UNIVERSIDADE FEDERAL DO CEARÁ
CENTRO DE CIÊNCIAS
DEPARTAMENTO DE MATEMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO
EM MATEMÁTICA EM REDE NACIONAL

FRANCISCO DAS CHAGAS ALVES BRITO

RESOLUÇÃO DE PROBLEMAS VIA INTEIROS ALGÉBRICOS

FORTALEZA

2017

FRANCISCO DAS CHAGAS ALVES BRITO

RESOLUÇÃO DE PROBLEMAS VIA INTEIROS ALGÉBRICOS

Dissertação apresentada ao Programa de Pós-graduação em Matemática em Rede Nacional do Departamento de Matemática da Universidade Federal do Ceará, como parte dos requisitos necessários para a obtenção do título de Mestre em Matemática. Área de concentração: Ensino de Matemática.

Orientador: Prof. Dr. Frederico Vale Girão

FORTALEZA

2017

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca Universitária
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

B875r Brito, Francisco das Chagas Alves.
Resolução de problemas via inteiros algébricos / Francisco das Chagas Alves Brito. – 2017.
49 f.

Dissertação (mestrado) – Universidade Federal do Ceará, Centro de Ciências, Departamento de Matemática, Programa de Pós-Graduação em Matemática em Rede Nacional, Fortaleza, 2017.
Orientação: Prof. Dr. Frederico Vale Girão.

1. Inteiros Algébricos. 2. Inteiros de Gauss. 3. Inteiros de Eisenstein. 4. Fatoração Única. 5. Resolução de Problemas. I. Título.

CDD 510

FRANCISCO DAS CHAGAS ALVES BRITO

RESOLUÇÃO DE PROBLEMAS VIA INTEIROS ALGÉBRICOS

Dissertação apresentada ao Programa de Pós-graduação em Matemática em Rede Nacional do Departamento de Matemática da Universidade Federal do Ceará, como parte dos requisitos necessários para a obtenção do título de Mestre em Matemática. Área de concentração: Ensino de Matemática.

Aprovoda em: 14/07/2017.

BANCA EXAMINADORA

Prof. Dr. Frederico Vale Girão (Orientador)
Universidade Federal do Ceará (UFC)

Prof. Dr. Antônio Caminha Muniz Neto
Universidade Federal do Ceará (UFC)

Prof. Me. Márcio Nascimento da Silva
Universidade Estadual Vale do Acaraú (UVA)

Dedico este trabalho a todas as pessoas que acreditaram que um dia ele se tornaria real.

AGRADECIMENTOS

Agradeço, primeiramente, ao criador pelo dom da vida e por todas as maravilhas que ele fez para nós.

Agradeço a meus pais, Raimundo Nonato Brito e Lúcia Alves Brito, por toda a atenção e amor a mim dedicados, sobretudo pelo esforço que fizeram para que eu pudesse concluir minha gradução.

Agradeço à minha esposa, Renata de Vasconcelos Fonteles Brito, por toda a dedicação e compreensão nos momentos em que tive que me dedicar mais ao curso e a este trabalho.

Agradeço a todos os professores pelos quais passei na minha vida acadêmica. Em especial, Delano Klinger Alves de Souza, José Emilson Lima Saraiva e José Ribeiro Filho pelas aulas de iniciação científica que muito me auxiliaram na vida acadêmica, inclusive no presente trabalho.

Agradeço, imensamente, ao meu orientador, Frederico Vale Girão, pela paciência comigo durante a elaboração desta dissertação e pelas belíssimas aulas ministradas no curso do PROFMAT.

Agradeço aos meus colegas de turma do PROFMAT. Em especial, Antônio Edilson Cardoso Portela, pelo apoio incondicinal, João Rodrigues de Souza Filho, a quem devo muitos favores, e Jânio Kléo de Souza Castro, pela imensa contribuição cognitiva e pessoal.

Agradeço à CAPES pelo apoio financeiro.

Enfim, agradeço a todos que contribuiram para esse momento.

"Pode-se alcançar a sabedoria por três caminhos. O primeiro caminho é o da meditação, que é o mais nobre. O segundo é o da imitação, que é o mais fácil e o menos satisfatório. Em terceiro lugar existe o caminho da experiência, que é o mais difícil."

Confúcio.

RESUMO

Neste trabalho, apresentamos as definições de domínio de integridade, domínio euclidiano, domínio de ideais principais e domínio de fatoração única e provamos as implicações Domínio Euclidiano $\Rightarrow$ Domínio de Ideais Principais $\Rightarrow$ Domínio de Fatoração Única. Verificamos que o conjunto dos inteiros de Gauss é um domínio de fatoração única, encontramos seus elementos primos e descrevemos diversas propriedades desse conjunto, aplicando-as especialmente para descrever, de maneira completa, as ternas pitagóricas e para calcular o número de maneiras de representar um inteiro como soma de dois quadrados. Verificamos também que o conjunto dos inteiros de Eisenstein é um domínio de fatoração única, também encontramos seus elementos primos e aplicamos as propriedades desse conjunto para descrever a forma geral de uma terna de inteiros que são lados de um triângulo com um ângulo de 60^{o}. Apresentamos a forma geral dos anéis de inteiros de $\mathbb{Q}[\sqrt{d}]$ e, para o caso $d < 0$, exibimos todos os valores de d que tornam esse anel um domínio de fatoração única. Por fim, aplicamos a teoria desenvolvida para resolver diversos problemas de olímpiadas de matemática.

Palavras-chave: Inteiros algébricos. Inteiros de Gauss. Inteiros de Eisenstein. Fatoração única. Resolução de problemas.

ABSTRACT

In this paper, we present the definitions of integral domain, euclidean domain, principal ideal domain and unique factorization domain and we prove the implications Euclidean Domain $\Rightarrow$ Principal Ideal Domain $\Rightarrow$ Unique Factorization Domain. We check that the set of Gaussian integers is a unique factorization domain, we find its prime elements and we describe several properties of this set, applying them especially to describe, completely, the Pythagorean triples and to calculate the number of ways one can write an integer as a sum of two squares. We also check that the set of Eisenstein integers is a unique factorization domain, we also find its prime elements and we apply the properties of this set to describe the general form of a triple of integers that are sides of a triangle with an angle of 60^{o}. We present the general form of the integers of $\mathbb{Q}[\sqrt{d}]$ and, for $d < 0$, we exhibit all values of d for which this ring a unique factorization domain. Lastly, we apply the developed theory to solve several problems of mathematical olympiads.

Keywords: Algebraic integers. Gaussian integers. Eisenstein integers. Unique factorization. Problem resolutions.

SUMÁRIO

1 INTRODUÇÃO

Por vezes estamos interessados em encontrar soluções inteiras para uma equação polinomial, ou seja, solucionar uma equação diofantina. Esta ideia foi a base do que é considerado o problema mais famoso e duradouro da matemática, o último teorema de Fermat, conjecturado no século XVII por Pierre de Fermat. A busca por provas ou contraprovas desse resultado foi determinante no desenvolvimento da teoria algébrica dos números, permitindo estabelecer-se diversas ferramentas poderosas e sofisticadas, muito contributivas para a matemática moderna.

Este trabalho procura reunir propriedades e técnicas de conjuntos dotados de uma certa estrutura algébrica, para utilizá-las na resolução de diversos problemas em $\mathbb{Z}$ que seriam, no mínimo, trabalhosos se resolvidos utilizando apenas a aritmética dos inteiros.

Na primeira seção, abordamos algumas definições e aspectos gerais de Álgebra, no que diz respeito a anéis, domínios de integridade, domínios euclidianos, domínios de ideais principais e domínios de fatoração única. O principal objetivo dessa seção é provar que todo domínio euclidiano é um domínio de ideais principais e todo domínio de ideais principais é um domínio de fatoração única, para que possamos, ao provar que determinado anel é um domínio euclidiano, usar a propriedade da fatoração única na solução de diversas situações. Nas duas seções que se seguem, trabalhamos para mostrar dois casos, extremamente úteis, de domínios euclidianos, e expor algumas aplicações da fatoração única nesses domínios.

Na quarta seção, discutimos brevemente a forma geral dos inteiros algébricos de $\mathbb{Q}[\sqrt{d}]$ e encontramos alguns casos em que este anel de inteiros possui fatoração única. Na última seção, realizamos o principal objetivo do trabalho, que é aplicar as propriedades dos inteiros algébricos que possuem fatoração única para a resolução de diversos problemas de olímpiadas de matemática, especialmente a resolução de algumas equações diofantinas não lineares.

2 ANÉIS, IDEAIS E DOMÍNIOS

Antes de tratar das definições que, de fato, interessam nesta seção, torna-se necessário rever algumas definições elementares de álgebra.

Nesta seção, bem como em todo o restante do trabalho, o conjunto dos inteiros não negativos será denotado por $\mathbb{Z}_+$.

2.1 Definições preliminares

Definição 2.1. *Um conjunto não vazio A munido de duas operações binárias, $+$ chamada adição e $\cdot$ chamada multiplicação, é dito um anel quando goza das seguintes propriedades:*

(i) $a + (b + c) = (a + b) + c, \forall a, b, c \in A$
(ii) $a + b = b + a, \forall a, b \in A$
(iii) $\exists e \in A$ *tal que* $a + e = e + a = a, \forall a \in A$
(iv) $\forall a \in A, \exists b \in A$ *tal que* $a + b = b + a = e$
(v) $a \cdot (b \cdot c) = (a \cdot b) \cdot c, \forall a, b, c \in A$
(vi) $a \cdot (b + c) = a \cdot b + a \cdot c, (b + c) \cdot a = b \cdot a + c \cdot a, \forall a, b, c \in A.$

Diremos que A é uma anel comutativo se além de ser um anel gozar da propriedade
(vii) $a \cdot b = b \cdot a, \forall a, b \in A$
Se um anel A gozar da propriedade
(viii) $\exists u \in A$ *tal que* $a \cdot u = u \cdot a = a, \forall a \in A$
então ele é dito um anel com identidade.
Um subconjunto $S \subset A$ que seja fechado para as operações de A e que ainda seja um anel é dito um subanel de A.

Desde que não haja ambiguidade, o produto $a \cdot b$, por simplicidade, será denotado por ab. O elemento e, descrito em *(iii)* é único, será chamado o elemento nulo de A e será denotado por 0. O elemento b, descrito em *(iv)* também é único, será chamado o simétrico de a e será denotado por $-a$. O elemento u, descrito em *(viii)*, desde que exista, é único, será chamado o elemento identidade de A e será denotado por 1. O leitor pode encontrar facilmente, em livros como GARCIA and LEQUAIN (2003), demontrações da unicidade dos elementos descritos nesse parágrafo e de que o produto do elemento nulo por qualquer elemento de A é o próprio elemento nulo.

Definição 2.2. *Em um anel com identidade A, um elemento u é dito uma unidade quando é invertível, isto é,*

$$\exists x \in A \text{ tal que } xu = ux = 1.$$

Definição 2.3. *Dado um anel comutativo A, um ideal de A é um conjunto não vazio $I \subset A$ que goza das propriedades:*

(i) I é fechado para a adição.

(ii) $ax = xa \in I, \forall a \in I, \forall x \in A$.

Definição 2.4. *Dado um anel comutativo A, o ideal gerado por um subconjunto finito $\{a_1, a_2, \ldots, a_n\}$ de A é*

$$I(a_1, a_2, \ldots, a_n) = \{a_1x_1 + a_2x_2 + \ldots + a_nx_n \text{ tal que } x_1, x_2, \ldots, x_n \in A\}.$$

Se I for gerado por um conjunto unitário, então I é dito um ideal principal.

Definição 2.5. *Seja I um ideal de um anel comutativo A, com $I \neq A$.*

(1) Se $ab \in I$ implicar em $a \in I$ ou $b \in I$ dizemos que I é um ideal primo.

(2) Se os únicos ideais de A contendo I são I e A dizemos que I é um ideal maximal.

Proposição 2.1. *Seja A um anel comutativo com identidade. Se $I \subset A$ é um ideal maximal, então I é um ideal primo.*

Demonstração. Sejam $a, b \in A$ tais que $ab \in I$. Suponha $a \notin I$, devemos mostrar que $b \in I$.

Para tanto, tome J o ideal gerado por $I \cup \{a\}$. Como $I \subsetneq J$, tem-se $J = A$. Desta forma, $1 \in J$ e existem $m, n \in A$ e $z \in I$, tais que $am + zn = 1$. Multiplicando a equação anterior por b, obtemos

$$(ab)m + z(bn) = b.$$

Portanto, $b \in I$ e I é um ideal primo.

□

Definição 2.6. *Um anel comutativo com identidade é dito um domínio de integridade, ou simplesmente um domínio, quando não possui divisores de 0, isto é,*

$$ab = 0 \Leftrightarrow a = 0 \text{ ou } b = 0.$$

Uma propriedade importante dos domínios integrais é a existência de uma lei de cancelamento como descrita na proposição a seguir.

Proposição 2.2. *Seja R um domínio e sejam $a, b, c \in R$, com $a \neq 0$. Então*

$$ab = ac \Rightarrow b = c.$$

Demonstração.

$$ab = ac \Rightarrow a(b - c) = 0.$$

Como R é um domínio e $a \neq 0$, temos $b - c = 0$ e, consequentemente, $b = c$.

□

Definição 2.7. *Um corpo é um domínio R no qual todo elemento não nulo é invertível, isto é,*

$$\forall a \in R \setminus \{0\}, \exists b \in R \text{ tal que } ab = 1.$$

Neste caso, b é dito o elemento inverso de a e pode ser denotado por a^{-1}.

Em outras palavras, um corpo é um domínio onde todo elemento não nulo é uma unidade.

2.2 Domínios euclidianos

Primeiramente, dado um domínio de integridade R, vamos definir uma norma sobre R.

Definição 2.8. *Uma norma em um domínio R é qualquer função $N : R \to \mathbb{Z}_+$.*
Se $N(x) > 0, \forall x \in R, x \neq 0$, dizemos que N é uma norma positiva.

Vale perceber que, dada a definição acima, é possível estabelecer inúmeras normas sobre o mesmo domínio R. Inclusive, dado qualquer domínio, a função $N(x) = 0, \forall x$, define uma norma trivial sobre R, chamada de norma nula.

Definição 2.9. *Um domínio euclidiano é um domínio de integridade R munido de uma norma N que goza da seguinte propriedade: Dados $a, b \in R$, com $b \neq 0$, existem $q, r \in R$ tais que $a = qb + r$, com $r = 0$ ou $N(r) < N(b)$.*

A ideia por trás desta definição é estabelecer uma estrutura similar à encontrada em $\mathbb{Z}$ sobre outros domínios de integridade R, sempre que possível. De fato, $\mathbb{Z}$ é um domínio euclidiano com a norma $N(x) = |x|$; a demonstração para este fato é facilmente encontrada em qualquer livro de álgebra elementar, como GARCIA and LEQUAIN (2003). Além disso, todo corpo K é um domínio euclidiano, no qual qualquer norma serve, pois dados $a, b \in K$, com $b \neq 0$ temos $a = ab^{-1}b + 0$. Desta forma, basta tomar $q = ab^{-1}, r = 0$.

Proposição 2.3. *Se R é um domínio euclidiano, então todo ideal $I \subset R$ é principal.*

Demonstração. Sejam R um domíno euclidiano e $I \subset R$ um ideal. Se I é o ideal nulo, não há nada a provar.

Se I não é o ideal nulo, considere o conjunto $A = \{N(x); x \in I \setminus \{0\}\}$. Tem-se que A é um subconjunto de $\mathbb{Z}$ limitado inferiormente. Logo, A possui um menor elemento, isto é, existe um elemento de menor norma não nula $d \in I$.

Provaremos que $I = I(d)$. A inclusão $I(d) \subset I$ decorre imediatamente das definições de ideal e ideal principais. Para a inclusão $I \subset I(d)$, usaremos o fato de que R é um domínio euclidiano.

Dado $a \in I$ existem $q, r \in R$ tais que $a = qd + r$, com $r = 0$ ou $N(r) < N(d)$. Obviamente, $qd \in I(d) \subset I$. Daí, $r = a - qd \in I$. Como d é o elemento de menor norma não nula, segue que $r = 0$. Devemos ter então $a = qd \in I(d)$, completando a demonstração.

□

2.3 Domínios de ideais principais

Definição 2.10. *Um domínio R é dito um domínio de ideais principais quando todo ideal de R é principal.*

A Proposição 2.3 garante que todo domínio euclidiano é um domínio de ideais principais.

Proposição 2.4. *Seja R um domínio de ideais principais e sejam a e b elementos não nulos de R. Se d é um gerador do ideal principal gerado por a e b, então*

(1) d é um máximo divisor comum de a e b, isto é, $d \mid a$ e $d \mid b$ e, se d' é tal que $d' \mid a$ e $d' \mid b$, então $d' \mid d$.

(2) d pode ser escrito como uma combinação R-linear de a e b, isto é, existem $x, y \in R$ tais que

$$d = ax + by.$$

(3) d é único a menos de uma multiplicação por uma unidade.

Demonstração.

(1) Basta perceber que $I(a), I(b) \subset I(a, b) = I(d)$. Então $d \mid a$ e $d \mid b$. Além disso, como $I(d) = I(a, b)$ é o menor ideal que contém $I(a)$ e $I(b)$, dado d' tal que $I(a), I(b) \subset I(d')$ então $I(d) \subset I(d')$. De outra forma, se d' é tal que $d' \mid a$ e $d' \mid b$, então $d' \mid d$.

(2) Obviamente, $d \in I(a, b)$. Segue imediatamente da definição de $I(a, b)$ que existem $x, y \in R$ tais que $d = ax + by$.

(3) Suponha $I(d) = I(d') = I(a, b)$. Podemos assumir d e d' não nulos. Assim,

$$d \in I(d') \Rightarrow d = xd', \exists x \in R.$$

$$d' \in I(d) \Rightarrow d' = yd, \exists y \in R.$$

Daí,

$$d = xyd \Rightarrow d(1 - xy) = 0 \Rightarrow xy = 1.$$

Portanto, x e y são ambos unidades.

□

Note que a implicação $d(1 - xy) = 0 \Rightarrow xy = 1$ só é verdadeira porque $d \neq 0$ e R é um domínio.

Definição 2.11. *Seja R um domínio.*

(1) Um elemento não nulo $r \in R$ que não é uma unidade é dito irredutível em R se, sempre que $r = ab$, com $a, b \in R$, então ou a ou b é uma unidade.

(2) Um elemento $p \in R$ é dito primo em R se o ideal gerado por p, $I(p)$, é um ideal primo. Em outras palavras, $p \in R$ não nulo é dito primo se não é uma unidade e sempre que $p \mid ab$, com $a, b \in R$, tem-se $p \mid a$ ou $p \mid b$.

Proposição 2.5. *Em um domínio de integridade todo elemento primo é irredutível.*

Demonstração. Seja R um domínio e seja $p \in R$ tal que $I(p)$ é um ideal primo. Daí, $ab = p \in I(p) \Rightarrow a \in I(p)$ ou $b \in I(p)$. Digamos que $a \in I(p)$. Então, existe $r \in R$ tal que $a = pr$. Daí, $p = (pr)b = p(rb) \Rightarrow 1 = rb$. Logo, r e b são unidades e, portanto, p é irredutível.

□

A condição de R ser um domíno é realmente necessária e foi utilizada no cancelamento $p = (pr)b = p(rb) \Rightarrow 1 = rb$. Em geral, não é verdade que todo elemento irredutível seja primo. Por exemplo, na seção 5 deste trabalho veremos que 2 é irredutível em $\mathbb{Z}[\sqrt{-3}]$, mas não é primo neste domínio. No próximo resultado será mostrada a condição usual para que um elemento irredutível seja primo sobre um domínio R.

Proposição 2.6. *Em um domínio de ideais principais um elemento é primo se, e somente se, é irredutível.*

Demonstração. Na Proposição 2.5 mostramos que, em um domínio R, se $p \in R$ é primo então p é irredutível. Resta-nos mostrar que, sendo R um domínio de ideais principais, se p é irredutível, então p é primo, isto é, $I(p)$ é um ideal primo.

Suponha p irredutível e seja M um ideal que contém $I(p)$. Por hipótese, M é principal, isto é, existe $m \in R$ tal que $M = I(m)$. Como $p \in I(p) \subset I(m)$, temos $p = rm$. Mas p é irredutível, então ou r ou m é unidade em R, isto é, ou $I(m) = I(p)$ ou $I(m) = I(1) = R$. Assim, os únicos ideais de R contendo $I(p)$ são $I(p)$ e R. Portanto,

$I(p)$ é um ideal maximal. Logo, $I(p)$ é um ideal primo (Proposição 2.1).

□

A Proposição 2.6 nos dá uma forma alternativa de provar que um domínio R não é um domínio de ideais principais, bastando provar que existe um elemento irredutível que não é primo. Por exemplo, $\mathbb{Z}[\sqrt{-3}]$ não é um domínio de ideais principais.

2.4 Domínios de fatoração única

Nesta subseção provaremos que todo domínio de ideais principais é um domínio de fatoração única. Em particular, todo domínio euclidiano é um domínio de fatoração única.

Definição 2.12. *Um domínio de fatoração única é um domínio de integridade no qual todo elemento não nulo $r \in R$ que não é uma unidade goza das duas propriedades seguintes:*

(1) r pode ser escrito como produto finito de elementos irredutíveis p_i de R (não necessariamente distintos), $r = p_1 p_2 \dots p_n$.

(2) A decomposição descrita em (1) é única, a menos da ordem dos fatores e de multiplicações por unidades, isto é, se $r = q_1 q_2 \dots q_m$, onde cada q_j é um elemento irredutível de R, então $m = n$ e há uma reordenação dos índices j tal que $q_i = u_i p_i$, onde u_i é uma unidade de R.

Um exemplo trivial de domínio de fatoração única é um corpo, pois neste todo elemento não nulo é unidade, logo não há um elemento que contrarie o disposto na definição acima.

Teorema 2.1. *Todo domínio de ideais principais é um domínio de fatoração única. Em particular, todo domínio euclidiano é um domínio de fatoração única.*

Demonstração. A segunda afirmação segue diretamente da primeira, já que todo domínio euclidiano é um domínio de ideais principais (Proposição 2.3).

Seja R um domínio de ideais principais e seja $r \in R$ um elemento não nulo que não é uma unidade. Devemos mostrar que r pode ser escrito como produto finito de elementos irredutíveis de R e depois mostrar que esta decomposição é unica, a menos de multiplicações por unidade.

Se r é irredutível, não há nada a fazer. Senão, por definição existem $r_1, r_2 \in R$, onde ambos são não nulos e não são unidades, tais que $r = r_1 r_2$. Se $r_1, r_2 \in R$ são ambos irredutíveis então r se escreve como produto finito de irredutíveis. Supondo r_1 redutível, então existem $r_{11}, r_{12} \in R$, onde ambos são não nulos e não são unidades, tais que $r_1 = r_{11} r_{12}$. Devemos mostrar que após uma quantidade finita de etapas obtemos

apenas elementos irredutíveis. Suponha que este processo não termine após um número finito de etapas, então encontraríamos uma sequência de inclusões próprias $I(r) \subset I(r_1) \subset I(r_{11}) \subset \ldots \subset R$. Mostraremos que esta sequência não pode ser infinita.

Dada uma sequência infinita de ideais $I_1 \subseteq I_2 \subset \ldots \subseteq R$, seja $I = \cup_{i=1}^{\infty} I_i$. Como R é um domínio de ideais principais, existe $a \in I$ tal que $I = I(a)$. Mas, pela definição de I, temos $a \in I_n$ para algum n. Daí, $I_n \subseteq I = I(a) \subseteq I_n$, donde $I = I_n$ e a sequência $I_1 \subseteq I_2 \subset \ldots \subseteq R$ é estacionária a partir de I_n. Logo, não podemos ter uma sequência ascendente infinita de inclusões próprias em um domínio de ideais principais. Portanto, a sequência $I(r) \subset I(r_1) \subset I(r_{11}) \subset \ldots \subset R$ é finita e o processo de decomposição termina, isto é, r pode ser escrito como produto finito de irredutíveis.

Resta-nos mostrar que a fatoração é única. Para tanto, sejam $r = p_1 p_2 \ldots p_n$ e $r = q_1 q_2 \ldots q_m$ duas fatorações de r, onde cada p_i e cada q_j é irredutível. Então,

$$p_1 p_2 \ldots p_n = q_1 q_2 \ldots q_m. \tag{1}$$

Como R é um domínio de ideais principais, então cada p_i e cada q_j são elementos primos. Daí,

$$p_1 \mid r \Rightarrow p_1 \mid q_j, \exists j \in \{1, 2, \ldots, m\}.$$

Sem perda de generalidade, suponha $p_1 \mid q_1$, isto é, $q_1 = u_1 p_1$. Segue da irredutibilidade de q_1 que u_1 é uma unidade. A equação 1 torna-se

$$p_1 p_2 \ldots p_n = u_1 p_1 q_2 \ldots q_m.$$

Aplicando o cancelamento,

$$p_2 \ldots p_n = u_1 q_2 \ldots q_m.$$

Como o cancelamento é uma associação $1 - 1$ dos p_i com os q_j, se tivéssemos $m \neq n$ teríamos um produto de irredutíveis resultando em uma unidade. Logo, deve-se ter $m = n$ e, nesse caso, o cancelamento é uma associação bijetiva, sendo portanto $q_i = u_i p_i, \forall i \in \{1, 2, \ldots, n\}$ (a menos de reordenação). Isso termina a demonstração.

□

O Teorema 2.1 garante que $\mathbb{Z}$ é um domínio de fatoração única, uma vez que é um domínio euclidiano.

De fato, temos

Domínio Euclidiano ⇒ Domínio de Ideais Principais ⇒ Domínio de Fatoração Única.

Realmente, as implicações acima não são equivalências, mas não é muito fácil encontrar contraexemplos. Mesmo assim, a seguir daremos um contraexemplo para a recíproca de cada implicação, podendo o leitor conferir a verificação destes fatos em (DUMMIT and

FOOTE, 2004)

Exemplo 2.1. (a) $\mathbb{Z}\left[1+\frac{\sqrt{-19}}{2}\right]$ é um domínio de ideais principais que não é um domínio euclidiano.

(b) $\mathbb{Z}[x]$ é um domínio de fatoração única que não é um domínio de ideais principais.

A partir da próxima seção, trabalharemos com domínios integrais que mostraremos ser domínios euclidianos, a fim de poder futuramente utilizar suas propriedades de fatoração única e domínio de ideais principais para resolver problemas.

3 INTEIROS DE GAUSS $\mathbb{Z}[i]$

Nesta seção iremos mostrar que $\mathbb{Z}[i]$ é um domínio euclidiano e, consequentemente, um domínio de fatoração única. Estes resultados serão amplamente utilizados na resolução dos problemas da Seção 6.

3.1 Definições e resultados preliminares

Definimos o conjunto dos inteiros de Gauss como o subconjunto dos complexos $\mathbb{Z}[i] = \{a + bi; a, b \in \mathbb{Z}\}$, onde $i^2 = -1$. Como $\mathbb{Z}$ é um subanel de $\mathbb{R}$, tem-se que $\mathbb{Z}[i]$ é um subanel do corpo $\mathbb{R}[i] = \mathbb{C}$, sendo, portanto, um domínio.

As operações usuais, que tornam $\mathbb{C}$ um corpo e $\mathbb{Z}[i]$ um domínio são

$$(x + yi) + (z + wi) = (x + z) + (w + w)i$$
$$(x + yi)(z + wi) = (xz - yw) + (xw + yz)i.$$

Além disso, $\mathbb{Z}[i]$ herda de $\mathbb{C}$ a definição de conjugado (dado $a = x + yi \in \mathbb{Z}[i]$, definimos $\overline{a} = x - yi$, o conjugado de a), que possui diversas propriedades. Em particular, dado $a = x + yi \in \mathbb{Z}[i]$, temos $a + \overline{a} = 2x \in \mathbb{Z}, a\overline{a} = x^2 + y^2 \in \mathbb{Z}$ e, se $z \in \mathbb{Z}$, $\overline{z} = z$.

Proposição 3.1. *Dados $a, b \in \mathbb{Z}[i]$, temos*

(I) $\overline{a + b} = \overline{a} + \overline{b}$.

(II) $\overline{ab} = \overline{a} \cdot \overline{b}$.

Demonstração. Sejam $a = x + yi, b = w + zi$, então

(I) $\overline{a + b} = \overline{(x + w) + (y + z)i} = (x + w) - (y + z)i = (x - yi) + (w - zi) = \overline{a} + \overline{b}$.

(II) $\overline{ab} = \overline{(xw - yz) + (xz + yw)i} = (xw - yz) - (xz + yw)i = (xw - yz) + (-xz - yw)i = (x - yi)(w - zi) = \overline{a} \cdot \overline{b}$.

□

Em $\mathbb{Z}[i]$, assim como em $\mathbb{Z}$, dizemos que a divide b e escrevemos $a \mid b$ quando existe c tal que $b = ac$.

Exemplo 3.1.

(I) $(1 + i) \mid 2$, pois $(1 + i)(1 - i) = 2$.

(II) $(1 + i) \nmid (1 + 2i)$, pois caso contrário existiria $x + yi$ com $x, y \in \mathbb{Z}$ tal que $(x + yi) + (1 + i) = 1 + 2i$. Então

$$\begin{cases} x - y = 1 \\ x + y = 2 \end{cases}$$

Daí, $2x = 3$, o que é absurdo.

Proposição 3.2. *Dados $a, b \in \mathbb{Z}[i]$, se $a \mid b$ então $\overline{a} \mid \overline{b}$. Em particular, se $b \in \mathbb{Z}$ então $a \mid b \Rightarrow \overline{a} \mid b$.*

Demonstração. Sejam $a, b \in \mathbb{Z}[i]$. Se $a \mid b$ então existe $c \in \mathbb{Z}[i]$ tal que $b = ac$. Desta forma, $\overline{b} = \overline{ac} = \overline{a} \cdot \overline{c}$. Logo, $\overline{a} \mid \overline{b}$.

Em particular, se $b \in \mathbb{Z}$ então $\overline{b} = b$. Portanto, $a \mid b \Rightarrow \overline{a} \mid \overline{b} = b$.

□

3.2 Norma e unidades

Dado $a = x + yi \in \mathbb{Z}[i]$, temos $a\overline{a} = x^2 + y^2$. Desta forma, $a \cdot \overline{a} \in \mathbb{Z}_+, \forall a \in \mathbb{Z}[i]$. Assim, $N(z) = z \cdot \overline{z}, \forall z \in \mathbb{Z}[i]$ define uma norma natural sobre $\mathbb{Z}[i]$. Vale notar que $a \mid N(a), \forall a \in \mathbb{Z}[i]$ e que o fato de $\overline{a \cdot b} = \overline{a} \cdot \overline{b}$ acarreta $N(ab) = (ab)\overline{(ab)} = ab\overline{a}\overline{b} = (a\overline{a})(b\overline{b}) = N(a)N(b)$, ou seja, a norma N é multiplicativa. Além disso, a Proposição 3.2 diz, em outras palavras, que se $a \mid b$ então $N(a) \mid N(b)$. Ainda, se $a = x+yi \in \mathbb{Z}[i] \setminus \{0\}$ temos $N(a) = x^2+y^2 \geq 1$. Assim, dado b não nulo, tem-se $N(ab) \geq N(a), \forall a \in \mathbb{Z}[i]$.

Exemplo 3.2. A norma de $1 + i$ é $N(1 + i) = (1 + i)(1 - i) = 1^2 + 1^2 = 2$.
A norma de $3 - 5i$ é $N(3 - 5i) = (3 - 5i)(3 + 5i) = 3^2 + 5^2 = 34$.

Proposição 3.3. *Sejam $m \in \mathbb{Z} \setminus \{0\}$ e $\alpha \in \mathbb{Z}[i]$. Se $\alpha \mid m$, então existe um racional não nulo k tal que $\frac{m}{\alpha} = k\overline{\alpha}$.*

Demonstração. Das propriedades operatórias do conjugado segue que

$$m = \alpha\beta \Rightarrow \overline{m} = m = \overline{\alpha} \cdot \overline{\beta}.$$

Daí,

$$m^2 = \alpha\overline{\alpha}\beta\overline{\beta} = \alpha\overline{\alpha}N(\beta)$$

Portanto,

$$\frac{m}{\alpha} = \frac{N(\beta}{m}\alpha.$$

□

De maneira análoga ao que ocorre em $\mathbb{Z}$, as unidades em $\mathbb{Z}[i]$ são todos os elementos invertíveis $z \in \mathbb{Z}[i]$, ou seja, todos os elementos $z \in \mathbb{Z}[i]$ para os quais existe $z' \in \mathbb{Z}[i]$ tal que $z \cdot z' = 1$.

Proposição 3.4. *As únicas unidades de* $\mathbb{Z}[i]$ *são* $1, -1, i$ *e* $-i$.

Demonstração. Se z é unidade em $\mathbb{Z}[i]$ então existe $z' \in \mathbb{Z}[i]$ tal que $zz' = 1$, mas isto implica $N(zz') = N(z)N(z') = N(1) = 1$. Daí, deve-se ter $N(z) = N(z') = 1$.

Sendo $z = x + yi$ devemos ter $x^2 + y^2 = 1$. Daí, $x = \pm 1$ e $y = 0$ ou $x = 0$ e $y = \pm 1$. Logo, $z \in \{1, -1, i, -i\}$.

□

Observe que

$$N(z) = 1 \Rightarrow z\overline{z} = 1 \Rightarrow z \text{ é unidade.}$$

Daí, $z \in \mathbb{Z}[i]$ é unidade se, e somente se, $N(z) = 1$.

Assim como em $\mathbb{Z}$, diremos que $a \in \mathbb{Z}[i]$ é redutível quando este puder ser escrito como produto de fatores $b, c \in \mathbb{Z}[i]$, onde ambos não são unidades, isto é, $N(b), N(c) > 1$. Desta forma, o Exemplo 3.1 mostra que 2, apesar de ser primo em $\mathbb{Z}$, é redututível em $\mathbb{Z}[i]$.

Exemplo 3.3.
$1 + i$ é irredutível em $\mathbb{Z}[i]$, pois

$$(x + yi)(z + wi) = 1 + i \Rightarrow N(x + yi)N(z + wi) = N(1 + i) = 2.$$

Como 2 é irredutível em $\mathbb{Z}_+$, tem-se que $N(x + yi) = 1$ ou $N(z + wi) = 1$, isto é, $x + yi$ é uma unidade ou $z + wi$ é uma unidade.

3.3 $\mathbb{Z}[i]$ é um domínio euclidiano

Vamos, nessa subseção, ver como fuciona a divisão euclidiana em $\mathbb{Z}[i]$. Mas antes vamos descrever o conjunto $\mathbb{Q}[i] = \{s + ti; s, t \in \mathbb{Q}\}$. $\mathbb{Q}[i]$ é, naturalmente, um subcorpo de $\mathbb{C}$ que contém $\mathbb{Z}[i]$. Além disso, todo elemento de $\mathbb{Q}[i]$ pode ser visto como uma fração de elementos de $\mathbb{Z}[i]$ com denominador não nulo e vice-versa. Também naturalmente, as definições de norma e conjugado em $\mathbb{Q}[i]$ coincidem com as de $\mathbb{Z}[i]$.

O conjunto $\mathbb{Q}[i]$ nos dará um suporte valioso no que se segue sobre a divisão euclidiana em $\mathbb{Z}[i]$.

Teorema 3.1. $\mathbb{Z}[i]$ *é um domínio euclidiano.*

Demonstração. Precisamos mostrar que, dados $\alpha, \beta \in \mathbb{Z}[i]$, existem $q, r \in \mathbb{Z}[i]$ tais que $\alpha = q\beta + r$, com $N(r) < N(\beta)$.

Sejam $\alpha = x + yi$ e $\beta = m + ni$, com $\beta \neq 0$. Em $\mathbb{Q}[i]$ temos

$$\frac{\alpha}{\beta} = \frac{\alpha\overline{\beta}}{N(\beta)} = \frac{(x+yi)(m-ni)}{m^2+n^2} = \frac{xm+yn-xni+ymi}{m^2+n^2} = \frac{xm+yn}{m^2+n^2} + \frac{ym-xn}{m^2+n^2}i.$$

Se escrevemos $\alpha = q\beta + r$ com $q, r \in \mathbb{Z}[i]$ então temos em $\mathbb{Q}[i]$

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

Daí,

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

A fim de tornar o valor de $N(r)$ pequeno, devemos tomar q suficientemente próximo de $\frac{\alpha}{\beta} = \frac{xm+yn}{m^2+n^2} + \frac{ym-xn}{m^2+n^2}i$. De fato, tomando $q = a + bi$ onde a é o inteiro mais próximo de $\frac{xm+yn}{m^2+n^2}$ e b é o inteiro mais próximo de $\frac{ym-xn}{m^2+n^2}i$ teremos

$$\left|\frac{xm+yn}{m^2+n^2} - a\right| \leq \frac{1}{2}, \left|\frac{ym-xn}{m^2+n^2} - b\right| \leq \frac{1}{2}.$$

Daí,

$$N(r) = N(\beta)N\left(\frac{\alpha}{\beta} - q\right) \leq N(\beta)\left(\left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2\right) = \frac{N(\beta)}{2} < N(\beta)$$

Perceba que q é escolhido em $\mathbb{Z}[i]$ e que r, apesar da escrita carregada, é $\alpha - q\beta$. Logo $r \in \mathbb{Z}[i]$. Portanto, o resultado está demosntrado.

□

Note que os argumentos utilizados na demonstração mostram a existência da divisão euclidiana, mas não garantem a unicidade de quociente ou resto. A unicidade, de fato, não é verdadeira. O exemplo a seguir ilustra essa situação.

Exemplo 3.4. Neste exemplo vamos exibir dois pares diferentes de quociente e resto para uma mesma divisão de inteiros de Gauss.

$$15 + 19i = (10 - 2i)(1 + 2i) + (1 + i).$$

Como $N(1 + i) = 2 < 5 = N(1 + 2i)$, a expressão acima é uma divisão euclidiana de $15 + 19i$ por $1 + 2i$ obtendo quociente $10 - 2i$ e resto $1 + i$.

De outro modo,

$$15 + 19i = (11 - 2i)(1 + 2i) + (-i).$$

Como $N(-i) = 1 < 5 = N(1+2i)$, a expressão acima é uma divisão euclidiana de $15+19i$ por $1 + 2i$ obtendo quociente $11 - 2i$ e resto $-i$.

Como consequência do Teorema 3.1 e do Teorema 2.1 temos que $\mathbb{Z}[i]$ é um domínio de ideais principais e um domínio de fatoração única. Assim, $\pi \in \mathbb{Z}[i]$ é primo se, e somente se, é irredutível.

Dizemos que dois inteiros de Gauss α e β são coprimos (ou relativamente primos) quando todo divisor comum destes é unidade. Além disso, dizemos que γ é máximo divisor comum de α e β quando $\gamma \mid \alpha$, $\gamma \mid \beta$ e se δ é tal que $\delta \mid \alpha$ e $\delta \mid \beta$, então $\delta \mid \gamma$.

Proposição 3.5. *Qualquer que seja $z \in \mathbb{Z}$ com $|z| \neq 1$ os inteiros de Gauss $z+i$ e $z-i$ são coprimos.*

Demonstração. Se γ é um divisor comum de $z+i$ e $z-i$, então $\gamma \mid [(z+i)-(z-i)] = 2i$. Segue que $\gamma \mid 2$. Se fosse $\gamma = 2$, teríamos $2 \mid (z+i)$, o que é absurdo.

Como $\gamma \mid 2 = -i(1+i)^2$ e $1+i$ é irredutível (logo primo), tem-se que $\gamma \mid (1+i)$. Se fosse $\gamma = 1+i$ teríamos $z+i = (x+yi)(1+i)$, $z-i = (x-yi)(1-i) = -i(x-yi)(1+i) = (y-xi)(1+i)$, para algum $x+yi \in \mathbb{Z}[i]$. Daí, teríamos

$$\begin{cases} x-y=z \\ x+y=1 \end{cases} \text{ e } \begin{cases} x+y=z \\ y-x=-1 \end{cases}$$

de onde encontramos $z=1$, contradizendo o fato de $|z| \neq 1$. Portanto, γ tem que ser uma unidade. Consequentemente, $z+i$ e $z-i$ são coprimos.

□

Observe que $1-zi = -i(z+i)$ e $1+zi = i(z-i)$ e, portanto, o resultado acima também é válido para os números $1+zi$ e $1-zi$.

Proposição 3.6. *Se $x \in \mathbb{Z}$ é ímpar, então $x+2i$ e $x-2i$ são coprimos.*

Demonstração. Se $d \in \mathbb{Z}[i]$ é um divisor comum de $x+2i$ e $x-2i$, então $d \mid 4i = (x+2i)-(x-2i)$. Logo, $d \mid 4 = 2^2 = -(1+i)^4$. Como $1+i$ é irredutível (portanto, primo) e $\mathbb{Z}[i]$ tem fatoração única, existe uma unidade $u \in \mathbb{Z}[i]$ e um natural $n \in \{0,1\}$ tais que

$$d = u(1+i)^n, \exists n \in \{0,1,2,3,4\}.$$

Como $-i(1+i)^2 = 2 \nmid x+2i$, tem-se que $n \in \{0,1\}$.

Suponha $n=1$, então $1+i \mid x+2i$, isto é, existe $a+bi \in \mathbb{Z}[i]$ tal que $(a+bi)(1+i) = (x+2i)$. Daí,

$$\begin{cases} a-b=x \\ a+b=2 \end{cases} \Rightarrow 2a = x+2 \Rightarrow 2 \mid x \text{ (absurdo, pois } x \text{ é ímpar).}$$

Logo, $1+i \nmid x+2i$.

Portanto, $n=0$ e d é uma unidade, concluindo que $x+2i$ e $x-2i$ são coprimos .

□

Proposição 3.7. *Se α e β são inteiros de Gauss coprimos e $\alpha\beta = a^n$ para algum $a \in \mathbb{Z}[i]$, então existem inteiros de Gauss γ e δ tais que $\alpha = \gamma^n$ e $\beta = \delta^n$*

Demonstração. Sejam $\alpha = p_1^{a_1}p_2^{a_2}\dots p_k^{a_k}$ e $\beta = q_1^{b_1}q_2^{b_2}\dots q_r^{b_r}$ as fatorações em primos de α e β. Como α e β são coprimos então $p_i \neq uq_j$ quaisquer que sejam $i = 1, 2, \dots, k$, $j = 1, 2, \dots, r$ e u unidade de $\mathbb{Z}[i]$.

Desta forma, $a^n = p_1^{a_1}p_2^{a_2}\dots p_k^{a_k}q_1^{b_1}q_2^{b_2}\dots q_r^{b_r}$ é a fatoração em primos de a^n. Segue que existem inteiros a_i' e b_j' tais que $a_i = a_i'n$ e $b_j = b_j'n$ para todo $i = 1, 2, \dots, k$, $j = 1, 2, \dots, r$.

Por fim, sejam $\gamma = p_1^{a_1'}p_2^{a_2'}\dots p_k^{a_k'}$ e $\delta = q_1^{b_1'}q_2^{b_2'}\dots q_r^{b_r'}$, então $\alpha = \gamma^n$ e $\beta = \delta^n$.

□

3.4 Números primos

Se $z \in \mathbb{Z}[i]$ é redutível, isto é, se existem $x, y \in \mathbb{Z}[i]$ tais que $z = xy$, com $1 < N(x), N(y) < N(z)$, então $N(z)$ é redutível em $\mathbb{Z}_+$, pois $N(z) = N(x)N(y)$. Deste modo, se $N(z)$ é um primo em $\mathbb{Z}_+$, então z é um primo em $\mathbb{Z}[i]$, o que já nos fornece alguns números primos de $\mathbb{Z}[i]$.

Da definição da norma N, dado um primo $\pi \in \mathbb{Z}[i]$ tem-se $\pi | N(\pi)$. Desta forma, π divide pelo menos um dos fatores primos de $N(\pi)$ em $\mathbb{Z}_+$. Suponhamos que π divida pelo menos dois primos, p e q, em $\mathbb{Z}_+$. Como p e q são distintos podemos tomar $a, b \in \mathbb{Z}$ tais que $ap + bq = 1$. Daí $\pi \mid 1$, o que é absurdo. Logo, todo primo $\pi \in \mathbb{Z}[i]$ divide exatamente um fator de $N(\pi)$ primo em $\mathbb{Z}_+$.

Proposição 3.8. *Se $\pi = a + bi$ com $|ab| > 1$ é primo em $\mathbb{Z}[i]$ então π e $\overline{\pi}$ são relativamente primos.*

Demonstração. Se γ é um divisor comum de π e $\overline{\pi}$, então $\gamma \mid \pi$. Mas π é primo; logo, γ é uma unidade ou $\gamma = u_1\pi$, onde u_1 é uma unidade. Além disso, como $|ab| > 1$, tem-se $|a| > 1$ ou $|b| > 1$. Logo não podemos ter $a \mid \pi$ e $b \mid \pi$ simultaneamente. Se γ é uma unidade, o resultado está provado.

Por outro lado, se $\gamma = u_1\pi$, então $N(\gamma) = N(\pi) = N(\overline{\pi})$. Daí, $\overline{\pi} = u_2\gamma$, onde u_2 é uma unidade. Assim, $\overline{\pi} = u_1u_2\pi$. Mas u_1u_2 é uma unidade; portanto, deve-se ter $\overline{\pi} = u\pi$, com $u \in \{1, -1, i, -i\}$. Tem-se

$$u = 1 \Rightarrow \overline{\pi} = \pi \Rightarrow a - bi = a + bi \Rightarrow b = 0 \Rightarrow |ab| = 0.$$

$$u = -1 \Rightarrow \overline{\pi} = -\pi \Rightarrow a - bi = -a - bi \Rightarrow a = 0 \Rightarrow |ab| = 0.$$

$$u = i \Rightarrow \overline{\pi} = i\pi \Rightarrow a - bi = -b + ai \Rightarrow a = -b, \Rightarrow a \mid \pi, b \mid \pi.$$

$$u = -i \Rightarrow \overline{\pi} = -i\pi \Rightarrow a - bi = b - ai \Rightarrow a = b, \Rightarrow a \mid \pi, b \mid \pi.$$

Portanto, não pode ser $\gamma = u\pi$. Segue que γ é uma unidade e π e $\overline{\pi}$ são relativamente primos. De fato, π e $\overline{\pi}$ são ambos primos e este resultado prova que diferem por mais que uma multiplicação por unidade.

□

Observe que $1 + i$ é primo em $\mathbb{Z}[i]$ e $1 - i = -i(1 + i)$, mas neste caso $a = b = 1$, não ferindo, portanto, o resultado acima.

Teorema 3.2. *Os números primos em $\mathbb{Z}[i]$ são de uma das formas a seguir:*

(i) O primo $1 + i$ e seus produtos pelas unidades.

(ii) Os números primos $p \in \mathbb{Z}_+$ da forma $4k + 3$ e seus produtos pelas unidades.

(iii) Para cada p primo em $\mathbb{Z}_+$ da forma $4k + 1$, os números $\pi = a + bi, \overline{\pi} = a - bi$ tais que $a^2 + b^2 = p$, e seus produtos pelas unidades.

Demonstração. Seja π um primo em $\mathbb{Z}[i]$ então, como vimos no início dessa subseção, π divide exatamente um primo p em $\mathbb{Z}_+$. Temos então três possibilidades.

(i) $p = 2$.

(ii) p é da forma $4k + 3$.

(iii) p é da forma $4k + 1$.

Como $2 = (1 + i)(1 - i) = -i(1 + i)^2$, $1 + i$ é primo e $\mathbb{Z}[i]$ é um domínio de fatoração única, segue que (i) $\Rightarrow \pi = u(1 + i)$ onde u é uma unidade.

Seja p um primo em $\mathbb{Z}$ da forma $4k + 3$. Suponha que exista $\pi = a + bi \in \mathbb{Z}[i]$ tal que $\pi \mid p$. Então $p = \phi\pi$ para algum $\phi \in \mathbb{Z}[i]$. Como p é primo, segue da Proposição 3.3 que $\phi = \pm\overline{\pi}$. Como $p > 0$, deve ser $\phi = \overline{\pi}$. Desta forma, $p = \pi\overline{\pi} = a^2 + b^2$, o que gera uma contradição no módulo 4. Logo, se p é primo em $\mathbb{Z}$ da forma $4k + 3$, este não é redutível em $\mathbb{Z}[i]$ e, portanto, é primo em $\mathbb{Z}[i]$.

Seja $p = 4k + 1$ primo em $\mathbb{Z}$ e seja $x = 1 \cdot 2 \cdot \ldots \cdot \frac{p-1}{2}$, então

$$x \equiv 1 \cdot 2 \cdot \ldots \cdot \frac{p-1}{2} \pmod{p}.$$

Como x tem uma quantidade par de fatores, tem-se que

$$x \equiv (-1) \cdot (-2) \cdot \ldots \cdot \left(-\frac{p-1}{2}\right) \equiv (p-1) \cdot (p-2) \cdot \ldots \cdot \frac{p+1}{2} \pmod{p}.$$

Daí,

$$x^2 \equiv 1 \cdot 2 \cdot \ldots \cdot \frac{p-1}{2} \cdot \frac{p+1}{2} \cdot \ldots \cdot (p-2) \cdot (p-1) \equiv (p-1)! \equiv -1 \pmod{p}.$$

Segue que $p \mid (x^2+1) = (x+i)(x-i)$. Sendo π primo em $\mathbb{Z}[i]$ tal que $\pi \mid p$ temos duas opções, $\pi = p$ ou $\pi \notin \mathbb{Z}$.

Se fosse $\pi = p$ teríamos $p \mid (x+i)$ ou $p \mid (x-i)$ o que implicaria em $p \mid 1$, o que é absurdo.

Temos então $\pi \notin \mathbb{Z}$. Sendo $\pi = a+bi$, tem-se $p = \phi\pi$ o que implica $\phi = \overline{\pi}$ (como já foi visto nesta mesma demonstração). Pela Proposição 3.8, $p = \pi\overline{\pi}$ é a fatoração em primos de p, concluido que $\pi, \overline{\pi}$ e seus produtos pelas unidades são os únicos primos que dividem p, o que termina a demonstração.

□

Note que a Proposição 3.8 garante que no item (iii) os primos π e $\overline{\pi}$ diferem por mais que uma multiplicação por unidade.

Proposição 3.9. *Sejam $a, b \in \mathbb{Z}$, com $mdc(a,b) = 1$ e a com paridade diferente de b, então $a+bi$ e $a-bi$ são coprimos em $\mathbb{Z}[i]$.*

Demonstração. Suponha que a proposição seja falsa. Sem perda de generalidade, suponha a par e b ímpar. Se $d \in \mathbb{Z}[i]$ é um divisor comum de $a+bi$ e $a-bi$ e $\pi \in \mathbb{Z}[i]$ é um primo tal que $\pi \mid d$, então $\pi \mid 2a$ e $\pi \mid 2b$.

Se $\pi \nmid 2$, então $\pi \mid a$ e $\pi \mid b$. Daí, $N(\pi) \mid a^2$ e $N(\pi) \mid b^2$, contradizendo $mdc(a,b) = 1$.

Se $\pi \mid 2$, então $\pi = 1+i$. De $\pi \mid d$ segue que $a+bi = (c+di)(1+i)$ para algum $c+di \in \mathbb{Z}[i]$. Daí $a+bi = (c-d)+(c+d)i$, isto é

$$\begin{cases} a = c-d \\ b = c+d \end{cases}$$

Mas $c+d$ e $c-d$ possuem a mesma paridade, contradizendo o fato de a e b terem paridades diferentes.

Portanto, não existe $\pi \in \mathbb{Z}[i]$ primo tal que $\pi \mid d = mdc(a+bi, a-bi)$. Logo, d é uma unidade e os inteiros $a+bi$ e $a-bi$ são coprimos.

□

3.5 Aplicações

3.5.1 *Ternas pitagóricas*

Uma terna de números inteiros (a,b,c) é dita uma terna pitagórica quando $a^2+b^2 = c^2$.

Uma aplicação simples e interessante do que vimos a cerca dos inteiros de Gauss é encontrar a forma geral das ternas pitagóricas.

Teorema 3.3. *Se (a, b, c) é uma terna pitagórica, então existem $m, n, d \in \mathbb{Z}_+$, com $mdc(m, n) = 1$ tais que*

$$a = d(m^2 - n^2), b = d(2mn), c = d(m^2 + n^2).$$

Demonstração. Se (a, b, c) é uma terna pitagórica, então

$$a^2 + b^2 = c^2 \tag{2}$$

Se $d \in \mathbb{Z}$ é o mdc entre a e b então $d \mid a, d \mid b \Rightarrow d^2 \mid (a^2 + b^2) = c^2 \Rightarrow d \mid c$. Tome $a' = \frac{a}{d}, b' = \frac{b}{d}, c' = \frac{c}{d}$, então $a'^2 + b'^2 = \frac{a^2}{d^2} + \frac{b^2}{d^2} = \frac{c^2}{d^2} = c'^2$ e $mdc(a', b') = 1$.

Note que a' e b' não podem ser ambos pares, pois $mdc(a, b) = 1$; também não podem ser ambos ímpares, pois isto geraria uma contradição (mod 4). Assim, além de serem coprimos, a e b têm paridades diferentes.

Partindo desse ponto, temos

$$(a' + b'i)(a' - b'i) = c^2.$$

As Proposições 3.9 e 3.7 garantem que $a' + b'i$ e $a' - b'i$ são ambos quadrados perfeitos. Daí, existe $m + ni \in \mathbb{Z}[i]$ tal que $a' + b'i = (m + ni)^2 = (m^2 - n^2) + 2mni$ e $a' - b'i = (m - ni)^2 = (m^2 - n^2) - 2mni$, isto é,

$$\begin{cases} a' = m^2 - n^2 \\ b' = 2mn \end{cases} \Rightarrow c^2 = (m^2 - n^2)^2 + (2mn)^2 = m^4 + 2m^2n^2 + n^4 = (m^2 + n^2)^2.$$

Note que a' e b' são coprimos se, e somente se, m e n o são. Desta forma, as soluções de (2) são $a = d(m^2 - n^2), b = d(2mn)$, ou vice-versa. Consequentemente, $c = d(m^2 + n^2)$, onde m e n são coprimos.

□

3.5.2 *Representações como soma de dois quadrados*

Um problema interessante da aritmética de $\mathbb{Z}_+$ é encontrar os inteiros que podem ser escritos como soma de dois quadrados. Este problema já é uma boa aplicação, mas nesta subseção abordaremos um problema ainda mais interessante, cuja solução passa pelo primeiro problema. Encontraremos o número de formas de escrever um número inteiro como soma de quadrados a partir da sua fatoração em primos em $\mathbb{Z}$.

Teorema 3.4. *Dado $n \in \mathbb{Z}_+$, o número de pares $(a, b) \in \mathbb{Z}$ tais que $n = a^2 + b^2$ é igual a $4(x-y)$, onde x é o número de divisores de n da forma $4k+1$ e y é o número de divisores de n da forma $4k+3$.*

Demonstração.
Note que $n = a^2 + b^2 \Leftrightarrow n = (a+bi)(a-bi)$.

Seja $a + bi = (1+i)^k p_1^{\beta_1} \dots p_r^{\beta_r} q_1^{\alpha_1} \dots q_t^{\alpha_t}$ a fatoração em primos de $a+bi$ em $\mathbb{Z}[i]$, onde cada p_i é um primo em $\mathbb{Z}_+$ da forma $4k+3$ e cada q_i é tal que $N(q_i)$ é um primo em $\mathbb{Z}_+$ da forma $4k+1$. Assim, $a - bi = (1-i)^k p_1^{\beta_1} \dots p_r^{\beta_r} \overline{q_1}^{\alpha_1} \dots \overline{q_t}^{\alpha_t}$.

Daí,

$$n = 2^k p_1^{2\beta_1} \dots p_r^{2\beta_r} q_1^{\alpha_1} \dots q_t^{\alpha_t} \overline{q_1}^{\alpha_1} \dots \overline{q_t}^{\alpha_t},$$

onde os pares $q_i, \overline{q_i}$ são primos que diferem mais que uma multiplicação por unidade (Proposição 3.8). Desta forma, n se escreve como soma de quadrados se, e somente se, é da forma anterior, isto é, se, e somente se, todo primo da forma $4k+3$ que aparece na fatoração de n tem expoente par.

Portanto, o número de representações de n como soma de quadrados é zero se algum primo da forma $4k+3$ tem expoente ímpar na fatoração de n e, se todo primo da forma $4k+3$ tem expoente par na fatoração de n, equivale ao número de formas de escolhermos $c+di$ com

$$(c+di)(c-di) = \epsilon^k p_1^{2\beta_1} \dots p_r^{2\beta_r} q_1^{\alpha_1} \dots q_t^{\alpha_t} \overline{q_1}^{\alpha_1} \dots \overline{q_t}^{\alpha_t}.$$

Pelo teorema da fatoração única e pela multiplicidade do conjugado devemos ter

$$c + di = \epsilon(1+i)^k p_1^{2\beta_1} \dots p_r^{2\beta_r} q_1^{\gamma_1} \overline{q_1}^{\alpha_1 - \gamma_1} \dots q_t^{\gamma_t} \overline{q_t}^{\alpha_t - \gamma_t}, 0 \leq \gamma_i \leq \alpha_i.$$

De fato, o número de escolhas de $c+di$ é igual a quatro vezes o número de escolhas dos γ_i's, sendo quatro por causa do número de escolhas possíveis para ϵ. Cada γ_i pode ser escolhido de $\alpha_i + 1$ formas. Daí, se l é o número de representações de n como soma de quadrados, então

$$l = 4(\alpha_1 + 1) \dots (\alpha_t + 1).$$

Por outro lado, seja $n = 2^k p_1^{\gamma_1} \dots p_r^{\gamma_r} q_1^{\alpha_1} \dots q_t^{\alpha_t}$ a fatotação em primos de n em $\mathbb{Z}_+$, onde cada p_i é um primo da forma $4k+3$ e cada q_i é um primo da forma $4k+1$. Um divisor ímpar de n é da forma $d = p_1^{a_1} \dots p_r^{a_r} q_1^{b_1} \dots q_t^{b_t}$, com $0 \leq a_i \leq \gamma_i$ e $0 \leq b_i \leq \alpha_i$. Se $a_1 + \dots + a_r$ é par, então d é da forma $4k+1$. Caso contrário, é da forma $4k+3$. Se x é o número de divisores de n da forma $4k+1$ e y é o número de divisores de n da forma $4k+3$, pode-se verificar que se algum γ_i é ímpar então $x = y$, isto é, $x - y = 0$. Daí, $l = 0 = 4 \cdot 0 = 4(x-y)$. Verifica-se também que se todo γ_i é par, então $x - y = (\alpha_1 + 1) \dots (\alpha_t + 1)$. Daí, $l = 4(\alpha_1 + 1) \dots (\alpha_t + 1) = 4(x-y)$.

□

4 INTEIROS DE EISENSTEIN $\mathbb{Z}[\omega]$

Nesta seção iremos mostrar que $\mathbb{Z}[\omega]$, a exemplo de $\mathbb{Z}[i]$, é um domínio euclidiano, consequentemente um domínio de fatoração única. Estes resultados também serão utilizados na Seção 6.

4.1 Definição e resultados preliminares

Definimos o conjunto $\mathbb{Z}[\omega]$ dos inteiros de Eisenstein como o subconjunto dos complexos $\mathbb{Z}[\omega] = \{a + b\omega; a, b \in \mathbb{Z}\}$, onde $\omega = \frac{-1+\sqrt{-3}}{2}$, donde $\omega^2 + \omega + 1 = 0$. Veremos na Seção 5 que $\mathbb{Z}[\omega]$ é o anel dos inteiros de $\mathbb{Q}[\sqrt{-3}]$.

Assim como $\mathbb{Z}[i]$, por ser subanel de um corpo, $\mathbb{Z}[\omega]$ é um domínio. A exemplo do que já foi visto na Seção 3, $\mathbb{Z}[\omega]$ herda de $\mathbb{C}$ as definições de conjugado e norma. Em especial, $\overline{\omega} = \omega^2$, consequentemente $\overline{\omega} = -(1 + \omega)$. As propriedades descritas na Proposição 3.1 também são válidas em $\mathbb{Z}[\omega]$.

4.2 Norma e unidades

Seja $\xi = a + b\omega \in \mathbb{Z}[\omega]$. Então

$$\xi\overline{\xi} = (a + b\omega)\overline{(a + b\omega)} = (a + b\omega)(a + b\overline{\omega}) = (a + b\omega)[(a - b) - b\omega] =$$

$$= a^2 - ab - ab\omega + ab\omega - b^2\omega - b^2\omega^2 = a^2 - ab + b^2.$$

Notoriamente, $a^2 - ab + b^2 \in \mathbb{Z}_+, \forall a, b \in \mathbb{Z}$. Desta forma, $\xi\overline{\xi}$ é uma boa definição para norma em $\mathbb{Z}[\omega]$.

Definição 4.1. *Definimos a norma em $\mathbb{Z}[\omega]$ como a função $N : \mathbb{Z}[\omega] \to \mathbb{Z}_+$ que associa cada $\xi = a + b\omega$ o valor inteiro não negativo $N(\xi) = \xi\overline{\xi} = a^2 - ab + b^2$.*

Perceba que $N(\pm 1) = N(\pm\omega) = N(\pm(1+\omega)) = 1$. De fato, estes são os únicos elementos de norma 1 em $\mathbb{Z}[\omega]$. A afirmação que vamos provar a seguir é equivalente a esta e mostra que estes elementos são também as únicas unidades em $\mathbb{Z}[\omega]$.

Proposição 4.1. *$u \in \mathbb{Z}[\omega]$ é unidade se, e somente se, $u \in \{\pm 1, \pm\omega, \pm(1 + \omega)\}$.*

Demonstração. Seja $u = a + b\omega \in \mathbb{Z}[\omega]$ uma unidade. Então existe $u' \in \mathbb{Z}[\omega]$ tal que $uu' = 1$.

Note que

$$uu' = 1 \Rightarrow N(u)N(u') = 1 \Rightarrow N(u) = N(u') = 1 \Rightarrow a^2 - ab + b^2 = 1.$$

Se for $a = b$, então

$$a^2 - ab + b^2 = a^2 = b^2 = 1 \Rightarrow u = \pm(1 + \omega).$$

Se for, $a > b$, então $a^2 - ab > 0$. Daí,

$$a^2 - ab + b^2 > b^2 \Rightarrow 1 > b^2 \Rightarrow b = 0 \Rightarrow a = \pm 1 \Rightarrow u = \pm 1.$$

Analogamente, se for $a < b$ teremos

$$1 > a^2 \Rightarrow a = 0 \Rightarrow b = \pm 1 \Rightarrow u = \pm\omega.$$

□

A exemplo dos inteiros de Gauss, $u \in \mathbb{Z}[\omega]$ é unidade se, e somente se, $N(u) = 1$.

4.3 $\mathbb{Z}[\omega]$ é um domínio euclidiano

Teorema 4.1. *$\mathbb{Z}[\omega]$ é um domínio euclidiano.*

Demonstração. Devemos mostrar a existência de uma divisão euclidiana em $\mathbb{Z}[\omega]$, isto é, dados $\alpha = a + b\omega, \beta = c + d\omega \in \mathbb{Z}[\omega]$, com $\beta \neq 0$, existem $q, r \in \mathbb{Z}[\omega]$, tais que $\alpha = q\beta + r$, com $r = 0$ ou $N(r) < N(\beta)$. Na verdade, $r = 0 \Leftrightarrow N(r) = 0$, então a condição sobre r pode ser reescrita como $0 \leq N(r) < N(\beta)$.

Como $\beta \neq 0$, temos

$$\frac{\alpha}{\beta} = \frac{\alpha\overline{\beta}}{\beta\overline{\beta}} = \frac{(ac - bd) + (ad + bc - bd)\omega}{c^2 - cd + d^2} = \frac{ac - bd}{c^2 - cd + d^2} + \frac{ad + bc - bd}{c^2 - cd + d^2}\omega.$$

Tomando $q = m + n\omega$ onde m e n são os valores inteiros mais próximos de $\frac{ac-bd}{c^2-cd+d^2}$ e $\frac{ad+bc-bd}{c^2-cd+d^2}$, respectivamente, teremos

$$\left| m - \frac{ac - bd}{c^2 - cd + d^2} \right| \leq \frac{1}{2} \text{ e } \left| n - \frac{ad + bc - bd}{c^2 - cd + d^2} \right| \leq \frac{1}{2}.$$

Daí,

$$N(r) = N(\alpha - q\beta) = N\left(\beta\left(\frac{\alpha}{\beta} - q\right)\right) = N(\beta)N\left(\frac{ac - bd}{c^2 - cd + d^2} - m + \left(\frac{ad + bc - bd}{c^2 - cd + d^2} - n\right)\omega\right).$$

Logo,

$$N(r) \leq N(\beta)\left(\frac{1}{4}+\frac{1}{4}+\frac{1}{4}\right) < N(\beta).$$

□

Vejamos um exemplo de divisão euclidiana em $\mathbb{Z}[\omega]$.

Exemplo 4.1.
Como $N(\omega) = 1 < 3 = N(1-\omega)$, a igualdade $5+2\omega = (3+2\omega)(1-\omega)+\omega$ é uma divisão euclidiana de $5+2\omega$ por $1-\omega$, obtendo quociente $3+2\omega$ e resto ω.

O Teorema 4.1 implica que $\mathbb{Z}[\omega]$ é um domínio de ideais principais e de fatoração única. Na próxima seção iremos procurar os elementos primos de $\mathbb{Z}[\omega]$.

4.4 Números primos

A exemplo do que acontece em $\mathbb{Z}[i]$, utilizando as mesmas técnicas podemos provar que se $N(\pi)$ é primo então π é primo e todo primo de Eisenstein divide exatamente um primo em $\mathbb{Z}_+$. Além disso, como $\mathbb{Z}[\omega]$ é um domínio de ideais principais, as definições de elemento primo e irredutível são equivalentes.

Exemplo 4.2.
$1-\omega$ é primo em $\mathbb{Z}[\omega]$, uma vez que $N(1-\omega) = 1^2 - 1\cdot(-1) + (-1)^2 = 3$.

Teorema 4.2. *Os primos de Eisenstein são de uma das formas a seguir:*

(i) O primo $1-\omega$ e suas multiplicações pelas unidades.

(ii) Os primos inteiros da forma $3k+2$ e suas multiplicações pelas unidades.

(iii) Para cada primo inteiro p da forma $3k+1$, os primos $\pi, \overline{\pi} \in \mathbb{Z}[\omega]$ tais que $p = \pi\overline{\pi}$ e suas multiplicações pelas unidades.

Demonstração. Seja $\pi = a+b\omega \in \mathbb{Z}[\omega]$ primo, com $a, b \neq 0$ e seja p primo em $\mathbb{Z}_+$ tal que $\pi \mid p$. Então p é de uma das formas a seguir:

(i) $p = 3k$, para algum inteiro k.

(ii) $p = 3k+2$, para algum inteiro k.

(iii) $p = 3k+1$, para algum inteiro k.

Se (i), então $p = 3$, mas $3 = N(1-\omega) = (1-\omega)\overline{(1-\omega)}$. Além disso, $\overline{1-\omega} = 2+\omega = (1-\omega)(1+\omega)$. Daí, $3 = (1+\omega)(1-\omega)^2$ e, como $1-\omega$ é primo (Exemplo 4.2), esta é a fatoração em primos de 3. Portanto, os únicos primos de Eisenstein que dividem 3 são $1-\omega$ e suas multiplicações por unidades.

Se (ii), então a Proposição3.3 aplicada a $\mathbb{Z}[\omega]$, junto com o fato de p ser primo, garante que $p = N(\pi) = a^2 - ab + b^2$. Mas $a^2 - ab + b^2 \equiv 0, 1 \pmod 3$. Daí, p é primo

em $\mathbb{Z}[\omega]$.

Se (iii), pela lei de reciprocidade quadrática, temos

$$\left(\frac{p}{-3}\right)\left(\frac{-3}{p}\right) = (-1)^{(\frac{p-1}{2})(\frac{-3-1}{2})} = 1 \Rightarrow \left(\frac{-3}{p}\right) = 1.$$

Daí, existe um inteiro x tal que $p \mid (x-1)^2+3 = x^2-2x+1+4 = (x+2\omega)(x+2\omega^2)$. Como $p \nmid 2$, existe um primo $\pi \in \mathbb{Z}[\omega]$ tal que $\pi \mid p$ e, como p é primo em $\mathbb{Z}_+$, temos $p = \pi\overline{\pi}$. Logo, π e $\overline{\pi}$ são os únicos primos em $\mathbb{Z}[\omega]$ que dividem p. Isto termina a demonstração.

□

Proposição 4.2. *Se $a, b \in \mathbb{Z}$ são tais que $mdc(a,b) = 1$, então os inteiros de Eisenstein $a + b\omega$ e $\overline{a+b\omega} = (a-b) - b\omega$ são coprimos.*

Demonstração. Seja d um máximo divisor comum de $a+b\omega$ e $(a-b)-b\omega$ e seja $\pi \in \mathbb{Z}[\omega]$ primo tal que $\pi \mid d$. Então $\pi \mid b+2b\omega = b(1+2\omega) = b\omega(1-\omega) \Rightarrow \pi \mid b(1-\omega)$ e $\pi \mid (2a-b)$.

Se $\pi \nmid (1-\omega)$ então $\pi \mid b \Rightarrow \pi \mid 2a \Rightarrow \pi = 2u$ para alguma unidade $u \in \mathbb{Z}[\omega]$, pois caso contrário teríamos $\pi \mid a$, o que resultaria em $N(\pi) \mid a^2, N(\pi) \mid b^2$, contradizendo $mdc(a,b) = 1$. No entanto, $2 \nmid (a+b\omega)$. Logo, a hipótese $\pi \nmid (1-\omega)$ é falsa.

Como $\pi \mid (1-\omega)$, tem-se $\pi = u(1-\omega)^k$, para alguma unidade $u \in \mathbb{Z}[\omega]$ e para algum $k \in \mathbb{Z}_+$. Se $k \geq 1$, então $3 \mid d$. No entanto, $3 \nmid a+b\omega$. Logo, $k = 0$ e d é uma unidade, concluindo que $a+b\omega$ e $\overline{a+b\omega} = (a-b)-b\omega$ são coprimos.

□

Proposição 4.3. *Se α e β são inteiros de Eisenstein coprimos e $\alpha\beta = a^n$ para algum $a \in \mathbb{Z}[\omega]$, então existem inteiros de Eisenstein γ e δ tais que $\alpha = \gamma^n$ e $\beta = \delta^n$*

Demonstração. O único fato utilizado para provar a Proposição 3.7, que é a versão dessa proposição em $\mathbb{Z}[i]$, foi a fatoração única em $\mathbb{Z}[i]$. Portanto, como $\mathbb{Z}[\omega]$ é um domínio de fatoração única, a demosntração do resultado segue a mesma argumentação.

□

4.5 Alicações

4.5.1 *Triângulos com ângulo de* 60^o

Um problema interessante com solução elegante utilizando os inteiros de Eisenstein é encontrar todas as ternas de números inteiros positivos (a,b,c) que são lados de um triângulo com um ângulo de 60^o. Este problema é muito similar ao das ternas pitagóricas, diferindo apenas pelo fato de nas ternas pitagóricas o ângulo em questão ser 90^o.

Seja (a,b,c) uma terna de números inteiros positivos que são lados de um triângulo com um ângulo de 60^o. Sem perda de generalidade, suponha que a é o lado oposto ao

ângulo de 60º. Pela lei dos cossenos, temos

$$a^2 = b^2 + c^2 - 2bc\cos 60^o = b^2 - bc + c^2 \tag{3}$$

Seja $d = mdc(b, c)$ e sejam $b' = \frac{b}{d}, c' = \frac{c}{d}$. Temos

$$b'^2 - b'c' + c'^2 = \frac{b^2}{d^2} - \frac{bc}{d^2} + \frac{c^2}{d^2} = \frac{a^2}{d^2} = \left(\frac{a}{d}\right)^2.$$

Tomando então $a' = \frac{a}{d}$, teremos

$$a'^2 = b'^2 - b'c' + c'^2 = (b + c\omega)(\overline{b + c\omega}),\ \text{com}\ mdc(b, c) = 1.$$

Segue das Proposições 4.2 e 4.3 que $b' + c'\omega$ e $\overline{b' + c'\omega} = (b' - c') - c'\omega$ são ambos quadrados, isto é, existe $m + n\omega$ tal que $b' + c'\omega = (m + n\omega)^2$ e $(b' - c') -' c\omega = (m - n - n\omega)^2$. Daí,

$$\begin{cases} b' = m^2 - n^2 \\ c' = 2mn - n^2 \end{cases}$$

Por cosequência,

$a'^2 = b'^2 - b'c' + c'^2 = m^4 - 2m^2n^2 + n^4 - (2m^3n - m^2n^2 - 2mn^3 + n^4) + 4m^2n^2 - 4mn^3 + n^4 \Rightarrow$
$\Rightarrow a'^2 = m^4 - 2m^3n + 3m^2n^2 - 2mn^3 + n^4 = (m^2 - mn + n^2)^2.$

Desta forma, as soluções de 3 são $a = d(m^2 - mn + n^2), b = d(m^2 - n^2), c = d(2mn - n^2)$ e suas permutações.

5 ANÉIS DE INTEIROS DE $\mathbb{Q}[\sqrt{d}]$

Definimos $\mathbb{Q}[\sqrt{d}]$ como o conjunto $\{a + b\sqrt{d}; a, d \in \mathbb{Q}\}$, onde d é um inteiro livre de quadrados.

Em $\mathbb{Q}[\sqrt{d}]$ definimos as operações + (adição) e · (multiplicação), pondo

$$(a + b\sqrt{d}) + (e + f\sqrt{d}) = (a + e) + (b + f)\sqrt{d}$$
$$(a + b\sqrt{d})(e + f\sqrt{d}) = (a + b\sqrt{d}) \cdot (e + f\sqrt{d}) = (ae + dbf) + (af + be)\sqrt{d}$$

Com as operações acima descritas, prova-se facilmente que $\mathbb{Q}[\sqrt{d}]$ é um corpo.

Dado $\alpha = a + b\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$, definimos o conjugado de α como $\overline{\alpha} = a - b\sqrt{d}$ e a norma $N(\alpha) = \alpha\overline{\alpha} = a^2 - db^2$. Sempre que $d < 0$ teremos $N(\alpha) \geq 0, \forall\alpha$. Além disso, $N(\alpha) = 0 \Leftrightarrow \alpha = 0$.

5.1 Resultados preliminares

O objeto de estudo desta seção são os anéis de inteiros quadráticos de $\mathbb{Q}[\sqrt{d}]$, que serão chamados, simplesmente, inteiros de $\mathbb{Q}[\sqrt{d}]$.

Definimos o anel dos inteiros de $\mathbb{Q}[\sqrt{d}]$ como o conjunto

$$\{\alpha \in \mathbb{Q}[\sqrt{d}]; \alpha \text{ é raiz de um polinômio } P(x) = x^2 + a_1x + a_0 \in \mathbb{Z}[x]\}.$$

Um resultado muito importante dessa seção é a caracterização dos anéis de inteiros de $\mathbb{Q}[\sqrt{d}]$, descrita no resultado a seguir, que pode ser encontrado em DUMMIT and FOOTE (2004) e CONRAD (2014).

Teorema 5.1. *Dado $d \in \mathbb{Z}$ livre de quadrados, o anel de inteiros de $\mathbb{Q}[\sqrt{d}]$ é*
(i) $\mathbb{Z}[\sqrt{d}]$, se $d \equiv 2, 3 \pmod 4$.
(ii) $\mathbb{Z}\left[\frac{-1+\sqrt{d}}{2}\right]$, se $d \equiv 1 \pmod 4$.

Exemplo 5.1.
$\mathbb{Z}[i] = \mathbb{Z}[\sqrt{-1}]$ é o anel de inteiros de $\mathbb{Q}[\sqrt{-1}]$, uma vez que $-1 \equiv 3 \pmod 4$.
$\mathbb{Z}[\omega] = \mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$ é o anel de inteiros de $\mathbb{Q}[\sqrt{-3}]$, uma vez que $-3 \equiv 1 \pmod 4$.

De fato, apesar de, intuitivamente, sermos levados a pensar que o anel de inteiros de $\mathbb{Q}[\sqrt{d}]$ é sempre $\mathbb{Z}[\sqrt{d}]$, isto não é sempre verdade. Veja o seguinte exemplo.

Exemplo 5.2. $\omega = \frac{-1+\sqrt{-3}}{2} \notin Z[\sqrt{-3}]$, mas $\omega \in \mathbb{Q}[\sqrt{-3}]$ e é raiz de $x^2 + x + 1 \in \mathbb{Z}[x]$, logo é um inteiro de $\mathbb{Q}[\sqrt{-3}]$ e, portanto, o anel de inteiros de $\mathbb{Q}[\sqrt{-3}]$ não se restringe a

$\mathbb{Z}[\sqrt{-3}]$.

Na verdade, sempre que $d \equiv 1 \pmod 4$, o elemento $\frac{-1+\sqrt{d}}{2} \in \mathbb{Q}[\sqrt{d}]$ é tal que $\frac{-1+\sqrt{d}}{2} \notin \mathbb{Z}[\sqrt{d}]$ e $\frac{-1+\sqrt{d}}{2}$ é raiz de $x^2 + x + \frac{1-d}{4} \in \mathbb{Z}[x]$.

5.2 Anéis de inteiros de $\mathbb{Q}[\sqrt{d}]$ que são domínios de fatoração única

Um dos principais problemas do estudo dos corpos $\mathbb{Q}[\sqrt{d}]$ é encontrar os valores de d que tornam o anel de inteiros de $\mathbb{Q}[\sqrt{d}]$ um domínio de fatoração única. Nas Seções 3 e 4 mostramos que o anel de inteiros de $\mathbb{Q}[\sqrt{d}]$ para $d \in \{-1, -3\}$ é um domínio de fatoração única. A seguir mostraremos que isto também é verdade para $d = -2$.

Proposição 5.1. *$\mathbb{Z}[\sqrt{-2}]$ é um domínio euclidiano e, portanto, um domínio de fatoração única.*

Demonstração. Devemos mostrar que dados $\alpha = a + b\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}]$ e $\gamma = c + d\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}]$, existem $q, r \in \mathbb{Z}[\sqrt{-2}]$ tais que $\alpha = q\gamma + r$, com $N(r) < N(\gamma)$.

Note que

$$\frac{\alpha}{\gamma} = \frac{\alpha\overline{\gamma}}{N(\gamma)} = \frac{ac + 2bd}{c^2 + 2d^2} + \frac{bc - ad}{c^2 + 2d^2}\sqrt{-2}.$$

Tomando $q = m + n\sqrt{-2}$, onde m e n são os inteiros mais próximos de $\frac{ac+2bd}{c^2+2d^2}$ e $\frac{bc-ad}{c^2+2d^2}$, respectivamente, então

$$\left|\frac{ac + 2bd}{c^2 + 2d^2} - m\right| \leq \frac{1}{2}, \left|\frac{bc - ad}{c^2 + 2d^2} - n\right| \leq \frac{1}{2}.$$

Daí,

$$r = \alpha - q\gamma = \frac{\alpha}{\gamma}\gamma - q\gamma = (\frac{\alpha}{\gamma} - q)\gamma$$

e

$$N(r) = N\left(\left(\frac{\alpha}{\gamma} - q\right)\gamma\right) = N(\gamma)N\left(\frac{\alpha}{\gamma} - q\right) \leq N(\gamma)\left(\left(\frac{1}{2}\right)^2 + 2\left(\frac{1}{2}\right)^2\right) = \frac{3}{4}N(\gamma) < N(\gamma).$$

Portanto, existe um algoritmo de divisão em $\mathbb{Z}[\sqrt{-2}]$, conluindo que este domínio é euclidiano e, consequentemente, de fatoração única.

□

De fato, $\mathbb{Z}[\sqrt{-2}]$ é o anel dos inteiros de $\mathbb{Q}[\sqrt{-2}]$, uma vez que $-2 \equiv 2 \pmod 4$. Os resultados obtidos nas Seções 3 e 4, juntamente com a Proposição 5.1 garantem que os anéis de inteiros de $\mathbb{Q}[\sqrt{d}]$ com $d < 0$ são domínios de fatoração única se $d \geq -3$.

Proposição 5.2. *Se a e b são inteiros não nulos tais que $mdc(a,b)=1$, então $a+b\sqrt{-2}$ e $a-b\sqrt{-2}$ são coprimos em $\mathbb{Z}[\sqrt{-2}]$.*

Demonstração. Se π é um primo em $\mathbb{Z}[\sqrt{-2}]$ tal que $\pi \mid (a+b\sqrt{-2})$ e $\pi \mid (a-b\sqrt{-2})$, então $\pi \mid 2a$ e $\pi \mid 2b\sqrt{-2}$. Se $\pi \nmid 2$, então $\pi \nmid \sqrt{-2}$, concluindo que $\pi \mid a$ e $\pi \mid b$, contrariando $mdc(a,b)=1$. Por outro lado, se $\pi \mid 2 = -\sqrt{-2}^2$, então $\pi \mid \sqrt{-2}$. Como $\sqrt{-2}$ é irredutível em $\mathbb{Z}[\sqrt{-2}]$, tem-se que $\pi = u\sqrt{-2}$, onde u é uma unidade em $\mathbb{Z}[\sqrt{-2}]$, isto é, $u \in \{1,-1\}$ (Proposição 5.5). No entanto, $\sqrt{-2} \nmid a+b\sqrt{-2}$. Logo, não é possível tomar um primo $\pi \in \mathbb{Z}[\sqrt{-2}$ tal que $\pi \mid (a+b\sqrt{-2})$ e $\pi \mid (a-b\sqrt{-2})$, concluido que todo divisor comum de $a+b\sqrt{-2}$ e $a-b\sqrt{-2}$ é unidade.

□

Proposição 5.3. *Seja R um domínio de fatoração única e sejam $\alpha, \beta \in R$ primos entre si tais que $\alpha\beta = a^n$, para algum $a \in R$ e algum $n \in \mathbb{N}$. Então, existem $\gamma, \delta \in R$ tais que $\alpha = \gamma^n, \beta = \delta^n$.*

Demonstração. A demonstração deste fato é idêntica a da Proposição 3.7, uma vez que o único argumento utilizado foi o fato de $\mathbb{Z}[i]$ ser um domínio de fatoração única.

□

Proposição 5.4. *Seja R um domínio euclidiano e sejam $a,b,c,d \in R$ tais que $ab=cd$. Existem $m,n,p,q \in R$ tais que $a=mn, b=pq, c=mp, d=nq$.*

Demonstração. Como R é um domínio euclidiano, podemos sempre calcular o máximo divisor comum de dois elementos de R.

Seja $m = mdc(a,c)$. Tome $n = \frac{a}{m}$ e $p = \frac{c}{m}$. Temos então $a = mn$ e $c = mp$. Além disso,

$$nb = pd, mdc(n,p) = 1.$$

Daí, concluímos que $n \mid d, p \mid b$ e $\frac{b}{p} = \frac{d}{n}$. Tome, por fim, $q = \frac{b}{p} = \frac{d}{n}$. Então $b = pq$ e $d = nq$, terminando a demonstração.

□

Proposição 5.5. *Se $d \in \mathbb{Z}$ é tal que $d \leq -2$, então as únicas unidades de $\mathbb{Z}[\sqrt{d}]$ são 1 e -1.*

Demonstração. É evidente que 1 e -1 são unidades em $\mathbb{Z}[\sqrt{d}]$. Seja $u = a+b\sqrt{d}$ uma unidade em $\mathbb{Z}[\sqrt{d}]$. Então existe $x \in \mathbb{Z}[\sqrt{d}]$ tal que $ux = 1$. Daí, $ux\overline{ux} = 1 \Rightarrow u\overline{u} =$

$N(u) = 1$. Por fim, $1 = N(u) = a^2 - db^2 \geq a^2 + 2b^2 \Rightarrow a^2 = 1, b^2 = 0 \Rightarrow u = \pm 1$.

□

Proposição 5.6. *Seja $R = \mathbb{Z}[\sqrt{d}]$, onde $d < -3$. Então $2, \sqrt{d}$ e $1 + \sqrt{d}$ são irredutíveis em R.*

Demonstração. Primeiro, perceba que dado $\alpha = a + b\sqrt{d}$ um elemento não nulo de $\mathbb{Z}[\sqrt{d}]$, temos $N(\alpha\beta) \geq N(\beta), \forall \beta \in \mathbb{Z}[\sqrt{d}]$. Além disso,

$$b = 0 \Rightarrow N(\alpha) = a^2.$$

$$b = 1 \Rightarrow N(\alpha) \geq -d, \text{ sendo } N(\alpha) = d \Leftrightarrow a = 0.$$

$$b > 1 \Rightarrow N(\alpha) > -d.$$

Se $\alpha, \beta \in \mathbb{Z}[\sqrt{d}]$ são tais que $\alpha\beta = 2$, então $N(\alpha)N(\beta) = 4$. Daí, há três opções:
(i) $N(\alpha) = 1, N(\beta) = 4 \Rightarrow 2$ é irredutível em $\mathbb{Z}[\sqrt{d}]$.
(ii) $N(\alpha) = 4, N(\beta) = 1 \Rightarrow 2$ é irredutível em $\mathbb{Z}[\sqrt{d}]$.
(iii) $N(\alpha) = 2, N(\beta) = 2$. De fato, esta não é uma possibilidade, pois $N(\alpha)$ é um quadrado perfeito ou $N(\alpha) \geq -d \geq 3$.

Portanto, 2 é irredutível em $\mathbb{Z}[\sqrt{d}]$.

Se $\alpha, \beta \in \mathbb{Z}[\sqrt{d}]$ são tais que $\alpha\beta = \sqrt{d}$, então $N(\alpha\beta) = -d$. Daí, $N(\alpha) \leq N(\alpha\beta) = d$. Temos então duas opções:
(i) $N(\alpha) = -d \Rightarrow N(\beta) = 1 \Rightarrow \sqrt{d}$ é irredutível em $\mathbb{Z}[\sqrt{d}]$.
(ii) $N(\alpha) < -d$. De fato, esta não é uma possibilidade pois, neste caso, $N(\alpha)$ seria um quadrado perfeito e $d = -N(\alpha)N(\beta)$ não seria livre de quadrados.

Portanto, $\sqrt{d}$ é irredutível em $\mathbb{Z}[\sqrt{d}]$.

Para $1 + \sqrt{d}$, basta perceber que não pode ser $N(\alpha) = -d$, pois $N(\alpha)N(\beta) = -d + 1$ e $mdc(-d, -d + 1) = 1$. Desta forma, $N(\alpha) = -d + 1$ ou $N(\alpha) < -d$ e repete-se os argumentos utilizados para provar que $\sqrt{d}$ é irredutível. Logo, $1 + \sqrt{d}$ também é irredutível em $\mathbb{Z}[\sqrt{d}]$.

□

Proposição 5.7. *Seja $R = \mathbb{Z}[\sqrt{d}]$, onde $d < -3$ é um inteiro livre de quadrados. Então R não é um domínio de fatoração única.*

Demonstração. Segue da Proposição 5.6 que 2 é irredutível em $\mathbb{Z}[\sqrt{d}]$.

Se d é ímpar, temos que $2 \mid (1 + \sqrt{d})(1 - \sqrt{d}) = 1 - d$, mas $2 \nmid (1 + \sqrt{d})$ e $2 \nmid (1 - \sqrt{d})$. Desta forma, 2 é um elemento irredutível de $\mathbb{Z}[\sqrt{d}]$ que não é primo.

Se d é par, temos que $2 \mid (2 + \sqrt{d})(2 - \sqrt{d}) = 4 - d$, mas $2 \nmid (2 + \sqrt{d})$ e $2 \nmid (2 - \sqrt{d})$. Desta forma, 2 é um elemento irredutível de $\mathbb{Z}[\sqrt{d}]$ que não é primo.

De todo modo, $\mathbb{Z}[\sqrt{d}]$ não é um domínio de ideais principais. Consequentemente, não é um domínio de fatoração única.

□

De fato, a Proposição 5.7 mostra que os anéis de inteiros de $\mathbb{Q}[\sqrt{d}]$, com $d \equiv 2, 3 \pmod 4, d < -3$, não são domínios de fatoração única. Resta-nos agora, para $d < 0$, os anéis de inteiros de $\mathbb{Q}[\sqrt{d}]$, com $d \equiv 1 \pmod 4, d < -3$.

O problema de encontrar os anéis de inteiros que são domínios de fatoração única foi primeiro solucionado para $d < 0$ por Kurt Heegner in 1952, e de maneira independente, por Stark e A. Baker em 1966 e pode ser encontrado em STARK (1970) e DUMMIT and FOOTE (2004). O terorema a seguir descreve o resultado para $d < 0$.

Teorema 5.2. *O anel dos inteiros de $\mathbb{Q}[\sqrt{d}]$, onde $d < 0$ é um inteiro livre de quadrados, é um domínio de fatoração única se, e somente se,*

$$d \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}.$$

Pouco se sabe a respeito da fatoração única nos anéis de inteiros de $\mathbb{Q}[\sqrt{d}]$ quando $d > 0$. De fato, esse caso, apesar de não fugir ao objetivo deste texto, não é contemplado por sua complexidade. Para maiores detalhes o leitor pode consultar as referências deste trabalho.

Concluida toda a parte teórica, agora nos resta aplicar essas técnicas nos problemas da próxima seção.

6 PROBLEMAS

Nesta seção serão enunciados alguns problemas relacionados com o tema desse trabalho, vários deles são problemas de olímpiadas bastante reconhecidas de Matemática, e apresentadas suas devidas soluções tomando como referencial teórico o conteúdo do trabalho.

Problema 6.1. *(OCM 2015)Considere o conjunto:*

$$\mathfrak{B} = \{a^2 + 3b^2; a, b \in \mathbb{Z}\}$$

Mostre que se $n \in \mathfrak{B}$ *e* p *é um fator primo de* n *tal que* $p \in \mathfrak{B}$*, então* $\frac{n}{p} \in \mathfrak{B}$*.*

Solução.
Note que

$$n = a^2 + 3b^2 \Leftrightarrow n = (a+b)^2 - (a+b)2b + (2b)^2 \Leftrightarrow n = \xi\overline{\xi},\ com\ \xi = (a+b) + 2b\omega.$$

Desta forma, $n \in \mathfrak{B} \Leftrightarrow \exists \xi = l + m\omega \in \mathbb{Z}[\omega]$*, com* m *par, tal que* $N(\xi) = n$*.*

Se p *é primo em* $\mathbb{Z}_+$ *e existe* $\pi = x + y\omega \in \mathbb{Z}[\omega]$ *tal que* $p = \pi\overline{\pi}$*, então* π *e* $\overline{\pi}$ *são primos em* $\mathbb{Z}[\omega]$ *(Teorema 3.2).*

Partindo desse ponto, se $n, p \in \mathfrak{B}$ *então existem* $\xi = l + m\omega, \pi = x + y\omega \in \mathbb{Z}[\omega]$*, com* m *e* y *pares e* π *primo, tais que* $n = N(\xi)$ *e* $p = N(\pi)$*. Daí, temos que* x *é ímpar, senão teríamos* $2|\pi$ *e* p *não seria primo em* $\mathbb{Z}_+$*.*

De $p|n$ *segue* $\pi\overline{\pi}|\xi\overline{\xi} \Rightarrow \pi|\xi\overline{\xi} \Rightarrow \pi|\xi$ *ou* $\pi|\overline{\xi}$*. Sem perda de generalidade, suponha* $\pi|\xi$*. Daí, temos* $\overline{\pi}|\overline{\xi}$ *e segue que*

$$\exists \sigma = u + v\omega \in \mathbb{Z}[\omega]\ tal\ que\ \xi = \sigma\pi, \overline{\xi} = \overline{\sigma\pi}.$$

Assim,

$$\frac{n}{p} = \frac{\sigma\pi\overline{\sigma\pi}}{\pi\overline{\pi}} = \sigma\overline{\sigma}.$$

Resta-nos mostrar que v *é par.*

Note que

$$\xi = \sigma\pi = (u + v\omega)(x + y\omega) = (ux - vy) + (uy + vx - vy)\omega$$

Note também que v *ímpar acarreta* $(uy + vx - vy)$ *ímpar, o que contradiz o fato de que* $\xi = l + m\omega$ *com* m *par. Logo,* v *é par e* $\frac{n}{p} = \sigma\overline{\sigma}, \sigma = u + v\omega$*. Portanto,* $\frac{n}{p} \in \mathfrak{B}$*.*

Problema 6.2. *Demonstrar que se um número inteiro pode ser escrito de maneira única como soma de dois quadrados, a menos da ordem dos quadrados, então tal número é*

primo.

Solução. *Seja $p \in \mathbb{Z}$, tal que existem $a, b \in \mathbb{Z}$ com $p = a^2 + b^2$ e esta é a única representação de p como soma de dois quadrados, a menos da ordem. Então $z = a + bi \in \mathbb{Z}[i]$ é tal que $p = uz\overline{z}$, onde $u \in \{1, -1, i, -1\}$, é a única maneira de escrever p como produto de inteiros de Gauss, logo z é um primo em $\mathbb{Z}[i]$. Daí, temos três opções (Proposição 3.2):*

(I) $z = 1 \pm i$.
(II) $z \in \mathbb{Z}$ *tal que* z *é um primo inteiro da forma* $4k + 3$.
(III) $z \in \mathbb{Z}[i]$ *tal que* $N(z) = z\overline{z}$ *é um primo inteiro da forma* $4k + 1$.
Daí, analisando caso a caso, temos

(I) $\Rightarrow p = (1 + i)(1 - i) = 2$.
(II) $\Rightarrow p$ *é um primo em* $\mathbb{Z}$
(III) $\Rightarrow p = z\overline{z}$ *é primo.*
Segue, de todo modo, que p é primo.

Problema 6.3. *Dado p um primo ímpar, prove que existem inteiros a, b e k tais que $a^2 + b^2 - 1 = kp$.*

Solução. *Dado p um primo ímpar, considere a progressão aritmática (a_n), com $a_1 = 1$ e $a_n = 1 + (n - 1) \cdot 4p$. Todos os termos desta sequência são da forma $4k + 1$.*

Pelo teorema de Dirichlet sobre progressões aritméticas, existem infinitos primos nesta sequência. Desta forma, seja a_m um termo de (a_n) que é primo, por ser da forma $4k + 1$, este não é primo de Gauss e existe $\pi = a + bi$ um primo de Gauss, tal que $a_m = \pi\overline{\pi} = a^2 + b^2$ (Proposição 3.2).

Note que

$$a_m = 1 + (m - 1) \cdot 4p.$$

Pondo $k = 4(m - 1)$, temos

$$a_m = kp + 1.$$

Portanto, existem $a, b, k \in \mathbb{Z}$ tais que

$$a^2 + b^2 = kp + 1,$$

concluindo a solução.

Problema 6.4. *Determine todos os pares de inteiros (x, y) tais que $y^3 = x^2 + 1$.*

Solução.
Note que x deve ser par, pois do contrário teríamos uma contradição módulo 8. Ainda,

$$y^3 = x^2 + 1 \Rightarrow y^3 = (x+i)(x-i).$$

A Proposição 3.9 implica que $(x+i), (x-i)$ são coprimos, portanto, são ambos cubos (Proposição 3.7).

Seja $u + vi \in \mathbb{Z}[i]$ tal que $x + i = (u+v)^3$, então $x + i = (a^3 - 3ab^2) + (3a^2b - b^3)i$. Daí,

$$\begin{cases} 3a^2b - b^3 = 1 \\ a^3 - 3ab^2 = x \end{cases}$$

Da primeira equação temos

$$3a^2b - b^3 = 1 \Rightarrow b(3a^2 - b^2) = 1 \Rightarrow |b| = |3a^2 - b^2| = 1.$$

Se $3a^2 - b^2 = 1$ temos $3a^2 = 2$, absurdo.

Se $3a^2 - b^2 = -1$ temos $3a^2 = 0 \Rightarrow a = 0$. Desta forma, $b = -1$ e $a = 0$, implicando em $x = a^3 - 3ab^2 = 0$ e $y^3 = x^2 + 1 \Rightarrow y = 1$.

Portanto, o único par que satisfaz as condições do problema é $(0, 1)$.

Problema 6.5. *Sejam $x, y, z \in \mathbb{N}$ tais que $xy = z^2 + 1$. Prove que existem inteiros a, b, c, d tais que $x = a^2 + b^2, y = c^2 + d^2$ e $z = ac + bd$.*

Solução. *Observe, inicialmente, que $xy = z^2 + 1 \Rightarrow xy = (z+i)(z-i)$, então existem $m, n, p, q \in \mathbb{Z}[i]$ tais que $x = mn, y = pq, z + i = mp, z - i = nq$ (Proposição 5.4). Como $mn, pq \in \mathbb{Z}_+$, temos que existem $k, l \in \mathbb{Q}_+$ tais que $n = k\overline{m}, p = l\overline{q}$ (Proposição 3.3). Assim,*

$$x = km\overline{m}, y = lq\overline{q}, z + i = lm\overline{q} \text{ e } z - i = kq\overline{m}.$$

Como $N(z+i) = N(z-i)$, temos que

$$N(mp) = N(nq) \Rightarrow N(lm\overline{q}) = N(k\overline{m}q) \Rightarrow k^2N(m\overline{q}) = l^2N(\overline{(m\overline{q})}) \Rightarrow l = k.$$

Sejam $u, v \in \mathbb{Z}_+$ tais que $\frac{u}{v} = k$ é uma fração irredutível, então

$$z + i = \frac{u}{v}m\overline{q} \text{ e } z - i = \frac{u}{v}\overline{m}q.$$

Como $z + i$ e $z - i$ são coprimos (Proposição 3.5) e $u \mid z + i, z - i$, conclui-se que u é uma unidade de $\mathbb{Z}[i]$. Como $u \in \mathbb{Z}_+$, tem-se $u = 1$.

De maneira análoga, temos também

$$z + i = \frac{v}{u}\overline{n}p \text{ e } z - i = \frac{v}{u}n\overline{p},$$

de onde segue que $v = 1$. *Desta forma,* $k = 1, n = \overline{m}$ *e* $p = \overline{q}$.

Se $m = a + bi$ *e* $q = c + di$, *então*

$$x = mn = m\overline{m} = a^2 + b^2,$$

$$y = pq = \overline{q}q = c^2 + d^2,$$

$$z = \frac{(z+i)+(z-i)}{2} = \frac{mp+nq}{2} = ac + bd.$$

Além disso, temos que $1 = \frac{(z+i)-(z-i)}{2i} = \frac{mp-nq}{2i} = bc - ad$.

Problema 6.6.

(a) (OIbM 2001) Prove que, para cada inteiro n, *o número de soluções inteiras de* $x^2 - xy + y^2 = n$ *é finito e divisível por* 6.

(b) Determine todas as soluções inteiras de $x^2 - xy + y^2 = 727$.

Solução.

(a) Se a equação não tiver solução, não há nada a fazer.

Se a equação tem alguma solução, então cada par (x, y) *solução de* $x^2 - xy + y^2 = n$ *está em correspondência com um inteiro de Eisenstein* $\xi = x + y\omega$ *tal que* $N(\xi) = x^2 - xy + y^2 = n$. *Desta forma,* ξ *é um divisor de* n. *Como o conjunto de divisores de* n *em* $\mathbb{Z}[\omega]$ *é finito, então o conjunto solução de* $x^2 - xy + y^2 = n$ *também é finito.*

Dada uma solução $\xi = 1\xi$, *o produto de* ξ *por cada uma das outras cinco unidades também é uma solução, pois* $N(u\xi) = N(u)N(\xi) = N(\xi)$. *Além disso, se* $u_1\xi = u_2\xi$ *então* $u_1 = u_2$, *isto é, o produto de* ξ *por cada unidade gera uma solução diferente. Logo, o número de soluções de* $x^2 - xy + y^2 = n$ *é divisível por* 6.

(b) 727 *é um primo da forma* $3k + 1$ *em* $\mathbb{Z}$. *Assim, dado* $\pi \in \mathbb{Z}[\omega]$ *tal que* $N(\pi) = \pi\overline{\pi} =$ 727, *tanto* π *quanto* $\overline{\pi}$ *são primos em* $\mathbb{Z}[\omega]$ *(Proposição 4.2). Logo,* $727 = u\pi\overline{\pi}$ *onde* $u \in \{1, -1, \omega, -\omega, 1 + \omega, -(1 + \omega)\}$ *é a única maneira de escrever* 727 *como produto de inteiros de Eisenstein, e as soluções de* $N(\xi) = 727$ *são os elementos do conjunto* $\{\pi, \overline{\pi}, -\pi, -\overline{\pi}, \omega\pi, \omega\overline{\pi}, -\omega\pi, -\omega\overline{\pi}, (1+\omega)\pi, (1+\omega)\overline{\pi}, -(1+\omega)\pi, -(1+\omega)\overline{\pi}\}$

Tomando $\pi = 31 + 13\omega$ *econtramos o conjunto solução* $\{31 + 13\omega, 18 - 13\omega, -31 - 13\omega, -18 + 13\omega, -13 + 18\omega, 13 + 31\omega, 13 - 18\omega, -13 - 31\omega, -18 - 31\omega, -31 - 18\omega, 18 + 31\omega, 31 + 18\omega\}$.

Portanto, os pares $\{(31, 13), (18, -13), (-31, -13), (-18, 13), (-13, 18), (13, 31), (13, -18),$

$(-13,-31),(-18,-31),(-31,-18),(18,31),(31,18)\}$ *são todas as soluções inteiras de* $x^2-xy+y^2=727$.

Problema 6.7. *Prove que se* n *é um inteiro positivo tal que a equação* $x^3-3xy^2+y^3=n$ *tem soluções inteiras* (x,y)*, então ela tem pelo menos três soluções.*

Solução. *Inicialmente perceba que dado* $x+y\omega\in\mathbb{Z}[\omega]$ *temos,*

$$(x+y\omega)^3=x^3+3x^2y\omega+3xy^2\omega^2+y^3\omega^3=(x^3-3xy^2+y^3)+(3x^2y-3xy^2)\omega.$$

Daí, sendo $u=x+y\omega$*, segue que* $x^3-3xy^2+y^3=n\Rightarrow n=Re(u^3)$*. Como* $u^3=(u\omega)^3=(u\omega^2)^3$*, basta mostrar que* $u=x+y\omega, u\omega=-y+(x-y)\omega$ *e* $u\omega^2=(y-x)+(-x)\omega$ *são distintos dois a dois.*

Se $u=u\omega$ *teríamos*

$$\begin{cases} x=-y \\ y=x-y \end{cases}$$

Se $u=u\omega^2$*, teríamos*

$$\begin{cases} x=y-x \\ y=-x \end{cases}$$

Se $u\omega=u\omega^2$*, teríamos*

$$\begin{cases} -y=y-x \\ x-y=-x \end{cases}$$

De todo modo segue $x=y=0$ *o que contradiz o fato de* x *e* y *serem positivos. Logo,* $u, u\omega$ *e* $u\omega^2$ *são dois a dois distintos. Portanto, se* (x,y) *é solução de* $x^3-3xy^2+y^3=n$ *então* $(-y,x-y)$ *e* $(y-x,-x)$ *também são soluções da equação, que tem pelo menos três soluções.*

Problema 6.8. *Resolva a equação* $x^2+4=y^3$.

Solução. *A equação pode ser escrita como* $(2+ix)(2-ix)=y^3$.

Se x *é impar então* $2+ix$ *e* $2-ix$ *são relativamente primos (Proposição 3.6). Daí ambos são cubos (Proposição 3.7). Desta forma,* $2+ix=(a+bi)^3, \exists a,b\in\mathbb{Z}$*. Comparando as partes real e imaginária, segue que*

$$\begin{cases} a(a^2-3b^2)=2 \\ 3a^2b-b^3 \end{cases}$$

Da primeira equação, segue $a=\pm1$ *ou* $a=\pm2$*. Tanto* $a=1$ *como* $a=2$ *não geram soluções inteiras para* b*. Se* $a=-1$*, então* $b=\pm1\Rightarrow x=\pm2$*, contradizendo o fato de* x

ser ímpar. Segue que $a = -2$ *e* $b = \pm 1 \Rightarrow x = \pm 11, y = 5$.

Se x *é par, então* y *também é par e podemos escrever* $x = 2u, y = 2v, \exists u, v \in \mathbb{Z}$. *Daí,* $x^2 + 4 = y^3 \Leftrightarrow 4u^2 + 4 = 8v^3 \Leftrightarrow u^2 + 1 = 2v^3$, *isto é,* $(u+i)(u-i) = 2v^3$. *Como* $u+i$ *e* $u - i$ *são relativamente primos e* $2 = (1+i)(1-i)$, *segue da foatoração única em* $\mathbb{Z}[i]$ *que* $u + i = (1+i)(a+bi)^3, \exists a, b \in \mathbb{Z}$. *Comparando as partes real e imaginária, temos*

$$\begin{cases} (a+b)(a^2 - 4ab + b^2) = 1 \\ (a-b)(a^2 + 4ab + b^2) = u \end{cases}$$

Da primeira equação segue que $a-b = a^2-4ab+b^2 = 1$ *ou* $a-b = a^2-4ab+b^2 = -1$. *Esta última equação não tem soluções inteiras. Temos, então,* $a = 1, b = 0$ *ou* $a = 0, b = -1$. *Daí,* $x = 2, y = 2$ *ou* $x = -2, y = 2$. *Portanto, todas as soluções de* $x^2 + 4 = y^3$ *são* $(\pm 11, 5), (\pm 2, 2)$.

Problema 6.9. *Prove que a equação* $x^3 - 2 = y^2$ *tem* $(3, \pm 5)$ *como únicas soluções inteiras.*

Solução. *Podemos escrever a equação como* $x^3 = y^2 + 2 = (y + \sqrt{-2})(y - \sqrt{-2})$. *Note que* y *tem que ser ímpar, pois caso contrário chegaríamos a uma contradição no módulo* 4.

Se $\delta = mdc(y + \sqrt{-2}, y - \sqrt{-2})$ *então* $\delta | -2\sqrt{-2} = \sqrt{-2}^3$. *É fácil ver que* $\sqrt{-2}$ *é irredutível em* $\mathbb{Z}[\sqrt{-2}]$. *Desta forma,* $\delta = u\sqrt{-2}^k$ *para algum* $k \in \{0, 1, 2, 3\}$. *Por outro lado, se* $\sqrt{-2} \mid (y \pm \sqrt{-2})$ *então* $\sqrt{-2} \mid x^3 = y^2 + 2$, *mas* x *é ímpar. Logo,* $\sqrt{-2} \nmid \delta$. *Conlui-se que* $y + \sqrt{-2}$ *e* $y - \sqrt{-2}$ *são relativamente primos. Desta forma, como o produto de* $y + \sqrt{-2}$ *e* $y - \sqrt{-2}$ *é um cubo e* $\mathbb{Z}[\sqrt{-2}]$ *é um domínio de fatoração única (Proposição 5.1), a Proposição 5.3 garante que são ambos cubos. Segue que* $y + \sqrt{-2} = (a + b\sqrt{-2})^3 \exists a + b\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}]$. *Comparando as partes real e imaginária, temos*

$$\begin{cases} y = a^3 - 6ab^2 \\ 1 = 3a^2b - 2b^3 \end{cases}$$

A segunda equação implica $b(3a^2 - 2b^2) = 1$. *Daí,*

$$b = 3a^2 - 2b^2 = 1 \Rightarrow a = \pm 1 \text{ ou } b = 3a^2 - 2b^2 = -1 \Rightarrow a \notin \mathbb{Z}.$$

Portanto, $y = -1 + 6 = 5$ *ou* $y = 1 - 6 = -5$ *e* $x^3 = (\pm 5)^2 + 2 = 27 \Rightarrow x = 3$ *são as únicas soluções inteiras de* $x^3 - 2 = y^2$.

Problema 6.10. *Seja* S *o conjunto dos inteiros positivos da forma* $a^2 + 2b^2$, *onde* a *e* b *são inteiros e* $b \neq 0$. *Prove que se* p *é um primo e* $p^2 \in S$, *então* $p \in S$.

Solução. *Como* $p^2 = a^2 + 2b^2 = (a + b\sqrt{-2})(a - b\sqrt{-2})$, *com* $b \neq 0$, *então sua fatoração em* $\mathbb{Z}[\sqrt{-2}]$ *não é composta apenas de primos inteiros. Se* $\pi = m + n\sqrt{-2}$, *com* $n \neq 0$, *é um primo tal que* $\pi \mid p^2$ *então* $\pi \mid p$ *e* $\overline{\pi} \mid p$. *Como* π *e* $\overline{\pi}$ *são coprimos (Proposição 5.2), temos* $N(\pi) = m^2 + 2n^2 \mid p$. *Desta forma, existe* $k \in \mathbb{Z}_+$ *tal que* $p = k(m^2 + n^2)$. *Como* p *é primo em* $\mathbb{Z}_+$ *conclui-se que* $k = 1$.

Portanto, $p = \pi\overline{\pi} = m^2 + 2n^2$, *onde* $n \neq 0$, *ou seja,* $p \in S$.

Problema 6.11. *(IMO - 2001) Sejam* $a, b, c, d \in \mathbb{Z}$, *com* $a > b > c > d > 0$. *Suponha que*

$$ac + bd = (b + d + a - c)(b + d - a + c).$$

Prove que $ab + cd$ *não é primo.*

Solução.

Primeiramente, note que

$$ac + bd = (b + d + a - c)(b + d - a + c) \Leftrightarrow$$

$$\Leftrightarrow ac + bd = b^2 + bd - ab + bc + bd + d^2 - ad + cd + ab + ad - a^2 + ac - bc - cd + ac - c^2 \Leftrightarrow$$

$$\Leftrightarrow a^2 - ac + c^2 = b^2 + bd + d^2 \Leftrightarrow$$

$$\Leftrightarrow (a + c\omega)(a + c\omega^2) = (b - d\omega)(b - d\omega^2)$$

Como $a > b > c > 1$, *então* $mdc(b, d) = k > 1 \Rightarrow k \mid (ab + cd)$ *e* $ab + cd$ *não é primo. Podemos, então, supor* $mdc(b, d) = 1$. *Analogamente, podemos supor* $mdc(a, c) = mdc(a, b) = mdc(b, c) = 1$. *De fato, isto significa que* $a + c\omega$ *e* $a + c\omega^2$ *são coprimos e que* $b - d\omega$ *e* $b - d\omega^2$ *são também coprimos (Proposição 4.2).*

Se $\pi \in \mathbb{Z}[\omega]$ *é um primo que divide* $b - d\omega$, *então* $\pi \nmid (b - d\omega^2), \overline{\pi} \mid (b - d\omega^2), \overline{\pi} \nmid (b - d\omega)$ *e* $\overline{\pi}$ *divide exatamente um dos números* $a + c\omega, a + c\omega^2$. *Sem perda de generalidade, suponhamos* $\overline{\pi} \mid (a + c\omega)$. *Assim,*

$$N(\pi) \mid (a + c\omega)(b - d\omega) = ab + cd + (bc - ad + cd)\omega.$$

Como $N(\pi) \in \mathbb{Z}$, *segue que* $N(\pi) \mid ab + cd$. *Se* $N(\pi) \neq ab + cd$, *então* $ab + cd$ *é redutível, logo não é primo.*

Suponha, então, que todo primo que divide $b - d\omega$ *é tal que* $N(\phi) = ab + cd$.

Observe que $\pi \mid (b - d\omega) \Rightarrow \overline{\pi} \nmid (b - d\omega)$ *e estes são os únicos elementos primos, a menos de multiplicações por unidades, com norma igual a* $N(\pi)$. *Daí, existe* ϵ *uma unidade em* $\mathbb{Z}[\omega]$ *e existe um natural* k *tal que* $b - d\omega = \epsilon\pi^k$ *e* $b + d + d\omega = b - d\omega^2 = \overline{\epsilon\pi}^k$. *Analogamente, existe* ϵ' *uma unidade em* $\mathbb{Z}[\omega]$ *tal que* $a - c - c\omega = a + c\omega^2 = \overline{\epsilon'}\pi^k$ *e*

$a + c\omega = \epsilon'\overline{\pi}^k$. *Desta forma, existe* $u \in \mathbb{Z}[\omega]$ *uma unidade tal que* $b + d + d\omega = u(a + c\omega)$.

Se fosse $u = \pm 1$ *teríamos* $c = \pm d$, *o que contraria o fato de* $mdc(c, d) = 1$.

Se fosse $u = \pm\omega$ *teríamos* $a = \pm b$, *o que contradiz* $mdc(a, b) = 1$.

Finalmente, se fosse $u = \pm(1 + \omega)$ *teríamos* $a = \pm d$, *o que contradiz* $mdc(a, d) = 1$.

Portanto, $b + d + d\omega \neq u(a + c\omega)$, *qualquer que seja a unidade* $u \in \mathbb{Z}[\omega]$, *consequentemente* $N(\pi) \neq ab + cd$ *e* $ab + cd$ *é redutível, logo não é primo.*

7 CONCLUSÃO

Neste trabalho, mostramos alguns conceitos de álgebra elementar, como as definições de anéis, domínios, corpos e ideais, ressaltando características e estruturas peculiares de alguns conjuntos, atráves de exemplos, proposições e problemas resolvidos. Os principais conjuntos abordados foram $\mathbb{Z}[i]$ (inteiros de Gauss), $\mathbb{Z}[\omega]$ (inteiros de Eisenstein) e $\mathbb{Z}[\sqrt{-2}]$, todos subconjuntos de $\mathbb{C}$, mostrando sua aplicabilidade em nível médio.

As ferramentas reunidas neste trabalho concedem ao professor material para aperfeiçoamento próprio ou para elaborar uma sequência de aulas ou um minicurso preparatório para alunos que visam disputar competições matemáticas. Como exemplo de conteúdo para tais fins, podemos destacar a caracterização das ternas pitagóricas e das ternas de inteiros que são lados de um triângulo com ângulo de 60^o.

Ainda, em nível menos trivial, foram abordados os conceitos de ideal principal e fatoração única, que trazem ao professor alguns conteúdos fundamentais como a definição de número primo e irredutível, cuja formulação no ensino fundamental rotineiramente é confundida sem prejuízo ao aprendizado dos discentes, cabendo ao professor o conhecimento mais profundo para compreender os motivos da equivalência entre as definições.

Por fim, este trabalho busca enriquecer o conhecimento dos professores de Matemática e melhorar o nível do ensino de Matemática na educação básica, finalidade esta que é um dos pilares do PROFMAT.

REFERÊNCIAS

ANDREESCU, Titu; ANDRICA, Dorin; CUCUREZEANU, Ion. *An introduction to Diophantine equations: a problem-based approach*. Springer Science & Business Media, 2010.

CONRAD, Keith. Factoring in quadratic fields. 2014.

DUMMIT, David Steven; FOOTE, Richard M. *Abstract algebra*, v. 3. Wiley Hoboken, 2004.

ENDLER, Otto. *Teoria dos números algébricos*, v. 15. IMPA, CNPq, 1986.

GARCIA, Arnaldo; LEQUAIN, Yves. *Elementos de álgebra*. IMPA, 2003.

GONÇALVES, Adilson. *Introdução à álgebra*. IMPA, 1979.

MARTINEZ, Fabio Brochero; MOREIRA, Carlos Gustavo; SALDANHA, Nicolau; TENGAN, Eduardo. Teoria dos Números: um passeio com primos e outros números familiares pelo mundo inteiro. *Coleção Projeto Euclides, IMPA*, 2013.

STARK, Harold M. *An introduction to number theory*. Tech. rep., Markham Publishing Company Chicago, Illinois, 1970.