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

Inteiros Gaussianos[†]

por

Thaise Oliveira de Lima

sob a orientação do

Prof. Dr. Napoleón Caro Tuesta

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

Fevereiro/ 2022
João Pessoa - PB

[†]O presente trabalho foi realizado com apoio da CAPES, Coordenação de Aperfeiçoamento de Pessoal de Nível Superior.

Catalogação na publicação
Seção de Catalogação e Classificação

L732i Lima, Thaise Oliveira de.
Inteiros gaussianos / Thaise Oliveira de Lima. - João Pessoa, 2022.
37 f. : il.

Orientação: Napoleón Caro Tuesta.
Dissertação (Mestrado) - UFPB/CCEN.

1. Matemática - Inteiros gaussianos. 2. Domínio euclideano. 3. Fatoração única. 4. Soma de quadrados. 5. Identidades trigonométricas. I. Tuesta, Napoleón Caro. II. Título.

UFPB/BC CDU 51(043)

Elaborado por WALQUELINE DA SILVA ARAUJO - CRB-15/514

UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE CIÊNCIAS EXATAS E DA NATUREZA
DEPARTAMENTO DE MATEMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA EM REDE NACIONAL
Fone/Ramal: (83) 3216-7563 http://www.ufpb.br/pos/profmat

ATA DA SESSÃO PÚBLICA DE DEFESA DE TRABALHO DE CONCLUSÃO DE CURSO DE MESTRADO PROFISSIONAL REALIZADA NO DEPARTAMENTO DE MATEMÁTICA DO CENTRO DE CIÊNCIAS EXATAS E DA NATUREZA DA UNIVERSIDADE FEDERAL DA PARAÍBA

No dia vinte e um de fevereiro de dois mil e vinte e dois (21/02/2022), às 14:00 horas, por meio da plataforma virtual Google Meet, por meio do link: https://meet.google.com/uif-rppv-mtd, em conformidade com o parágrafo único do Art. 80 da Resolução CONSEPE nº 79/2013, que regulamenta a defesa de trabalho final por videoconferência, seguindo os mesmos preceitos da defesa presencial, em sessão pública, teve início a defesa de trabalho de conclusão de curso intitulado *"**Inteiros Gaussianos**"*, da aluna **THAISE OLIVEIRA DE LIMA**, que havia cumprido, anteriormente, todos os requisitos para a obtenção do grau de Mestra em Matemática, sob a orientação do professor Napoleon Caro Tuesta. A Banca Examinadora, aprovada pelo Colegiado do Programa de Pós-Graduação em Matemática em Rede Nacional – PROFMAT, foi composta pelos professores Napoleón Caro Tuesta (presidente), Lizandro Sanchez Challapa (membro interno/UFPB) e Ivan Italo Gonzales Gargate (membro externo/UTFPR). O professor Napoleón Caro Tuesta, em virtude da sua condição de presidente, iniciou os trabalhos e depois das formalidades de apresentação, convidou a aluna a discorrer sobre o conteúdo do seu trabalho de conclusão. Concluída a explanação, a candidata foi arguida pela Banca Examinadora, que em seguida, sem a presença da aluna, finalizando os trabalhos, reuniu-se para deliberar, tendo concedido a menção: **APROVADA**. Face à aprovação, declarou o presidente achar-se a avaliada legalmente habilitada a receber o Grau de **Mestra** em Matemática, cabendo à Universidade Federal da Paraíba, providências como, de direito, a expedição do Diploma a que a mesma fez jus. Nada mais havendo a tratar, foi lavrada a presente ata que será assinada pelos membros da Banca Examinadora.

João Pessoa, 21 de fevereiro de 2022.

Banca Examinadora

Napoleón Caro Tuesta

Lizandro Sanchez Challapa

Ivan Italo Gonzales Gargate

Agradecimentos

Quero agradecer a Deus por ter me dado força para continuar e concluir mais uma etapa.

Ao meu pai, por ser a minha base e a minha inspiração de força, sabedoria e integridade.

À minha mãe, por acreditar na minha capacidade e por me proteger.

À minha irmã Talita, por estar sempre me apoiando e compartilhando sonhos.

À minha amiga Janieli, por sempre me ajudar e me ouvir durante todo esse processo.

Ao meu orientador Prof. Dr. Napoleón Caro Tuesta, que indicou o tema desse trabalho e esteve presente no seu desenvolvimento. Obrigada pelo empenho e pela confiança.

Aos professores do PROFMAT da UFPB, por nos incentivar em cada disciplina, por serem responsáveis pelos meus conhecimentos durante este processo. Gratidão por cada aula extra, pela paciência, por cada palavra de conforto e esperança.

Dedicatória

Dedico este trabalho aos meus pais e minha irmã Talita.

Resumo

O objetivo principal deste trabalho é estudar algumas propriedades algébricas do anel dos inteiros gaussianos $\mathbb{Z}[i]$. Por exemplo, provaremos que $\mathbb{Z}[i]$ é um domínio euclideano e, portanto, um domínio de fatoração única. Como uma aplicação de caráter aritmética, caracterizamos os números primos que podem ser expressados como soma de dois quadrados. No capítulo final, apresentamos algumas aplicações dos inteiros gaussianos à trigonometria.

Palavras-chaves: Inteiros Gaussianos; domínio euclideano; fatoração única; soma de quadrados; identidades trigonométricas.

Abstract

The main objective of this work is to study algebraic properties of some ring of Gaussian integers $\mathbb{Z}[i]$. For example, we will prove that $\mathbb{Z}[i]$ is a domain Euclidean and therefore a unique factoring domain. As an application of arithmetic character, characterizing the prime numbers that can be expressed as the sum of two squares. In the final chapter we present some applications from Gaussian integers to trigonometry.

Key-words: Gaussian integers; Euclidean domain; unique factorization; sum of squares; trigonometric identities.

Sumário

Capítulo 1

Números complexos

1.1 Introdução

O conceito de número complexo se desenrolou paulatinamente. Ao contrário do que muitos pensam, os números complexos não surgiram com o aparecimento de raízes quadradas de números negativos nas equações de 2 ° grau, já que esta solução era descartada para os números reais e a equação não havia solução.

As primeiras ideias para o que viria a ser o conjunto dos números complexos se deu na busca/disputa pela resolução de equações de 3 ° grau entre Girolamo Cardano e Nicoló Fontana(Tartaglia), onde foi percebido que os números reais eram insuficientes e que o conceito de número necessitava ser estendido.

Das contribuições de Leonard Euler, temos a utilização, pela primeira vez, do símbolo i para representar $\sqrt{-1}$, em que $i^2 = -1$. Assim, surgiu o número complexo $z = a + bi$, onde a e b são números reais.

1.2 Definição

O conjunto dos números complexos, denotado por $\mathbb{C}$, é definido como o conjunto dos pares ordenados de números reais $z = (x, y) \in \mathbb{R}$ x $\mathbb{R}$, em que as operações de adição e multiplicação são definidas por:

$$z_1 + z_2 = (x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$$

e

$$z_1 \cdot z_2 = (x_1, y_1) \cdot (x_2, y_2) = (x_1x_2 - y_1y_2, x_1y_2 + y_1x_2).$$

Tais operações satisfazem as seguintes propriedades:

A1. Comutatividade da adição: $z_1 + z_2 = z_2 + z_1$ para todo $z_1, z_2 \in \mathbb{C}$.

A2. Associatividade da adição: $(z_1+z_2)+z_3 = z_1+(z_2+z_3)$ para todo $z_1, z_2, z_3 \in \mathbb{C}$.

A3. Existência de elemento neutro: existe um número complexo $0 = (0,0)$ tal que $z_1 + 0 = 0 + z_1 = z_1$.

A4. Existência de elemento simétrico da adição: para todo número complexo $z = (a,b)$ existe um número complexo $-z = (-a,-b)$ tal que $z + (-z) = 0 = (-z) + z$.

M1. Comutatividade da multiplicação: $z_1 \cdot z_2 = z_2 \cdot z_1$ para todo $z_1, z_2 \in \mathbb{C}$.

M2. Associatividade da multiplicação: $(z_1 \cdot z_2) \cdot z_3 = z_1 \cdot (z_2 \cdot z_3)$ para todo $z_1, z_2, z_3 \in \mathbb{C}$.

M3. Existência de elemento neutro: existe um número complexo $1 = (1,0)$ tal que $z \cdot 1 = 1 \cdot z = z$ para todo número complexo z.

M4. Existência do inverso multiplicativo: para todo número complexo $z = (x,y)$ não nulo, existe o inverso multiplicativo de z, a saber, $z^{-1} = (\frac{x}{x^2+y^2}, \frac{-y}{x^2+y^2})$ é o número complexo tal que $z \cdot z^{-1} = 1$.

D. Distributividade: $z_1 \cdot (z_2 + z_3) = z_1 \cdot z_2 + z_1 \cdot z_3$ para todo $z_1, z_2, z_3 \in \mathbb{C}$.

Em consequência, o conjunto $\mathbb{C}$ juntamente com as operações de adição e multiplicação definidas formam um *corpo*.

É comum identificar um número complexo da forma $(x,0)$ com o número real x. Por outro lado, o número complexo $(0,1)$ é usualmente denotado por i. Dessa forma, da definição de multiplicação temos que

$$i^2 = i.i = (0,1) \cdot (0,1) = (0-1, 0+0) = (-1,0) = -1.$$

Dado um número complexo $z = (x,y)$ arbitrário, podemos escrever

$$z = (x,y) = (x,0) + (0,y) = (x,0) + (y,0) \cdot (0,1) = x + yi.$$

A representação $z = x + yi$ é chamada de *forma algébrica*, onde x é chamado de *parte real* e y de *parte imaginária*, ou ainda, $x = Re(z)$ e $y = Im(z)$. A unidade imaginária é representada pela letra i que é o número (0, 1).

Dois números complexos $z_1 = a + bi$ e $z_2 = c + di$, com a, b, c e $d \in \mathbb{R}$ são iguais quando $a = c$ e $b = d$, assim z_1 e z_2 têm, respectivamente, as partes reais iguais e as partes imaginárias iguais.

1.3 Representação gráfica

A representação gráfica de um número complexo foi desenvolvida, no início do século XIX, por Gauss e Jean Robert Argand, de forma independente, associaram as partes real e imaginária de um número complexo com as coordenadas de um ponto no plano cartesiano.

Conhecido como Plano de Argand- Gauss, a representação geométrica de números complexos que estão na forma algébrica. Formado por dois eixos: o vertical para representar a parte imaginária e o eixo horizontal para indicar o número real.

Da mesma forma que cada par ordenado de números reais (a, b) pode ser representado no plano cartesiano por um único ponto, cada ponto $P(a, b)$, no plano, está associado a um único número complexo $z = a + bi$ com a e $b \in \mathbb{R}$.

Podemos representar um número complexo $z = a + bi$ como o vetor determinado por o segmento de reta orientado $\vec{OP}$, cuja origem é o ponto $O = (0, 0)$ e extremidade no ponto $P(a, b)$.

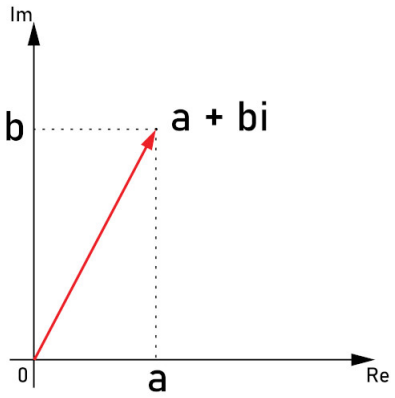


Figura 1: Representação geométrica de números complexos.

1.4 Valor absoluto ou módulo de um número complexo

Com essa representação gráfica dos números complexos, podemos definir o **valor absoluto** ou **módulo** de um número complexo $z = a + bi$ por

$$|z| = \sqrt{a^2 + b^2},$$

onde o valor absoluto representa a distância de z a origem.

Proposição 1.1 *Sejam* $z = a + bi$ *e* $w = c + di \in \mathbb{C}$; *são válidas as seguintes propriedades:*

1)$|z| \geq 0$, *com* $|z| = 0 \Leftrightarrow z = 0$;
2) $|\alpha z| = |\alpha||z|$, $\forall \alpha \in \mathbb{R}$;
3)$|zw| = |z||w|$;
4) $|z^{-1}| = |z|^{-1}$;
5)$|\frac{z}{w}| = \frac{|z|}{|w|}$.

Demonstração:

1) Usando a definição de módulo de um número complexo,
$|z| = \sqrt{a^2 + b^2} \geq 0$.
Quando $|z| = \sqrt{a^2 + b^2} = 0$ com $a = 0$ e $b = 0 \in \mathbb{R}$, isso nos leva a concluir que $a = b = 0 \Rightarrow z = 0$.

2) Queremos provar que $|\alpha z| = |\alpha||z|$, $\forall \alpha \in \mathbb{R}$ e $z = a + bi \in \mathbb{C}$.
Ou seja, $|\alpha(a + bi)| = |\alpha||a + bi|$, $\forall \alpha \in \mathbb{R}$.
Assim, $|\alpha(a + bi)| = |(\alpha a) + (\alpha b)i| = \sqrt{(\alpha a)^2 + (\alpha b)^2}$
$= \sqrt{(\alpha)^2(a^2 + b^2)} = |\alpha|\sqrt{a^2 + b^2}$.
Portanto, $= |\alpha||a + bi|$.

3) Vamos provar que $|zw| = |z||w|$ para z e $w \in \mathbb{C}$.
Veja que $|zw|^2 = |(a+bi)(c+di)|^2 = |(ac-bd)+(ad+bc)i|^2 = (ac-bd)^2+(ad+bc)^2$
$= (ac)^2 - 2acbd + (bd)^2 + (ad)^2 + 2abcd + (bc)^2$
$= a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2$
$= a^2(c^2 + d^2) + b^2(c^2 + d^2) = (a^2 + b^2)(c^2 + d^2)$
$= |z|^2|w|^2$.
Consequentemente, $|zw| = |z||w|$.

4) Para provar que o módulo do inverso multiplicativo de z é o inverso multiplicativo do módulo de z, usaremos o fato de $z.\frac{1}{z} = 1 \Rightarrow |z|.|\frac{1}{z}| = 1$, mas $|\frac{1}{z}| = \frac{1}{|z|}$.
Portanto, $|z^{-1}| = |z|^{-1}$

5) Para demonstrar que $|\frac{z}{w}| = \frac{|z|}{|w|}$.
Assim, $|\frac{z}{w}| = |z.\frac{1}{w}| = |z|.\frac{1}{|w|} = \frac{|z|}{|w|}$. ■

1.5 Conjugado de um número complexo

O **conjugado** de um número complexo $z = a + bi$ é definido como $\bar{z} = a - bi$. Sendo assim, z e $\bar{z}$ são números complexos conjugados com partes reais iguais e

partes imaginárias opostas.

Veja que $|z|^2 = a^2 + b^2 = (a + bi)(a - bi) = a^2 - b^2i^2 = a^2 + b^2$. Obtendo uma relação simples entre o valor absoluto, o número complexo e o seu conjugado de tal forma que $|z|^2 = z.\bar{z}$.

Proposição 1.2 *Sejam $z = a + bi$ e $w = c + di \in \mathbb{C}$ são válidas as seguintes propriedades:*

1) $z = \bar{\bar{z}}$;
2) $\overline{z + w} = \bar{z} + \bar{w}$;
3)$\overline{z.w} = \bar{z}.\bar{w}$;
4) $\overline{z}^{-1} = \overline{z^{-1}}$;
5) $\overline{(\frac{z}{w})} = \frac{\bar{z}}{\bar{w}}$;
6) $|z| = |\overline{z}|$.

Demonstração:

1) Temos que $\overline{z} = a - bi$, então $\bar{\bar{z}} = a - (-b)i = a + bi = z$.
Portanto, $z = \bar{\bar{z}}$ para todo $z = a + bi \in \mathbb{C}$.

2) Para provar que $\overline{z + w} = \bar{z} + \bar{w}$ com z e $w \in \mathbb{C}$, vejamos que:

$$\begin{aligned}
\overline{z + w} &= \overline{(a + bi) + (c + di)} \\
&= \overline{(a + c) + (bi + di)} \\
&= (a + c) - (b + d)i \\
&= (a - bi) + (c - di) \\
&= \overline{z} + \overline{w}.
\end{aligned}$$

3) Queremos provar que $\overline{z.w} = \bar{z}.\bar{w}$ com z e $w \in \mathbb{C}$, vejamos que:

$$\begin{aligned}
\overline{z.w} &= \overline{(a + bi).(c + di)} \\
&= \overline{(ac - bd) + (ad + bc)i} \\
&= (ac - bd) - (ad + bc)i \\
&= [ac - (-b)(-d)] + [a(-d) + c(-b)]i \\
&= (a - bi).(c - di) \\
&= \bar{z}.\bar{w}.
\end{aligned}$$

4) Para $z = a + bi \in \mathbb{C}$, temos que:
$z.z^{-1} = 1 \Rightarrow \overline{(z.z^{-1})} = \overline{1}$.
Pelo item 3), $\overline{z}.\overline{(z^{-1})} = 1$.

Portanto, $\overline{z}^{-1} = \overline{z^{-1}}$.

5) Seja z e $w \in \mathbb{C}$, com $w \neq 0$.
Vejamos que $\overline{(\frac{z}{w})} = \overline{(z.\frac{1}{w})}$ e pelo item 3), temos que:
$\overline{z}.\overline{(\frac{1}{w})} = \overline{z}.\frac{1}{\overline{w}} = \frac{\overline{z}}{\overline{w}}$.
Portanto, $\overline{(\frac{z}{w})} = \frac{\overline{z}}{\overline{w}}$.

6) É fácil ver que $|\overline{z}| = \sqrt{a^2 + (-b)^2} = |z|$. De fato, $|z| = |\overline{z}|$. ■

1.6 Representação polar

Além de identificar um número complexo $z = a + bi$ com um ponto no plano cartesiano ou ainda com um vetor que determina o argumento e o módulo de z, podemos representá-lo através das coordenadas polares(r, θ).

O argumento de um complexo $z = a + bi \neq 0$, com a e $b \in \mathbb{C}$, é definido como qualquer dos ângulos $\theta = arg\ z$ que o vetor $\vec{z}$ forma com o eixo horizontal positivo, medido no sentido anti-horário. Vale ressaltar que todo número complexo tem infinitos argumentos, mas podemos determinar, de maneira única, que θ pertence ao intervalo $(-\pi, \pi)$ e é representado por $arg\ z$.

Considere o número complexo $z = a + bi$, com a e b diferentes de zero, e o ponto Z=(a, b) que o representa.

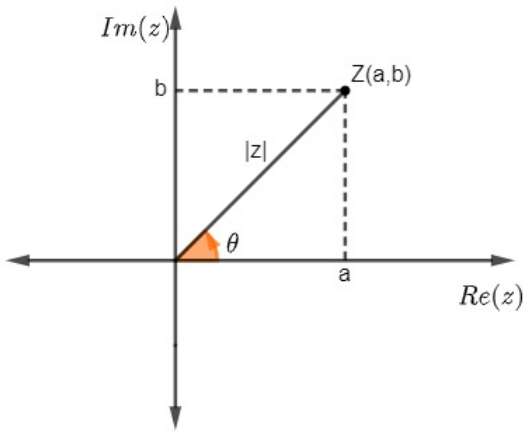


Figura 2: Módulo de um número complexo.

Observando a figura acima e sabendo que θ é argumento de $z = a + bi$, temos que:

$$a = cos\ \theta\ |z|$$

e

$$b = sen\ \theta\ |z|.$$

Desta forma, um número complexo $z \neq 0$ pode ser definido de forma única por $r = |z|$ e $\theta = arg(z)$ para $\theta \in (-\pi, \pi)$, que são as coordenadas polares do ponto Z no plano.

Podemos reescrever

$z = a + bi = |z| \cos\ \theta + |z|\ sen\ \theta i$

$z = r\ cos\ \theta + r\ sen\ \theta i$

$z = r(cos\ \theta + sen\ \theta i)$,

esta representação é chamada de **forma trigonométrica** ou **polar** do número complexo $z = a + bi$.

Definição: Dado $x \in \mathbb{R}$, definimos exponencial de x por

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \frac{x^4}{4!} + ... = \sum_{n=0}^{\infty} \frac{x^n}{n!}.$$

Fórmula de Euler: Dado $\theta \in \mathbb{R}$, vale a identidade $e^{i\theta} = cos\ \theta + sen\ \theta i$.

A expansão da função exponencial e^x, da função seno e da função cosseno em série de Taylor para os valores de $x \in \mathbb{R}$ são resultados que nos levam a veracidade da fórmula de Euler.

A expressão $e^{i\theta}$ na expansão de série de potências dada pela definição acima nos leva a:

$$e^{i\theta} = 1 + i\theta + \frac{(i\theta)^2}{2!} + \frac{(i\theta)^3}{3!} + \frac{(i\theta)^4}{4!} + ...$$

$$e^{i\theta} = 1 + i\theta - \frac{\theta^2}{2!} - i\frac{\theta^3}{3!} + \frac{\theta^4}{4!} + i\frac{\theta^5}{5!} + ...$$

$$e^{i\theta} = \underbrace{1 - \frac{\theta^2}{2!} + \frac{\theta^4}{4!} - \frac{\theta^6}{6!} + \cdots}_{cos\ \theta} + i\underbrace{(\theta - \frac{\theta^3}{3!} + \frac{\theta^5}{5!} - \frac{\theta^7}{7!} + \cdots)}_{sen\ \theta}.$$

$$e^{i\theta} = cos\ \theta + sen\ \theta i.$$

Portanto, podemos representar por $z = |z|e^{i\theta}$, visto que $e^{i\theta} = cos\ \theta + sen\ \theta i$. E quando $\theta = \pi$, teremos que $e^{i\pi} = cos\ \pi + sen\ \pi i = -1 + 0i = -1 \Rightarrow e^{i\pi} + 1 = 0$.

Dados dois números complexos $z_1 = r_1\ cos\ \theta_1 + r_1\ sen\ \theta_1 i$ e $z_2 = r_2\ cos\ \theta_2 + r_2\ sen\ \theta_2 i$ diferentes de zero, a representação polar do produto $z_1.z_2$ é

$z_1.z_2 = (r_1\ cos\ \theta_1 + r_1\ sen\ \theta_1 i).(r_2\ cos\ \theta_2 + r_2\ sen\ \theta_2 i)$

$z_1.z_2 = r_1.r_2[cos\ \theta_1.cos\ \theta_2 - sen\ \theta_1.sen\ \theta_2] + [cos\ \theta_1.sen\ \theta_2 + cos\ \theta_2.sen\ \theta_1]i$
$z_1.z_2 = r_1.r_2[cos\ (\theta_1 + \theta_2) + sen\ (\theta_1 + \theta_2)i]$

E se $z_2 \neq 0$ devemos encontrar uma expressão para $\frac{z_1}{z_2}$ na forma trigonométrica, vejamos:

$$\frac{z_1}{z_2} = \frac{r_1(\ cos\ \theta_1 + \ sen\ \theta_1 i)}{r_2(\ cos\ \theta_2 + \ sen\ \theta_2 i)},$$

multiplicando por $\frac{cos\ \theta_2 - \ sen\ \theta_2 i}{cos\ \theta_2 - \ sen\ \theta_2 i}$.

$$= \frac{r_1(\ cos\ \theta_1 + \ sen\ \theta_1 i)}{r_2(\ cos\ \theta_2 + \ sen\ \theta_2 i)}.\frac{cos\ \theta_2 - \ sen\ \theta_2 i}{cos\ \theta_2 - \ sen\ \theta_2 i}$$

$$= \frac{r_1}{r_2}.\frac{(cos\ \theta_1.cos\ \theta_2 - cos\ \theta_1.sen\ \theta_2 i + sen\ \theta_1.cos\ \theta_2 i + sen\ \theta_1.sen\ \theta_2)}{cos^2\ \theta_2 + sen^2\ \theta_2}$$

$$= \frac{r_1}{r_2}.\frac{(cos\ \theta_1.cos\ \theta_2 + sen\ \theta_1.sen\ \theta_2) + (sen\ \theta_1.cos\ \theta_2 - sen\ \theta_2.cos\ \theta_1)i}{cos^2\ \theta_2 + sen^2\ \theta_2}$$

$$\frac{z_1}{z_2} = \frac{r_1}{r_2}.[cos\ (\theta_1 - \theta_2) + sen\ (\theta_1 - \theta_2)i]$$

1.7 Potência de um complexo

Podemos calcular a potência z^n, $n \in \mathbb{N}$ e $z \in \mathbb{C}$ na forma algébrica $(a+bi)^n$, isso significa que usaríamos o binômio de Newton e ficaria muito trabalhoso. Então seja $z = r(cos\ \theta + sen\ \theta i)$ na forma trigonométrica.

Veja que:
$z^2 = z\ .\ z = r(cos\ \theta + sen\ \theta i)\ .\ r(cos\ \theta + sen\ \theta i)$
$z^2 = r^2[cos\ (\theta + \theta) + sen(\theta + \theta)i]$
$z^2 = r^2[cos\ (2\theta) + isen(2\theta)]$

O mesmo cálculo é aplicado para as demais potências z^3, z^4, z^5 e nos é sugestivo e induz que $z^n = \underbrace{r.r.\cdots.r}_{n\ \text{vezes}}.[cos\ (\underbrace{\theta + \theta + \cdots + \theta}_{n\ \text{vezes}}) + sen\ (\underbrace{\theta + \theta + \cdots + \theta}_{n\ \text{vezes}})i]$.

Proposição 1.3 ***(Fórmula de De Moivre)*** *Se n é um número inteiro, então* $[r(cos\ \theta + isen\ \theta)]^n = r^n[cos\ (n\theta) + sen\ (n\theta)i]$.

Sendo z um número complexo diferente de zero e n um número natural, temos que $z^n = r^n[cos\ (n\theta) + sen\ (n\theta)i]$. A demonstração é deixada para o leitor e pode ser feita por indução para $n \in \mathbb{N}$ e também é válida para expoente inteiro negativo.

1.8 Raiz de um complexo

Dado z um número complexo e $k \in \mathbb{Z}$. Chamamos z_k uma raiz enésima de z quando $(z_k)^n = z$. Veja que as raízes quadradas de -1 são i e $-i$, porque $i^2 = -1$ e $(-i)^2 = (-i)(-i) = -1$.

Vamos calcular $\sqrt[n]{r.[cos\ \theta + sen\ \theta i]}$ para determinar os complexos z tais que $z^n = r.[cos\ \theta + sen\ \theta i]$.

Sendo $z = s.[cos\ \alpha + sen\ \alpha i]$ teremos $(s.[cos\ \alpha + sen\ \alpha i])^n = r.(cos\ \theta + sen\ \theta i)$.

Aplicando a fórmula de De Moivre,

$s^n.\ [cos\ (n\alpha) + sen\ (n\alpha)i] = r.\ [cos\ \theta + sen\ \theta i]$.

Pela proposição 1.3, temos que $s^n = r$ e $(n\alpha = \theta + 2k\pi), k$ inteiro.

Assim $s = \sqrt[n]{r}$ e $\alpha = \frac{\theta+2k\pi}{n}$.

Portanto,

$$z_k = \sqrt[n]{z} = \sqrt[n]{r.\ (cos\ \theta + sen\ \theta i)} = \sqrt[n]{r}.\ [cos\ \left(\frac{\theta + 2k\pi}{n}\right) + sen\ \left(\frac{\theta + 2k\pi}{n}\right) i], k \in \mathbb{Z}.$$

Vejamos que, se $0 \leq k \leq n-1$, as raízes não se repetem. Calculando os valores de z_k para cada valor atribuído a $k \in \mathbb{Z}$, temos:

Para $k = 0 \Rightarrow z_0 = \sqrt[n]{r}.\ [cos\ \left(\frac{\theta}{n}\right) + sen\ \left(\frac{\theta}{n}\right) i]$.
Para $k = 1 \Rightarrow z_1 = \sqrt[n]{r}.\ [cos\ \left(\frac{\theta+2\pi}{n}\right) + sen\ \left(\frac{\theta+2\pi}{n}\right) i]$.
Para $k = 2 \Rightarrow z_2 = \sqrt[n]{r}.\ [cos\ \left(\frac{\theta+4\pi}{n}\right) + sen\ \left(\frac{\theta+4\pi}{n}\right) i]$.
Para $k = 3 \Rightarrow z_3 = \sqrt[n]{r}.\ [cos\ \left(\frac{\theta+6\pi}{n}\right) + sen\ \left(\frac{\theta+6\pi}{n}\right) i]$.

$\vdots$

Para $k = n-1 \Rightarrow z_{n-1} = \sqrt[n]{r}.\ [cos\ \left(\frac{\theta+(n-1)\pi}{n}\right) + sen\ \left(\frac{\theta+(n-1)\pi}{n}\right) i]$.

Perceba que os n valores de z são todos diferentes entre si no intervalo $[0, 2\pi)$ e que os argumentos aumentam em progressão aritmética de razão $\left(\frac{2\pi}{n}\right)$. Geometricamente, os números complexos z_k estão igualmente distribuídos sobre uma circunferência centrada na origem e de raio $\sqrt[n]{r}$.

Capítulo 2

Inteiros Gaussianos

2.1 Introdução

Carl Friedrich Gauss,também chamado de Príncipe da Matemática, nasceu em 1777 e viveu até 1855. Foi físico, astrônomo e um dos maiores matemáticos de todos os tempos. Gauss contribuiu para todas as áreas da Matemática e da Teoria dos Números.

Desde criança as suas habilidades em matemática eram surpreendentes, uma história bem conhecida foi a que ilustra como Gauss deduziu a fórmula da soma dos n primeiros termos de uma progressão aritmética. Na adolescência, obteve os primeiros resultados sobre a geometria esférica. Destinou-se também a visões axiomáticas das provas matemáticas em teoria dos números e aritmética. Provou o teorema da Reciprocidade Quadrática.

Contribuiu com grandes progressos na Matemática e suas aplicações na Astronomia, Estatística e Física. Defendeu a concepção de objetos matemáticos abstratos quando publicou trabalhos sobre os números imaginários.

2.2 Definição

O conjunto dos números complexos da forma $a + bi$, onde a e b são inteiros é denominado o conjunto dos inteiros gaussianos em homenagem a Gauss.

Para ser chamado de anel, os inteiros gaussianos $\mathbb{Z}[i] = \{a + bi |\ a, b \in \mathbb{Z}\}$ devem satisfazer as seguintes propriedades:

A1: Comutatividade da adição

Sejam $z = a + bi$ e $x = c + di$ com $z, x \in \mathbb{Z}[i]$, então $z + x = (a + bi) + (c + di) = (a + c) + (b + d)i = (c + di) + (a + bi) = x + z$.

A2: Associatividade da adição

Sejam $z = a + bi, x = c + di$ e $y = e + gi$ com $z, x, y \in \mathbb{Z}[i]$, então $(z + x) + y = (a+bi+c+di)+e+gi = (a+c+e)+(b+d+g)i = a+bi+(c+di+e+gi) = z+(x+y)$

A3: Existência do elemento neutro da adição

Existe $0 = 0 + 0i$ e $z \in \mathbb{Z}[i]$, donde $z = (0 + 0i) + z = (0 + 0i) + (a + bi) = (a + bi) + (0 + 0i) = a + bi = z$.

A4: Existência do elemento simétrico da adição

Para cada $z = a + bi \in \mathbb{Z}[i]$, existe $z' = -a - bi \in \mathbb{Z}[i]$, tal que $z + z' = 0 + 0i$, com z e z' pertencentes aos inteiros gaussianos.

M1: Comutatividade da multiplicação

Sejam $z = a + bi$ e $x = c + di$ com $z, x \in \mathbb{Z}[i]$, então $z.x = (a + bi).(c + di) = ac + adi + bci - bd = (ac - bd) + (ad + bc)i = (a + di).(a + bi) = x.z$.

M2: Associatividade da multiplicação

Sejam $z = a+bi, x = c+di$ e $y = e+gi$ com $z, x, y \in \mathbb{Z}[i]$, então $(z.x).y = z.(x.y)$

M3: Existência do elemento neutro da multiplicação

Existe um inteiro gaussiano 1 tal que $z \cdot 1 = 1 \cdot z = z$ para todo inteiro gaussiano z.

M4: Distributiva

Sejam $z = a + bi, x = c + di$ e $y = e + gi$ com $z, x, y \in \mathbb{Z}[i]$, então $z \cdot (x + y) = z \cdot x + z \cdot y$ para todo $z, y, x \in \mathbb{Z}[i]$.

Na linguagem da Álgebra, os inteiros gaussianos formam um anel e o anel dos inteiros gaussianos é denotado por $\mathbb{Z}[i]$. Verificaremos que os inteiros reais e inteiros gaussianos se assemelham na aplicação de definições como divisibilidade, números primos, fatoração única.

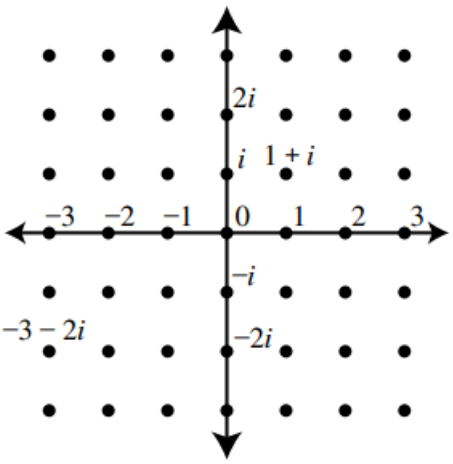


Figura 3: Os inteiros gaussianos, uma rede quadrada em $\mathbb{C}$.

Os inteiros gaussianos $\mathbb{Z}[i] = \{a + bi |\ a, b \in \mathbb{Z}\}$ são a rede dos inteiros $\mathbb{C}$, como mostra a figura acima, e forma um anel comutativo.

2.3 Função Norma de inteiro gaussiano

Definição: O conjugado de $z = a + bi \in \mathbb{Z}[i]$ é definido como $\bar{z} = a - bi \in \mathbb{Z}[i]$.

Definição: A função $N : \mathbb{Z}[i] \to \mathbb{Z}$ é definida para todo $z = a + bi \in \mathbb{Z}[i]$ como $N(z) = z.\bar{z} = (a + bi)(a - bi) = a^2 + b^2$.

Exemplo: $N(4 + 7i) = (4 + 7i)(4 - 7i) = 4^2 + 7^2 = 16 + 79 = 95$.

Teorema 2.1 *A norma é multiplicativa, isto é, se r e $s \in \mathbb{Z}[i]$, então $N(rs) = N(r)N(s)$.*

Demonstração:

Sejam $r = a + bi$ e $s = c + di$, então $r.s = (ac - bd) + (ad + bc)i$.

$N(rs) = (ac - bd)^2 + (ad + bc)^2 = (ac)^2 + (bd)^2 + (ad)^2 + (bc)^2 = a^2(c^2 + d^2) + b^2(c^2 + d^2) = (a^2 + b^2)(c^2 + d^2) = N(a + bi)N(c + di) = N(r)N(s)$. ■

2.4 Inversos multiplicativos

Definição:

Definimos que z é invertível nos $\mathbb{Z}[i]$, se existir $z' \in \mathbb{Z}[i]$, tal que $zz' = 1$.

Teorema 2.2 *Os números 1, -1, i, -i são os únicos que têm inversos multiplicativos, chamados de unidades do anel dos inteiros gaussianos.*

Demonstração:

Sejam $z = a + bi$ e $z' = a' + b'i \in \mathbb{Z}[i]$ tais que $z.z' = 1$. Aplicando o fato que a norma é multiplicativa, temos que $N(zz') = N(z)N(z') = N(1) = 1$. Como a $N(z)$ e a $N(z')$ são números inteiros positivos diferentes de 0, portanto $N(z) = N(z') = 1$. Isso significa que $N(z) = a^2 + b^2 = 1$, ou seja, $a = \pm 1$ e $b = 0$ ou $a = 0$ e $b = \pm 1$. É recíproco para z'.

Desta forma, os únicos inteiros gaussianos invertíveis em $\mathbb{Z}[i]$ são -1, 1, i e -i. São chamados de unidades do anel dos inteiros gaussianos. ■

Teorema 2.3 *$s = (a + bi)$ é uma unidade em $\mathbb{Z}[i]$ se, e somente se, $N(s) = 1$.*

Demonstração:

($\Rightarrow$) Suponhamos que $s = (a+bi) \in \mathbb{Z}[i]$ é uma unidade. Então existe algum $r = (c+di) \in \mathbb{Z}[i]$, onde c e d são diferentes de zero, de modo que $(a+bi)(c+di) = (1+0i)$. Então sabemos que $N((a + bi)(c + di)) = N(1 + 0i)$ e, pelo Teorema 2.1, podemos dizer que $N(a+bi)N(c+di) = N(1+0i)$. Portanto, $(a^2+b^2)(c^2+d^2) = (1^2+0^2) = 1$. Dado que $(a^2 + b^2)$, $(c^2 + d^2) \in \mathbb{Z}^+$ e $(a^2 + b^2)(c^2 + d^2) = 1$, sabemos que $(a^2 + b^2)$ e $(c^2 + d^2)$ são unidades em $\mathbb{Z}$. Porque $(a^2 + b^2)$ e $(c^2 + d^2)$ não são negativos e ambos devem ser iguais a 1. Portanto, $1 = (a^2 + b^2) = N(a + bi) = N(s)$.

($\Leftarrow$) Em seguida, assuma para algum $s = (a + bi) \in \mathbb{Z}[i]$ que $N(s) = 1$. Então $(a^2 + b^2) = 1$, o que implica que $a^2 = 1 - b^2$. Como $a^2 \geq 0$, consideramos dois casos:

Caso 1 : Seja $b^2 = 0$. Então $b = 0$ e $a^2 = 1 - 0 = 1$. Portanto, $a = 1$ ou $a = -1$. Se $a = 1$, então $(a + bi) = (1 + 0i)$. Temos que $(1 + 0i)(1 + 0i) = (1 + 0i)$, $s = (a + bi)$ é uma unidade em $\mathbb{Z}[i]$. Se $a = -1$, então $(a + bi) = (-1 + 0i)$. Dado que $(-1 + 0i)(-1 + 0) = (1 + 0i)$, $s = (a + bi)$ é uma unidade em $\mathbb{Z}[i]$.

Caso 2 : Seja $b^2 = 1$. Então $a^2 = 1 - 1 = 0$. Portanto, $a = 0$ e $b = 1$ ou $b = -1$. Se $b = 1$, $(a + bi) = (0 + i)$. Temos que $(0 + i)(0 - i) = (1 + 0i)$, $s = (a + bi)$ é uma unidade em $\mathbb{Z}[i]$. Se $b = -1$, $(a + bi) = (0 - i)$. Dado que $(0 - i)(0 + i) = (1 + 0i)$, $s = (a + bi)$ é uma unidade em $\mathbb{Z}[i]$. ■

Problemas

1- Mostre que nenhum inteiro gaussiano que não seja uma unidade tem um inverso multiplicativo no anel dos inteiros gaussianos.

Demonstrado no Teorema 2.2

2- Mostre que se $a + bi \neq \pm 1, \pm i$, então $|a + bi| > 1$.

Demonstração:

Seja $z = a + bi \in Z[i]$ e $|a + bi| = \sqrt{a^2 + b^2}$, se $z \neq \pm 1$ e $z \neq \pm i$, então podemos afirmar que $|z| \neq 1$, como não pode ser menor que 1, de fato, $|z| > 1$. ■

3- Mostre que $(a + bi)(a - bi)$ é um número real.

Demonstração:
A multiplicação em questão se refere a um número e o seu conjugado e já vimos que $(a+bi)(a-bi) = a^2 - b^2i^2 = a^2 + b^2$, como a e b são números inteiros, podemos afirmar que $a^2 + b^2$ é um número real. ■

2.5 Divisibilidade de inteiros gaussianos

2.5.1 $\mathbb{Z}[i]$ como um domínio euclidiano

Definição: Um domínio integral D é chamado de Domínio Euclidiano se houver uma função d dos elementos diferentes de zero de D para os inteiros positivos de modo que o seguinte seja verdadeiro:

1. $d(a) \leq d(ab)\ \forall\ a, b \in D$ tal que $a, b \neq 0$.

2. Para todo $a, b \in D$ onde $b \neq 0$, existe $q, r \in D$ tal que $a = bq + r$ onde $d(r) < d(b)$.

O teorema seguinte mostra que a função norma gaussiana satisfaz a proposta propriedade de d acima, tornando $\mathbb{Z}[i]$ um domínio euclidiano.

Teorema 2.4 *O conjunto de inteiros gaussianos forma um domínio euclidiano.*

Demonstração: Sejam g e h elementos diferentes de zero em $\mathbb{Z}[i]$. Sabemos que $1 \leq N(h)$. Como $1 \leq N(g)$, isso implica que $N(g) \leq N(g)N(h)$. Dado $m = (a+bi), n = (c+di) \in \mathbb{Z}[i]$, onde $(c+di) \neq (0+0i)$. Como $(c+di) \neq (0+0i)$, sabemos que $(c+di)^{-1} = \frac{1}{c+di} = (\frac{c}{c^2+d^2} - \frac{d}{c^2+d^2}i)$, onde $\frac{c}{c^2+d^2}$ e $-\frac{d}{c^2+d^2}$ são racionais. Dessa forma, $(c+di)^{-1} \in \mathbb{Q}[i]$, o campo dos racionais gaussianos. Além disso, sabemos que $(a+bi)(c+di)^{-1} = (x+yi)$ para qualquer $(x+yi) \in \mathbb{Q}[i]$. Sejam $s, t \in \mathbb{Z}$, tal que $\frac{-1}{2} \leq (s-x) \leq \frac{1}{2}$ e $\frac{-1}{2} \leq (t-y) \leq \frac{1}{2}$. Assim:

$$\begin{aligned}(a+bi)(c+di)^{-1} &= (x+yi) \\ &= (x+s-s)+(y+t-t)i \\ &= x+s-s+yi+ti-ti \\ &= (s+ti)+(x-s)+(y-t)i.\end{aligned}$$

Então $(a+bi)(c+di)^{-1} = (s+ti)+(x-s)+(y-t)i$.

Multiplicando a igualdade por $(c+di)$ teremos $(a+bi) = (s+ti)(c+di) + ((x-s)+(y-t)i)(c+di)$. Já sabemos que $(s+ti) \in \mathbb{Z}[i]$, pois $s, t \in \mathbb{Z}$. Então $(s+ti)$ é o nosso q, fazendo $((x-s)+(y-t)i)(c+di)$ de resto r. Isolando r, temos

que $r = (a + bi) - (s + ti)(c + di)$. Sendo $\mathbb{Z}[i]$ um anel, o conjunto é fechado para multiplicação e adição. Portanto, $r \in \mathbb{Z}[i]$. Por último, sabemos que;

$$\begin{aligned} N([(x-s)+(y-t)i](c+di)) &= N((x-s)+(y-t)i)N(c+di) \\ &= ((x-s)^2+(y-t)^2)(c^2+d^2) \\ &\leq ((\frac{1}{2})^2+(\frac{1}{2})^2)(c^2+d^2) \\ &= (\frac{1}{2})(c^2+d^2) \\ &< (c^2+d^2) \\ &= N(c+di). \ \blacksquare \end{aligned}$$

Veremos que o anel dos inteiros gaussianos $\mathbb{Z}[i]$ possui propriedades do anel dos inteiros Z.

Definição: Se r e s são inteiros gaussianos, dizemos que r divide s, $r|s$, quando existir $\alpha \in \mathbb{Z}[i]$ tal que $s = r.\alpha$.

Exemplo 1: Como $2 + 11i = (2 + i)(3 + 4i)$, segue que $2 + i$ e $3 + 4i$ dividem $2 + 11i$.

Exemplo 2: $1 + 2i$ não divide $3 + 4i$, pois $= \frac{3+4i}{1+2i} = \frac{3+4i}{1+2i}.\frac{1-2i}{1-2i} = \frac{11-2i}{5} = \frac{11}{5} - \frac{2}{5}i$

Como as partes $\frac{11}{5}$ e $\frac{2}{5}i$ não são números inteiros, então $1 + 2i$ não divide $3 + 4i$

Teorema 2.5 *Seja $z = a + bi \in \mathbb{Z}[i]$ e $c \in \mathbb{Z}$. Então $c|z$ se, e somente se, $c|a$ e $c|b$ em $\mathbb{Z}$.*

Demonstração:

Como $c|(a+bi)$ em $\mathbb{Z}[i]$, então existe $x = m+ni \in \mathbb{Z}[i]$ tal que $a+bi = c(m+ni)$. Isso significa que, $a = cm$ e $b = cn$, sendo assim, $c|a$ e $c|b$.

Reciprocamente, se $c|a$ e $c|b$ então $a = cm$ e $b = cn$, para algum $m, n \in Z$. Como $z = a + bi$, então $z = cm + cni = c(m + ni)$, para algum $c \in Z$ e $x = m + ni \in Z[i]$. De fato, $c|z$. $\blacksquare$

Teorema 2.6 *Para $r, s \in \mathbb{Z}[i]$, se $r|s \in Z[i]$, então $N(r)|N(s) \in \mathbb{Z}$.*

Demonstração:

Se $r|s$, então $s = c.r$ tal que $c \in \mathbb{Z}[i]$. Aplicando o Teorema 2.1, temos que $N(s) = N(cr) = N(c)N(r)$, portanto, $N(r)|N(s) \in \mathbb{Z}$. $\blacksquare$

2.6 Fatoração de inteiros de Gauss

O produto de dois inteiros gaussianos r e s resulta um inteiro gaussiano x, sendo, $x = rs$, dizemos que r e s dividem x. Chamamos $x = rs$ de fatoração de x. No caso da fatoração acima, se os fatores r e s não são uma unidade, então essa fatoração é não trivial de x.

Se um inteiro gaussiano não é zero ou uma unidade, então o seu valor absoluto é maior que um, e todos os fatores não triviais de x têm valor absoluto menor que $|x|$.

Definição

Se w e z forem inteiros gaussianos, ambos não nulos, então definimos o máximo divisor comum de w e z, $mdc(w, z)$, como qualquer divisor comum de w e z de norma máxima. Como w e z são diferentes de zero, o conjunto de divisores comuns é finito(pois a norma é multiplicativa e não negativa) e contém elementos de norma máxima, então $mdc(w, z)$ existe. Ao tomar múltiplos unitários de um valor de $mdc(w, z)$, obtemos quatro valores de $mdc(w, z)$. Com $mdc(w, z)$ definido acima, temos as seguintes propriedades:

i) $mdc(w, z)$ é único até a multiplicação por unidades;

ii) cada divisor comum de w e z divide $mdc(w, z)$, e

iii) $mdc(w, z)$ é uma combinação linear de inteiros gaussianos w e z.

A propriedade (i) diz que $mdc(w, z)$ assume exatamente quatro valores. A prova dessas propriedades produzindo o $mdc(w, z)$ por meio do algoritmo euclidiano se encontra em [5].

Definição

Um inteiro gaussiano z é considerado **primo** se for fatorado apenas por $z = u.r$, onde o fator u é uma unidade. Sendo z e $r \in \mathbb{Z}[i]$ chamados de **associados** quando $z = u.r$ e u é uma unidade. Dois primos que se diferem por um fator de unidade são chamados de **associados**.

Lema 2.1 *Mostre que se z é primo, então $\bar{z}$ também é.*

Demonstração: Vamos supor que z não é primo em $\mathbb{Z}[i]$. Então $z = ab$, onde a e $b \in \mathbb{Z}[i]$ são divisores não triviais de z. Temos $\bar{z} = \bar{a}\bar{b} = \bar{a}\bar{b}$ e portanto $\bar{z}$ tem uma fatoração de números não triviais, ou seja, $\bar{z}$ também não é primo em $\mathbb{Z}[i]$. ■

2.7 O Teorema Fundamental da Aritmética

Definição

Dizemos que dois inteiros gaussianos a e b são relativamente primos se $z|a$ e $z|b$ para $z \in \mathbb{Z}[i]$ implica que z é uma unidade em $\mathbb{Z}[i]$.

Teorema 2.7 *Sejam g e h inteiros gaussianos primos entre si, então 1 pode ser expresso por*

$$rg + th = 1, \tag{2.1}$$

com r e t inteiros gaussianos.

Para a demonstração usaremos o algoritmo euclidiano, que será formulado como um lema.

Lema 2.2 *Dados dois inteiros gaussianos g e h, tomamos sem perda da generalidade*

$$|g| \leq |h|$$

.

Então, há um inteiro gaussiano f tal que

$$|h - fg| < |g|. \tag{2.2}$$

Demonstração:

Devemos mostrar que, para cada uma das quatro unidades u, é verdadeiro que

$$|h - ug| < |h|. \tag{2.3}$$

Veremos melhor geometricamente na figura que segue. Veja, na figura, que o ponto h está no círculo de raio $|h|$ com centro na origem. Os quatro pontos $h - g, h + g, h - ig, h + ig$ estão localizados em um círculo de centro h e de raio $|g|$. Um desses pontos encontra- se dentro da cunha com vértice h, formando um ângulo $\frac{\pi}{2}$ e simétrico em relação à linha que passa por h e a origem. Chamaremos de ponto h_1, onde $h_1 = h - u_1 g$.

Como $|g| \leq |h|$ e com a ajuda da figura, podemos deduzir que $|h_1| < |h|$, provando que a desigualdade 2.3 pode ser satisfeita. Seja P o pé da perpendicular da origem O a um lado da cunha e seja Q a interseção do círculo de raio $|g|$ em torno de h com o lado da cunha. Obviamente $|h_1| \leq |Q|$. O triângulo retângulo QPh é isósceles, então $|h - P| = |P| = \frac{|h|}{\sqrt{2}}$, e

$$|h - Q| = |g|,$$

$$|P - Q| = \pm(|g| - \frac{|h|}{\sqrt{2}}).$$

Pelo Teorema de Pitágoras,

$$|Q|^2 = (|g| - \frac{|h|}{\sqrt{2}})^2 + (\frac{|h|}{\sqrt{2}})^2 = |g|^2 - \sqrt{2}|g||h| + |h|^2.$$

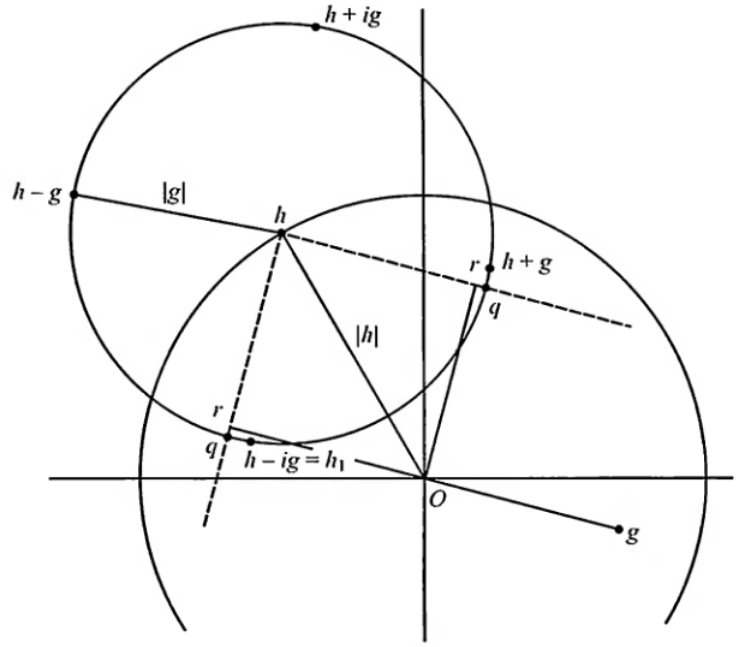


Figura 4.

Em consequência de $|g| \leq |h|$,

$$|Q|^2 \leq |h|^2 + |g|^2 - \sqrt{2}|g|^2 = |h|^2 - (\sqrt{2} - 1)|g|^2.$$

Assim

$$|h_1|^2 \leq |h|^2 - (\sqrt{2} - 1)|g|^2.$$

Se $|h_1| < |g|$, a desigualdade 2.2 é alcançada com $f = u_1$; caso contrário, repetimos esse processo com h_1 em vez de h.

Na próxima etapa, obteremos um inteiro gaussiano

$$h_2 = h_1 - u_2 g = (h - u_1 g) - u_2 g = h - (u_1 + u_2)g = h - f_2 g.$$

Novamente, se $|h_2| < |g|$, finalizamos. Caso não, continuar dessa maneira teremos uma sequência de inteiros gaussianos h_j, cada um da forma $h - fg$, subtraindo em valor absoluto em cada etapa por um valor definido. Sendo assim, após um número finito de etapas, chegamos a $|h_k| < |g|$. Provando o lema. ■

Demonstração:

Agora vamos mostrar o Teorema Fundamental usando o lema, vamos considerar todos os inteiros gaussianos da forma $rg + th$, r e t inteiros gaussianos. Tome $s = rg + gh$ um de menor valor absoluto diferente de zero. Uma vez que g e h não são zero e são da forma $rg + th = 1$, como s é aquele com o menor valor absoluto positivo, segue que

$$|s| \leq |g|, \ |s| \leq |h|.$$

Aplicando o lema em h e s, existe um inteiro gaussiano f tal que $|h - fs|$ é menor $|s|$. Como $h - fs$ também tem a forma (2.1) e, pela propriedade, mínima de s, $h - fs = 0$. Isso significa que s divide h. Da mesma maneira, podemos concluir que s divide g; dado que h e g são relativamente primos, seus únicos divisores comuns são as unidades. Logo, s é uma unidade. Dessa forma, prova que uma das unidades pode ser representada na forma (2.1). Porém, a unidade 1 também pode ser representado por $rh + tg = 1$. E a demonstração é concluída. ■

2.8 Fatoração única de inteiros gaussianos

Veremos que a forma quadrada da estrutura dos $\mathbb{Z}[i]$ tem papel fundamental na fatoração única.

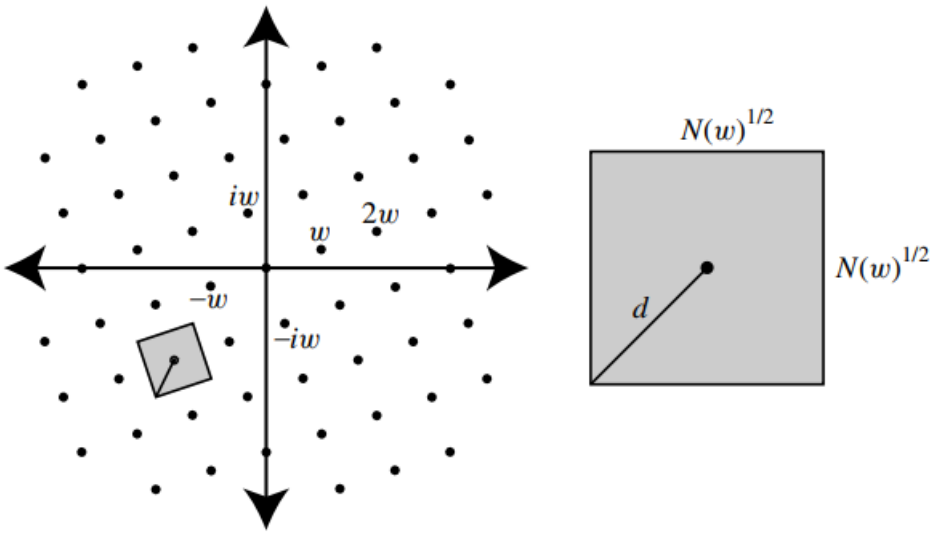


Figura 5: Propriedade de divisão.

Teorema 2.8 *Se $w \neq 0$ e z são inteiros gaussianos, então existem inteiros gaussianos α e β tal que $z = \alpha w + \beta$ e $N(\beta) < N(w)$.*

Demonstração: Veja que a subrede $w\mathbb{Z}[i] = \{\alpha w | \alpha \in \mathbb{Z}[i]\} \subseteq \mathbb{Z}[i]$ tem uma forma quadrada, conforme a figura 5. Portanto, cada $z \in \mathbb{Z}[i]$ encontra- se dentro de d unidades de um ponto em $w\mathbb{Z}[i]$ onde $d = \frac{\sqrt{N(w)}}{\sqrt{2}} < \sqrt{N(w)}$. Escolha α de tal forma que $N(z - \alpha w)$ seja minimizado(tal que α não seja único) e seja $\beta = z - \alpha w$. ■

Teorema 2.9 *Sejam a e b inteiros gaussianos primos entre si e $a|bc$, então $a|c$.*

Demonstração: Pelo Teorema Fundamental da Aritmética, podemos escrever que $ax + by = 1$ com x e y inteiros gaussianos e a e b inteiros gaussianos primos entre si.

Se $a|bc$ existe $e \in \mathbb{Z}[i]$ tal que $bc = ae$

Multiplicando $ax + by = 1$ por c, temos $axc + byc = c$. Substituindo bc por ae na última equação temos que $c = acx + aey = a(cx + ey)$ e, portanto $a|c$. ■

Teorema 2.10 *Se $a \in Z[i]$ e $a|bc$ Então $a|b$ ou $a|c$.*

Demonstração:

Vamos supor que a não divide b. Ou seja, a e b são primos entre si. Pelo teorema anterior, podemos concluir que $a|c$. ■

2.9 Soma de quadrados

Muitos inteiros podem ser escritos como soma de dois quadrados. Vejamos que os números primos $2, 5, 13, 17, 29, 37, ...$ podem ser escritos como a soma de dois quadrados e ambos deixam resto 1, exceto o primo 2, no módulo 4. Temos também que os números primos $3, 7, 11, 19, 23, 31, ...$ não podem ser escritos como soma de dois quadrados e ambos deixam resto 3 no módulo 4. [2], [1]

Definição: Seja $a, b \in \mathbb{Z}$. Então a é um resíduo quadrático módulo b se a equação $x^2 \equiv a \ mod \ b$ tem uma solução em $\mathbb{Z}$. Do contrário, a é chamado de módulo não residual quadrático b.

Definição: Seja $a, p \in \mathbb{Z}$ tal que p é um primo ímpar e $p \nmid a$. O símbolo de Legendre, denotado por $\left(\frac{a}{p}\right)$, definido por:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{se } a \text{ é resíduo quadrático módulo de } p \\ -1, & \text{se } a \text{ não é resíduo quadrático módulo } p. \end{cases}$$

Lema 2.3 *O critério de Euler afirma que se $a, p \in \mathbb{Z}$ tal que p é um primo ímpar e $p \nmid a$, então $\frac{a}{p} = a^{\frac{p-1}{2}} \ mod \ p$.*

A demonstração do critério de Euler pode ser encontrada na página 287 em [1].

Lema 2.4 *Seja p um primo $\in \mathbb{Z}$ tal que $p \equiv 1 \ mod \ 4$, então existem alguns $a, b, m \in \mathbb{Z}$ onde $a^2 + b^2 = pm$ com $0 < m < p$.*

Demonstração: Seja p primo em $\mathbb{Z}$, onde $p \equiv 1 \ mod\ 4$. Vamos considerar o símbolo Legendre $(\frac{-1}{p})$. Pelo critério de Euler, sabemos $(\frac{-1}{p}) \equiv (-1)^{\frac{p-1}{2}} \ mod\ p$. Desde $p \equiv 1 \ mod\ 4$, sabemos que p é ímpar, tornando $(p-1)$ e $\frac{p-1}{2}$. Portanto, $(-1)^{\frac{p-1}{2}} = 1$, o que implica que -1 é um resíduo quadrático $mod\ p$. Por resíduo quadrático, sabemos que existe um $a \in \mathbb{Z}$ onde $0 < a \leq \frac{p-1}{2}$ tal que $a^2 \equiv -1 \ mod\ 4$. Então $p|a^2+1$, e podemos dizer que $pm = a^2+1$ para alguns $m \in \mathbb{Z}$. Como $a \leq \frac{p-1}{2}$, há $a < \frac{p}{2}$ que implica que $a^2 < (\frac{p}{2})^2$. Então $a^2+1 < (\frac{p}{2})^2+1$. Ou seja, $pm < (\frac{p}{2})^2+1$. Como $3 \leq p$, sabemos que $(\frac{p}{2})^2 + 1 < p^2$. Ou seja, $pm < p^2$, implica que $m < p$. Como $0 < a^2 + 1 = pm$, sabemos que $0 < m$. Assim, $0 < m < p$. ■

Lema 2.5 *Se $a, b \in \mathbb{Z}$ tais que a e b podem ser escritos como a soma de dois quadrados, então o produto ab também pode ser escrito como soma de dois quadrados.*

Demonstração: Seja $a, b \in \mathbb{Z}$ tal que $a^2 = c^2 + d^2$ e $b^2 = x^2 + y^2$ para algum $c, d, x, y \in \mathbb{Z}$.

Então

$$\begin{aligned} ab &= (c^2+d^2)(x^2+y^2) \\ &= c^2x^2 + c^2y^2 + d^2x^2 + d^2y^2 \\ &= c^2x^2 + c^2y^2 + d^2x^2 + d^2y^2 + 2cdxy - 2cdxy \\ &= (c^2x^2 + 2cdxy + d^2y^2)(c^2y^2 - 2cdxy + d^2x^2) \\ &= (cx+dy)^2 + (cy-dx)^2. \end{aligned}$$

Como $(cx+dy)$ e $(cy-dx) \in \mathbb{Z}$, o produto ab pode ser escrito como a soma de dois quadrados. ■

Teorema 2.11 *Se p é um primo em $\mathbb{Z}$ tal que $p \equiv 1 \ mod\ 4$, p é expresso como a soma de dois quadrados.*

Demonstração: Seja p primo em $\mathbb{Z}$ tal que $p \equiv 1 \ mod\ 4$. Pelo lema 2.4, sabemos que existe um $m \in \mathbb{Z}$ onde $a^2 + b^2 = pm$ com $0 < m < p$. Tome n o menor inteiro tal que exista $x, y \in \mathbb{Z}$, então $x^2 + y^2 = np$ com $0 < n < p$. Então $1 \leq n$. Se $n = 1$, obtemos $p = a^2 + b^2$. Assuma $1 < n$. Seja $h, k \in \mathbb{Z}$ onde h é o menor resíduo absoluto de $x \ (mod\ n)$ e k é o menor resíduo absoluto de $y \ (mod\ n)$. Então $h \equiv x \ mod\ n$ onde $-[\frac{n}{2}] < h < [\frac{n}{2}]$ e $k \equiv y \ mod\ n$ onde $-[\frac{n}{2}] < k < [\frac{n}{2}]$. Como $h \equiv x \ mod\ n$, $h^2 \equiv x^2 \ mod\ n$. Da mesma forma, dizemos que $k^2 \equiv y^2 \ mod\ n$. Portanto, $h^2+k^2 \equiv x^2+y^2 \ mod\ n$. Já que $x^2+y^2 = np$, teremos $x^2+y^2 \equiv 0 \ mod\ n$. Assim, $h^2+k^2 \equiv 0 \ mod\ n$. Sendo assim, existe $z \in \mathbb{Z}$ tal que $h^2+k^2 = nz$. Portanto, $(x^2+y^2)(h^2+k^2) = n^2pz$.

Pelo Lema 2.5, sabemos $(x^2+y^2)(h^2+k^2) = (xh+yk)^2 + (xk-yh)^2$. Por transitividade, sabemos que $(xh+yk)^2 + (xk-yh)^2 = n^2pz$. Como $h \equiv x \ mod\ n$

e $k \equiv y \ mod\ n$, podemos dizer $(xh + yk)^2 \equiv (x^2 + y^2)^2 \ mod\ n$. Assim, $(xh + yk) \equiv 0 \ mod\ n$. Além disso, $(xk - yh)^2 \equiv (xy - yx)^2 \equiv 0 \ mod\ n$. Desde que $(xh + yk) \equiv (xk - yh) \equiv 0 \ mod n$, podemos dizer que $\frac{xh+yk}{n}, \frac{xk-yh}{n} \in \mathbb{Z}$. Dividindo $(xh + yk)^2 + (xk - yh)^2 = n^2pz$ por n^2, temos $\frac{(xh+yk)^2}{n^2} + \frac{(xk-yh)^2}{n^2} = pz$. Ou seja, $(\frac{(xh+yk)}{n})^2 + (\frac{(xk-yh)}{n})^2 = pz$. Já vimos que $nz = h^2 + k^2$, e definimos h, k de modo que $-[\frac{n}{2}] < h, k < [\frac{n}{2}]$. Sabemos que $h^2, k^2 \leq \frac{n^2}{4}$. Sendo assim, $h^2 + k^2 \leq \frac{n^2}{4} + \frac{n^2}{4} = \frac{n^2}{2}$. Como $nz = h^2 + k^2$, então $nz \leq \frac{n^2}{2}$. Isso implica que $z \leq \frac{n}{2}$. Como $n > 0$, sabemos que $\frac{n}{2} < n$ e que $z < n$. Além disso, $n > 0$ e $nz = h^2 + k^2$, $z > 0$. Portanto, $0 < z < n$. Desde que $(\frac{(xh+yk)}{n})^2 + (\frac{(xk-yh)}{n})^2 = pz$, onde $\frac{xh+yk}{n}, \frac{xk-yh}{n} \in \mathbb{Z}$, contradiz a ideia de que n é o menor inteiro onde pn é a soma de dois quadrados. Então, $n = 1$ e $p = x^2 + y^2$. ■

Teorema 2.12 *Se p é um primo ímpar em $\mathbb{Z}$ e $p = x^2 + y^2$ para algum $x, y \in \mathbb{Z}$, então $p \equiv 1 \ mod\ 4$.*

Demonstração: Seja $p, x, y \in \mathbb{Z}$ onde p é um primo ímpar em $\mathbb{Z}$. Assuma $p = x^2+y^2$. Veja que quando $a \in \mathbb{Z}$ é ímpar, $a^2 \equiv 1 \ mod\ 4$ e quando é par, $a^2 \equiv 0 \ mod\ 4$. Para algum $h \in \mathbb{Z}, b^2 = (2h)^2 = 4h^2 \equiv 0 \ mod\ 4$. Ou seja, a soma de quaisquer dois quadrados são congruentes a $0, 1$ ou 2 módulo 4. Se $p = x^2 + y^2 \equiv 0 \ mod\ 4$, então $4|x^2 + y^2$, o que implica em p par que é absurdo, pois p é um primo ímpar. Se $p = x^2 + y^2 \equiv 2 \ mod\ 4$, então $4|(x^2 + y^2) - 2$. Teríamos que $(x^2 + y^2) - 2 = 4k$, para algum $k \in \mathbb{Z}$. Reescrevendo, $(x^2 + y^2) = 4k + 2 = 2(k + 1)$, o que implica que p é par. Mais uma contradição. Portanto, $p \equiv 1 \ mod\ 4$. ■

2.10 Os primos gaussianos

Definição: Um inteiro gaussiano $\alpha = a + bi$ é chamado de **primo gaussiano** se seus únicos divisores são $\pm(a + bi), \pm 1, \pm i$.

Se α é um inteiro primo isso não implica que necessariamente α seja um primo gaussiano. No teorema abaixo, usaremos a norma para determinar se algum inteiro gaussiano é primo em $\mathbb{Z}[i]$.

Teorema 2.13 *Se $N(\alpha)$ é primo em $\mathbb{Z}$, então α é primo gaussiano e, portanto, irredutível em $\mathbb{Z}[i]$.*

Demonstração:

Vamos supor que α seja um elemento redutível em $\mathbb{Z}[i]$. Seja β e γ elementos que não são unidades e $\in \mathbb{Z}[i]$, $\alpha = \beta\ \gamma$.

Aplicando a função norma para ambo os lados, temos $N(\alpha) = N(\beta\gamma) = N(\beta)N(\gamma)$.

Como β e γ não são unidades, então $N(\beta) > 1$, $N(\gamma) > 1$. Como $N(\alpha)$ pode ser escrito como produto de dois fatores que não são unidades e $\mathbb{Z}$ é um domínio euclidiano. Então, podemos concluir que $N(\alpha)$ não é primo em $\mathbb{Z}$. ■

Teorema 2.14 *Se p é um primo gaussiano $\in \mathbb{Z}[i]$ e $p|\alpha\beta$ para α e β pertencentes aos inteiros gaussianos, então $p|\alpha$ ou $p|\beta$.*

Demonstração: Dados p é um primo $\in \mathbb{Z}[i]$ e $p|\alpha\beta$ para α e $\beta \in \mathbb{Z}[i]$. Vamos supor que p e α são relativamente primos. Pelo Teorema 2.7, sabemos que $p.r + \alpha.s = 1$ para alguns r e $s \in \mathbb{Z}[i]$. Multiplicando por β , teremos $p\beta r + \alpha\beta s = \beta$. Como $p|\alpha\beta$ implica que existe $w \in \mathbb{Z}[i]$ tal que $p.w = \alpha\beta$.

Substituindo $p.w = \alpha\beta$ em $p\beta r + \alpha\beta s = \beta$, temos que $p.(\beta r + p.w.s) = \beta$. Consequentemente, $p|\beta$. ■

Teorema 2.15 *Todo primo $p \in \mathbb{Z}$ da forma $4n + 3$ é um primo gaussiano.*

Demonstração:

Vamos supor p um primo no anel de inteiros reais da forma $4n+3$ e não seja um primo gaussiano, então a fatoração não trivial é $p = st$, com s e t inteiros gaussianos e ambos não são unidades. Aplicando o valor absoluto ao quadrado do produto, temos:

$$p^2 = |s|^2|t|^2.$$

Sendo p um primo real, a única fatoração não trivial é $p^2 = pp$. Consequentemente,

$$|s|^2 = |t|^2 = p$$

.

Seja $s = a + bi$, para a e b inteiros reais. Pela relação acima, podemos expressar que $a^2 + b^2 = p$.

Como o quadrado de um inteiro real é congruente a 0 ou 1 mod 4 , podemos concluir que a soma de dois inteiros reais nunca terá a forma $4n+3$. Por contradição, o teorema fica provado. ■

Lema 2.6 *Se $a, b, p \in \mathbb{Z}$ tal que p é primo, $p \equiv 3 \ mod\ 4$. Se $p|a^2 + b^2$, então $p|a$ e $p|b$.*

Demonstração: Seja $a, b, p \in \mathbb{Z}$ tal que p é primo, $p \equiv 3 \ mod\ 4$. Vamos supor que $p|a^2 + b^2$. Pelo Teorema2.15 , sabemos que $p \equiv 3 \ mod\ 4$ é um primo em $\mathbb{Z}[i]$. Além disso, podemos reescrever $p|a^2+b^2$ como $p|(a+bi)(a-bi)$. Pelo Teorema 2.14, podemos afirmar que $p|(a + bi)$ ou $p|(a - bi)$. Em ambos os casos, vemos que $p|a$ e $p|b$. ■

Teorema 2.16 *Se p um número primo, então $(p-1)! \equiv -1 \ mod\ p$.*

A demonstração do Teorema de Wilson pode ser encontrada na página 240 em [1].

Teorema 2.17 *Todo primo $p \in \mathbb{Z}$ da forma $4n+1$ pode ser fatorado em primos, onde $p = q\bar{q}$, sendo q um primo gaussiano.*

Demonstração:

Seja p um primo real qualquer, então $(p-1)! \equiv -1 \; mod \; p$.

Fatorando $(p-1)!$ da seguinte forma: $(p-1)! = [1.2. \; ... \; .\frac{p-1}{2}][(p-1)(p-2). \; ... \; .\frac{p+1}{2}] = fg$. Cada fator f e g é o produto de $\frac{(p-1)}{2}$ fatores, e o j-ésimo fator de g é congruente com o negativo do j-ésimo fator de f. Segue que $g \equiv (-1)^{\frac{(p-1)}{2}} f$. Quando p tem a forma $4n+1$, então $\frac{(p-1)}{2}$ é par, então $f \equiv g \; mod \; p$. Usando o Teorema de Wilson, podemos concluir que $f^2 \equiv \; -1 \; mod \; p$, o que significa que f^2+1 é divisível por p. Nos inteiros gaussianos, podemos escrever f^2+1 como $f+i$ ou $f-i$. Este produto é divisível por p. Se p fosse um primo gaussiano, ele dividiria um dos fatores $f+i$ ou $f-i$; mas não é possível, pois teríamos que $f \pm i = p(a+bi)$. Olhando para a parte imaginária temos que $pb = \pm 1$, o que é um absurdo pois p é primo em $\mathbb{Z}$. Portanto, p não é primo em $\mathbb{Z}[i]$.

Seja q um primo gaussiano que divide p tal que $p = qw$. Aplicando o conjugado complexo temos $p = \bar{q}\bar{w}$, o que mostra que $\bar{q}$ divide p. Como q e $\bar{q}$ são primos distintos, segue o teorema 2.14 que também seu produto $q\bar{q} = |q|^2$ divide p. Como p é um primo real, $|q|^2 = p$. ■

Agora veremos que os inteiros gaussianos que se encontram nas quatro linhas da figura abaixo desempenharão um papel fundamental.

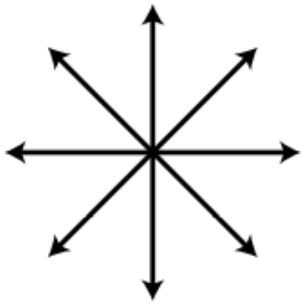


Figura 6: As quatro linhas em $\mathbb{C}$.

As quatro linhas são determinas em $\in \mathbb{C}$ como:

$$Im(z) = 0, Re(z) = Im(z), Re(z) = 0 \; e \; Re(z) = -Im(z).$$

Lema 2.7 *Seja $z \neq 0$ um inteiro gaussiano. Existe um número natural n tal que z^n é real se, e somente se, z está em uma das quatro linha na figura acima.*

Demonstração:

($\Leftarrow$) Seja $z = a + bi \in \mathbb{Z}[i]$ diferente de zero. Tome $n = 1, 2$ ou 4.

Quando $n = 1$ e $z = a \in \mathbb{Z}[i]$, $z^1 = a^1$ é um número real.

Para $n = 2$ e $z = bi \in \mathbb{Z}[i]$, $z^2 = (bi)^2 = -b^2$ é um número real.

Quando o inteiro gaussiano z tiver $Re(z) = Im(z)$ ou $Re(z) = -Im(z)$, o z^4 será um número real.

($\Rightarrow$) Seja $z^n = m \in \mathbb{Z}$ com $z = a + bi \neq 0$. O caso geral decorre facilmente do caso onde z não é uma unidade e é primitivo, isto é, $mdc(a, b) = 1$. Nesse caso, seja w qualquer primo gaussiano divisor de z. Então $w|m$ e também $\bar{w}|\bar{m} = m$, pois m é real. Como $\bar{w}$ é um primo gaussiano que divide $m = z^n$, vemos que $\bar{w}|z$. ■

Fatoração única implica imediatamente no seguinte.

Fato. Se w é um primo gaussiano que divide z, w e $\bar{w}$ não são associados, então $w\bar{w} \in \mathbb{Z}$ divide z.

Demonstração:

Como z é primitivo, o fato implica que z é um produto de primos gaussianos, cada um dos quais é associado de seu conjugado. Seja $v = c + di$ um fator primo gaussiano de z. Como v e $\bar{v}$ são associados, vemos que $c = 0, d = 0$ ou $c = \pm d$. Os dois primeiros casos não são possíveis, pois z é primitivo. E o terceiro caso implica que $c = \pm 1$ já que v é primo. Segue que v é um associado de $1 + i$ e $z = u(1 + i)^l$ para alguma unidade u e l um número natural. ■

Capítulo 3

Aplicações à trigonometria

A série *Gregory* pode ser encontrada aplicando a Série de MacLaurin na função arco tangente de x e é representada por

$$arctg\ x = x - \frac{x^3}{3} + \frac{x^5}{5} - \frac{x^7}{7} + \frac{x^9}{9} - ..., |x| \leq 1. \tag{3.1}$$

Combinada com a identidade $\frac{\pi}{4} = arctg\ 1$, chegamos na série de *Leibniz*

$$\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - ..., |x| \leq 1. \tag{3.2}$$

Vale salientar que esta série foi um avanço na aproximação dos dígitos decimais do número π, embora não seja indicada por ter uma taxa de convergência muito lenta. Outras identidades utilizaram os x^n termos na série de *Gregory* para obter boas aproximações de π. Presumivelmente, buscavam- se uma identidade do tipo $\pi = r.arctg\ x$, com r e x racionais e $|x| < 1$ em que exigiria uma avaliação da função arco tangente e essa avaliação convergiria rapidamente. Veremos que tal identidade não existe.

Iremos estudar as aplicações do lema 2.7 na formação de identidades tangentes, triângulos e polígonos em placas geográficas. Vamos fixar $k \in \mathbb{Z}$ e $n \in \mathbb{N}$ para este capítulo.

3.1 Aplicações

Corolário 3.1 *Os únicos valores racionais de* tan $k\pi/n$ *são* 0 *e* ± 1.

Demonstração: Seja $b \in \mathbb{Z}$ e $a \in \mathbb{N}$, vamos supor que tan $k\pi/n = b/a$.

Temos $\frac{k\pi}{n} = arg(a + bi) \Longrightarrow k\pi = arg(a + bi)^n \Longrightarrow (a + bi)^n \in \mathbb{Z}$.

Sendo assim, cada $arg(a + bi)$ representado por $k\pi/n$ é um múltiplo inteiro de $\pi/4$ e o lema 2.7 implica tan $k\pi/n = 0$ e tan $k\pi/n = \pm 1$. ■

Chegamos ao resultado da inexistência em identidades de arco tangente de ângulo único para π.

Corolário 3.2 *Identidades da forma $k\pi = n\ arctg\ x$ com x racional têm $x = 0$ ou $x = \pm 1$. Em particular, $\pi = 4\ arctg\ 1$ é a identidade mais eficiente para calcular π.*

Demonstração: Supondo $k\pi/n = arctg\ x$, aplicando tangente temos que tan $k\pi/n = x$ e pelo corolário 3.1, $x = 0$ e $x = \pm 1$. ■

Corolário 3.3 *As identidades de arco tangente de múltiplos ângulos racionais para π têm a forma $\frac{k\pi}{n} = \sum_{j=1}^{l} m_j\ arctg\ \frac{b_j}{a_j}$ em que todas as variáveis são inteiros racionais. Se essa fórmula for verdadeira, então $\frac{k\pi}{n} = \frac{j\pi}{4}$ para algum inteiro j.*

Demonstração: Usando o módulo 2π, teremos

$\frac{k\pi}{n} = \sum_{j=1}^{l} m_j\ arctg\ \frac{b_j}{a_j} = \sum_{j=1}^{l} m_j\ arg(a_j + ib_j) = arg \prod_{j=1}^{l} (a_j + ib_j)^{m_j}$.

Chamando o produtório de s, então s^n é real e também $arg\ s = \frac{k\pi}{n}$ é um múltiplo de $\frac{\pi}{4}$ conforme o lema 2.7. ■

O motivo da existência de identidades de múltiplos ângulo não triviais é simples. Basta olhar para identidades de ângulo duplo

$$\frac{k\pi}{n} = m_1\ arctg\ \frac{b_1}{a_1} + m_2\ arctg\ \frac{b_2}{a_2}. \tag{3.3}$$

Tome $s_j = a_j + b_j$ para $j = 1, 2$ e $s = s_1^{m_1} s_2^{m_2}$. A equação acima 3.3 implica que s^n é real(por outro lado, se $(s_1^{m_1} s_2^{m_2})^n$ é real, onde $s_j = a_j + ib_j$, e $a_j \neq 0$ para $j = 1, 2$, assim temos uma identidade da forma 3.3 para algum $k \in \mathbb{Z}$. Como s^n é real, a prova do lema 2.7 mostra que se $w \in \mathbb{Z}[i]$ é um divisor primo de s, então w também é. A diferença é que esses primos conjugados podem aparecer separadamente s_1 e s_2, em relação ao caso de ângulo único.

O lema 2.7 também tem várias aplicações para triângulos. Digamos que um ângulo é racional, desde que seja comensurável com um ângulo reto; equivalentemente, sua medida de grau é racional ou sua medida em radianos é um múltiplo racional de π. Dizemos que um lado de um triângulo é racional desde que seu comprimento seja racional.

Corolário 3.4 *Um triângulo retângulo com ângulos agudos racionais e pernas(lados) racionais é um triângulo $45 - 45 - 90$.*

Demonstração: Suponha que o triângulo Δ ABC tem um ângulo reto em C, pernas(lados) racionais a e b opostos aos ângulos em A e B, respectivamente. O ângulo β em B é um múltiplo racional de π. Então $\tan\beta = \frac{b}{a}$ é racional e igual a $+1$ pelo corolário 3.1, pois os comprimentos dos lados são positivos. Portanto, $\beta = \frac{\pi}{4}$ e o resultado segue. ■

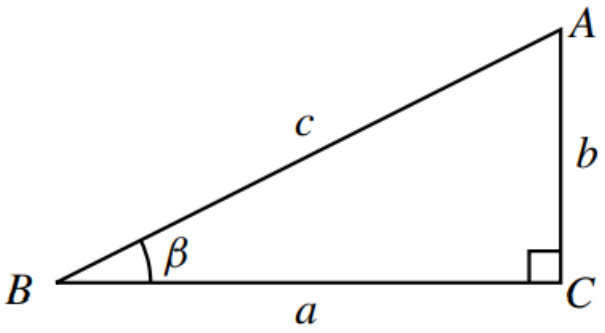


Figura 7.

Corolário 3.5 *Os ângulos agudos em um triângulo retângulo com comprimentos laterais racionais nunca são racional.*

Demonstração: Suponha que o triângulo Δ ABC tem um ângulo reto em C, lados racionais a, b e c opostos aos ângulos em A, B e C, respectivamente. E o ângulo β em B é um múltiplo racional de π. O corolário anterior implica que $a = b$. Aplicando o Teorema de Pitágoras, temos que $2a^2 = c^2$, uma contradição à fatoração única de inteiros racionais. ■

Isso significa que todo triângulo cujos comprimentos laterais formam um triplo pitagórico tem medida de ângulos agudos de grau irracional, sendo esta a explicação por não ter os ângulos de tais triângulos enfatizados no ensino básico.

Vale mencionar lembrar que um *geoboard* é uma placa plana contendo pinos em forma de rede quadrada, conforme a figura seguinte. Para formar os polígonos e ângulos , são colocados elásticos em torno dos conjuntos de pinos. Como construir um triângulo equilátero, polígonos regulares e certos ângulos em *geoboard* são os questionamentos mais frequentes. É preciso ter um pouco de cuidado aqui como mostrado à direita na figura abaixo. Cada segmento reto de S do elástico se estende entre dois pinos P_1 e P_2; se S não é paralelo ao segmento conectando os centros de P_1 e P_2, então os ângulos e polígonos que podem ser construídos dependem do diâmetro dos pinos.

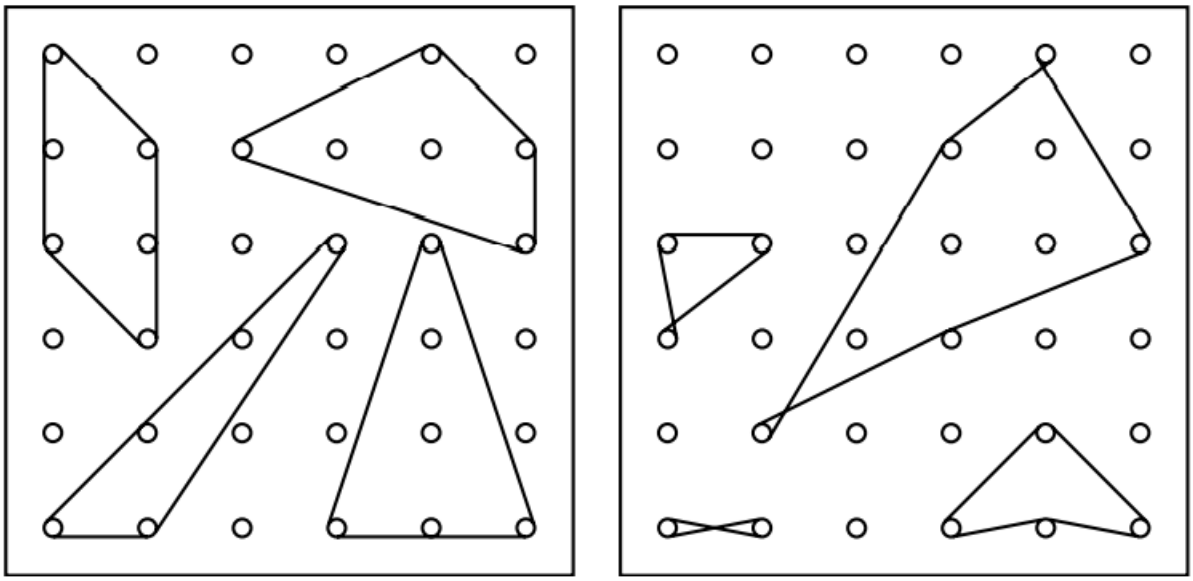


Figura 8: Dois geoboards 6 x 6.

Para se ter mais exatidão, podemos fazer essa suposição paralela ou idealizar e transformar os pinos em pontos, este será adotado. Vamos definir ângulo de rede como um ângulo formado por raios $v\vec{w}$ e $v\vec{z}$, com $v, w, z \in \mathbb{Z}[i]$ e $v \neq w, z$. Vejamos a figura abaixo.

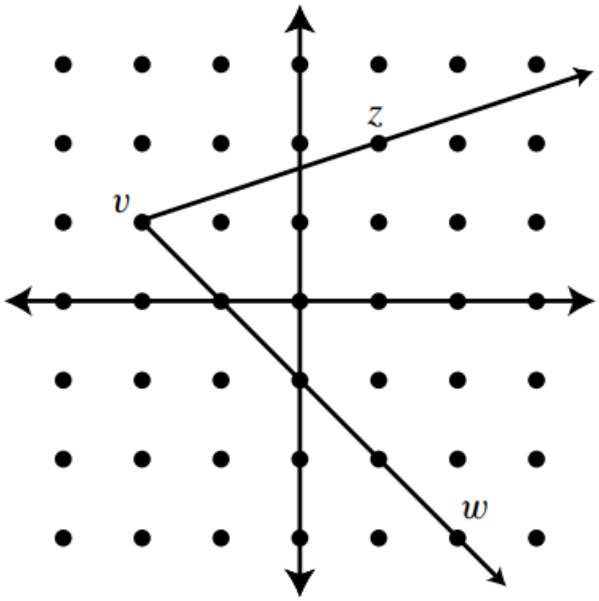
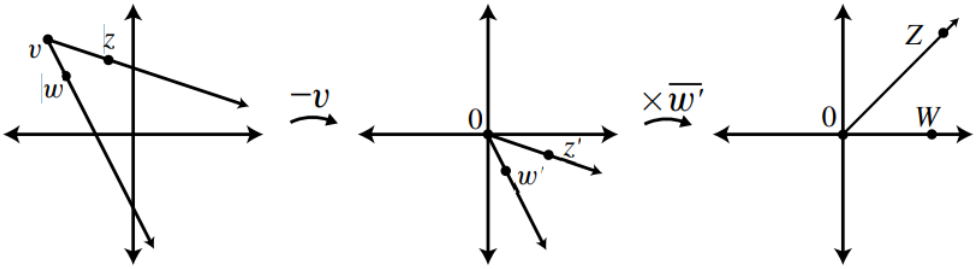


Figura 9: Um ângulo de rede.

Corolário 3.6 *Se um ângulo de rede é racional, então sua medida é um múltiplo inteiro de* $\frac{\pi}{4}$.

Demonstração: Dados os raios $v\vec{w}$ e $v\vec{z}$ formando um ângulo de rede racional. A estratégia é aplicar dois ângulos preservando as transformações algébricas de $\mathbb{Z}[i]$ para que o lema 2.7 seja aplicado ao ângulo congruente resultante. De início, transladando por $-v$, que mapeia $\mathbb{Z}[i]$ em si mesmo e é uma isometria de $\mathbb{C}$. Deixe $w' = w - v$ e $z' = z - v$. Em seguida, multiplicando por $\overline{w'} \neq 0$, que mapeia $\mathbb{Z}[i]$ em si mesmo e é uma transformação de similaridade. Mais especificamente, esta segunda transformação gira cerca de 0 por $arg\ \overline{w'}$ e dimensiona todos os comprimentos de $\sqrt{N(\overline{w'})}$; deixe $W = w'\overline{w'}$ e $Z = z'\overline{w'}$. O ângulo formado por $0\vec{W}$ e $0\vec{Z}$ é racional, sendo congruente ao ângulo original, e $W > 0$. Portanto, Z^n é real para algum número natural n. Pelo lema 2.7, a prova é finalizada. ■



3.2 Observações finais

Existem outras séries para $arctg\ x$, assim como acontece com a série de Gregory, eles também beneficiam em termos de convergência de argumentos de pequeno valor absoluto. As identidades arco tangentes foram originalmente descobertas usando fórmulas da adição de ângulos (co)tangentes. A teoria dos números de inteiros gaussianos impulsionou na busca por essas identidades.

O fato do corolário 2 de que $k\pi = n\ arctg\ \frac{b}{a}$ tem apenas as soluções inteiras racionais óbvias, isto é, $b = 0$ ou $\frac{b}{a} = \pm 1$.

O corolário 3 mostra de fato que as identidades racionais arco tangente em geral só podem realizar inteiros múltiplos de $\frac{\pi}{4}$. Outra abordagem do corolário 1 é mostrar que as únicas raízes racionais da função $tan(k\ arctg\ x), k \in \mathbb{N}$ são $x = 0$ e $x = \pm 1$.

Referências Bibliográficas

[1] Hefez, Abramo. Aritmética/ Abramo Hefez- Rio de Janeiro: SBM, 2014.

[2] May, Catrina A., "Application of the Euler Phi Function in the Set of Gaussian Integers"(2015). Honors Theses. 11.

[3] Lima, Elon Lages. A matemática do ensino médio - volume 3/ Elon Lages lima, Paulo Cezar Pinto Carvalho, Eduardo Wagner, Augusto César Morgado. -6.ed. - Rio de Janeiro: SBM 2006.

[4] Góes, Anderson Roges Teixeira. Números complexos e equações algébricas/ Anderson Roges Teixeira Góes, Heliza Colaço Góes. Curitiba: InterSaberes, 2015.(Série Matemática em Sala de Aula).

[5] Jack S. Calcut. Gaussian Integers and Arctangent for π, Amer. Matemática. Mensal 116 (2009), pp. $515 - 530$.

[6] Peter D. Lax. Appendix I of The Geometry of Numbers, pp. 139 - 150. Mathematical Association of America, 2000.

[7] Mundo Educação. Plano de Argand-Gauss (plano complexo). Disponível em: <https://mundoeducacao.uol.com.br/matematica/plano-argandgauss.htm>. Acesso em: 12 de dezembro de 2021 às 21 : 07 : 00.

[8] Carneiro, Luís Sales. Números complexos : por que não estudar? / Luís Sales Carneiro. â Campina Grande, 2019.

[9] ROQUE, Tatiana. História da Matemática: uma visão crítica, desfazendo mitos e lendas. Rio de Janeiro: Zahar, 2012.

[10] InfoEscola. Carl Friederich Gauss. Disponível em: <://www.infoescola.com/biografias/carl-friederich-gauss/>. Acesso em 19 de março de 2022 às 20 : 07 : 00.