Anéis quadráticos euclidianos

José Fernandes Andrade

UFBA

O algoritmo euclidiano, também conhecido como algoritmo da divisão, é uma das propriedades mais importantes do conjunto dos números inteiros. Este algoritmo também é válido em outros anéis e é a condição principal para um anel ser euclidiano. Alguns livros didáticos voltados para o ensino de graduação, (por exemplo, [2], [6], [8], [9] e [12]), além do anel dos números inteiros e o dos polinômios em uma indeterminada sobre um corpo, apresentam um ou dois anéis quadráticos como exemplos de anéis euclidianos. Não encontramos, porém, na literatura em português, um estudo sistemático dos anéis quadráticos que são euclidianos. Um estudo neste sentido pode ser encontrado no texto clássico [11], que utiliza estruturas, terminologias e notações comuns à sua época.

O objetivo principal deste artigo é estudar os anéis quadráticos euclidianos. Começamos introduzindo os anéis quadráticos. Veremos na próxima seção que os anéis quadráticos são da forma $\mathbb{Z}[\theta]$ onde $\theta = \sqrt{m}$ se $m \equiv 2$ ou $m \equiv 3 \bmod 4$ e $\theta = \frac{1+\sqrt{m}}{2}$ se $m \equiv 1 \bmod 4$ e m é um inteiro livre de quadrado. O número de anéis quadráticos que são euclidianos é bem pequeno e eles estão completamente determinados: $\mathbb{Z}[\theta]$ é um anel euclidiano somente para os seguintes valores de m: $-11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73$. Neste artigo, vamos mostrar, por meio do algoritmo da divisão, que $\mathbb{Z}[\theta]$ é um anel euclidiano quando m assume os valores $-11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 13, 17, 21, 29$. As provas são construtivas e incluímos vários exemplos para esclarecer o seu funcionamento.

Para $m < 0$, isto é $m = -1, -2, -3, -7, -11$, as primeiras demonstrações apareceram no livro de Dickson ([7]) e no artigo de Perron ([15]). Para os valores positivos de m, o resultado é essencialmente devido a Chatland e Davenport ([5]). A lista completa dos valores de m para os quais $\mathbb{Z}[\theta]$ é um anel euclidiano apareceu inicialmente nos artigos de Inkeri ([13]) e Chatland ([4]), mas estranhamente com a inclusão indevida de $m = 97$. Barnes e Swinnerton ([1]) mostraram que para $m = 97$, $\mathbb{Z}[\theta]$ não é um anel euclidiano.

O texto foi elaborado de forma a poder ser utilizado como referência em disciplinas de álgebra no nível de graduação e também em atividades de iniciação científica.

1 Anéis quadráticos

Dizemos que um número complexo α é *algébrico* se existe um polinômio não nulo $f(X) \in \mathbb{Q}[X]$ tal que $f(\alpha) = 0$, em que $\mathbb{Q}[X] = \{a_n X^n + a_{n-1}X^{n-1} + \ldots + a_0; a_i \in \mathbb{Q}\}$ é o anel de polinômios em X com coeficientes em $\mathbb{Q}$. Neste caso, $\mathbb{Q}[\alpha] = \{f(\alpha); f(X) \in \mathbb{Q}[X]\}$ é um corpo algébrico. $\mathbb{Q}[\alpha]$ é um *corpo quadrático* quando α anula um polinômio de grau 2. O polinômio mônico de menor grau que anula α é chamado *polinômio mínimo* de α. É fácil verificar que o polinômio mínimo de α é único (veja, por exemplo, [10]).

Suponha que $\mathbb{Q}[\alpha]$ seja um corpo quadrático. Como α anula um polinômio de grau 2, α é da forma $\alpha = \frac{a+b\sqrt{m}}{c}$, com $a, b, c \in \mathbb{Z}$ e m livre de quadrado. Podemos supor também que a, b, c são primos entre si, isto é, $(a, b, c) = 1$. Segue que $b\sqrt{m} = c\alpha - a$, logo $mb^2 = (c\alpha - a)^2$ e α é raiz do polinômio $c^2X^2 - 2acX + a^2 - mb^2$. Na verdade, como $\mathbb{Q}[\alpha] = \mathbb{Q}[\sqrt{m}]$, todo elemento $\beta \in \mathbb{Q}[\alpha]$ também é da forma $\frac{a+b\sqrt{m}}{c}$ com $a, b, c \in \mathbb{Z}$ e, portanto, todo elemento $\beta \in \mathbb{Q}[\alpha]$ satisfaz uma equação de grau 2.

Apresentamos agora uma definição fundamental para o nosso artigo: $\alpha \in \mathbb{C}$ é um *inteiro algébrico* se α anula um polinômio mônico $X^n + a_{n-1}X^{n-1} + \ldots + a_0 \in \mathbb{Z}[X]$. Neste caso, dizemos também que α é *inteiro* ou *integral sobre* $\mathbb{Z}$.

Definimos então os inteiros de $\mathbb{Q}[\sqrt{m}]$ como sendo o conjunto dos inteiros algébricos que estão em $\mathbb{Q}[\sqrt{m}]$. Assim, um inteiro de $\mathbb{Q}[\sqrt{m}]$ é um elemento deste corpo que anula um polinômio mônico de grau 2 em $\mathbb{Z}[X]$

(para uma demonstração desse fato, veja o Apêndice no final do artigo).

Finalmente, para cada inteiro m livre de quadrado, o conjunto dos inteiros de $\mathbb{Q}[\sqrt{m}]$ é um anel chamado *anel quadrático*.

Seja $\alpha = \frac{a+b\sqrt{m}}{c}$ um inteiro de $\mathbb{Q}[\sqrt{m}]$, com $c > 0$ e $(a,b,c) = 1$.

Se $b = 0$, então $a/c \in \mathbb{Q}$ e como α é raiz de um polinômio mônico em $\mathbb{Z}[X]$, segue que $c = 1$ e $\alpha = a \in \mathbb{Z}$.

Se $b \neq 0$, então α anula o polinômio $X^2 - 2\frac{a}{c}X + \frac{a^2-mb^2}{c^2}$, e devido à unicidade do polinômio mínimo, este polinômio tem coeficientes em $\mathbb{Z}$ e, portanto, $c|2a$ e $c^2|(a^2 - mb^2)$. Seja $d = (a,c)$. Temos então que $d^2|a^2$ e $d^2|c^2$, logo $d^2|(a^2 - mb^2)$ e, portanto, $d^2|mb^2$. Como m é livre de quadrado, resulta que $d^2|b^2$ e finalmente, $d|b$. Como $(a,b,c) = 1$, segue que $d = 1$. Como $c|2a$ e $d = (a,c) = 1$, temos que $c|2$ e, consequentemente, só temos dois valores possíveis para c: $c = 1$ ou $c = 2$. Se $c = 2$ então a é ímpar, e como $4|(a^2 - mb^2)$, segue que $a^2 \equiv mb^2 \equiv 1 \bmod 4$. Logo b é ímpar e $m \equiv 1 \bmod 4$. Temos então dois casos:

1. Se $m \not\equiv 1 \bmod 4$ (i. e. $m \equiv 2,3 \bmod 4$), então $c = 1$ e os inteiros de $\mathbb{Q}[\sqrt{m}]$ são os elementos de $\mathbb{Z}[\sqrt{m}]$.

2. Se $m \equiv 1 \bmod 4$, os inteiros de $\mathbb{Q}[\sqrt{m}]$ são os elementos de $\mathbb{Z}[\theta]$, onde $\theta = \frac{1+\sqrt{m}}{2}$.

   Com efeito, se $c = 1$, então $a + b\sqrt{m} = a - b + 2b(\frac{1+\sqrt{m}}{2}) = a - b + 2b\theta \in \mathbb{Z}[\theta]$. Se $c = 2$, então a e b são ímpares e $\frac{a+b\sqrt{m}}{2} = \frac{a-b}{2} + \frac{b+b\sqrt{m}}{2} = \frac{a-b}{2} + b\theta \in \mathbb{Z}[\theta]$.

   Neste caso, os elementos de $\mathbb{Z}[\theta]$ podem ser escritos de uma das seguintes formas, de acordo com nossa conveniência: i) $a + b\theta$, com $a, b \in \mathbb{Z}$; ou ii) $\frac{a}{2} + \frac{b}{2}\sqrt{m}$ com $a, b \in \mathbb{Z}$ e de mesma paridade, isto é, $a \equiv b \bmod 2$.

Seja

$$\theta = \begin{cases} \frac{1+\sqrt{m}}{2} & \text{se } m \equiv 1 \bmod 4 \\ \sqrt{m} & \text{se } m \equiv 2,3 \bmod 4\,. \end{cases}$$

Assim, para cada inteiro m livre de quadrado, $\mathbb{Z}[\theta]$ é o anel quadrático formado pelos inteiros de $\mathbb{Q}[\sqrt{m}]$.

$\mathbb{Z}[i]$ é um exemplo com $m = -1 \equiv 3 \bmod 4$ e $\mathbb{Z}\left[\frac{1+i\sqrt{3}}{2}\right]$ com $m = -3 \equiv 1 \bmod 4$.

2 Norma

A norma de um elemento de $\mathbb{Z}[\theta]$ é fundamental para que anéis quadráticos sejam euclidianos. Vamos defini-la para todos os elementos de $\mathbb{Q}[\sqrt{m}]$.

Seja $\alpha = r + s\sqrt{m} \in \mathbb{Q}[\sqrt{m}]$. Definimos o *conjugado* de α como $\overline{\alpha} = r - s\sqrt{m}$ e a *norma* de α como

$$N(\alpha) = \alpha\overline{\alpha} = (r + s\sqrt{m})(r - s\sqrt{m}) = r^2 - ms^2\,.$$

Observações:

1. É fácil verificar que $N(\alpha\beta) = N(\alpha)N(\beta), \forall \alpha, \beta \in \mathbb{Q}[\sqrt{m}]$.

2. Se $\alpha = r + s\sqrt{m} \in \mathbb{Z}[\theta]$, então $N(\alpha) \in \mathbb{Z}$. Isto é claro quando $r, s \in \mathbb{Z}$. Quando $m \equiv 1 \bmod 4$ e $r = \frac{a}{2}$ e $s = \frac{b}{2}$ com a e b ímpares, então $N(\alpha) = \frac{a^2-mb^2}{4}$. Como $a^2 \equiv b^2 \equiv m \equiv 1 \bmod 4$, temos que $4|(a^2 - mb^2)$ e $N(\alpha) \in \mathbb{Z}$.

3. Quando $m > 0$, temos $-mb^2 \leq a^2 - mb^2 \leq a^2$. Logo, $|N(a + b\sqrt{m})| = |a^2 - mb^2| \leq \max\{a^2, mb^2\}$.

3 Anéis quadráticos euclidianos complexos

Os anéis quadráticos com $m < 0$ são chamados anéis quadráticos complexos, porque estão contidos em $\mathbb{C}$ mas não em $\mathbb{R}$. Nesta seção estudaremos os anéis quadráticos complexos que são euclidianos.

Um anel A é um *anel euclidiano* se existe uma aplicação $d : A - \{0\} \to \mathbb{N}$ tal que:

1. $d(\alpha\beta) \geq d(\alpha), \forall \alpha, \beta \in A - \{0\}$.

2. Existe um algoritmo da divisão em A, isto é, dados $\alpha, \beta \in A, \beta \neq 0$, existem $q, r \in A$ tais que $\alpha = q\beta + r$ com $r = 0$ ou $d(r) < d(\beta)$.

$\mathbb{Z}$ é um exemplo de anel euclidiano. Nos nossos anéis quadráticos, usaremos como d a função norma definida na seção anterior. Como $N(\alpha\beta) = N(\alpha)N(\beta)$, a primeira condição da definição de anel euclidiano é sempre verificada, e portanto basta nos preocuparmos com a segunda condição, ou seja, com o algoritmo da divisão. Observamos que não está sendo exigida unicidade para q e r.

Teorema 3.1. *Se $m < 0$, existe um algoritmo da divisão em $\mathbb{Z}[\theta]$ (isto é $\mathbb{Z}[\theta]$ é um anel euclidiano) para $m = -1, -2, -3, -7, -11$.*

Demonstração. Dados $\alpha, \beta \in \mathbb{Z}[\theta]$, $\beta \neq 0$, queremos encontrar $q, r \in \mathbb{Z}[\theta]$ tais que $\alpha = q\beta + r$ com $N(r) < N(\beta)$. Mas,

$$N(r) = N(\alpha - q\beta) = N((\frac{\alpha}{\beta} - q)\beta) = N(\frac{\alpha}{\beta} - q)N(\beta)\,,$$

e portanto basta mostrar que se $\gamma \in \mathbb{Q}[\theta] = \mathbb{Q}[\sqrt{m}]$, o corpo das frações de $\mathbb{Z}[\theta]$, existe $q \in \mathbb{Z}[\theta]$ tal que $N(\gamma - q) < 1$.

Quando $m \equiv 2, 3 \bmod 4$, isto é, quando $m = -1, -2$, se $\gamma = a + b\sqrt{m}$ 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 $q = x + y\sqrt{m}$,

$$\begin{aligned} N(\gamma - q) &= N(a - x + (b - y)\sqrt{m}) \\ &\leq (a - x)^2 - m(b - y)^2 \\ &\leq \frac{1}{4} + |m|\frac{1}{4} < 1\,. \end{aligned}$$

Quando $m \equiv 1 \bmod 4$, isto é, quando $m = -3, -7, -11$, se $\gamma = a + b\sqrt{m}$ como acima 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 tomamos $x = \frac{u}{2}$ com $u \in \mathbb{Z}$, $u \equiv v \bmod 2$, tal que $|a - x| \leq \frac{1}{2}$. Conforme vimos na construção dos anéis quadráticos na Seção 2, no caso em que $m \equiv 1 \bmod 4$, u e v têm que ter a mesma paridade.

Assim, se $q = x + y\sqrt{m}$,

$$\begin{aligned} N(\gamma - q) &= N(a - x + (b - y)\sqrt{m}) \\ &= (a - x)^2 - m(b - y)^2 \\ &\leq \frac{1}{4} + |m|\frac{1}{16} < 1\,. \end{aligned}$$

□

Observações:

1. Estes são os únicos valores para m, com $m < 0$, tais que $\mathbb{Z}[\theta]$ possui um um algoritmo da divisão.

2. Todo anel euclidiano é um anel fatorial, e portanto todo elemento não nulo e não inversível se escreve de maneira única como um produto finito de elementos irredutíveis. Existem anéis quadráticos que são fatoriais mas que não são euclidianos, por exemplo, quando $m = -19$ ou $m = -43$. Para $m = -19$, o leitor encontra uma demonstração destas propriedades nos artigos [16] ou [3].

3. Nos nossos exemplos, como $\frac{\alpha}{\beta} = \frac{\alpha\overline{\beta}}{\beta\overline{\beta}}$ e $\beta\overline{\beta} \in \mathbb{Z}$, vamos tomar sempre $\beta \in \mathbb{Z}$.

Exemplo 3.1. *Sejam $m = -11$, $\alpha = 19 + 10\sqrt{-11}$ e $\beta = 6$.*

Neste exemplo, $m \equiv 1 \bmod 4$. Vamos encontrar $q = x + y\sqrt{-11}$, $r = s + t\sqrt{-11} \in \mathbb{Z}\left[\frac{1+\sqrt{-11}}{2}\right]$ tais que $\alpha = q\beta + r$ com $N(r) < N(\beta)$. Escrevendo $\frac{\alpha}{\beta} = a + b\sqrt{-11} = \frac{19}{6} + \frac{10}{6}\sqrt{-11}$, temos $a = \frac{19}{6}$ e $b = \frac{10}{6} = \frac{5}{3}$. Vamos tomar inicialmente $y = \frac{v}{2}$ com $v \in \mathbb{Z}$ tal que $|b - y| \leq \frac{1}{4}$. Seja $y = \frac{3}{2}$. Então

$$|b - y| = \left|\frac{5}{3} - \frac{3}{2}\right| = \frac{1}{6} \leq \frac{1}{4}\,.$$

Como $y = \frac{v}{2} = \frac{3}{2}$, com $v \in \mathbb{Z}$ número ímpar, vamos tomar agora $x = \frac{u}{2}$ com $u \in \mathbb{Z}$ número ímpar tal que $|a - x| \leq \frac{1}{2}$. Seja $x = \frac{7}{2}$. Assim,

$$|a - x| = \left|\frac{19}{6} - \frac{7}{2}\right| = \left|\frac{-2}{6}\right| = \frac{1}{3} \leq \frac{1}{2}\,.$$

Segue que

$$\begin{aligned} q &= x + y\sqrt{-11} = \frac{7}{2} + \frac{3}{2}\sqrt{-11}\,, \\ r &= \alpha - q\beta \\ &= 19 + 10\sqrt{-11} - (\frac{7}{2} + \frac{3}{2}\sqrt{-11})6 \\ &= -2 + \sqrt{-11} \end{aligned}$$

e

$$\begin{aligned} N(r) &= N(-2 + \sqrt{-11}) \\ &= 4 + 11 = 15 < 36 = N(6) = N(\beta)\,. \end{aligned}$$

4 Anéis quadráticos euclidianos reais

Os anéis quadráticos reais (contidos em $\mathbb{R}$) são euclidianos, isto é, possuem um algoritmo da divisão, apenas quando $m = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73$. Faremos a demonstração para $m = 2, 3, 5, 6, 7, 13, 17, 21, 29$. Usaremos

$$N(a + b\sqrt{m}) = |a^2 - mb^2|$$

para que a norma fique sempre positiva. Neste caso, conforme vimos na Seção 3, $N(a+b\sqrt{m}) = |a^2 - mb^2| \leq \max\{a^2, mb^2\}$.

Teorema 4.1. *Existe um algoritmo da divisão em $\mathbb{Z}[\theta]$ para $m = 2, 3, 5, 13$.*

Demonstração. Como na demonstração do teorema anterior, basta mostrar que se $\gamma \in \mathbb{Q}[\theta]$, existe $q \in \mathbb{Z}[\theta]$ tal que $N(\gamma - q) < 1$.

Quando $m \equiv 2, 3 \bmod 4$, isto é, quando $m = 2, 3$, se $\gamma = a + b\sqrt{m}$ 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 $q = x + y\sqrt{m}$,

$$\begin{aligned} N(\gamma - q) &= N(a - x + (b - y)\sqrt{m}) \\ &\leq |(a-x)^2 - m(b-y)^2| \\ &\leq \max\{\frac{1}{4}, \frac{m}{4}\} < 1\,. \end{aligned}$$

Quando $m \equiv 1 \bmod 4$, isto é, quando $m = 5, 13$, se $\gamma = a + b\sqrt{m}$ 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 tomamos $x = \frac{u}{2}$ com $u \in \mathbb{Z}$, $u \equiv v \bmod 2$, tal que $|a - x| \leq \frac{1}{2}$. Conforme vimos na construção dos anéis quadráticos na Seção 2, no caso em que $m \equiv 1 \bmod 4$, u e v têm que ter a mesma paridade.

Assim, se $q = x + y\sqrt{m}$,

$$\begin{aligned} N(\gamma - q) &= N(a - x + (b - y)\sqrt{m}) \\ &= |(a-x)^2 - m(b-y)^2| \\ &\leq \max\{\frac{1}{4}, \frac{m}{16}\} < 1\,. \end{aligned}$$

□

Teorema 4.2. *Existe um algoritmo da divisão em $\mathbb{Z}[\theta]$ para $m = 6, 7, 17, 21, 29$.*

Demonstração. Começamos observando que, quando $m \equiv 1 \bmod 4$, um elemento $x + y\theta \in \mathbb{Z}[\theta]$ pode ser escrito na forma

$$x + y\theta = x + y(\frac{1+\sqrt{m}}{2}) = x + \frac{y}{2} + \frac{y}{2}\sqrt{m}\,.$$

Assim, dado $\gamma = a + b\sqrt{m} \in \mathbb{Q}[\theta]$, queremos encontrar $q = x + y\sqrt{m} \in \mathbb{Z}[\theta]$ tal que

$$|(a-x)^2 - m(b-y)^2| < 1\,, \tag{1}$$

se $m \equiv 2, 3 \bmod 4$, ou $q = x + \frac{y}{2} + \frac{y}{2}\sqrt{m} \in \mathbb{Z}[\theta]$ tal que

$$|(a - x - \frac{y}{2})^2 - m(b - \frac{y}{2})^2| < 1\,, \tag{2}$$

se $m \equiv 1 \bmod 4$.

As duas desigualdades (1) e (2) acima podem ser escritas na forma

$$|(a - x - \lambda y)^2 - n(b - y)^2| < 1 \tag{3}$$

onde $\lambda = 0, n = m$ se $m \equiv 2, 3 \bmod 4$, e $\lambda = \frac{1}{2}, n = \frac{m}{4}$ se $m \equiv 1 \bmod 4$. Neste último caso, substituímos também $2b$ por b. Com estas convenções, podemos supor $0 \leq a \leq \frac{1}{2}$ e $0 \leq b \leq \frac{1}{2}$. No caso $m \equiv 1 \bmod 4$ teríamos $b \leq \frac{1}{4}$ e portanto $2b \leq \frac{1}{2}$.

Vamos mostrar que para $n < 8$ a desigualdade (3) tem solução. A condição $n < 8$ significa $m = 6, 7$ se $m \equiv 2, 3 \bmod 4$ e $m < 4n = 32$, isto é, $m = 17, 21, 29$ se $m \equiv 1 \bmod 4$.

Vamos verificar que, tomando $y = 0$, um dos três valores para x, $x = -1$, $x = 0$ ou $x = 1$ vai satisfazer a desigualdade (3), isto é,

$$-1 < (a - x - \lambda y)^2 - n(b - y)^2 < 1\,.$$

Estas duas desigualdades podem ser escritas na forma

$$\begin{aligned} P(x,y): \quad (a - x - \lambda y)^2 &< 1 + n(b-y)^2 \\ Q(x,y): \quad n(b-y)^2 &< 1 + (a - x - \lambda y)^2\,. \end{aligned}$$

Evidentemente, se $a = b = 0$, tomamos $x = y = 0$. Suponha que a e b não sejam ambos nulos. Vamos mostrar que pelo menos um dos pares $P(-1,0)$ e $Q(-1,0)$, $P(0,0)$ e $Q(0,0)$ ou $P(1,0)$ e $Q(1,0)$ são desigualdades verdadeiras, e assim encontramos x, y que satisfazem (3). Temos:

$$\begin{aligned} P(-1,0): \quad (1+a)^2 &< 1 + nb^2 \\ Q(-1,0): \quad nb^2 &< 1 + (1+a)^2 \\ P(0,0): \quad a^2 &< 1 + nb^2 \\ Q(0,0): \quad nb^2 &< 1 + a^2 \\ P(1,0): \quad (1-a)^2 &< 1 + nb^2 \\ Q(1,0): \quad nb^2 &< 1 + (1-a)^2\,. \end{aligned}$$

Como $0 \leq a \leq \frac{1}{2}$, $n > 0$ e a e b não são ambos nulos, resulta que $P(0,0)$ e $P(1,0)$ são verdadeiras. Vamos então supor que $Q(0,0)$ e $Q(1,0)$ sejam falsas e vamos mostrar que, neste caso, $P(-1,0)$ e $Q(-1,0)$ são ambas verdadeiras.

Suponha que $P(-1,0)$ também seja falsa. Então $(1+a)^2 \geq 1 + nb^2$. Como $Q(1,0)$ é falsa, $1 + nb^2 \geq 1 + 1 + (1-a)^2 = 2 + (1-a)^2$. Juntando estas duas desigualdades temos $(1+a)^2 \geq 2 + (1-a)^2$, resultando

assim $a \geq \frac{1}{2}$. Como estamos supondo $0 \leq a \leq \frac{1}{2}$, segue que $a = \frac{1}{2}$. Substituindo $a = \frac{1}{2}$ em $(1+a)^2 \geq 1 + nb^2 \geq 2 + (1-a)^2$, obtemos $\frac{9}{4} \geq 1 + nb^2 \geq \frac{9}{4}$, e portanto $nb^2 = \frac{5}{4}$. Mas, pelo lema a seguir, este valor $nb^2 = \frac{5}{4}$ não é possível. Assim se $Q(1,0)$ é falsa, então $P(-1,0)$ é verdadeira.

Vamos mostrar que diante da condição $n < 8$, $Q(-1,0)$ também é verdadeira. Mas $Q(-1,0)$ é $nb^2 < 1 + (1+a)^2$. Como $n < 8$ e $b^2 \leq \frac{1}{4}$, temos $nb^2 < 8 \times \frac{1}{4} = 2 \leq 1 + (1+a)^2$, e portanto $Q(-1,0)$ é verdadeira, concluindo a demonstração. □

Lema 4.1. *$nb^2 = \frac{5}{4}$ não pode acontecer.*

Demonstração. Suponha inicialmente que $m \equiv 2,3 \bmod 4$. Neste caso, como $n = m$ e escrevendo $b = \frac{p}{q}$ com p e q primos entre si, temos $4mp^2 = 5q^2$ e portanto $p^2 | 5q^2$. Como p e q são primos entre si, $p^2 | 5$ e consequentemente $p = 1$. Assim, $4m = 5q^2$ e portanto $q^2 | 4m$. Como m é livre de quadrado, resulta $q = 2$. Segue que $4m = 5 \times 4$ e $m = 5 \equiv 1 \bmod 4$. Contradição.

Suponha agora que $m \equiv 1 \bmod 4$. Neste caso $m = 4n$, logo, $mb^2 = 5$. Como acima, escrevendo $b = \frac{p}{q}$ com p e q primos entre si, resulta que $p^2 | 5$ e $p = 1$. Temos então $5q^2 = m$, e portanto $q^2 | m$, e como m é livre de quadrado, $q = 1$. Logo $b = 1$, contradizendo $0 \leq b \leq \frac{1}{2}$. □

Observações:

1. A demonstração do teorema anterior serve também quando $m = 2,3,5,13$ e é devida a Oppenheim ([14]).

2. Enquanto nos Teoremas 4.1 e 5.1 obtivemos $q = x + y\sqrt{m}$ bem determinados, na demonstração deste último teorema, encontramos um valor para y bem determinado e três valores possíveis para x. Pelo menos um deles atende às condições do algoritmo da divisão.

Exemplo 4.1. *Sejam $m = 7$, $\alpha = 114 + 200\sqrt{7}$ e $\beta = 45$.*

Neste exemplo, $m \equiv 3 \bmod 4$. Vamos encontrar $q = x + y\sqrt{7}$, $r = s + t\sqrt{7} \in \mathbb{Z}[\sqrt{7}]$ tais que $\alpha = q\beta + r$ com $N(r) < N(\beta)$. Escrevendo $\frac{\alpha}{\beta} = a + b\sqrt{7} = \frac{114}{45} + \frac{200}{45}\sqrt{7}$, temos $a = \frac{114}{45}$ e $b = \frac{200}{45}$ e vamos tomar $x_0, y \in \mathbb{Z}$ tais que $|a - x_0| \leq \frac{1}{2}$ e $|b - y| \leq \frac{1}{2}$. Escolhendo $x_0 = 3$ e $y = 4$, temos

$$|a - x_0| = \left|\frac{114}{45} - 3\right| = \left|\frac{-21}{45}\right| \leq \frac{1}{2}$$

e

$$|b - y| = \left|\frac{200}{45} - 4\right| = \left|\frac{20}{45}\right| \leq \frac{1}{2}.$$

Assim, já temos o valor de y e três candidatos para x: $x = x_{-1} = x_0 - 1 = 2$, $x = x_0 = 3$ ou $x = x_1 = x_0 + 1 = 4$. Pelo menos um deles vai atender às condições do algoritmo da divisão. Sejam $q_i = x_i + y\sqrt{29}$ e $r_i = \alpha - q_i\beta$, $i = -1, 0, 1$. Testamos então:

$$\begin{aligned} r_{-1} &= \alpha q_{-1}\beta \\ &= 114 + 200\sqrt{7} - (2 + 4\sqrt{7}) = 24 + 20\sqrt{7} \\ r_0 &= \alpha q_0 \beta \\ &= 114 + 200\sqrt{7} - (3 + 4\sqrt{7}) = -21 + 20\sqrt{7} \\ r_1 &= \alpha q_1 \beta \\ &= 114 + 200\sqrt{7} - (4 + 4\sqrt{7}) = -66 + 20\sqrt{7}. \end{aligned}$$

Como $N(\beta) = N(45) = 2025$, $N(r_{-1}) = N(24 + 20\sqrt{7}) = 2224$, $N(r_0) = N(-21 + 20\sqrt{7}) = 2359$ e $N(r_1) = N(-66 + 20\sqrt{7}) = 1556$, os valores procurados para q e r são: $q = q_1 = 4 + 4\sqrt{7}$ e $r = r_1 = -66 + 20\sqrt{7}$.

Observação: Como $|b - y| = \left|\frac{20}{45}\right|$ estava próximo de $\frac{1}{2}$, 20 foi um resto grande. Assim, $m(b-y)^2 = 7 \times \left|\frac{20}{45}\right|^2$ assumiu um valor grande, o qual teve que ser compensado com o maior valor para $|a - x|$: $\left|\frac{-66}{45}\right|$.

Exemplo 4.2. *Sejam $m = 29$, $\alpha = 42 + 66\sqrt{29}$ e $\beta = 5$.*

Neste exemplo, $m \equiv 1 \bmod 4$. Vamos encontrar $q = x + y\sqrt{29}$, $r = s + t\sqrt{29} \in \mathbb{Z}\left[\frac{1+\sqrt{29}}{2}\right]$ tais que $\alpha = q\beta + r$ com $N(r) < N(\beta)$. Escrevendo $\frac{\alpha}{\beta} = a + b\sqrt{29} = \frac{42}{5} + \frac{66}{5}\sqrt{29}$, temos $a = \frac{42}{5}$ e $b = \frac{66}{5}$. Vamos tomar inicialmente $y = \frac{v}{2}$ com $v \in \mathbb{Z}$ tal que $|b - y| \leq \frac{1}{4}$. Seja $y = \frac{26}{2} = 13$. Neste caso,

$$|b - y| = \left|\frac{66}{5} - 13\right| = \frac{1}{5} \leq \frac{1}{4}.$$

Como $y \in \mathbb{Z}$, vamos tomar agora $x_0 \in \mathbb{Z}$ tal que $|a - x_0| \leq \frac{1}{2}$. Escolhendo $x_0 = 8$ temos

$$|a - x_0| = \left|\frac{42}{5} - 8\right| = \frac{2}{5} \leq \frac{1}{2}.$$

Assim, já temos o valor de y e três candidatos para x: $x = x_{-1} = x_0 - 1 = 7$, $x = x_0 = 8$ e $x = x_1 = x_0 + 1 = 9$. Pelo menos um deles vai atender às condições do algoritmo da divisão. Sejam $q_i = x_i + y\sqrt{29}$ e $r_i = \alpha - q_i\beta$, $i = -1, 0, 1$. Testamos então:

$$\begin{aligned} r_{-1} &= \alpha q_{-1}\beta \\ &= 42 + 66\sqrt{29} - 5(7 + 13\sqrt{29}) = 7 + \sqrt{29} \\ r_0 &= \alpha q_0\beta \\ &= 42 + 66\sqrt{29} - 5(8 + 13\sqrt{29}) = 2 + \sqrt{29} \\ r_1 &= \alpha q_1\beta \\ &= 42 + 66\sqrt{29} - 5(9 + 13\sqrt{29}) = -3 + \sqrt{29}\,. \end{aligned}$$

Como $N(\beta) = N(5) = 25$, $N(r_{-1}) = N(7 + \sqrt{29}) = 20$, $N(r_0) = N(2 + \sqrt{29}) = 25$ e $N(r_1) = N(-3 + \sqrt{29}) = 20$, encontramos dois pares para q e r: $q = q_{-1} = 7 + 13\sqrt{29}$ e $r = r_{-1} = 7 + \sqrt{29}$ e $q = q_1 = 9 + 13\sqrt{29}$ e $r = r_1 = -3 + \sqrt{29}$.

Exemplo 4.3. *Sejam $m = 29$, $\alpha = 35 - 96\sqrt{29}$ e $\beta = 7$.*

Neste exemplo, $m \equiv 1 \bmod 4$. Como antes, vamos encontrar $q = x + y\sqrt{29}$, $r = s + t\sqrt{29} \in \mathbb{Z}\left[\frac{1+\sqrt{29}}{2}\right]$ tais que $\alpha = q\beta + r$ com $N(r) < N(\beta)$. Escrevendo $\frac{\alpha}{\beta} = a + b\sqrt{29} = \frac{35}{7} - \frac{96}{7}\sqrt{29}$, temos $a = \frac{35}{7} = 5$ e $b = -\frac{96}{7}$. Vamos tomar inicialmente $y = \frac{v}{2}$ com $v \in \mathbb{Z}$ tal que $|b - y| \leq \frac{1}{4}$. Seja $y = -\frac{27}{2}$. Neste caso,

$$|b - y| = \left|-\frac{96}{5} + \frac{27}{2}\right| = \left|-\frac{3}{14}\right| = \frac{3}{14} \leq \frac{1}{4}\,.$$

Como $y = \frac{v}{2} = \frac{-27}{2}$ com $v \in \mathbb{Z}$ número ímpar, vamos tomar agora $x_0 = \frac{u}{2}$ com $u \in \mathbb{Z}$ número ímpar tal que $|a - x_0| \leq \frac{1}{2}$. Escolhemos $x_0 = \frac{9}{2}$. Assim,

$$|a - x_0| = \left|5 - \frac{9}{2}\right| = \frac{1}{2} \leq \frac{1}{2}\,.$$

Assim, já temos o valor de y e três candidatos para x: $x = x_{-1} = x_0 - 1 = \frac{7}{2}$, $x = x_0 = \frac{9}{2}$ e $x = x_1 = x_0 + 1 = \frac{11}{2}$. Pelo menos um deles vai atender às condições do algoritmo da divisão. Sejam $q_i = x_i + y\sqrt{29}$ e $r_i = \alpha - q_i\beta$, $i = -1, 0, 1$. Testamos então:

$$\begin{aligned} r_{-1} &= \alpha q_{-1}\beta \\ &= 35 - 96\sqrt{29} - 7(\frac{7}{2} - \frac{27}{2}\sqrt{29}) = \frac{21}{2} - \frac{3}{2}\sqrt{29} \\ r_0 &= \alpha q_0\beta \\ &= 35 - 96\sqrt{29} - 7(\frac{9}{2} - \frac{27}{2}\sqrt{29}) = \frac{7}{2} - \frac{3}{2}\sqrt{29} \\ r_1 &= \alpha q_1\beta \\ &= 35 - 96\sqrt{29} - 7(\frac{11}{2} - \frac{27}{2}\sqrt{29}) = \frac{-7}{2} - \frac{3}{2}\sqrt{29}\,. \end{aligned}$$

Como $N(\beta) = N(7) = 49$, $N(r_{-1}) = N(\frac{21}{2} - \frac{3}{2}\sqrt{29}) = 45$, $N(r_0) = N(\frac{7}{2} - \frac{3}{2}\sqrt{29}) = 53$ e $N(r_1) = N(-\frac{7}{2} - \frac{3}{2}\sqrt{29}) = 53$, tomamos $q = q_{-1} = \frac{7}{2} - \frac{27}{2}\sqrt{29}$ e $r = r_{-1} = \frac{21}{2} - \frac{3}{2}\sqrt{29}$.

Observação. No exemplo acima, poderíamos ter tomado $x_0 = \frac{11}{2}$, em vez de $x_0 = \frac{9}{2}$. Neste caso os três valores possíveis para x seriam $x = x_{-1} = \frac{9}{2}$, $x = x_0 = \frac{11}{2}$ e $x = x_1 = \frac{13}{2}$. Desse modo, $q = \frac{13}{2} - \frac{27}{2}\sqrt{29}$ e $r = -\frac{21}{2} - \frac{3}{2}\sqrt{29}$ atenderiam ao algoritmo da divisão.

Exemplo 4.4. *Sejam $m = 17$, $\alpha = 35 - 96\sqrt{17}$ e $\beta = 7$.*

Em relação ao exemplo anterior, não se alteram os valores para a, b, y e x_0. Os valores possíveis para q e r são: $q_{-1} = \frac{7}{2} - \frac{27}{2}\sqrt{17}$ e $r_{-1} = \frac{21}{2} - \frac{3}{2}\sqrt{17}$, $q_0 = \frac{9}{2} - \frac{27}{2}\sqrt{17}$ e $r_0 = \frac{7}{2} - \frac{3}{2}\sqrt{17}$ e $q_1 = \frac{11}{2} - \frac{27}{2}\sqrt{17}$ e $r_1 = \frac{-7}{2} - \frac{3}{2}\sqrt{17}$. Como $N(\beta) = N(7) = 49$, $N(r_{-1}) = 72$ e $N(r_0) = N(r_1) = 26$, podemos tomar $q = q_0$ e $r = r_0$ ou $q = q_1$ e $r = r_1$.

5 Apêndice

Neste apêndice, vamos mostrar que todo inteiro de $\mathbb{Q}[\sqrt{m}]$ anula um polinômio mônico de grau 2 em $\mathbb{Z}[X]$.

Com efeito, primeiro observamos que os elementos de $\mathbb{Q}[\sqrt{m}]$ que anulam um polinômio mônico de $\mathbb{Z}[X]$ de grau 1 são os elementos de $\mathbb{Z}$. Suponha, então, que α seja um inteiro de $\mathbb{Q}[\sqrt{m}]$ que anula um polinômio $f(X) \in \mathbb{Z}[X]$ de grau 2, mas não anula um polinômio de grau 1. Lembramos que um polinômio de $\mathbb{Z}[X]$ é *primitivo* se o máximo divisor comum de seus coeficientes for 1. Podemos supor que $f(X) = a_2X^2 + a_1X + a_0$ é primitivo com $a_2 > 0$. Vamos mostrar que $a_2 = 1$ e, assim, α anula um polinômio mônico de grau 2 em $\mathbb{Z}[X]$.

Como α é um inteiro algébrico, α anula um polinômio mônico $g(X) \in \mathbb{Z}[X]$ de grau ≥ 2. Aplicando o algoritmo da divisão, existem $q(X), r(X) \in \mathbb{Q}[X]$ tais que $g(X) = f(X)q(X) + r(X)$, com grau de $r(X) < 2$ ou $r(X) = 0$. Como $g(\alpha) = f(\alpha) = 0$, temos que $r(\alpha) = 0$. Como α não anula um polinômio de grau < 2, segue que $r(X) = 0$ e, assim, $g(X) = f(X)q(X)$. Eliminando os denominadores de $q(X)$ podemos escrever $dg(X) = f(X)q_1(X)$, com $d \in \mathbb{Z}$ e $q_1(X) = b_m X^m + b_{m-1}X^{m-1} + \ldots + b_0 \in \mathbb{Z}[X]$ um polinômio primitivo. Como, pelo Lema de Gauss (veja, por exemplo, [9]), o produto de dois polinômios primitivos é um polinômio primitivo, resulta $d = 1$ e $g(X) = f(X)q_1(X)$. Comparando os coeficientes do termo de mais alto grau nesta última igualdade, obtemos $1 = a_2 b_m$ e $a_2 = 1$.

Referências

[1] BARNES, E. S.; SWINNERTON-DYER, H. P. F. The inhomogeneous minima of binary quadratic forms I. *Acta Mathematica*, v. 87, p. 259–323, 1952.

[2] BIRKOFF, G.; MACLANE, S. *Álgebra moderna básica*. 4. ed. Rio de Janeiro: Guanabara, 1980.

[3] CÁMPOLI, O. A principal ideal domain that is not a euclidean domain. *American Mathematical Monthly*, v. 95, p. 868–871, 1988.

[4] CHATLAND, H. On the euclidean algorithm in quadratic number fields. *Bulletin of the American Mathematical Society*, v. 55, p. 948–953, 1949.

[5] CHATLAND, H.; DAVENPORT, H. Euclids algorithm in real quadratic fields. *Canadian Journal of Mathematics*, v. 2, p. 289–296, 1950.

[6] DEAN, R. *Elementos de álgebra abstrata*. Rio de Janeiro: LTC, 1974.

[7] DICKSON, L. *Algebren und ihre Zahlentheorie. Mit einem kapitel über idealtheorie von A. Speiser.* Zürich-Leipzig: Orell Füssli Verlag, 1927.

[8] DOMINGUES, H.; IEZZI, G. *Álgebra moderna*. 2. ed. São Paulo: Atual, 1982.

[9] GARCIA, A.; LEQUAIN, Y. *Elementos de álgebra.* Rio de Janeiro: IMPA, 2002. (Projeto Euclides)

[10] GONÇALVES, A. *Introdução à álgebra*. Rio de Janeiro: IMPA, 1979. (Projeto Euclides)

[11] HARDY, G. H.; WRIGHT, E. M. *An introduction to the theory of numbers.* 4. ed. New York: Oxford University Press, 1960.

[12] HERNSTEIN, I. *Tópicos de álgebra.* São Paulo: Polígono, 1970.

[13] INKERI, K. Über den Euklidischen Algorithmus in quadratischen Zahlkörpern. *Annales Academiae Scientiarum Fennicae. Series A. Sectio 1. Mathematica-Physica*, v. 41, p. 1–35, 1947.

[14] OPPENHEIM, A. Quadratic fields with and without Euclid's algorithm. *Mathematische Annalen*, v. 109, p. 349–352, 1934.

[15] PERRON, O. Quadratische Zahlkörper mit Euklidischen Algorithmus. *Mathematische Annalen*, v. 107, p. 489–495, 1933.

[16] WILSON, J. A principal ideal ring that is not a euclidean ring. *Mathematics Magazine*, v. 46, p. 34–38, 1973.

José Fernandes Silva Andrade
Instituto de Matemática – UFBA
jandrade@ufba.br