Números Inteiros de Eisenstein

por

Diego de Lima Lisboa

Dissertação apresentada ao Corpo Docente do Mestrado Profissional em Matemática em Rede Nacional PROFMAT CCEN-UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

Área de Concentração: Aritmética

Aprovada por:

Prof. Dr. Bruno Henrique Carvalho Ribeiro - UFPB (Orientador)

Prof. Dr. Ricardo Burity Croccia Macedo - UFPB

Prof. Dr. Rodrigo Genuino Clemente - UFRPE

Agosto/2017

Catalogação na publicação
Seção de Catalogação e Classificação

L769n Lisboa, Diego de Lima.
Números inteiros de Eisenstein / Diego de Lima Lisboa. - João Pessoa, 2017.
38 f.

Orientação: Bruno Henrique Carvalho Ribeiro.
Dissertação (Mestrado) - UFPB/CCEN.

1. Matemática. 2. Números inteiros - Teoria. 3. Números inteiros - Anel - Eisenstein. I. Ribeiro, Bruno Henrique Carvalho. II. Título.

UFPB/BC

Universidade Federal da Paraíba
Centro de Ciências Exatas e da Natureza
PPGM - Departamento de Matemática
Mestrado Profissional em Matemática
em Rede Nacional PROFMAT

DIEGO DE LIMA LISBOA

NÚMEROS INTEIROS DE EISENSTEIN

Agosto/2017
João Pessoa - PB

Universidade Federal da Paraíba
Centro de Ciências Exatas e da Natureza
PPGM - Departamento de Matemática
Mestrado Profissional em Matemática
em Rede Nacional PROFMAT

Números Inteiros de Eisenstein

por

Diego de Lima Lisboa

sob orientação do

Prof. Dr. Bruno Henrique Carvalho Ribeiro

Dissertação apresentada ao Corpo Docente do Mestrado Profissional em Matemática em Rede Nacional PROFMAT-CCEN-UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

Agosto/2017
João Pessoa - PB

Dedicatória

Dedico esse trabalho e todo o sacrifício nele depositado aos meus amados pais, João Lisboa e Maria da Penha, que me ensinaram os valores das conquistas difíceis e tanto doaram de si para que este sonho se tornasse realidade

Agradecimentos

A árvore floresceu e os frutos estão sendo colhidos. Não posso esquecer-me de agradecer a cada um que plantou, direta ou indiretamente, uma semente de esperança, estímulo, confiança ou sabedoria dentro de mim, para que essa colheita acontecesse.

Agradeço ao meu orientador e amigo, Profº Dr. Bruno Henrique Carvalho Ribeiro, por todo apoio científico, material e psicológico durante a produção desse trabalho.

Aos meus pais, João Lisboa e Maria da Penha, que me educaram desde cedo e sempre se sacrificaram, para que eu pudesse chegar até aqui. À minha irmã, Joana D'arc, pelo companheirismo, compreensão das dificuldades e cooperação.

Aos meus tios, José Ivanildo e Ivone David, por sempre acreditar no meu potencial, me incentivando e estimulando nos estudos. Aos demais familiares, que estavam sempre dispostos e presentes a ajudar.

A meu amigo César, pela imensa ajuda, e o grande estímulo de sempre continuar. Ao meu amigo Anderson Mikael, pelo grande companheirismo nas horas difícies, principalmente em momentos de desestímulos e fraquezas. Ao meu amigo Eudes Mendes, pela grande força e colaboração em minha vida acadêmica. Ao meu mais novo amigo, pelo grande companheirismo e simplicidade de vê a vida, mesmo em momentos desesperadores.

À minha grande amiga Gilmara Santos, pelo auxílio no trabalho, me deixando dar as saídas necessárias para ir à universidade, sempre que preciso, me apoiando na busca cada vez maior de conhecimento. Ao meu amigo Erinaldo, pela ajuda em tudo que era possível e estava ao seu alcance. Ao colega de trabalho, Josuéliton, pelo auxílio, na parte em inglês.

À UFPB, na figura dos professores.

Aos colegas de sala, principalmente a Mailson, o qual sempre estivemos juntos, trazendo sempre aquele café indispensável para a turma, e se reunindo sempre que possível para o estudo das provas. A Manoel e Rafael, que me aturou durante a dissertação toda, tirando dúvidas do latex, e a todos que contribuíram, de alguma forma, para o desenvolvimento desse trabalho, muito obrigado.

A mim mesmo, por escolher ombros tão generosos para me apoiar e poder enxergar mais longe.

E, por fim, quero agradecer a alguém que não conheço bem, mas que acredito existir, alguns chamam de Deus, outros de Cosmo, alguns acham que é, simplesmente, o amor, e há tantos outros nomes quantos se possam imaginar. A esse ser, ou essa energia, onde estiver, e seja como for, obrigado por estar em mim e nos meus, conectando cada um, pois, unidos somos mais que o melhor de cada um.

Resumo

Norteado pelo desenvolvimento da Teoria dos Números Inteiros, o presente trabalho explorará de forma significativa o estudo das propriedades, teoremas, lemas e corolários desta teoria a um domínio mais geral, conhecido como o anel dos números Inteiros de Eisesntein, representado por $\mathbb{Z}[\omega]$, baseado na relação existente entre eles e o anel dos Inteiros Gaussianos, $\mathbb{Z}[i]$, buscando compreender de forma mais significativa, simploria e sistemática a aritmética deste anel, construindo as noções de divisibilidade entre dois inteiros de Eisenstein quaisquer, de como determinar um máximo divisor comum, de como identificar os irredutíveis e quais critérios utilizá-los, porquê que certos elementos primos $\mathbb{Z}$ não são irredutíveis em $\mathbb{Z}[\omega]$, construir a decomposição de irredutíveis deste anel tal como demonstrar a unicidade desta fatoração, além do interesse de ajudar ao aprimoramento de uma melhor compreeensão de vários problemas envolvendo números inteiros e ampliar de forma significativa a teoria existente nos Inteiros de Eisenstein.

Palavras-Chave: Inteiros, anel, Eisenstein, irredutíveis

Abstract

Based on the development of the Theory of Integer Numbers, the present work will study of the properties, theorems, lemmas and corollaries of this theory to a more general domain, known as the Eisesntein Integer Ring, represented by $\mathbb{Z}[\omega]$, based on the relationship between them and the ring of the Gaussian Integer,$\mathbb{Z}[i]$, seeking to understand in a most significant, simplistic and systematic way the arithmetic of this ring, constructing the notions of divisibility between two integers of Eisenstein, how to determine a common maximum divisor, how to identify the irreducible ones, and what criteria to use, why certain prime elements in $\mathbb{Z}$ are not irreducible in $\mathbb{Z}[\omega]$. We will also construct the irreducible decomposition of this ring as well as demonstrate the uniqueness of this factorization. Our interest is helping to improve a better understanding of various problems involving whole numbers and The theory of Eisenstein's Integers.

Keywords: Integers, ring, Eisenstein, irreducible

Sumário

Introdução

O fascínio e o encanto pelo números e suas propriedades acompanham o densenvolvimento das mais diversas civilizações das quais temos informações. Não há dúvidas de que o conceito de números inteiros é um dos mais clássicos, indispensável e fundamental das ciências em gerais. Isto fica claro, na obra "Os Elementos", de Euclides (360 a.C - 295 a.C), onde já aparecia o conceito como os dos números pares, ímpares, primos e compostos, entre outros. Assim, não é tão impressionante que a Teoria dos Números seja atualmente um dos ramos de pesquisas mais efervecentes da Matemática e que, mais do nunca, continua a fascinar e desafiar as atuais gerações de matemáticos.

Diferentemente de muitas áreas da Matemática, a Teoria dos Números se distingue muito menos por seus métodos e mais por seus problemas, cujo tema comum subjacente é o número inteiro, o qual tive o prazer de conhecer bem sua teoria na disciplina feita ao longo do curso, conhecida na grade do mestrado como Aritmética (MA14), uma das grandes motivadoras para o desenvolvimento da temática deste trabalho, pois nesta compreendemos que enquanto um analista utiliza-se de métodos analíticos para resolver seus problemas e dilemas, um algebrista emprega métodos algébricos para atacar questões. Em Teoria dos Números um mesmo problema pode requerer para sua resolução a utilização simultânea de métodos algébricos, analíticos, topológicos, geométricos e combinatórios, além de um pouco de imaginação.

Este aspecto multidisciplinar, aliado à simplicidade dos conceitos e à busca pelo caráter fundamental dos teoremas, corolários, lemas e propriedades, torna a Teoria dos Números, uma das áreas mais populares e misteriosas em toda a Matemática, gerando cada vez mais curiosos e pesquisadores a desenvolver e aprofundar teorias que possam ser embasadas em fundamentações teóricas já existentes, podendo ramificar outras novas teorias e aperfeiçoar cada vez mais outras.

Naturalmente a escolha do tema é um reflexo do gosto da experiência vivida ao longo do curso desencadeada pela disciplina Aritmética e a temática exposta, Inteiros de Eisenstein, será articulosamente baseada no estudo dos inteiros, desenvolvidos na disciplina, destacando-se os aspectos mais relevantes que estes números trazem para a teoria dos Números.

O grande motivador para o estudo dos Inteiros de Eisenstein foi desenvolvido através dos Inteiros de Gauss, que surgiu entre os anos de 1808 e 1825, quando o mesmo investigava questões relacionadas à reciprocidade cúbica, $x^3 \equiv q\,(mod\,p)$ e reciprocidade biquadrática, $x^4 \equiv q\,(mod\,p)$, com p e q números primos, quando percebeu que essa investigação se tornava mais simples no anel $\mathbb{Z}[i]$, conjunto chamado posteriormente de Inteiros Gaussianos, formado pelos números complexos da forma $a + bi$, onde a e b são números inteiros, do que no conjunto dos números inteiros.

Nessa investigação, Gauss observou que tal conjunto obtém uma série de propriedades parecidas como os inteiros, porém mais gerais, como por exemplo, a divisibilidade que se torna mais complexa, de modo que 5 é primo em $\mathbb{Z}$ e pode ser escrito como produto de dois elementos, $(1+2i)(1-2i)$, em $\mathbb{Z}[i]$. E foi também durante essa investigação, que Gauus analisou o Teorema Fundamental da Álgebra, teorema este que ofereceu a Gauss sua tese de doutorado, continua a valer em domínio de integridade mais geral, domínios esses que se possuírem fatoração única são chamados de domínio de integridade de Gauss.

O mesmo ainda descobriu que muito da Teoria de Euclides sobre a fatoração de inteiros poderia ser transportada para $\mathbb{Z}[i]$, com consequências importantes para a Teoria dos Números, desenvolvendo dessa forma a fatoração em irredutíveis para estes números e demonstrando que essa decomposição em irredutíveis é única, como acontece nos números inteiros. O uso que Gauss fez desse novo tipo de número foi de fundamental importância para a demonstração do Último Teorema de Fermat, fora que os mesmos também podem ser soluções de equações polinomais de coeficientes inteiros, gerando o que chamamos de números inteiros algébricos. Generalizando, dessa forma a noção de um número inteiro para um inteiro algébrico, oportunizando o conhecimento da Teoria dos Números Algébricos, surgida por meio das tentativas de solução da equação diofantina, mais conhecida como Equação de Fermat, $x^n + y^n = z^n$, de modo que os inteiros algébricos aparecem com naturalidade como ferramenta a tratar desse problema, tambem como nas resoluções das reciprocidade cúbicas, entre outras.

Norteado nessa conjuntura e abrangendo um pouco mais o campo para certos tipos de anéis, o trabalho desenvolverá o estudo dessas estruturas para os inteiros de Eisenstein, (Berlin, 16 de abril de 1823 - 11 de outubro de 1852), matemático alemão especialista em teoria do números e análise matemática, que provou diversos resultados matemáticos que escaparam até mesmo de Gauss.

Para este desenvolvimento, o trabalho será dividido em dois capítulos, no primeiro capítulo introduziremos a definição dos inteiros de Eisenstein, conjunto este formado pelos elementos da forma $a + b\omega, a, b \in \mathbb{Z}$, com ω sendo uma das raízes cúbicas da equação $x^3 + 1 = 0$. Estudando a norma de tais números, como se comporta a Divisibilidade e seus Critérios, o Teorema da Divisão, a idéia de associados para ideais que possuem mais de uma unidade, o Algoritmo de Euclides, tais como determinar um máximo divisor comum entre dois números de Eisenstein usando o algoritmo expandindo-o até chegarmos a compreensão do teorema de Bézout.

No segundo capítulo, definiremos os irredutíveis em $\mathbb{Z}[\omega]$ buscando quem são esses números, quais critérios que podem ser usados para identificá-los, quais tipos de propriedades estes trazem consigo, quando um inteiro primo em $\mathbb{Z}$ também será irredutível em $\mathbb{Z}[\omega]$, construindo a partir desse conhecimento o desenvolvimento da decomposição de um Inteiro de Eisenstein em produto de irredutíveis de inteiros de Eisenstein, demonstrando ainda que esta decomposição pode também ser única.

Sendo este estudo motivado na busca de querer oferecer uma expansão dos inteiros de Gauss aos inteiros de Eisenstein, objetivando desenvolver um pouco dessa teoria aritmética dos inteiros em campos mais gerais, assim como ampliar o conhecimento desses números, facilitar métodos e critérios de sua estrutura algébrica, expandindo ao máximo essa teoria, abordando naturalmente os aspectos mais re-

levantes que esta poderia exigir, bastando dizer que da árvore matemática de problemas a parte apreciável da Teoria dos Números é a abragência sobre os Números Inteiros.

Capítulo 1

Inteiros de Eisenstein

Neste capítulo ampliaremos o estudo das propriedades aritméticas dos números inteiros ao anel, estrutura algébrica munida de duas operações binárias: adição $(a,b) \to a+b$ e multiplicação $(a,b) \to a \cdot b$, $\mathbb{Z}[\omega]$, conhecido como inteiros de Eisenstein, sendo $\omega = \dfrac{-1+\sqrt{3}i}{2}$, uma das raízes cúbicas da unidade, $x^3 = 1 \Rightarrow x^3 - 1 = 0 \Rightarrow (x-1)(x^2+x+1) = 0$, mas especificadamente do momento $x^2+x+1=0$, com $\omega^2 = \left(\frac{-1+\sqrt{3}i}{2}\right)^2 = \frac{-4-2\sqrt{3}i}{4} = \frac{-1-\sqrt{3}i}{2} = \bar{\omega} = -1 - \left(\frac{-1+\sqrt{3}i}{2}\right) = -1-\omega$, na perspectiva de entender a arimética desse anel como também nos ajudar a compreender melhor problemas envolvendo números inteiros.

O anel dos inteiros de Eisenstein é o subanel do anel dos números complexos $\mathbb{C}$

$$\mathbb{Z}[\omega] \stackrel{\text{def}}{=} \{a + b \cdot \omega \in \mathbb{C} \,|\, a, b \in \mathbb{Z}\}$$

.

Munido das operações de adição e multiplicação herdadas de $\mathbb{C}$. Deste modo, se $z_1 = a + b\,\omega$ e $z_2 = c + d\,\omega$, então:

- $z_1 + z_2 = (a+c) + (b+d)\,\omega$;
- $z_1 \cdot z_2 = (a+b\,\omega)\cdot(c+d\,\omega) = ac + ad\,\omega + bc\,\omega + bd\,\omega^2 = (ac-bd) + (ad+bc-bd)w$

E norma definida pela função

$$\begin{array}{rcl} N : \mathbb{Z}[\omega] & \longrightarrow & \mathbb{Z} \\ a + b \cdot \omega & \longrightarrow & |z|^2 = z \cdot \bar{z} = a^2 - a \cdot b + b^2 \end{array}$$

De fato,

$$\begin{aligned} |z|^2 = z \cdot \bar{z} &= \left[\left(a - \frac{b}{2}\right) + \frac{b\sqrt{3}i}{2}\right] \cdot \left[\left(a - \frac{b}{2}\right) - \frac{b\sqrt{3}i}{2}\right] \\ &= \left(a - \frac{b}{2}\right)^2 + \left(\frac{b\sqrt{3}}{2}\right)^2 \\ &= a^2 - a\,b + \frac{b^2}{4} + \frac{3\,b^2}{4} \\ &= a^2 - a\,b + b^2 \end{aligned}$$

Observe que das definições acima apresentadas concluiremos facilmente que a função N é multiplicativa, ou seja, para quaisquer dois elementos a, b no domínio de N, tem-se $N(ab) = N(a)N(b)$, como mostraremos na proposição seguinte.

Proposição 1.1. *A função N é multiplicativa, isto é, $N(\alpha\, z) = N(\alpha) \cdot N(z)$, $\forall\, \alpha,\, z \in \mathbb{Z}[\omega]$.*

Demonstração. Sejam α, z quaisquer elementos de $\mathbb{Z}[\omega]$. Então,

$$\begin{aligned} N(\alpha\, z) &= \alpha\, z \cdot \overline{\alpha\, z} \\ &= \alpha \cdot z \cdot \bar{\alpha} \cdot \bar{z} \\ &= \alpha\, \bar{\alpha} \cdot z\, \bar{z} \\ &= N(\alpha) \cdot N(z) \end{aligned}$$

□

Elementos invertíveis com respeito a multiplicação de um anel é o que chamamos de unidades deste anel. Ou seja, existem c e $c^{'} \in \mathbb{Z}[\omega]$ tal que $c \cdot c^{'} = 1$.
O lema a seguir mostrará que o conjunto das unidades de $\mathbb{Z}[\omega]$, comparado com o dos $\mathbb{Z}$, $\{-1, +1\}$, tem quatro unidades a mais.

Lema 1.1. *O conjunto das unidades em $\mathbb{Z}[\omega]$, que denotaremos por $U(\mathbb{Z}[\omega])$, é um grupo cíclico de ordem 6 formado pelas raízes sextas da unidade, $\{\pm 1, \pm w, \pm w^2\}$.*

Demonstração. Seja $u \in \mathbb{Z}[\omega]$, com $u = a + b\,\omega$ uma unidade. Então, existe $v \in \mathbb{Z}[\omega]$, tal que $u \cdot v = 1$, e dessa forma, $N(u) \cdot N(v) = 1$.
Como $N(u)$ e $N(v)$ são inteiros, temos que $N(u) = N(v) = 1$.
Daí, $a^2 + b^2 - a\,b = 1 \Rightarrow (2a - b)^2 + 3\,b^2 = 4 \Rightarrow (2a - b, b) = (-1, \pm 1), (1, \pm 1), (\pm 2, 0)$
$\Rightarrow (a, b) = (\pm 1, 0), (0, \pm 1), (1, 1), (-1, -1)$.
Então, $U(\mathbb{Z}[\omega]) = \{\pm 1, \pm w, 1 + w, -1 - w\} = \{\pm 1, \pm w, \pm w^2\}$.
Porém precisamos ainda mostrar que $U(\mathbb{Z}[\omega])$ é um grupo cíclico.

Definição 1.1. *Um grupo G é cíclico se existe um elemento $a \in G$ tal que o grupo gerado por esse elemento a coinde com G.*

De fato, $G =< U(\mathbb{Z}[\omega]), \cdot >$ é ciclico, pois o elemento $(-\omega)$ gera G.
Note:

$$\begin{aligned}
(-\omega)^1 &= -\omega;\\
(-\omega)^2 &= (-\omega)\cdot(-\omega) = \omega^2;\\
(-\omega)^3 &= (-\omega)^2\cdot(-\omega) = \omega^2\cdot(-\omega) = (-1-\omega)\cdot(-\omega) = -1;\\
(-\omega)^4 &= (-\omega)^3\cdot(-\omega) = (-1)\cdot(-\omega) = \omega;\\
(-\omega)^5 &= (-\omega)^4\cdot(-\omega) = \omega\cdot(-\omega) = \omega^2;\\
(-\omega)^6 &= (-\omega)^5\cdot(-\omega) = -\omega^2\cdot(-\omega) = \omega^3 = \omega^2\cdot\omega = (-1-\omega)\cdot\omega = 1.
\end{aligned}$$

Daí, $< -\omega >= \{\pm 1, \pm\omega, \pm\omega^2\} = U(\mathbb{Z}[\omega])$.
Sendo $U(\mathbb{Z}[\omega])$ cíclico. □

Definida a caracterização dos elementos do anel $\mathbb{Z}[\omega]$, as operações munidas a eles, sua norma e suas unidades, partiremos para a construção da aritmética desses elementos, começando pela divisibilidade entre eles.

1.1 Divisibilidade

Na busca de características das propriedades de divisibilidade para os inteiros de Eisenstein, nos decaímos no seguinte problema, quando essa divisão será inteira? Objetivado por essa indagação mergulharemos na busca de tais características, percebendo pela definição atribuída a um número de Eisenstein, que a divisão entre eles tem a mesma definição dos inteiros.

Definição 1.2. *Dizemos que um inteiro de Eisenstein β divide um inteiro de Eisenstein α, se podemos encontrar um $c \in \mathbb{Z}[\omega]$ tal que $\alpha = c\cdot\beta$, e denotamos $\beta \mid \alpha$.*

Exemplo:

- $(1+2\,\omega) \mid (4+2\,\omega)$, pois

$$\begin{aligned}
(1+2\,\omega)\cdot(b+c\,\omega) &= 4+2\,\omega\\
(b-2c)+(c+2b-2c)\omega &= 4+2\,\omega\\
(b-2c)+(2b-c) &= 4+2\,\omega
\end{aligned}$$

  E assim $b-2c=4$ e $2b-c=2 \Rightarrow b=0$ e $c=-2 \Rightarrow b+c\omega = -2\,\omega \in \mathbb{Z}[\omega]$.

- $(-2-\omega) \nmid (3+2\omega)$, pois

$$\begin{aligned}
(-2-\omega)\cdot(a+b\omega) &= 3+2\omega\\
(-2a+b)+(-2b-a+b)\omega &= 3+2\omega\\
(-2a+b)+(-a-b)\omega &= 3+2\omega
\end{aligned}$$

  E assim $-2a+b=3$ e $-a-b=2 \Rightarrow a=\frac{-5}{3}$ e $b=\frac{-1}{3} \Rightarrow a+b\omega = -\frac{5}{3}-\frac{1}{3}\,\omega \notin \mathbb{Z}[\omega]$.

É de fundamental importância ressaltarmos que sendo A um anel, dizemos que dois elementos α, $\beta \in A$ são ditos associados se existir um $\delta \in U(A)$ tal que $\alpha = \delta \cdot \beta$.

Exemplo: Sejam $\alpha = 3 - 2\omega$ e $\beta = 2 + 5w$, então usando a definição de divisibilidade acima, teremos:

$$\begin{aligned} (3-2\omega)(a+b\omega) &= 2+5\omega \\ (3a+2b)+(3b-2a+2b)\omega &= 2+5\omega \\ (3a+2b)+(-2a+5b)\omega &= 2+5\omega \end{aligned}$$

E assim, $3a + 2b = 2$ e $-2a + 5b = 5 \Rightarrow a = 0$ e $b = 1 \Rightarrow a + b\omega = \omega$. Portanto, $2 + 5\omega = (\omega)(2 - 2\omega)$, sendo desta forma α e β associados.

Teorema 1.1. *O inteiro de Eisenstein $\alpha = a+b\,\omega$ é divisível por um número inteiro c se, e somente se, $c \,|\, a$ e $c \,|\, b$ em $\mathbb{Z}$.*

Demonstração. ($\Rightarrow$): Suponha que $c \,|\, (a + b\omega) \in \mathbb{Z}$, então $a + b\,\omega = c \cdot (m + n\,\omega)$ para algum $m, n \in \mathbb{Z}$, como os inteiros de Eisenstein é subgrupo do complexos $\mathbb{C}$, teremos assim $a = c \cdot m$ e $b = c \cdot n \Rightarrow c \,|\, a$ e $c \,|\, b$.
($\Leftarrow$): Se $c \,|\, a$ e $c \,|\, b$, então $a = c \cdot m$ e $b = c \cdot n$ para algum $m, n \in \mathbb{Z}$, e daí $a + b\,\omega = c\,m + c\,n\,\omega = c(m + n\,\omega)$, e portanto $c \,|\, (a + b\,\omega)$. □

No entanto, isso não significa que outros aspectos dos $\mathbb{Z}$ permanecem o mesmo para $\mathbb{Z}[\omega]$. Por exemplo, veremos que alguns primos de $\mathbb{Z}$ não são primos em $\mathbb{Z}[\omega]$. E que a multiplicidade da norma transforma as relações de divisibilidade em $\mathbb{Z}[\omega]$ em relações de divisibilidade em $\mathbb{Z}$.

Teorema 1.2. *Se $\alpha \,|\, \beta$ em $\mathbb{Z}[\omega]$, então $N(\alpha) \,|\, N(\beta)$ em $\mathbb{Z}$*

Demonstração. Se $\alpha \,|\, \beta \in \mathbb{Z}[\omega]$, então existe $\gamma \in \mathbb{Z}[\omega]$ tal que $\beta = \alpha \cdot \gamma$. Dessa forma, $N(\beta) = N(\alpha \cdot \gamma) = N(\alpha) \cdot N(\gamma) \to N(\alpha) \,|\, N(\beta)$.

□

O Teorema (1.2) tem uma propriedade interessante por propiciar de forma rápida e prática como verificar se um inteiro de Eisenstein não é divisível por outro inteiro de Eisenstein, de modo que transforma um problema de divisibilidade em $\mathbb{Z}[\omega]$ em $\mathbb{Z}$, trazendo um apelo óbvio, já que é mais confortável trabalhar com a divisibilidade em $\mathbb{Z}$.

Note também que o teorema (1.2), verificaria de forma mais rápida e prática que $(-2-\omega) \nmid (3+2\,\omega)$, pois a $N(-2-\omega) = (-2)^2 - (-2)\cdot(-1) + (-1)^2 = 4-2+1 = 3$ não divide $N(3+2\,\omega) = 3^2 - 3\cdot 2 + 2^2 = 9 - 6 + 4 = 7$, facilitando o processo para essa descorberta.

Porém é importante observar que a recíproca do teorema não é sempre verdadeira, observe que se $\alpha = 3+2\,\omega$ e $\beta = 6+2\,\omega$, $N(\alpha) = 3^2 - 3\cdot 2 + 2^2 = 7$ e $N(\beta) = 6^2 - 6\cdot 2 + 2^2 = 28$, e daí $N(\alpha) \,|\, N(\beta)$, e isto, não garante que $(3+2\,\omega) \,|\, (6+2\,\omega)$.

Objetivando facilitar a abordagem ao teorema da divisão em $\mathbb{Z}[\omega]$ observa-se que função norma N possui a propriedade Euclidiana, como apresentaremos na proposição a seguir.

Definição 1.3. *Uma função $f : A \setminus \{0\} \to \mathbb{Z}$, é dita Euclidiana,*

- *se $a, b \in A \setminus \{0\}$ e $b \,|\, a$, então $f(b) \leq f(a)$.*
- *se $a, b \in A \setminus \{0\}$, e $b \nmid a$, então existem $q, r \in A$ tais que $a = b \cdot q + r$, onde $f(r) < f(b)$.*

Proposição 1.2. *A função N é euclidiana.*

Demonstração. Sejam $\alpha, \beta \in \mathbb{Z}[\omega]$,

- se β divide α, existe $\gamma \in \mathbb{Z}[\omega]$ tal que $\alpha = \beta\,\gamma$, então $N(\beta) \leq N(\beta) \cdot N(\gamma) = N(\beta\,\gamma) = N(\alpha)$.
- se β não divide α, com $\beta \neq 0$, mostraremos que existem $q, r \in \mathbb{Z}[\omega]$ tais que $\alpha = \beta\,q + r$, onde $N(r) < N(\beta)$.
  De fato,
  Escreva $\frac{\alpha}{\beta} = x + y\,\omega$, com $x, y \in \mathbb{Q}$, e considere $m, n \in \mathbb{Z}$, os inteiros mais próximos de x e y, tais que $|x - m| \leq \frac{1}{2}$ e $|y - n| \leq \frac{1}{2}$. Então, tome $q = mx + n\omega$ e $r = \alpha - \beta\,q$.
  Que pela desigualdade triangular teremos,

$$\begin{aligned} \left|\frac{\alpha}{\beta} - q\right| &= |x + y\,\omega - (m + n\,\omega)| \\ &= |(x - m) + (y - n)\omega| \\ &\leq |x - m| + |y - m| \\ &\leq \frac{1}{2} + \frac{1}{2} = 1. \end{aligned} \tag{1.1}$$

  Note que como 1 e ω são linearmente independentes sobre $\mathbb{R}$, a primeira desigualdade é estrita, a menos que $x - m = 0$ ou $y - n = 0$, mas nestes dois casos a segunda desigualdade é estrita.
  Assim, multiplicando (1.1) por $|\beta|$, obteremos:

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

□

Analisando que a função N é Euclidiana, já temos a capacidade de compreender melhor o teorema da divisão para os Inteiros de Eisenstein, o que faremos a seguir.

1.2 Teorema da Divisão

O teorema da divisão em $\mathbb{Z}[\omega]$ é análogo à divisão com resto em $\mathbb{Z}$.

Teorema 1.3. *(Teorema da divisão) Para $\alpha, \beta \in \mathbb{Z}[\omega]$ com $\beta \neq 0$, existem $q, r \in \mathbb{Z}[\omega]$ tal que $\alpha = \beta\, q + r$ com $N(r) < N(\beta)$.*

A demonstração do Teorema está feita na proposição (1.2) acima.
Observe que os números q e r são o quociente e o resto da divisão, respectivamente, e o resto é limitado pelo tamanho de β (norma), que representa o divisor. Também é necessário observar que há uma sutileza na tentativa de calcular q e r, como comprovado na demonstração feita da proposição supracitada.
Para deixar claro a sutileza da escolha de q e r, acompanhe o seguinte exemplo.

Exemplo: Considere $\alpha = 13 + 7\,\omega$ e $\beta = 3 + 2\,\omega \Rightarrow N(\beta) = 3^2 - 3 \cdot 2 + 2^2 = 7$.
Note que pela representação queremos escrever $\alpha = \beta\, q + r$ onde $N(r) < N(\beta)$.
A ideia dessa problemática consiste em considerar a relação $\frac{\alpha}{\beta}$ e racionalizar o denominador $\frac{\alpha \cdot \bar{\beta}}{\beta \cdot \bar{\beta}}$, dessa forma teremos:
$\beta = 3+2\,\omega = 3+2\cdot\left(\frac{-1+\sqrt{3}i}{2}\right) = 2+\sqrt{3}i \Rightarrow \bar{\beta} = 2-\sqrt{3}i = 1-2\,\left(\frac{-1+\sqrt{3}i}{2}\right) = 1-2\,\omega$.
E assim, $\frac{\alpha \cdot \bar{\beta}}{\beta \cdot \bar{\beta}} = \frac{(13+7\,\omega)(1-2\,\omega)}{N(\beta)} = \frac{27-5\,\omega}{7} = \frac{27}{7} - \frac{5}{7}\omega$. Daí, observa-se que $\left(\frac{27}{7}\right) = 3,857...$ e $\left(-\frac{5}{7}\right) = -0,714...$, e substituindo $3,857...$ por 3 e $-0,714...$ por 0, temos $q = 3$, acarretando que:

$$\begin{aligned} r &= \alpha - \beta\, q \\ &= (13 + 7\,\omega) - (3 + 2\,\omega) \cdot 3 \\ &= (13 + 7\omega) - (9 + 6\,\omega) \\ &= 4 + \omega \end{aligned}$$

Proporcionando que $N(r) = 4^2 - 4 \cdot 1 + 1^2 = 13$ seja maior que a $N(\beta) = 7$. Isso se deu pela escolha equivocada das aproximações para $\left(\frac{27}{7}\right)$ e $\left(-\frac{5}{7}\right)$, pois de acordo com o teorema deveremos escolher os inteiros mais próximos dos respectivos números para garantir o que desejamos, ou seja, $3,857...$ por 4 e $-0,5714...$ por -1, obtendo $q = 4 - \omega$, e:

$$\begin{aligned} r &= \alpha - \beta\, q \\ &= (13 + 7\,\omega) - (3 + 2\omega) \cdot (4 - \omega) \\ &= (13 + 7\,\omega) - (14 + 7\,\omega) \\ &= -1 \end{aligned}$$

E dessa forma, a $N(r) = (-1)^2 - (-1) \cdot 0 + 0^2 = 1$ sendo menor que $N(\beta) = 7$, como procuravamos.
Portanto, $13 + 7\,\omega = (3 + 2\,\omega) \cdot (4 - \omega) + (-1)$.

As vezes é necessário atentar-se que o número procurado pode estar no meio entre dois múltiplos, implicando que o mesmo é equidistante dos dois inteiros mais próximo dele, e assim teríamos duas escolhas para o quociente e o resto, acarretando

que estes não são únicos em $\mathbb{Z}[\omega]$.

Exemplo: Considere $\alpha = 5 + 7\,\omega$ e $\beta = 2 + 2\,\omega$, com $N(\beta) = 2^2 - 2 \cdot 2 + 2^2 = 4$ e $\bar{\beta} = -2\,\omega$. Daí, $\frac{\alpha}{\beta} = \frac{\alpha \cdot \bar{\beta}}{\beta \cdot \bar{\beta}} = \frac{(5+7\,\omega)(-2\,\omega)}{4} = \frac{14+4\,\omega}{4} = \frac{7}{2} + \omega$. Observamos assim que $\left(\frac{7}{2}\right) = 3,5$ acarretando que o mesmo possui a mesma distância de 3 e 4, possibilitando q ser igual a $3 + \omega$ ou $4 + \omega$, obtendo os restos, respectivamente:

$$\begin{aligned} r_1 &= (5 + 7\,\omega) - (2 + 2\,\omega)(3 + \omega) \\ &= (5 + 7\,\omega) - (4 + 6\,\omega) \\ &= 1 + \omega \\ &\Rightarrow N(r_1) = 1. \end{aligned}$$

$$\begin{aligned} r_2 &= (5 + 7\,\omega) - (2 + 2\,\omega)(4 + \omega) \\ &= (5 + 7\,\omega) - (6 + 8\,\omega) \\ &= -1 - \omega \\ &\Rightarrow N(r_2) = 1. \end{aligned}$$

Analisando sobre um ponto de vista mais a fundo, observamos que em $\mathbb{Z}[\omega]$, a unicidade do quociente e do resto são irrelevantes em algumas aplicações, como por exemplo no algoritmo de Euclides.

De fato, caso consideremos as unidades em $\mathbb{Z}$ como $\{-1, 1\}$, então os divisores de um certo número só se diferem em seus associados. Usando essa ideia conseguimos definir o algoritmo de Euclides em $\mathbb{Z}[\omega]$.

1.3 O Algoritmo de Euclides

Definição 1.4. *Para $\alpha \neq 0$ e $\beta \in \mathbb{Z}[\omega]$, o <u>maior divisor comum</u> de α e β é um divisor comum com a norma máxima.*

Esta definição é análoga a definição usual de maior divisor comum (mdc) em $\mathbb{Z}$, exceto o conceito não está preso com um número específico. Se δ é o maior divisor comum de α e β, por isso são (pelo menos), seus múltiplos unitários $-\delta, \delta\,\omega, -\delta\,\omega, \delta\,\omega^2$, $-\delta\,\omega^2$.

E desta forma fica claro que pode-se falar de um máximo divisor comum em $\mathbb{Z}[\omega]$, mas não o maior divisor comum, e analisar que o mesmo aconteceria com os $\mathbb{Z}$ se definíssemos o maior divisor comum como um divisor comum com o de maior valor absoluto, em vez de o maior divisor comum positivo.

Teorema 1.4. *(Algoritmo de Euclides) Tomando α e $\beta \in \mathbb{Z}[\omega]$ diferentes de zero,*

e aplicando repetidamente o teorema da divisão onde o resto é diferente de zero,

$$\begin{aligned} \alpha &= \beta \cdot \gamma_1 + \delta_1, \, para \, N(\delta_1) < N(\beta) \\ \beta &= \delta_1 \cdot \gamma_2 + \delta_2, \, para \, N(\delta_2) < N(\delta_1) \\ \delta_1 &= \delta_2 \cdot \gamma_3 + \delta_3, \, para \, N(\delta_3) < N(\delta_2) \\ &\vdots \end{aligned}$$

O último resto diferente de zero é divisível por todos os divisores comuns de α e β, e será o divisor comum, por isso é um máximo divisor comum de α e β.

Demonstração. Dados α e $\beta \in \mathbb{Z}[\omega]$, então:

- Se $\beta \mid \alpha$, então mdc $(\alpha, \beta) = \beta$.
- Se $\beta \nmid \alpha$, logo pela divisão euclidiana, podemos escrever

$$\alpha = \beta \cdot \gamma_1 + \delta_1, \, com \, N(\delta_1) < N(\beta)$$

Dai, temos duas possibilidades,

- i)$\delta_1 \mid \beta$, e assim o mdc $(\beta, \delta_1) = \delta_1$, e como mdc $(\beta, \delta_1) =$ mdc $(\beta, \alpha - \beta \cdot \gamma_1) =$ mdc (β, α), então mdc $(\beta, \alpha) = \delta_1$.
- ii)$\delta_1 \nmid \beta$, podendo dessa forma efetuar a divisão de β por δ_1, obtendo

$$\beta = \delta_1 \cdot \gamma_2 + \delta_2, com \, N(\delta_2) < N(\delta_1)$$

E novamente,aparece duas possibilidades,

- i)$\delta_2 \mid \delta_1$, acarretando que o mdc$(\delta_1, \delta_2) = \delta_2$, e como mdc $(\delta_1, \delta_2) =$ mdc $(\delta_1, \beta - \delta_1 \cdot \gamma_2) =$ mdc $(\delta_1, \beta) =$ mdc $(\alpha - \beta \cdot \gamma_1, \beta) =$ mdc (α, β), então mdc $(\alpha, \beta) = \delta_2$.
- ii)$\delta_2 \nmid \delta_1$, poderemos efetuar a divisão de δ_1 por δ_2, obtendo

$$\delta_1 = \delta_2 \cdot \gamma_3 + \delta_3, \, com \, N(\delta_3) < N(\delta_2)$$

E assim continuaremos o procedimento até que pare. Concluindo que o mdc entre α e β será o último resto diferente de zero das divisões sucessivas efetuadas. □

Exemplo: Sejam $\alpha = 32 + 4\omega$ e $\beta = 2 + \omega$, então pelo teorema da divisão, temos $\gamma_1 = 12 - 8\omega$ e $\delta_1 = 0$, e assim:

$$32 + 4\omega = (2 + \omega) \cdot (12 - 8\omega)$$

E dessa forma, o mdc $(\alpha, \beta) = 2 + \omega$.

Exemplo: Sejam $\alpha = 4 + 13\omega$ e $\beta = -6 + 5\omega$, primeiro teorema da divisão, teremos $\gamma_1 = -\omega$ e $\delta_1 = -1 + 2\omega$, e aplicando o algoritmo de Euclides, encontraremos:

$$\begin{aligned} 4 + 13\omega &= (-6 + 5\omega)(-\omega) + (-1 + 2\omega) \\ -6 + 5\omega &= (-1 + 2\omega)(4 + \omega) + 0 \end{aligned}$$

E assim, pelo algoritmo de Euclides, teremos que o mdc $(\alpha, \beta) = -1 + 2\omega$.

Observa-se também que como em $\mathbb{Z}$ quando dois números a e b possuem a unidade como máximo divisor comum, os mesmos são chamados de primos entre si, co-primos, ou relativamente primos, em $\mathbb{Z}[\omega]$ também, como definiremos a seguir.

Definição 1.5. *Quando α e $\beta \in \mathbb{Z}[\omega]$ têm as unidades $\pm 1, \pm\omega, \pm\omega^2$ como um máximo divisor comum, chamamos de relativamente primos, ou primos entre si.*

Exemplo: Sejam $\alpha = 32 + 8\omega$ e $\beta = 5 + 2\omega$, então pelo teorema da divisão, temos $\gamma_1 = 6 - \omega$ e $\delta_1 = -w$, e assim:

$$32 + 8\omega = (5 + 2\omega) \cdot (6 - \omega) + (-\omega)$$

Aplicando o algoritmo de Euclides, encontraremos:

$$\begin{aligned} 32 + 8\omega &= (5 + 2\omega) \cdot (6 - \omega) + (-\omega) \\ 5 + 2\omega &= (-\omega) \cdot (3 + 5\omega) + 0 \end{aligned}$$

E daí, o mdc $(\alpha, \beta) = -\omega$, acarretando que α e β são relativamente primos.

Com isto, nota-se que se ϵ é um divisor comum de α e β, então $N(\epsilon) \mid N(\alpha)$ e $N(\epsilon) \mid N(\beta)$, de modo que $N(\epsilon) \mid \text{mdc}\,(\alpha, \beta)$.

Esta observação, nos garante que se mdc $(\alpha, \beta) = 1$, então qualquer divisor comum de α e β tem norma dividindo 1, logo sua norma deve ser 1, e portanto, o divisor comum seria uma unidade. No geral, é necessário utilizar o algoritmo de Euclides em $\mathbb{Z}[\omega]$, a fim de calcular o maior divisor comum em $\mathbb{Z}[\omega]$.

Sendo de suma importância observar que encontrado um máximo divisor comum em $\mathbb{Z}[\omega]$ pelo algoritmo de Euclides, qualquer outro máximo divisor comum será um associado do já encontrado, como mostraremos no corolário.

Corolário 1.1. *Sejam α e $\beta \in \mathbb{Z}[\omega]$ com $\beta \neq 0$ e δ um máximo divisor comum produzido pelo algoritmo de Euclides. Então qualquer máximo divisor comum de α e β será um múltiplo unitário de δ.*

Demonstração. Suponha que δ seja um máximo divisor comum de α e β, e agora considere δ' um divisor comum de α e β tal que $\delta' \mid \delta$, ou seja, $\delta = \delta' \cdot \gamma$, e assim temos:

$$N(\delta) = N(\delta') \cdot N(\gamma) \geq N(\delta')$$

Como δ é um máximo divisor comum, sua norma é máxima entre todas as normas dos divisores comuns, assim a desigualdade $N(\delta) \geq N(\delta')$ tem de ser uma igualdade. Isso implica $N(\gamma) = 1$, então $\gamma = \pm 1, \pm\omega, \pm\omega^2$.
Assim, δ e δ' são múltiplos unitários um do outro. □

1.4 Teorema de Bézout

Um teorema de fundamental importância para os números inteiros, que traz consigo inúmeras aplicações, é o teorema de Bézout, que também pode ser explicitado e caracterizado para os inteiros de Einsteins.

Teorema 1.5. *Teorema de Bézout Sejam α e $\beta \in \mathbb{Z}[\omega]$, ambos não nulos, com $mdc(\alpha, \beta) = \delta$, então $\alpha x + \beta y = \delta$, para algum $x, y \in \mathbb{Z}[\omega]$.*

Demonstração. Considere os conjuntos $C = \{\gamma = \alpha x + \beta y \,|\, x, y \in \mathbb{Z}[\omega]\}$, $D = \{N(\gamma);\ \gamma \in C\}$ e $D^* = D \setminus \{0\}$.
Daí, note que $D^* \subset \mathbb{N}$, o que implica que D^* possui menor elemento.
Seja k o menor elemento de D^*, então existe $\gamma_0 \neq 0 \in C$ tal que $k = N(\gamma_0)$.
Agora suponha que $\gamma_0 \nmid \alpha$, então $\alpha = \gamma_0 q + r$, com $N(r) < N(\gamma_0)$.
Então,

$$\begin{aligned} r &= \alpha - \gamma_0 q \\ r &= \alpha - (\alpha x_0 + \beta y_0) q \\ r &= \alpha - \alpha x_0 q - \beta y_0 q \\ r &= \alpha(1 - x_0 q) + \beta(-y_0 q) \end{aligned}$$

Assim, $r \in C$, e como $N(r) < N(\gamma_0)$, Absurdo!
Pois $k = N(\gamma_0)$ era o menor elemento de D^*, e portanto $\gamma_0 \,|\, \alpha$.
Analogamente, $\gamma_0 \,|\, \beta$.
E dessa forma γ_0 é um divisor comum de α e β.

Agora, vamos mostrar que $\gamma_0 = \text{mdc}(\alpha, \beta)$.
De fato, seja γ um divisor comum de α e β, então $\gamma \,|\, \alpha$ e $\gamma \,|\, \beta$, e assim $\alpha = \gamma q_1$ e $\beta = \gamma q_2$, como $\gamma_0 = \alpha x_0 + \beta y_0 \Rightarrow \gamma_0 = \gamma(q_1 x_0 + q_2 y_0) \Rightarrow \gamma \,|\, \gamma_0$.
Como γ divide γ_0 e γ_0 é um divisor comum, tem-se que γ_0 será um máximo divisor comum. □

Corolário 1.2. *Sendo α e β inteiros de Eisenstein, não nulos, então α e β são primos relativos se, e somente se, podemos escrever $\alpha x + \beta y = 1$, para algum $x, y \in \mathbb{Z}[\omega]$.*

Demonstração.

($\Rightarrow$): Se α e β são relativamente primos, então 1 é um máximo divisor comum de α e β. Portanto, podemos tomar $x, y \in \mathbb{Z}[\omega]$ pelo Teorema de Bézout.

($\Leftarrow$): Se $\alpha x + \beta y = 1$ para algum $x, y \in \mathbb{Z}[\omega]$, então qualquer divisor comum de α e β é um divisor de 1, e portanto, é um associado deste, logo temos α e β relativamente primos □

Exemplo: Seja $\alpha = 7 + 3\omega$ e $\beta = 2 + 4\omega$, então pelo algoritmo de Euclides, temos:

$$\begin{aligned} 7 + 3\omega &= (2 + 4\omega)(-1 - 2\omega) + (1 + 3\omega) \\ 2 + 4\omega &= (1 + 3\omega) \cdot 1 + (1 + \omega). \end{aligned}$$

Daí,

$$\begin{aligned} 1+3\,\omega &= (7+3\,\omega)-(2+4\,\omega)(-1-2\,\omega) && (1.2)\\ 1+\omega &= (2+4\,\omega)-(1+3\,\omega) && (1.3)\end{aligned}$$

Subtituindo (1.2) em (1.3), tem-se

$$\begin{aligned} 1+\omega &= (2+4\,\omega)-[(7+3\,\omega)-(2+4\,\omega)(-1-2\,\omega)]\\ &= (7+3\,\omega)\cdot(-1)+(2+4\,\omega)\cdot(1-(-1-2\,\omega))\\ &= (7+3\,\omega)\cdot(-1)+(2+4\,\omega)\cdot(2+2\,\omega).\end{aligned}$$

Multiplicando ambos os lados por $-\omega$, teremos:

$$\begin{aligned} (1+\omega)\cdot(-\omega) &= (7+3\,\omega)\cdot(-1)\cdot(-\omega)+(2+4\,\omega)\cdot(2+2\,\omega)\cdot(-\omega)\\ 1 &= (7+3\,\omega)\cdot(\omega)+(2+4\,\omega)\cdot 2.\end{aligned}$$

Esta caracterização do Teorema de Bézout para os inteiros de Eisenstein reproduz todas as consequências habituais que existem sobre os inteiros, como apresentaremos nos três corolários a seguir.

Corolário 1.3. *Suponha que $\alpha \mid \beta\gamma$ em $\mathbb{Z}[\omega]$ com α e β relativamente primos. Então $\alpha \mid \gamma$*

Demonstração. Tome $\beta\gamma = \alpha\delta$ para algum $\delta \in \mathbb{Z}[\omega]$ e $\text{mdc}\,(\alpha,\beta) = 1 \Rightarrow \alpha\,x+\beta\,y = 1$ para alguns $x, y \in \mathbb{Z}[\omega]$.
Multiplicando ambos os lados da equação por γ, temos:

$$\begin{aligned}\gamma &= \gamma\alpha\,x+\gamma\beta\,y\\ &= \alpha\gamma\,x+\alpha\delta\,y\\ &= \alpha(\gamma\,x+\delta\,y)\end{aligned}$$

E assim, $\alpha \mid \gamma$. □

Corolário 1.4. *Se $\alpha \mid \gamma$ e $\beta \mid \gamma \in \mathbb{Z}[\omega]$ com α e β relativamente primos, então $\alpha\beta \mid \gamma$.*

Demonstração. Sendo α e $\beta \in \mathbb{Z}[\omega]$ relativamente primos, tem-se $\text{mdc}\,(\alpha,\beta) = 1 \Rightarrow \alpha\,x+\beta\,y = 1$ para x, $y \in \mathbb{Z}[\omega]$.
Multiplicando $\alpha\,x+\beta\,y = 1$ por γ teremos $\gamma\alpha\,x+\gamma\beta\,y = \gamma$ $(*)$, como por hipótese $\alpha \mid \gamma$ e $\beta \mid \gamma \Rightarrow \gamma = \alpha\sigma$ e $\gamma = \beta\delta$ para algum $\sigma, \delta \in \mathbb{Z}[\omega]$.
E assim, de $(*)$, teremos

$$\begin{aligned}\gamma &= \beta\,\delta\,\alpha\,x+\alpha\,\sigma\,\beta\,y\\ &= (\alpha\,\beta)(\delta\,x)+(\alpha\,\beta)(\sigma\,y)\\ &= (\alpha\,\beta)(\delta\,x+\sigma\,y).\end{aligned}$$

Assim, $\alpha\beta \mid \gamma$. □

Corolário 1.5. *Para α, β, γ em $\mathbb{Z}[\omega]$ não nulos, α e β são relativamente primos para γ se, e somente se, se $\alpha\beta$ é relativamente primo para γ.*

Demonstração.

($\Rightarrow$): Sabemos que $\text{mdc}\,(\alpha, \gamma) = 1 \Rightarrow \alpha\, x + \beta\, y = 1$, para x, $y \in \mathbb{Z}[\omega]$ e $\text{mdc}\,(\beta, \gamma) = 1 \Rightarrow \beta\, z + \gamma\delta = 1$ para z, $\delta \in \mathbb{Z}[\omega]$.
Temos:

$$\begin{cases} \alpha\, x + \gamma\, y &= 1 \\ \beta\, z + \gamma\delta &= 1 \end{cases}$$

Multiplicando a primeira equação por β, tem-se:

$$\begin{cases} \alpha\beta\, x + \gamma\beta\, y &= \beta \\ \beta\, z + \gamma\delta &= 1 \end{cases}$$

Substituindo β em $\beta\, z + \gamma\delta = 1$, teremos $(\alpha\beta\, x + \gamma\beta\, y)z + \gamma\delta = 1$, então $(\alpha\beta)(zx) + \gamma(\beta\, y\, z) + \gamma\delta = 1 \Rightarrow (\alpha\beta)(zx) + \gamma(\beta yz + \delta) = 1$
Daí, o $\text{mdc}\,(\alpha\beta, \gamma) = 1$.
Portanto, $\alpha\beta$ é relativamente primo com γ.

($\Leftarrow$): Sabemos que $\text{mdc}\,(\alpha\beta, \gamma) \Rightarrow \alpha\beta\, r + \gamma\, s = 1$, para r, $s \in \mathbb{Z}[\omega]$.
Considere:

$x = \beta\, r$ e $y = s$.

$z = \alpha r$ e $\delta = s$.
Então, $\alpha x + \gamma y = 1 \Rightarrow \text{mdc}\,(\alpha, \gamma) = 1$ e $\beta z + \gamma\delta = 1 \Rightarrow \text{mdc}\,(\beta, \gamma) = 1$. E assim, α e β são relativamente primos γ. □

Capítulo 2

Números Irredutíveis de Eisenstein

Iniciaremos neste capítulo, o estudo dos números irredutíveis de Eisenstein, que quando se trata dos números inteiros, são mais conhecido como números primos. É uma das ferramentas mais importante de toda a Matemática, pois tais números desempenham papel fundamental na construção da Aritmética, e neste momento utilizaremos a importância e a relevância dos mesmos para tratarmos de forma mais interessante, as propriedades, teoremas e curiosidades dos irredutíveis (primos) em $\mathbb{Z}[\omega]$.
Para esse estudo, começaremos definindo um número irredutível.

2.1 Números Irredutíveis

Definição 2.1. *Um elemento $\beta \neq 0$ de um domínio de anel A é dito irredutível se não for uma unidade e sempre que $\beta = \alpha\,\delta$ com $\alpha, \delta \in A$, então α ou δ é uma unidade.*

Dois irredutíveis β_1 e β_2 são ditos associados se eles diferem de uma unidade, ou seja, $\beta_1 = u\,\beta_2$, com $u \in U(A)$. Por exemplo, em $A = \mathbb{Z}$, as unidades são ± 1 e os elementos irredutíveis são da forma $\pm p$, onde p é um número primo, então p e $-p$ são associados. Porém elementos associados devem ser vistos não como primos distintos mas como um "único primo"para efeitos de fatoração.

No intuito de facilitar algumas demonstrações que virão a seguir, definiremos a congruência entre dois números de Eisenstein, análoga a congruência em $\mathbb{Z}$

Definição 2.2. *Sejam $\alpha\,\beta$, $\gamma \in \mathbb{Z}[\omega]$. Dizemos que $\alpha \equiv \beta\,(mod\,\gamma) \Leftrightarrow \gamma \,|\, \alpha - \beta$.*

Lema 2.1. *Se $\beta \,|\, \alpha \in \mathbb{Z}[\omega]$ e $N(\beta) = 1$ ou $N(\beta) = N(\alpha)$, então ou β é unidade ou é um múltiplo unitário de α.*

Demonstração. Se $\beta \,|\, \alpha \in \mathbb{Z}[\omega]$ e $N(\beta) = 1$, então $\beta = \pm 1, \pm\omega, \pm\omega^2$. Agora, se $\beta \,|\, \alpha$ e $N(\beta) = N(\alpha)$, teremos que $\alpha = \beta\delta$, e aplicando a norma em ambos os lados, $N(\alpha) = N(\beta)N(\delta)$, como sabemos que $N(\beta) = N(\alpha)$, tem-se $N(\delta) = 1$, acarretando que $\delta = \pm 1, \pm\omega, \pm\omega^2$, e então $\beta = \pm\alpha, \pm\omega\alpha, \pm\omega^2\alpha$. □

E assim, quando $N(\alpha) > 1$, há sempre doze divisores de α: $\pm 1, \pm\omega, \pm\omega^2, \pm\alpha$, $\pm\omega\alpha, \pm\omega^2\alpha$, esses fatores são chamados de triviais de α. Eles são analogos aos quatros divisores triviais ± 1 e $\pm n$ para algum $n \in \mathbb{Z}$ com $|n| > 1$. E desta forma,

qualquer outro fator de α é chamado de não trivial.

Isso parece bastante inicialmente, pois, os primos em $\mathbb{Z}$ têm o menor número possível de divisores. Porém, os irredutíveis de Eisenstein têm nada menos que doze divisores, e apesar de parecer um absurdo, isto está correto, pois além das seis unidades, cada inteiro de Eisenstein tem mais seis divisores, justamente os multiplos unitários deste inteiro.

Definição 2.3. *Seja $\alpha \in \mathbb{Z}[\omega]$, dizemos que α tem fatoração não-trivial, quando o mesmo puder ser decomposto em números inteiros de Eisenstein com norma superior a 1.*

Definição 2.4. *Seja $\alpha \in \mathbb{Z}[\omega]$ com $N(\alpha) > 1$. Então, se existir um fator não trivial de α, este será chamado de composto e se α só tem fatores triviais, este será irredutível.*

Assim, um número inteiro de Eisenstein composto é aquele que possui fatoração não-trivial. Por exemplo, uma fatoração trivial de $18+7\omega$ é $(-11-18\omega)\cdot\omega$, e não trivial de $18+7\omega$ é $(4+3\omega)\cdot(3-2\omega)$, uma não trivial de 3 é $(-2-\omega)\cdot(-1+\omega)$ e o interessante é que o número 3 é primo em $\mathbb{Z}$. Isto gera perguntas tais como, quais números primos de $\mathbb{Z}$ serão primos em $\mathbb{Z}[\omega]$?

Por exemplo, o número 5 também é primo em $\mathbb{Z}[\omega]$, e para mostrar isso, vamos argumentar por contradição:
Considere que 5 é um número composto em $\mathbb{Z}[\omega]$, então, existe uma fatoração não trivial tal que $5 = \alpha\,\beta$, com α e $\beta \in \mathbb{Z}[\omega]$, $N(\alpha) > 1$ e $N(\beta) > 1$. Aplicando as normas de ambos os lados na decomposição do 5 teremos $N(5) = N(\alpha)\,N(\beta)$, com $N(\alpha) > 1$ e $N(\beta) > 1$, e portanto $N(\alpha) = N(\beta) = 5$.
Tome $\alpha = d + e\,\omega$, teremos $d^2 - de + e^2 = 5 \Rightarrow d^2 - ed + e^2 - 5 = 0$ o que pode ser considerada uma equação do segundo grau em função de d, e fazendo o estudo de discriminante desta equação, $b^2 - 4ac$, em que a é o coeficiente da varável do de segundo grau, b é o coeficiente da variável do de primeiro grau e c o termo indenpendete das variáveis, para que ela admita raizes reais, obteremos $\frac{-2\sqrt{15}}{3} \leq e \leq \frac{2\sqrt{15}}{3} \Rightarrow -2,58 \leq e \leq 2,58$, como $e \in \mathbb{Z} \Rightarrow e = -2, -1, 0, 1, 2$.
E assim, se:

- $e = -2 : d^2 + 2d - 1 = 0 \Rightarrow d = -1 \pm \sqrt{2} \notin \mathbb{Z}$
- $e = -1 : d^2 + d - 4 = 0 \Rightarrow d = \frac{-1\pm\sqrt{17}}{2} \notin \mathbb{Z}$
- $e = 0 : d^2 - 5 = 0 \Rightarrow d = \pm\sqrt{5} \notin \mathbb{Z}$
- $e = 1 : d^2 - d - 4 = 0 \Rightarrow d = \frac{1\pm\sqrt{17}}{2} \notin \mathbb{Z}$
- $e = 2 : d^2 - 2d - 1 = 0 \Rightarrow d = 1 \pm \sqrt{2} \notin \mathbb{Z}$

Portanto, não existem inteiros $\underline{d}$ e $\underline{e}$ que satisfaçam a equação, de modo que temos uma contradição.
Assim, 5 tem apenas a fatoração trivial em $\mathbb{Z}[\omega]$, então 5 é irredutível em $\mathbb{Z}[\omega]$.

Esta construção, nos proporciona indagações tais como, quando um número primo em $\mathbb{Z}$ será irredutível em $\mathbb{Z}[\omega]$? Quando um inteiro de Eisenstein será irredutível? Na busca de responder estas indagações, construiremos a partir de agora quando teremos inteiros irredutíveis em $\mathbb{Z}[\omega]$, observando-se que sempre é mais confortável e ágil trabalhar nos $\mathbb{Z}$. Por isso, tentaremos sempre que possível utilizar a norma como critério.

2.2 Critérios para os Irredutíveis de Eisenstein

Teorema 2.1. *Se a norma de um inteiro de Eisenstein é primo em $\mathbb{Z}$, então o inteiro de Eisenstein será irredutivel em $\mathbb{Z}[\omega]$.*

Demonstração. Tome $\alpha \in \mathbb{Z}[\omega]$ e p primo em $\mathbb{Z}^+$, com $N(\alpha) = p$.
Agora, devemos mostrar que α só tem fatores triviais, isto é, seus fatores tem norma 1 ou $N(\alpha)$, então α é irredutível em $\mathbb{Z}[\omega]$.
Considere assim qualquer fatoração de $\alpha \in \mathbb{Z}[\omega]$, $\alpha = \beta\,\gamma$. Aplicando a norma, teremos $p = N(\beta)\,N(\gamma)$, sendo uma equação em números inteiros positivos, e p primo em $\mathbb{Z}^+$, por isso $N(\beta) = 1$ ou $N(\gamma) = 1$.
Acarretando que β ou γ é uma unidade, de modo que α não adimite fatores não triviais.
E assim, α é irredutível. □

A recíproca do Teorema (2.1) é falsa, pois existem irredutíveis de Eisenstein cuja a norma não é prima em $\mathbb{Z}$, e mesmo assim este é irredutível em $\mathbb{Z}[\omega]$. Por exemplo, o número 5 que tem norma 25, e é primo em $\mathbb{Z}[\omega]$.

Na busca de construir um critério para determinarmos quando um inteiro de Eisenstein é irredutível em $\mathbb{Z}[\omega]$, demonstraremos a seguir quatro lemas e dois teoremas.

Lema 2.2. *Seja $p \in \mathbb{Z}$ primo, exceto 2 e 3. Então, $p \equiv 1\,(mod\,6)$ ou $p \equiv 5\,(mod\,6)$.*

Demonstração. Todo número inteiro é expresso por uma das formas: $6k$, $6k+1$, $6k+2$, $6k+3$, $6k+4$, $6k+5$, com $k \in \mathbb{Z}$.
Daí note que:
As formas $6k$, $6k+2$, $6k+4$ são características de números pares, inclusive o 2 (para $k = 0$, na forma $6k+2$), e portanto todos, exceto o 2, são compostos.
A forma $6k+3$, caracteriza os múltiplos de 3, inclusive o 3 (para $k = 0$), e portanto todos, exceto o 3, são compostos.
Assim, as formas $6k+1$ e $6k+5$ podem constituir números primos, exceto o 2 e o 3, conforme acima.
E deste modo, conclui-se que os primos, excetos 2 e 3, são congruentes a 1 ou 5 módulo 6.

□

Lema 2.3. *Seja $p \in \mathbb{Z}$ um primo. Então $p \equiv 1\,(mod\,3) \Leftrightarrow p \equiv 1\,(mod\,6)$*

Demonstração. ($\Rightarrow$) Sabemos que todo primo $p \neq 2 \in \mathbb{Z}$ é congruente a 1 módulo 2, como por hipotese $p \equiv 1\,(mod\,3) \Rightarrow p \equiv 1\,mod([2,3]) \Rightarrow p \equiv 1\,(mod\,6)$
($\Leftarrow$) Sendo $p \equiv 1\,(mod\,6)$, então p é da forma $6k+1$ podendo ser escrito da forma $3 \cdot (2k) + 1 \Rightarrow 3k' + 1$ e assim congruente a 1 módulo 3. □

Lema 2.4. *Seja $p \in \mathbb{Z}$ primo. Se $p \equiv 1$ ou $7\,(mod\,12) \Rightarrow p \equiv 1\,(mod\,6)$.*

Demonstração. Sendo $p \equiv 1$ ou $7\,(mod\,12)$, tem-se $p = 12k+1$ ou $p = 12k' + 7$, os quais poderiam ser escrito, respectivamente, da forma $p = 6 \cdot (2k) + 1$ ou $p = 6 \cdot (2k' + 1) + 1$, ou seja, $p = 6k_1 + 1$ ou $p = 6k_1' + 1$.
E então p é congruente a 1 módulo 6. □

Teorema 2.2. *Seja $p \neq 2 \in \mathbb{Z}$ um primo. Então, $(-3)^{\frac{p-1}{2}} \equiv 1\,(mod\,p) \Leftrightarrow p \equiv 1\,(mod\,6)$.*

Demonstração. Primeiramente observe que $(-3)^{\frac{p-1}{2}} \equiv 1\,(mod\,p) \Rightarrow (-1)^{\frac{p-1}{2}} \cdot 3^{\frac{p-1}{2}} \equiv 1\,(mod\,p)$.
E para que isto ocorra, é necessário, que $(-1)^{\frac{p-1}{2}} = 1$ e $3^{\frac{p-1}{2}} = 1$ ou $(-1)^{\frac{p-1}{2}} = -1$ e $3^{\frac{p-1}{2}} = -1$.
Note que $(-1)^{\frac{p-1}{2}}$ é igual a 1 quando $\frac{p-1}{2}$ for par e igual a -1, quando $\frac{p-1}{2}$ for ímpar. Como p é um primo diferente de 2, ou seja, ímpar, então existem duas possubilidades para ele em termos de congruência módulo 4, ser congruente a 1 ou 3 módulo 4. Sendo:

$p \equiv 1\,(mod\,4)$, tem-se $\frac{p-1}{2} = \frac{4k}{2} = 2k$, par;

$p \equiv 3\,(mod\,4)$, tem-se $\frac{p-1}{2} = \frac{4k'+2}{2} = \frac{2(2k')+1}{2} = 2k' + 1$, ímpar.

E assim, $(-1)^{\frac{p-1}{2}} = \begin{cases} 1, & se \quad p \equiv 1\,(mod\,4) \\ -1, & se \quad p \equiv 3\,(mod\,4) \end{cases}$

Dessa forma obteremos que, $3^{\frac{p-1}{2}} = \begin{cases} 3^{\frac{p-1}{2}}, & se \quad p \equiv 1\,(mod\,4) \\ -(3^{\frac{p-1}{2}}), & se \quad p \equiv 3\,(mod\,4) \end{cases}$

E assim

- $3^{\frac{p-1}{2}} = 1$
  $\Leftrightarrow \begin{cases} p & \equiv & 1\,(mod\,4) \\ 3^{\frac{p-1}{2}} & = & 1 \end{cases}$ ou $\begin{cases} p & \equiv 3 & (mod\,4) \\ 3^{\frac{p-1}{2}} & = & -1 \end{cases}$
  $\Leftrightarrow \begin{cases} p & \equiv & 1\,(mod\,4) \\ p & \equiv & 1\,(mod\,3). \end{cases}$ ou $\begin{cases} p & \equiv & 3\,(mod\,4) \\ p & \equiv & 2\,(mod\,3) \end{cases}$
  $\Leftrightarrow \quad p \equiv 1\,(mod\,12) \quad$ ou $\quad p \equiv 11\,(mod\,12).$

- $3^{\frac{p-1}{2}} = -1$
  $\Leftrightarrow \begin{cases} p & \equiv & 1\,(mod\,4) \\ 3^{\frac{p-1}{2}} & = & -1 \end{cases}$ ou $\begin{cases} p & \equiv 3 & (mod\,4) \\ 3^{\frac{p-1}{2}} & = & 1 \end{cases}$
  $\Leftrightarrow \begin{cases} p & \equiv & 1\,(mod\,4) \\ p & \equiv & 2\,(mod\,3). \end{cases}$ ou $\begin{cases} p & \equiv & 3\,(mod\,4) \\ p & \equiv & 1\,(mod\,3) \end{cases}$
  $\Leftrightarrow \quad p \equiv 5\,(mod\,12) \quad$ ou $\quad p \equiv 7\,(mod\,12).$

E portanto, $3^{\frac{p-1}{2}} = \begin{cases} 1, & se \quad p \equiv 1 \text{ ou } 11\,(mod\,12) \\ -1, & se \quad p \equiv 5 \text{ ou } 7\,(mod\,12) \end{cases}$

Diante das demontrações necessárias acima, podemos de fato, provar o teorema.

($\Rightarrow$): No caso,

1. $(-1)^{\frac{p-1}{2}} = 1$ e $3^{\frac{p-1}{2}} = 1$, temos $p \equiv 1\,(mod\,4)$ e $p \equiv 1$ ou $11\,(mod\,12)$, e estas condições fornecem $p \equiv 1\,(mod\,12)$ e pelo lema (2.4) temos $p \equiv 1\,(mod\,6)$.

2. $(-1)^{\frac{p-1}{2}} = -1$ e $3^{\frac{p-1}{2}} = -1$, temos $p \equiv 3\,(mod\,4)$ e $p \equiv 5$ ou $7\,(mod\,12)$, e estas condições fornecem $p \equiv 7\,(mod\,12)$ que pelo lema (2.4) temos $p \equiv 1\,(mod\,6)$.

($\Leftarrow$): Se tivermos $p = 6k + 1$, então:

1. para k par, então $p \equiv 1\,(mod\,12)$ temos $(-3)^{\frac{p-1}{2}} = 1$;

2. para k ímpar, então $p \equiv 7\,(mod\,12)$ temos $(-3)^{\frac{p-1}{2}} = 1$

□

Lema 2.5. *Seja $p \in \mathbb{Z}$ primo. Então, $p = \alpha^2 + 3\beta^2$ para alguns inteiros α e $\beta \in \mathbb{Z} \Leftrightarrow p = 3$ ou $p \equiv 1\,(mod\,6)$*

Demonstração. ($\Rightarrow$) Se $\alpha = 0$, então $p = 3\beta^2$, tem-se $p = 3$, pois p é primo.
Se $\alpha \neq 0$, então temos $\alpha \equiv 1\,(mod\,3)$ ou $\alpha \equiv 2\,(mod\,3)$, obtendo assim p será congruente a 1 módulo 3, que pelo lema (2.2) teremos $p \equiv 1\,(mod\,6)$.
($\Leftarrow$) Se $p = 3 \Rightarrow 3 = 0^2 + 3 \cdot (1)^2$.
Se $p \equiv 1\,(mod\,6)$, pelo teorema (2.2), existe $\alpha \in \mathbb{Z}$ tal que $\alpha^2 + 3 = pt$ (1), para $t \in \mathbb{Z}$, $0 < t < p$.
Assim,
Se $t = 1 \Rightarrow p = \alpha^2 + 3 \cdot (1)^2$.
Se $t \neq 1$, então tome $\beta \in \mathbb{Z}$ tal que $\beta \equiv \alpha\,(mod\,t)$, com $\beta \in \left(-\frac{t}{2}, \frac{t}{2}\right)$, daí $\alpha^2 \equiv \beta^2\,(mod\,t)$. Logo, $(\alpha^2 + 3) \equiv (\beta^2 + 3)\,(mod\,t)$, e assim para algum $\delta \in \mathbb{Z}$, $1 < \delta < t$, temos $\beta^2 + 3 = \delta t$ (2).
E de (1) $\cdot$ (2), obtemos $(\alpha^2+3)(\beta^2+3) = p\delta t^2 \Leftrightarrow (\alpha\beta+3)^2+3(\alpha-\beta)^2 = p\delta t^2$, como t divide ambos os membros, então $\left(\frac{\alpha\beta+3}{t}\right)^2 + 3\left(\frac{\alpha-\beta}{t}\right)^2 = \delta p$, logo podemos escrever um múltiplo menor de p na forma $\alpha^2 + 3\beta^2$.
Daí, tomando $\delta = 1$ já obteremos p. Caso, $\delta \neq 1$, repetimos o procedimento acima um número finito de vezes até obtermos o resultado. □

Teorema 2.3. *Seja $p \in \mathbb{Z}$ primo. Então, $p = a^2 - ab + b^2$ para $a\,b \in \mathbb{Z} \Leftrightarrow p = 3$ ou $p \equiv 1\,(mod\,6)$.*

Demonstração. ($\Rightarrow$)Seja $p = a^2 - ab + b^2$ como hipotese. Então:

- se a e b são ambos pares, ou seja, $a = 2k$ e $b = 2k_1 \Rightarrow b - a = 2n$, $n \in \mathbb{Z} \Rightarrow b = a + 2n$. Logo,

$$\begin{aligned} p &= a^2 - a(a + 2n) + (a^2 + 4an + 4n^2) \\ &= a^2 - a^2 - 2an + a^2 + 4an + 4n^2 \\ &= a^2 + 2an + n^2 + 3n^2 \\ &= (a + n)^2 + 3n^2. \end{aligned}$$

  Pelo lema(2.5), temos $p = 3$ ou $p \equiv 1\,(mod\,6)$.

- se a e b são ambos ímpares, ou seja, $a = 2k+1$ e $b = 2k_1+1 \Rightarrow b-a = 2n, n \in \mathbb{Z}$, e daí a demonstração é analóga ao caso de a e b pares.

- se um deles é par e outro é ímpar. Digamos a par, daí a pode ser escrito da forma $2n, n \in \mathbb{Z}$. Logo,

$$\begin{aligned} p &= (2n)^2 - 2nb + b^2 \\ &= 4n^2 - 2nb + b^2 \\ &= n^2 - 2nb + b^2 + 3n^2 \\ &= (n-b)^2 + 3n^2. \end{aligned}$$

  Pelo lema (2.5), temos $p = 3$ ou $p \equiv 1\,(mod\,6)$.

E assim, se $p \in \mathbb{Z}$ primo é da forma $a^2 - ab + b^2$, então $p = 3$ ou $p \equiv 1\,(mod\,6)$.

($\Leftarrow$) Se $p = 3$ ou $p \equiv 1\,(mod\,6)$, então:

- $2^2 - 2 \cdot 1 + 1^2 = 3 \Rightarrow p = 3$

- pelo lema (2.5) existem α e $\beta \in \mathbb{Z}$ tal que $p = \alpha^2 + 3\beta^2$. Daí tome $\alpha = a - \frac{b}{2}$ e $\beta = \frac{b}{2}$, com a, $b \in \mathbb{Z}$, e assim

$$\begin{aligned} p &= \alpha^2 + 3\beta^2 \\ &= \left(a - \frac{b}{2}\right)^2 + 3\left(\frac{b}{2}\right)^2 \\ &= a^2 - 2 \cdot a \cdot \frac{b}{2} + \frac{b^2}{4} + 3\frac{b^2}{4} \\ &= a^2 - ab + b^2. \end{aligned}$$

Portanto, se $p = 3$ ou $p \equiv 1\,(mod\,6)$, então $p = a^2 - ab + b^2$ para algum a, $b \in \mathbb{Z}$. □

Agora que identificamos alguns requisitos necessários para a caracterização dos irredutíveis em $\mathbb{Z}[\omega]$, poderemos responder as indagações norteadores dessa busca.

Teorema 2.4. *Seja α irredutível em $\mathbb{Z}$, com $N(\alpha) = p$ primo, então $p = 3$ ou $p \equiv 1\,(mod\,6)$.*

Demonstração. Pelo teorema (2.1), como $N(\alpha)$ é prima, α é irredutível em $\mathbb{Z}[\omega]$, e por hipótese $N(\alpha) = p \Rightarrow a^2 - ab + b^2 = p$, que pelo teorema (2.3), $p = 3$ ou $p \equiv 1\,(mod\,6)$ □

Dessa forma, observe que o número $2+3\omega$ é irredutível em $\mathbb{Z}[\omega]$, pois tem norma $2^2 - 2 \cdot 3 + 3^2 = 4 - 6 + 9 = 7$, que é congruente a 1 módulo 6.

A pergunta que nós falta ainda ser respondida é quando um primo em $\mathbb{Z}$ será um irredutível em $\mathbb{Z}[\omega]$, e a resposta para esta indagação será respondida pelo seguinte teorema.

Teorema 2.5. *Seja $p \in \mathbb{Z}$ primo. Então, p será irredutível em $\mathbb{Z}[\omega]$ se, somente se, $p = 2$ ou $p \equiv 5\,(mod\,6)$.*

Demonstração.

($\Rightarrow$): Suponha por absurdo que p primo em $\mathbb{Z}$, com $p = 2$ ou congruente a 5 módulo 6, possa ser fatorado em $\mathbb{Z}[\omega]$, ou seja, $p = \alpha\,\beta$, com α, $\beta \in \mathbb{Z}[\omega] - U(\mathbb{Z}[\omega])$.
Dessa forma, temos $p^2 = N(\alpha)\,N(\beta)$, como α e β não são as unidades, pois por hipótese p não possui fatoração trivial, e assim $N(\alpha) \neq 1$ e $N(\beta) \neq 1 \Rightarrow N(\alpha) = N(\beta) = p$.
Escrevendo $\alpha = a + b\omega$, a, $b \in \mathbb{Z}$, tem-se $p = a^2 - ab + b^2$, que pelo teorema (2.2), temos $p = 3$ ou $p \equiv 1(mod\,6)$. Absurdo, pois $p = 2$ ou $p \equiv 5\,(mod\,6)$. Logo, p não pode ser fatorado em $\mathbb{Z}[\omega]$.

($\Leftarrow$): Seja p primo em $\mathbb{Z}$ e irredutível em $\mathbb{Z}[\omega]$, com $p \neq 2$ e $p \not\equiv 5\,(mod\,6)$, então pelo lema (2.3), $p = 3$ ou $p \equiv 1\,(mod\,6)$, podendo assim, ser escrito da forma $a^2 - ab + b^2$.
Porém, p sendo da forma $a^2 - ab + b^2$, então p também poderá ser escrito como $(a + b\,\omega)(a + b\,\omega^2)$, que ao aplicar a norma de ambos os lados teremos, $N(p) = N(a + b\,\omega)N(a + b\,\omega^2) \Rightarrow p^2 = N(a + b\,\omega)N(a + b\,\omega^2)$, mas como a $N(a + b\,\omega) = p$, tem-se que $N(a + b\,\omega^2) = p$, acarrentando que $a + b\,\omega$ e $a + b\,\omega^2$ são irredutíveis em $\mathbb{Z}[\omega]$. O que tornaria p escrito como o produto de dois irredutíveis em $\mathbb{Z}[\omega]$, ou seja fatorável. Absurdo! Pois p era irredutível em $\mathbb{Z}[\omega]$.
Portanto, $p = 2$ ou $p \equiv 5\,(mod\,6)$. □

Esse teorema traz um resultado bastante forte, pois este garante que todo primo em $\mathbb{Z}$ que não for 2 ou congruente a 5 módulo 6, será composto em $\mathbb{Z}[\omega]$.
Isto, garante que os números 3, 7, entre outros, serão compostos em $\mathbb{Z}[\omega]$, e uma maneira de achar esta fatoração é utilizando a norma, como mostraremos no exemplo a seguir.

Exemplo: Escreva 3 como o produto de irredutíveis em $\mathbb{Z}[\omega]$.

Utilizando o teorema (2.4) sabemos que 3 não é irredutível em $\mathbb{Z}[\omega]$, por isso pode ser decomposto como $\alpha \cdot \beta$, com α e $\beta \in \mathbb{Z}[\omega]$, desta forma teremos $N(\alpha)N(\beta) = 9$, como $N(\alpha)$ e$N(\beta)$ são diferentes de 1, pois α e β não são as unidades, e a norma são números inteiros positivos, teremos $N(\alpha) = N(\beta) = 3$.
Escrevendo $\alpha = a + b\omega$, com a, $b \in \mathbb{Z}$, tem-se $a^2 - ab + b^2 = 3 \Rightarrow a^2 - ba + b^2 - 3 = 0$, como precisamos que esta equação tenha solução devemos ter o discriminante da mesma maior ou igual a 0. Discriminando a equação para a, temos $b^2 - 4(b^2 - 3) \geq 0 \Rightarrow -3b^2 + 12 \geq 0 \Rightarrow -2 \leq b \leq 2$, sendo $b \in \mathbb{Z} \Rightarrow b = -2, -1, 0, 1, 2$. Assim, se:

- $b = -2 \Rightarrow a^2 + 2a + 1 = 0 \Rightarrow (a + 1)^2 = 0 \Rightarrow a = -1 \Rightarrow \alpha = -1 - 2\omega$.
- $b = -1 \Rightarrow a^2 + a - 2 = 0 \Rightarrow (a + 2)(a - 1) = 0 \Rightarrow a = -2$ ou $1 \Rightarrow \alpha = -2 - \omega$ ou $\alpha = 1 - \omega$.
- $b = 0 \Rightarrow a^2 - 3 = 0 \Rightarrow a \notin \mathbb{Z}$.
- $b = 1 \Rightarrow a^2 - a - 2 = 0 \Rightarrow (a - 2)(a + 1) = 0 \Rightarrow a = -1$ ou $2 \Rightarrow \alpha = -1 + \omega$ ou $\alpha = 2 + \omega$.
- $b = 2 \Rightarrow a^2 - 2a + 1 = 0 \Rightarrow (a - 1)^2 = 0 \Rightarrow a = 1 \Rightarrow \alpha = 1 + 2\omega$.

Daí, α pode assumir qualquer um dos valores acima, pois os outros serão associados do número de Eisenstein escolhido.
Então, tomemos $\alpha = 1+2\omega$, portanto precisamos descobrir β tal que $\alpha \cdot \beta = 3$. Note também que β assumirá algum dos números de Eisenstein acima, pois a norma deste também é 3, precisamos apenas descobrir quais destes será o número necessário, para que em produto com o α escolhido resulte em 3. Além disto é importante ressaltar que tais números escolhidos para α e β são irredutíveis em $\mathbb{Z}[\omega]$, pois ambos possuem norma prima, como garantido pelo resultado do teorema (2.1).
Assim, procurando o $\beta = c + d\omega$, temos:

$$\begin{aligned} (1+2\omega)(c+d\omega) &= 3 \\ (c-2d)+(2c+d-2d)\omega &= 3 \\ (c-2d)+(2c-d)\omega &= 3 \end{aligned}$$

E dessa forma, $c-2d=3$ e $2c-d=0 \Rightarrow c=-1$ e $d=-2 \Rightarrow \beta = -1-2\omega$
Portanto, $3 = (1+2\omega)(-1-2\omega)$.

2.3 Fatoração Única

Diante do exposto já sabemos o suficiente sobre os irredutíveis de Eisenstein, então voltaremos a nossa atenção agora para a construção fatoração única. A existência de uma fatoração em $\mathbb{Z}[\omega]$ será provada de forma similar à prova da fatoração em $\mathbb{Z}$, primeiro estabeleceremos a existência de tal fatoração e depois de sua unicidade.

Teorema 2.6. *Seja $\alpha \in \mathbb{Z}[\omega]$, com $N(\alpha) > 1$. Então α pode ser escrito como um produto de números irredutíveis em $\mathbb{Z}[\omega]$.*

Demonstração. A nossa prova será por indução em $N(\alpha)$.
Suponha que $N(\alpha) = 2$, isto significa que, $a^2 - ab + b^2 = 2 \Rightarrow a^2 - ab + b^2 - 2 = 0$.
Discriminando a equação em função de a para determinamos quando ela existirá teremos, $b^2 - 4(b^2-2) \geq 0 \Rightarrow -3b^2 + 8 \geq 0 \Rightarrow -\frac{2\sqrt{6}}{3} \leq b \leq \frac{2\sqrt{6}}{3} \Rightarrow -1,63... \leq b \leq 1,63...$, como $b \in \mathbb{Z} \Rightarrow b = -1, 0, 1$.
Daí, se:

- $b = -1 \Rightarrow a^2 + a - 1 = 0 \Rightarrow a \notin \mathbb{Z}$, logo não existe α.
- $b = 0 \Rightarrow a^2 - 2 = 0 \Rightarrow a \notin \mathbb{Z}$, logo não existe α.
- $b = 1 \Rightarrow a^2 - a - 1 = 0 \Rightarrow a \notin \mathbb{Z}$, logo não existe α.

Assim, não existe inteiro de Eisenstein que a satisfaz $N(\alpha) = 2$.
Tomemos agora $N(\alpha) = 3$, isto significa que $a^2 - ab + b^2 = 3 \Rightarrow a^2 - ab + b^2 - 3 = 0$, que do exemplo acima temos: $\alpha = -1+2\omega$, $-2-2\omega$, $1-\omega$, $-1+\omega$, $2+\omega$ ou $1+2\omega$, portanto α é irredutível pelo teorema (2.1).
Agora vamos supor $n \geq 4$ e $3 < N(\alpha) \leq n$, onde se $N(\gamma) < N(\alpha)$, então γ pode ser fatorável em fatores irredutíveis em $\mathbb{Z}[\omega]$.

E daí queremos mostrar que todo inteiro de Eisenstein com norma n será um produto de números irredutíveis em $\mathbb{Z}[\omega]$.
Se:

- não houver inteiro de Eisenstein com norma n, então não há nada a provar.
- n for um número primo em $\mathbb{Z}$, então α é irredutível em $\mathbb{Z}[\omega]$, pelo resultado do teorema (2.1), e sua fatoração é imediata.
- tivermos um inteiro de Eisenstein com norma n, que seja composto, então podemos escrever $\alpha = \beta\delta$, onde a $N(\beta)$, $N(\delta) < N(\alpha) = n$, que por hipótese tem-se β e δ são fatoráveis em irredutíveis de $\mathbb{Z}[\omega]$, e portanto α será um produto de irredutíveis em $\mathbb{Z}[\omega]$.

E portanto, α pode ser escrito como um produto de números irredutíveis em $\mathbb{Z}[\omega]$. □

Note que escrevemos $3 = (1+2\omega)(-1-2\omega) = (-2-\omega)(-1+\omega)$ de seis combinações possíveis, devido aos associados unitários que encontramos no exemplo anterior, e que todos os fatores são primos em $\mathbb{Z}[\omega]$, pois suas normas são primas em $\mathbb{Z}$. Na verdade isto também pode acontecer em $\mathbb{Z}$, como por exemplo: $8 = 2{\cdot}4 = (-2){\cdot}(-4)$, o que mostra que a fatoração também não seria única se consideressemos em $\mathbb{Z}$ as unidades como $-1, 1$, uma vez que poderíamos combinar outres fatores. Logo, as questões de sinais são evitadas em $\mathbb{Z}$, para concetramos a atenção à propriedades interessantes que ficaram mais complexas caso fosse admitido as duas unidades, e daí a decisão de trabalhar apenas com os números primos positivos em $\mathbb{Z}$. E isto deixará mais claro a necessidade e importância das unidades na fatoração em $\mathbb{Z}[\omega]$.

Tendo estabelecido a existência da fatoração de irredutíveis em $\mathbb{Z}[\omega]$, partiremos agora para a sua unicidade.

Lema 2.6. *Seja π um irredutível em $\mathbb{Z}[\omega]$ e $\alpha_1, \alpha_2, ..., \alpha_r \in \mathbb{Z}[\omega]$, se $\pi \mid \alpha_1\alpha_1...\alpha_r$, então π divide algum α_j, com $1 \leq j \leq r$.*

Demonstração. Faremos a prova por indução em r.
Considere $r = 2$, ou seja, $\pi \mid \alpha_1\alpha_2 \Rightarrow \alpha_1\alpha_2 = \pi\sigma$, com $\sigma \in \mathbb{Z}[\omega]$.
Agora, suponha que $\pi \nmid \alpha_1$, isto implica que π e α_1 são relativamente primos, assim $\pi\gamma + \alpha_1\delta = 1 \Rightarrow \alpha_2\pi\gamma + \alpha_2\alpha_1\delta = \alpha_2$, com γ, $\delta \in \mathbb{Z}[\omega]$.
Substituindo $\alpha_1\alpha_2$ por $\pi\sigma$ na igualdade anterior $\alpha_2\pi\gamma + \pi\sigma\delta = \alpha_2 \Rightarrow \pi(\alpha_2\gamma + \sigma\delta) = \alpha_2 \Rightarrow \pi \mid \alpha_2$.
Suponha agora que:

- se $\pi \mid \alpha_1\alpha_2...\alpha_r$, então π dividirá $\alpha_1\alpha_2...\alpha_r\alpha_{r+1}$.
- se $\pi \mid \alpha_1\alpha_2...\alpha_r\alpha_{r+1} \Rightarrow \alpha_1\alpha_2...\alpha_r\alpha_{r+1} = \pi\sigma$, com $\sigma \in \mathbb{Z}[\omega]$ e $\pi \nmid \alpha_1\alpha_2...\alpha_r = \beta$, $\beta \in \mathbb{Z}[\omega]$, então π e β são relativamente primos, assim $\pi\gamma + \beta\delta = 1 \Rightarrow \alpha_{r+1}\pi\gamma + \alpha_{r+1}\beta\delta = \alpha_{r+1}$.
  Substituindo $\alpha_1\alpha_2...\alpha_r\alpha_{r+1} = \pi\sigma$ na igualdade anterior, $\alpha_{r+1}\pi\gamma + \pi\sigma\delta = \alpha_{r+1} \Rightarrow \pi(\alpha_{r+1}\gamma + \sigma\delta) = \alpha_{r+1} \Rightarrow \pi \mid \alpha_{r+1}$.

E portanto, se $\pi \mid \alpha_1\alpha_1...\alpha_r$, então π divide algum α_j, com $1 \leq j \leq r$. □

Teorema 2.7. *(Fatoração Única) Qualquer $\alpha \neq 0 \in \mathbb{Z}[\omega]$, com $N(\alpha) > 1$ tem uma fatoração única em irredutíveis no seguinte sentido, se:*

$$\alpha = \pi_1\pi_2...\pi_r = \pi_1^{'}\pi_2^{'}...\pi_s^{'}$$

onde o $\pi_i s$ e $\pi_j^{'} s$ são irredutíveis em $\mathbb{Z}[\omega]$, então $r = s$ e depois de uma adequada renumaração cada π_i é um múltiplo unitário de $\pi_j^{'}$.

Demonstração. O teorema (2.5) mostra que cada $\alpha \in \mathbb{Z}[\omega]$, com $N(\alpha) > 1$ tem uma fatoração de irredutíveis em $\mathbb{Z}[\omega]$.
Quando α é irredutível, sua fatoração é obviamente única.
Agora, vamos mostrar a unicidade em geral por indução em $N(\alpha)$.
Suponha que $n \geq 3$ e $1 < N(\alpha) < n$ com α tendo uma fatoração única.
Podemos dessa forma supor que há inteiros de Eisenstein com norma n (caso contrário, não há nada a verificar), e só nos concentramos sobre os α compostos com a norma n.
Considere as duas fatorações de irredutíveis de α como exposto no enunciado do teorema, suponha que $\pi_1 \mid \alpha$, assim podemos escrever:

$$\pi_1 \mid \pi_1^{'}\pi_2^{'}...\pi_s^{'}$$

Pelo lema (2.6), tem-se que $\pi_1 \mid \pi_j^{'}$ para algum $1 \leq j \leq s$.
Tome $j = 1$ (sem perda de generalidade), ou seja, $\pi_1 \mid \pi_1^{'}$, e assim $\pi_1^{'} = \ell\pi_1$, como $\pi_1^{'}$ e π_1 são irredutíveis em $\mathbb{Z}[\omega]$, então $\ell \in \{\pm 1, \pm\omega, \pm\omega^2\}$.
Observando as duas fatorações de α, temos:

$$\pi_1\pi_2...\pi_r = \ell\pi_1\pi_2^{'}...\pi_s^{'}$$

Cancelando π_1 em ambos os lados, resulta-se:

$$\pi_2\pi_3...\pi_r = \ell\pi_2^{'}\pi_3^{'}...\pi_s^{'} \tag{2.1}$$

Tome, agora $\beta = \pi_2\pi_3...\pi_r$, com $N(\beta) < N(\alpha)$.
Como ℓ é uma unidade, e $\ell\pi_2^{'}$ é um produto sobre o lado direito de (2.1), realmente irredutível, então (2.1) tem duas fatorações de irredutíveis para β, com $(r-1)$ irredutíveis do lado esquerdo e $(s-1)$ irredutíveis do lado direito.
Porém, como $N(\beta) < n$, a hipótese indutiva diz que β tem fatoração única, então $(r-1) = (s-1) \Rightarrow r = s$ e, após nova rotulagem apropriada, temos que π_2 e $\ell\pi_2^{'}$ são múltiplos unitários, e daí observa-se que nesta construção, π_i e $\pi_i^{'}$ seram múltiplos unitários para $i > 2$, e assim a prova estará completa. □

Vamos ilustrar a fatoração única de $\alpha = 4 + 2\omega$. Sabemos que $N(\alpha) = 4^2 - 4 \cdot 2 + 2^2 = 12 = 4 \cdot 3$, e daí tem-se que α tem fatores não triviais onde uma norma é 3 e outra é 4, tomando $\beta = 1 + 2\omega$ e $\gamma = -2 - 2\omega$, temos $N(\beta) = 3$ e $N(\gamma) = 4$, assim temos algumas possibilidades de produtos de dois números de Eisenstein que tem norma 12:

a) $\beta \cdot \beta = (1 + 2\omega)(1 + 2\omega) = -3$.

b) $\beta \cdot \gamma = (1+2\omega)(-2-2\omega) = 2-2\omega$

c) $\gamma \cdot \gamma = (-2-2\omega)(-2-2\omega) = 4\omega$

Analisando (b), multiplicando por $-\omega^2$ temos que:

$$\begin{aligned}(1+2\omega)(-2-2\omega)(-\omega^2) &= (2-2\omega)(-\omega^2)\\ -(1+2\omega)(2+2\omega)(1+\omega) &= 4+2\omega\end{aligned}$$

E assim a fatoração de $4+2\omega$ é $-(1+2\omega)(2+2\omega)(1+\omega)$.

O favorecimento do conhecimento do número de Eisenstein é que os mesmo podem proporcionar resoluções de problemas interessantes em $\mathbb{Z}$ facilitando métodos e até mesmo encurtando caminhos de resoluções, como mostraremos nos exemplos a seguir.

2.4 Aplicações Interessantes dos Inreiros de Eisenstein

Exemplo: Resolver a equação diofantina $y^5 = x^2 + x + 1$.

Solução: Primeiro observe que $N(x-\omega) = x^2+x+1 = y^5$ e $y^5 = (x-\omega)(x-\omega^2)$, então assim seria mais fácil trabalhar em $\mathbb{Z}[\omega]$.
Seja $\delta \in \mathbb{Z}[\omega]$ tal que $\delta \mid (x-\omega)$ e $\delta \mid (x-\omega^2)$, daí $\delta \mid (x-\omega)-(x-\omega^2) \Rightarrow \delta \mid (\omega-\omega^2) = \omega(1-\omega)$, como ω é unidade e $1-\omega$ é irredutível, pois tem norma 3, temos que $x-\omega$ e $x-\omega^2$ temo no máximo $1-\omega$ como fator comum.
Sendo o produto de $x-\omega$ e $x-\omega^2$ uma quinta potência e os elementos de $U(\mathbb{Z}[\omega])$ também são quintas potências perfeitas, pois o sinal se preserva, podemos concluir utilizando a fatoração única que $x-\omega = [(1-\omega)]^k\alpha^5$ com $\alpha \in \mathbb{Z}[\omega]$.
Tomando as normas, temos $N(x-\omega) = N(1-\omega)^k N(\alpha)^5 \Rightarrow y^5 = 3^k N(\alpha)^5$, e assim k também deve ser um múltiplo de 5, e concluímos dessa forma que $x-\omega = \beta^5$ para algum $\beta \in \mathbb{Z}[\omega]$.
Agora escrevendo $\beta = m + n\omega$, $m, n \in \mathbb{Z}$, obtemos que $x-\omega = \beta^5$ é igual a

$$(m^5 - 10m^3n^2 + 10m^2n^3 - n^5) + (5m^4n - 10m^3n^2 + 5mn^4 - n^5)\omega$$

Daí, $5m^4n - 10m^3n^2 + 5mn^4 - n^5 = -1 \Rightarrow n(5m^4 - 10m^3n + 5mn^3 - n^4) = -1$, como n e $(5m^4 - 10m^3n + 5mn^3 - n^4) \in \mathbb{Z} \Rightarrow n = \pm 1$, assim:

- $n = -1 \Rightarrow 5m^4 + 10m^3 - 5m^2 - 1 = 1 \Rightarrow 5m^4 - 10m^3 + 5m^2 - 2 = 0 \Rightarrow m \notin \mathbb{Z}$.
- $n = 1 \Rightarrow 5m^4 - 10m^3 + 5m^2 - 1 = -1 \Rightarrow 5m^4 - 10m^3 + 5m^2 = 0 \Rightarrow 5m^2(m^2 - 2m + 1) = 0 \Rightarrow 5m^2(m-1)^2 = 0 \Rightarrow m = 0$ ou $m = 1$, logo obtemos $(m, n) = (0, 1)$ ou $(1, 1)$.

E como $x = m^5 - 10m^3n^2 + 10m^2n^3 - n^5$ e $x^2 + x + 1 = y^5$ Obtemos:

- $(m,n) = (0,1) \Rightarrow x = 0^5 - 10 \cdot 0^3 \cdot 1^2 + 10 \cdot 0^2 \cdot 1^3 - 1^5 = -1 \Rightarrow y^5 = (-1)^2 - 1 + 1 = 1 \Rightarrow y = 1 \Rightarrow (x,y) = (-1,1)$.
- $(m,n) = (1,1) \Rightarrow x = 1^5 - 10 \cdot 1^3 \cdot 1^2 + 10 \cdot 1^2 \cdot 1^3 - 1^5 = 1 - 10 + 10 - 1 = 0 \Rightarrow y^5 = (0)^2 - 0 + 1 = 1 \Rightarrow y = 1 \Rightarrow (x,y) = (0,1)$.

Portanto, (x,y) correspondem as soluções $(-1,1)$ e $(0,1)$.

Exemplo: Ache todos os a, b, $c \in \mathbb{Z}_+^*$ lados de um triângulo com um ângulo de $60°$.

Solução: Vamos supor , sem perda de generalidade, que o ângulo de $60°$ está entre os lados de medidas a e b, e pela lei dos cossenos, temos:

$$c^2 = a^2 + b^2 - 2\,ab\,cos(60°) = a^2 + b^2 - ab = (a + b\omega)(a + b\omega^2) = N(a + b\omega)$$

Seja $\delta \in \mathbb{Z}[\omega]$ tal que $\delta \,|\, (a + b\omega)$ e $\delta \,|\, (a + b\omega^2) \Rightarrow \delta \,|\, (b\omega - b\omega^2) = b\omega(1 - \omega)$, como ω é unidade e $1 - \omega$ é irredutível, temos que $a + b\omega$ e $a + b\omega^2$ tem no máximo $1 - \omega$ como fator comum.
Sendo o produto de $a+b\omega$ e $a+b\omega^2$ um quadrado perfeito e os elementos de $U(\mathbb{Z}[\omega])$ também quadrados perfeitos positivos, podemos concluir através da fatoração única que $a + b\omega = (1 - \omega)^k \cdot \alpha^2$, com $\alpha \in \mathbb{Z}[\omega]$.
Tomando as normas, tem-se $N(a+b\omega) = [N(1-\omega)]^k N(\omega)^2 \Rightarrow c^2 = 3^k N(\alpha)^2$, e assim k também deve ser um múltiplo de 2, e concluímos dessa forma que $a + b\omega = \beta^2$ para algun $\beta \in \mathbb{Z}[\omega]$.
Agora escrevendo $\beta = m + n\omega$, m, $n \in \mathbb{Z}$, obtemos que $a + b\omega = \beta^2$ é igual a

$$(m^2 - n^2) + (2mn - n^2)\omega$$

Daí, $a = m^2 - n^2$, $b = 2mn - n^2$ e

$$\begin{aligned}
c^2 &= a^2 - ab + b^2 \\
&= (m^2 - n^2)^2 - [(m^2 - n^2)(2mn - n^2)] + (2mn - n^2)^2 \\
&= m^4 - 2m^2n^2 + n^4 - (2m^3n - m^2n^2 - 2mn^3 + n^4) + 4m^2n^2 - 4mn^3 + n^4 \\
&= m^4 + n^4 + 3m^2n^2 - 2mn^3 - 2m^3n \\
&= m^4 + 2m^2n^2 - 2mn(m^2 + n^2) + m^2n^2 + n^4 \\
&= (m^2 + n^2)^2 - 2(m^2 + n^2)mn + (mn)^2 \\
&= (m^2 + n^2 - mn)^2
\end{aligned}$$

$\Rightarrow c = m^2 - mn + n^2$.
E portanto, $a = m^2 - n^2$, $b = 2mn - n^2$ e $c = m^2 - mn + n^2$, para todo m, $n \in \mathbb{Z}$, com $m > n$.

Exemplo: Resolva a equação $a^2 - ab + b^2 = 1729$ para os inteiros $a > b > 0$.
Solução: Notamos que $a^2 - ab + b$ é a norma de um número inteiro de Eisenstein, que pode ser expresso pela fatoração $(a + b\omega)(a + b\omega^2)$, com a, $b \in \mathbb{Z}$.
Sabemos que $1729 = 7 \cdot 13 \cdot 19$, e que estes números em $\mathbb{Z}[\omega]$ podem ser fatorados

em irredutíveis da forma:

$$\begin{aligned} 7 &= (3+\omega)(3+\omega^2) \\ 13 &= (4+\omega)(4+\omega^2) \\ 19 &= (5+2\omega)(5+2\omega^2) \end{aligned} \tag{2.2}$$

Como $1729 = (a+b\omega)(a+b\omega^2) = a^2-ab+b^2$ em $\mathbb{Z}[\omega]$, então cada fator $a+b\omega$ deve ser da forma $uABC$, com u uma unidade e

$$\begin{aligned} A &= 3+\omega \, ou \, 3+\omega^2 \\ B &= 4+\omega \, ou \, 4+\omega^2 \\ C &= 5+2\omega \, ou \, 5+2\omega^2 \end{aligned}$$

Daí, observa-se que existem 8 opções possíveis para $A \cdot B \cdot C$. E para cada escolha de A, B, C, multiplicada por uma das seis unidades, é possível obter um par de a, b que satisfaz, $a \geq b \geq 0$:

$$\begin{aligned} ABC &= (3+\omega)(4+\omega)(5+2\omega) = 43+40\omega \\ ABC &= (3+\omega)(4+\omega)(5+2\omega^2) = 45+8\omega \\ ABC &= (3+\omega)(4+\omega^2)(5+2\omega) - 48+23\omega \\ ABC &= (3+\omega)(4+\omega^2)(5+2\omega^2) = 32-15\omega \Rightarrow -\omega^2 ABC = 47+32\omega \\ ABC &= (3+\omega^2)(4+\omega)(5+2\omega) = 47+32\omega \\ ABC &= (3+\omega^2)(4+\omega)(5+2\omega^2) = 25-23\omega \Rightarrow \omega^2 ABC = 48+25\omega \\ ABC &= (3+\omega^2)(4+\omega^2)(5+2\omega) = 37-8\omega \Rightarrow -\omega^2 ABC = 45+37\omega \\ ABC &= (3+\omega^2)(4+\omega^2)(5+2\omega^2) = 3-40\omega \Rightarrow -\omega^2 ABC = 43+3\omega. \end{aligned}$$

Assim, os 8 possíveis pares (a,b) que resolvem o problema são:

$(43,3)$, $(43,40)$, $(45,8)$, $(45,37)$, $(47,15)$, $(47,32)$, $(48,23)$ e $(48,25)$.

Podemos assim generalizar essa problemática para na seguinte situação:

Exemplo: Prove que, para cada inteiro n, o número de soluções inteiras de $x^2-xy+y^2 = n$ é finito e divisível por 6.

Demonstração. Da situação anterior, sabemos que $x^2-xy+y^2 = (x+y\omega)(x+y\omega^2) = n$, com x, y, $n \in \mathbb{Z}$. Como $n \in \mathbb{Z}$, este pode ser escrito como $n_1^{\alpha_1} n_2^{\alpha_2} ... n_r^{\alpha_j}$, com $r \in \mathbb{N}$, onde cada n_i, $1 \leq i \leq r$ é primo em $\mathbb{Z}$, e assim poderemos obter em $\mathbb{Z}[\omega]$ cada $n_i = (x_i + y_i\omega)(x_i + y_i\omega^2)$ na forma de irredutível.
E assim, cada fator $x_i+y_i\omega$ deverá ser da forma $uA_1A_2A_3...A_r$, com $u \in \pm 1, \pm\omega, \pm\omega^2$ e

$$\begin{aligned} A_1 &= (x_1+y_1\omega) \, ou \, (x_1+y_1\omega^2) \\ A_2 &= (x_2+y_2\omega) \, ou \, (x_2+y_2\omega^2) \\ A_3 &= (x_3+y_3\omega) \, ou \, (x_3+y_3\omega^2) \\ &\vdots \\ A_r &= (x_r+y_r\omega) \, ou \, (x_r+y_r\omega^2) \end{aligned}$$

Daí, observa-se que existem 2^r opções possíveis para $A_1 \cdot A_2 \cdot ... A_r$, que multiplicadas por u, essa quantidade será múltipla de 6.
E assim a quantidade de soluções da equação $x^2 - xy + y^2 = n.$ com $n \in \mathbb{Z}$ é finita e divisível por 6. □

Nesse estudo fica claro a importância que à Teoria dos Números tem para Matemática de modo geral, relacionando conceitos com estruturas, despertando o nosso interesse em expandir o anel dos inteiros de Eisenstein como exposto no desenvolvimento desse trabalho, que foi de proporcionar as especificidades dos mesmos, ampliando um pouco da aritmética dos inteiros e dos inteiros de Gauss, promovendo uma preparação para a generalização de conhecimentos e transferência para anéis com estruturas semelhantes de diversos contextos.

Referências

1. HEFEZ, Abramo. Aritmética - 1^a, 2^a edição, 2014 - Rio de Janeiro - Ed. Sociedade Brasileira da Matemática.

2. MARTINEZ, Fabio E. Brochero; MOREIRA, Carlos Gustavo T. de A.; SALDANHA, Nicolau C.; TENGAN, Eduardo. Teoria dos Números: um passeio com primos - 3^a edição - pdf - livrariavirtual.impa.br.

3. Disponivel em: <http://www.ime.unicamp.br/ftorres/MPM1AC2014.pdf>. Acesso: 15 de junho de 2017.

4. Disponível em: <//http: math.stackexchange.com>. Acesso em: 25 de junho de 2017.

5. Disponível em: <http://www.math.purdue.edu>. Acesso em: 22 de julho de 2017.