é norma euclidiano quando $d = 11, 19, 29, 41, 57, 73$.*

Demonstração. Para os seis casos, $d = 11, 19, 29, 41, 57, 73$, começaremos aplicando uma transformação unimodular integral em $N_d(x, y)$ de modo que tenhamos

$$f_1\left(\left(X + \frac{B}{2f_1}Y\right)^2 - \frac{\delta}{4f_1^2}Y^2\right),$$

onde $f_1 = N_d(p, r)$, para inteiros p e r que são primos entre si, e B é um número inteiro, como fizemos em 4.10.

Precisamos demonstrar que, para quaisquer números reais X_1 e Y_1, existem inteiros u e v que satisfazem a desigualdade

$$|f_1|\left|\left(\left((X_1 + u) + \frac{B}{2f_1}(Y_1 + v)\right)^2 - \frac{\delta}{4f_1^2}(Y_1 + v)^2\right)\right| < 1.$$

Definindo

$$X_0 = X_1 + \frac{B}{2f_1}Y_1 \text{ e } Y_0 = Y_1,$$

e substituindo na expressão acima, seguida da divisão por $|f_1|$, obtemos

$$\left|\left(u + \frac{B}{2f_1}v + X_0\right)^2 - \frac{\delta}{4f_1^2}(v + Y_0)^2\right| < \frac{1}{|f_1|}. \tag{4.19}$$

Com isso encontramos uma expressão adequada à 4.15 que nos permitirá aplicação do resultado anterior. Mas antes, faremos algumas observações a respeito de X_0 e Y_0 a fim de simplificação nos cálculos. Sem perda de generalidade, na expressão acima, podemos assumir que

$$0 \leq X_0 \leq \frac{1}{2} \text{ e } |Y_0| \leq \frac{1}{2}. \tag{4.20}$$

Além disso, utilizando as transformações

$$(u, v) \to (-u, -v) \text{ e } (u, v) \to (-1 - u, -v),$$

de forma apropriada, podemos sempre assumir que

$$0 \leq Y_0 \leq \frac{1}{2} \text{ quando } X_0 = 0 \text{ ou } X_0 = \frac{1}{2}. \tag{4.21}$$

caso 1. Seja $d = 11$, tome $f_1 = N_d(3, 2) = -2$. Aplicando a transformação unimodular

$$x = 3X + 2Y,\ y = X + Y$$

em $N_{11}(x, y)$ e manipulando-a conforme o que foi feito em 4.10 obtemos

$$N_{11}(x, y) = -2\left(\left(X + \frac{5}{2}Y\right)^2 - \frac{11}{4}Y^2\right).$$

Com mais algumas manipulações chegamos na expressão equivalente à construída em 4.19, ou seja,

$$\left|\left(u + \frac{5}{2}v + X_0\right)^2 - \frac{11}{4}(v + Y_0)^2\right| < \frac{1}{2}, \tag{4.22}$$

que é o nosso objetivo a ser demonstrado. Defina

$$\beta^2 = \frac{11}{4}Y_0^2 \leq \frac{11}{16} < \frac{3}{4}; \tag{4.23}$$

Agora, observe que 4.12 é satisfeito com $m = 2$, e de acordo com 4.13, temos $B_2(\beta) = \frac{1}{2}$. Portanto, pelo Lema 4.19, tomando $v = 0$, podemos escolher um inteiro u apropriado, isto é, de forma que u satisfaça 4.19, exceto quando

$$X_0 \equiv \ 1 \pmod 1 \text{ e } \beta^2 = \frac{1}{2}. \tag{4.24}$$

No caso em que 4.24 seja verdadeiro, de acordo com 4.20, 4.21 e 4.23, teremos

$$X_0 = 0 \text{ e } Y_0 = \sqrt{\frac{2}{11}}.$$

neste cenário, tomando $u = -1$ e $v = 2$ temos

$$\left|\left(u + \frac{5}{2}v + X_0\right)^2 - \frac{11}{4}(v + Y_0)^2\right| = \left|(-1+5)^2 - \frac{11}{4}\left(2 + \sqrt{\frac{2}{11}}\right)^2\right|$$

$$= \left|4^2 - (4.02\ldots)^2\right| < \frac{1}{2}.$$

Portanto, em qualquer caso, existem inteiros u e v que satisfazem 4.22.

caso 2. Quando $d = 29$, tome $f_1 = N_{29}(2, 1) = -1$. Aplicando a transformação unimodular

$$x = 2X + Y,\ y = X + Y,$$

obtemos

$$f(x, y) = -\left(\left(X^2 + \frac{7}{2}Y\right)^2 - \frac{29}{4}Y^2\right).$$

Agora, encontrando a forma equivalente à construída 4.19, temos

$$\left|\left(u + \frac{7}{2}v + X_0\right)^2 - \frac{29}{4}(v + Y_0)^2\right| < 1. \tag{4.25}$$

Escreva

$$\beta^2 = \frac{29}{4}Y_0^2 \leq \frac{29}{16} < \frac{8}{4} < \frac{10}{4}. \tag{4.26}$$

Observe que 4.12 é satisfeito com $m = 3$ e, por 4.13, $B_3(\beta) = 1$. Então pelo Lema 4.19, 4.25 é satisfeito quando tomamos $v = 0$ e um inteiro apropriado u, exceto quando

$$X_0 \equiv \frac{3}{2} \pmod 1 \text{ e } \beta^2 = \frac{5}{4}. \tag{4.27}$$

Contudo, a validade de 4.27, juntamente com 4.20, 4.21 e 4.26, implica que

$$X_0 = \frac{1}{2} \text{ e } Y_0 = \sqrt{\frac{5}{29}}.$$

Neste caso tomando $u = -1,\ v = 2$ temos

$$\left|\left(u+\frac{7}{2}v+X_0\right)^2-\frac{29}{4}\left(v+Y_0\right)^2\right|$$
$$=\left|(6.5)^2-\frac{29}{4}\left(2+\sqrt{\frac{5}{29}}\right)^2\right|$$
$$=\left|(6.5)^2-(6.503\ldots)\right|<1.$$

Portanto em qualquer caso existem inteiros u, v satisfazendo 4.25.

caso 3. Quando $d = 41$, tome $f_1 = N_{41}(2, 1) = -4$. Aplicando a transformação unimodular

$$x = 2X + Y,\ y = X + Y,$$

obtemos

$$f(x, y) = -4\left(\left(X^2+\frac{13}{8}Y\right)^2-\frac{41}{64}Y^2\right).$$

Agora, encontrando a forma em 4.19, temos

$$\left|\left(u+\frac{13}{8}v+X_0\right)^2-\frac{41}{64}\left(v+Y_0\right)^2\right|<\frac{1}{4}. \tag{4.28}$$

Defina

$$\beta^2=\frac{41}{64}Y_0^2<\frac{1}{4}. \tag{4.29}$$

Então 4.12 é satisfeito com $m = 0$ e, de acordo com a definição 4.13, $B_0(\beta) = \frac{1}{4}$. Tomando $v = 0$, podemos, de acordo com o Lema 4.19, escolher um valor apropriado para u que satisfaça 4.28, a menos que ocorra

$$X_0\equiv\frac{1}{2}\pmod 1 \text{ e } \beta^2=0. \tag{4.30}$$

Por sua vez, a validade de 4.30, juntamente com 4.20 e 4.29, implicam que

$$X_0=\frac{1}{2} \text{ e } Y_0=0.$$

Para esse caso específico, tome $u = 2,\ v = -1$ e assim, temos

$$\left|\left(u+\frac{13}{8}v+X_0\right)^2-\frac{41}{64}(v+Y_0)^2\right|$$
$$=\left|\left(2-\frac{13}{8}+\frac{1}{2}\right)^2-\frac{41}{64}(-1)^2\right|$$
$$=\left|\left(\frac{7}{8}\right)^2-\frac{41}{64}\right|=\frac{1}{8}<\frac{1}{4}.$$

Portanto em qualquer caso existem inteiros u, v satisfazendo 4.28.

caso 4. Quando $d = 57$, tome $f_1 = N_{57}(10, 3) = 4$. Aplicando a transformação unimodular

$$x = 10X + 3Y,\ y = 3X + Y,$$

obtemos

$$f(x,y) = 4\left(\left(X^2 + \frac{5}{8}Y\right)^2 - \frac{57}{64}Y^2\right),$$

seguida das manipulações apropriadas, obtemos a forma descrita em 4.19,

$$\left|\left(u + \frac{5}{8}v + X_0\right)^2 - \frac{57}{64}(v + Y_0)^2\right| < \frac{1}{4}. \tag{4.31}$$

Escreva

$$\beta^2 = \frac{571}{64}Y_0^2 < \frac{1}{4}. \tag{4.32}$$

Observe que tomando $m = 0$, então 4.12 é satisfeito, e, mais ainda, $B_0(\beta) = \frac{1}{4}$. Tomando $v = 0$ e aplicando o Lema 4.31, temos, então, garantido a existência de um u apropriado, satisfazendo 4.31, exceto quando

$$X_0 \equiv \frac{1}{2} \pmod 1 \text{ e } \beta^2 = 0. \tag{4.33}$$

Neste caso, 4.20, 4.29 e 4.33 implicam que

$$X_0 = \frac{1}{2} \text{ e } Y_0 = 0.$$

Agora tomando $u = 1,\ v = 1$ temos

$$\begin{aligned}
&\left|\left(u + \frac{5}{8}v + X_0\right)^2 - \frac{57}{64}(v + Y_0)^2\right| \\
&= \left|\left(2 - \frac{5}{8} + \frac{1}{2}\right)^2 - \frac{57}{64}\right| \\
&= \left|\left(\frac{7}{8}\right)^2 - \frac{57}{64}\right| < \frac{1}{4}.
\end{aligned}$$

Portanto em qualquer caso existem inteiros u, v satisfazendo 4.31.

caso 5. Quando $d = 73$, tome $f_1 = 4$. Aplicando a transformação unimodular

$$x = 34X + 15Y,\ y = 9X + 4Y,$$

obtemos

$$f(x,y) = 4\left(\left(X^2 + \frac{5}{8}Y\right)^2 - \frac{73}{64}Y^2\right).$$

Agora, transformando-a para a forma em 4.19, temos

$$\left|\left(u + \frac{5}{8}v + X_0\right)^2 - \frac{73}{64}(v + Y_0)^2\right| < \frac{1}{4}. \tag{4.34}$$

Agora, temos que provar que para todos reais X_0, Y_0 satisfazendo 4.20 existem inteiros u, v satisfazendo 4.34. Pela complexidade desse caso, vamos considerar os casos separadamente:

1. (a) $0 \le X_0 < \frac{1}{2}$, $Y_0 = 0$;
   (b) $X_0 = \frac{1}{2}$, $Y_0 = 0$.

2. $0 \leq X_0 \leq \frac{1}{2}$, $0 < |Y_0| < \frac{4}{\sqrt{73}}$.

3. (a) $0 \leq X_0 \leq \frac{3}{16}$, $-\frac{1}{2} \leq Y_0 \leq -\frac{4}{\sqrt{73}}$;
   (b) $\frac{3}{16} < X_0 \leq \frac{1}{2}$, $-\frac{1}{2} \leq Y_0 \leq -\frac{4}{\sqrt{73}}$.

4. (a) $0 \leq X_0 \leq 0.105$, $\frac{4}{\sqrt{73}} \leq Y_0 \leq \frac{1}{2}$;
   (b) $0.105 \leq X_0 \leq 0.15$, $\frac{4}{\sqrt{73}} \leq Y_0 \leq \frac{1}{2}$;
   (c) $0.15 \leq X_0 \leq \frac{3}{16}$, $\frac{4}{\sqrt{73}} \leq Y_0 \leq \frac{1}{2}$;
   (d) $\frac{3}{16} \leq X_0 \leq \frac{1}{2}$, $\frac{4}{\sqrt{73}} \leq Y_0 \leq \frac{1}{2}$.

1. Em **(a)**, 4.34 é satisfeito com $u = v = 0$.
Em **(b)** tome $u = -1$, $v = 1$ e assim temos

$$\left|\left(u - \frac{5}{8}v + X_0\right)^2 - \frac{73}{64}(v + Y_0)^2\right|$$

$$= \left|\left(-1 - \frac{5}{8} + \frac{1}{2}\right)^2 - \frac{73}{64}\right| = \left|\frac{81}{64} - \frac{73}{64}\right| < \frac{1}{4},$$

e 4.34 é satisfeito.

2. Temos

$$-\frac{1}{4} < -\frac{73}{64}Y_0^2 \leq X_0^2 - \frac{73}{64}Y_0^2 < X_0^2 \leq \frac{1}{4},$$

portanto 4.34 é satisfeito com $u = v = 0$.

3. No caso **(a)**, 4.34 é satisfeito tomando $u = v = 1$. De fato, nestas condições, mostraremos os valores máximos e mínimos de $\left(1 + \frac{5}{8} + X_0\right)^2 - \frac{73}{64}(1 + Y_0)^2$ possuem módulo menor que $\frac{1}{4}$:

$$\begin{cases} \left|(1 - \frac{5}{8} + \frac{3}{16})^2 - \frac{73}{64}(1 - \frac{1}{2})^2\right| = \left|\frac{81}{256} - \frac{73}{256}\right| < \frac{1}{4} \\ \left|(1 - \frac{5}{8} + 0)^2 - \frac{73}{64}(1 - \frac{4}{\sqrt{73}})^2\right| = |(0.375)^2 - (0.568\ldots)^2| < \frac{1}{4} \end{cases}$$

No caso **(b)** temos

$$-\frac{1}{4} = \left(\frac{3}{16}\right)^2 - \frac{73}{64}\left(\frac{1}{2}\right)^2 < X_0^2 - \frac{73}{64}Y_0^2 < \frac{1}{4},$$

portanto 4.34 é satisfeito tomando $u = v = 0$.

4. Em cada caso, mostraremos que existem inteiros u e v tais que os valores máximos e mínimos de $\left(u + \frac{5}{8}v + X_0\right)^2 - \frac{73}{64}(v + Y_0)^2$ tenha valor absoluto menor que $\frac{1}{4}$.

Em **(a)**, 4.34 é satisfeito se tomarmos $u = v = -1$. De fato

$$\begin{cases} \left|\left(1 - \frac{5}{8} + 0\right)^2 - \frac{73}{64}(-1 + \frac{1}{2})^2\right| = \left|\left(\frac{3}{8}\right)^2 - (\frac{73}{256})^2\right| < \frac{1}{4} \\ \left|(1 - \frac{5}{8} + 0.105)^2 - \frac{73}{64}(-1 + \frac{4}{\sqrt{73}})^2\right| = |(0.27)^2 - (0.5680\ldots)^2| < \frac{1}{4} \end{cases}$$

Em **(b)**, 4.34 é satisfeito quando tomamos $u = -3$ e $v = -2$. De fato

$$\begin{cases} \left|(3-\frac{10}{8}+0.105)^2-\frac{73}{64}(-2+\frac{1}{2})^2\right| = \left|(-1.645)^2-\frac{73}{256}\frac{9}{4}\right| < \frac{1}{4} \\ \left|(-3-\frac{10}{8}+0.15)^2-\frac{73}{64}(-2+\frac{4}{\sqrt{73}})^2\right| = |(-1.6)^2-(1.63\ldots)^2| < \frac{1}{4} \end{cases}$$

Em **(c)**, 4.34 é satisfeito se tomarmos $u = 2$ e $v = 1$. De fato

$$\begin{cases} \left|(2-\frac{5}{8}+0.105)^2-\frac{73}{64}(1+\frac{4}{\sqrt{73}})^2\right| = |(1.5625)^2-(1.568\ldots)^2| < \frac{1}{4} \\ \left|(2-\frac{5}{8}+0.15)^2-\frac{73}{64}(1+\frac{1}{2})^2\right| = |(-1.525)^2-2.56\ldots| < \frac{1}{4} \end{cases}$$

O caso **(d)** é similar ao caso **(b)** de **3**, e isso conclui a prova do caso $d = 73$.

6. Quando $d = 19$, tome $f_1 = 5$. Aplicando a transformação unimodular

$$x = 9X + 4Y,\ y = 2X + Y,$$

obtemos

$$f(x,y) = 5\left(\left(X^2+\frac{2}{5}Y\right)^2-\frac{19}{25}Y^2\right).$$

Agora, encontrando a forma em descrita em 4.19, temos

$$\left|\left(u-\frac{2}{5}v+X_0\right)^2-\frac{19}{25}(v+Y_0)^2\right| < \frac{1}{5},$$

ou, equivalentemente,

$$|(5u-2v+5X_0)^2-19(v+Y_0)^2| < 5. \tag{4.35}$$

Tomando $u = v = 0$ em 4.35 vemos que é satisfeita exceto quando

$$\sqrt{5} = 2.236\cdots \le 5X_0 \le 2.5,\ 0 \le Y_0 \le \frac{1}{2}\sqrt{\frac{5}{19}} = 0.2564\ldots. \tag{4.36}$$

Para provar que 4.35 é satisfeito para valores inteiros u e v quando X_0 e Y_0 satisfazem a condição 4.36 consideraremos os casos **A**, **B**, **C**, **D**, **E** e **F**.

Caso A.

(a) $\sqrt{5} \le 5X_0 \le 2.5$, $0 \le Y_0 < 5\sqrt{\frac{1.01}{19}} - 1 = 0.1527\ldots$;

(b) $\sqrt{5} \le 5X_0 < 2.5$, $Y_0 = \sqrt{\frac{1.01}{19}} - 1 = 0.1527\ldots$;

(c) $5X_0 = 2.5$, $Y_0 = \sqrt{\frac{1.01}{19}} - 1 = 0.1527\ldots$;

(d) $\sqrt{5} \le 5X_0 \le 2.5$, $\sqrt{\frac{1.01}{19}} - 1 = 0.1527\cdots < Y_0 \le \frac{1}{2}\sqrt{\frac{5}{19}}$.

Em **(a)** tome $u = -1$ e $v = 1$. Então

$$\begin{cases} \left|(-5-2v+\sqrt{5})^2-19(1)^2\right| = |(4.764\ldots)^2-19| = |22.68\cdots-19| < 5, \\ \left|(-5-2+2.5)^2-19\left(5\sqrt{\frac{1.01}{19}}\right)^2\right| < |20.25-25.25| = 5. \end{cases}$$

Em **(b)** tome $u = -1$ e $v = 1$ e obtemos o resultado como no caso **(a)**.

Em **(c)** tome $u = 6$ e $v = 5$. Então

$$\left|(30 - 10 + 2.5)^2 - 19(5.1527\ldots)^2\right| < |506.25 - 504.45\ldots| < 5.$$

Em **(d)** tome $u = v = 1$. Então

$$\begin{cases} \left|(5 - 2 + 2.5)^2 - 19\left(5\sqrt{\frac{1.01}{19}}\right)^2\right| < |30.25 - 20.25| = 5, \\ \left|(5 - 2 + \sqrt{5})^2 - 19\left(1 + \frac{1}{2}\sqrt{\frac{5}{19}}\right)^2\right| < |(5.236\ldots)^2 - 19(1.256\ldots)^2| = |27.41\cdots - 29.99\ldots| < 5. \end{cases}$$

Caso B.

$$\sqrt{5} \leq 5X_0 \leq 2.338, \begin{cases} (a) \ -0.09 \leq Y_0 \leq 0, \\ (b) \ -0.157 \leq Y_0 \leq -0.09, \\ (c) \ -\frac{1}{2}\sqrt{\frac{5}{19}} \leq Y_0 \leq -0.157. \end{cases}$$

Em **(a)** tome $u = 0$ e $v = -1$. Então

$$\begin{cases} |(2 + 2.338)^2 - 19(-1)^2| < |18.81 - 19| < 5, \\ |(2 + 2.336\ldots)^2 - 19(-1.09)^2)^2| = |17.94\cdots - 22.57\ldots| < 5. \end{cases}$$

Em **(b)** tome $u = v = 2$. Então

$$\begin{cases} |(10 - 4 + 2.338)^2 - 19(2 - 0.157)| < |65.52 - 64.53| < 5, \\ |(10 - 4 + 2.338)^2 - 19(2 - 0.09)^2)^2| = |67.8\cdots - 69.3\ldots| < 5. \end{cases}$$

Em **(c)** tome $u = v = 0$. Então

$$\begin{cases} |(2.338)^2 - 19(-0.157)| = |5.466\cdots - 69.3\ldots| < 5, \\ \left|(2.338)^2 - 19(-\frac{1}{2}\sqrt{\frac{5}{19}})^2\right| = |5 - 1.25| < 5. \end{cases}$$

Caso C.

$$2.338 \leq 5X_0 \leq 2.347, \begin{cases} (a) \ -0.11 \leq Y_0 \leq 0, \\ (b) \ -0.15 \leq Y_0 \leq -0.1, \\ (c) \ -0.159 \leq Y_0 \leq -0.15, \\ (d) \ -0.165 \leq Y_0 \leq -0.159, \\ (e) \ -\frac{1}{2}\sqrt{\frac{5}{19}} \leq Y_0 \leq -0.165. \end{cases}$$

Em **(a)** tome $u = 0$ e $v = -1$. Então

$$\begin{cases} |(2 + 2.347)^2 - 19(-1)^2| < |18.89 - 19| < 5, \\ |(2 + 2.338\ldots)^2 - 19(-1.11)^2)^2| = |18.81\cdots - 23.40\ldots| < 5. \end{cases}$$

Em **(b)** tome $u = 2$ e $v = -1$. Então

$$\begin{cases} |(10 + 10 + 2.347)^2 - 19(-5.11)^2| = |499.38\cdots - 498.07\ldots| < 5, \\ |(10 + 10 + 2.338\ldots)^2 - 19(-5.15)^2)| = |498.98\cdots - 503.92\ldots| < 5. \end{cases}$$

Em **(c)** tome $u = -6$ e $v = 12$. Então

$$\begin{cases} |(-30 - 24 + 2.338)^2 - 19(12 - 0.159)^2| = |2668.962\cdots - 2663.976\ldots| < 5, \\ |(-30 - 24 - 2.347\ldots)^2 - 19(12 - 0.159)^2| = |2668.03\cdots - 2668.03\ldots| < 5. \end{cases}$$

Em **(d)** tome $u = -6$ e $v = 12$. Então

$$\begin{cases} |(175 - 56 + 2.347)^2 - 19(28 - 0.165)^2| = |14725.09\cdots - 14720.95\ldots| < 5, \\ |(175 - 56 + 2.338\ldots)^2 - 19(28 - 0.59)^2| = |14722.91\cdots - 14727.30\ldots| < 5. \end{cases}$$

Em **(e)** tome $u = v = 0$. Então

$$\begin{cases} |(2.347)^2 - 19(0.165)^2| = |5.508\cdots - 0.517\ldots| < 5, \\ \left|(2.338\ldots)^2 - 19(-\frac{1}{2}\sqrt{\frac{5}{19}})^2\right| = |5.46\cdots - 1.25| < 5. \end{cases}$$

Caso D.

$$2.347 \leq 5X_0 \leq 2.36, \begin{cases} (a) \ -0.12 \leq Y_0 \leq 0, \\ (b) \ -0.15 \leq Y_0 \leq -0.12, \\ (c) \ -0.16 \leq Y_0 \leq -0.15, \\ (d) \ -0.1626 \leq Y_0 \leq -0.16, \\ (e) \ -0.2 \leq Y_0 \leq -1.626, \\ (e) \ -\frac{1}{2}\sqrt{\frac{5}{19}} \leq Y_0 \leq -0.2. \end{cases}$$

Em **(a)** tome $u = 0$ e $v = -1$. Então

$$\begin{cases} |(2 + 2.36)^2 - 19(-1)^2| = |19.00\cdots - 19| < 5, \\ |(2 + 2.347)^2 - 19(-1.12)^2| = |18.89\cdots - 23.83\ldots| < 5. \end{cases}$$

Em **(b)** tome $u = v = 2$. Então

$$\begin{cases} |(10 - 4 + 2.36)^2 - 19(2 - 0.15)^2| = |69.88\cdots - 65.02\ldots| < 5, \\ |(10 - 4 + 2.347)^2 - 19(2 - 0.12)^2| = |69.55\cdots - 67.15\ldots| < 5. \end{cases}$$

Em **(c)** tome $u = -6$ e $v = 12$. Então

$$\begin{cases} |(-30 - 24 + 2.347)^2 - 19(12 - 16)^2| = |2668.03\cdots - 2663.52\ldots| < 5, \\ |(-30 - 24 + 2.36)^2 - 19(28 - 0.15)^2| = |2666.68\cdots - 2668.02\ldots| < 5. \end{cases}$$

Em **(d)** tome $u = 35$ e $v = 28$. Então

$$\begin{cases} |(175 - 56 + 2.36)^2 - 19(28 - 0.1626)^2| = |14728.24\cdots - 14723.49\ldots| < 5, \\ |(175 - 56 + 2.347)^2 - 19(28 - 0.16)^2| = |14725.09\cdots - 14726.24\ldots| < 5. \end{cases}$$

Em **(e)** tome $u = 7$ e $v = 6$. Então

$$\begin{cases} |(35 - 12 + 2.36)^2 - 19(-0.2)^2| = |5.56\cdots - 0.76| < 5, \\ |(35 - 12 + 2.347)^2 - 19(6 - 0.1626)^2| = |642.47\cdots - 647.42\ldots| < 5. \end{cases}$$

Em **(f)** tome $u = v = 0$. Então

$$\begin{cases} |(2.36)^2 - 19(0.20)^2| = |5.56\cdots - 0.76| < 5, \\ \left|(2.347)^2 - 19(-\frac{1}{2}\sqrt{\frac{5}{19}})^2\right| = |5.50\cdots - 1.25| < 5. \end{cases}$$

Caso E.

$$2.36 \leq 5X_0 \leq 2.425, \begin{cases} (a) \ -0.12 \leq Y_0 \leq 0, \\ (b) \ -0.15 \leq Y_0 \leq -0.12, \\ (c) \ -0.16 \leq Y_0 \leq -0.15, \\ (d) \ -0.188 \leq Y_0 \leq -0.162, \\ (e) \ -0.2 \leq Y_0 \leq -1.626, \\ (e) \ -\frac{1}{2}\sqrt{\frac{5}{19}} \leq Y_0 \leq -1.88. \end{cases}$$

Em **(a)** tome $u = 0$ e $v = -1$. Então

$$\begin{cases} |(2 + 2.425)^2 - 19(-1)^2| = |19.58\cdots - 19| < 5, \\ |(2 + 2.36)^2 - 19(-1.12)^2| = |19.00\cdots - 23.83\ldots| < 5. \end{cases}$$

Em **(b)** tome $u = v = 0$. Então

$$\begin{cases} |(10 + 10 + 2.425)^2 - 19(-5.12)^2| = |502.88\cdots - 498.07| < 5, \\ |(10 + 10 + 2.36)^2 - 19(-5.15)^2| = |501.01\cdots - 503.92\ldots| < 5. \end{cases}$$

Em **(c)** subdividiremos o intervalo que contém $5X_0$ em dois intervalos e consequentemente em dois casos:

$$\begin{cases} (c1) \ 2.36 \leq 5X_0 \leq 2.39, \\ (c2) \ 2.39 \leq 5X_0 \leq 2.425, \end{cases}$$

Em **(c1)** tome $u = -6$ e $v = 12$. Então

$$\begin{cases} |(-30 - 24 + 2.36)^2 - 19(12 - 0.162)^2| = |2666.68\cdots - 2662.62\ldots| < 5, \\ |(-30 - 24 + 2.39)^2 - 19(12 - 0.15)^2| = |2663.59\cdots - 2668.02\ldots| < 5. \end{cases}$$

Em **(c2)** tome $u = -2$ e $v = -5$. Então

$$\begin{cases} |(10 + 10 + 2.425)^2 - 19(-5.15)^2| = |502.88\cdots - 503.92\ldots| < 5, \\ |(10 + 10 + 2.39)^2 - 19(-5.15)^2| = |501.31\cdots - 506.27\ldots| < 5. \end{cases}$$

Em **(d)** tome $u = 7$ e $v = 6$. Então

$$\begin{cases} |(35 - 12 + 2.425)^2 - 19(6 - 0.188)^2| = |646.43\cdots - 641.80\ldots| < 5, \\ |(35 - 12 + 2.36)^2 - 19(6 - 0.162)^2| = |643.12\cdots - 647.56\ldots| < 5. \end{cases}$$

Em **(e)** tome $u = -2$ e $v = -1$. Então

$$\begin{cases} |(-10 + 2 + 2.36)^2 - 19(-1.188)^2| = |31.809\cdots - 26.815\ldots| < 5, \\ |(-10 + 2 + 2.425)^2 - 19(-1.256\ldots)^2| = |31.08\cdots - 29.97\ldots| < 5. \end{cases}$$

Caso F.

$$2.425 \leq 5X_0 \leq 2.5, \begin{cases} (a) \ -0.137 \leq Y_0 \leq 0, \\ (b) \ -0.170 \leq Y_0 \leq -0.137, \\ (c) \ -0.172 \leq Y_0 \leq -0.170, \\ (d) \ -\frac{1}{2}\sqrt{\frac{5}{19}} \leq Y_0 \leq -0.172. \end{cases}$$

Em **(a)** tome $u = 0$ e $v = -1$. Então

$$\begin{cases} |(2 + 2.5)^2 - 19(-1)^2| = |20.25 - 19| < 5, \\ |(2 + 2.425)^2 - 19(-1.137\ldots)^2| = |19.58\cdots - 24.56\ldots| < 5. \end{cases}$$

Em **(b)** tome $u = 2$ e $v = -5$. Então

$$\begin{cases} |(10 + 10 + 2.5)^2 - 19(-5.137)^2| = |506.25 - 501.38\ldots| < 5, \\ |(10 + 10 + 2.425)^2 - 19(-5.170)^2| = |502.88\cdots - 507.84\ldots| < 5. \end{cases}$$

Em **(c)** tome $u = 7$ e $v = 6$. Então

$$\begin{cases} |(35 - 12 + 2.5)^2 - 19(6 - 0.172)^2| = |650.25 - 645.34\ldots| < 5, \\ |(35 - 12 + 2.425)^2 - 19(6 - 0.170)^2| = |646.43\cdots - 645.78\ldots| < 5. \end{cases}$$

Em **(d)** tome $u = -2$ e $v = -1$. Então

$$\begin{cases} |(-10 + 2 + 2.425))^2 - 19(1.172)^2| = |31.080\cdots - 26.098\ldots| < 5, \\ |(-10 + 2 + 2.5)^2 - 19(-1.256\ldots)^2| = |30.25 - 29.97\cdots - 645.78\ldots| < 5. \end{cases}$$

o que completa a prova do caso $d = 19$. ■

A partir dos Teoremas 4.18 e 4.20 podemos enunciar

Teorema 4.21. *O anel quadrático $\mathcal{O}_d$ é norma euclidiano quando*

$$d = 2, 3, 5, 6, 7, 13, 11, 17, 19, 21, 29, 33, 37, 41, 57, 73.$$

No restante do trabalho demonstraremos que os anéis quadráticos citado no teorema anterior são os únicos anéis quadráticos reais norma euclidianos.

5 Finitude dos anéis quadráticos reais norma euclidianos

Diversas abordagens surgiram com o intuito de estabelecer ao menos a finitude dos anéis quadráticos norma euclidianos, seja de forma geral ou sob certas condições relacionadas ao discriminante dos anéis. Poderíamos citar, por exemplo, o trabalho de P. Erdös and Ch. Ko [24] onde foi demonstrado que para p primo suficientemente grande não há anéis quadráticos norma euclidianos $\mathcal{O}_p$ quando $p \equiv 1, 17, 23 \pmod{24}$, bem como o trabalho de H. Heilbronn [23] onde foi demonstrado um resultado análogo para o caso $\mathcal{O}_d$ onde d é um inteiro positivo composto. Esses estudos, somados à pesquisas anteriores, culminaram, em 1938, na comprovação da finitude dos anéis quadráticos norma euclidianos. Contudo, ainda não foi possível estabelecer um limite superior para o conjunto dos discriminantes de anéis quadráticos reais norma euclidianos. Assim sendo, tal resultado é pouco prático para lidar com a classificação completa dos corpos quadráticos. No entanto, em 1948, no trabalho [9], H. Davenport estabeleceu, por meio da teoria das formas quadráticas binárias, um limite superior para o discriminante dos corpos quadráticos norma euclidianos. É esse desenvolvimento que exploraremos neste capítulo.

Diante disso, o propósito deste capítulo será encontrar um inteiro d_0 de modo que o anel quadrático $\mathcal{O}_d$ não seja norma euclidiano para todo $d \geq d_0$. Novamente, como feito no Capítulo 4, utilizaremos a teoria das formas quadráticas binárias. No entanto, uma vez interessados em situações não euclidianas, investigaremos condições para que o mínimo não homogêneo $M(f)$ de uma forma quadrática binária f seja maior do que 1, ou seja, procuraremos exibir a existência de números reais x_0 e y_0 tais $|f(x+x_0, y+y_0)| > 1$, para todos inteiros x e y. Em seguida, veremos condições suficientes sobre a forma quadrática binária f de modo que a escolha de x_0 e y_0 possa ser tomada no conjunto dos números racionais, de onde surgirão aplicações imediatas sobre as formas N_d definidas em 4.1.

5.1 Resultados sobre formas quadráticas

O objetivo da seção será demonstrar o seguinte teorema:

Teorema 5.1. *Seja*

$$f(x, y) = ax^2 + bxy + cy^2 = a(x + \theta y)(x + \theta' y)$$

uma forma quadrática com coeficientes reais a, b, c. Suponhamos que $a \neq 0$ e que θ e θ' são números irracionais. Então, existem números reais p e q tais que

$$|f(x + p, y + q)| > \frac{1}{128}\sqrt{\delta}, \tag{5.1}$$

para todos inteiros x, y, onde δ é o discriminante da forma quadrática $f(x, y)$.

No entanto, será necessário a introdução de algumas definições, bem como, alguns lemas, que nos auxiliarão no nosso objetivo. Iniciamos dando a seguinte definição:

Definição 5.2. Uma forma quadrática binária

$$f(x, y) = ax^2 + bxy + cy^2 = a(x + \theta y)(x + \theta' y),$$

onde $a, b, c, \theta, \theta' \in \mathbb{R}$, será dita reduzida se

$$\theta > 2, \quad \frac{1 - \sqrt{5}}{2} = -0.618 \cdots \leq \theta' \leq \frac{3 - \sqrt{5}}{2} = 0.382 \ldots . \tag{5.2}$$

Lema 5.3. *Se $f(x, y) = ax^2 + bxy + cy^2 = a(x + \theta y)(x + \theta' y)$ é uma forma quadrática binária com discriminante estritamente positivo, onde θ e θ' são números irracionais, então $f(x, y)$ é equivalente a alguma forma quadrática binária reduzida.*

Demonstração: Denote

$$M = \inf \{ |f(x, y)|, \ (x, y) \in \mathbb{Z} \times \mathbb{Z} \setminus \{(0, 0)\} \}.$$

Dividiremos nossa demonstração em dois casos: $M = 0$ e $M > 0$.

Caso 1. Suponhamos $M = 0$. Inicialmente, mostraremos que, sendo $M = 0$, sempre existe uma forma quadrática $g(x, y)$, equivalente a $f(x, y)$, cujo módulo do coeficiente do termo x^2 é arbitrariamente pequeno. Seja $\varepsilon > 0$, devido a $M = 0$, existem inteiros p e q tais que $|f(p, q)| < \varepsilon$. Podemos supor, sem prejuízo, que $mdc(p, q) = 1$. De fato,

$$\left| f\left(\frac{p}{mdc(p, q)}, \frac{q}{mdc(p, q)} \right) \right| = \frac{\varepsilon}{(mdc(p, q))^2} < \varepsilon$$

e, como $mdc(p, q) = 1$, existem inteiros r, s, tais que

$$ps - qr = 1.$$

Portanto a forma equivalente

$$g(x, y) = f(px + qy, rx + sy) = f(p, r)x^2 + (2apq + bps + brq + 2crs)xy + f(q, s)y^2$$

$$= a'x^2 + b'xy + c'y^2 = a'(x + y\vartheta)(x + y\vartheta'),$$

é uma forma quadrática com a propriedade desejada. Agora, reescrevendo $g(x, y)$ como

$$g(x, y) = a'(x + y\vartheta)(x + y\vartheta'),$$

pela Observação 4.3 e pela Proposição 4.8, temos a igualdade dos módulos dos discriminantes de g e f, isto é,

$$a'^2 |\vartheta - \vartheta'| = a^2 |\theta - \theta'|.$$

Portanto, como a' é arbitrariamente pequeno, por comparação, $|\vartheta - \vartheta'|$ deve ser arbitrariamente grande. Suponhamos sem perda de generalidade que $\vartheta > \vartheta'$. Determine um inteiro n tal que

$$-0.618 \cdots < \vartheta' + n \leq 0.382 \ldots,$$

e escreva $\vartheta_1 = \vartheta + n$ e $\vartheta_1' = \vartheta' + n$. Agora considere a forma quadrática

$$g'(x,y) = a'(x+\vartheta_1 y)(x+\vartheta_1' y) = a'(x+y(\vartheta+n))(x+(\vartheta'+n))$$

$$= a'(x+ny+\vartheta y)(x+ny+\vartheta' y) = g(x+ny,y).$$

Pela construção, $g'(x,y)$ é uma forma equivalente a $g(x,y)$ e, portanto, equivalente a $f(x,y)$, e como $\vartheta_1 - \vartheta_1'$ é arbitrariamente grande, o mesmo ocorre com ϑ_1, assim a forma quadrática estará na forma reduzida tomando ε suficientemente pequeno.

Caso 2. Suponhamos $M > 0$. Como no caso anterior, podemos encontrar uma forma equivalente cujo módulo do coeficiente da variável x é tão próximo de M quanto queremos. Portanto, sem perda de generalidade, suponhamos que a forma $f(x,y) = a(x-\theta y)(x-\theta' y)$ dada tenha o coeficiente a satisfazendo

$$M \leq |a| < \frac{M}{1-\varepsilon},$$

onde ε é um número real arbitrariamente pequeno. Com isso e pela definição de M, temos

$$\frac{M}{1-\varepsilon}|(x+\theta y)(x+\theta' y)| > |a||(x+\theta y)(x+\theta' y)| > M,$$

para todo par de inteiros x, y não simultaneamente nulos. Particularmente, temos a desigualdade

$$|(x+\theta y)(x+\theta' y)| > 1-\varepsilon, \tag{5.3}$$

satisfeita para todos inteiros x e y, não simultaneamente nulos. Sem perda de generalidade suponhamos $\theta > \theta'$. Como no caso anterior, tome um inteiro n tal que

$$-0.618\cdots < \theta' + n \leq 0.382\ldots$$

Portanto, fazendo como no caso anterior, podemos encontrar uma forma

$$g(x,y) = a'(x+\vartheta y)(x+\vartheta' y)$$

equivalente a $f(x,y)$ no qual ϑ' satisfaz

$$-0.618\cdots < \vartheta' \leq 0.382\ldots, \tag{5.4}$$

assim, podemos também supor, sem prejuízo, θ' satisfazendo a condição 5.4.

Tomando os valores $x = 0$ e $y = 1$ na desigualdade 5.3, obtemos

$$|\theta\theta'| > 1-\varepsilon. \tag{5.5}$$

Portanto

$$\theta > \frac{1-\varepsilon}{|\theta'|} > 1.618\ldots(1-\varepsilon). \tag{5.6}$$

Agora mostraremos que pelo menos um dos três pares

$$\theta, \theta';\ 2-\theta', 2-\theta;\ 1-\frac{1}{\theta'}, 1-\frac{1}{\theta}. \tag{5.7}$$

satisfaz a condição de redução. Uma vez que a cada par podemos corresponder uma forma equivalente a forma dada, afirmação que demonstraremos no próximo lema, isso será suficiente para demonstrarmos o resultado. Se $\theta > 2$ então o primeiro par em 5.7

satisfaria a condição de redutibilidade. Então, podemos supor $\theta < 2$. Pela desigualdade 5.5, temos

$$|\theta'| > \frac{1-\varepsilon}{2}$$

e como ε é arbitrariamente pequeno, podemos tomar ε de tal forma que tenhamos

$$|\theta'| > 0.382\ldots,$$

portanto, como θ' satisfaz a condição 5.4, temos $-0.618\cdots < \theta' < -0.382\ldots$. Assim, $2-\theta' > 2$ e $1-\dfrac{1}{\theta'} > 2$. Por fim, observamos que

$$0 < 2-\theta \leq 0.382\ldots \text{ se } \theta \geq 1.618\ldots,$$

$$0 < 1-\frac{1}{\theta} \leq 0.382\ldots \text{ se } \theta \leq 1.618\ldots.$$

Com isso concluímos a demonstração. ■

Lema 5.4. *Seja $f(x,y) = a(x+\theta y)(x+\theta' y)$ uma forma quadrática, então a cada par em 5.7 podemos corresponder uma forma quadrática equivalente a f.*

Demonstração: Para θ e θ' o resultado é claro. Para $(2-\theta)$ e $(2-\theta')$ basta observar que

$$g(x,y) = a(x-y(2-\theta)(x-y(2-\theta')) = f(x-2y,-y).$$

Para o par $\left(1-\frac{1}{\theta}\right)$ e $\left(1-\frac{1}{\theta'}\right)$, temos

$$g(x,y) = a\theta\theta'\left(x-y\left(1-\frac{1}{\theta}\right)\right)\left(x-y\left(1-\frac{1}{\theta'}\right)\right) =$$

$$a\theta\theta'\left(x-y+y\frac{1}{\theta}\right)\left(x-y+y\frac{1}{\theta'}\right) = a(y+\theta(x-y))(y+\theta'(x-y)) = f(y,-x+y)$$

■

Lema 5.5. *Seja $f_0(x,y) = a_0(x+\theta_0 y)(x+\theta_0' y)$ uma forma quadrática reduzida, onde θ_0 e θ_0' são números irracionais. Então, existem inteiros*

$$\ldots, t_{-2}, t_{-1}, t_0, t_1, t_2, \ldots$$

todos maiores que ou iguais a 2, e sinais + ou −

$$\ldots, u_{-2}, u_{-1}, u_0, u_1, u_2, \ldots$$

tais que os números θ_n, θ_n', definidos para $n > 0$ e $n < 0$ pelas recorrências

$$\theta_n = t_n + \frac{u_{n+1}}{\theta_{n+1}},\ \theta_n' = t_n + \frac{u_{n+1}}{\theta_{n+1}'}, \tag{5.8}$$

com todos satisfazendo a condição de redução, isto é,

$$\theta_n > 2,\ \frac{1-\sqrt{5}}{2} \leq \theta_n' \leq \frac{3-\sqrt{5}}{2}.$$

Além disso, o sinal u_{n+1} é oposto ao sinal de θ_{n+1}'. Por fim, para todo n há uma forma reduzida

$$f_n(x,y) = a_n(x+\theta_n y)(x+\theta_n' y) \tag{5.9}$$

equivalente a $f_0(x,y)$, e a equivalência entre $f_n(x,y)$ e $f_{n+1}(x,y)$ é expressa por

$$f_n(x,y) = f_{n+1}(y, u_{n+1}(x+t_n y)). \tag{5.10}$$

Demonstração: Defina t_0 como o inteiro mais próximo de θ_0 e escreva

$$\theta_0 = t_0 + \frac{u_1}{\theta_1},$$

onde $u_1 = \pm 1$ e, pela construção $\theta_1 > 2$.

De maneira geral, após termos definido θ_n, podemos prosseguir para a definição dos elementos u_{n+1} e θ_{n+1}, que de forma análoga, satisfazem

$$\theta_n = t_n + \frac{u_{n+1}}{\theta_{n+1}},$$

onde t_n é o inteiro mais próximo de θ_n, $u_{n+1} = \pm 1$ e $\theta_{n+1} > 2$. Portanto, com essa abordagem, estabelecemos uma sequência de inteiros $t_0, t_1, t_2, \ldots$, de reais $\theta_0, \theta_1, \ldots$, todos maiores ou iguais a 2, bem como uma sequência de sinais $u_0, u_1, u_2, \ldots$. A partir disso, podemos definir a recorrência

$$\theta'_n = t_n + \frac{u_{n+1}}{\theta'_{n+1}}.$$

Agora, nosso objetivo será demonstrar a desigualdade

$$\frac{1-\sqrt{5}}{2} \leq \theta'_n \leq \frac{3-\sqrt{5}}{2}, \tag{5.11}$$

para todo $n \geq 0$. Começamos com a hipótese de que θ'_0 satisfaz a condição 5.11. Agora, vamos mostrar que se a condição é verdadeira para $n \geq 0$, então também é verdadeira para $n+1$. Para isso, iniciamos observando que

$$\theta'_{n+1} = -\frac{u_{n+1}}{t_n - \theta'_n}, \tag{5.12}$$

assim, se θ'_n satisfaz a condição 5.11,

$$t_n - \theta'_n \geq \begin{cases} 2 - 0.382\cdots = 1.618\ldots \text{ sempre ocorre;} \\ 3 - 0.382\cdots = 2.618\ldots \text{ se } u_{n+1} = -1, \text{ e, portanto, } t \geq 3. \end{cases} \tag{5.13}$$

Vamos analisar o que ocorre de acordo com o valor de u_{n+1}.

1. Se $u_{n+1} = -1$, pela relação 5.12 e pela desigualdade 5.13,

$$\theta'_{n+1} = -\frac{-1}{t_n - \theta_n} \leq \frac{1}{3 - 0.382\ldots} = 0.382\ldots.$$

   Observamos que, como $t_n - \theta'_n \geq 0$, de acordo com 5.12, $\theta'_{n+1} \geq 0$.

2. Se $u_{n+1} = 1$, novamente pela relação 5.12 e pela desigualdade 5.13,

$$\theta'_{n+1} = -\frac{1}{t_n - \theta_n} \geq -\frac{1}{2 - 0.382\ldots} = -0.682\ldots.$$

   e, por fim, como no caso anterior, utilizando $t_n - \theta'_n \geq 0$, e pela relação 5.12, temos $\theta'_{n+1} \leq 0$.

Portanto, em qualquer caso, θ'_{n+1} satisfaz a condição 5.11. Logo, pelo princípio da indução finita, a sequência θ_n satisfaz 5.11, para todo $n \geq 0$.

Agora, nosso objetivo será estender as sequências $t_n,\ u_n, \theta_n,\ \theta'_n$, até aqui definidas, a todos os índices n inteiros. Defina u_0 como o sinal oposto de θ'_0. É válido observar, novamente, que, pela relação 5.12 e pela desigualdade 5.13, θ' possui sinal contrário a u_{n+1}, para todo $n \geq 0$. Agora, defina o inteiro t_{-1} de forma que θ'_{-1} definido por

$$\theta'_{-1} = t_{-1} + \frac{u_0}{\theta_0},$$

satisfaça

$$\frac{1-\sqrt{5}}{2} < \theta'_{-1} \leq \frac{3-\sqrt{5}}{2}.$$

Então, t_{-1} satisfaz a desigualdade

$$t_{-1} > -0.618\cdots + \frac{1}{|\theta'_0|} \geq -0.618\cdots + 1.618\cdots = 1,$$

em particular, $t_{-1} \geq 2$. Além disso, quando $u_0 = -1$, pela definição, temos $\theta'_0 > 0$, e assim,

$$t_{-1} > -0.618\cdots + \frac{1}{|\theta'_0|} \geq -0.618\cdots + 2.618\cdots = 2,$$

donde segue que $t_{-1} \geq 3$.

De maneira geral, podemos definir recursivamente, θ'_{-m}, u_{-m+1} e t_{-m}, de forma que u_{-m+1} seja o sinal oposto de θ'_{-m+1}, t_{-m} um inteiro escolhido de forma que satisfaça

$$\theta'_{-m} = t_{-m} + \frac{u_{-m+1}}{\theta_{-m+1}},$$

onde θ'_{-m} é um número real satisfazendo

$$\frac{1-\sqrt{5}}{2} < \theta'_{-m} \leq \frac{3-\sqrt{5}}{2}.$$

A partir da definição, t_{-m} satisfaz a desigualdade

$$t_{-m} > -0.618\cdots + \frac{1}{|\theta'_{-m+1}|} \geq -0.618\cdots + 1.618\cdots = 1,$$

em particular, como t_{-m} é um inteiro, $t_{-m} \geq 2$. Além disso, quando $u_{-m+1} = -1$, pela definição, temos $\theta'_{-m+1} > 0$, e assim,

$$t_{-1} > -0.618\cdots + \frac{1}{|\theta'_0|} \geq -0.618\cdots + 2.618\cdots = 2,$$

donde segue que $t-1 \geq 3$. Agora, mostraremos que $\theta_{-m} \leq 2$. Pelo que vimos logo acima,

$$\theta_{-m-1} = t_{-m-1} + \frac{u_{-m}}{\theta'_{-m}} > \begin{cases} 2 \text{ se } u_{-m} = 1; \\ 3 - \frac{1}{2} \text{ se } u_{-m} = -1. \end{cases}$$

assim, sempre teremos, $\theta_{-m} > 2$. Dessa forma, provamos todas as afirmações a respeito dos números θ_n, θ'_n, u_n, t_n, para todo n inteiro.

Finalmente, em relação às formas quadráticas binárias $f_n(x, y)$ definidas em 5.10, começamos observando que

$$x + \theta_n y = x + \left(t_n + \frac{u_{n+1}}{\theta_{n+1}}\right) y = \frac{u_{n+1}}{\theta_{n+1}} \left(X + \theta_{n+1} Y\right),$$

onde,

$$X = y,\ Y = u_{n+1}(x + t_n y). \tag{5.14}$$

De maneira, completamente análoga, temos a relação

$$x + \theta'_n y = \frac{u_{n+1}}{\theta'_{n+1}} \left(X + \theta'_{n+1} Y\right).$$

Usando esses fatos, podemos escrever

$$(x + \theta_n y)(x + \theta'_n y) = \frac{1}{\theta_{n+1}\theta'_{n+1}} (X + \theta_{n+1} Y)(X + \theta'_{n+1} Y). \tag{5.15}$$

Com isso, agora temos os recursos necessários para desenvolver a relação entre as formas definidas em 5.10. Começando com $f_0(x, y) = a_0(x + \theta_0 y)(x + \theta'_0 y)$, a relação definida em 5.10 nos fornece formas equivalentes para todos os inteiros n, uma vez que as relações em 5.14 sempre pode ser vista como uma transformação linear de determinante ± 1. Além disso, pela relação 5.15, temos

$$f_n(x, y) = a_n(x + \theta_n y)(x + \theta'_n y) = \frac{a_n}{\theta_{n+1}\theta'_{n+1}} (X + \theta_{n+1} Y)(X + \theta'_{n+1} Y) = f_{n+1}(X, Y).$$

A partir da expressão acima, podemos estabelecer uma relação de recorrência para os termos a_n da seguinte maneira:

$$a_n = \theta_{n+1}\theta'_{n+1} a_{n+1}.$$

Por fim, observamos que a_n está bem definido uma vez que sempre ocorre $\theta_n, \theta'_n, a_n \neq 0$, pois θ_0 e θ'_0 são irracionais. Com isso, finalizamos a demonstração. ■

A seguir definiremos algumas novas sequências, que serão essenciais ao longo do capítulo. Iniciamos com a seguinte definição:

Definição 5.6. Defina, para todo inteiro n, ϕ_n por

$$\phi_n \coloneqq -\frac{u_n}{\theta'_n}. \tag{5.16}$$

Observação 5.7. Como definimos u_n e θ'_n de forma que seus sinais sejam opostos, é imediato que $\phi_n > 0$ e uma vez que θ'_n satisfaz a condição de redutibilidade, temos

$$\phi_n \geq \begin{cases} 1.618\ldots \text{ sempre,} \\ 2.618\ldots \text{ se } u_n = -1. \end{cases} \tag{5.17}$$

A segunda relação de recorrência definida em 5.8 nos permite encontrar a seguinte recorrência

$$\phi_n = t_{n-1} + \frac{u_{n-1}}{\phi_{n-1}}. \tag{5.18}$$

Definição 5.8. Para todo $n \in \mathbb{Z}$, defina

$$v_n \coloneqq \left\lfloor \frac{1}{2}\theta_n \right\rfloor . \tag{5.19}$$

Particularmente, v_n é um inteiro positivo satisfazendo

$$1 \leq v_n < \frac{1}{2}\theta_n.$$

A partir da definição anterior, podemos dar duas novas definições, que serão essenciais no decorrer do desenvolvimento da seção.

Definição 5.9. Para todo n inteiro, defina

$$\beta_n \coloneqq v_n + \frac{u_{n+1}}{\theta_{n+1}}v_{n+1} + \frac{u_{n+1}u_{n+2}}{\theta_{n+1}\theta_{n+2}}v_{n+2} + \ldots; \tag{5.20}$$

$$\beta'_n \coloneqq \frac{v_{n-1}}{\phi_n} - \frac{v_{v-2}}{\phi_n\phi_{n-1}} + \frac{v_{n-3}}{\phi_n\phi_{n-1}\phi_{n-2}} - \ldots. \tag{5.21}$$

Para que as definições 5.20 e 5.21 tenham sentido é necessário que as séries β_n e β'_n sejam convergentes, para todo inteiro n. Para mostrar a convergência de β_n, observe que

$$\frac{v_{n+v}}{\theta_{n+1}\ldots\theta_{n+v}} < \frac{\frac{1}{2}\theta_{n+v}}{\theta_{n+1}\ldots\theta_{n+v}} < \frac{1}{2^v},$$

logo, a série β_n é absolutamente convergente, portanto, convergente. Além do mais,

$$\beta_n \geq v_n - \frac{u_{n+1}}{\theta_{n+1}}v_{n+1} - \frac{u_{n+1}u_{n+2}}{\theta_{n+1}\theta_{n+2}}v_{n+2} - \cdots > v_n - \frac{1}{2} - \frac{1}{2^2} - \cdots > 0. \tag{5.22}$$

Diante disso, β_n é bem definido como um número real positivo, para todo n inteiro.

Já para a convergência de β'_n, note que

$$v_{m-1} < \frac{1}{2}\theta_{m-1} < \frac{1}{2}\left(t_{m-1} + \frac{1}{\theta_m}\right) < \frac{1}{2}\left(t_{m-1} + \frac{1}{2}\right) <$$

$$< \frac{1}{2}(t_{m-1} + 2 - 2(0.618\ldots)) \leq \frac{1}{2}(t_{m-1} + t_{m-1} - 2(0.618\ldots)) \leq t_{m-1} - 0.618\cdots \leq \phi_m.$$

Portanto,

$$v_{m-1} < \phi_m, \tag{5.23}$$

para todo m inteiro.

Particularmente, pelas definições 5.19 e 5.8 e pela recorrência 5.18,

$$\frac{v_{n-v-1}}{\phi_n\ldots\phi_{n-v}} < \frac{1}{\phi_n\ldots\phi_{n-v+1}} \leq \frac{v_{n-v}}{\phi_n\ldots\phi_{n-v+1}}$$

para qualquer inteiro n e qualquer natural v. Portanto os termos da série β'_n formam uma sequência decrescente. Além disso, β'_n é resultado de uma soma alternada desses termos, o que implica em sua convergência. Como $0 < \frac{v_{n+1}}{\phi_n} < 1$, então

$$0 < \beta'_n < 1, \tag{5.24}$$

para todo inteiro n.

Lema 5.10. *As definições 5.20 e 5.21 implicam nas relações de recorrência*

$$\beta_n = v_n + u_{n+1}\frac{\beta_{n+1}}{\theta_{n+1}}; \tag{5.25}$$

$$\beta'_n = \frac{v_{n-1} - \beta'_{n-1}}{\phi_n}. \tag{5.26}$$

Lema 5.11. *Para todo n,*

$$\beta_n \leq \frac{3}{4}\theta_n. \tag{5.27}$$

Demonstração: Primeiramente, vamos provar a desigualdade mais fraca

$$\beta_n \leq \theta_n, \tag{5.28}$$

para todo n inteiro. Com base nas definições 5.20 e 5.19, podemos escrever

$$\frac{\beta_n}{\theta_n} \leq \frac{v_n}{\theta_n} + \frac{v_{n+1}}{\theta_n\theta_{n+1}} + \frac{v_{n+2}}{\theta_n\theta_{n+1}\theta_{n+2}} + \cdots < \frac{1}{2}\left(1 + \frac{1}{2} + \frac{1}{2^2}\ldots\right) = 1.$$

Dessa forma, segue a desigualdade $\beta_n \leq \theta_n$.

Agora vamos a demonstração da desigualdade $\beta_n \leq \theta_n$. Se $\theta_n > 4$, pela recorrência 5.25 e pela desigualdade 5.28,

$$\frac{\beta_n}{\theta_n} \leq \frac{1}{\theta_n}\left(v_n + \frac{\beta_{n+1}}{\theta_{n+1}}\right) < \frac{1}{\theta_n}\left(\frac{1}{2}\theta_n + 1\right) < \frac{3}{4}.$$

Agora, consideremos $\theta_n < 4$. Quando $\theta_n < 4$ é imediato da definição, em 5.19, que $v_n = \left\lfloor \frac{1}{2}\theta_n \right\rfloor = 1$. Uma vez que

$$\theta_n = t_n + \frac{u_{n+1}}{\theta_{n+1}},$$

quando $u_{n+1} = 1$, temos

$$\theta_n \geq 2 + \frac{1}{\theta_n}.$$

Por outro lado, quando $u_{n+1} = -1$, temos

$$\theta_n \geq 3 - \frac{1}{\theta_{n+1}} \geq 2 + \frac{1}{\theta_{n+1}}.$$

Dessa forma, sempre temos a desigualdade

$$\theta_n \geq 2 + \frac{1}{\theta_{n+1}}.$$

Multiplicando a desigualdade acima por θ_{n+1}, obtemos

$$\theta_n\theta_{n+1} \geq 2\theta_{n+1} + 1.$$

Pela recorrência 5.25 e pela expressão acima, segue

$$\frac{\beta_n}{\theta_n} \leq \frac{1}{\theta_n}(1 + \frac{\beta_{n+1}}{\theta_{n+1}}) = \frac{\theta_{n+1} + \beta_{n+1}}{\theta_n\theta_{n+1}} \leq \frac{\theta_{n+1} + \beta_{n+1}}{2\theta_{n+1} + 1} \leq \frac{\theta_{n+1} + v_{n+1} + \frac{\beta_{n+2}}{\theta_{n+2}}}{2\theta_{n+1} + 1} <$$

$$< \frac{\theta_{n+1} + \frac{1}{2}\theta_n + \frac{\beta_{n+2}}{\theta_{n+2}}}{2\theta_{n+1}+1} = \frac{\frac{3}{2}\theta_{n+1} + \frac{\beta_{n+2}}{\theta_{n+2}}}{2\theta_{n+1}+1}.$$

Portanto,

$$\frac{\beta_n}{\theta_n} - \frac{3}{4} < \frac{\frac{3}{2}\theta_{n+1} + \frac{\beta_{n+2}}{\theta_{n+2}}}{2\theta_{n+1}+1} - \frac{3}{4} = \frac{1}{2\theta_{n+1}+1}\left(\frac{\beta_{n+2}}{\theta_{n+2}} - \frac{3}{4}\right).$$

Então, seguindo a última desigualdade, se $\beta_{n+2} \leq \frac{3}{4}\theta_{n+2}$, então $\beta_n \leq \frac{3}{4}\theta_n$ também ocorrerá. Caso contrário, podemos repetir o mesmo argumento r vezes, para $n+2, n+4, \ldots, n+2r$ e obter a seguinte desigualdade:

$$\frac{\beta_n}{\theta_n} - \frac{3}{4} < \left(\frac{1}{2\theta_{n+3}+1} \cdots \frac{1}{2\theta_{n+2r-1}+1}\right)\left(\frac{\beta_{n+2r}}{\theta_{n+2r}} - \frac{3}{4}\right).$$

Como θ_n é sempre maior que 2 e, como já provamos a desigualdade mais fraca, $\frac{\beta_n}{\theta_n} < 1$, segue que

$$\frac{\beta_n}{\theta_n} - \frac{3}{4} < \frac{1}{5^r}\left(1 - \frac{3}{4}\right) = \frac{1}{4(5^r)}.$$

Uma vez que r pode ser tomado arbitrariamente grande, podemos afirmar que

$$\frac{\beta_n}{\theta_n} - \frac{3}{4} \leq 0,$$

ou seja,

$$\beta_n \leq \frac{3}{4}\theta_n$$

■

Corolário 5.12. *Pela recorrência 5.25 e pela desigualdade 5.27, temos*

$$|\beta_n - v_n| = \frac{\beta_{n+1}}{\theta_{n+1}} \leq \frac{3}{4}. \tag{5.29}$$

Em particular

$$\beta_n \geq \frac{1}{4} \tag{5.30}$$

Lema 5.13. *Para todo n,*

$$\beta'_n \leq \frac{1}{2}. \tag{5.31}$$

Demonstração: Pela definição 5.19 e pela recorrência 5.8, temos

$$2v_{n-1} < 2 \cdot \frac{1}{2}\theta_{n-1} = \theta_{n-1} < t_{n-1} + \frac{1}{2}.$$

Como v_n e t_n são inteiros, para qualquer n inteiro, a partir da desigualdade acima, podemos concluir que $2v_{n-1} < t_{n-1}$. Agora, como

$$\phi_n = t_{n-1} + \frac{u_{n-1}}{\phi_{n-1}} \geq t_{n-1} - \frac{1}{\phi_{n-1}},$$

segue que

$$\phi_n \geq 2v_{n-1} - \frac{1}{\phi_{n-1}} > 0.$$

Pela recorrência 5.26,

$$\beta'_n = \frac{v_{n-1} - \beta'_{n-1}}{\phi_n},$$

e, usando a desigualdade anterior, obtemos

$$\beta'_n \leq \frac{v_{n-1} - \beta'_{n-1}}{2v_{n-1} - \frac{1}{\phi_{n-1}}} = \frac{\phi_{n-1}(v_{n-1} - \beta'_{n-1})}{2v_{n-1}\phi_{n-1} - 1} = \frac{\phi_{n-1}v_{n-1} - v_{n-2} + \beta'_{n-2}}{2v_{n-1}\phi_{n-1} - 1}.$$

Assim temos,

$$\beta'_n - \frac{1}{2} \leq \frac{\phi_{n-1}v_{n-1} - v_{n-2} + \beta'_{n-2}}{2v_{n-1}\phi_{n-1} - 1} - \frac{1}{2} = \frac{\beta'_{n-2} - v_{n-2} + \frac{1}{2}}{2v_{n-1}\phi_{n-1} - 1} \leq \frac{\beta'_{n-2} - \frac{1}{2}}{2v_{n-1}\phi_{n-1} - 1}.$$

Se $\beta'_{n-2} \leq \dfrac{1}{2}$, o resultado segue, uma vez que $2v_{n-1}\phi_{n-1} - 1 > 0$. Caso não, primeiro observamos que, pela desigualdade 5.17,

$$2v_{n-1}\phi_{n-1} - 1 \geq 2(1.618\ldots) - 1 = \sqrt{5},$$

e assim, cheguamos a desigualdade

$$\beta'_n - \frac{1}{2} \leq \frac{1}{\sqrt{5}}\left(\beta'_{n-2} - \frac{1}{2}\right).$$

Repetindo o mesmo argumento v vezes, para v arbitrariamente grande, obtemos a desigualdade

$$\beta'_n - \frac{1}{2} \leq \frac{1}{(\sqrt{5})^v}\left(\beta'_{n-2v} - \frac{1}{2}\right) < \frac{1}{2(\sqrt{5})^v},$$

que por sua vez, implica em

$$\beta'_n \leq \frac{1}{2}.$$

■

Lema 5.14. *Para todo n,*

$$\frac{\beta_n}{\theta_n - \theta'_n} > \frac{1}{4(4 - \frac{1}{3} - \theta'_n)}. \tag{5.32}$$

Demonstração: Vamos dividir a demonstração em dois casos: $u_{n+1} = 1$ ou $u_{n+1} = -1$. Se $u_{n+1} = 1$, pela recorrência 5.8 temos,

$$\theta_n = t_n + \frac{1}{\theta_{n+1}}$$

e, pela recorrência 5.25 e pela desigualdade 5.22, obtemos a relação

$$\beta_n = v_n + \frac{\beta_{n+1}}{\theta_{n+1}} > v_n.$$

Como, por 5.19,

$$v_n = \left\lfloor \frac{1}{2}\theta_n \right\rfloor,$$

então

$$v_n = \left\lfloor \frac{1}{2}(t_n + \frac{1}{\theta_{n+1}}) \right\rfloor,$$

o que implica em $v_n = \frac{1}{2}t_n$ ou $v_n = \frac{1}{2}(t_n - 1)$. Logo, em qualquer caso, teremos $t_n \leq 2v_n + 1$. Agora, substituindo t_n por $2v_n + 1$ em

$$\theta_n = t_n + \frac{1}{\theta_{n+1}}$$

obtemos a desigualdade

$$\theta_n \leq 2v_n + 1 + \frac{1}{\theta_{n+1}} < 2v_n + 1 + \frac{1}{2} = 2v_n + \frac{3}{2}.$$

Portanto, neste caso, utilizando a desigualdade $\beta_n > v_n$, temos

$$\frac{\beta_n}{\theta_n - \theta'_n} > \frac{v_n}{2v_n + \frac{3}{2} - \theta'_n} \geq \frac{1}{\frac{7}{2} - \theta'_n} > \frac{1}{4(4 - \frac{1}{3} - \theta'_n)}.$$

Agora, suponhamos $u_{n+1} = -1$. Novamente, pelas recorrências 5.8 e 5.25,

$$\theta_n = t_n - \frac{1}{\theta_{n+1}},\ \beta_n = v_n - \frac{\beta_{n+1}}{\theta_{n+1}}. \tag{5.33}$$

Logo,

$$v_n = \left\lfloor \frac{1}{2}\theta_n \right\rfloor = \left\lfloor \frac{1}{2}(t_n - \frac{1}{\theta_{n+1}}) \right\rfloor,$$

e assim

$$v_n \leq \frac{1}{2}(t_n - 1).$$

Portanto, substituindo v_n por $\frac{1}{2}(t_n - 1)$ na primeira igualdade em 5.33, segue a desigualdade

$$\theta_n = t_n - \frac{1}{\theta_{n+1}} \leq 2v_n + 2 - \frac{1}{\theta_{n+1}} \tag{5.34}$$

Pela segunda igualdade em 5.33, temos

$$\frac{\beta_{n+1}}{\theta_{n+1}} = \frac{v_{n+1} - \frac{\beta_{n+2}}{\theta_{n+2}}}{\theta_{n+1}} \leq \frac{v_{n+1} + \frac{\beta_{n+2}}{\theta_{n+2}}}{\theta_{n+1}},$$

e, pelo Lema 5.11, sabemos que $\frac{\beta_{n+2}}{\theta_{n+2}} \leq \frac{3}{4}$, logo

$$\frac{\beta_{n+1}}{\theta_{n+1}} \leq \frac{v_{n+1} + \frac{\beta_{n+2}}{\theta_{n+2}}}{\theta_{n+1}} = \frac{v_{n+1}}{\theta_{n+1}} - \frac{\beta_{n+2}}{\theta_{n+1}\theta_{n+2}} < \frac{1}{2} + \frac{3}{4\theta_{n+1}}. \tag{5.35}$$

Vamos analisar esse caso em dois subcasos: $\theta_{n+1} < 3$ ou $\theta_{n+1} > 3$. Primeiramente, suponhamos $\theta_{n+1} < 3$. Por 5.33 e por 5.34, segue a desigualdade

$$\frac{\beta_n}{\theta_n - \theta'_n} \geq \frac{v_n - \frac{\beta_{n+1}}{\theta_{n+1}}}{2v_n + 2 - \frac{1}{\theta_{n+1}} - \theta'_n}.$$

Pelo Lema 5.11 e pela suposição $\theta_{n+1} < 3$, segue a desigualdade

$$\frac{\beta_n}{\theta_n - \theta'_n} > \frac{v_n - \frac{3}{4}}{2v_n + 2 - \frac{1}{3} - \theta'_n}.$$

Uma maneira de majorarmos um valor inferior para o lado direito da desigualdade é observarmos que a função

$$g(x) = \frac{x - \frac{3}{4}}{2x + 2 - \frac{1}{3} - \theta'_n}$$

é crescente. Portanto, pondo $v_n = 1$, obtemos a desigualdade

$$\frac{\beta_n}{\theta_n - \theta'_n} > \frac{v_n - \frac{3}{4}}{2v_n + 2 - \frac{1}{3} - \theta'_n} \geq \frac{1}{4(4 - \frac{1}{3} - \theta'_n)}.$$

Agora, suponhamos $\theta_{n+1} > 3$. Iniciamos observando que pela recorrência, 5.25, pela igualdade 5.19 e pelo Lema 5.11, podemos obter a expressão

$$\frac{\beta_n}{\theta_n} \leq \frac{v_n + \frac{\beta_{n+1}}{\theta_{n+1}}}{\theta_n} \leq \frac{v_n}{\theta_n} + \frac{\beta_{n+1}}{\theta_n \theta_{n+1}} \leq \frac{1}{2} + \frac{3}{4\theta_n}, \tag{5.36}$$

para todo inteiro n. Claramente, quando $\theta_{n+1} > 3$, a desigualdade 5.36 é melhor que o Lema 5.11.

Agora, novamente, segue, por 5.33 e 5.34, a desigualdade

$$\frac{\beta_n}{\theta_n - \theta'_n} \geq \frac{v_n - \frac{\beta_{n+1}}{\theta_{n+1}}}{2v_n + 2 - \frac{1}{\theta_{n+1}} - \theta'_n}.$$

Além disso, aplicando a desigualdade 5.36, chegamos a desigualdade

$$\frac{\beta_n}{\theta_n - \theta'_n} > \frac{v_n - \frac{1}{2} - \frac{3}{4\theta_{n+1}}}{2v_n + 2 - \frac{1}{\theta_{n+1}} - \theta'_n}.$$

De maneira análoga ao que fizemos anteriormente, também observemos que o lado direito da desigualdade é crescente em função de v_n, então, substituindo v_n por 1, obtemos

$$\frac{\beta_n}{\theta_n - \theta'_n} > \frac{\frac{1}{2} - \frac{3}{4\theta_{n+1}}}{4 - \frac{1}{\theta_{n+1} - \theta'_n}}.$$

Agora, o lado direito da desigualdade acima é crescente em função de θ_{n+1}, substituindo θ_{n+1} por 3, obtemos a desigualdade 5.32. ■

Lema 5.15. *Para todo n,*

$$\frac{\beta_n \beta'_n}{\theta_n - \theta'_n} > \frac{1}{128}. \tag{5.37}$$

Demonstração: Por meio da desigualdade 5.32, da recorrência 5.26 e da igualdade 5.16, podemos chegar na expressão

$$\frac{\beta_n \beta'_n}{\theta_n - \theta'_n} > \frac{\beta'_n}{4(\frac{11}{3} - \theta'_n)} = \frac{v_{n-1} - \beta'_{n-1}}{4\phi_n(\frac{11}{3} - \theta'_n)} = \frac{v_{n-1} - \beta'_{n-1}}{4(\frac{11}{3}\phi_n + u_n)}.$$

A partir dessa expressão, com base no Lema 5.13, obtemos

$$\frac{\beta_n \beta'_n}{\theta_n - \theta'_n} > \frac{v_{n+1} - \frac{1}{2}}{4(\frac{11}{3}\phi_n + u_n)}. \tag{5.38}$$

Agora, por meio da recorrência 5.18, da desigualdade 5.17 e da igualdade 5.19, podemos estabelecer a desigualdade

$$\phi_n = t_{n-1} + \frac{u_{n-1}}{\phi_{n-1}} \leq \left\lfloor \theta_n + \frac{1}{\theta_{n+1}} \right\rfloor + \frac{u_{n-1}}{\phi_{n-1}} + \leq 2v_{n-1} + 2 + 0.618\ldots.$$

Substituindo a última desigualdade em 5.38, obtemos

$$\frac{\beta_n\beta'_n}{\theta_n - \theta'_n} > \frac{v_{n-1} - \frac{1}{2}}{4(\frac{22}{3}v_{n-1} + \frac{11}{3}(2.618\ldots) + u_n)}.$$

O valor da expressão à direita da desigualdade aumenta à medida que v_{n-1} aumenta. Caso seja $v_{n-1} \geq 2$, então

$$\frac{\beta_n\beta'_n}{\theta_n - \theta'_n} > \frac{\frac{3}{2}}{4(\frac{44}{3} + \frac{11}{3}(2.618\ldots) + 1)} > \frac{1}{70} > \frac{1}{128}.$$

Dessa forma, podemos assumir $v_{n-1} = 1$. Isso implica imediatamente que, pela igualdade 5.19, $\theta_{n-1} < 4$ e, por t_n ser o inteiro mais próximo de θ_n, $t_{n-1} \leq 4$. Além disso, nestas condições, se $u_n = 1$, por 5.8, temos $t_{n-1} \leq 3$. Portanto, podemos concluir

$$\phi_n \leq t_{n-1} + \frac{1}{\phi_{n-1}} \leq 3.618\ldots,$$

Assim, neste caso, por 5.38, temos

$$\frac{\beta_n\beta'_n}{\theta_n - \theta'_n} \geq \frac{v_{n-1} - \frac{1}{2}}{4(\frac{11}{3}\phi_n + u_n)} \geq \frac{\frac{1}{2}}{4(\frac{11}{3}(3.618\ldots) + 1)} > \frac{1}{115} > \frac{1}{128}.$$

Então, podemos supor $u_n = -1$. Neste caso, como

$$\phi_n \leq t_{n-1} + \frac{1}{\phi_{n-1}} \leq 4.618\ldots,$$

pela desigualdade 5.38, podemos concluir

$$\frac{\beta_n\beta'_n}{\theta_n - \theta'_n} \geq \frac{v_{n-1} - \frac{1}{2}}{4(\frac{11}{3}\phi_n + u_n)} > \frac{\frac{1}{2}}{4(\frac{11}{3}(4.618\ldots) - 1)} > \frac{1}{128}.$$

■

Neste ponto iniciaremos a demonstração do Teorema 5.1. Observamos inicialmente que pelo Lema 5.3 é suficiente provarmos o resultado para uma forma quadrática reduzida

$$f_0(x, y) = a_0(x - \theta_0 y)(x - \theta'_0 y).$$

Queremos mostrar a existência de números reais p_0, q_0 satisfazendo

$$|f_0(x + p_0, y + q_0)| > \frac{1}{128}\sqrt{\delta} \tag{5.39}$$

para todos inteiros x, y. Utilizando a notação já introduzida, defina p_0, q_0 como os números que satisfazem

$$p_0 + \theta_0 q_0 = \beta_0, \quad p_0 + \theta'_0 q_0 = \beta'_0. \tag{5.40}$$

Então, como $\delta = a_0^2(\theta_0 - \theta'_0)^2$, a inequação 5.39, que é o objetivo da nossa demonstração, é equivalente a

$$|(x + \theta_0 y + \beta_0)(x + \theta'_0 y + \beta'_0)| > \frac{1}{128}(\theta_0 - \theta'_0). \tag{5.41}$$

Para provarmos o teorema, suponhamos a existência de inteiros x_0, y_0 violando 5.41 e chegaremos a uma contradição. Os três lemas subsequentes nos levarão a essa contradição.

Lema 5.16. *Suponhamos que exista x_0, y_0 que viole 5.41. Então existe um inteiro (positivo, negativo ou zero) n e inteiros x, y tais que*

$$|x + \theta_n y + \beta_n| \leq \frac{1}{\sqrt{128}}\theta_n, \tag{5.42}$$

$$|x + \theta'_n y + \beta'_n| \leq \frac{1}{\sqrt{128}}(\theta_n - \theta'_n), \tag{5.43}$$

$$|(x + \theta_n y + \beta_n)(x + \theta'_n y + \beta'_n)| \leq \frac{1}{128}(\theta_n - \theta'_n). \tag{5.44}$$

Demonstração: Sejam

$$L_n(x, y) = x + \theta_n y + \beta_n, \quad L'_n(x, y) = x + \theta'_n y + \beta'_n.$$

Então, por 5.8 e 5.20,

$$L_n(x, y) = x + \left(t_n + \frac{u_{n+1}}{\theta_{n+1}}\right) y + v_n + u_{n+1}\frac{\beta_{n+1}}{\theta_{n+1}} = \frac{u_{n+1}}{\theta_{n+1}} L_{n+1}(y, u_{n+1}(x + t_n y + v_n)). \tag{5.45}$$

Analogamente,

$$L'_n(x, y) = \frac{u_{n+1}}{\theta'_{n+1}} L_{n+1}(y, u_{n+1}(x + t_n y + v_n)). \tag{5.46}$$

Observamos que

$$\frac{1}{\theta_{n+1}\theta'_{n+1}} = \pm\frac{\theta_n - \theta'_n}{\theta_{n+1} - \theta_{n+1}}.$$

Portanto, se definirmos inteiros x_n, y_n para todo $n > 0$ e para todo $n < 0$, por

$$x_{n+1} = y_n, \quad y_{n+1} = u_{n+1}(x_n + t_n y_n + v_n),$$

a suposição que x_0 e y_0 violam 5.41 implica em

$$|L_n(x_n, y_n)L'_n(x_n, y_n)| \leq \frac{1}{128}(\theta_n - \theta'_n), \tag{5.47}$$

para todo n.

Primeiramente, suponha que $L_(x_n, y_n) \neq 0$ para todo n. Por 5.45, temos, para todo n,

$$\left|\frac{L_{n+1}(x_{n+1}, y_{n+1})}{L_n(x_n, y_n)}\right| = \theta_{n+1} > 2.$$

Portanto, como $|L_n(x_n, y_n)|$ tende a 0 quando $n \to -\infty$ e tende a ∞ quando $n \to \infty$, haverá, exatamente, um inteiro n para o qual temos

$$|L_{n-1}(x_{n-1}, y_{n-1})| < \frac{1}{\sqrt{128}} \leq |L_n(x_n, y_n)|. \tag{5.48}$$

Então, novamente, por 5.45, temos

$$|L_n(x_n, y_n)| = \theta_n |L_{n-1}(x_{n-1}, y_{n-1})| < \frac{1}{\sqrt{128}}\theta_n.$$

Portanto, utilizando 5.47, chegamos a

$$|L'_n(x_n, y_n)| \leq \frac{1}{128}(\theta_n - \theta'_n).$$

Com isso provamos todas as afirmações feitas no enunciado do lema.

Agora, vamos ao caso $L(x_n, y_n) = 0$ para algum n e, portanto para todo n, uma vez que

$$L_n(x_n, y_n) = \frac{u_{n+1}}{\theta_{n+1}} L_{n+1}(x_{n+1}, y_{n+1}).$$

Como

$$L'_{n+1}(x_{n+1}, y_{n+1}) = |\theta'_{n+1} L'_n(x_n, y_n)|,$$

onde $|\theta_{n+1}| \leq 0.618\ldots$, claramente 5.43 e 5.44 será satisfeito para n suficiente grande, o que demonstra o lema. ■

Lema 5.17. *Se inteiros x e y satisfazem 5.42 e 5.43, então $y = 0$*

Demonstração: 5.42 e 5.43 implicam que

$$|(\theta_n - \theta'_n)y + \beta_n - \beta'_n| \leq \frac{1}{\sqrt{128}}(2\theta_n - \theta'_n). \tag{5.49}$$

Se $y \geq 1$, obtemos

$$\theta_n - \theta'_n + \beta_n - \beta'_n \leq \frac{1}{\sqrt{128}}(2\theta_n - \theta'_n).$$

Como $\beta_n \geq v_n - \frac{3}{4}$, pelo Corolário 5.12, e $\beta'_n \leq \frac{1}{2}$, pelo Lema 5.13, então

$$\theta_n - \theta'_n + v_n - \frac{5}{4} \leq \frac{1}{\sqrt{128}}(2\theta_n - \theta'_n),$$

portanto,

$$\left(1 - \frac{1}{\sqrt{32}}\right)\theta_n \leq \left(1 - \frac{1}{\sqrt{128}}\right)\theta'_n - v_n + \frac{5}{4} < 0.382\cdots - 1 + \frac{5}{4}.$$

Mas a desigualdade acima é impossível, uma vez que $\theta_n > 2$.

Se $y \leq -2$, 5.49 implica que

$$2(\theta_n - \theta'_n) - (\beta_n - \beta'_n) \leq \frac{1}{\sqrt{128}}(2\theta_n - \theta'_n).$$

Como, de acordo com o Lema 5.11, $\beta_n \leq \frac{3}{4}\theta_n$ e, por 5.24, $\beta'_n > 0$, então

$$\frac{5}{4}\theta_n - 2\theta'_n < \frac{1}{\sqrt{128}}(2\theta_n - \theta'_n),$$

e, consequentemente,

$$\left(\frac{5}{4} - \frac{1}{\sqrt{32}}\theta_n\right) < \left(2 - \frac{1}{\sqrt{128}}\right)\theta'_n < 2(0.382\ldots),$$

o que é impossível.

Finalmente, se $y = -1$, então, por 5.42 e 5.43,

$$|x - \theta_n + \beta_n| \leq \frac{1}{\sqrt{128}}\theta_n,$$

$$|x - \theta'_n + \beta'_n| \leq \frac{1}{\sqrt{128}}(\theta_n - \theta'_n).$$

Portanto, pelo Lema 5.11, obtemos

$$x \geq \left(1 - \frac{1}{\sqrt{128}}\right)\theta_n - \beta_n \geq \left(\frac{1}{4} - \frac{1}{\sqrt{128}}\right)\theta_n. \tag{5.50}$$

Por outro lado,

$$x \leq \frac{1}{\sqrt{128}}\theta_n + \left(1 - \frac{1}{\sqrt{128}}\right)\theta_n - \beta_n < \frac{1}{\sqrt{128}}\theta_n + 0.382\ldots\ . \tag{5.51}$$

Portanto, a partir das desigualdades 5.50 e 5.51, chegamos a desigualdade

$$\left(\frac{1}{4} - \frac{1}{\sqrt{32}}\right)\theta_n < 0.382\ldots.$$

Dessa forma, devemos ter $\theta_n < 6$. Substituindo $\theta_n < 6$ em 5.51, segue

$$x < \left(\frac{6}{\sqrt{128}} + 0.382\ldots\right) < 1,$$

mas isso contradiz 5.50 e o fato que x deve ser um inteiro positivo. Portanto, também não há solução quando $y = -1$. Com isso finalizamos o lema. ■

Lema 5.18. *As desigualdades 5.42, 5.43 e 5.44 não possuem solução quando $y = 0$.*

Demonstração: Substituindo $y = 0$ em 5.42 e 5.43 temos

$$|x + \beta_n| \leq \frac{1}{\sqrt{128}}\theta_n, \tag{5.52}$$

$$|x + \beta'_n| \leq \frac{1}{\sqrt{128}}(\theta_n - \theta'_n). \tag{5.53}$$

Portanto,

$$\beta_n - \beta'_n \leq \frac{1}{\sqrt{128}}(2\theta_n - \theta'_n),$$

e, por 5.29 e pelo Lema 5.13,

$$v_n - \frac{3}{4} - \frac{1}{2} \leq \frac{1}{\sqrt{128}}(2\theta_n - \theta'_n),$$

$$\left(\frac{1}{2}\theta_n - 1\right) - \frac{5}{4} \leq \frac{1}{\sqrt{128}}(2\theta_n - \theta'_n),$$

e daí, temos

$$\left(\frac{1}{2} - \frac{1}{\sqrt{32}}\right)\theta_n \leq \frac{9}{4} + \frac{1}{\sqrt{128}}(0.618\ldots),$$

e portanto segue

$$\theta_n < 7.3.$$

Da desigualdade 5.52, obtemos

$$x \leq -\beta_n + \frac{1}{\sqrt{128}}\theta_n \leq -v_n + \frac{3}{4} + \frac{7.3}{\sqrt{128}} < 1.$$

Com isso, x é um inteiro menor ou igual a 0. Por outro lado, a partir das desigualdades 5.53 e 5.24, chegamos a

$$x \geq -\beta'_n - \frac{1}{\sqrt{128}}(\theta_n - \theta'_n) > -\frac{1}{2} - \frac{1}{\sqrt{128}}(7.3 + 0.618\ldots) > -2.$$

Dessa forma, $x = 0$ ou -1. Se $x = 0$, a desigualdade 5.44 torna-se

$$\beta_n \beta'_n \leq \frac{1}{128}(\theta_n - \theta'_n),$$

contradizendo o Lema 5.15. Por fim, suponhamos $x = -1$. Como, pelas desigualdades 5.24 e 5.31, $0 < \beta'_n < \frac{1}{2}$, e substituindo x por -1 na desigualdade 5.53, obtemos

$$\frac{1}{2} \leq |-1 + \beta'_n| \leq \frac{1}{\sqrt{128}}(\theta_n - \theta'_n),$$

ou seja,

$$\frac{1}{2}\sqrt{128} \leq (\theta_n - \theta'_n).$$

Portanto,

$$\theta_n \geq \sqrt{32} - 0.618\cdots > 5$$

e $v_n = \left\lfloor \frac{1}{2}\theta_n \right\rfloor \geq 2$. Agora, observe que

$$|(x + \beta_n)(x + \beta'_n)| = (\beta_n - 1)(1 - \beta'_n).$$

Pela recorrência 5.25 e pelo Lema 5.11 obtemos

$$\beta_n - 1 \geq v_n - \frac{3}{4} - 1.$$

Por outro lado, pelo Lema 5.13,

$$1 - \beta'_n \geq \frac{1}{2}.$$

Logo, segue

$$|(x + \beta_n)(x + \beta'_n)| = (\beta_n - 1)(1 - \beta'_n) \geq \left(v_n - \frac{3}{4} - 1\right)\frac{1}{2} \geq \frac{1}{16}v_n.$$

Agora, pela igualdade 5.19 e $\theta_n > 5$,

$$\frac{1}{16}v_n > \frac{1}{16}\left(\frac{1}{2}\theta_n - 1\right) > \frac{1}{16}\left(\frac{3}{10}\theta_n\right).$$

Assim,

$$|(x + \beta_n)(x + \beta'_n)| > \frac{1}{16}\left(\frac{3}{10}\theta_n\right) > \frac{\theta_n - \theta'_n}{\sqrt{128}},$$

o que contradiz 5.44 e demonstra o resultado. ■

Com a demonstração do último lema finalizamos a demonstração do Teorema 5.1.

5.2 Aplicação à classificação dos anéis quadráticos norma euclidianos

Nesta seção, nosso objetivo será demonstrar a finitude dos anéis quadráticos reais norma euclidianos. Por hora, nos encarregaremos em demonstrar o seguinte teorema:

Teorema 5.19. *Seja*

$$f(x,y) = ax^2 + bxy + cy^2$$

uma forma quadrática binária com coeficientes inteiros, cujo discriminante $\delta > 0$ não é um quadrado perfeito. Então existem números racionais p e q satisfazendo

$$|f(x+p, y+q)| > \frac{1}{128}\sqrt{\delta},$$

para todos inteiros x, y.

Dividiremos a prova do Teorema 5.19 em dois lemas com o objetivo de mostrarmos que, mediante a hipótese do Teorema, podemos tomar p_0 e q_0 definidos em 5.40 como números racionais.

Lema 5.20. *Seja $f_0(x,y)$ é uma forma quadrática com coeficientes inteiros cujo discriminante não é um quadrado perfeito. Então existe um inteiro positivo N tal que, com a notação do Lema 5.5,*

$$\theta_{n+N} = \theta_n,\ \theta'_n = \theta'_{n+N},\ t_n = t_{n+N},\ u_n = u_{n+N}.$$

Demonstração: Escreva

$$f_n(x,y) = a_n x^2 + b_n xy + c_n y^2 = a_n(x - \theta_n y)(x - \theta'_n y).$$

pelo Lema 4.8, temos a igualdade

$$|a_n|(\theta_n - \theta'_n) = \sqrt{\delta},$$

onde δ é o discriminante comum de todas as formas equivalentes f_n. Além disso, pela condição de redução,

$$\theta_n - \theta'_n > 2 - 0.382\ldots,$$

de onde podemos concluir que a sequência a_n é limitada. Pela recorrência 5.10,

$$a_n = f_n(1,0) = f_{n+1}(0, \pm 1) = c_n,$$

assim, podemos concluir que a sequência c_{n+1} é também limitada. Pela identidade $b_n^2 - 4a_n c_n = \sqrt{\delta}$ e pela finitude das sequências a_n, c_n segue que a b_n é também uma sequência limitada. Assim, há apenas um número finito de formas

$$f_n(x,y) = a_n x^2 + b_n xy + c_n y^2.$$

Portanto, necessariamente, existem naturais r e N tais que

$$a_r = a_{r+N},\ b_r = b_{r+N},\ c_r = c_{r+N}.$$

Em particular segue a igualdade

$$f_r(x,y) = a_r(x - y\theta_r)(x - y\theta'_r) = f_{r+N}(x,y) = a_{r+N}(x - y\theta_{r+N})(x - y\theta'_{r+N}),$$

de onde seguem as igualdades

$$\theta_r = \theta_{r+N},\ \theta'_r = \theta'_{r+N}.$$

A partir da periodicidade de período N das sequências θ_n e θ'_n, o resultado segue para as demais sequências devido a forma como foram construídas no Lema 5.5. ■

Lema 5.21. *Com a hipótese do lema anterior, os números β_0, β'_0 definidos em 5.20 e 5.21 são expressos na forma*

$$\beta_0 = p_0 + \theta q_0,\ \beta'_0 = p_0 + \theta' q_0,$$

onde p_0 e q_0 são racionais.

Demonstração: Considere d como o maior fator livre de quadrados de δ. Inicialmente, observe que os números θ_0 e θ'_0 são as raízes do polinômio quadrático

$$f_0(x,1) = a_0x^2 + b_0x + c_0 = a_0(x - \theta_0)(x - \theta'_0).$$

Portanto, devido à resolução de equações quadráticas, podemos afirmar que θ_0 e θ'_0 são elementos conjugados no corpo quadrático $\mathbb{Q}(\sqrt{d})$. De maneira geral, pelas relações de recorrência definidas em 5.9, podemos afirmar que θ_n e θ'_n são raízes de

$$f_n(x,1) = a_nx^2 + b_nx + c_n = a_n(x - \theta_n)(x - \theta'_n),$$

para todo $n \in \mathbb{Z}$. Além disso, de acordo com o Lema 4.8, θ_n e θ'_n são também elementos conjugados de $\mathbb{Q}(\sqrt{d})$.

Com base nas definições de β_0 e β'_0, em 5.20 e 5.21, respectivamente, e de acordo com o lema anterior, podemos reescrever

$$\beta_0 = \left(v_0 + \frac{u_1}{\theta_1} + \frac{u_1u_2}{\theta_1\theta_2}v_2 + \cdots + \frac{u_1\ldots u_{N-1}}{\theta_1\ldots\theta_{N-1}}v_{N-1}\right)\left(1 + \frac{u_1\ldots u_N}{\theta_1\ldots\theta_N} + \left(\frac{u_1\ldots u_N}{\theta_1\ldots\theta_N}\right)^2 + \ldots\right) =$$

$$= \left(v_0 + \frac{u_1}{\theta_1} + \frac{u_1u_2}{\theta_1\theta_2}v_2 + \cdots + \frac{u_1\ldots u_{N-1}}{\theta_1\ldots\theta_{N-1}}v_{N-1}\right)\left(1 - \frac{u_1\ldots u_N}{\theta_1\ldots\theta_N}\right)^{-1};$$

$$\beta'_0 = \left(\frac{v_{-1}}{\phi_0} - \frac{v_{-2}}{\phi_0\phi_{-1}} + \frac{v_{-3}}{\phi_0\phi_{-1}\phi_{-2}} - \cdots + \frac{(-1)^{N-1}v_{-N}}{\phi_0\phi_{-1}\ldots\phi_{-N+1}}\right)\cdot$$

$$\cdot\left(1 + \frac{(-1)^N}{\phi_{-1}\ldots\phi_{-N}} + \left(\frac{(-1)^N}{\phi_{-1}\ldots\phi_{-N}}\right)^2 + \ldots\right) =$$

$$= \left(\frac{v_{-1}}{\phi_0} - \frac{v_{-2}}{\phi_0\phi_{-1}} + \frac{v_{-3}}{\phi_0\phi_{-1}\phi_{-2}} - \cdots + \frac{(-1)^{N-1}v_{-N}}{\phi_0\phi{-1}\ldots\phi_{-N+1}}\right)\left(1 - \frac{(-1)^N}{\phi_{-1}\ldots\phi_{-N+1}}\right)^{-1},$$

onde N é o período em comum das sequências, como demonstrado no lema anterior. A partir dessas expressões, podemos concluir que β_0 e β'_0 são elementos de $\mathbb{Q}(\sqrt{d})$, uma vez que θ_n e θ'_n pertencem a $\mathbb{Q}(\sqrt{d})$, como também os elementos u_n e v_n, pois são inteiros,

e, pela definição 5.6, também $\phi_n \in \mathbb{Q}(\sqrt{d})$. Além disso, podemos mostrar que esses elementos são conjugados. De fato, o conjugado de θ_n é $\theta'_n = -\frac{u_n}{\phi_n}$, o que implica que o conjugado de β_0 é

$$(v_0 - v_1\phi_1 + v_2\phi_1\phi_2 - \cdots + (-1)^{N-1}v_{N-1}\phi_1\phi_2 \ldots \phi_{N-1})(1 - (-1)^N\phi_1\phi_2 \ldots \phi_N)^{-1}.$$

Multiplicando a expressão acima por

$$\frac{(-1)^N\phi_1\phi_2 \ldots \phi_N}{(-1)^N\phi_1\phi_2 \ldots \phi_N},$$

obtemos

$$\left(\frac{v_0 - v_1\phi_1 + v_2\phi_1\phi_2 - \cdots + (-1)^{N-1}v_{N-1}\phi_1\phi_2 \ldots \phi_{N-1}}{(-1)^N\phi_1\phi_2 \ldots \phi_N}\right) \cdot \left(\frac{1 - (-1)^N\phi_1\phi_2 \ldots \phi_N}{(-1)^N\phi_1\phi_2 \ldots \phi_N}\right)^{-1} =$$

$$= \left(\frac{v_{-1}}{\phi_0} - \frac{v_{-2}}{\phi_0\phi_{-1}} + \frac{v_{-3}}{\phi_0\phi_{-1}\phi_{-2}} - \cdots + \frac{(-1)^{N-1}v_{-N}}{\phi_0\phi{-1} \ldots \phi_{-N+1}}\right)\left(1 - \frac{(-1)^N}{\phi_{-1} \ldots \phi_{-N+1}}\right)^{-1} = \beta'_0.$$

Observe que usamos o fato de v_0 ser igual a v_{-N}. Logo, o conjugado de β_0 é β'_0. Dessa forma, existem números racionais r, s, u, e v tais que

$$\theta_0 = r + s\sqrt{d},\ \theta'_0 = r - s\sqrt{d};\ \beta_0 = u + v\sqrt{d},\ \beta'_0 = u - v\sqrt{d}.$$

Dado que também temos

$$\beta_0 = p_0 + \theta q_0,\ \beta'_0 = p_0 + \theta' q_0,$$

seguem

$$u + v\sqrt{d} = p_0 + (r + s\sqrt{d})q_0,\ u - v\sqrt{d} = p_0 + (r - s\sqrt{d})q_0$$

donde concluímos que p_0 e q_0 são números racionais. ■

Com isso, finalizamos a demonstração do Teorema 5.19.

Podemos empregar o Teorema 5.19 a fim de obtermos resultados sobre as formas quadráticas definidas em 4.1 e assim encontrar condições relacionado a um anel quadrático não possuir o algoritmo euclidiano.

Teorema 5.22. *O algoritmo de Euclides não é válido em anéis quadráticos $\mathcal{O}_d$ cujo discriminante excede* $(128)^2$.

Demonstração: Consideremos a forma quadrática $N_d(x, y)$ definida em 4.1 e seja δ_d seu discriminante. Para que o anel quadrático $\mathcal{O}_d$ não seja norma euclidiano, é suficiente que, para quaisquer inteiros x e y, existam números racionais p e q tais que

$$|N_d(p + x, q + y)| > 1.$$

De acordo com o Teorema 5.19, para a forma quadrática N_d, existe um par de racionais p e q, tais que para todos os inteiros x e y, ocorre

$$|N_d(p + x, q + y)| > \frac{1}{128}\sqrt{\delta_d}.$$

Como

$$\frac{1}{128}\sqrt{\delta_d} = \begin{cases} \frac{1}{128}\sqrt{d}, \text{ se } d \equiv 1 \pmod 4; \\ \frac{1}{64}\sqrt{d}, \text{ se } d \equiv 2,3 \pmod 4 \end{cases} \tag{5.54}$$

então

$$|N_d(p+x, q+y)| > \frac{1}{128}\sqrt{\delta_d} > 1, \tag{5.55}$$

para $d > 128^2$. Portanto, não existem anéis quadráticos $\mathcal{O}_d$ que sejam norma euclidianos para valores d livre de quadrados e maiores que 128^2. ■

A partir das relações 5.54 e 5.55 podemos concluir que não há anéis quadráticos de discriminante d maior que 64^2 quando $d \equiv 2,3 \pmod 4$. Assim enunciamos

Teorema 5.23. *O algoritmo de Euclides não é válido em anéis quadráticos $\mathcal{O}_d$ cujo discriminante excede $(64)^2$ quando $d \equiv 2,3 \pmod 4$.*

Apesar de podermos encontrar uma cota significantemente melhor em anéis quadráticos de discriminante $d \equiv 2,3 \pmod 4$ utilizando o método desenvolvido neste capítulo, no próximo capítulo abordaremos um método elementar no qual poderemos melhorar de modo expressivo a cota superior de discriminante de anéis quadráticos $d \equiv 2,3 \pmod 4$, o que será essencial para a classificação de tais anéis.

6 Classificação de anéis quadráticos reais

Neste capítulo classificaremos os anéis quadráticos reais, o objetivo será demonstrar que os únicos anéis quadráticos reais norma euclidianos são os anéis citados no Teorema 4.21, isto é, os anéis quadráticos com discriminante $d = 2$, 3, 5, 6, 7, 13, 11, 17, 19, 21, 29, 33, 37, 41, 57 ou 73. Na seção 6.1, classificaremos os anéis quadráticos com discriminante congruente a 2 ou 3 módulo 4. Nas próximas duas seções classificaremos os anéis quadráticos com discriminante congruente a 1 módulo 4. A Seção 6.2 será dedicada a classificação dos anéis quadráticos com discriminante composto e a Seção 6.3 será dedicada a classificação dos anéis quadráticos com discriminante primo. Assim, ao final deste capítulo, teremos demonstrado:

Teorema 6.1. *Um anel quadrático real $\mathcal{O}_d$ é norma euclidiano se, e somente, $d = 2$, 3, 5, 6, 7, 13, 11, 17, 19, 21, 29, 33, 37, 41, 57 ou 73.*

6.1 Classificação de anéis quadráticos com discriminante $d \not\equiv 1 \pmod 4$

Nesta seção demonstraremos que os únicos anéis quadráticos reais $\mathcal{O}_d$ norma euclidianos, onde $d \equiv 2, 3 \pmod 4$, são os anéis quadráticos com discriminante $d = 2, 3, 6, 7, 11, 19$. Usaremos uma abordagem elementar para demonstrar que não há anéis quadráticos norma euclidianos $\mathcal{O}_d$ para $d \leq 74$ e $d \equiv 2, 3 \pmod 4$, e diante disso, haverá poucos casos a serem verificados o que nos permite a verificação caso a caso. Seguiremos a referência [11].

Proposição 6.2. *Seja $\mathcal{O}_d$ um anel quadrático com discriminante $d \equiv 2 \pmod 4$. Suponhamos que seja possível encontrar um inteiro ímpar t satisfazendo*

$$2d < t^2 < 3d, \tag{6.1}$$

então $\mathcal{O}_d$ não será norma euclidiano.

Demonstração: Suponhamos que o par $(0, \frac{t}{d})$, para algum inteiro t, satisfaça a inequação

$$\left|(x-0)^2 - d\left(y - \frac{t}{d}\right)^2\right| < 1, \tag{6.2}$$

onde x e y são inteiros. Multiplicando a desigualdade por d obtemos

$$|dx^2 - (dy - t)^2| < d.$$

Defina o inteiro $z = dy - t$, o substitua na igualdade acima e assim chegaremos em

$$|z^2 - dx^2| < d. \tag{6.3}$$

Como

$$z^2 - dx^2 = (dy - t)^2 - dx^2 \equiv t^2 \pmod d,$$

segue que existe um inteiro m satisfazendo

$$z^2 - dx^2 = t^2 + md. \tag{6.4}$$

Substituindo $z^2 - dx^2$ por $t^2 + md$ em 6.3, haverá apenas dois possíveis valores para m, de forma que 6.4 e 6.3 sejam satisfeitos simultaneamente. Suponhamos que t seja um inteiro satisfazendo

$$2d < t^2 < 3d.$$

Neste caso, teríamos

$$z - dx^2 = t^2 - md,$$

onde $m = 2$ ou 3. Reescrevendo a última igualdade chegamos em

$$z - t^2 = d(x^2 - m),$$

onde o lado direito da igualdade é congruente, possivelmente, a $2, 4, 6 \pmod 8$, no entanto, o lado esquerdo da igualdade é congruente a no máximo 0, 3, 7 $\pmod 8$, o que implica na impossibilidade da igualdade. Assim, a desigualdade 6.2 não possui solução com x e y inteiros, portanto, de acordo com a observação 2.61, o anel quadrático não será norma euclidiano. ■

Proposição 6.3. *Se $d \equiv 2 \pmod 4$, então $\mathcal{O}_d$ não é norma euclidiano para $d \geq 27$.*

Demonstração: Para mostrar que $\mathcal{O}_d$ não é um anel quadrático norma euclidiano, vamos utilizar a contra-positiva do resultado anterior para estabelecer um limite inferior para o conjunto dos inteiros livres de quadrados d tais que o anel quadrático $\mathcal{O}_d$ seja norma euclidiano. Em outras palavras, queremos encontrar um valor mínimo de d a partir do qual seja possível encontrar um inteiro ímpar t que satisfaça a desigualdade

$$2d < t^2 < 3d. \tag{6.5}$$

Dizer que não exista um inteiro ímpar t que não satisfaz a inequação 6.5 é equivalente a dizer que existe um inteiro u satisfazendo

$$(2u - 1)^2 < 2d < 3d \leq (2u + 1)^2 \tag{6.6}$$

e, portanto, satisfazendo

$$3(2u - 1)^2 < 6d < 2(2u + 1)^2. \tag{6.7}$$

Mas a desigualdade

$$3(2u - 1)^2 < 2(2u + 1)^2$$

ocorre apenas quando $u \leq 4$. Dessa forma, é impossível que haja um inteiro $u \geq 5$ satisfazendo a desigualdade 6.6 e assim haverá um inteiro ímpar t satisfazendo 6.5. Portanto, utilizando desses fatos, podemos estabelecer um limite superior para os valores de d nos quais existe um inteiro ímpar que satisfaça 6.5. De fato, como vimos, para que 6.6 ocorra, é necessário que $u \leq 4$, e, consequentemente, pela desigualdade 6.7, temos $3d < 9^2$, ou seja, $d < 27$. Portanto, para $d > 27$, sempre haverá um inteiro ímpar t que satisfaça a desigualdade 6.5. ■

Teorema 6.4. *Os anéis quadráticos com discriminante $d \equiv 2 \pmod 4$ não são norma euclidianos exceto quando $d = 2, 6$.*

Demonstração: Pela proposição anterior basta analisar os casos onde $d < 27$, isto é, 10, 14, 18, 22, 26. Para $d = 10$, tome $t = 5$, assim, $2 \cdot 10 < t^2 < 3 \cdot 10$. Os caso $d = 18$ e $d = 22$ são análogos, em ambos basta tomar $t = 7$. Para $d = 26$, tome $t = 39$. Observamos que $58d < t^2 < 59d$. Dessa forma, $z^2 - t^2 = d(x^2 - m)$, com $m = 58$ ou 59. Os possíveis resíduos de $z^2 - t^2$ módulos 8 são $0, 3$ ou 7. Entretanto, os possíveis resíduos de $d(x^2 - m)$ módulo 8 são $2, 4$ ou 6. Assim, não existe solução para a equação $z^2 - t^2 = d(x^2 - m)$ em x e z. Para $d = 14$, mostraremos que $(\frac{1}{2}, \frac{1}{2})$ não satisfaz nenhuma inequação da forma

$$\left| \left(x - \frac{1}{2}\right)^2 - 14\left(y - \frac{1}{2}\right)^2 \right| < 1,$$

onde x e y são inteiros. Podemos reescrever a inequação como

$$\left|(2x - 1)^2 - 14\,(2y - 1)^2\right| < 4.$$

No entanto, observe que $(2x - 1)^2 - 14(2y - 1)^2 \equiv 3 \pmod 8$. Portanto, necessariamente temos $(2x - 1)^2 - 14(2y - 1)^2 = 3$. No entanto, essa última equação não possui solução, pois implicaria que

$$3 = (2x - 1)^2 - 14(2y - 1)^2 \equiv (2x - 1)^2 \pmod 7.$$

Mas 3 não é um resíduo quadrático módulo 7, o que significa que não há nenhum inteiro x que satisfaça essa equação. ■

Proposição 6.5. *Seja $\mathcal{O}_d$ um anel quadrático com discriminante $d \equiv 3 \pmod 4$. Suponhamos que seja possível encontrar um inteiro ímpar t satisfazendo*

$$5d < t^2 < 6d,$$

então $\mathcal{O}_d$ não será norma euclidiano.

Demonstração: Seja t é um inteiro ímpar tal que $5d < t^2 < 6d$. Para que o par $(0, \frac{t}{d})$ satisfaça a inequação

$$\left| (x - 0)^2 - d\left(y - \frac{t}{d}\right)^2 \right| < 1,$$

com x, y inteiros, usando um argumento análogo ao utilizado na demonstração da Proposição 6.2, é necessário que a equação

$$z - dx^2 = t^2 - md \iff z^2 - t^2 = d(x^2 - m),$$

onde $m = 5$ ou 6, tenha solução nas variáveis inteiras z, x e t. Agora, analisando as congruências modularmente, temos:

1. $d(x^2 - m^2) \equiv 1, 2, 4, 5,$ ou $6 \pmod 8$;
2. $z^2 - t^2 \equiv 0, 3,$ ou $7 \pmod 8$.

Portanto, a equação $z^2 - t^2 = d(x^2 - m)$ não possui solução e dessa forma, concluímos que $\mathcal{O}_d$ não é um anel quadrático norma euclidiano quando t satisfaz a desigualdade $5d < t^2 < 6d$.

■

Proposição 6.6. *Se $d \equiv 3 \pmod 4$, então o anel quadrático $\mathcal{O}_d$ não é norma euclidiano para $d \geq 74$.*

Demonstração: Caso não exista t ímpar tal que $5d < t^2 < 6d$, deve existir u inteiro tal que $(2u-1)^2 \leq 5d < 6d < (2u+1)^2$, o que implica na desigualdade $5(2u+1)^2 < 6(2u-1)^2$. No entanto, isso ocorre somente quando $u < 11$. Neste caso temos $21^6 < 6d$, isto é, $74 < d$. Assim, concluímos que para $d > 74$, sempre existe um inteiro ímpar t que satisfaça a desigualdade $5d < t^2 < 6d$. Portanto, o anel quadrático $\mathcal{O}_d$ não é norma euclidiano para valores $d > 74$. ■

Teorema 6.7. *Os anéis quadráticos com discriminante $d \equiv 3 \pmod 4$ não são norma euclidianos exceto quando $d = 3, 7, 11, 19$.*

Demonstração: De acordo com a proposição anterior, resta-nos analisar os casos $d \leq 74$, ou seja,

$$d = 15,\ 23,\ 27,\ 31,\ 35,\ 39,\ 43,\ 47,\ 51,\ 55,\ 59,\ 63,\ 67,\ 71.$$

Para os seguintes valores

$$d = 15,\ 23,\ 31,\ 39,\ 43,\ 51,\ 55,\ 63,\ 67,\ 71$$

podemos encontrar um inteiro ímpar t satisfazendo

$$5d < t^2 < 6d.$$

Quando $d = 47$, tome $t = 25$. Então $13d < t^2 < 14d$, assim, temos $z^2 - t^2 = d(x^2 - m)$, com $m = 13$ ou 14. Como $m \equiv 5$ ou $6 \mod 8$. Os possíveis resíduos de $z^2 - t^2 \mod 8$ são $0, 3$ ou 7. No entanto, os possíveis resíduos $d(x^2 - m) \mod 8$ são $0, 1, 4, 5$ ou 6. Portanto, $z^2 - t^2 = d(x^2 - m)$ não possui solução para x e z.

Quando $d = 59$ tome $t = 47$. Logo, $37d < t^2 < 38d$ e $z^2 - t^2 = d(x^2 - m)$, com $m = 37$ ou 38. Por um lado, 0, 3 ou 7 são os possíveis resíduos de $z^2 - t^2 \mod 8$. Por outro lado, $d(x^2 - m)$ é possivelmente congruente a 1, 2, 4, 5 ou 6. Assim podemos afirmar que para $(0, \frac{47}{59})$ não existem x, y inteiros tais que

$$\left|(x-0)^2 - d\left(y - \frac{47}{59}\right)^2\right| < 1,$$

Por fim, chegamos ao último caso, considere $d = 35$. Vamos mostrar que $(\frac{1}{2}, \frac{1}{2})$ não satisfaz a inequação

$$\left|\left(x - \frac{1}{2}\right)^2 - 35\left(y - \frac{1}{2}\right)^2\right| < 1, \tag{6.8}$$

para inteiros x e y. Multiplicando 6.8 por 4, obtemos a inequação equivalente

$$|(2x-1)^2 - 35(2y-1)^2| < 4.$$

Como

$$(2x-1)^2 - 35(2y-1)^2 \equiv 2 \pmod 4,$$

segue que

$$(2x-1)^2 - 35(2y-1)^2 = \pm 2.$$

Mas isso é um absurdo, uma vez que

$$(2x-1)^2 - 35(2y-1)^2 \equiv 1 \text{ ou } 4 \ (mod\ 5)$$

e

$$\pm 2 \equiv 2 \text{ ou } 3 \pmod 5.$$

Assim, está demonstrado o resultado. ■

A partir disso podemos enunciar:

Teorema 6.8. *O anel quadrático real* $\mathcal{O}_d$ *com com discriminante* $d \equiv 2, 3 \pmod 4$ *é norma euclidiano apenas para os valores* $d = 2,\ 3,\ 6,\ 7,\ 11,\ 19$.

Portanto, finalizamos a lista de anéis quadráticos cujo discriminante é congruente a 2 ou 3 módulo 4. Nas próximas seções lidaremos com a classificação dos anéis quadráticos reais com discriminante congruente a 1 módulo 4, no entanto, essa será uma tarefa mais complicada.

6.2 Classificação de anéis quadráticos com discriminante composto $d \equiv 1 \pmod 4$

Nesta seção faremos a classificação de anéis quadráticos com discriminante composto congruente a 1 módulo 4. Na Subseção 6.2.1 demonstraremos que o discriminante de um anel quadrático é da forma p ou pq, onde p e q são primos, além disso, no caso composto, deve ocorrer $p \equiv q \equiv 3 \pmod 4$. Na Subseção 6.2.2 demonstraremos que p ou q deve ser necessariamente igual a 3. Por fim, na Subseção 6.2.3 faremos a classificação dos anéis quadráticos com discriminante da forma $3q$, culminando assim na classificação dos anéis quadráticos com discriminante composto. Dessa forma, ao final da seção teremos demonstrado

Teorema 6.9. *Um anel quadrático real com discriminante d composto e congruente módulo 1 módulo 4 é norma euclidiano apenas quando* $d = 21, 33$ *ou* 57.

6.2.1 Discriminante de anéis quadráticos são da forma p ou pq

Se o anel quadrático $\mathcal{O}_d$ for um domínio euclidiano, ele será automaticamente um domínio de ideais principais. Sob essa premissa, serão estabelecidas condições necessárias na decomposição de d para que o anel $\mathcal{O}_d$, com $d \equiv 1 \pmod 4$, também seja um domínio de ideais principais. Embora não abordemos aqui, há resultados análogos para os casos em que $d \equiv 2, 3 \pmod 4$. Mais informações podem ser encontradas na referência [10].

A importância desse resultado é imediata, pois não só possibilita resolver uma ampla variedade de casos, mas também fornece diretrizes valiosas na abordagem do problema. Em resumo, essa condição desempenha um papel fundamental na organização de como abordaremos a classificação dos corpos quadráticos norma euclidiano.

Lema 6.10. *Se o primo p divide o inteiro positivo livre de quadrados d, então existe uma unidade positiva* η_p *em* $\mathcal{O}_d$ *tal que* $\sqrt{p\eta_p} \in \mathbb{Q}(\sqrt{d})$.

Demonstração: Seja $\alpha = mdc(p, \sqrt{d})$ em $\mathcal{O}_d$, observe que tal α existe por $\mathcal{O}_d$ ser domínio de ideais principais. Então, $\alpha^2 = mdc(p^2, d)$. Observemos que p divide α^2, uma vez que que p^2 e d são divisíveis por p. Além disso, pela definição de α, temos que $N(\alpha)$ divide

$N(p) = p^2$ e $N(\sqrt{d}) = d$. Logo deve ocorrer $N(\alpha) = \pm p$ e assim $N(\alpha^2) = p^2 = N(p)$. Desta forma, $N\left(\frac{\alpha^2}{p}\right) = 1$, donde segue a existência de uma unidade η_p em $\mathbb{Q}(\sqrt{d})$ tal que

$$\alpha^2 = p\eta_p.$$

Como $\alpha \in \mathbb{Q}(\sqrt{d})$, em particular,

$$\sqrt{p\eta_p} \in \mathbb{Q}(\sqrt{d}).$$

Observamos, por fim, que a unidade η deve ser de fato positiva, já que $\mathbb{Q}(\sqrt{d})$ e $\mathbb{C} \setminus \mathbb{R}$ não possuem elementos em comum. ■

Teorema 6.11. *Se o conjunto dos inteiros algébricos de* $\mathbb{Q}(\sqrt{d})$*, com* $d \equiv 1 \pmod 4$*, é um domínio de ideais principais, então apenas os seguintes casos são possíveis:*

1. $d = p$*, onde* p *é um primo tal que* $p \equiv 1 \pmod 4$*;*
2. $d = pq$*, onde* p *e* q *são primos tais que* $p \equiv q \equiv 3 \pmod 4$*.*

Demonstração: Seja ϵ a unidade fundamental de $\mathcal{O}_d$. Logo, para qualquer unidade $\eta \in \mathcal{O}_d$ existe um inteiro n tal que $\eta = \pm\epsilon^n$. Portanto, podemos supor, sem perda de generalidade, que no lema anterior η_p pode ser tomado como $\eta_p = 1$, se n é par, ou $\eta_p = \epsilon$ ou $\eta_p = \frac{1}{\epsilon}$, se n é impar.

Caso tenhamos $\eta_p = 1$, então $\sqrt{p} \in \mathbb{Q}(\sqrt{d})$ que por sua vez implica na igualdade $p = d$.

Caso aconteça $\eta_p = \epsilon$ ou $\eta_p = \frac{1}{\epsilon}$, onde necessariamente ocorrerá $p \neq d$. Por p ser diferente de d, existe um primo q, com $q \neq p$, tal que $q \mid d$. Agora, pelo lema anterior aplicado a q, ocorre a existência de uma unidade $\eta_q = \epsilon$ ou $\frac{1}{\epsilon}$ tal que $\sqrt{q\eta_q} \in \mathbb{Q}(\sqrt{d})$. Daí,

$$\sqrt{p\eta_p}\sqrt{q\eta_q} = \sqrt{pq\eta_p\eta_q} \in \mathbb{Q}(\sqrt{d}).$$

Uma vez que $\eta_p\eta_q$ é sempre um quadrado perfeito em $\mathcal{O}_d$, então

$$\sqrt{pq} \in \mathbb{Q}(\sqrt{d}).$$

Como consequência, temos $d = pq$. A partir daqui mostraremos que $p \equiv q \equiv 1 \pmod 4$ não pode ocorre. Iniciamos mostrando que existem $a, b \in \mathbb{Z}$ tais que $pq = a^2 + b^2$. Pelo Lema 2.65 como $p \equiv q \equiv 1 \pmod 4$ existem $r, s, p, q \in \mathbb{Z}$ tais que

$$pq = (r^2+s^2)(p^2+q^2) = N(r+is)N(p+iq) = N((rp-sq)+i(rq+sp)) = (rp-sq)^2+(rq+sp)^2,$$

assim, como $(rp - sq), (rq + sp) \in \mathbb{Z}$, segue a afirmação. Seja $a, b \in \mathbb{Z}$ tais que

$$pq = a^2 + b^2.$$

Uma vez que pq é um inteiro ímpar então a ou b é também um inteiro ímpar. Suponhamos que a seja ímpar.

Defina $e = b + \sqrt{pq}$ e $w = mdc(a, e)$. Seja $\alpha = mdc(e, 2)$, então

$$N(\alpha) \mid N(e) = ee' = -a^2 \text{ e } N(\alpha) \mid N(2) = 4,$$

como a é ímpar, $N(\alpha) = \pm 1$ e daí α é uma unidade em $\mathbb{Q}(\sqrt{d})$. Defina $\beta = mdc(e, e')$, então

$$\beta = mdc(e, e') = mdc(e, e' + e) = mdc(e, 2b),$$

como mostramos que $mdc(2, e)$ é uma unidade segue que

$$\beta = mdc(e, b) = mdc(b + \sqrt{pq}, b) = mdc(\sqrt{pq}, b).$$

Portanto,

$$N(\beta) \mid N(b) = b^2 \text{ e } N(\beta) \mid pq,$$

e como $a^2 + b^2 = pq$, segue que p e q não dividem b e assim $N(\beta) = \pm 1$, em particular, β é uma unidade em $\mathbb{Q}(\sqrt{d})$. Agora, seja $w = mdc(a, e)$, então

$$w^2 = mdc(a^2, e^2) = mdc(-ee', e^2),$$

como $\beta = mdc(e, e')$ é associado a 1, segue que

$$w^2 = e \cdot mdc(-e', e),$$

dessa forma w^2 é associado a e, logo $\dfrac{w^2}{e}$ é uma unidade em $\mathbb{Q}(\sqrt{d})$. Como

$$N\left(\frac{w^2}{e}\right) = \frac{N(w)}{N(e)} = \frac{N(w)^2}{-a^2},$$

segue que $\dfrac{w^2}{e}$ é uma unidade de norma negativa. Assim, para finalizarmos a basta demonstrar que é impossível uma unidade de norma negativa em $\mathcal{O}_d$. Como $\sqrt{p\eta_p} \in \mathbb{Q}(\sqrt{pq})$, então existe $\theta \in \mathbb{Q}(\sqrt{pq})$ tal que $\eta_p = \dfrac{(\theta)^2}{p}$, que por sua vez implica em $\eta_p' = \dfrac{(\theta')^2}{p}$. Como η_p e η_p' são números positivos, o mesmo ocorre com o valor da norma $N(\eta_p) = \eta_p \eta_p' > 0$. Como observamos no inicio da demonstração, η_p pode ser tomado como ϵ ou $\frac{1}{\epsilon}$. Em qualquer umas das situações o valor positivo de $N(\eta_p)$ implica no valor positivo de $N(\epsilon)$. Uma vez que toda unidade em $\mathcal{O}_d$ é da forma $\pm\epsilon^n$, n inteiro, então é impossível a existência de uma unidade de norma negativa. ■

Corolário 6.12. *Se o conjunto dos inteiros algébricos de* $\mathbb{Q}(\sqrt{d})$*, com* $d \equiv 1 \pmod 4$*, é um domínio euclidiano, então apenas os seguintes casos são possíveis:*

1. $d = p$*, onde* p *é um primo tal que* $p \equiv 1 \pmod 4$*;*
2. $d = pq$*, onde* p *e* q *são primos tais que* $p \equiv q \equiv 3 \pmod 4$*.*

6.2.2 Classificação de anéis quadráticos com discriminante $\neq 3q$

Nesta subseção faremos a classificação dos anéis quadráticos com discriminante pq, onde p e q são primos satisfazendo $3 < p < q$. Mais precisamente, demonstraremos que nenhum desses anéis é norma euclidiano. De acordo com o Corolário 6.12 podemos considerar apenas os casos $p \equiv q \equiv 3 \pmod 4$, portanto, objetivo principal desta seção será demonstrar o seguinte teorema:

Teorema 6.13. *Não há anéis quadráticos norma euclidianos* $\mathcal{O}_{pq}$*, onde* p *e* q *são primos satisfazendo* $7 \leq p < q$ *e* $p \equiv q \equiv 3 \pmod 4$*.*

Para a demonstração do teorema desenvolveremos diversos lemas que nos permitirão desenvolver uma ligação entre anéis quadráticos norma euclidianos, como na hipótese do teorema, com a teoria relacionada ao símbolo de Legendre.

Vamos supor que $\mathcal{O}_{pq}$ seja um anel quadrático norma euclidiano, onde p e q são primos satisfazendo $7 \leq p < q$ e desenvolveremos resultados a fim de obter uma contradição. Durante toda seção denotaremos $\epsilon = \frac{q}{p} > 1$.

Lema 6.14. *Se o anel quadrático $\mathcal{O}_m$, com $m \equiv 1 \pmod 4$, é norma euclideano, então qualquer inteiro r, com $0 < r < m$ e r resíduo quadrático módulo m, satisfaz pelo menos uma das seguintes equações*

$$mx^2 - y_1^2 = -4r \quad ou \quad mx^2 - y_1^2 = 4(m-r). \tag{6.9}$$

Demonstração: No item 2 da Observação 2.61 tome $a = 0$ e $b = \frac{z}{m}$, e assim temos

$$|mx^2 - (my - 2z)^2| < 4m.$$

Como $mx^2 - (my - 2z)^2 \equiv -z^2 \equiv -r \pmod m$, então uma das equações é satisfeita

$$mx^2 - y_1^2 = -4r \quad \text{ou} \quad mx^2 - y_1^2 = 4(m-r).$$

Isso demonstra o resultado. ■

Definição 6.15. Sejam a e b dois números inteiros. Seja $b = b_1 b_2 \dots b_n$ a representação de b como produto de potências de primos. Caso tenhamos

$$\left(\frac{a}{b_1}\right) = \left(\frac{a}{b_2}\right) = \cdots = \left(\frac{a}{b_n}\right) = 1$$

denotaremos, brevemente, por

$$\left(\frac{a}{b}\right)^* = 1,$$

onde $\left(\frac{*}{*}\right)$ denota o símbolo de Kronecker.

Vamos, agora, provar

Lema 6.16. *Se $\mathcal{O}_m$, com $m \equiv 1 \pmod 4$, é um anel quadrático norma euclidiano, então:*

1. *Para todo número inteiro r com*

$$\left(\frac{r}{m}\right)^* = 1,$$

onde $0 < r < m$ e $(r, m) = 1$, sempre ocorre

$$\left(\frac{m}{r}\right)^* = 1$$

ou

$$\left(\frac{m}{r-m}\right)^* = 1.$$

2. *Caso* m *seja um inteiro composto, onde podemos assumir* $m = pq$ *com* $p \equiv q \equiv 3 \pmod 4$*, para cada número inteiro* r *com*

$$\left(\frac{r}{q}\right) = \left(\frac{p}{q}\right),$$

onde $0 < r < q$*,* $(r, p) = (r - q, p) = 1$*, temos*

$$\left(\frac{m}{r}\right)^* = 1 \quad e \quad \left(\frac{r}{p}\right) = \left(\frac{p}{q}\right),$$

ou

$$\left(\frac{m}{r-q}\right)^* = 1 \quad e \quad \left(\frac{r-q}{p}\right) = \left(\frac{p}{q}\right).$$

Demonstração: Utilizaremos o lema anterior. Para cada inteiro não nulo r, definimos o inteiro ímpar r_0 como $r = 2^e r_0$, onde e é um número inteiro. Se r satisfaz as condições da hipótese do item 1, então, de acordo com o lema anterior, temos

$$\left(\frac{m}{r_0}\right)^* = 1 \text{ ou } \left(\frac{m}{(r-m)_0}\right)^* = 1,$$

em conformidade com qual equação, em 6.9, é satisfeita por r. No primeiro caso, temos $\left(\frac{m}{r_0}\right) = 1$, e devido a $\left(\frac{r}{m}\right)^* = 1$, também temos

$$\left(\frac{m}{r}\right) = \left(\frac{m}{2^e r_0}\right) = \left(\frac{m}{2^e}\right)\left(\frac{m}{r_0}\right) = \left(\frac{2^e}{m}\right)\left(\frac{r_0}{m}\right) = \left(\frac{r}{m}\right) = 1,$$

onde $\left(\frac{r}{m}\right) = 1$ é em decorrência de 6.9, o que implica em $\left(\frac{m}{2^e}\right) = 1$. O caso $r - m = 2^e(r-m)_0$ é análogo. Assim, provamos a primeira parte do teorema.

Se as condições da parte 2 são atendidas para r, logo as equações $x^2 \equiv rp \pmod q$ e $x^2 \equiv rp \pmod q$ possuem soluções, o que é equivalente a dizer que $x^2 \equiv rp \pmod m$ possui solução, portanto pr é um resíduo quadrático módulo m e $0 < pr < m$. Então, podemos aplicar o Lema 6.14 a pr em vez de r. Neste caso, y_1 em 6.9 deve ser divisível por p, e assim, podemos reescrevê-la como

$$qx^2 - py_2^2 = -4r \quad \text{ou} \quad = 4(q-r),$$

onde $x \equiv y_2 \pmod 2$. Isso implica novamente que

$$\left(\frac{pq}{r_0}\right)^* = 1 \quad \text{ou} \quad \left(\frac{pq}{(r-q)_0}\right)^* = 1$$

Agora, podemos concluir de maneira semelhante à primeira parte do teorema, já que

$$\left(\frac{pq}{r}\right) = \left(\frac{r}{pq}\right) = \left(\frac{r}{q}\right)\left(\frac{r}{p}\right) = \left(\frac{p}{q}\right)\left(\frac{r}{p}\right) = \left(\frac{p}{q}\right)\left(\frac{-q}{p}\right) = 1$$

ou

$$\left(\frac{pq}{r-q}\right) = \left(\frac{r-q}{pq}\right) = \left(\frac{r-q}{q}\right)\left(\frac{r-q}{p}\right) =$$

$$= \left(\frac{r}{q}\right)\left(\frac{r-q}{p}\right) = \left(\frac{p}{q}\right)\left(\frac{r-q}{p}\right) = \left(\frac{p}{q}\right)\left(\frac{-q}{p}\right) = 1,$$

são satisfeitos. Com isso, provamos também a segunda parte do teorema. ■

Definição 6.17. Seja p um primo. Diremos $x, x+1, \ldots, x+a$ formam uma sequência para p, de $a+1$ elementos, se

$$\left(\frac{x}{p}\right) = \left(\frac{x+1}{p}\right) = \cdots = \left(\frac{x+a}{p}\right). \tag{6.10}$$

Dependendo se o valor comum em 6.10 é 1 ou -1 diremos que a sequência é positiva ou negativa, respectivamente.

Definição 6.18. Chamamos uma sequência $x, x+1, \ldots, x+a$ de uma sequência máxima para p quando nem $x-1, x$ nem $x+a, x+a+1$ formam uma sequência para p.

Definição 6.19. Chamamos uma sequência $x, x+1, \ldots, x+a$ de sequência interna (para p) quando $p \nmid (x-1)$ e $p \nmid (x+a+1)$.

Lema 6.20. *Se $x, x+1, \ldots, x+a$ é uma sequência para p, então, para cada y com $x\epsilon < y < (x+a)\epsilon$, vale*

$$\left(\frac{y}{q}\right) = \left(\frac{x}{p}\right). \tag{6.11}$$

Demonstração: Vamos demonstrar o caso específico onde $x, x+1$ é uma sequência para p, já que o caso geral é resultado de aplicações sucessivas desse caso. Vamos dividir a demonstração nos casos: $\left(\frac{x}{p}\right) = \left(\frac{x+1}{p}\right) = 1$ e $\left(\frac{x}{p}\right) = \left(\frac{x+1}{p}\right) = -1$. Suponhamos $\left(\frac{x}{p}\right) = \left(\frac{x+1}{p}\right) = 1$, Denote $x+1 = b$, então teremos

$$\left(\frac{b}{p}\right) = \left(\frac{b-1}{p}\right),$$

e devemos considerar $2 \leq b \leq p-1$. Seja y um inteiro satisfazendo $(b-1)\frac{q}{p} < y < b\frac{q}{p}$, então $0 < pb - qy < q$. Defina $r = qb - py$. Claramente, $0 < r < q$. Além disso, $(r, p) = (bq, p) = 1$ e $(r-q, p) = ((b-1)q, p) = 1$. Agora, observe que

$$\left(\frac{r}{p}\right) = \left(\frac{qb}{p}\right) = \left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$$

e

$$\left(\frac{r-q}{p}\right) = \left(\frac{(b-1)q}{p}\right) = \left(\frac{b}{p}\right) = \left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right).$$

Logo, pela Lema 6.16, não pode ocorrer

$$\left(\frac{r}{q}\right) = \left(\frac{p}{q}\right),$$

ou seja, temos a igualdade

$$\left(\frac{r}{q}\right) = -\left(\frac{p}{q}\right),$$

e a partir daí, substituindo r por $qb - py$, obtemos

$$\left(\frac{-py}{q}\right) = -\left(\frac{p}{q}\right),$$

o que implica em

$$\left(\frac{y}{q}\right) = 1 = \left(\frac{x-1}{p}\right) = \left(\frac{x}{p}\right),$$

como queríamos. Agora, suponhamos $\left(\frac{x}{p}\right) = \left(\frac{x+1}{p}\right) = -1$. Seja y um inteiro satisfazendo

$$\frac{q}{p}x < q - y < \frac{q}{p}(x+1)$$

então

$$\frac{q}{p}(p-x-1) < q - y < \frac{q}{p}(p-x).$$

Como

$$\left(\frac{p-x-1}{p}\right) = \left(\frac{-x-1}{p}\right) = -\left(\frac{x+1}{p}\right) = 1$$

e

$$\left(\frac{p-x}{p}\right) = 1,$$

podemos aplicar o caso já demonstrado à sequência $p-x-1, p-x$ e obter

$$\left(\frac{p-x}{p}\right) = \left(\frac{q-y}{q}\right),$$

ou seja,

$$\left(\frac{x}{p}\right) = \left(\frac{y}{q}\right).$$

Com isso finalizamos a demonstração. ■

É importante observar que até o momento não fizemos nenhuma suposição sobre $p > q$ ou $p < q$, ou seja, p e q podem ser intercambiados nas hipótese dos resultados. Em vista dessa observação, provamos o seguinte

Lema 6.21. *Se*

$$\left(\frac{y}{q}\right) = \left(\frac{y+1}{q}\right) = -\left(\frac{x}{p}\right), \tag{6.12}$$

então não ocorre $y < x\epsilon < y+1$.

Demonstração: Caso ocorra $y < x\epsilon < y+1$, então $y\epsilon^{-1} < x < (y+1)\epsilon^{-1}$ e pela observação e o lema anterior deve ocorrer

$$\left(\frac{y}{q}\right) = \left(\frac{y+1}{q}\right) = \left(\frac{x}{p}\right).$$

o que contradiz a hipótese do resultado a ser demonstrado. ■

Para prosseguirmos será necessário a introdução de um novo conceito:

Definição 6.22. Seja $p(a_1, a_2, \ldots, a_e)$ o número de soluções de

$$\left(\frac{r}{p}\right) = a_1,\ \left(\frac{r+1}{p}\right) = a_2, \ldots, \left(\frac{r+e-1}{p}\right) = a_e,\ 0 < r < p,$$

onde $a_i \in \{\pm 1\}$.

Exemplo 6.23. Seja p um primo ímpar, $p(1)$ denota a quantidade de elementos positivos r no intervalo $(0, p)$ tal que $\left(\frac{r}{p}\right) = 1$, ou seja, $p(1)$ denota a quantidade de resíduos quadráticos módulo p.

Exemplo 6.24. Tome $p = 5$. Vamos calcular $p(-1, -1)$. Iniciamos calculando o símbolo de Legendre para os elementos módulo p: $\left(\frac{1}{p}\right) = 1$, $\left(\frac{2}{p}\right) = -1$, $\left(\frac{3}{p}\right) = -1$ e $\left(\frac{4}{p}\right) = 1$. Logo, a única solução $\left(\frac{r}{p}\right) = \left(\frac{r+1}{p}\right) = -1$ é $r = 2$. Portanto, $p(-1, -1) = 1$.

Mais adiante faremos o uso dos seguintes teoremas demonstrados no trabalho de E. Jacobsthal, [19]:

Teorema 6.25. *Seja p um primo ímpar, então*

$$p(1, 1) = \left\lfloor \frac{p}{4} \right\rfloor .$$

Teorema 6.26. *Seja p um primo ímpar, então*

$$p(1, 1, 1) = \left\lfloor \frac{p}{8} \right\rfloor .$$

Lema 6.27. *Se $\left(\frac{x}{p}\right) = \left(\frac{x+a}{p}\right)$, onde $0 < x < x + a < p$, então, para todo y com $x\epsilon < y < (x + a)\epsilon$, $py \equiv qx \pmod a$,*

$$\left(\frac{y}{q}\right) = \left(\frac{a}{pq}\right)\left(\frac{x}{p}\right). \tag{6.13}$$

Demonstração: Seja n tal que $0 \leq n < a$ e $a \mid (x + np)$. Devido a

$$(y + nq)p = py + npq \equiv qx + npq = (x + np)q \pmod a,$$

temos $a \mid (y + nq)$. Para os números inteiros $u = \dfrac{1}{a}(x + np)$, $u + 1 = \dfrac{1}{a}(x + a + np)$, $v = \dfrac{1}{a}(y + nq)$ temos

$$\left(\frac{u}{p}\right) = \left(\frac{ax}{p}\right) = \left(\frac{a(a + x)}{p}\right) = \left(\frac{u + 1}{p}\right), \ \left(\frac{v}{q}\right) = \left(\frac{ay}{q}\right),$$

$$u\varepsilon = \frac{1}{a}(x\varepsilon + nq) < v < \frac{1}{a}((x + a)\varepsilon + nq) = (u + 1)\varepsilon.$$

Ao aplicar o Lema 6.20 a $x = u$ e $a = 1$, segue de 6.11, $\left(\frac{v}{q}\right) = \left(\frac{u}{p}\right)$, ou seja, $\left(\frac{ax}{p}\right) = \left(\frac{ay}{q}\right)$, logo multiplicando a igualdade por $\left(\frac{a}{p}\right)$, obtemos 6.13. ■

Lema 6.28. *Nas hipótese do Lema 6.27, sempre existe um y com $x\epsilon < y < (x + a)\epsilon$ e $py \equiv qx \pmod a$.*

Demonstração: Se y satisfaz a desigualdade $x\epsilon < y < (x+a)\epsilon$, então, equivalentemente, y satisfaz a desigualdade $0 < py - qx < aq$. Assim, basta mostrarmos que existe um y satisfazendo a última desigualdade e $py \equiv qx \pmod a$. Como p é relativamente primo com a, então existe um y satisfazendo $py \equiv qx \pmod a$, a partir daí podemos tomar uma solução $y + ka$, com k inteiro, satisfazendo $0 < py - qx < aq$. O que completa a demonstração. ■

Lema 6.29. *Sejam inteiros positivos $x_1, x_2, \ldots, x_l$ e a tais que $0 < x_1, \ldots, x_l < p - a$, $a \geq 2$ e $2 \leq l \leq a$. Se $x_1, x_2, \ldots, x_l$ são dois a dois incongruentes módulo a e*

$$\left(\frac{x_1}{p}\right) = \cdots = \left(\frac{x_l}{p}\right) = \left(\frac{x_1 + a}{p}\right) = \cdots = \left(\frac{x_l + a}{p}\right),$$

então existem inteiros $y_1, \ldots, y_l$, dois a dois incongruentes módulo a, com $x_i\epsilon < y_i < (x_i + a)\epsilon$, $i = 1, \ldots, l$, satisfazendo

$$\left(\frac{y_1}{q}\right) = \cdots = \left(\frac{y_l}{q}\right) = \left(\frac{a}{pq}\right)\left(\frac{x_1}{p}\right).$$

Demonstração: É imediato da aplicação do Lema 6.27 a $x = x_1, x_2, \ldots, x_l$. ■

Lema 6.30. *Se houver uma sequência com a elementos, $a \geq 2$, para p então*

$$1 = \left(\frac{2}{pq}\right) = \left(\frac{3}{pq}\right) = \cdots = \left(\frac{a-1}{pq}\right).$$

Demonstração: Para cada b inteiro tal que $1 \leq b \leq a - 1$, pelos Lemas 6.27 e 6.28, existe um inteiro y, satisfazendo $x\epsilon < y < (x + a)\epsilon$ e

$$\left(\frac{b}{pq}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{q}\right).$$

Pelo Lema 6.20, $\left(\frac{x}{p}\right)\left(\frac{y}{q}\right) = 1$, de onde podemos concluir que

$$\left(\frac{b}{pq}\right) = 1.$$

Fazendo esse processo para $b = 1, \ldots, a - 1$ demonstramos o lema. ■

Parte do próximo resultado será demonstrar que será demonstrar que não há anéis quadráticos euclidianos com discriminante $7q$.

Lema 6.31. *$p \geq 11$ e* $\left(\frac{2}{pq}\right) = 1$.

Demonstração: De acordo com a identidade 6.26, para $p \geq 11$ existe pelo menos uma sequência de três elementos. Portanto, pelo Lema 6.30, segue $1 = \left(\frac{2}{pq}\right)$. Resta-nos provarmos a impossibilidade para $p = 7$. Para $p = 7$, temos $\left(\frac{5}{q}\right) = \left(\frac{6}{p}\right) = -1$. Isso resulta em uma contradição com Lema 6.27 caso tenhamos algum y satisfazendo $\frac{5q}{7} < y < \frac{6q}{7}$ e que seja um resíduo quadrático módulo q. Se $q > 154$, o comprimento do intervalo $\left(\sqrt{\frac{5q}{7}}, \sqrt{\frac{6q}{7}}\right)$ é maior que 1 e, portanto, contém pelo menos um inteiro cujo quadrado é um y, logo temos uma contradição. Para os demais valores de q, calculamos um resíduo não quadrático z tal que $\frac{q}{7} < z < \frac{2q}{7}$ e portanto $q - z$ é um y adequado:

Conforme o Lema 6.31, podemos simplificar o Lema 6.27 quando $a = 2$ da seguinte forma:

Lema 6.32. *Se* $\left(\frac{x}{p}\right) = \left(\frac{x+2}{p}\right)$, *onde $0 < x < p - 2$, então para todo y satisfazendo $x\epsilon < y < (x + 2)\epsilon$ e $y \equiv x \pmod 2$ temos*

$$\left(\frac{y}{q}\right) = \left(\frac{x}{p}\right).$$

q	11	19	23	31	43	47	59	67	71	79	83	103	107	127	131	139	151
z	2	3	5	6	8	10	10	18	14	12	18	20	20	20	30	27	27

Tabela 6.1: Escolha de z para valores q

■

Aqui, introduziremos dois conceitos relacionados à sequência para p:

Definição 6.33. Seja $x, x+1, \ldots, x+a$ é uma sequência para p. Dizemos que a sequência $x, x+1, \ldots, x+a$ é uma sequência máxima para p quando nem $x-1, x$ nem $x+a, x+a+1$ formam uma sequência para p.

Definição 6.34. Seja $x, x+1, \ldots, x+a$ é uma sequência para p. Chamamos uma sequência $x, x+1, \ldots, x+a$ de sequência interna para p quando $p \nmid (x-1)$ e $p \nmid (x+a+1)$.

Lema 6.35. *Se existe uma sequência interna e máxima de a elementos para p, com $a \geq 2$, então $(\frac{a+1}{pq}) = -1$ ou $\epsilon < \frac{a+1}{a-1}$.*

Demonstração: Seja $x, x+1, \ldots, x+a-1$ uma sequência máxima e interna. Em particular, a sequência satisfaz:

$$-\left(\frac{x-1}{p}\right) = \left(\frac{x}{p}\right) = \left(\frac{x+1}{p}\right) = \cdots = \left(\frac{x+a-1}{p}\right) = -\left(\frac{x+a}{p}\right).$$

Aplicando o Lema 6.27 a $x-1$ e $x+a$ (em vez de $x,\ x+a$), obtemos que, para todo y no intervalo $(x\epsilon, (x+a-1)\epsilon)$ com $py \equiv qx \pmod{a+1}$,

$$\left(\frac{y}{q}\right) = \left(\frac{a+1}{pq}\right)\left(\frac{x-1}{p}\right) = -\left(\frac{a+1}{pq}\right)\left(\frac{x}{p}\right). \tag{6.14}$$

Agora, se o comprimento do intervalo $(x\epsilon, (x+a-1)\epsilon)$ for maior do que $a+1$, isto é, $(a-1)\epsilon > a+1$, então existe pelo menos um y satisfazendo 6.14. Além disso, pelo Lema 6.20 aplicado a $x, x+1, \ldots, x+a-1$, temos

$$\left(\frac{y}{q}\right) = \left(\frac{x}{p}\right),$$

e, assim segue $(\frac{a+1}{pq}) = -1$ ou $\epsilon < \frac{a+1}{a-1}$. O que demonstra o lema. ■

Em particular, para $a = 3$, podemos derivar o seguinte resultado:

Lema 6.36. *Se $\epsilon > 2$, então não existem sequências máximas de três elementos para p.*

Demonstração: Como $\left(\frac{1}{p}\right) = \left(\frac{4}{p}\right)$, então uma sequência máxima de três elementos só pode ser interna. Para demonstrar o lema, vamos utilizar a contra positiva do lema 6.35. Para isso basta observar que $(\frac{a+1}{pq}) = 1$ e $\epsilon > \frac{a+1}{a-1}$, de onde segue a não existência de sequências máximas e internas de três elementos para p, mas pela observação inicial, não existe sequências máximas de três elementos para p. ■

A seguir vamos definir uma notação para o números de sequências máximas para um primo p com determinado número de elementos.

Definição 6.37. Seja p um primo ímpar. Denotaremos por p_a, $a > 2$, o número de sequências máximas para p com a elementos.

A partir das identidades 6.25 e 6.26, juntamente com a definição acima, podemos enunciar o seguinte lema

Lema 6.38. *Seja p um primo ímpar. Então*

$$\sum_{a\geq 2}(a-1)p_a = \left\lfloor \frac{p}{4} \right\rfloor, \tag{6.15}$$

$$\sum_{a\geq 2}(a-2)p_a = \left\lfloor \frac{p}{8} \right\rfloor, \tag{6.16}$$

Subtraindo $\frac{3}{2}$ vezes 6.16 de 6.15 e omitindo os termos negativos, obtemos:

$$p_2 + \frac{1}{2}p_3 \geq \left\lfloor \frac{p}{4} \right\rfloor - \frac{3}{2}\left\lfloor \frac{p}{8} \right\rfloor. \tag{6.17}$$

Agora provaremos

Lema 6.39. *Se $\epsilon > 2$, então*

$$1 = \left(\frac{2}{pq}\right) = \left(\frac{3}{pq}\right)$$

Demonstração: De acordo com o Lema 6.36, $p_3 = 0$. Pelo Lema 6.31, sabemos que $p \geq 11$, o que implica $\left\lfloor \frac{p}{8} \right\rfloor \geq 1$, então, de acordo com 6.16, deve haver pelo menos uma sequência positiva para p com pelo menos 4 elementos. Portanto, pelo Lema 6.30 segue o lema. ■

Lema 6.40. $\epsilon < 3$.

Demonstração: Vamos supor que $\epsilon > 2$, já que não há necessidade de provarmos algo quando $\epsilon \leq 2$. De acordo com o Lema 6.36, $p_3 = 0$. Para $p \geq 23$, de acordo com 6.17, $p_2 \geq 2$, o que significa que há pelo menos uma sequência interna e máxima de dois elementos. Também para $p = 19$, a sequência $2, 3$ é máxima de dois elementos. Logo, para $p \geq 19$, de acordo com 6.35, temos $(\frac{3}{pq}) = -1$ ou $\epsilon < 3$. Pelo Lema 6.39, não ocorre $\left(\frac{3}{pq}\right) = -1$, assim segue a validade do Lema 6.40, exceto para o caso $p = 11$. No entanto, para $p = 11$ não pode ocorrer $\epsilon > 2$, o que entraria em contradição com o Lema 6.36, pois $3, 4, 5$ é uma sequência máxima de três elementos. Assim finalizamos a demonstração do resultado. ■

Lema 6.41. *Se $\epsilon > 2$ e*

$$1 = \left(\frac{2}{pq}\right) = \left(\frac{3}{pq}\right) = \cdots = \left(\frac{r}{pq}\right),$$

onde $r \geq 2$, então $1, 2, \ldots, r$ é uma sequência para p.

Demonstração: Primeiro provaremos que $\left(\frac{2}{p}\right) = 1$. Suponha que essa igualdade não seja verdadeira, então, seguindo a hipótese, $(\frac{2}{p}) = (\frac{2}{q}) = -1$. Além disso, pela hipótese e pelo Lema 6.40, $2 < \epsilon < 3$. Tomando $x = 1$ e $y = 2$, temos $y = 2 < x\epsilon = \epsilon < 3 = y + 1$, então, pela contrapositiva do Lema 6.21, $-1 = \left(\frac{2}{q}\right) \neq \left(\frac{3}{q}\right) = 1$. De acordo com o Lema 6.39, $1 = (\frac{3}{pq}) = \left(\frac{3}{p}\right)\left(\frac{3}{q}\right) = \left(\frac{3}{p}\right)$. Portanto temos os seguintes valores para o símbolo de Legendre:

i	2	3	4	5	6	7	8
(i/p)	-1	1	1	-1	-1		-1
(i/q)	-1	1	1		-1		-1

Tabela 6.2: Valores dos símbolos de Legendre

onde $(\frac{5}{p}) = -1$ é uma consequência do Lema 6.36. Como $2 < \epsilon$, então também $8 < 4\epsilon$ e, mais ainda, $3\epsilon > 8$, uma vez que o contrário implicaria $3\epsilon < 8 < 4\epsilon$ e de acordo com o Lema 6.20 aplicado à sequência $3, 4$ teríamos $-1 = \left(\frac{8}{p}\right) = \left(\frac{3}{p}\right) = 1$, o que é uma contradição. Mas $3\epsilon > 8$ implica que $5\epsilon < 15 < 16 = \frac{8}{3}6 < 6\epsilon$, o que entra em contradição com o Lema 6.20 aplicado à sequência 5, 6, uma vez que $1 = \left(\frac{16}{q}\right) \neq -1 = \left(\frac{5}{p}\right)$. Do que foi provado até aqui segue-se que o Lema 6.41 é verdadeiro para $r = 2$, razão pela qual, a partir de agora, assumiremos $r \geq 3$. Logo, de $r \geq 3$, para p, existe uma sequência $1, 2, \ldots, s$ no qual $s \geq 2$. Assumimos $s < r$, pois caso contrário o lema estaria provado. Como $2 < \epsilon < 3 \leq s + 1 < s\epsilon$ segue do Lema 6.20, aplicado a sequência $1, \ldots, s$, que $3, 4, \ldots, s + 1$ é uma sequência positiva para q. Em particular, $(\frac{s+1}{q}) = 1$, que por meio da hipótese e por $s + 1 \leq r$, implica que $(\frac{s+1}{p}) = 1$. Então $1, 2, \ldots, s, s + 1$ também é uma sequência para p. Podemos repetir o processo até concluirmos que $1, 2, \ldots, r$ é uma sequência para p, o que prova o lema. ■

Lema 6.42. *Não ocorre*

$$1 = \left(\frac{2}{pq}\right) = \left(\frac{3}{pq}\right) = \cdots = \left(\frac{p-1}{pq}\right).$$

Demonstração: Suponhamos o contrário, isto é, é válida a igualdade

$$1 = \left(\frac{2}{pq}\right) = \left(\frac{3}{pq}\right) = \cdots = \left(\frac{p-1}{pq}\right).$$

Como $1, 2, \ldots, p - 1$ nunca é uma sequência para $p > 2$, então segue do Lema 6.42 que $\epsilon < 2$. Agora, observe que para $x = 1, 2, \ldots, p - 1$

$$\left(\frac{x}{q}\right) = \left(\frac{x}{p}\right) = -\left(\frac{p-x}{p}\right) = -\left(\frac{p-x}{q}\right) = \left(\frac{x-p}{q}\right).$$

Assim, se p' é uma solução de $pp' \equiv -1 \pmod q$, então segue que $p'x,\ p'x + 1$ é uma sequência para q de dois elementos, e, mais ainda, todas as sequências dessa forma são duas a duas distintas módulo q. Como $q \equiv 3 \pmod 4$, portanto $\left(\frac{-1}{q}\right) = -1$, então, para cada sequência negativa $a, a + 1$ podemos sempre corresponder uma sequência positiva $q - a - 1,\ q - a$. Como temos $p - 1$ sequências $p'x,\ p'x + 1$, positivas e negativas, então, de acordo com o Teorema 6.25,

$$p - 1 \leq 2q(1, 1) = 2\left\lfloor\frac{q}{4}\right\rfloor = 2\left(\frac{q-3}{4}\right) = \frac{q-3}{2}.$$

Logo, $q \geq 2p+1$ o que contradiz $\epsilon = \frac{q}{p} < 2$. Essa contradição demonstra o Lema 6.42. ■

Lema 6.43. *Se $s \geq 1,\ t - s \geq 2$,*

$$1 = \left(\frac{2}{pq}\right) = \left(\frac{3}{pq}\right) = \cdots = \left(\frac{t-1}{pq}\right) = -\left(\frac{t}{pq}\right),$$

$$-\left(\frac{s}{p}\right) = \left(\frac{s+1}{p}\right) = \left(\frac{s+2}{p}\right) = \cdots = \left(\frac{t-p}{p}\right) = -\left(\frac{t}{p}\right),$$

então $\epsilon > \frac{s+1}{s}$.

Demonstração: Suponhamos o contrário, ou seja, $s\epsilon < s+1$, e vamos chegar a um absurdo. De $s\epsilon < s+1$ segue que o intervalo $(s\epsilon, t\epsilon)$ contém o sistema completo de resíduos $s+1, s+2, \ldots, t \pmod{t-s}$. Agora, aplicando o Lema 6.27 aos valores $x = s$ e $a = t-s$, então existe um y, satisfazendo $s+1 \leq y \leq t$, tal que

$$\left(\frac{y}{q}\right) = \left(\frac{t-s}{pq}\right)\left(\frac{s}{p}\right).$$

No entanto, a partir da hipótese seguem que $(\frac{y}{q}) = -(\frac{s}{p})$ e $(\frac{t-s}{pq}) = 1$. Assim, chegamos a uma contradição. Essa contradição prova o Lema 6.43. ■

Lema 6.44. *Se* $2 \leq r \leq p-2$,

$$1 = \left(\frac{2}{pq}\right) = \left(\frac{3}{pq}\right) = \cdots = \left(\frac{r}{pq}\right),$$

e se $1, 2, \ldots, r$ *não formam uma sequência para* p*, então* $\epsilon < \frac{r+1}{r}$.

Demonstração: Demonstraremos que, nas condições da hipótese, a suposição de $\epsilon < \frac{r}{r-1}$ implica em $\epsilon < \frac{r+1}{r}$. Mas antes justificaremos a procedência da suposição. Vamos fazê-la de acordo com $1, 2, \ldots, r-1$ formam ou não uma sequência para p. Se $1, 2, \ldots, r-1$ formam uma sequência para p, então neste caso temos $(\frac{r}{p}) = -1$ e $(\frac{r}{q}) = -1$. A aplicação do Lema 6.20 à sequência $1, 2, \ldots, r-1$ implica que $(r-1)\epsilon < r$, portanto, $\epsilon < \frac{r}{r-1}$. Agora, vamos ao caso $1, 2, \ldots, r-1$ não formam uma sequência para p. neste caso, pelo Lema 6.41, temos a validade para o caso base $r = 2$, já que $\epsilon < 2 = \frac{r}{r-1}$, e uma vez que demonstraremos que a validade de $\epsilon < \frac{r}{r-1}$ implica na validade de $\epsilon < \frac{r+1}{r}$ podemos fazer a suposição $\epsilon < \frac{r}{r-1}$ sem prejuízos, para $r \geq 2$.

A partir de agora, vamos mostrar que

$$\frac{r+1}{r} < \epsilon < \frac{r}{r-1} \tag{6.18}$$

é uma contradição. e assim demonstraremos o Lema 6.44. Distinguiremos a demonstração nos casos **1) - 2.2.2)**:

1) $\left(\frac{r-1}{p}\right) = \left(\frac{r+1}{p}\right) = \mu$. Neste cenário, temos $\left(\frac{r^2-1}{p}\right) = \left(\frac{r^2}{p}\right) = 1$, $(r^2-1)\epsilon = (r-1)\epsilon(r+1) < r(r+1) < r^2\epsilon$, a partir daí, conforme o Lema 6.20, $\left(\frac{r(r+1)}{q}\right) = 1$ e $\left(\frac{r}{q}\right) = \left(\frac{r+1}{q}\right)$. Portanto, a situação é a seguinte:

i	$r-1$	r	$r+1$
(i/p)	μ	v	μ
(i/q)	μ	v	v

.

Tabela 6.3: Valores dos símbolos de Legendre

1.1) $\mu = v$. Neste caso é necessário que seja $r \geq 3$. Como $1, 2, \ldots, r$ não é uma sequência para p, existe um elemento s em $1, 2, \ldots, r-2$ com $\left(\frac{s}{p}\right) = -\mu$. Escolhemos

s como o maior elemento com essa propriedade. Agora, denote t o menor número da sequência $r+2, r+3, \ldots, p-1$ com $\left(\frac{t}{p}\right) = -\mu$. Claro que existe um elemento t satisfazendo essa condição, pois caso contrário, $r-1, r, \ldots, p-1$ seria uma sequência para p e como

$$(r-1)\epsilon < r < p-1 < (p-1)\epsilon,$$

então, pelo Lema 6.20, $r, r+1, \ldots, p-1$ seria uma sequência para q, logo

$$\left(\frac{r}{pq}\right) = \left(\frac{r+1}{pq}\right) = \cdots = \left(\frac{p-1}{pq}\right),$$

o que contradiz o Lema 6.42, assim comprovando a existência de t. Como

$$(r-1)\epsilon < r < t = (r+1) + (t-r-1) < r\epsilon + (t-r-1)\epsilon = (t-1)\epsilon,$$

segue do Lema 6.20 que $r, r+1, \ldots, t$ é uma sequência para q. Logo, de acordo com o Lema 6.43, $\epsilon > \frac{s+1}{s}$. Mas isso é um absurdo, uma vez que $s \leq r-2$ e $\epsilon < \frac{r}{r-1}$.

1.2) $\mu = -v$. neste caso temos

$$(r-1)\epsilon < r+1 < (r+1)\epsilon,\ r+1 \equiv r-1 \pmod 2$$

de onde surge uma contradição com o Lema 6.32 quando tomando $x = r-1$.

2) $\mu = \left(\frac{r-1}{p}\right) \neq \left(\frac{r+1}{p}\right) = -\mu$. Este caso será dividido nos seguintes casos.

2.1) $\mu = \left(\frac{r-1}{p}\right) = \left(\frac{r}{p}\right)$ e $-\mu = \left(\frac{r+1}{p}\right)$. Por 6.18 temos $(r-1)\epsilon < r+1 < r\epsilon$, logo, de acordo com o Lema 6.20, $(\frac{r+1}{q}) = \mu$. Agora, tudo funciona da mesma forma que no caso **1.1)** com a simplificação de que agora tomamos $t = r+1$.

2.2) $\mu = \left(\frac{r-1}{p}\right)$ e $-\mu = \left(\frac{r}{p}\right) = \left(\frac{r+1}{p}\right)$. Neste caso considere a desigualdade

$$r\epsilon = (r-1)\epsilon + \epsilon < r+2 = (r+1)+1 < r\epsilon + \epsilon = (r+1)\epsilon,$$

de onde resulta, por aplicação do Lema 6.20, que $(\frac{r+2}{q}) = -\mu$. Portanto, como descrito na próxima tabela, teremos os seguintes valores para os símbolos de Legendre

i	$r-1$	r	$r+1$	$r+2$
(i/p)	μ	$-\mu$	$-\mu$	
(i/q)	μ	$-\mu$		$-\mu$

.

Tabela 6.4: Valores dos símbolos de Legendre

2.2.1) $\left(\frac{r+1}{q}\right) = -\mu$. Se pensarmos em μ sendo substituído por $-\mu$, então, estamos lidando novamente com um caso semelhante ao caso **1.1)**, com a diferença de que agora $r = 2$ também é possível e escolhemos s como $s = r-1$.

2.2.2) $\left(\frac{r+1}{q}\right) = \mu$. Como $\left(\frac{2}{p}\right) = \left(\frac{2}{q}\right)$, então segue os valores

i	$2r-2$	$2r$	$2r+2$
(i/p)	e	$-e$	
(i/q)		$-e$	e

.

Tabela 6.5: Valores dos símbolos de Legendre

Agora considere as desigualdades, resultante de 6.18 e $\epsilon < 2$,

$$(2r-2)\epsilon < 2r = (r+1)+(r-1) < r\epsilon + (r-1)\epsilon = (2r-1)\epsilon$$

e

$$(2r-1)\epsilon = 2(r-1)\epsilon + \epsilon < 2r+2 < 2r\epsilon.$$

Caso ocorresse $(\frac{2r-1}{p}) = e$, pela primeira das duas desigualdades acima, teríamos

$$(2r-2)\epsilon < 2r < (2r-1)\epsilon,$$

mas por

$$\left(\frac{2r-2}{p}\right) = \left(\frac{2r-1}{p}\right) = e,$$

de acordo com com o Lema 6.20 teríamos,

$$\left(\frac{2r}{q}\right) = e,$$

o que é uma contradição. No caso $\left(\frac{2r-1}{p}\right) = -e$, chegaremos a uma contradição semelhante, mas agora utilizaremos a segunda desigualdade das duas anteriores, de onde concluímos que

$$(2r-1)\epsilon < 2r+2 < 2r\epsilon.$$

Assim, aplicando o Lema 6.20 a sequência $2r-1$, $2r$ deveríamos ter

$$-e = \left(\frac{2r-2}{p}\right) = \left(\frac{2r+2}{q}\right) = e$$

o que é uma contradição. Já o caso $\left(\frac{2r-1}{p}\right) = 0$, ou seja, $p \mid (2r-1)$, também é impossível. De fato, neste caso teríamos a igualdade $r = \frac{p+1}{2}$. Além disso, temos $q = \epsilon p < \frac{pr}{r-1} < p+3$. Agora, utilizando a igualdade $r = \frac{p+1}{2}$ podemos ainda demonstrar que $\frac{pr}{r-1} < p+3$, ou seja, $0 < 3r - 3 - p$, assim, obtemos $q = \epsilon p < \frac{pr}{r-1} < p+3$, o que é um absurdo, já que por $p \equiv q \pmod 4$, devemos ter $q \geq p+4$. Com isso provamos o Lema 6.44 ■

Com isso, finalizamos a demonstração do último lema da seção. Agora iniciaremos a demonstração do Teorema 6.13.

Demonstração do Teorema 6.13: Seja u tal que

$$1 = \left(\frac{2}{pq}\right) = \left(\frac{3}{pq}\right) = \cdots = \left(\frac{u-1}{pq}\right), \ \left(\frac{u}{pq}\right) = -1. \tag{6.19}$$

De acordo com o Lema 6.42, existe pelo menos um u com essas propriedade e, mais ainda, segundo o Lema 6.31, u pode ser tomado sendo um primo ímpar satisfazendo

$$3 < u < p-1.$$

Vamos dividir o problema em dois casos: $1, 2, \ldots, u-1$ é ou não uma sequência para p.

A) $1, 2, \ldots, u-1$ não é uma sequência para p. Por 6.19 e como $u > 2$, segue do Lema 6.44 que $\epsilon < \frac{u}{u-1}$.

Se $\left(\frac{u-1}{p}\right) = \left(\frac{u}{p}\right) = \mu$, então, segue de 6.19, $\left(\frac{u}{q}\right) = -\mu$ e $(u-1)\epsilon < u < u\epsilon$ uma contradição com 6.20. Então segue os valores dos símbolos de Legendre (i/p) e (i/q) :

i	$u-1$	u
(i/p)	μ	$-\mu$
(i/q)	μ	μ

.

Tabela 6.6: Valores dos símbolos de Legendre

Agora, tome s o maior número da sequência $1, 2, \ldots, u-2$ com $\left(\frac{s}{p}\right) = -\mu$ e defina $t = s$, assim seguindo a notação do Lema 6.43 chegamos em

$$\epsilon > \frac{s+1}{s} > \frac{u}{u-1}$$

o que é uma contradição.

B) $1, 2, \ldots, u-1$ é uma sequência para p. Defina v satisfazendo

$$1 = \left(\frac{2}{q}\right) = \left(\frac{3}{q}\right) = \cdots = \left(\frac{v-1}{q}\right), \ \left(\frac{v}{q}\right) = -1. \tag{6.20}$$

Vamos mostrar que $v \geq u$. Devido a 6.31, $\left(\frac{2}{pq}\right) = 1$ e como $1, 2, \ldots, u-1$ é uma sequência para p com $u > 3$, $\left(\frac{2}{p}\right) = 1$, logo $v \geq 3$. Portanto, v deve ser um número primo ímpar. Como, por 6.40, $\epsilon < 3$, assim segue $1 \cdot \epsilon < v$, e caso também ocorra $v < (u-1)\epsilon$, então por 6.20 seguiria $\left(\frac{v}{q}\right) = 1$, o que é uma contradição, logo segue que $v \geq u$. Agora vamos que $1, 2, \ldots, u$ não é uma sequência para p. Se $1, 2, \ldots, u$ fossem uma sequência para p, também seguiria, por 6.20, que $v \geq u+1$, mas isso contradiria as identidades 6.19 e 6.20. De fato, por 6.19 e 6.20 e considerando $u \leq v-1$, teríamos $1 = \left(\frac{u}{pq}\right) = \left(\frac{u}{p}\right)\left(\frac{u}{q}\right) = 1(-1) = -1$. Portanto, $1, 2, \ldots, u-1$ é uma sequência máxima para p. Consequentemente, de acordo com 6.19 e 6.20, $v \neq u$, ou seja, $v \geq u+2$. Agora vamos provar que $u \geq 5$. Suponhamos o contrário, assim seguem $u = 3$ e

i	1	2	3	4	5	6	7	8	9	10
(i/p)	1	1	- 1	1		-1		1	1	
(i/q)	1	1	1	1		1		1	1	

.

Tabela 6.7: Valores dos símbolos de Legendre

Pelo Lema 6.39, é necessário que ϵ seja menor do que 2. Logo, $3\epsilon < 6$. Aplicando o Lema 6.21 aos valores $x = 3$, então $(\frac{5}{q}) = 1$ não é possível, o que implica que $(\frac{5}{q}) = -1$. Como $\left(\frac{3}{q}\right) = \left(\frac{4}{q}\right) = 1$ e $\left(\frac{3}{q}\right) = -1$ então, pelo Lema 6.21, não pode ocorrer $3 < 3\epsilon < 4$. Portanto, concluímos que $3\epsilon > 4$ que é equivalente a $6\epsilon > 8$, e novamente, utilizando o Lema 6.21, não pode ocorrer $8 < 6\epsilon < 9$. Assim, $6\epsilon > 9$, ou seja, $\epsilon > \frac{3}{2}$. Agora, note que não pode ocorrer $\left(\frac{5}{p}\right) = \left(\frac{7}{p}\right) = 1$, pois isso faria com que $7, 8, 9, 10$ fossem uma sequência de quatro termos para p, o que é impossível de acordo com o Lema 6.30 e $\left(\frac{3}{pq}\right) = -1$. Também não pode ocorrer o caso $\left(\frac{5}{p}\right) = \left(\frac{7}{p}\right) = -1$, pois isso contradiria o Lema 6.32. De fato, devido a $3\epsilon < 9 < 7\epsilon$, podemos aplicar o Lema 6.32 aos valores $x = 3$ ou $x = 5$, dependendo se $9 < 5\epsilon$ ou $5\epsilon < 9$ e então, em ambos os casos seguiria $\left(\frac{9}{q}\right) = -1$, o que é um absurdo. Portanto, temos $\left(\frac{5}{p}\right) = -\left(\frac{7}{p}\right)$. Assim, apenas os dois casos descritos nas tabelas 6.8 e 6.9 são possíveis.

No primeiro caso, descrito na tabela 6.8, por $\epsilon > \frac{3}{2}$, que é equivalente a $10\epsilon > 15$, não pode ocorrer $15 > 8\epsilon$, já que se ocorresse, pelo Lema 6.20 ocorreria $-1 = \left(\frac{15}{q}\right) = \left(\frac{9}{p}\right) = 1$.

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
(i/p)	1	1	- 1	1	1	-1	-1	1	1	1					
(i/q)	1	1	1	1	-1	1		1	1	-1		1			-1

Tabela 6.8: Possibilidades dos Valores dos símbolos de Legendre

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
(i/p)	1	1	- 1	1	-1	-1	1	1	1	-1					
(i/q)	1	1	1	1	-1	1		1	1	-1		1			-1

.

Tabela 6.9: Possibilidades dos Valores dos símbolos de Legendre

Então $8\epsilon > 15$, ou seja, $\epsilon > \frac{15}{8}$. Daí segue que $6\epsilon < 12 < 7\epsilon$ o que nos leva a uma contradição com o Lema 6.20. No segundo caso, situação descrita na tabela 6.9, segue de forma semelhante que, devido a $6\epsilon > 9$, $5\epsilon > 9$, ou seja, $\epsilon > \frac{9}{5}$. Então, $7\epsilon < 15 < 9\epsilon$, levando novamente a uma contradição com o Lema 6.20. Essas duas contradições prova que é impossível $u \geq 5$. Agora a situação é a seguinte:

i	1	2	...	$u-1$	u	$u+1$	$u+2$	$u+3$	$u+4$
(i/p)	1	1		1	-1	1		1	

i	1	2	...	$v-1$	v	$v+1$	$v+2$	$v+3$	$v+4$	$v+5$
(i/q)	1	1		1	-1	1		1		1

.

Tabela 6.10: Valores dos símbolos de Legendre

Como $u \geq 5$ e $v \geq 7$, e u e v são ímpares, todas as afirmações estão corretas. Entre os números $u+2$, $u+4$, um deles é divisível por 3, o que explica por que a ainda deve conter mais um resíduo quadrático módulo p. O mesmo se aplica aos valores (i/q), mas desta vez considerando valores $v+2$ e $v+4$. A partir dos Lemas 6.20 e 6.21, $(u-1)\epsilon < v$ e $u\epsilon > v-1$, ou seja,

$$\frac{v-1}{u} < \epsilon < \frac{v}{u-1}. \tag{6.21}$$

Também é claro que $\frac{p}{2} > u-1$ uma vez que os elementos $1, \ldots, u-1$ são resíduos quadráticos módulo p. Então $p \geq 2u-1$, e, como $2 \nmid u$, até mesmo, $p \geq 2u+1$ deve ocorrer. Em qualquer caso, é $p \geq u+6$. Da mesma forma, $q \geq 2v+1 \geq v+8$.

Agora, distinguimos o restante da demonstração nos dois casos seguintes:

1) $\left(\frac{u+2}{p}\right) = 1$. De acordo com 6.19, temos

$$\left(\frac{u}{pq}\right) = -1.$$

Aplicando o Lema 6.29 a

$$l = 3, a = u, x_1 = 1, x_2 = 2, x_3 = 3,$$

segue que para cada um dos intervalos

$$(\epsilon, (u+1)\epsilon),\ (2\epsilon, (u+2)\epsilon),\ (3\epsilon, (u+3)\epsilon)$$

existe um y_1, y_2, y_3, respectivamente, de modo que eles são distintos (até mesmo módulo u) e $(\frac{y_i}{q}) = -1$ $(i = 1, 2, 3)$. Seguindo as informações obtidas até aqui sobre os símbolos

de Lagrange, entre os inteiros $1, 2, \ldots, v+5$ há no máximo dois resíduos não quadráticos módulo q, portanto, como y_1, y_2, y_3 formam uma sequência de três resíduos quadráticos módulo q é necessário que o maior entre eles seja maior ou igual que $v+6$. Assim, denotando $y = \max\{y_1, y_2, y_3\}$, segue $y \geq v+6$. Dessa forma, temos

$$(u+1)\epsilon = (u-1)\epsilon + 2\epsilon < v+6 \leq y < (u+3)\epsilon.$$

Agora, aplicando 6.20 à sequência $u+1, u+2, u+3$, segue que $(\frac{y}{q}) = 1$, o que é uma contradição.

2) $\left(\frac{u+2}{p}\right) = -1$. Primeiro, consideramos o caso $\epsilon < 2$. Por agora, mostraremos que $\left(\frac{v+2}{q}\right) = 1$ não é possível. Caso ocorresse $(\frac{v+2}{q}) = 1$, aplicando o Lema 6.21 a $x = u+2, y = v+1$, então não ocorreria

$$v+1 < (u+2)\epsilon < v+2.$$

Mas como, utilizando a desigualdade 6.21,

$$(u+2)\epsilon = u\epsilon + 2\epsilon > (v-1) + 2 = v+1,$$

então deveria ocorrer

$$v+2 < (u+2)\epsilon.$$

Assim, também, utilizando novamente a desigualdade 6.21, teríamos

$$u\epsilon = (u-1)\epsilon + \epsilon < v+2 < (u+2)\epsilon.$$

Como $u \equiv v+2 \pmod 2$ e $\left(\frac{u}{p}\right) = \left(\frac{u+2}{p}\right)$, logo, aplicando o Lema 6.32 a $x = u$ e $y = v+2$, seque que $\left(\frac{v+2}{q}\right) = \left(\frac{u}{p}\right) = -1$, ou seja, uma contradição. A partir de agora poderemos supor $\left(\frac{v+2}{q}\right) = -1$. Vamos mostrar que essa suposição também nos leva uma contradição. Iniciamos analisando o que ocorre quando supomos $u = 5$. Sendo $u = 5$, $\epsilon < 2$ e, pela desigualdade 6.21, $v - 1 < u\epsilon$, temos

$$v < u\epsilon + 1 < 11.$$

Como v é um número primo maior que $u = 5$, v só pode ser igual a 7, mas isso também é impossível, pois teríamos $\left(\frac{9}{q}\right) = \left(\frac{v+2}{q}\right) = -1$. Portanto, podemos assumir $u \geq 7$. A partir disso, temos $u + 5 < 2u$, o que implica $\frac{u+5}{2} < u$ e assim segue $\left(\frac{\frac{u+5}{2}}{p}\right) = 1$, daí obtemos $\left(\frac{u+5}{p}\right) = 1$. Nessas condições, vamos obter mais duas informações essenciais para prosseguirmos. Primeiro, como observado anteriormente $v+2$ ou $v+4$, ou mesmo ambos, devem ser um resíduo quadrático, mas diante da suposição $\left(\frac{v+2}{q}\right) = -1$, então $\left(\frac{v+4}{q}\right) = 1$. Além, disso como observado, $v+2$ ou $v+4$ é divisível por 3, como $v+2$ não é um resíduo quadrático módulo q então $v+2$ não pode ser divisível por 3, pois, como $\frac{v+2}{q} < v$, isso implicaria em

$$\left(\frac{v+2}{q}\right) = \left(\frac{\frac{v+2}{3}}{q}\right)\left(\frac{3}{q}\right) = 1,$$

o que é uma contradição. Logo $3 \mid v+4$ e $3 \mid v+7$ que implica $\frac{v+7}{3} < v$ e assim segue

$$\left(\frac{v+4}{q}\right) = \left(\frac{v+7}{q}\right) = 1.$$

Segundo, como observamos anteriormente, a suposição $\left(\frac{u+2}{p}\right) = -1$ implica $\left(\frac{u+4}{p}\right) = 1$. Além disso, como 2 divide $u+5$, e como $\frac{u+5}{2} < u$, procedendo de maneira análoga ao que fizemos logo acima, $\left(\frac{u+5}{p}\right) = 1$, dessa forma temos que $u+3, u+4, u+5$ formam uma sequência positiva para p. Agora aplicamos o Lema 6.29 a

$$l = 4,\ a = u, x_1 = 1,\ x_2 = 3,\ x_3 = 4,\ x_4 = 5$$

de onde concluímos que para cada intervalo

$$(\epsilon, (u+1)\epsilon),\ (3\epsilon, (u+3)\epsilon),\ (4\epsilon, (u+4)\epsilon),\ (5\epsilon, (u+5)\epsilon)$$

existe $y_i, i = 1, 2, 3, 4$, respectivamente, todos distintos e para os quais $\left(\frac{y_i}{q}\right) = -1$. Novamente denotarmos y o maior entre eles. Devido a

$$\left(\frac{v+4}{q}\right) = \left(\frac{v+7}{q}\right) = 1,$$

entre os valores $1, 2 \ldots, v+7$ há apenas dois resíduos não quadráticos, e como $y < v+8$ implicaria a existência de três resíduos não quadráticos dentre esses elementos, o que seria uma contradição, então $y \geq v+8$. Por outro lado, utilizando a desigualdade 6.21,

$$(u+3)\epsilon = (u-1)\epsilon + 4\epsilon < v+8 \leq y < (u+5)\epsilon.$$

Além disso, como $u+3, u+4, u+5$ é uma sequência positiva para p segue que $\left(\frac{y}{q}\right) = 1$, ou seja, uma contradição.

Agora, vamos considerar o caso em que $\epsilon > 2$. Posteriormente, examinaremos a possibilidade de $u = 5$, portanto, por enquanto, suponhamos que $u \geq 7$. Assim, $\left(\frac{u+4}{p}\right) = \left(\frac{u+5}{p}\right) = 1$. Além disso, $\left(\frac{u+6}{p}\right) = 1$ deve ser ocorrer, pois, caso contrário, $u+3, u+4, u+5$ seria uma sequência máxima para p, o que é impossível de acordo com o Lema 6.36. Agora podemos aplicar o Lema 6.29 a

$$l = 5, x_1 = 1, x_2 = 3, x_3 = 4, x_4 = 5, x_5 = 6,$$

e assim obtermos que para cada um dos intervalos

$$(\epsilon, (u+1)\epsilon),\ (3\epsilon, (u+3)\epsilon),\ (4\epsilon, (u+4)\epsilon),\ (5\epsilon, (u+5)\epsilon),\ (6\epsilon, (u+6)\epsilon)$$

existe y_i, $i = 1, 2, 3, 4, 5$, respectivamente, distintos e que satisfazem $(\frac{y_i}{q}) = -1$. É claro que, $u = 7$ é impossível devido a suposição $\left(\frac{u+2}{p}\right) = -1$. Portanto, $u \geq 11$ e $v \geq 13$, o que implica em $\left(\frac{v+7}{q}\right) = \left(\frac{v+9}{q}\right) = \left(\frac{v+11}{q}\right) = 1$. Além disso, entre os números $v+2, v+4, v+6, v+8, v+10$, pode haver no máximo três resíduos não quadráticos módulo q, portanto, o maior dos y_i, que chamaremos novamente de y, deve ser maior ou igual a $v+12$. Agora, utilizando novamente a desigualdade 6.21,

$$(u+3)\epsilon = (u-1)\epsilon + 4\epsilon < v+12 \leq y < (u+6)\epsilon,$$

e $u+3, u+4, u+5, u+6$ é uma sequência positiva para p, de modo que, de acordo com o Lema 6.20, surge a contradição $(\frac{y}{q}) = 1$.

Finalmente, resta considerar $u = 5$. Neste caso, podemos descrever os valores dos símbolos de Legendre conforme descrito na tabela 6.11.

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
(i/p)	1	1	1	1	-1	1	-1	1	1	-1					
(i/q)	1	1	1	1	1	1			1			1			1

Tabela 6.11: Valores dos símbolos de Legendre

Aplicando o Lema 6.32 a $x = 5$, concluímos que todo elemento ímpar no intervalo $(5\epsilon, 7\epsilon)$ satisfaz $\left(\frac{y}{q}\right) = \left(\frac{5}{p}\right) = -1$, ou seja, são resíduos não quadráticos módulo q. Como $\left(\frac{15}{q}\right) = 1$, então $15 \notin (5\epsilon, 7\epsilon)$. Além disso, como pelo Lema 6.40, $\epsilon < 3$, logo $15 < 5\epsilon$ não pode ocorrer, o que implica $7\epsilon < 15$. Agora, aplicando o Lema 6.27 a $x = 7, a = 3$, e levando em consideração que $\left(\frac{3}{pq}\right) = 1$, o que por sua vez implica em $p \equiv q \pmod 3$, chegamos à conclusão de que todos os inteiros no intervalo $(7\epsilon, 10\epsilon)$ que satisfazem $y \equiv 7 \equiv 1 \pmod 3$ devem satisfazer $\left(\frac{y}{q}\right) = \left(\frac{3}{pq}\right)\left(\frac{7}{p}\right) = -1$, isto é, devem ser resíduos não quadráticos módulo q. No entanto, como $\epsilon > 2$, $7\epsilon < 16 < 10\epsilon$. Mas, como $\left(\frac{16}{q}\right) = 1$, temos uma contradição. Assim, provamos o teorema. ■

A partir dos Teorema 6.13 e 6.12, podemos concluir que os anéis quadráticos $\mathcal{O}_d$, com discriminante composto d congruente a 1 módulo 4, são norma euclidianos apenas, possivelmente, quando $d = 3q$, onde q é um inteiro primo $\equiv 3 \pmod 4$. Portanto, a partir de agora, no decorrer do capítulo, focaremos na classificação dos anéis quadráticos com discriminante $d = 3q$.

6.2.3 Classificação de anéis quadráticos com discriminante $3q$

O Objetivo desta subseção será classificar os anéis quadráticos com discriminante da forma $3q$. A partir do Teorema 6.13 juntamente com o Teorema 6.12, podemos concluir que os anéis quadráticos $\mathcal{O}_d$, com d livre de quadrados e composto, são norma euclidianos apenas, possivelmente, quando $d = 3q$, onde q é um número primo satisfazendo $q \equiv 3 \pmod 4$. De maneira mais especifica, podemos dividir a analise nos casos $q \equiv 7 \pmod 8$ ou $q \equiv 3 \pmod 8$, de acordo com as possibilidades da classe de q módulo 8. Iniciaremos com a classificação dos anéis quadráticos com discriminante $3q$, onde $q \equiv 7 \pmod 8$. Em seguida lidaremos com a classificação dos anéis quadráticos com discriminante $3q$, onde $q \equiv 3 \pmod 8$.

Classificação de anéis quadráticos com discriminante $3q$ onde $q \equiv 7 \pmod 8$

Agora, trataremos da classificação dos anéis quadráticos norma euclidianos $\mathcal{O}_{3q}$, onde $q \equiv 7 \pmod 8$, demonstrando que $\mathcal{O}_{21}$ é o único corpo quadrático norma euclidiano satisfazendo essas condições. Seguiremos a referência [12]. Vale ressaltar que essa abordagem é totalmente elementar.

Teorema 6.45. *Anéis quadráticos da forma $\mathcal{O}_{3q}$, onde p é um primo da forma $p = 8k+7$, não são norma euclidianos, exceto quando $p = 7$.*

Demonstração: Suponhamos o contrário, isto é, $\mathcal{O}_{3q}$ é norma euclidiano, para algum $p > 7$. A propriedade euclidiana no anel quadrático $\mathcal{O}_{3q}$ implica que para quaisquer racionais a, b devem existir inteiros x, y, de mesma paridade, tais que

$$|(x - 2a)^2 - d(y - 2b)^2| < 4.$$

Tomando $a = 0$ e $b = \dfrac{g}{p}$, obtemos que

$$|px^2 - 3(py - 2g)^2| < 4p. \tag{6.22}$$

Um cálculo simples nos mostra que

$$px^2 - 3(py - 2g)^2 \equiv -3 \cdot 4g^2 \pmod{4p}.$$

Além disso, como $p = 8k + 7$ é primo temos duas possibilidades: $p = 24k + 7$ ou $p = 24k + 23$. Vamos dividir nossa análise de acordo com essas duas possibilidades.

Caso 1. Suponhamos $p = 24k + 7$. Neste caso observe que é sempre possível obter soluções para a equação

$$-3 \cdot 4g^2 \equiv 8q^2 \pmod{4p}.$$

Na expressão acima, tomando q suficientemente pequeno, pela desigualdade 6.22, pelo menos umas das igualdades deve ocorrer

$$px^2 - 3(py - 2q)^2 = 8q^2 \tag{6.23}$$

$$px^2 - 3(py - 2q)^2 = 8q^2 - 4p \tag{6.24}$$

Vamos mostrar que a equação 6.23 não possui solução para qualquer escolha de q. Primeiro suponhamos x e y pares, então a existência de uma solução de 6.23 implica na existência de uma solução de $px^2 - 3Y^2 = 2q^2$. Tomando uma solução (x, Y, q) na qual temos $mdc(x, Y, q) = 1$ e analisando a equação módulo 3 teremos $p \equiv 1 \pmod 3$ e $2q^2 \equiv 2 \pmod 3$, o que seria impossível. Agora, suponhamos que a 6.23 admita uma solução com x e y ímpares. No entanto, analisando-a módulo 8 chagamos a uma impossibilidade, já que $px^2 \equiv 7 \pmod 8$ e $3Y^2 \equiv 3 \pmod 8$.

Para a equação 6.24, tome $q = 3$, assim temos, $px^2 - 3Y^2 = 8 \cdot 3^2 - 4p$. Mas, analisando a equação módulo $p - 2 \cdot 3^2$ obtemos

$$\left(\frac{p}{p - 2 \cdot 3^2}\right)\left(\frac{3}{p - 2 \cdot 3^2}\right) = \left(\frac{p - 2 \cdot 3^2}{p}\right)\left(\frac{p - 2 \cdot 3^2}{3}\right) = -1,$$

o que implica que a equação não possui solução inteira.

Caso 2. Suponhamos, agora, $p = 24k + 23$. Neste caso, temos a validade da equação $px^2 - 3Y^2 \equiv -8q^2 \pmod{4p}$ e de maneira análoga, tomando q, suficientemente pequeno, uma das equações deverá possuir solução, para inteiros x, y e q, com x e y de mesma paridade,

$$px^2 - 3(py - 2q)^2 = 8q^2 \tag{6.25}$$

$$px^2 - 3(py - 2q)^2 = 8q^2 - 4p. \tag{6.26}$$

Como no caso anterior, a equação 6.25 não possui solução inteiras. Para a equação 6.26, vamos dividir nossa análise em três casos de acordo com as possibilidades de $p \equiv n \pmod 9$, que no caso é $n = 2, 5, 8$.

(a) Para $n = 2$, tome $q = 1$. Vamos mostrar que nessas condições a equação 6.26 não possui solução. Como $p = 24k + 23$, $k > 0$, então $p - 2 \equiv 0 \pmod 3$, o que nos permitirá analisar a equação módulo $\frac{p-2}{3}$. Substituindo $q = 1$ na equação 6.26, observe que $px^2 - 3Y^2 = 8 - 4p = 4(2 - p) \equiv 0 \pmod{\frac{p-2}{3}}$. Assim temos

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

(b) Para $n = 5$, tome $q = 2$. Então, nessas condições, analisando a equação módulo $\frac{p-8}{3}$, obtemos a equação modular $px^2 - 3Y^2 \equiv 0 \pmod{\frac{p-8}{3}}$. No entanto, a equação modular não possui solução uma vez que

$$\left(\frac{p}{\frac{p-8}{3}}\right)\left(\frac{3}{\frac{p-8}{3}}\right) = -\left(\frac{\frac{p-8}{3}}{3}\right) = -1.$$

(c) Para $n = 8$, tome $q = 4$. Então, nessas condições basta mostrarmos que a equação $px^2 - 3Y^2 \equiv 0 \pmod{\frac{p-32}{3}}$ não possui solução. Para isso note que

$$\left(\frac{p}{\frac{p-32}{3}}\right)\left(\frac{3}{\frac{p-32}{3}}\right) = -\left(\frac{\frac{p-32}{3}}{3}\right) = -1.$$

Com isso finalizamos a demonstração do resultado. ■

Classificação de anéis quadráticos com discriminante $3q$ **onde** $q \equiv 3 \pmod 8$

Por fim, mostraremos que os únicos anéis quadráticos $\mathcal{O}_{3q}$ norma euclidianos com discriminante $q \equiv 3 \pmod 8$ são $\mathcal{O}_{33}$ e $\mathcal{O}_{57}$. Seguiremos a referência [13], também ressaltamos que essa abordagem será completamente elementar.

Proposição 6.46. *Seja $\mathcal{O}_{pq}$ um anel quadrático, onde p e q são primos. a fim de que $\mathcal{O}_{pq}$ seja norma euclidiano é necessário que para todo inteiro positivo $s < p$ satisfazendo uma equação da forma*

$$-qt^2 \equiv s \ (mod\ p),$$

uma das equações

$$px^2 - qY^2 = 4s \tag{6.27}$$

$$px^2 - qY^2 = 4s - 4p \tag{6.28}$$

tenha solução inteiras.

Demonstração: No item dois da observação 2.61 tome $a = 0$ e $b = \frac{t}{p}$, assim

$$|px^2 - qY^2| < 4p,$$

com x, Y inteiros, onde $Y = py - 2t$. Observando que $px^2 - qY^2 \equiv -4qt^2 \pmod p$ segue o resultado. ■

Lema 6.47. *Suponhamos que exista um inteiro positivo $s < p$ tal que s satisfaça a equação modular $-3t^2 \equiv s \pmod p$, para algum t, e que também possamos escrever s como $s = 3\sigma$, onde σ satisfaz:*

1. *$mdc(\sigma, 6p) = 1$;*
2. *$\left(\frac{\sigma}{3}\right) = 1$.*

Então o anel quadrático $\mathcal{O}_{3q}$ não é norma euclidiano.

Demonstração. É suficiente mostrarmos que as equações

$$px^2 - 3Y^2 = 4s = 4 \cdot 3\sigma, \tag{6.29}$$

$$px^2 - 3Y^2 = 4s - 4p = -4(p - 3\sigma) \tag{6.30}$$

não possuem soluções nas variáveis inteiras x, Y. Pela a hipótese

$$-3t^2 \equiv s = 3\sigma \ (mod\ p),$$

logo

$$\left(\frac{\sigma}{p}\right) = -1.$$

Por $\text{mdc}(\sigma, 6p) = 1$, qualquer solução da equação 6.29 deve satisfazer

$$\left(\frac{p}{\sigma}\right)\left(\frac{3}{\sigma}\right) = 1.$$

No entanto, isso não ocorre, pois,

$$\left(\frac{p}{\sigma}\right)\left(\frac{3}{\sigma}\right) = \left(\frac{\sigma}{p}\right)\left(\frac{\sigma}{3}\right) = (-1)(1) = (-1).$$

Portanto a equação 6.29 não tem solução. Já a equação 6.30 nunca possui solução, pois o lado esquerdo de 6.30 é congruente a px^2 módulo 3 e o lado direito congruente a $-4p$ módulo 3, o que implicaria, em caso de existência de uma solução, em

$$x^2 \equiv 2 \pmod 3.$$

Portanto, ambas equações não possuem solução. ■

As condições 1 e 2 no lema acima são equivalentes a $\sigma \equiv 1 \pmod 6$. Já as condições imposta sobre $s = 3\sigma$ podem ser resumidas a $\sigma < \frac{p}{3}$ e $\left(\frac{\sigma}{p}\right) = -1$.

Teorema 6.48. *Anéis quadráticos da forma $\mathcal{O}_{3q}$, onde p é um primo da forma $p = 8k+3$, não são norma euclidianos, exceto quando $p = 11$ ou 19.*

Demonstração. Para mostrarmos que o anel quadrático não é norma euclidiano basta exibirmos σ satisfazendo:

$$\sigma < \frac{p}{3}, \quad \sigma \equiv 1 \pmod 6, \quad \left(\frac{\sigma}{p}\right) = -1. \tag{6.31}$$

Demonstração. Vamos dividir a demonstração em dois casos: $p = 24k + 11$ e $p = 24k + 19$. Em ambos os casos $k \geq 1$. Se $p = 24k + 11$ então $p \equiv 5 \pmod 6$. Para $p > 108$ sempre existe um inteiro B tal que

$$\frac{7p}{36} < B < \frac{11p}{54},$$

pois

$$\frac{11p}{54} - \frac{7p}{36} > 1.$$

Além disso

$$0 < 6B - p, \ 36B - 7p < \frac{p}{3}$$

e $6B - p,\ 36B - 7p \equiv 1 \pmod 6$. Observamos também que entre $6B - p$ e $36B - 7p$ pelo menos um deles não é resíduo quadrático $\pmod p$, uma vez que se ambos fossem, 6 também seria um resíduo quadrático módulo p o que é impossível, uma vez que p é um primo da forma $24k + 11$. Dessa forma, se $p > 108$, então o algoritmo euclidiano não é válido, já que existiria um σ satisfazendo as condições 6.31.

Resta verificarmos o caso $p < 108$, isto é, $p = 59,\ 83,\ 107$. Para estes casos tome $\sigma = 13, 13, 7$, respectivamente. Em cada caso σ satisfaz as condições 6.31.

Caso $p = 24k + 19$, então $p \equiv 5 \pmod 6$. Se $p > 108$, tome um inteiro C tal que

$$\frac{5p}{36} < C < \frac{4p}{27}.$$

Logo

$$p - 6C,\ 36C - 5p \equiv 1 \pmod 6$$

e

$$0 < p - 6C,\ 36C - 5p < \frac{p}{3}.$$

Além disso $p - 6C$ e $36C - 5p$ não podem ser simultaneamente resíduos quadráticos $\pmod p$, uma vez que nesse caso -6 seria resíduo quadrático módulo p e portanto p não poderia ser da forma $24k+19$, como no casos anterior o algoritmo euclidiano não é válido. Por fim resta verificar os casos $p = 43, 67$. Em ambos os casos tome $\sigma = 7$ e aplique o lema. ■

6.3 Classificação de anéis quadráticos com discriminante primo $p \equiv 1 \pmod 4$

Nesta seção, abordaremos a classificação dos anéis quadráticos $\mathcal{O}_p$ em que p é um primo congruente a 1 módulo 4. Dividiremos a demonstração de acordo com as possibilidades da classe de p módulo 24, ou seja, $p \equiv 1, 5, 13$ ou $17 \pmod{24}$. Na Subseção 6.3.1 lidaremos com o caso $p \equiv 5 \pmod{24}$. Na Subseção 6.3.2, nos encarregaremos do caso $p \equiv 13 \pmod{24}$, onde aplicaremos uma estratégia computacional, com exceção dos casos $p = 61$ e $p = 109$, para os quais desenvolveremos uma outra abordagem para lidarmos com suas classificações. Na Subseção 6.3.3 trataremos do caso $p \equiv 17 \pmod{24}$, onde utilizaremos resultados semelhantes ao da Subseção 6.3.2. Por fim, na Subseção 6.3.4 faremos a classificação dos corpos com o caso $p \equiv 1 \pmod{24}$. A maior parte dos casos em que $p \equiv 1 \pmod{24}$, a abordagem seguirá uma estratégia semelhante à utilizada no caso $p \equiv 13 \pmod{24}$, as exceções são os casos $p = 97,\ 193,\ 241,\ 313,\ 337,\ 457$ e 601. Para o caso $p = 97$, mostraremos a existência de um par ordenado racional (x_0, y_0) tal que $M(N_{97}; x_0, y_0) \geq 1$. Para os casos $p = 193,\ 241,\ 313,\ 337,\ 457$ e 601 faremos uma adaptação da teoria desenvolvida no Capítulo 5 a fim de classificar seu respectivos corpos quadráticos.

Dessa forma ao final desta seção teremos demonstrado

Teorema 6.49. *Um anel quadrático com discriminante p primo congruente módulo 1 módulo 4 é norma euclidiano apenas quando* $p = 5, 13, 17, 29, 41$ *ou* 73.

6.3.1 Classificação de anéis quadráticos com discriminante $p \equiv 5 \pmod{24}$

Lema 6.50. *Seja $\mathcal{O}_p$ um anel quadrático norma euclidiano, com $p \equiv 5 \pmod{24}$. Então para todo inteiro s tal que $0 < s < \frac{p}{2}$, $(s, 3p) = 1$ e $s \equiv 1 \pmod 4$, vale $\left(\frac{s}{p}\right) = 1$.*

Demonstração: Seja um número inteiro s tal que $0 < s < \frac{p}{2}$, $(s, 3p) = 1$ e $s \equiv 1 \pmod 4$. Então, para s, temos que $3s - p \equiv 2 \pmod 4$. Como $\left(\frac{p}{2}\right) = -1$, então $\left(\frac{p}{3s-p}\right)^* \neq 1$; da mesma forma, $\left(\frac{p}{3s}\right)^* \neq 1$, devido a $\left(\frac{p}{3}\right) = -1$. Pela contra positiva do primeiro item do Lema 6.16 aplicado a $r = 3s$, segue que $\left(\frac{3s}{p}\right)^* \neq 1$. Portanto, temos $\left(\frac{3s}{p}\right) = -1$, ou seja, $\left(\frac{s}{p}\right) = 1$. ■

Teorema 6.51. *Seja $\mathcal{O}_p$, onde p é primo $\equiv 5 \pmod{24}$, um anel quadrático. Então $\mathcal{O}_p$ é norma euclidiano apenas quando $p = 5$ ou $p = 29$.*

Demonstração: Suponha então que $p \equiv 5 \pmod{24}$ e $\mathcal{O}_p$ seja um anel quadrático norma euclidiano. Inicialmente vamos utilizar o lema anterior para demostrar que não há anéis quadráticos quando $p > 432$. Sendo $p > 432$, existe um número inteiro A tal que

$$\frac{2p - 36}{432} < A < \frac{2p - 36}{432} + \frac{p}{432}.$$

Defina $s_1 = 12A + 1$ e $s_2 = p - 144A - 12$. Então, $0 < s_1,\ s_2 < \frac{p}{3}$, $3 \nmid s_1, s_2$ e $s_1, s_2 \equiv 1 \pmod 4$. Ambos os números $s_1,\ s_2$ satisfazem as hipóteses impostas sobre s no lema anterior e, assim, devido a $s_2 = p - 12s_1$ e $\left(\frac{3}{p}\right) = -1$:

$$\left(\frac{s_2}{p}\right) = -\left(\frac{s_1}{p}\right),$$

portanto, um dos s_i contradiz o lema anterior.

Assim, restam apenas os primos $p = 5, 29, 101, 149, 269, 389$ a serem verificados. Desses, os quatro últimos são excluídos em decorrência do lema anterior e devido a $\left(\frac{29}{101}\right) = \left(\frac{13}{149}\right) = \left(\frac{29}{269}\right) = \left(\frac{29}{389}\right) = -1$. No entanto, para $p = 5$ e $p = 29$, o anel quadrático $\mathcal{O}_p$ é norma euclidiano. Portanto, o teorema está provado. ■

6.3.2 Classificação de anéis quadráticos com discriminante $p \equiv 13 \pmod{24}$

Diante da finitude de corpos quadráticos, cujo discriminante é limitado superiormente por um valor relativamente baixo, menor que $(128)^2$, podemos sempre levar em consideração uma abordagem manual, isto é, deixando de lado teorias e resultados mais elaborados, que podem ser aplicados a múltiplos casos simultaneamente, para nos concentrarmos à uma abordagem mais simples, focada na verificação individual de cada caso. Com isso em mente introduziremos alguns resultados que nos permitirão ter esse tipo de abordagem. O primeiro teorema desta subseção é particularmente útil no decorrer do restante trabalho, no tratamento dos casos $\mathcal{O}_p$, onde p é um primo congruente a 1 ou 17 módulo 24. No entanto, essa abordagem não é suficiente para lidarmos com todos os casos desta subseção, em particular, o método falha na classificação dos anéis quadráticos $\mathcal{O}_{61}$ e $\mathcal{O}_{109}$, para os quais recorreremos a uma outra abordagem. A primeira parte desta subseção é baseada na referência [15]. Já a teoria desenvolvida para classificar os anéis quadráticos $\mathcal{O}_{61}$ e $\mathcal{O}_{109}$ é baseada na referência [18].

Teorema 6.52. *Para um primo p da forma $4k+1$, o algoritmo de Euclides não pode existir em $\mathcal{O}_p$, se p pode ser escrito na forma*

$$p = q_1 m_1 + q_2 m_2,$$

onde m_1, m_2, q_1, q_2 são inteiros positivos e resíduos não quadráticos módulo p, e onde q_i é um primo ímpar cujo expoente de sua maior potência que divide $q_i m_i$ é ímpar, com $i = 1, 2$.

Demonstração: Relembramos que, para que $\mathcal{O}_p$ seja norma euclidiano, é necessário e suficiente que a inequação tenha solução em inteiros x, y

$$|(x-2r)^2 - p(y-2s)^2| < 4,$$

para quaisquer racionais r, s. Dado que q_1 e m_1 são resíduos não quadráticos módulo p, $q_1 m_1$ é um resíduo quadrático módulo p e a equação

$$z^2 \equiv q_1 m_1 \pmod p$$

possui solução, digamos, z_1. Tomando $r = 0$ e $s = \frac{z_1}{p}$, obtemos

$$|px^2 - (py - 2z_1)^2| < 4p.$$

Uma vez que o lado esquerdo da desigualdade é congruente à $4z_1$, então, umas das seguintes equações deve possuir solução

$$px^2 - (py - 2z_1)^2 = -4q_1 m_1, \tag{6.32}$$

$$px^2 - (py - 2z_1)^2 = 4p - 4q_1 m_1 = 4q_2 m_2. \tag{6.33}$$

Vamos demonstrar que a equação 6.32 não possui solução. Suponhamos $x \equiv 0 \pmod{q_1}$. Neste caso, também ocorre $(py - 2z)^2 \equiv 0 \pmod{q_1}$ e assim para a maior potência p^m de p, que divide o lado esquerdo da equação 6.32, tem-se m um inteiro par. No entanto, por hipótese, o expoente da maior potência que divide o lado direito da equação 6.32 é um número ímpar, o que impossibilita a igualdade. Se $x \not\equiv 0 \pmod{q_1}$, então, segue a partir da equação 6.32, que px^2 é um resíduo quadrático módulo q_1. Mas isso é impossível, pois

$$\left(\frac{p}{q_1}\right) = \left(\frac{q_1}{p}\right) = -1.$$

Portanto, a equação 6.32 é impossível. Da mesma forma a equação 6.33 não possui solução, o que demonstra o resultado ■

Teorema 6.53. *Seja p um primo da forma $24n + 13$ e sejam u e v os dois menores resíduos não quadráticos ímpares módulo p, que por sua vez também são primos. Se*

$$3uv < p, \tag{6.34}$$

então o algoritmo de Euclides não existe em $\mathcal{O}_p$.

Demonstração: Escreva

$$p = 3uv + 2b_1 \tag{6.35}$$

e

$$p = uv + 2b_2, \tag{6.36}$$

onde, devido a 6.34, b_1 e b_2 são inteiros positivos. Para primos da forma $24n+13$, sabemos que o número 2 é um resíduo não quadrático e o número 3 é um resíduo quadrático. A partir da igualdade 6.35, segue que

$$\left(\frac{2b_1}{p}\right) = \left(\frac{-3uv}{p}\right) = \left(\frac{uv}{p}\right) = 1.$$

Dessa forma, chegamos à conclusão que b_1 é um resíduo não quadrático módulo p. De maneira análoga, a partir da igualdade 6.36, podemos concluir que b_2 também é um resíduo não quadrático módulo p. Além disso, das igualdades 6.35 e 6.36, podemos deduzir

$$p = 3b_2 - b_1.$$

Portanto, podemos concluir que b_1 ou b_2 deve ser um número ímpar. Vamos considerar primeiro o caso em que b_1 é ímpar. Como b_1 é um resíduo não quadrático módulo p, então deve existir um divisor primo q de b_1, cujo expoente da maior potência que divide b_1 é um número ímpar. Também, pela igualdade 6.35, podemos concluir que q é diferente de u e v, já que, p é primo e $u, v < p$. Utilizando as notações do Teorema 6.52, escreva

$$q_1 = u,\ m_1 = 3v,\ q_2 = q,\ m_2 = 2\frac{b_1}{q}.$$

Assim, a igualdade 6.35 nos leva às condições do Teorema 6.52, o que implica a não existência do algoritmo em $\mathcal{O}_p$ sob essas condições. Se, por outro lado, b_2 é ímpar, como b_2 também não é um resíduo quadrático módulo p, então deve existir um primo ímpar q' que não é um resíduo quadrático módulo p cujo expoente da maior potência que divide b_2 é um número ímpar. Seguindo a notação do Teorema 6.52, escreva

$$q_1 = u,\ m_1 = v,\ q_2 = q',\ m_2 = 2\frac{b_2}{q'},$$

donde, pelo Teorema 6.52, segue que $\mathcal{O}_p$ não é norma euclidiano. ■

Lema 6.54. *Se p é um primo da forma $8n + 5$, então o menor resíduo não quadrático ímpar u módulo p satisfaz*

$$u < \sqrt{p+4} + 2$$

Demonstração: Veja [16], Teorema 2.

Teorema 6.55. *Seja p um número primo da forma $24n + 13$. Sejam u, v os dois menores resíduos não quadráticos ímpares módulo p, que também são números primos. Se a condição*

$$8u < v, \tag{6.37}$$

for satisfeita, então o algoritmo de Euclides não exite em $\mathcal{O}_p$.

Demonstração: Dado que a desigualdade 6.37 não é verdadeira para os valores $p = 13, 37$ e 61, podemos assumir $p \geq 109$. Sabendo que u é o menor resíduo não quadrático módulo p, de acordo com o lema anterior, podemos estabelecer a relação

$$u < \sqrt{p+4} + 2. \tag{6.38}$$

Portanto, para $p > 96$, podemos afirmar que

$$p - 8u > p - 8\sqrt{p+4} - 16 > 0, \tag{6.39}$$

uma vez que temos

$$(p-16)^2 = p^2 - 32p + 256 > 64p + 256.$$

Agora, considere $2ku$ como o maior múltiplo de $2u$ que seja menor que p. Os oito números seguintes

$$2(k-3)u,\ 2(k-2)u,\ 2(k-1)u,\ 2ku,\ 2(k+1)u,\ 2(k+2)u,\ 2(k+1)u,\ 2(k+4)u \tag{6.40}$$

pertencem ao intervalo $[p - 8u,\ p + 8u]$ e são inteiros positivos, conforme a desigualdade 6.39. Esses números também formam uma progressão aritmética com razão $2u$, e, portanto, existem exatamente dois elementos nesse conjunto que são divisíveis por 4 mas não por 8. Além disso, a diferença entre os dois números deve ser igual a $8u$. Logo, pelo menos um desses dois números, digamos, $4lu$, onde l é um inteiro ímpar, não é divisível por u^2, pois caso contrário u^2 dividiria a diferença entre os números, que por sua vez é $8u$, o que implicaria em uma contradição, já que u é um primo ímpar. Então

$$(l, 2u) = 1. \tag{6.41}$$

Além disso, como $4lu$ é um dos números do conjunto 6.40, temos

$$p - 8u < 4lu < p + 8u, \tag{6.42}$$

ou seja,

$$|p - 4lu| < 8u. \tag{6.43}$$

Portanto, $|p-4lu|$ é um inteiro ímpar que é menor que $8u$ e, de acordo com a desigualdade 6.37, também é menor que v. Como $|p - 4lu|$ não é divisível por u, e todos os inteiros ímpares menores que v que não são divisíveis por u são resíduos quadráticos módulo p, assim podemos concluir que $|p-4lu|$ é de fato um resíduo quadrático módulo p. Portanto, lu também é um resíduo quadrático módulo p e, como resultado, l é um resíduo não quadrático módulo p. Por 6.41, l e $2u$ são inteiros coprimos, logo, deve existir um divisor primo w de l que é diferente de u e que é um resíduo não quadrático módulo p. Seguindo a construção, podemos afirmar que $v \leq w$, e, conforme a desigualdade 6.42,

$$4uv \leq 4uw \leq 4lu < p + 8u,$$

$$3uv + uv < p + 8u,$$

$$3uv + u(v-8) < p.$$

Portanto, por 6.37, $3uv < p$. Com isso, utilizando o Teorema 6.53, podemos concluir o resultado. ■

Teorema 6.56. *Se o menor resíduo não quadrático ímpar u módulo um primo p da forma $24k + 13$ satisfaz a condição $24u^2 < p$, então o algoritmo de Euclides não exite em $\mathcal{O}_p$.*

Demonstração: Suponhamos que os inteiros ímpares u e v sejam os menores resíduos não quadráticos módulo p e assuma $u < v$. Se $8u < v$, o resultado segue do Teorema 6.55. Se, entretanto, $v < 8u$, então

$$3uv < 24u^2 < p$$

e assim o resultado segue diretamente do Teorema 6.53. ■

Teorema 6.57. *Não existe anéis quadráticos $\mathcal{O}_p$ que são norma euclidianos quando p é um primo da forma $24n + 13$ e $p > 109$.*

Demonstração: Devido ao Teorema 5.22, estamos interessados em investigar apenas os anéis quadráticos com discriminante menor que 128^2. A maior parte dos casos podem ser investigados utilizando o Teorema 6.56. A partir do teorema podemos dar os seguintes critérios:

- Se 5 não é um resíduo quadrático módulo p e $24 \cdot 5^2 = 600 < p$, então $\mathcal{O}_p$ não é norma euclidiano;
- Se 7 não é um resíduo quadrático módulo p e $1176 < p$, então $\mathcal{O}_p$ não é norma euclidiano;
- Se 11 não é um resíduo quadrático módulo p e $2904 < p$, então $\mathcal{O}_p$ não é norma euclidiano;
- Se 13 não é um resíduo quadrático módulo p e $4056 < p$, então $\mathcal{O}_p$ não é norma euclidiano;
- Se 17 não é um resíduo quadrático módulo p e $6936 < p$, então $\mathcal{O}_p$ não é norma euclidiano;
- Se 19 não é um resíduo quadrático módulo p e $8664 < p$, então $\mathcal{O}_p$ não é norma euclidiano;
- Se 23 não é um resíduo quadrático módulo p e $10584 < p$, então $\mathcal{O}_p$ não é norma euclidiano.

Utilizando os critérios, podemos concluir que na maior parte dos casos o algoritmo euclidiano não é válido, exceto para os anéis com discriminante: 13, 37, 61, 109, 157, 181, 229, 277, 349, 373, 397, 421, 541, 661, 709, 829, 1021, 1069, 1381, 1429, 1549, 1621, 1789, 2221, 2269, 2389, 3061, 3301, 3469, 5581, 6301, 6829, 7309, 8941, 13381.

Para 13 e 17 o algoritmo é válido. Para 61 e 109 ainda não podemos responder. Já para os demais casos a resposta é negativa. Podemos provar a afirmação utilizando os Teoremas 6.53 e 6.52. Inicialmente utilizaremos apenas o Teorema 6.53. Procederemos como se segue: Para 157, Os dois menores resíduos não quadráticos ímpares módulo 157 são 5 e 7 e como $3 \cdot 5 \cdot 7 < 157$, pelo Teorema 6.53, $\mathcal{O}_p$ não é norma euclidiano. Os seguintes casos seguem analogamente:

- 277: $3 \cdot 5 \cdot 11 < 277$;
- 349: $3 \cdot 7 \cdot 11 < 349$;
- 373: $3 \cdot 5 \cdot 11 < 373$;
- 397: $3 \cdot 5 \cdot 7 < 379$;

- 421: $3 \cdot 13 \cdot 19 > 379$;
- 541: $3 \cdot 11 \cdot 13 < 541$;
- 661: $3 \cdot 7 \cdot 13 < 661$;
- 709: $3 \cdot 13 \cdot 17 < 709$;
- 829: $3 \cdot 7 \cdot 19 < 829$;
- 1021: $3 \cdot 7 \cdot 13 < 1021$;
- 1069: $3 \cdot 7 \cdot 11 < 1061$;
- 1381: $3 \cdot 11 \cdot 19 < 1381$;
- 1429: $3 \cdot 11 \cdot 29 < 1429$;
- 1549: $3 \cdot 13 \cdot 19 < 1549$;
- 1621: $3 \cdot 17 \cdot 23 < 1621$;
- 1789: $3 \cdot 11 \cdot 13 < 1789$;
- 2221: $3 \cdot 11 \cdot 13 < 2221$;
- 2269: $3 \cdot 11 \cdot 19 < 2269$;
- 2389: $3 \cdot 11 \cdot 19 < 2389$;
- 3061: $3 \cdot 13 \cdot 19 < 3061$;
- 3301: $3 \cdot 17 \cdot 19 < 3301$;
- 3469: $3 \cdot 13 \cdot 23 < 3469$;
- 5581: $3 \cdot 17 \cdot 19 < 5581$;
- 6301: $3 \cdot 17 \cdot 19 < 6301$;
- 6829: $3 \cdot 17 \cdot 19 < 6829$;
- 7309: $3 \cdot 19 \cdot 31 < 7309$;
- 8941: $3 \cdot 23 \cdot 37 < 8941$;
- 13381: $3 \cdot 29 \cdot 37 < 13381$.

Os casos 181, 229 e 421 podem ser analisados utilizando o Teorema 6.52:

- $181 = 7 \cdot 17 + 2 \cdot 31$;
- $229 = 7 \cdot 13 + 6 \cdot 23$;
- $421 = 13 \cdot 19 + 6 \cdot 23$; ■

Contudo, há ainda dois casos sem resposta, os anéis quadráticos com discriminante $p = 61$ ou $p = 109$. Posteriormente demonstraremos que $\mathcal{O}_{61}$ e $\mathcal{O}_{109}$ não são norma euclidianos e assim ao final desta subseção teremos demonstrado o seguinte teorema

Teorema 6.58. *Um anel quadrático com discriminante $p \equiv 13 \pmod{24}$ é norma euclidiano apenas quando $p = 13$ ou $p = 37$.*

Os anéis quadráticos $\mathcal{O}_{61}$ e $\mathcal{O}_{109}$ não são norma euclidianos.

Agora, introduziremos o método desenvolvido por L. Rédei, em [18], a fim de demonstrar que os anéis quadráticos $\mathcal{O}_{61}$ e $\mathcal{O}_{109}$ não são norma euclidiano.

Para um μ fixo, $\bar{\mu}$ deve sempre representar um elemento em $\mathcal{O}_p$ tal que $|N(\bar{\mu})| < |N(\mu)|$. Sob a hipótese de $\mathcal{O}_p$ ser norma euclidiano, para todo α em $\mathcal{O}_p$, existe um $\bar{\mu}$ satisfazendo a congruência

$$\alpha \equiv \bar{\mu} \pmod{\mu}.$$

Portanto, podemos derivar uma equivalência para que $\mathcal{O}_p$ seja norma euclidiano:

Lema 6.59. *Em $\mathcal{O}_p$, o algoritmo de Euclides existe se, e somente se, para todo $\mu \neq 0$ em $\mathcal{O}_p$, as classes de resíduos $\bar{\mu} \pmod{\mu}$, com $|N(\bar{\mu})| < |N(\mu)|$, contiverem todos os elementos de $\mathcal{O}_p$.*

Definição 6.60. Se μ satisfaz a condição acima, dizemos que é um módulo euclidiano. Caso contrário dizemos que μ é um módulo não euclidiano.

Como as unidades em $\mathcal{O}_p$ não são módulos não euclidianos, vamos assumir daqui em diante que μ é diferente de zero e diferente de uma unidade.

A presença de um módulo não euclidiano é característica da ausência do algoritmo de Euclides. Diante disso, o foco dos resultados da seção será o desenvolvimento de resultados que nos permitirão encontrar um módulo não euclidiano. Veremos que a partir de determinadas condições uma boa escolha para um módulo não euclidiano será $\epsilon + 1$.

Claramente, o seguinte se aplica:

Lema 6.61. *Se μ for um módulo não euclidiano, o mesmo se aplica ao seu conjugado e a todos os seus associados e múltiplos.*

Com um μ fixo, há sempre infinitos $\bar{\mu}$, já que todos os associados surgem simultaneamente como um $\bar{\mu}$. No entanto, ao selecionar deles um sistema máximo de elementos não associados $\bar{\mu_1}, \bar{\mu_2}, \ldots, \bar{\mu_M}$, todos os $\bar{\mu}$ são representados por $\eta\bar{\mu_j}$ (η unidade em $\mathcal{O}_p$). Agora, definamos:

Definição 6.62. O menor número natural $\{\mu\}$ tal que $\mu \mid (\epsilon^{\{\mu\}} + \sigma)$, $\sigma = \pm 1$, é chamado de índice de μ.

Seguindo com o raciocínio anterior, diante da definição de $\{\mu\}$, todos os resíduos $\bar{\mu} \pmod \mu$ estão entre os resíduos $\pm\epsilon^i\bar{\mu_j} \pmod \mu$ ($i = 0, 1, \ldots, \{\mu\} - 1;\ j = 1, 2, \ldots, M$). Assim, se queremos encontrar um módulo não euclidiano μ, parece vantajoso ter um índice pequeno $\{\mu\}$, especialmente quando $\{\mu\} = 1$. Portanto, uma escolha imediata para μ seria $\mu = \epsilon \pm 1$. A partir de agora, desenvolveremos resultados com o intuito de encontramos condições para que μ não seja um módulo euclidiano.

Definição 6.63. Para $\omega \in \mathbb{Q}(\sqrt{p})$, definimos $||\omega||$ como o maior número entre $|\omega|$ e $|\omega'|$.

Lema 6.64. *Para qualquer μ, em cada classe de resíduos $\bar{\mu} \pmod \mu$, existe um $\bar{\mu}$ para o qual $||\bar{\mu}|| \leq \sqrt{\epsilon^{\{\mu\}}|N(\bar{\mu})|}$, e portanto $||\bar{\mu}|| \leq \sqrt{\epsilon^{\{\mu\}}|N(\mu)|}$.*

Demonstração: Iniciamos definindo $\eta = \epsilon^{\{\mu\}}$. Então, pela definição, $\mu \mid (\eta + \sigma)$, onde $\sigma = \pm 1$. Consideremos uma classe de resíduos arbitrários $\bar{\mu} \pmod \mu$ e suponhamos que $||\bar{\mu}||$ seja menor possível entre os elementos dessa classe. Como $-\sigma\eta\bar{\mu} = \sigma(\eta+\sigma)\bar{\mu}+\bar{\mu} \equiv \bar{\mu} \pmod \mu$ e $-\sigma\eta^{-1}\bar{\mu} \equiv (\sigma + \eta)\eta^{-1}\bar{\mu} + \bar{\mu} \equiv \bar{\mu} \pmod \mu$, temos:

$$||\eta\bar{\mu}|| \geq ||\bar{\mu}|| \tag{6.44}$$

$$||\eta^{-1}\bar{\mu}|| \geq ||\bar{\mu}|| \tag{6.45}$$

Primeiramente, suponhamos $||\bar{\mu}|| = |\bar{\mu}|$. Inicialmente observamos que $\eta = \epsilon^{\{\mu\}} > 1$ então, naturalmente, $|\eta^{-1}\bar{\mu}| < |\bar{\mu}|$, isso juntamente com a desigualdade 6.45 implica em $|(\eta^{-1}\bar{\mu})'| \geq |\bar{\mu}|$, que por sua vez, observando $\eta\eta' = \pm 1$, implica em

$$|\eta\bar{\mu'}| \geq |\bar{\mu}|.$$

Multiplicando a última igualdade por $|\bar{\mu}|$ obtemos

$$|\eta N(\bar{\mu})| \geq |\bar{\mu}|^2 = ||\bar{\mu}||^2.$$

Agora, suponha $||\bar{\mu}|| = |\bar{\mu'}|$, novamente, por $\eta > 1$, temos $|\eta^{-1}\bar{\mu'}| < |\bar{\mu'}|$. Como

$$|\eta^{-1}\bar{\mu'}| = |\eta^{-1}\eta\eta'\bar{\mu'}| = |\eta'\bar{\mu'}|,$$

segue que

$$|\eta'\bar{\mu}'| = |(\eta\bar{\mu})'| = |\bar{\mu}'|.$$

Então, pela desigualdade 6.44 deve ocorrer $|(\eta\bar{\mu})| \geq |\bar{\mu}'|$. Multiplicando $|\bar{\mu}'|$ na desigualdade, obtemos

$$|\eta N(\bar{\mu})| \geq |\bar{\mu}'|^2 = ||\bar{\mu}||^2.$$

Assim, demonstramos o lema. ■

Lema 6.65. *Seja $\mathcal{O}_p$ um anel quadrático norma euclidiano, onde p é um primo* $\equiv 1 \pmod 4$*. Então, para*

$$\mu = \epsilon + 1,$$

em cada classe de resíduos $\bar{\mu} \pmod{\epsilon+1}$, existe um representante $\bar{\mu}$ tal que

$$\bar{\mu} = \frac{x + y\sqrt{p}}{2}, \text{ com } x \equiv y \pmod 2 \tag{6.46}$$

$$|x^2 - py^2| < 8t, \tag{6.47}$$

$$|x| \leq 2t + 1, \ |y| \leq 2u. \tag{6.48}$$

Demonstração: Inicialmente observe que

$$N(\epsilon + 1) = 2t. \tag{6.49}$$

Pela propriedade euclidiana, para cada classe de resíduos, sempre podemos tomar um $\bar{\mu}$, na forma 6.46, satisfazendo $|N(\bar{\mu})| < |N(\epsilon + 1)|$. Dessa forma, pela observação inicial, a condição 6.47 também é satisfeita. De acordo com o Lema 6.64 e a observação inicial, podemos ainda nos restringirmos a escolha de um $\bar{\mu}$ satisfazendo $||\bar{\mu}|| < \sqrt{2t\epsilon}$. Como

$$2t < \epsilon < 2u\sqrt{p}, \tag{6.50}$$

segue-se que

$$||\bar{\mu}|| < \epsilon \tag{6.51}$$

Agora, mostraremos que as desigualdade em 6.48 são uma consequência de 6.46, 6.47 e 6.51. Considerando o caso em que $x \geq 0, y \geq 0$, os demais casos seguirão de maneira análoga. A partir de 6.46 e 6.51, temos $x < 2\epsilon - y\sqrt{p}$. Ao elevar ao quadrado, obtemos $4y\epsilon\sqrt{p} < 4\epsilon^2 - (x^2 - py^2)$, assim, por 6.47, obtemos a desigualdade $y\epsilon\sqrt{p} < \epsilon^2 - 2t$ e, pela desigualdade 6.50, $y\epsilon\sqrt{p} < 2u\epsilon\sqrt{p} + \epsilon$, ou seja, $y < 2u + \frac{1}{\sqrt{p}}$. Como y é um número inteiro, então a segunda desigualdade em 6.48 é verdadeira. Se a primeira desigualdade fosse falsa, então teríamos $x^2 - py^2 \geq (2t+2)^2 - p(2u)^2 = 8t$, o que é impossível de acordo com 6.47. Isso prova o resultado. ■

Resultados mais interessante surgem quando impomos a condição $u \geq \frac{3}{2}$.

Lema 6.66. *No lema anterior, se $u \geq \frac{3}{2}$ podemos substituir 6.48 por*

$$|x| < 2t, \ |y| < 2u. \tag{6.52}$$

Demonstração: Se $|y| = 2u$, então de acordo com a escolha de $\bar{\mu}$ em 6.46, $|x| \neq 2t \pm 1$. Além disso, $|x| = 2t$ pode ser excluído, pois, de acordo com 6.49, teríamos

$$\bar{\mu} = \pm t \pm u\sqrt{p} \equiv \pm t \pm (t+1) \equiv \pm 1 \pmod{\epsilon + 1},$$

e essas classes residuais já são representadas por $\bar{\mu} = \pm 1$. Levando em consideração 6.48, resta-nos apenas as possibilidades $|x| \leq 2t - 2$. Neste caso teríamos

$$x^2 - py^2 \leq (2t-2)^2 - p(2u)^2 = -8t,$$

o que contradiz 6.47. Portanto, y deve satisfazer a segunda desigualdade em 6.52. Se x não satisfizesse a primeira desigualdade em 6.52, teríamos

$$x^2 - py^2 \geq (2t)^2 - p(2u-1)^2 = 4pu - p - 4,$$

então, de acordo com a desigualdade 6.47, $4pu - p - 4 < 8t$ e, conforme a desigualdade 6.50, $pu - p - 4 < 8u\sqrt{p}$. Como $u \geq \frac{3}{2}$, isso resultaria em $5p - 4 < 12\sqrt{p}$. Essa contradição comprova o resultado. ■

Definição 6.67. Seja $\mathbb{Q}(\sqrt{d})$ um corpo quadrático e seja $\alpha = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$. Denotamos a primeira e segunda coordenadas de α como $(\alpha)_1 = a$ e $(\alpha)_2 = b$, respectivamente.

O próximo lema que nos permitirá demonstrar que em $\mathcal{O}_{61}$ e $\mathcal{O}_{109}$ o número $\mu = \epsilon + 1$ não é um módulo euclidiano, onde ϵ é a unidade fundamental do respectivo anel quadrático.

Lema 6.68. *Seja $\mathcal{O}_p$ um anel quadrático norma euclidiano, com p primo $\equiv 1 \pmod 4$, e com unidade fundamental ϵ cuja segunda coordena satisfaz $u \geq \frac{3}{2}$. Então, para todo α em $\mathcal{O}_p$, é possível determinar ω em $\mathcal{O}_p$ de modo que as seguintes condições se aplicam:*

$$|(\alpha + (\epsilon+1)\omega)_1| < t, \tag{6.53}$$

$$|(\alpha + (\epsilon+1)\omega)_2| < u, \tag{6.54}$$

$$|N(\alpha + (\epsilon+1)\omega)| < 2t. \tag{6.55}$$

Demonstração: Do Lema 6.59 aplicado a $\mu = \epsilon + 1$, segue que existe um $\bar{\mu}$ tal que $\bar{\mu} \equiv \alpha \pmod{\epsilon + 1}$. Devido à suposição $u \geq \frac{3}{2}$, pelo Lema 6.66, obtemos o Lema 6.68. ■

Para aplicações posteriores, observamos o seguinte:

Lema 6.69. *Se α é racional, então 6.55 se torna*

$$|\alpha^2 + 2\alpha((\epsilon+1)\omega)_1 + 2tN(\omega)| < 2t \tag{6.56}$$

e se 6.53 também for válida, então

$$|N(\omega)| < |\alpha| + 1 + \frac{\alpha^2}{2t}, \tag{6.57}$$

até mesmo quando α e ω não são inteiros.

Também para a aplicações do Lema 6.68 aos casos $\mathcal{O}_{61}$ e $\mathcal{O}_{109}$ precisaremos do seguinte lema

Lema 6.70. *Seja $\mathcal{O}_p$ um anel quadrático norma euclidiano, onde p primo $\equiv 1 \pmod 4$, cuja unidade fundamental $\epsilon = t + u\sqrt{p}$ possui coordenadas positivas maiores que 1. Dado $m \in \mathbb{Z}_+$, considere*

$$S = \{\alpha \in \mathcal{O}_d : \ |N(\alpha)| = m\},$$

então, a menos de sinal, existe no máximo um único $\beta \in S$ em que pelo menos uma das desigualdades

$$|((\epsilon+1)\beta)_2| < \frac{t-1}{2}, \tag{6.58}$$

$$|((\epsilon+1)\epsilon'\beta')_2| < \frac{t-1}{2}, \tag{6.59}$$

seja verdadeira. Se S for especialmente o conjunto de todas as unidades, então 6.59 e 6.59 só valem quando $|\beta| = 1$, e portanto

$$|(\epsilon+1)_2| = |((\epsilon+1)\epsilon')_2| = u. \tag{6.60}$$

Além disso, podemos concluir que se β for associado a um racional (inteiro) α, então

$$|((\epsilon+1)\beta)_2| = |((\epsilon+1)\epsilon'\beta')_2| = |\alpha|u, \tag{6.61}$$

assim sendo, neste caso, a existência do representante β é condicionada ao módulo de α.

Demonstração: Iniciamos mostrando que

$$|((\epsilon+1)\epsilon^n)_2| < \frac{t-1}{2}$$

não ocorre, para todo $n \in \mathbb{Z} \setminus \{-1, 0\}$. Se n é positivo, como as coordenadas de ϵ são maiores que 1 segue o resultado. Se $-n$ é negativo, então,

$$|((\epsilon+1)\epsilon^{-n})_2| = |(\epsilon^{-n+1} + \epsilon^{-n})_2| = |(\epsilon'^{n-1} - \epsilon'^{n})_2| = |(\epsilon^n - \epsilon^{n-1})_2| = |(\epsilon^{n-1}(\epsilon-1))_2|$$

Como $\epsilon(\epsilon-1) = t^2 + u^2p - t + (2t-1)u$, a partir disso, observando que $\epsilon^{n-1}(\epsilon-1)$ terá sempre coordenadas positivas, segue que para todo $n \geq 2$,

$$|((\epsilon+1)\epsilon^{-n})_2| = |(\epsilon^{n-1}(\epsilon-1))_2| \geq \frac{t-1}{2}.$$

Assim, podemos derivar as afirmações de quando S consistir das unidades ou dos associados de um número racional (inteiro). A partir de agora, dispensaremos essas possibilidades para S.

Para a situação em que β não é associado a uma unidade nem a um racional, considere os números a_n e b_n satisfazendo

$$(\epsilon+1)\epsilon'^n = a_n + b_n(\epsilon+1),\ n = 0, 1, 2, \ldots. \tag{6.62}$$

Vamos mostrar que a_n e b_n são inteiros que satisfazem

$$a_1 = 2t, b_1 = 1, \tag{6.63}$$

$$\left(2t + 1 + \frac{1}{t}\right) b_n - 1 + \frac{1}{t} \geq a_n > (2t+1)b_n > 0,\ n = 2, 3, \ldots. \tag{6.64}$$

Obtemos, multiplicando 6.62 por $\epsilon' = 2t - \epsilon$, as relações

$$a_{n+1} = (2t+1)a_n - 2tb_n,\ b_{n+1} = a_n - b_n.$$

Como $a_0 = 0$ e $b_0 = -1$, então seguem 6.63 e

$$a_2 = 4t^2,\ b_2 = 2t - 1.$$

Portanto, 6.64 vale inicialmente para $n = 2$, mas também, por indução, para todos os valores seguintes. De fato, se $n \geq 2$:

$$a_{n+1} - (2t+1)b_{n+1} = b_n,\ \left(2t + 1 + \frac{1}{t}\right) b_{n+1} - a_{n+1} = \frac{1}{t}a_n - \left(1 + \frac{1}{t}\right) b_n > b_n > 1 - \frac{1}{t}.$$

Note que se β pertence a S, então, pela definição de S, $\epsilon'\beta'$ também pertencerá, logo podemos supor, sem perda de generalidade, que β satisfaz a desigualdade 6.58. Como todo elemento de S é da forma $\epsilon^n\beta$ ou $\epsilon^n\beta'$ com n inteiro, precisamos mostrar que se β satisfaz 6.58 ou 6.59, então

$$|((\epsilon+1)\epsilon^n\beta)_2| < \frac{t-1}{2},\ \forall n \in \mathbb{Z} \setminus \{0\}, \tag{6.65}$$

e

$$|((\epsilon+1)\epsilon'^n\beta')_2| < \frac{t-1}{2},\ \forall n \in \mathbb{Z} \setminus \{1\} \tag{6.66}$$

não podem ser satisfeitos.

Iniciamos provando que 6.65 é impossível. Como, $|\epsilon^{-1}| = |\epsilon'|$, 6.65 é equivalente à

$$|((\epsilon+1)\epsilon'^n\beta)_2| < \frac{t-1}{2},\ \forall n \in \mathbb{Z} \setminus \{0\} \tag{6.67}$$

usaremos a última devido à devido a aplicação da identidade 6.62. Podemos assumir, sem perda de generalidade, $n > 0$ em 6.67, pois caso $n < 0$, poderíamos tomar, em 6.58, $\beta^* = \epsilon'^n\beta$ em vez de β, e posteriormente, na nova relação 6.67, n seria positivo. Substituindo a identidade 6.62 em 6.67, obtemos

$$|(a_n\beta - b_n(\epsilon+1)\beta)_2| < \frac{t-1}{2}.$$

Logo, devido a $b_n > 0$,

$$a_n|(\beta)_2| < b_n|((\epsilon+1)\beta)_2| + \frac{t-1}{2}.$$

Como β não é racional, então $|(\beta)_2| \geq \frac{1}{2}$ e, portanto, por 6.58, 6.63 e 6.64, temos

$$\frac{1}{2}a_n < \frac{t-1}{2}(b_n+1),\ tb_n < \frac{t-1}{2}(b_n+1).$$

No entanto, isso é uma contradição, já que $b_n \geq 1$. Com isso demonstramos a impossibilidade de 6.65.

Agora, mostraremos que 6.66 é impossível. De acordo com 6.58, as coordenadas de β devem ser diferentes de zero e como β não é um racional, também devem de sinais opostos, o que implica que β' possui coordenadas de mesmo sinal. Se $n < 0$, então obteremos de 6.66 e $|\epsilon'^{-1}| = |\epsilon|$

$$|((\epsilon+1)\epsilon^{-n}\beta')_2| < \frac{t-1}{2},$$

com $-n > 0$, mas, como as coordenadas de ϵ são maiores que 1, teríamos um absurdo. Portanto, em 6.66, ocorrerá $n > 0$, ou seja, $n \geq 2$. Substituindo a identidade definida em 6.62 na inequação 6.66 e passando ao conjugado, obtemos

$$|((a_n - b_n(\epsilon'+1))\beta)_2| < \frac{t-1}{2}.$$

Por $\epsilon' = 2t - \epsilon$ podemos reescrever $a_n - b_n(\epsilon' + 1)$ como

$$(-a_n + (2t+2)b_n)\epsilon + (a_n - (2t+1)b_n)(\epsilon + 1).$$

De 6.64, resulta que

$$(-a_n + (2t+2)b_n)\ |(\epsilon\beta)_2| < (a_n - (2t+1)b_n)\ |((\epsilon+1)\beta)_2| + \frac{t-1}{2}.$$

Como $|(\epsilon\beta)_2| \geq \frac{1}{2}$ e, por 6.58,

$$|((\epsilon+1)\beta)_2| \leq \frac{t}{2} - \frac{3}{4},$$

então

$$\frac{1}{2}(-a_n + (2t+2)b_n) < (a_n - (2t+1)b_n)\left(\frac{t}{2} - \frac{3}{4}\right) = \frac{t-1}{2},$$

o que implica em

$$(4t^2+1)b_n < \left(4t^2 - 1 + \frac{2t-1}{t}\right)b_n + \frac{t-1}{t}$$

e, consequentemente, na contradição $b_n < t - 1$. Com isso, provamos o Lema. ■

Agora demonstraremos que $\mathcal{O}_{61}$ não é norma euclidiano e posteriormente faremos o mesmo para $\mathcal{O}_{109}$.

Teorema 6.71. *$\mathcal{O}_{61}$ não é norma euclidiano.*

Demonstração: Seja

$$\epsilon = \frac{39 + 5\sqrt{61}}{2}$$

a unidade fundamental de $\mathcal{O}_{61}$, defina $t = (\epsilon)_1$ e $u = (\epsilon)_2$, então $\epsilon = t + u\sqrt{61}$, onde $2t$ e $2u$ são inteiros ímpares e, mais ainda, $2u \equiv 1 \pmod 4$. Vamos assumir que $\mathcal{O}_{61}$ seja norma euclidiano.

Defina o inteiro $a = t + \frac{1}{2}$. Qualquer ω em $\mathcal{O}_{61}$ pode ser expresso como

$$\omega = \frac{1}{2}(-(\epsilon' + 1) + \beta), \tag{6.68}$$

onde

$$\beta = \frac{r + s\sqrt{61}}{2},\ \text{com } r, s \text{ inteiros} \tag{6.69}$$

com r e s inteiros satisfazendo

$$r \equiv s \equiv 1 \pmod 2,\ r + s \equiv 2t + 1 \pmod 4. \tag{6.70}$$

De acordo com as expressões 6.49 e 6.68,

$$a + (\epsilon+1)\omega = t + \frac{1}{2} + (\epsilon+1)\frac{1}{2}(-(\epsilon'+1) + \beta) = \frac{1}{2} + \frac{1}{2}(\epsilon+1)\beta. \tag{6.71}$$

Agora, seguindo as notações dos Lemas 6.68 e 6.69, tomando $\alpha = \frac{1}{2}$ e $\omega = \frac{\beta}{2}$, seguem, dos Lemas 6.68 e 6.69, as desigualdade

$$\frac{1}{2}|((\epsilon+1)\beta)_2| < u, \tag{6.72}$$

$$\left|\frac{1}{4} + \frac{1}{2}((\epsilon+1)\beta)_1 + \frac{t}{2}N(\beta)\right| < 2t, \tag{6.73}$$

$$\frac{1}{4}|N(\beta)| < \frac{1}{2} + 1 + \frac{1}{8t}.$$

Logo, $|N(\beta)| \leq 6$. Além disso, se β fosse uma unidade, seguindo de acordo com a desigualdade 6.72 e o Lema 6.70, teríamos $\beta = \pm 1$ ou $\pm\epsilon'$, mas isso seria uma absurdo, já que para ambos, ω, definido em 6.68, não seria um inteiro algébrico em $\mathbb{Q}(\sqrt{61})$, logo $|N(\beta)| > 1$. Além disso, pelas relações 6.69 e 6.70, $N(\beta)$ deve ser ímpar, então podemos considerar $|N(\beta)| = 3$ ou 5.

Agora, observe que os elementos

$$\beta_3 = \pm(8 - \sqrt{61}),\ \beta_5 = \pm\frac{9+\sqrt{61}}{2},$$

onde $N(\beta_i) = i$, satisfazem a condição 6.72, o que implica que também satisfazem a condição 6.58. De acordo com o Lema 6.70, a menos de sinal, este é o motivo de considerarmos as possibilidade positiva e negativa para β_i, o mesmo pode valer apenas para $\epsilon'\beta_i' = \beta_i^*$, $i = 3, 5$, ou seja,

$$\beta_3^* = \pm\frac{7-\sqrt{61}}{2},\ \beta_5^* = \pm\frac{23-3\sqrt{61}}{2}.$$

Entre os oito números, apenas β_5 e β_5^* satisfazem as relações em 6.70. No entanto, para esses valores, a desigualdade 6.73 não é satisfeita, uma vez que o terceiro termo é $\pm\frac{5t}{2}$, e o termo do meio é ± 8 ou $\pm\frac{7}{2}$. Dessa forma, provamos $\mathcal{O}_{61}$ não é norma euclidiano. ■

Antes de demonstrarmos o caso $p = 19$, vamos provar o seguinte lema:

Lema 6.72. *As equações diofantina $x^2 - 109y^2 = \pm 4k$ não possuem solução para*

$$k = 2,\ 11,\ 13,\ 17,\ 19.$$

Portanto, podemos afirmar que não há elementos de norma

$$\pm 2,\ \pm 11,\ \pm 13,\ \pm 17,\ \pm 19$$

em $\mathcal{O}_{109}$.

Demonstração: Para $k = 2$, 13, 17, 19 a equação não é possível uma vez que nenhum deles é resíduo quadrático módulo 109. Para 11, não há solução já que 109 não é um resíduo quadrático módulo 11. ■

Teorema 6.73. *$\mathcal{O}_{109}$ não é norma euclidiano.*

Demonstração: Para provar a inexistência do algoritmo de Euclides em $\mathcal{O}_{109}$, iniciamos escolhendo um inteiro α satisfazendo $\sqrt{2t} \leq \alpha < \sqrt{2t} + 1$. Assim, pelo Lema 6.68, exite um $\omega \neq 0$, tal que

$$|(\alpha + (\epsilon+1)\omega)_2| = |((\epsilon+1)\omega)_2| < u. \tag{6.74}$$

Além disso, de acordo com 6.57, $|N(\omega)| \leq \alpha + 2$.

Seja $\epsilon = \frac{261+25\sqrt{109}}{2}$ a unidade fundamental de $\mathcal{O}_{109}$, então, tome $\alpha = 17$ e assim $|N(\omega)| \leq 19$. Pela expressão 6.74 e pelo Lema 6.70, ω não pode ser uma unidade nem um associado de um número racional. Pela hipótese de $\mathcal{O}_{109}$ ser um anel quadrático euclidiano temos, em particular, que $\mathcal{O}_{109}$ é um domínio de fatoração única, e levando

em consideração o Lema 6.72, a menos de associados e seus conjugados, existem apenas três primos não racionais em $\mathcal{O}_{109}$, $\omega_3, \omega_5, \omega_7$, onde $N(\omega_i) = i$, cujo valor absoluto de sua norma não excede 19. Tomando-os de forma que 6.74 seja satisfeito, temos

$$\omega_3 = \pm\frac{11-\sqrt{109}}{2},\ \omega_5 = \pm(21-2\sqrt{109}),\ \omega_7 = \pm(94-9\sqrt{109}).$$

A partir de combinações desses elementos e seus respectivos conjugados podemos construir outros elementos que satisfazem a condição 6.74, são eles:

$$\omega_{12} = 2\omega_3,\ \pm\omega_9 = \omega_3^2 = \pm\frac{115-11\sqrt{19}}{2},$$

$$\omega_{15} = \omega_3\omega_5 = \pm\frac{449-43\sqrt{109}}{2},\ \omega*_{15} = \omega_3'\omega_5 = \pm\frac{13-\sqrt{109}}{2}.$$

Então, além desses 14 números, pelo Lema 6.70, podemos nos limitar a verificar os valores:

$$\epsilon'\omega_3' = \pm\frac{23-7\sqrt{109}}{2},\ \epsilon'\omega_5' = \pm\frac{31-3\sqrt{109}}{2},\ \epsilon'\omega_7' = \pm\frac{9-\sqrt{109}}{2},$$

$$2\epsilon'\omega_3' = \pm(23-7\sqrt{109}),\ \epsilon'\omega_9' = \pm(10-\sqrt{109}),\ \epsilon'\omega_{15}' = \pm\frac{7-\sqrt{109}}{2},$$

$$\epsilon'\omega*_{15} = \pm(167-16\sqrt{109}).$$

No entanto, é fácil verificar que nenhum dos 28 números satisfazem 6.56, que nessas condições será, pelo Lema 6.69,

$$|289 + 17((263+25\sqrt{109})\omega)_1 + 261N(\omega)| < 261.$$

Portanto, $\mathcal{O}_{109}$ não é norma euclidiano. ■

6.3.3 Classificação de anéis quadráticos com discriminante $p \equiv 17 \pmod{24}$

Nesta subseção classificaremos os anéis quadráticos $\mathcal{O}_p$ com discriminante p primo satisfazendo $p \equiv 17 \pmod{24}$. Mostraremos que únicos os únicos anéis quadráticos norma euclidiano são os anéis com discriminantes $p = 17$ ou $p = 41$. Iniciaremos demonstrando que, neste caso, não há anéis quadráticos norma euclidianos $\mathcal{O}_p$ para p menor 3000, exceto por, $p = 89, 113, 137$. Para os demais casos, isto é, $p = 89, 113, 137$ ou $p > 3000$, utilizaremos uma abordagem semelhante a utilizada nos casos $\mathcal{O}_{61}$ e $\mathcal{O}_{109}$ a fim de demonstrarmos que os anéis quadráticos correspondentes a esses valores não são norma euclidianos. Esta seção é também baseada no trabalho de L. Rédei, desenvolvido em [18].

Teorema 6.74. *Não há anéis quadráticos norma euclidianos $\mathcal{O}_p$, onde p é um primo* $\equiv 17 \pmod{24}$ *e* $281 \leq p < 3001$

Demonstração: Representaremos os primos p da forma $24n+17$, que também são primos da forma $24n+1$, maiores que 281 e menores que 3000, na forma $p = q_1m_1+q_2m_2$ seguindo as hipóteses do Teorema 6.52.

- $257 = 3 \times 14 + 5 \times 43$
- $281 = 3 \times 46 + 11 \times 13$
- $353 = 3 \times 31 + 5 \times 52$
- $401 = 3 \times 26 + 17 \times 19$
- $449 = 3 \times 76 + 13 \times 17$
- $521 = 3 \times 28 + 19 \times 23$
- $569 = 3 \times 44 + 19 \times 23$
- $593 = 3 \times 7 + 11 \times 52$
- $617 = 3 \times 29 + 5 \times 106$
- $641 = 3 \times 38 + 17 \times 31$
- $761 = 3 \times 11 + 7 \times 104$
- $809 = 3 \times 94 + 17 \times 31$
- $857 = 3 \times 7 + 11 \times 76$
- $881 = 3 \times 23 + 7 \times 116$
- $929 = 3 \times 41 + 13 \times 62$
- $953 = 3 \times 11 + 5 \times 184$
- $977 = 3 \times 5 + 13 \times 74$
- $1049 = 3 \times 37 + 7 \times 134$
- $1097 = 3 \times 10 + 11 \times 97$
- $1193 = 3 \times 5 + 19 \times 62$
- $1217 = 3 \times 7 + 13 \times 92$
- $1289 = 3 \times 44 + 13 \times 89$
- $1361 = 3 \times 22 + 7 \times 185$
- $1409 = 3 \times 58 + 13 \times 95$
- $1433 = 3 \times 10 + 23 \times 61$
- $1481 = 3 \times 44 + 19 \times 71$
- $1553 = 3 \times 11 + 5 \times 304$
- $1601 = 3 \times 13 + 11 \times 142$
- $1697 = 3 \times 14 + 5 \times 331$
- $1721 = 3 \times 14 + 23 \times 73$
- $1889 = 3 \times 37 + 7 \times 254$
- $1913 = 3 \times 5 + 13 \times 146$
- $2081 = 3 \times 19 + 11 \times 184$
- $2129 = 3 \times 62 + 29 \times 67$
- $2153 = 3 \times 10 + 11 \times 193$
- $2273 = 3 \times 11 + 5 \times 448$
- $2297 = 3 \times 59 + 5 \times 424$
- $2393 = 3 \times 5 + 29 \times 82$
- $2417 = 3 \times 10 + 11 \times 217$
- $2441 = 3 \times 11 + 7 \times 344$
- $2609 = 3 \times 11 + 7 \times 368$
- $2633 = 3 \times 20 + 31 \times 83$
- $2657 = 3 \times 13 + 11 \times 238$
- $2729 = 3 \times 23 + 7 \times 380$
- $2753 = 3 \times 41 + 5 \times 526$
- $2777 = 3 \times 7 + 13 \times 212$
- $2801 = 3 \times 41 + 13 \times 206$
- $2897 = 3 \times 10 + 47 \times 61$
- $2969 = 3 \times 29 + 11 \times 262$ ■

Para os demais casos utilizaremos uma abordagem semelhante à utilizada nos casos $\mathcal{O}_{61}$ e $\mathcal{O}_{109}$. Mas, antes precisaremos de alguns resultados auxiliares.

Lema 6.75. *Seja $p \equiv 1 \pmod 8$, então a unidade fundamental $\epsilon = t + u\sqrt{p}$ de $\mathcal{O}_p$ possui coordenadas t e u inteiras. Além disso,*

$$t \equiv 0 \pmod 4, \ u \equiv 1 \pmod 2.$$

Demonstração: Para demonstrarmos que t e u são inteiros, de acordo com o Teorema 2.55, basta demonstrar que a equação diofantina, de incógnitas x e y,

$$x^2 - py^2 = -4$$

deve possuir apenas soluções x e y simultaneamente pares. Suponhamos o contrário, ou seja, x e y não são simultaneamente pares. Analisando a equação módulo 8 teríamos

$$0 \equiv x^2 - py^2 \equiv 4 \pmod 8 \text{ se } x, y \text{ forem simultaneamente ímpares,}$$

$$1, 3 \equiv x^2 - py^2 \equiv 4 \pmod 8 \text{ se } x \text{ for ímpar e } y \text{ for par}$$

ou

$$0 \equiv x^2 - py^2 \equiv 4 \pmod 8 \text{ se } x, y \text{ forem simultaneamente ímpares}$$

Logo, a partir das contradições podemos concluir que t e u são inteiros. Agora, analisando a equação

$$t^2 - pu^2 = -1$$

é imediato que u não pode ser par, pois, caso contrário -1 seria um resíduo quadrático módulo 4. Portanto, u é ímpar. Agora, analisando a equação módulo 8, mas desta vez com suposição de u ser ímpar, obtemos

$$t^2 \equiv 0 \pmod 8,$$

portanto, deve ocorrer $t \equiv 0 \pmod 4$. ■

Lema 6.76. *Seja $p \equiv 17 \pmod{24}$, então, com exceção de $\mathcal{O}_{17}$, não há anéis quadráticos norma euclidianos $\mathcal{O}_p$ quando $u = 1$.*

Demonstração: Se o número de elementos $\bar{\mu}$ determinado pela condições 6.46, 6.47 e 6.48 for menor que $2t$, então, conforme $N(\epsilon + 1) = 2t$, calculado anteriormente em 6.49, o Lema 6.59 e o Corolário 3.3, o algoritmo euclidiano não existirá no respectivo anel quadrático $\mathcal{O}_p$. Suponhamos $\epsilon = t + \sqrt{p}$. Denotando $a = t$, então $p = a^2 + 1$, onde $4 \mid a$. Pelo Lema 6.65, para cada classe de resíduos módulo $(\epsilon + 1)$, há sempre um representante $\bar{\mu}$, como em 6.46, satisfazendo uma das condições abaixo:

$$y = 0,\ |x| < \sqrt{8a},\ 2 \mid x;$$

$$y = \pm 1,\ |x^2 - a^2 - 1| < 8a,\ 2 \nmid x;$$

$$y = \pm 2,\ |x^2 - 4a^2 - 4| < 8a,\ 2 \mid x.$$

Para $a > 16$, as soluções das desigualdades acima são, respectivamente, os números pares entre $-\sqrt{8a}$ e $\sqrt{8a}$, seguida por $\pm(a \pm 1)$ e $\pm(a \pm 3)$, e por fim $\pm 2a$. Logo, o número total de $\bar{\mu}$ satisfazendo uma das condições é menor que $\sqrt{8a} + 21 < 2a = 2t$, o que implica, segundo a observação inicial, na inexistência do algoritmo de Euclides no anel. Portanto, o resultado é verdadeiro quando $p = a^2 + 1 > 16^2 + 1 = 257$. Já que para $a \leq 16$, exceto por 17, não há valores de p cuja coordenada u seja 1. ■

Lema 6.77. *Se $\epsilon = t + u\sqrt{p} > 1$ e $t^2 - pu^2 = -1$, então $t, u > 0$.*

Demonstração: Como $t^2 - pu^2 = (t + u\sqrt{p})(t - u\sqrt{p})$, então pela hipótese segue $0 > \epsilon' = (t - u\sqrt{p}) > -1$. Então

$$t = \frac{t}{2} + \frac{t}{2} + \frac{u\sqrt{p}}{2} - \frac{u\sqrt{p}}{2} = \frac{1}{2}\left((t + u\sqrt{p}) + (t - u\sqrt{p})\right) = \frac{1}{2}(\epsilon + \epsilon') > 0$$

e

$$u = \frac{1}{2\sqrt{p}}(2u\sqrt{p} + t - t) = \frac{1}{2\sqrt{p}}\left((t + u\sqrt{p}) + (t - u\sqrt{p})\right) = \frac{1}{2\sqrt{p}}(\epsilon + \epsilon') > 0$$

■

A partir dos últimos três lemas, podemos considerar que a unidade fundamental $t+u\sqrt{p}$ do anel quadrático $\mathcal{O}_p$, com $p \equiv 17 \pmod{24}$, tenha coordenadas estritamente maiores que 1, em particular, $u \geq \frac{3}{2}$, o que será de importância para aplicação de resultados já introduzidos à classificação de anéis quadráticos com discriminante $p \equiv 17 \pmod{24}$.

Teorema 6.78. *Além de $\mathcal{O}_{17}$ e $\mathcal{O}_{41}$ não há outros anéis quadráticos norma euclidianos com discriminante p primo congruente a 17 módulo 24.*

Demonstração: Seja um anel quadrático $\mathcal{O}_p$ com $p \equiv 17 \pmod{24}$, $p > 41$, nosso objetivo é demonstrar que esse anel quadrático não é norma euclidiano. Suponhamos o contrário, isto é, que $\mathcal{O}_p$ seja norma euclidiano. Tome $\epsilon = t + u\sqrt{p}$ como a unidade fundamental fundamental do anel quadrático, como discutido anteriormente, podemos assumir $t > 1$, $u \geq \frac{3}{2}$ e

$$t \equiv 0 \pmod 4,\ u \equiv 1 \pmod 2. \tag{6.75}$$

Com essas propriedades, $\alpha = \frac{\epsilon+1}{2} + 3 \in \mathcal{O}_p$, logo podemos aplicar o Lema 6.68 a α. Antes disso, observemos que sempre podemos escrever um elemento ω em $\mathcal{O}_p$ como

$$\omega = -\frac{1}{2} + \frac{\beta}{2},$$

onde β é um elemento de $\mathcal{O}_p$ satisfazendo

$$\beta \equiv 1 \pmod 2. \tag{6.76}$$

Assim, após a aplicação do Lema 6.68 a α e a substituição de ω por $-\frac{1}{2} + \frac{\beta}{2}$, obtemos a expressão

$$\alpha + (\epsilon + 1)\omega = 3 + \frac{1}{2}(\epsilon + 1)\beta.$$

Agora, ao aplicarmos o Lema 6.69 a $\alpha = 3$ e $\omega = \frac{\beta}{2}$, decorrem imediatamente as desigualdades

$$|6 + ((\epsilon + 1)\beta)_1| < 2t, \tag{6.77}$$

$$|((\epsilon + 1)\beta)_2| < 2u \tag{6.78}$$

$$|18 + ((\epsilon + 1)\beta)_1 + tN(\beta)| < 4t \tag{6.79}$$

$$|N(\beta)| < 16 + \frac{18}{t}. \tag{6.80}$$

Seguindo o Teorema 6.74, p pode assumir apenas os valores $89, 113, 137$ ou valores maiores que 3001. Nos três primeiros casos, as unidades fundamentais correspondentes aos anéis quadráticos são:

$$\epsilon = 500 + 53\sqrt{89},\ 776 + 73\sqrt{113},\ 1744 + 149\sqrt{137}, \tag{6.81}$$

respectivamente. Para os casos em que $p > 3001$ temos $t^2 - pu^2 = -1$, o que implica $t > \sqrt{3000} > 54$. Portanto, em qualquer situação, sempre ocorrerá,

$$t > 54. \tag{6.82}$$

A partir das desigualdades 6.80 e 6.82 é imediato que $|N(\beta)| \leq 16$, além disso, $|N(\beta)| \leq 15$, já que pela condição 6.76, $|N(\beta)|$ deve ser ímpar. Além disso, β não pode ser uma unidade, pois caso contrário, de acordo com a desigualdade 6.78 e o Lema 6.65, onde é claro que, pela relação $t - \sqrt{p}u > -1$,

$$\frac{t-1}{2} \geq 2u,$$

apenas $\beta = \pm 1$ ou $\beta = \pm\epsilon'$ seriam possíveis. Então $((\epsilon+1)\beta)_1 = \pm(t+1)$ ou $\pm(t-1)$. No entanto, ambos são incompatíveis com as desigualdades 6.79 e 6.82 e com $N(\beta) = \pm 1$, o que nos leva a uma contradição. De maneira semelhante podemos mostrar que β também não pode estar associado a um número racional (inteiro). Também deve ocorrer $(\beta, 3) = 1$. Se 3 fosse um fator de β, observe que 3 é um primo em $\mathcal{O}_p$, teríamos $(\beta, 3) \neq 1$, o que implicaria que 3 é divisor de β e, assim, 9 dividiria $|N(\beta)|$ e, uma vez que $|N(\beta)| \leq 15$, seguiria a igualdade $|N(\beta)| = 9$. Mas como, com base na suposição de $\mathcal{O}_p$ ser um domínio euclidiano, $\mathcal{O}_p$ é um domínio de fatoração única, então β e 3 deveriam ser associados, o que é uma contradição. Então, baseado nas últimas observações, concluímos que apenas

$$|N(\beta)| = 5, 7, 11, 13 \tag{6.83}$$

são possíveis.

Diante das possibilidade de $|N(\beta)|$ em 6.83, as coordenadas de β devem ser diferentes de zero e, mais ainda, de acordo com a desigualdade 6.78, devem ter sinais opostos. Além disso, devido a congruência 6.76, são também números inteiros com paridades distintas. Assim, podemos definir

$$\beta = \sigma(x - y\sqrt{p}), \tag{6.84}$$

onde x e y são números inteiros positivos, com $2 \nmid (x + y)$ e $\sigma = \pm 1$. a fim de simplificar a notação, definimos

$$b = N(\beta). \tag{6.85}$$

Com isso, podemos expressar

$$py^2 = x^2 - b. \tag{6.86}$$

Deste ponto em diante demonstraremos a impossibilidade para a existência do algoritmo para quando $p = 89, 113, 137$ ou $p > 3001$. Vamos começar considerando $p > 3001$, deixando os casos $p = 89, 113, 137$ de lado por este momento.

Por $p > 3001$, pela igualdade 6.86 e pelas possibilidades de $|N(\beta)|$ em 6.83, então

$$x > 54. \tag{6.87}$$

Agora, defina

$$x^* = tx - puy. \tag{6.88}$$

Como $\pm x^*$ é a primeira coordenada de $\epsilon\beta$ logo, também ocorrerá,

$$|x^*| > 54. \tag{6.89}$$

Pelo Teorema 2.55, temos

$$(t + u\sqrt{p})(t - u\sqrt{p}) = -1,$$

mas, como $t + u\sqrt{p} > 1$, então $0 > t - u\sqrt{p} > -1$. Em particular, ocorre a desigualdade $0 < t < u\sqrt{p}$, que por sua vez implica em $2t < t + u\sqrt{p}$. Logo,

$$-1 = (t + u\sqrt{p})(t - u\sqrt{p}) < 2t(t - u\sqrt{p}).$$

Portanto, por $-1 < 2t(t - u\sqrt{p})$, obtemos a desigualdade

$$u\sqrt{p} < t + \frac{1}{2t}.$$

Juntando as desigualdades, obtemos

$$t < u\sqrt{p} < t + \frac{1}{2t}. \tag{6.90}$$

Agora, para x e y definidos temos a relação a desigualdade

$$x - \frac{7}{x} < y\sqrt{p} < x + \frac{7}{x}. \tag{6.91}$$

De fato, como

$$x - \frac{7}{x} < y\sqrt{p} < x + \frac{7}{x} \iff \frac{7}{x} < -x + y\sqrt{p} < \frac{7}{x}$$

então, multiplicando a desigualdade equivalente por $(x + y\sqrt{p})$ e substituindo b definido em 6.85, demonstrar a inequação 6.91 é equivalente a demonstrar

$$x|b| < 7(x + y\sqrt{p}),$$

mas como, pela definição 6.83 e pela desigualdade 6.86, $|b| \leq 13$, basta demonstrarmos

$$13x < 7(x + y\sqrt{p}),$$

ou mesmo, a desigualdade equivalente

$$\frac{6}{7}x < y\sqrt{p}.$$

Elevando ao quadrado ambos os lados da desigualdade e utilizando 6.86, obtemos

$$\frac{36}{49}x^2 < x^2 - b \iff 0 < x^2\left(1 - \frac{36}{49}\right) - b$$

Como $|b| < 13$ e, por 6.87, $x > 54$, segue a validade da desigualdade e portanto também a validade da desigualdade 6.91. De acordo com 6.84,

$$((\epsilon + 1)\beta)_1 = \sigma((t + 1)x - puy). \tag{6.92}$$

Agora, vamos demostrar que

$$(t + 1)x - puy > 0. \tag{6.93}$$

Com base na igualdade 6.92 e nas desigualdade 6.79 e $|b| \geq 5$, temos que

$$|(t + 1)x - puy| \geq \frac{t - 18}{6}.$$

Se a desigualdade 6.93 fosse falsa, então teríamos

$$(t+1)x + \frac{t-18}{6} \leq puy.$$

Ao elevar ao quadrado e levando em consideração 6.86 e 6.83, que resultam em $py^2 \leq x^2 + 13$, então, obteríamos

$$(t+1)^2x^2 + (t+1)(t-18)\frac{x}{3} < p^2u^2y^2 \leq (t^2+1)(x^2+13),$$

o que simplificando resulta em

$$6tx^2 + (t+1)(t-18)x < 39(t^2+1)$$

e, portanto,

$$6x^2 + (t-18)x < 39t + \frac{39}{t}.$$

No entanto, segundo os limites inferiores para t e y, em 6.82 e 6.87, respectivamente, $6x^2 - 18x > \frac{39}{t}$, o que nos leva a $tx < 39t$, ou seja, $x < 39$, contradizendo 6.87, o que prova a desigualdade 6.93. Seguindo 6.92, 6.93, 6.77 e 6.79 chegamos na desigualdade

$$\frac{(|b|-4)t - 18}{6} < (t+1)x - puy < 2t + 6. \tag{6.94}$$

Agora, vamos, caso a caso, demonstrar a impossibilidade de $b = 5$, $b = -5$ e $|b| > 5$.

Quando $b = 5$, por 6.86, $x - y\sqrt{p} > 0$. Procedendo de maneira análoga ao que fizemos para demonstrar a desigualdade 6.91, podemos mostrar que $x - \frac{3}{x} < y\sqrt{p}$. Juntando as desigualdades obtemos

$$x - \frac{3}{x} < y\sqrt{p} < x. \tag{6.95}$$

A partir das desigualdades 6.95 e 6.90, podemos deduzir a expressão

$$(t+1)x - puy > (t+1)x - \left(t + \frac{1}{2t}\right)x = \frac{2t-1}{2t}x. \tag{6.96}$$

Da expressão acima e seguindo a desigualdade 6.94, obtemos ainda que $x < \frac{2t}{2t-1}(2t+6)$, então, de acordo com a desigualdade 6.82,

$$x \leq 2t + 7. \tag{6.97}$$

Da mesma forma, utilizando as desigualdades 6.90 e 6.95, obtemos a desigualdade

$$(t+1)x - puy < (t+1)x - t\left(x - \frac{3}{x}\right) = x + \frac{3t}{x} \tag{6.98}$$

e a partir da desigualdade 6.94,

$$x + \frac{3t}{x} > \frac{t-18}{6}.$$

Se $\frac{3t}{x} > x$, então

$$\frac{6t}{x} > \frac{t-18}{6},$$

de onde segue

$$x < \frac{36t}{t-18},$$

e, assim, de acordo com 6.82,

$$x < \frac{36 \cdot 54}{36} = 54,$$

o que entra em contradição com 6.87. Portanto, $x \geq \frac{3t}{x}$ e

$$x > \frac{t-18}{12}. \tag{6.99}$$

Segundo a definição 6.88 e a desigualdade 6.96, $x^* > -\frac{x}{2t}$, o que implica, de acordo com a desigualdade 6.97, em

$$x^* > -2. \tag{6.100}$$

Por outro lado, pela definição 6.88 e pela expressão 6.98, $x^* < \frac{3t}{x}$. Isso resulta, a partir da desigualdade 6.99, em $x^* < \frac{36t}{t-18}$, logo, por 6.82, $x^* < 54$, que juntamente com 6.100, entra em contradição com 6.89.

Caso seja $b = -5$. Novamente, partindo das expressões 6.86 e 6.87, obtemos

$$x < y\sqrt{p} < x + \frac{5}{2x}. \tag{6.101}$$

Daí e pela desigualdade 6.90, deduzimos a seguinte expressão

$$(t+1)x - puy > (t+1)x - \left(t + \frac{1}{2t}\right)\left(x + \frac{5}{2x}\right) > \frac{2t-1}{2t}x - (t+1)\frac{5}{2x}, \tag{6.102}$$

e, de acordo com 6.82,

$$(t+1)x - puy > \frac{2t-1}{2t}x - \frac{t+1}{20}.$$

Pela expressão acima, e pelas desigualdades 6.94 e 6.82,

$$x < \frac{2t}{2t-1}(2t+6) + \frac{2t}{2t-1}\frac{t+1}{20} < \frac{41t}{20} + 8 = \frac{41t+160}{20}. \tag{6.103}$$

A partir das desigualdades 6.90 e 6.101, temos

$$(t+1)x - puy < (t+1)x - tx = x \tag{6.104}$$

e, de acordo com a desigualdade 6.94,

$$x > \frac{t-18}{6}. \tag{6.105}$$

Agora, segundo a definição 6.88 e a desigualdade 6.102,

$$x^* > -\frac{x}{2t} - (t+1)\frac{5}{2x},$$

então, pelas desigualdade 6.103 e 6.105,

$$x^* > -\frac{41t+160}{40t} - \frac{15(t+1)}{t-18}.$$

Com isso, a partir da desigualdade 6.82, obtemos

$$x^* > -25. \tag{6.106}$$

Agora, pela definição 6.88 e pela desigualdade 6.104 segue que $x^* < 0$, e isso, juntamente com 6.106 e 6.89, resulta em uma contradição.

No caso em que $|b| > 5$, é imediato, por 6.83, que $7 \leq |b| \leq 13$. Também pela desigualdade 6.94, segue

$$\frac{t-6}{2} < (t+1)x - puy < 2t+6. \tag{6.107}$$

Com base nas desigualdades 6.90 e 6.91 chegamos a expressão

$$(t+1)x - puy > (t+1)x - \left(t + \frac{1}{2t}\right)\left(x + \frac{7}{x}\right) > \frac{2t-1}{2t}x - (t+1)\frac{7}{x}, \tag{6.108}$$

então, em concordância com 6.87,

$$(t+1)x - pux > \frac{2t-1}{2t}x - \frac{t+1}{7}.$$

Agora, pela expressão acima e de acordo com as desigualdades 6.82 e 6.107, temos

$$x < \frac{2t}{2t-1}(2t+3) + \frac{2t}{2t-1}\frac{t+1}{7} < \frac{15t}{7} + 9. \tag{6.109}$$

Baseado nas desigualdades 6.90 e 6.91, segue

$$(t+1)x - puy < (t+1)x - t\left(x - \frac{7}{y}\right) = x + \frac{7t}{x}, \tag{6.110}$$

então segundo a desigualdade 6.107,

$$x + \frac{7t}{x} > \frac{t-6}{2}.$$

Novamente, não pode ocorrer $\frac{7t}{x} > x$, pois então $\frac{14t}{x} > \frac{t-6}{2}$, o que entra em contradição com as desigualdades 6.82 e 6.87. Portanto, $x \geq \frac{7t}{x}$ e consequentemente

$$x > \frac{t-6}{4}. \tag{6.111}$$

Segundo a definição 6.88 e a desigualdade 6.108,

$$x^* > -\frac{x}{2t} - (t+1)\frac{7}{x},$$

o que implica, levando em consideração as inequações 6.109, 6.111 e 6.82,

$$x^* > -\frac{15t+63}{14t} - \frac{28(t+1)}{t-6},$$

e portanto

$$x^* > -35.$$

Entretanto, seguindo a definição 6.88 e as desigualdades 6.110, 6.111 e 6.82,

$$x^* < \frac{7t}{x} < \frac{28t}{t-6} < 32.$$

Como as duas últimas inequações contradizem 6.89, concluímos a demonstração para o caso $|b| > 5$, o que concluí concluindo a prova de não existência de anéis quadráticos com discriminante $p > 3001$. No entanto, ainda nos resta classificar os anéis quadráticos de discriminante $p = 89, 113$ ou 137. Em 6.81 foi dadas as respectivas unidades fundamentais de $\mathcal{O}_{89}$, $\mathcal{O}_{113}$ e $\mathcal{O}_{137}$, que serão utilizadas a fim de aplicarmos o Lema 6.70 a cada um dos casos.

Caso $p = 89$. De acordo com 6.83, como $N(\beta) = \pm 7,\ \pm 13$ não é possível, uma vez que ± 7 e ± 13 não são resíduos quadráticos módulo 89, apenas os casos $|N(\beta)| = 5, 11$ são possíveis. Semelhante ao que foi visto nos Teoremas 6.71 e 6.73, notamos que devido a 6.78, 6.81 e o Lema 6.70, seria possível que β fosse apenas

$$\beta_5 = \pm(19 - 2\sqrt{89}),\ \epsilon'\beta_5' = (66 - 7\sqrt{89}),\ \beta_{11} = \pm(10 - \sqrt{89}),\ \epsilon'\beta_{11}' = \pm(283 - 30\sqrt{89}).$$

No entanto, nenhum dos valores satisfaz 6.79.

Caso $p = 113$. Devido a 6.83, $|N(\beta)| = 7, 11$ ou 13. Agora, os possíveis candidatos a β seriam

$$\beta_7 = \pm(32 - 3\sqrt{113}),\ \epsilon'\beta_7' = \pm(85 - 8\sqrt{113}),\ \beta_{11} = \pm(202 - 19\sqrt{113}),$$

$$\epsilon'\beta_{11}' = \pm(21 - 2\sqrt{113}),\ \beta_{13} = \pm(489 - 46\sqrt{113}),\ \beta_{13}' = \pm(10 - \sqrt{113}).$$

no entanto, nenhum deles satisfaz 6.79.

Caso $p = 137$. Então, $|N(\beta)| = 7$ ou 11. Podemos concluir de maneira semelhante com

$$\beta_7 = \pm(12 - \sqrt{137}),\ \epsilon'\beta_7 = \pm(515 - 44\sqrt{137}),\ \beta_{11} = \pm(82 - 7\sqrt{137}),\ \epsilon'\beta_{11}' = \pm(117 - 10\sqrt{137}).$$

Com isso finalizamos a demonstração do teorema. ■

Assim podemos enunciar

Teorema 6.79. *Um anel quadrático com discriminante* $p \equiv 17 \pmod{24}$ *é norma euclidiano apenas quando* $p = 17$ *ou* $p = 41$.

6.3.4 Classificação de anéis quadráticos com discriminante $p \equiv 1 \pmod{24}$

Nesta subseção lidaremos com a classificação dos anéis quadráticos reais $\mathcal{O}_p$, onde p é um primo congruente a 1 módulo 24. Exceto pelos valores 97, 193, 241, 313, 337, 457 e 601, demonstraremos, utilizando o Teorema 6.52, que $\mathcal{O}_p$ não é um anel quadrático norma euclidiano. Para $p = 97$, exibiremos um par ordenado racional (x_0, y_0) tal que $M(N_{97}; x_0, y_0) \geq 1$ (veja a definição 4.11), assim demonstrando que $\mathcal{O}_{97}$ não é norma euclidiano. Para $p = 193$, 241, 313, 337, 457 ou 601 demonstraremos que os respectivos anéis quadráticos não são norma euclidianos utilizando uma abordagem adaptada à desenvolvida no Capítulo 5.

Lema 6.80. *Para* $p > 97$, *onde* $p \equiv 1 \pmod{24}$, *com possível exceção de* 193, 241, 313, 337, 457 *e* 601, *não existem anéis quadráticos* $\mathcal{O}_p$ *norma euclidianos.*

Demonstração: Devido ao Teorema 5.22, estamos interessados em investigar apenas os anéis quadráticos com discriminante menor que 128^2. Representaremos os primos p como na hipótese do lema, que também são congruentes a 1 módulo 4, na forma $p = q_1m_1+q_2m_2$ seguindo as hipóteses do Teorema 6.52:

- $409 = 14 \times 19 + 11 \times 13$
- $433 = 7 \times 29 + 10 \times 23$
- $577 = 14 \times 13 + 5 \times 79$
- $673 = 17 \times 15 + 19 \times 22$
- $769 = 23 \times 21 + 13 \times 22$
- $937 = 5 \times 7 + 41 \times 22$
- $1009 = 11 \times 52 + 19 \times 23$
- $1033 = 11 \times 13 + 89 \times 10$
- $1129 = 17 \times 19 + 31 \times 26$
- $1153 = 17 \times 14 + 61 \times 15$
- $1201 = 17 \times 26 + 23 \times 33$
- $1249 = 19 \times 44 + 7 \times 59$
- $1297 = 5 \times 154 + 17 \times 31$
- $1321 = 17 \times 39 + 47 \times 14$
- $1489 = 17 \times 39 + 59 \times 14$
- $1609 = 19 \times 14 + 17 \times 79$
- $1753 = 7 \times 165 + 13 \times 46$
- $1777 = 5 \times 21 + 19 \times 88$
- $1801 = 19 \times 78 + 11 \times 29$
- $1873 = 23 \times 60 + 17 \times 29$
- $2017 = 5 \times 26 + 17 \times 111$
- $2113 = 5 \times 277 + 7 \times 104$
- $2137 = 13 \times 129 + 5 \times 92$
- $2161 = 23 \times 70 + 19 \times 29$
- $2281 = 7 \times 51 + 13 \times 148$
- $2377 = 5 \times 62 + 13 \times 159$
- $2473 = 5 \times 31 + 19 \times 122$
- $2521 = 11 \times 53 + 17 \times 114$
- $2593 = 5 \times 275 + 29 \times 42$
- $2617 = 7 \times 122 + 41 \times 43$
- $2689 = 13 \times 46 + 17 \times 123$
- $2713 = 11 \times 153 + 5 \times 206$
- $2833 = 7 \times 15 + 11 \times 248$
- $2857 = 5 \times 138 + 11 \times 197$
- $2953 = 5 \times 42 + 13 \times 211$
- $3001 = 7 \times 65 + 19 \times 134$
- $3049 = 11 \times 94 + 13 \times 155$
- $3121 = 7 \times 220 + 17 \times 93$
- $3169 = 7 \times 86 + 17 \times 151$
- $3217 = 5 \times 87 + 13 \times 214$
- $3313 = 13 \times 45 + 11 \times 248$
- $3361 = 11 \times 68 + 13 \times 201$
- $3433 = 7 \times 10 + 19 \times 177$
- $3457 = 5 \times 42 + 17 \times 191$
- $3529 = 13 \times 57 + 17 \times 164$
- $3673 = 5 \times 13 + 11 \times 328$
- $3697 = 5 \times 92 + 13 \times 249$
- $3769 = 17 \times 14 + 11 \times 321$
- $3793 = 19 \times 60 + 7 \times 379$
- $3889 = 11 \times 38 + 13 \times 267$
- $4057 = 29 \times 20 + 19 \times 183$
- $409 = 14 \times 19 + 11 \times 13$
- $4129 = 7 \times 29 + 13 \times 302$
- $4153 = 13 \times 102 + 11 \times 257$

- $4177 = 11 \times 45 + 7 \times 526$
- $4201 = 11 \times 38 + 13 \times 291$
- $4273 = 5 \times 58 + 7 \times 569$
- $4297 = 5 \times 19 + 11 \times 382$
- $4441 = 13 \times 70 + 11 \times 321$
- $4513 = 19 \times 15 + 7 \times 604$
- $4561 = 17 \times 110 + 13 \times 207$
- $4657 = 5 \times 46 + 19 \times 233$
- $4729 = 11 \times 93 + 17 \times 218$
- $4801 = 23 \times 21 + 17 \times 254$
- $4969 = 7 \times 152 + 11 \times 355$
- $4993 = 5 \times 57 + 11 \times 428$
- $5113 = 5 \times 93 + 7 \times 664$
- $5209 = 11 \times 306 + 19 \times 97$
- $5233 = 5 \times 17 + 11 \times 468$
- $5281 = 7 \times 38 + 17 \times 295$
- $5449 = 7 \times 95 + 13 \times 368$
- $5521 = 7 \times 89 + 31 \times 158$
- $5569 = 19 \times 68 + 13 \times 329$
- $5641 = 7 \times 172 + 29 \times 153$
- $5689 = 17 \times 132 + 13 \times 265$
- $5737 = 37 \times 20 + 19 \times 263$
- $5857 = 5 \times 78 + 7 \times 781$
- $5953 = 5 \times 7 + 11 \times 538$
- $6073 = 5 \times 29 + 19 \times 312$
- $6121 = 7 \times 87 + 13 \times 424$
- $6217 = 17 \times 15 + 11 \times 542$
- $6257 = 5 \times 56 + 43 \times 139$
- $6337 = 5 \times 61 + 13 \times 464$
- $6361 = 17 \times 21 + 19 \times 316$
- $6481 = 13 \times 342 + 11 \times 185$
- $6529 = 11 \times 141 + 19 \times 262$
- $6553 = 11 \times 280 + 23 \times 151$
- $6577 = 5 \times 69 + 19 \times 328$
- $6673 = 5 \times 308 + 29 \times 177$
- $6793 = 7 \times 235 + 11 \times 468$
- $6841 = 29 \times 67 + 31 \times 158$
- $6961 = 7 \times 104 + 23 \times 271$
- $7057 = 13 \times 80 + 11 \times 547$
- $7129 = 7 \times 374 + 13 \times 347$
- $7177 = 5 \times 38 + 17 \times 411$
- $7297 = 7 \times 15 + 29 \times 248$
- $7321 = 7 \times 312 + 11 \times 467$
- $7369 = 13 \times 201 + 29 \times 164$
- $7393 = 23 \times 29 + 19 \times 354$
- $7417 = 5 \times 17 + 13 \times 564$
- $7489 = 37 \times 70 + 23 \times 213$
- $7537 = 5 \times 51 + 11 \times 662$
- $7561 = 13 \times 73 + 29 \times 228$
- $7681 = 13 \times 102 + 31 \times 205$
- $7753 = 5 \times 416 + 31 \times 183$
- $7873 = 13 \times 10 + 29 \times 267$
- $7993 = 5 \times 88 + 7 \times 1079$
- $8017 = 19 \times 90 + 17 \times 371$
- $8089 = 17 \times 295 + 29 \times 106$
- $8161 = 7 \times 29 + 23 \times 346$
- $8209 = 13 \times 14 + 23 \times 349$
- $8233 = 17 \times 165 + 23 \times 236$
- $8329 = 31 \times 219 + 11 \times 140$

- $8353 = 5 \times 17 + 13 \times 636$
- $8377 = 13 \times 135 + 11 \times 602$
- $8521 = 13 \times 31 + 11 \times 738$
- $8641 = 7 \times 136 + 11 \times 699$
- $8689 = 29 \times 195 + 37 \times 82$
- $8713 = 5 \times 404 + 23 \times 291$
- $8737 = 37 \times 30 + 29 \times 263$
- $8761 = 19 \times 71 + 17 \times 436$
- $8929 = 13 \times 114 + 11 \times 677$
- $9001 = 13 \times 42 + 19 \times 445$
- $9049 = 11 \times 53 + 17 \times 498$
- $9433 = 13 \times 80 + 11 \times 763$
- $9433 = 13 \times 80 + 11 \times 763$
- $9601 = 13 \times 174 + 41 \times 179$
- $9649 = 41 \times 212 + 11 \times 87$
- $9697 = 11 \times 30 + 17 \times 551$
- $9721 = 11 \times 774 + 17 \times 71$
- $9769 = 17 \times 390 + 43 \times 73$
- $9817 = 5 \times 42 + 13 \times 739$
- $9857 = 17 \times 345 + 23 \times 382$
- $9929 = 23 \times 57 + 13 \times 696$
- $9961 = 7 \times 292 + 11 \times 671$
- $10009 = 11 \times 105 + 19 \times 466$
- $10081 = 11 \times 119 + 13 \times 751$
- $10153 = 7 \times 211 + 17 \times 596$
- $10169 = 17 \times 329 + 19 \times 404$
- $10273 = 5 \times 238 + 31 \times 293$
- $10321 = 7 \times 41 + 29 \times 346$
- $10369 = 13 \times 207 + 11 \times 698$
- $10513 = 5 \times 28 + 11 \times 943$
- $10657 = 29 \times 353 + 7 \times 60$
- $10729 = 41 \times 53 + 23 \times 372$
- $10753 = 5 \times 351 + 11 \times 818$
- $10837 = 11 \times 24 + 31 \times 349$
- $10889 = 7 \times 269 + 11 \times 784$
- $10993 = 5 \times 156 + 7 \times 1459$
- $11057 = 7 \times 107 + 19 \times 573$
- $11113 = 5 \times 611 + 17 \times 474$
- $11161 = 7 \times 66 + 13 \times 823$
- $11257 = 17 \times 190 + 23 \times 349$
- $11329 = 11 \times 140 + 13 \times 753$
- $11353 = 7 \times 19 + 17 \times 660$
- $11489 = 11 \times 65 + 13 \times 884$
- $11497 = 7 \times 60 + 11 \times 1007$
- $11593 = 11 \times 40 + 19 \times 587$
- $11617 = 13 \times 245 + 17 \times 496$
- $11689 = 7 \times 264 + 13 \times 757$
- $11777 = 13 \times 37 + 17 \times 692$
- $11833 = 7 \times 20 + 11 \times 1063$
- $11849 = 11 \times 39 + 13 \times 913$
- $11897 = 11 \times 92 + 19 \times 573$
- $11953 = 5 \times 22 + 13 \times 911$
- $12049 = 19 \times 156 + 23 \times 395$
- $12073 = 7 \times 15 + 11 \times 1088$
- $12113 = 17 \times 32 + 13 \times 925$
- $12161 = 7 \times 103 + 11 \times 1024$
- $12241 = 13 \times 126 + 23 \times 461$
- $12289 = 19 \times 165 + 23 \times 398$
- $12377 = 7 \times 50 + 11 \times 112$

- $12377 = 7 \times 50 + 11 \times 1127$
- $12409 = 13 \times 63 + 19 \times 610$
- $12433 = 13 \times 160 + 17 \times 609$
- $12457 = 19 \times 330 + 23 \times 269$
- $12553 = 11 \times 230 + 13 \times 771$
- $12577 = 5 \times 126 + 13 \times 919$
- $12589 = 17 \times 469 + 31 \times 236$
- $12721 = 17 \times 52 + 19 \times 623$
- $12757 = 17 \times 29 + 23 \times 553$
- $12793 = 7 \times 120 + 11 \times 1163$
- $12841 = 23 \times 86 + 17 \times 639$
- $12889 = 11 \times 195 + 17 \times 632$
- $12953 = 5 \times 53 + 7 \times 1859$
- $13009 = 7 \times 23 + 11 \times 1168$
- $13033 = 5 \times 102 + 7 \times 1789$
- $13057 = 13 \times 201 + 7 \times 1511$
- $13177 = 7 \times 80 + 11 \times 1147$
- $13249 = 7 \times 13 + 17 \times 774$
- $13297 = 5 \times 153 + 13 \times 964$
- $13337 = 7 \times 316 + 11 \times 967$
- $13361 = 7 \times 324 + 13 \times 933$
- $13417 = 11 \times 40 + 19 \times 683$
- $13441 = 29 \times 110 + 17 \times 603$
- $13513 = 5 \times 126 + 13 \times 991$
- $13537 = 5 \times 63 + 11 \times 1202$
- $13633 = 5 \times 569 + 31 \times 348$
- $13681 = 11 \times 69 + 13 \times 994$
- $13729 = 17 \times 328 + 31 \times 263$
- $13873 = 11 \times 78 + 19 \times 685$
- $13921 = 11 \times 118 + 13 \times 971$
- $14081 = 11 \times 71 + 13 \times 1081$
- $14281 = 13 \times 124 + 41 \times 309$
- $14401 = 11 \times 145 + 19 \times 674$
- $14449 = 11 \times 62 + 13 \times 1059$
- $14593 = 11 \times 1123 + 5 \times 448$
- $14633 = 13 \times 339 + 7 \times 1973$
- $14681 = 7 \times 209 + 13 \times 1129$
- $14713 = 11 \times 399 + 29 \times 356$
- $14737 = 11 \times 80 + 31 \times 447$
- $14821 = 13 \times 49 + 17 \times 875$
- $14897 = 7 \times 31 + 11 \times 1349$
- $14929 = 11 \times 42 + 17 \times 851$
- $14969 = 11 \times 90 + 17 \times 879$
- $15017 = 17 \times 111 + 13 \times 1147$
- $15073 = 5 \times 366 + 41 \times 323$
- $15121 = 11 \times 129 + 31 \times 442$
- $15137 = 17 \times 72 + 13 \times 1169$
- $15193 = 17 \times 250 + 31 \times 353$
- $15217 = 7 \times 117 + 23 \times 626$
- $15241 = 11 \times 78 + 19 \times 757$
- $15289 = 17 \times 469 + 31 \times 236$
- $15313 = 5 \times 281 + 19 \times 732$
- $15361 = 7 \times 305 + 17 \times 778$
- $15401 = 11 \times 129 + 19 \times 722$
- $15473 = 7 \times 32 + 11 \times 1381$
- $15493 = 13 \times 261 + 17 \times 598$
- $15581 = 7 \times 12 + 11 \times 1411$
- $15601 = 17 \times 56 + 19 \times 771$
- $15649 = 11 \times 492 + 29 \times 353$

- $15737 = 17 \times 69 + 11 \times 1403$
- $15761 = 7 \times 28 + 11 \times 1433$
- $15817 = 5 \times 577 + 53 \times 244$
- $15889 = 7 \times 374 + 23 \times 577$
- $15913 = 11 \times 70 + 19 \times 797$
- $15937 = 7 \times 165 + 19 \times 778$
- $15973 = 17 \times 18 + 13 \times 1227$
- $16033 = 7 \times 15 + 11 \times 1448$
- $16057 = 7 \times 60 + 19 \times 823$
- $16141 = 11 \times 24 + 17 \times 949$
- $16217 = 7 \times 136 + 13 \times 1151$
- $16249 = 11 \times 680 + 37 \times 237$
- $16273 = 5 \times 322 + 31 \times 473$ ■

Nosso objetivo será demonstrar que $\mathcal{O}_p$ não é euclidiano quando $p = 97$, 193, 241, 313, 337, 457 ou 601. Portanto ao final desta subseção teremos demonstrado

Teorema 6.81. *Um anel quadrático com discriminante $p \equiv 1 \pmod{24}$ é norma euclidiano apenas quando $p = 73$.*

Com isso finalizaremos a classificação de todos os anéis quadráticos.

O anel $\mathcal{O}_{97}$ não é norma euclidiano

O anel quadrático $\mathcal{O}_{97}$ tem uma história pouco usual. Em 1942, no trabalho [18], L. Rédei afirmou que $\mathcal{O}_{97}$ era um anel quadrático norma euclidiano, apesar de não ter fornecido nenhuma demonstração. A partir daí, $\mathcal{O}_{97}$ foi indevidamente classificado como um anel quadrático norma euclidiano até 1952 quando E.S. Barnes e H.P.F. Swinnerton-Dyer, em [25], demonstraram que de fato não era. Descreveremos a demonstração utilizada por E.S. Barnes e H.P.F. Swinnerton-Dyer.

Definição 6.82. Seja $f(x, y) = ax^2 + bxy + cy^2$ e seja

$$T = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

uma transformação unimodular inteira. Dizemos que T é um automorfo de $f(x, y)$ se $f \circ T = \pm f$.

Definição 6.83. Sejam t e u a solução fundamental da equação de Pell

$$t^2 - Du^2 = \pm 4.$$

Dizemos que

$$T_0 = \begin{pmatrix} \frac{1}{2}t - \frac{1}{2}bu & -cu \\ au & \frac{1}{2}t + \frac{1}{2}bu \end{pmatrix} \tag{6.112}$$

é o automorfo fundamental.

Antes de iniciarmos o próximo resultado, introduziremos uma notação. Para pontos em $\mathbb{R}^2$, Utilizaremos a notação $(x, y) \equiv (u, v) \pmod 1$ quando $x \equiv u \pmod 1$ e $y \equiv v \pmod 1$ (veja a observação 4.14).

Proposição 6.84. *Seja T um automorfo de $f(x,y) = ax^2 + bxy + cy^2$ dado por 6.112, onde $t^2 - Du^2 = \pm 4,\ t > 0,\ u > 0$. Suponha $\{P_i\}$, $i = 1, \ldots, N$, um conjunto finito de pontos em $\mathbb{R}^2$ incongruentes módulo 1 tal que $\{T(P_i)\}$ é uma permutação de $\{P_i\}$. Suponha ainda que*

$$M(f; P_i) < K,\ i = 1, \ldots, N.$$

Então existe um ponto (x,y) com as seguintes propriedades:

1. $(x,y) \equiv P_i \pmod 1$*, para algum i;*
2. $|f(x,y)| < K$*;*
3. $\begin{cases} Dy^2 < K|a|(t+2), \text{ se } t^2 - Du^2 = 4; \\ ty^2 < K|a|u^2, \text{ se } t^2 - Du^2 = -4. \end{cases}$

Demonstração: Considere o conjunto dos pontos satisfazendo os itens 1 e 2. Desde que existe um número finito de pontos P_i, nós podemos escolher um par (x,y) nesse conjunto de tal forma que $|y|$ seja mínimo. O teorema estará provado se mostrarmos que esse valor $|y|$ satisfaz o item 3. Suponhamos que y não satisfaz essa condição. Então, considerando o caso $t^2 - Du^2 = 4$, temos

$$Dy^2 \geq K|a|(t+2). \tag{6.113}$$

Observe que podemos supor $a > 0$, uma vez que poderíamos trocar $f(x,y)$ por $-f(x,y)$, assim faremos. Também, como $f(-x,-y) = f(x,y)$, podemos supor $y > 0$ em 6.113. Então temos

$$|f(x,y)| < K \leq \frac{Dy^2}{a(t+2)},$$

isto é,

$$\left| \left(x + \frac{b}{2a} y \right)^2 - \frac{Dy^2}{a^2(t+2)} \right| < \frac{Dy^2}{a(t+2)},$$

ou

$$\frac{Dy^2}{4a^2} \left(1 - \frac{4}{t+2} \right) < \left(x + \frac{b}{2a} y \right)^2 < \frac{Dy^2}{4a^2} \left(1 + \frac{4}{t+2} \right).$$

Substituindo D por $\frac{t^2-4}{u^2}$ e simplificando, obtemos

$$\frac{y^2(t-2)^2}{4a^2u^2} < \left(x + \frac{b}{2a} y \right)^2 < \frac{y^2(t-2)(t+6)}{4a^2u^2} < \frac{y^2(t+2)^2}{4a^2u^2},$$

ou ainda

$$\frac{y(t-2)}{2au} < \left| x + \frac{b}{2a} y \right| < \frac{y(t+2)}{2au}. \tag{6.114}$$

Dessa forma temos duas possibilidades:

$$\frac{y(t-2)}{2au} < x + \frac{b}{2a} y < \frac{y(t+2)}{2au},$$

que resulta em

$$\left| aux - \frac{1}{2}(t - bu)y \right| < y \tag{6.115}$$

ou

$$\frac{y(t-2)}{2au} < -x - \frac{b}{2a} y < \frac{y(t+2)}{2au},$$

que por sua vez implica em

$$\left|aux + \frac{1}{2}(t + bu)y\right| < y. \tag{6.116}$$

Como a coordenada y de $T(x, y)$ e $T^{-1}(x, y)$ são $aux + \frac{1}{2}(t + bu)y$ e $-aux + \frac{1}{2}(t - bu)y$, respectivamente, e pela a hipótese, cada ponto de $T(x, y)$ e $T^{-1}(x, y)$ é congruente a algum ponto de P_i, então, uma vez que 6.115 ou 6.116 é satisfeito, há um ponto satisfazendo os itens 1 e 2 da hipótese com o menor valor possível de $|y|$, o que contradiz a escolha inicial de y.

Agora, consideremos o caso $t^2 - Du^2 = -4$. Então, segue

$$ty^2 \geq K|a|u^2,$$

como fizemos acima, podemos supor $a > 0,\ y > 0$. Então

$$|f(x, y)| < K \leq \frac{ty^2}{au^2},$$

isto é,

$$\frac{y^2}{4a^2}\left(D - \frac{4t}{u^2}\right) < \left(x + \frac{b}{2a}y\right)^2 < \frac{y^2}{4a^2}\left(D + \frac{4t}{u^2}\right).$$

Agora substituindo D por $\frac{t^2+4}{u^2}$ e fazendo as devidas manipulações obtemos 6.115. O restante da prova pode ser completado como anteriormente. ■

Teorema 6.85. *Se $f(x, y) = N_{97}(x, y) = x^2 + xy - 24y^2$, então*

$$M\left(f; \frac{374}{1401}, \frac{2587}{5604}\right) = \frac{3001}{2802}. \tag{6.117}$$

Em particular $\mathcal{O}_{97}$ não é norma euclidiano.

Demonstração: Escreva

$$P = \left(\frac{374}{1401}, \frac{2587}{5604}\right),\ K = \frac{3001}{2802}$$

Como

$$f\left(2 + \frac{374}{1401}, \frac{2587}{5604}\right) = K$$

temos

$$M(f; P) \leq K$$

Portanto, se 6.117 é falso, existirá uma solução de

$$|f(x, y)| < K,\ (x, y) \equiv P \pmod 1 \tag{6.118}$$

Agora aplicamos a Proposição 6.84. O automorfo fundamental de f é

$$T = \begin{pmatrix} 5035 & 27312 \\ 1138 & 6173 \end{pmatrix}$$

correspondendo a solução $t = 11208$, $u = 1138$ de $t^2 - 97u^2 = -4$. Por uma verificação simples temos

$$T(P) = (13295, 3153) + P \equiv P \pmod 1.$$

A Proposição 6.84 nos mostra que se 6.118 possui solução, então terá uma solução satisfazendo

$$y^2 < \frac{3001}{2802}\frac{u^2}{t} = \frac{971606761}{(2802)^2},$$

logo

$$|y| < \frac{31171}{2802} < 11 + \frac{2587}{5604} \tag{6.119}$$

Para provarmos o teorema, é suficiente mostrarmos que a inequação $|f(x,y)| < K$ não possui solução com

$$x = u + \frac{374}{1401},\ y = v + \frac{2587}{5604},$$

onde u, v são inteiros e, além disso, pela desigualdade 6.119,

$$-11 \leq y \leq 10. \tag{6.120}$$

Escreva

$$g(u,v) = f\left(u + \frac{374}{1401}, v + \frac{2587}{5604}\right) = u^2 + u\left(v + 1 - \frac{25}{5604}\right) - 24v^2 - \frac{30670}{1401}v - \frac{6893}{1401}.$$

Para cada v satisfazendo 6.120, é simples determinar o valor de u de forma que $|g(u,v)|$ seja mínimo. Vamos mostrar que em cada caso

$$|g(u,v)| \geq \frac{3001}{2802} = K.$$

$$g(u,0) = u^2 + \left(1 - \frac{25}{5604}\right)u - 476 - \frac{112}{1401},$$
$$|g(2,0)| = \frac{3001}{2802} = K;$$

$$g(u,1) = u^2 + \left(2 - \frac{25}{5604}\right)u - 50 - \frac{1137}{1401},$$
$$|g(-8,1)| = 2 - \frac{50}{1401} + \frac{1137}{1401} > 2;$$

$$g(u,2) = u^2 + \left(3 - \frac{25}{5604}\right)u - 144 - \frac{985}{1401},$$
$$|g(11,2)| = 10 + \frac{275}{5604} - \frac{985}{1401} > 9;$$

$$g(u,3) = u^2 + \left(4 - \frac{25}{5604}\right)u - 286 - \frac{833}{1401},$$
$$|g(-19,3)| = 1 + \frac{2855}{5604} > \frac{3}{2};$$

$$g(u,4) = u^2 + \left(5 - \frac{25}{5604}\right)u - 476 - \frac{681}{1401},$$
$$|g(-24,4)| = 20 - \frac{150}{5604} + \frac{681}{1401} > 20;$$

$$g(u,5) = u^2 + \left(6 - \frac{25}{5604}\right)u - 714 - \frac{529}{1401},$$
$$|g(24,5)| = 6 - \frac{150}{5604} - \frac{529}{1401} > 5;$$

$$g(u,6) = u^2 + \left(7 - \frac{25}{5604}\right)u - 1000 - \frac{377}{1401},$$
$$|g(-35,6)| = 20 - \frac{875}{5604} + \frac{377}{1401} > 20;$$

$$g(u,7) = u^2 + \left(8 - \frac{25}{5604}\right)u - 1334 - \frac{225}{1401},$$
$$|g(33,7)| = 19 - \frac{825}{5604} - \frac{225}{1401} > 18;$$

$$g(u,8) = u^2 + \left(9 - \frac{25}{5604}\right)u - 1716 - \frac{73}{1401},$$
$$|g(-46,8)| = 14 - \frac{1150}{5604} - \frac{73}{1401} > 13;$$

$$g(u,9) = u^2 + \left(10 - \frac{25}{5604}\right)u - 2146 + \frac{79}{1401},$$
$$|g(42,9)| = 38 - \frac{1050}{5604} - \frac{79}{1401} > 37;$$

$$g(u,10) = u^2 + \left(111 - \frac{25}{5604}\right)u - 2623 - \frac{1170}{1401},$$
$$|g(-57,10)| = 1 - \frac{1425}{5604} + \frac{1170}{1401} > \frac{3}{2};$$

$$g(u,-1) = u^2 - \frac{25}{5604}u - 7 - \frac{40}{1401},$$
$$|g(3,-1)| = 2 - \frac{75}{5604} - \frac{40}{1401} > \frac{3}{2};$$

$$g(u,-2) = u^2 - \left(1 + \frac{25}{5604}\right)u - 57 - \frac{192}{1401},$$
$$|g(-7,-2)| = 1 - \frac{175}{5604} + \frac{192}{1401} = \frac{6197}{5604} > K;$$

$$g(u,-3) = u^2 - \left(2 + \frac{25}{5604}\right)u - 156 - \frac{1057}{1401},$$
$$|g(14,-3)| = 12 - \frac{350}{5604} + \frac{1057}{1401} > 12;$$

$$g(u,-4) = u^2 - \left(3 + \frac{25}{5604}\right)u - 302 - \frac{905}{1401},$$
$$|g(19,-4)| = 2 - \frac{475}{5604} + \frac{905}{1401} > 2;$$

$$g(u,-5) = u^2 - \left(4 + \frac{25}{5604}\right) u - 496 - \frac{753}{1401},$$
$$|g(20,-5)| = 16 - \frac{500}{5604} - \frac{753}{1401} > 15;$$

$$g(u,-6) = u^2 - \left(5 + \frac{25}{5604}\right) u - 738 - \frac{601}{1401},$$
$$|g(30,-6)| = 12 - \frac{750}{5604} + \frac{601}{1401} > 12;$$

$$g(u,-7) = u^2 - \left(6 + \frac{25}{5604}\right) u - 1028 - \frac{449}{1401},$$
$$|g(-29,-7)| = 13 - \frac{725}{5604} - \frac{449}{1401} > 12;$$

$$g(u,-8) = u^2 - \left(7 + \frac{25}{5604}\right) u - 1366 + \frac{297}{1401},$$
$$|g(41,-8)| = 28 - \frac{1025}{5604} + \frac{297}{1401} > 28;$$

$$g(u,-9) = u^2 - \left(8 + \frac{25}{5604}\right) u - 1752 + \frac{145}{1401},$$
$$|g(-38,-9)| = 4 - \frac{950}{5604} - \frac{145}{1401} > 3;$$

$$g(u,-10) = u^2 - \left(9 + \frac{25}{5604}\right) u - 2186 - \frac{7}{1401},$$
$$|g(-42,-10)| = 44 - \frac{1050}{5604} + \frac{7}{1401} > 43;$$

$$g(u,-11) = u^2 - \left(9 + \frac{25}{5604}\right) u - 2668 - \frac{159}{1401},$$
$$|g(57,-11)| = 11 - \frac{1425}{5604} - \frac{159}{1401} > 10.$$

■

Os anéis $\mathcal{O}_{193}$, $\mathcal{O}_{241}$, $\mathcal{O}_{313}$, $\mathcal{O}_{337}$, $\mathcal{O}_{457}$ e $\mathcal{O}_{601}$ não são norma euclidianos

A partir daqui, demonstraremos que o anel quadrático $\mathcal{O}_d$ não é norma euclidiano para $d = 193, 241, 313, 337, 457, 601$. Para isso utilizaremos o método desenvolvido por H. Chatland e H. Davenport em [22], que é uma adaptação da teoria desenvolvida no Capítulo 5, que por sua vez é baseada no trabalho de H. Davenport desenvolvido em [9].

Teorema 6.86. *$\mathcal{O}_d$ não é norma euclidiano para*

$$d = 193,\ 241,\ 313,\ 337,\ 457,\ 601. \tag{6.121}$$

Como o método abordado na demonstração do teorema será uma adaptação da teoria desenvolvida no Capítulo 5, portanto, antes de tudo faremos uma recapitulação. Seja

$$f(x,y) = x^2 + xy - \frac{1}{4}(d-1)y^2$$

a forma-norma de $\mathbb{Q}(\sqrt{d})$, onde $d \equiv 1 \pmod 4$. Seja $\theta = \frac{1}{2}(1+\sqrt{d})$. Sejam $\theta_0 = \frac{1}{2}(u+\sqrt{d})$ e $\theta_0' = \frac{1}{2}(u-\sqrt{d})$, onde u é um inteiro ímpar escolhido de modo que

$$-0.618\cdots < \theta_0' < 0.382\ldots.$$

Os números nas últimas equações são $\frac{1}{2}(1-\sqrt{5})$ e $\frac{1}{2}(3-\sqrt{5})$. Claramente também temos $\theta_0 > 2$.

Seja $f_0(x,y) = (x+\theta_0 y)(x+\theta_0' y)$. Por meio do Lema 5.5, podemos encontrar uma cadeia de forma equivalentes

$$f_n(x,y) = a_n(x+\theta_n y)(x+\theta_n' y)$$

onde $\theta_n > 2$ e

$$-0.618\cdots \leq \theta_n' \leq 0.382\ldots.$$

Por comparação de discriminante temos

$$a_n(\theta_n - \theta_n') = \pm\sqrt{d}. \tag{6.122}$$

Essas formas estão conectadas pela relação de recorrência:

$$\theta_n = t_n + \frac{u_{n+1}}{\theta_{n+1}}, \theta_n' = t_n + \frac{u_{n+1}}{\theta_{n+1}'}, \tag{6.123}$$

onde t_n é o inteiro mais próximo de θ_n e u_n é o sinal oposto de θ_n'. Os números $a_n, \theta_n, \theta_n', t_n, u_n$ existem para todo inteiro n, (positivo, negativo e zero), e são periódicos com certo período N.

Argumentando de forma parecida ao que fizemos para obter a expressão 5.41, para demonstrar que o anel quadrático $\mathcal{O}_d$ não é norma euclidiano, é suficiente construir um elemento $\beta_0 \in \mathbb{Q}(\sqrt{d})$ tal que

$$|(x+\theta_0 y+\beta_0)(x+\theta_0' y+\beta_0')| \geq 1 \tag{6.124}$$

para todos inteiros x, y. A construção de β_0 será baseada na escolha de um conjunto de inteiros v_n, também com período N. Originalmente, no Capítulo 5, a escolha de v_n era feita por $v_n = \left\lfloor \frac{1}{2}\theta_n \right\rfloor$, no entanto essa escolha não nos levaria ao resultado desejado nos seis casos considerados. A escolha de v_n será feira separadamente de acordo com cada caso listado em 6.121. Aqui, também definiremos em termos de v_n

$$\beta_n = v_n + \frac{u_{n+1}}{\theta_{n+1}} v_{n+1} + \frac{u_{n+1}u_{n+2}}{\theta_{n+1}\theta_{n+2}} v_{n+2} + \ldots.$$

Como $\theta_n > 2$ e v_n são periódicos, essa série converge absolutamente. Além disso, no Lema 5.21 provamos que β_n é um elemento de $\mathbb{Q}(\sqrt{d})$ e seu conjugado β_n' é dado por

$$\beta_n' = v_{n-1}|\theta_n'| - v_{n-2}|\theta_n'\theta_{n-1}| + v_{n-3}||\theta_n'\theta_{n-1}\theta_{n-2}| - \ldots$$

Teorema 6.87. *Suponhamos que o inteiros v_n possam ser escolhidos de forma que para todo n*

$$1 < \beta_n < \theta_n,\ 0 < \beta'_n < 1,\ \theta'_n < \beta'_n < 1,\ \beta'_n - \theta'_n < 1, \tag{6.125}$$

$$\beta_n \beta'_n |a_n| > 1, \tag{6.126}$$

$$(\theta_n - \beta_n)(\beta'_n - \theta'_n)|a_n| > 1, \tag{6.127}$$

$$(\theta_n - \beta_n)(\beta'_n - \theta'_n)|a_n| > 1, \tag{6.128}$$

$$(1 + \theta_n - \beta_n)(1 + \beta'_n - \theta'_n)|a_n| > 1. \tag{6.129}$$

Então, o algoritmo de Euclides não é válido.

Demonstração: Suponhamos que existam inteiros x_0, y_0 que contradigam 6.124, ou seja,

$$|(x + \theta_0 y + \beta_0)(x + \theta'_0 y + \beta'_0)| < 1. \tag{6.130}$$

Defina

$$L_n(x, y) = x + \theta_n y + \beta_n,\ L'_n(x, y) = x + \theta'_n y + \beta'_n.$$

Das relações de recorrências satisfeitas por θ_n e β_n podemos encontrar a relação

$$L_n(x, y) = x + \left(t_n + \frac{u_{n+1}}{\theta_{n+1}}\right) y + v_n + \frac{u_{n+1}}{\theta_{n+1}} \beta_{n+1}$$

$$= \frac{u_{n+1}}{\theta_{n+1}} L_{n+1}(y, u_{n+1}(x + t_n y + v_n)).$$

Uma relação similar acontece para o caso L'_n, isto é,

$$L'_n(x, y) = \frac{u_{n+1}}{\theta'_{n+1}} L'_{n+1}(y, u_{n+1}(x + t_n y + v_n)).$$

Portanto, ao iniciarmos nossa sequência com os inteiros x_0, y_0 e definirmos inteiros x_n, y_n, para $n > 0$ e $n < 0$, pela relação de recorrência

$$x_{n+1} = y_n,\ y_{n+1} = u_{n+1}(x + t_n y + v_n),$$

obtemos a recorrência

$$|L_n(x_n, y_n)| = \frac{1}{\theta_{n+1}} |L_{n+1}(x_{n+1}, y_{n+1})| \tag{6.131}$$

para todo inteiro n.

A partir das relações 6.123 e 6.122 podemos chegar em

$$\frac{1}{\theta_{n+1}\theta'_{n+1}} = \pm \frac{\theta_n - \theta'_n}{\theta_{n+1} - \theta'_{n+1}} \text{ e } |a_{n+1}(\theta_{n+1} - \theta'_{n+1})| = |a_n(\theta_n - \theta'_n)|,$$

respectivamente, e a partir das relações acima podemos mostrar que

$$|a_{n+1} L_{n+1}(x_{n+1}, y_{n+1}) L'(x_{n+1}, y_{n+1})| = |a_{n+1}\theta_{n+1}\theta'_{n+1}||L_n(x_n, y_n) L'(x_n, y_n)| =$$

$$= |a_n L_n(x_n, y_n) L'(x_n, y_n)|,$$

ou seja, a expressão $|a_n L_n(x_n, y_n) L'(x_n, y_n)|$ é independe do valor de n. Em particular, pela desigualdade 6.130,

$$|a_n L_n(x_n, y_n) L'(x_n, y_n)| < 1 \tag{6.132}$$

para todo inteiro n.

Primeiro suponhamos $L_0(x_0, y_0) \neq 0$. Então, pela identidade 6.131, $|L_n(x_n, y_n)|$ aumenta gradualmente de 0 a $+\infty$ à medida que n aumenta de $-\infty$ a $+\infty$. Dessa forma, haverá exatamente um valor n tal que

$$|L_{n-1}(x_{n-1}, y_{n-1})| \leq d^{-\frac{1}{4}} < |L_n(x_n, y_n)|. \tag{6.133}$$

Então, por 6.131,

$$|L_n(x_n, y_n)| = \theta_n |L_{n-1}(x_{n-1}, y_{n-1})| \leq d^{-\frac{1}{4}}\theta_n. \tag{6.134}$$

Além disso, por 6.132 e 6.122,

$$|L'(x_n, y_n)| < |a_n L_n(x_n, y_n)|^{-1} < d^{\frac{1}{4}}|a_n|^{-1} = d^{-\frac{1}{4}}(\theta_n - \theta'_n). \tag{6.135}$$

Agora, suponha $L_0(x_0, y_0) = 0$. Como $(L_0(x_0, y_0)) = L'_0(x_0, y_0)$, então, claramente, $L'_0(x_0, y_0) = 0$. Além disso, pela recorrência 6.131, $L_n(x_n, y_n) = 0$ para todo n, e procedendo de maneira análoga ao caso de índice 0, $L'_n(x_n, y_n) = 0$ para todo n. Assim, neste caso, as inequações 6.132, 6.134 e 6.135 são todas satisfeitas para qualquer n.

Agora eliminamos os índices de x e y, e reescrevemos as inequações como

$$|a_n(x + \theta_n y + \beta_n)(x + \theta_n y + \beta'_n)| < 1, \tag{6.136}$$

$$|x + \theta_n y + \beta_n| \leq d^{-\frac{1}{4}}\theta_n, \tag{6.137}$$

$$|x + \theta'_n y + \beta'_n| < d^{-\frac{1}{4}}(\theta_n - \theta'_n). \tag{6.138}$$

Se $y \geq 1$ ou $y \leq -2$, combinamos 6.137 e 6.138 por subtração e obtemos

$$|(\theta_n - \theta'_n)y + (\beta_n - \beta'_n)| < d^{-\frac{1}{4}}(2\theta_n - \theta'_n).$$

Por 6.125, também podemos concluir que $0 < \beta_n - \beta'_n < \theta_n - \theta'_n$. Portanto, se $y \geq 1$ ou $y \leq -2$, obtemos

$$\theta_n - \theta'_n < d^{-\frac{1}{4}}(2\theta_n - \theta'_n).$$

No entanto, se $d^{\frac{1}{4}} > 3$, isso é impossível, pois implicaria em $3(\theta_n - \theta'_n) < 2\theta_n - \theta'_n$, isto é, $\theta_n < 2\theta'_n$, contradizendo $\theta_n > 2$ e $\theta_n > 2$ e $\theta'_n \leq 0.382\ldots$.

Se $y = 0$, a inequação 6.136 torna-se

$$|a_n(x + \beta_n)(x + \beta'_n)| < 1.$$

Agora, β'_n pertence ao intervalo $[0, 1]$ e β_n estará entre v_n e $v_n + u_{n+1}$, uma vez que

$$\beta_n = v_n + u_{n+1}\frac{\beta_{n+1}}{\theta_{n+1}}.$$

Portanto, se a última inequação é satisfeita por um inteiro x também deverá ser satisfeita quando x é substituído por algum dos quatro valores

$$0, -1, -v_n, -v_n - u_{n+1}.$$

De fato, considere a equação quadrática $q(x) = a_n(x + \beta_n)(x + \beta'_n)$. As raízes de $q(x)$ são $-\beta_n$ e $-\beta'_n$. Como valores 0, -1, $-v_n$ e $-v_n - u_{n+1}$ são números inteiros, então no intervalo aberto extremos 0 e -1 não haverá nenhum inteiro, bem como no intervalo aberto de extremos $-v_n$ e $-v_n - u_{n+1}$. Agora, como x é um inteiro e $0 < \beta'_n < 1$ e β_n

pertence ao intervalo de extremos v_n e $v_n + u_{n+1}$, então algum dos números 0, -1, $-v_n$ e $-v_n - u_{n+1}$ estará entre x e uma das raízes de $q(x)$, chamando esse número de p, podemos concluir que $|q(p)| < |q(x)|$, de onde concluímos a afirmação.

Agora, vamos demonstrar que cada um desses quatro valores nos leva a um absurdo. Os primeiros dois valores, isto é, 0 e -1, nos leva a uma desigualdade que contradiz 6.126 e 6.127. Os dois últimos, $-v_n$ e $-v_n - u_{n+1}$, nos leva a

$$a_n|(v_n - \beta_n)(v_n - \beta'_n)| < 1 \text{ ou } |a_n(v_n + u_{n+1} - \beta_n)(v_n + u_{n+1}\beta'_n)| < 1.$$

Usando a relação de recorrência para β_n e β'_n e a relação

$$|a_n| = |\theta_{n+1}\theta'_{n+1}a_{n+1}|, \tag{6.139}$$

segue, de 6.122,

$$|a_{n+1}\beta_{n+1}\beta'_{n+1}| < 1 \text{ ou } |a_{n+1}(\theta_{n+1} - \beta_{n+1})(\theta'_{n+1} - \beta'_{n+1})| < 1$$

o que contradiz 6.126 e 6.128.

Se $y = -1$, a inequação 6.136 torna-se

$$|a_n(x - \theta_n + \beta_n)(x - \theta'_n + \beta'_n)| < 1.$$

Vamos mostrar que não pode ocorre $|x - \theta_n + \beta_n| < 1$ ou $|x - \theta'_n + \beta'_n| < 1$. Visto que $0 < \beta'_n - \theta'_n < 1$, por 6.125, os únicos valores de x que satisfazem $|x - \theta'_n + \beta'_n| < 1$ são $x = 0$ e $x = -1$. Mas esses valores nos levam à contradições em relação a 6.128 e 6.129. Com relação à desigualdade $|x - \theta_n + \beta_n| < 1$, utilizando as identidades

$$\theta_n - \beta_n = t_n - v_n - \frac{u_{n+1}}{\theta_{n+1}}(\beta_{n+1} - 1), \tag{6.140}$$

podemos concluir que os únicos valores possíveis para x são $t_n - v_n$ e $t_n - v_n - u_{n+1}$. nestes casos obteremos

$$|a_n(t_n - v_n - \theta_n + \beta_n)(t_n - v_n - \theta'_n + \beta'_n)| < 1$$

ou

$$|a_n(t_n - v_n - u_{n+1} - \theta_n + \beta_n)(t_n - v_n - u_{n+1} - \theta'_n + \beta'_n)| < 1.$$

Usando a relações de recorrência 6.139 e 6.140, as desigualdades acima tornam-se

$$|a_{n+1}(\beta_{n+1} - 1)(\beta_{n+1} - 1)| < 1$$

e

$$|a_n(1 + \theta_{n+1} - \beta_{n+1})(1 + \theta'_{n+1} - \beta_{n+1} - 1)| < 1,$$

o que contradiz 6.127 e 6.129. Isso prova que as inequações 6.136, 6.137 e 6.138 não podem ser satisfeitas por nenhum par x, y de inteiros, o que finaliza a demonstração do teorema. ■

Para mostrar que o algoritmo de Euclides não é válido nos seis casos será suficiente exibir inteiros v_n, para um período completo, de forma a hipótese do Teorema 6.87 seja satisfeita. Os valores v_n, juntamente com os resultantes valores de β_n e β'_n, são dados nas seguintes tabelas. Usaremos P_n, Q_n, R_n e S_n para denotar os produtos 6.126, 6.127, 6.128 e 6.129, respectivamente. Será visto em cada caso que são todos maiores que 1 e as condições de 6.125 são todas satisfeitas.

n	θ_n	θ'_n	v_n	β_n	β'_n	$\lvert a_n \rvert$	P_n	Q_n	R_n	S_n
0	13.446	-0.446	6	6.703	0.271	1	1.82	4.16	4.84	2.19
1	2.241	-0.074	1	1.575	0.426	6	4.03	1.98	2.00	4.99
2	4.149	-0.482	2	2.385	0.277	3	1.98	3.01	4.01	2.00
3	6.723	-0.223	3	2.592	0.384	2	1.99	1.96	5.02	4.03
4	3.612	0.138	2	1.475	0.362	4	2.14	1.21	1.91	9.74
5	2.574	0.259	2	1.351	0.424	6	3.44	1.21	1.21	11.14
6	2.350	0.365	1	1.524	0.575	7	6.13	1.56	1.21	10.09
7	2.862	-0.612	2	1.501	0.260	4	1.56	1.48	4.74	1.21
8	7.223	0.277	3	3.607	0.482	2	3.48	2.70	1.48	7.34
9	4.482	-0.149	2	2.722	0.375	3	3.06	3.23	2.76	3.95
10	2.074	-0.241	1	1.498	0.392	6	3.52	1.82	2.19	3.47

Tabela 6.12: $d = 193$

n	θ_n	θ'_n	v_n	β_n	β'_n	$\lvert a_n \rvert$	P_n	Q_n	R_n	S_n
0	15.262	-0.262	7	7.396	0.396	1	2.93	3.86	5.18	3.03
1	3.816	-0.066	2	1.510	0.433	4	2.61	1.16	4.60	6.64
2	5.421	0.246	2	2.658	0.386	3	3.07	3.06	1.16	9.71
3	2.377	-0.210	1	1.564	0.340	6	3.19	2.23	2.68	4.90
4	2.652	-0.452	2	1.495	0.299	5	2.23	1.74	4.35	2.68
5	2.877	0.290	2	1.453	0.493	6	4.29	1.38	1.74	11.59
6	8.131	0.369	4	4.451	0.556	2	4.95	3.06	1.38	7.61
7	7.631	-0.131	4	3.442	0.451	2	3.11	2.68	4.88	4.33
8	2.710	0.123	2	1.513	0.436	6	3.96	1.74	2.25	9.05
9	3.452	0.348	1	1.680	0.543	5	4.56	1.55	1.74	11.15
10	2.210	-0.377	1	1.502	0.172	6	1.55	2.50	2.33	4.62
11	4.754	-0.421	3	2.389	0.348	3	2.50	2.72	5.46	2.33
12	4.066	0.184	2	2.485	0.489	4	4.86	3.03	1.93	7.18

Tabela 6.13: $d = 241$

n	θ_n	θ'_n	v_n	β_n	β'_n	$\lvert a_n \rvert$	P_n	Q_n	R_n	S_n
0	17.346	-0.346	8	8.525	0.520	1	4.44	3.61	7.64	1.31
1	2.891	-0.058	2	1.517	0.431	6	3.92	1.76	4.03	7.28
2	9.173	0.327	4	4.431	0.513	2	4.55	3.34	1.76	9.35
3	5.782	-0.115	3	2.494	0.402	3	3.01	2.68	5.10	6.21
4	4.586	0.164	3	2.319	0.425	4	3.94	3.04	2.37	9.65
5	2.418	0.207	1	1.646	0.532	8	7.01	2.42	2.01	9.56
6	2.391	-0.558	1	1.545	0.261	6	2.42	2.42	4.16	2.01
7	2.558	-0.391	2	1.393	0.289	6	2.42	1.68	4.75	4.16
8	2.261	0.295	1	1.373	0.505	9	6.23	1.66	1.68	13.43
9	3.836	-0.586	2	1.431	0.291	4	1.66	1.22	8.44	1.68
10	6.115	0.218	3	3.483	0.373	3	3.89	4.67	1.22	9.21
11	8.673	-0.173	5	4.185	0.454	2	3.80	3.48	5.63	4.09
12	3.058	0.109	2	2.491	0.496	6	7.41	4.51	1.31	5.76

Tabela 6.14: $d = 313$

n	θ_n	θ'_n	v_n	β_n	β'_n	$\lvert a_n \rvert$	P_n	Q_n	R_n	S_n
0	18.679	0.321	9	8.233	0.512	1	4.22	3.53	2.00	9.26
1	3.113	0.054	2	2.387	0.454	6	6.51	4.54	1.75	6.20
2	8.839	-0.339	4	3.421	0.525	2	3.59	2.30	9.36	1.75
3	6.226	0.107	3	3.602	0.372	3	4.02	4.90	2.09	7.99
4	4.420	-0.170	2	2.660	0.446	4	4.75	3.68	4.33	4.24
5	2.383	-0.240	1	1.574	0.373	7	4.11	2.52	3.47	4.91
6	2.613	-0.446	2	1.499	0.280	6	2.52	2.16	4.86	3.47
7	2.585	0.290	2	1.295	0.499	8	5.17	1.18	2.16	14.49
8	2.409	0.369	1	1.697	0.554	9	8.46	2.80	1.18	12.55
9	2.446	-0.613	1	1.706	0.274	6	2.80	3.08	3.94	1.18
10	2.240	-0.383	1	1.582	0.278	7	3.08	2.94	3.04	3.94
11	4.170	-0.420	2	2.427	0.303	4	2.94	3.98	5.04	3.04
12	5.893	-0.226	3	2.515	0.384	3	2.90	2.80	6.18	5.12
13	9.339	0.161	4	4.529	0.420	2	3.81	4.09	2.50	8.60
14	2.946	-0.113	2	1.559	0.405	6	3.79	2.00	4.31	6.90

Tabela 6.15: $d = 337$

n	θ_n	θ'_n	v_n	β_n	β'_n	$\lvert a_n \rvert$	P_n	Q_n	R_n	S_n
0	21.189	-0.189	10	10.711	0.104	1	1.11	8.71	3.06	8.12
1	5.297	-0.047	3	3.765	0.467	4	7.03	5.89	3.15	4.92
2	3.365	-0.198	2	2.573	0.502	6	7.75	4.70	3.32	3.22
3	2.741	-0.313	2	1.572	0.468	7	5.15	2.13	6.39	3.32
4	3.865	0.302	2	1.654	0.462	6	4.59	2.11	2.13	16.17
5	7.396	0.270	2	2.559	0.416	3	3.19	2.73	2.11	14.97
6	2.524	-0.149	2	1.410	0.235	8	2.66	2.51	3.42	10.42
7	2.099	0.318	1	1.239	0.560	12	8.33	1.26	2.51	16.90
8	10.094	-0.594	2	2.409	0.261	2	1.26	2.08	13.15	2.51
9	10.594	-0.094	5	4.338	0.164	2	1.42	5.58	3.23	10.76
10	2.465	0.090	1	1.632	0.436	9	6.40	3.21	2.59	10.79
11	2.149	-0.524	1	1.358	0.295	8	3.21	2.02	5.18	2.59
12	6.730	-0.396	3	2.411	0.279	3	2.02	3.05	8.75	5.18
13	3.698	0.135	3	2.179	0.368	6	4.81	4.47	2.12	11.60
14	3.313	0.259	2	2.719	0.681	7	12.96	3.84	1.76	6.45
15	3.198	-0.365	2	2.298	0.481	6	6.63	4.04	4.57	1.76
16	5.047	-0.297	1	1.505	0.451	4	2.72	1.11	10.60	4.57

Tabela 6.16: $d = 457$

n	θ_n	θ'_n	v_n	β_n	β'_n	$\lvert a_n \rvert$	P_n	Q_n	R_n	S_n
0	24.758	0.242	12	12.802	0.373	1	4.78	7.40	1.57	11.26
1	4.126	0.040	3	3.309	0.470	6	9.32	7.35	2.10	6.22
2	7.919	-0.253	3	2.448	0.639	3	4.69	1.57	14.64	2.10
3	12.379	0.121	6	6.838	0.286	2	3.91	8.34	1.83	10.92
4	2.640	-0.084	3	2.213	0.481	9	9.58	5.67	2.17	5.58
5	2.776	0.324	3	2.184	0.817	10	17.84	2.17	2.91	8.08
6	4.460	0.374	3	3.639	0.816	6	17.82	2.91	2.18	6.09
7	2.176	-0.276	1	1.391	0.602	10	8.38	1.55	6.89	2.18
8	5.689	-0.439	3	2.222	0.175	4	1.55	4.03	8.52	6.89
9	3.220	0.155	2	2.504	0.439	8	8.79	6.75	1.62	9.84
10	4.552	-0.352	3	2.293	0.549	5	6.29	2.92	10.17	1.62
11	2.230	0.187	1	1.576	0.458	12	8.66	3.74	2.13	14.47
12	4.352	-0.552	2	2.505	0.299	5	3.74	5.28	7.85	2.13
13	2.845	-0.220	2	1.437	0.374	8	4.30	2.19	6.68	7.83
14	6.439	0.311	3	3.626	0.505	4	7.33	5.20	2.19	12.29
15	2.276	-0.176	1	1.425	0.439	10	6.25	2.39	5.23	7.14
16	3.626	-0.460	2	1.540	0.258	6	2.39	2.41	8.98	5.23
17	2.676	0.224	2	1.230	0.391	10	4.80	1.40	2.41	2.04
18	3.084	0.360	2	2.376	0.580	9	12.40	5.20	1.40	12.00
19	11.879	-0.379	5	4.470	0.538	2	4.81	3.21	13.59	1.40
20	8.253	0.081	4	4.375	0.360	3	4.73	6.47	3.25	10.54
21	3.960	-0.126	2	1.483	0.460	6	4.09	1.57	8.71	8.64

Tabela 6.17: $d = 601$

7 Conclusão

Este trabalho fornece uma descrição abrangente e detalhada da classificação dos anéis quadráticos norma euclidianos. Ao meu ver, os principais benefícios resultante deste trabalho são reunir resultados apresentados em diferentes trabalhos relacionado ao tema em uma ordem lógica e natural e unificar suas terminologias e notações.

Quanto as perspectivas futuras, problemas semelhantes, no entanto, de características mais gerais, encontram-se em aberto, como por exemplo o problema de classificação de anéis quadráticos que são domínios de fatoração única ou o problema de classificação de anéis quadráticos euclidiano.

Referências

[1] GARCIA, A., LEQUAIN, Y. *Elementos de álgebra*. 6. ed. Rio de Janeiro: IMPA, 2015. 326 p.

[2] ENDLER, Otto. *Teoria dos números algébricos*. 2. ed. Rio de Janeiro: IMPA, 2014. 199 p.

[3] STEWART, I., TALL, D. *Algebraic Number Theory and Fermat's Last Theorem*. 3. ed. Natick: A K Peters, 2001.

[4] MARTINEZ, F. E. B. et al. *Teoria dos Números: um passeio com primos e outros números familiares pelo mundo inteiro*. 4. ed. Rio de Janeiro: IMPA, 2015.

[5] ALACA, S.; WILLIAMS, K. S. *Introductory Algebraic Number Theory*. 1. ed. New York: Cambridge University Press, 2004.

[6] LEMMERMEYER, F. *Quadratic Number Fields*. 1. ed. Springer Cham, 2021. 343 p.

[7] VARNAVIDES, P. *The Euclidean real quadratic number fields*, Indag. Math. v. 14, p. 111-112, 1952.

[8] VARNAVIDES, P. *Note on non-homogeneous quadratic forms*, Quart. J. Math. Oxford v. 19, p.54-58, 1948.

[9] DAVENPORT, H. *Indefinite binary quadratic forms and Euclid's algorithm in real quadratic fields*, Proc. London Math. Soc. v. 53, n. 2, p. 65-82, 1951.

[10] RÉDEI, L. Über, *Die quadratischen Zahlkörper mit Primzerlegung* Acta Sci. Math. (Szeged) v. 21, p. 1-3, 1960.

[11] EGGLETON, R. B., LACAMPAGNE, C. B., SELFRIDGE, J. L., *Euclidean Quadratic Fields*, Amer. Math. Monthly, v. 99, p. 829–837, 1992.

[12] HOFREITER, N. *Quadratische Zahlkörper mit und ohne Euklidischen Algorithmus*, Monatsh. Math. Phys. v. 42, p. 397–400, 1935.

[13] SCHUSTER, L. *Reellquadratische Zahlkörper ohne Euklidischen Algorithmus*, Monatsh. Math. Phys. v. 47, p. 117–127, 1938.

[14] BEHRBOHM, H., RÉDEI, L. *Der Euklidische Algorithmus in quadratischen Zahlkörpern*, J. Reine Angew. Math. v. 174, p. 192–205, 1936.

[15] BRAUER, A. *On the non-existence of the Euclidean algorithm in certain quadratic number fields*, Amer. J. Math. v. 62, n. 1, p. 697-716, 1940.

[16] BRAUER, A. *Über den kleinsten quadratischen Nichtrest*. Math Z v. 33, p. 161–176, 1931.

[17] RÉDEI, L. *Uber den Euklidischen Algorithmus in reellquadratischen Zahlkörpern*, J. Reine Angew. Math. v. 183, p. 183–192, 1941.

[18] RÉDEI, L. *Zur Frage des Euklidischen Algorithmus in quadratischen Zahlkörpern*, Math. Ann. v. 118, p. 588–608, 1942.

[19] JACOBSTHAL, E. *Anwendungen einer Formel aus der Theorie der quadratischen Reste*, Dissertação, Univ. Berlin, 1906.

[20] MATTHEWS, K. *Finding the fundamental unit of a real quadratic field*. Number Theory Web, Disponível em: http://www.numbertheory.org/php/unit.html, 2023.

[21] CHATLAND, H. *On the Euclidean algorithm in quadratic number fields*, Bull. Amer. Math. Soc. v. 55, p. 948–953, 1949.

[22] CHATLAND, H., DAVENPORT, H. *Euclids algorithm in real quadratic fields*, Canad. J. Math. v. 2, p. 289–296, 1950.

[23] HEILBRONN, H. *On Euclid's algorithm in real quadratic fields*, Proc. Cambridge Philos. Soc. vol. 34, p. 521-526, 1938.

[24] ERDÖS, P., Ko, C. *Note on the Euclidean algorithm*, J. London Math. Soc. v. 13, p. 3-8, 1938.

[25] BARNES, E.S., Swinnerton-Dyer, H.P.F. , *The inhomogeneous minima of binary quadratic forms I*, Acta Math. v. 87, p. 259–323, 1952.

[26] RAMÍREZ, V. V. *A new proof of the unique factorization of* $\mathbb{Z}[\frac{1+\sqrt{-d}}{2}]$ *for* $d = 3, 7, 11, 19{,}43, 67, 163$, Revista Colombiana de Matemáticas. v. 52, n.2, p. 139-143, 2016.

[27] STARK, H. M. *A complete determination of the complex quadratic fields of class-number one*, Michigan Math. J. v. 14, p. 1–27, 1967.

[28] DUBOIS, D. W., STEGER, A. *A note on the division algorithms in imaginary quadratic number fields*, Canad. J. Math. V. 19, P. 285-286, 1958.

[29] COLLISON, M. J. *The Unique Factorization Theorema: From Euclides to Gauss*, Mathematics Magazine. v. 53, n. 2, p. 96-100, 1980.