Universidade Federal da Paraíba
Centro de Ciências Exatas e da Natureza
Departamento de Matemática
Curso de Pós-Graduação em Matemática em Rede Nacional - PROFMAT

Números Primos Gaussianos[†]

por

Cybele Verde Aragão de Almeida

sob orientação do

Prof. Dr. Bruno Henrique Carvalho Ribeiro

Trabalho de Conclusão do Curso apresentado ao Corpo Docente do Curso de Pós-Graduação em Matemática em Rede Nacional PROFMAT CCEN-UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

Agosto/2014
João Pessoa - PB

[†]O presente trabalho foi realizado com apoio da CAPES

Números Primos Gaussianos

por

Cybele Verde Aragão de Almeida

Trabalho de Conclusão do Curso apresentado ao Corpo Docente do Curso de Pós-Graduação em Matemática em Rede Nacional PROFMAT CCEN-UFPB, como requisito para obtenção do título de Mestre em Matemática.

área de Concentração: Matemática

Aprovada por:

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

Prof. Dr. Antônio de Andrade e Silva - UFPB

Prof. Dr. Francisco Sibério Bezerra Albuquerque - UEPB

Agosto/2014

Agradecimentos

Primeiramente a DEUS, que sempre está presente no meu caminho me acompanhando.

À minha família, em especial, meus pais, por serem meus melhores amigos. Por sempre acreditarem em meu potencial e investirem no meu crescimento pessoal. Por me colocar no caminho do bem e sempre me ensinar o que é certo e o que é justo. Por estarem ao meu lado em todos os momentos de minha vida. Obrigado pai, obrigado mãe por serem os melhores pais que alguém pode ter, não sei se um dia vou poder agradecer o suficiente, amo vocês. Aos meus irmãos, Alexandre, Bruno e Júnior, pelo carinho e amizade que tem por mim, pelo respeito e apoio as minhas decisões, obrigado por contribuírem para união de nossa família, sei que sempre posso contar com vocês. As meus queridos sobrinhos, Gabriel e Cael, minhas cunhadas Eline e Fabiane, pelo carinho, pela força e apoio nas horas mais difíceis. Sou grata por vocês estarem sempre comigo.

Nathália Raphaella minha amiga e companheira em todas as horas.

Ao meu orientador, Prof. Dr. Bruno Henrique Carvalho Ribeiro que indicou o tema deste trabalho, acompanhou o seu desenvolvimento, ajudando sempre que foi solicitado. Só tenho agradecer essa oportunidade.

A todos os professores que ministraram as aulas no PROFMAT na UFPB, a todos os companheiros de turma 2012, em especial a Alessandro Mignac , Magnun Cesar, André Soares e Washington Gonçalves que contribuíram e acreditaram em meu potencial para que chegasse no final dessa etapa. Que durante os dois últimos anos, enfrentaram a estrada Recife - João Pessoa todos os sábados.

Ao corpo docente e meus amados alunos da Escola Adelaide Pessoa Câmara que souberam compreender minhas ausências, meus estresses e minhas angustias nesse momento tão importante da minha vida.

A todos que fazem parte da família EXATACOR, por ceder esse espaço e pela compreensâo das minhas faltas.

Aos meus amigos de João Pessoa, Alisson Thomas, Felipe, Samara e Bruno Farias, pela hospedagem durante desses dois anos.

A SBM - Sociedade Brasileira de Matemática, pela oportunidade oferecida aos professores da rede pública.

A CAPES - Coordenação de Aperfeiçoamento de Pessoal de Nível Superior pela bolsa concedida.

Dedicatória

A todos os que se alegram com o nosso sucesso.

Epígrafe

A Matemática é a rainha das ciências e a teoria dos números é a rainha das matemáticas. (Gauss)

Resumo

Nosso propósito neste trabalho é apresentar uma categoria especial de números: os números primos de Gauss. Fazemos uma abordagem histórica de como surgiu o interesse de Carl Friesrich Gauss nos estudos pelos números complexos, surgindo em sua homenagem, os números inteiros de Gauss. Citamos os teoremas mais importantes e/ou interessantes com suas proposições e suas respectivas demonstrações, e desenvolvemos alguns exemplos para facilitar a compreensão. Também serão apresentados os números primos Gaussianos e vamos concluir com atividades para o ensino médio envolvendo conceitos básicos dos números complexos, comparações entre os primos inteiros e primos Gaussianos, envolvendo Teorema Fundamental da Aritmética.

Abstract

Sumário

Introdução

Neste trabalho iremos abordar os números inteiros de Gauss que possibilitaram estudos nas áreas de Teoria dos Números, Teoria dos Números Algébricos, estudos dos Números Complexos. Estes números aparecem naturalmente em questões relacionadas ao último Teorema de Fermat, às reciprocidades cúbica e biquadrática e à fatoração única dos números primos.

No Capítulo 1, faremos um breve histórico sobre a obra do matemático alemão Carl F. Gauss, que produziu com desenvoltura em todos os ramos da matemática. É notório o prazer que sentia pela investigação em Aritmética. A sua obra monumental *"Disquisitiones Arithmeticae"* lançou os fundamentos da Teoria dos Números moderno. Em 1825, publicou um trabalho em que introduzia os números complexos da forma $a + bi$, com a e $b \in \mathbb{Z}$ e $i^2 = -1$. Esse conjunto é indicado por $\mathbb{Z}[i]$ e é denominado inteiros de Gauss ou conjunto dos inteiros Gaussianos em homenagem ao seu criador. Em seguida, introduzimos as principais propriedades dos números Inteiros Gaussianos: norma, divisibilidade, Teorema da Divisão, Algoritmo de Euclides, Teorema de Bézout e Fatoração única. Cada uma dessas propriedades tem teoremas e corolários importantes para podermos compreender os números primos Gaussianos.

No Capítulo 2, vamos definir quem são os números primos em $\mathbb{Z}[i]$ e aplicar as propriedades dos números inteiros Gaussianos para identificá-los. Mostraremos que nem todos primos inteiros positivos serão primos de Gauss, pois veremos que os primos p em $\mathbb{Z}$ na forma $4n + 1$ podem ser escritos pelo produto de dois inteiros Gaussianos.

No Capítulo 3, vamos apresentar propostas de atividades para o professor aplicar em sala de aula desenvolvidas para turmas do 3º ano do ensino médio, tendo como objetivo de despertar curiosidades nos alunos em relação aos primos Gaussianos.

Para finalizar, no Capítulo 4, iremos solucionar detalhadamente as atividades proposta no Capítulo 3.

Capítulo 1

Números Inteiros de Gauss

No ínicio deste capítulo vamos fazer uma abordagem histórica dos números inteiros de Gauss, mostrando sua importância, fornecendo ideias para que o Professor de Matemática possa trabalhar este assunto na série final do ensino médio. No decorrer do capítulo, vamos estabelecer várias definições, propriedades e teoremas relacionados aos números Gaussianos. Os números inteiros de Gauss não está presente no currículo do ensino médio, mas o Professor de Matemática pode fazer algumas adaptações para facilitar a compreensão dos alunos em relação os números complexos. As referências utilizadas para a elaboração deste capítulo foram BOYER [1], BUTLER [2], CONRAD [3], EVES [4], FUJIWARA [6], HEFEZ [7] e SIDKI [8].

1.1 Considerações Históricas

Considerado como um dos maiores matemáticos que já existiu, Carl Friesrich Gauss nasceu em Brunswich na Alemanha em 30 de Abril de 1777 e faleceu na cidade de Gottingen, 23 de Fevereiro de 1855. Gauss demonstrou desde muito cedo os seus dotes para a matemática. As suas contribuições para a teoria dos números, dos números complexos, da geometria e da álgebra são inúmeras. Por exemplo, a sua tese de doutoramento foi a primeira demonstração do teorema fundamental da álgebra. Gauss teve também uma importante contribuição para a astronomia, tendo se interessado pelo estudo das órbitas planetárias e pela determinação da forma da Terra. Um exemplo dessa contribuição foi o desenvolvimento de um método para calcular, com grande precisão, os parâmetros de uma órbita planetária a partir de apenas três observações da posição do planeta.

Entre 1808 e 1825 Carl F. Gauss investigava questões relacionadas à reciproci-

dade cúbica e à biquadrática, quando percebeu que essa investigação se tornava mais simples trabalhando sobre $\mathbb{Z}[i]$, chamado posteriormente de inteiros Gaussianos, do que em $\mathbb{Z}$, o conjunto dos números inteiros. O conjunto $\mathbb{Z}[i]$ é formado pelos números complexos da forma $a + bi$, onde a e b são números inteiros e $i^2 = -1$. Os inteiros de Gauss formam um conjunto com uma série de propriedades parecidas com a dos inteiros reais, porém mais gerais. A divisibilidade torna-se mais complexa: tome, por exemplo, 5 o qual é primo em $\mathbb{Z}$, mas que pode ser escrito como produto de dois elementos de $\mathbb{Z}[i]$, a saber $5 = (1 + 2i)(1 - 2i)$. Em verdade, nenhum primo real da forma $(4n+1)$ é um "primo de Gauss", ao passo que primos reais da forma $(4n-1)$ permanecem primos no sentido generalizado. No livro *Disquisitiones Arithmeticae*, Gauss inclui o Teorema Fundamental da Aritmética. Todo domínio de integridade em que a fatoração é única é chamado hoje de domínio de integridade de Gauss.

Gauss estendeu a ideia de número inteiro quando definiu o conjunto $\mathbb{Z}[i]$, pois descobriu que muito da teoria de Euclides sobre fatoração de inteiros poderia ser transportada para $\mathbb{Z}[i]$ com consequências importantes para a Teoria dos Números. Ele desenvolveu uma teoria de fatoração em primos para esses números complexos e demonstrou que essa decomposição em primos é única, como acontece com o conjunto dos números inteiros. A ferramenta que Gauss fez desse novo tipo de número foi de fundamental importância na demonstração do Último Teorema de Fermat. Os inteiros de Gauss são exemplos de um tipo particular de número complexo, a saber, números complexos que são soluções de uma equação polinomial: $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0$, onde todos os coeficientes $a_n, a_{n-1}, \ldots a_1$ e a_0 são números inteiros. Esses números complexos que são raízes de uma equação polinomial com coeficientes inteiros são chamados de números inteiros algébricos. Por exemplo, a unidade imaginária i, é um inteiro algébrico, pois satisfaz a equação $x^2 + 1 = 0$.

1.2 Os Inteiros de Gauss

Definição 1 *Os inteiros de Gauss são os elementos do conjunto:*

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}.$$

Vamos mostrar algumas das propriedades aritméticas dos inteiros de Gauss. Primeiramente, observamos que $\mathbb{Z}[i]$ é um subconjunto de $\mathbb{C}$, o conjunto dos números complexos. Sendo assim, consideremos o conjunto $\mathbb{Z}[i]$ munido das operações de adição e multiplicação herdadas de $\mathbb{C}$. Isto é, se $z_1 = a + bi$ e $z_2 = c + di$, então:

$$z_1 + z_2 = (a + c) + (b + d)i \text{ e}$$

$$z_1 \cdot z_2 = (ac - bd) + (ad + bc)i.$$

Elementos inversíveis com respeito a multiplicação são chamados de unidades. As unidades em $\mathbb{Z}[i]$, analogamente a $\mathbb{Z}$, são todos os elementos $z \in \mathbb{Z}[i]$ que possuem inverso, ou seja, é um elemento $z' \in \mathbb{Z}[i]$ tal que $z \cdot z' = 1$. As unidades de $\mathbb{Z}$ são 1 e -1, desde que $1 \cdot 1 = 1$ e $(-1) \cdot (-1) = 1$. Em $\mathbb{Z}[i]$ são quatro unidades. Mais uma vez, temos 1 e -1, mas também temos i e $-i$, observando que $i \cdot (-i) = 1$ e $(-i) \cdot i = 1$. Como podemos ter certeza de que existem apenas os quatro elementos multiplicativo?

A prova que exitem apenas quatro unidades no conjunto dos inteiros de Gauss é feita por contradição. O primeiro passo consiste em definir a norma de um número inteiro Gaussiano, que faremos mais adiante, embora seja o mesmo que para os números complexos.

1.2.1 A Norma

Em $\mathbb{Z}$, tamanho é medido pelo valor absoluto. Em $\mathbb{Z}[i]$, usamos a norma.

Definição 2 *A norma de* $a + bi \in \mathbb{Z}[i]$ *é* $N(a + bi) = a^2 + b^2$.

Assim, por exemplo, $N(57 - 11i) = 57^2 + 11^2 = 3370$. Alguns matemáticos preferem definir a norma como o valor $\sqrt{a^2 + b^2}$, que é a raíz quadrada da norma, aqui, será mais conveniente não extraírmos está raíz, pois a aritmética torna-se- á mais simples.

A seguir, o Lema que ajudará nas demosntrações das propriedades dos inteiros de Gauss.

Lema 1.1 *Para todos os números inteiros de Gauss* s *e* t, *temos* $N(s) \cdot N(t) = N(st)$.

Prova. Vamos considerar $s = a + bi \Rightarrow N(s) = a^2 + b^2$ e $t = c + di \Rightarrow N(t) = c^2 + d^2$. Nota-se que: $st = (a + bi) \cdot (c + di) = (ac - bd) + (ad + bc)i$. Utilizando uma álgebra:

$$\begin{aligned} N(st) &= (ac - bd)^2 + (ad + bc)^2 \\ &= a^2c^2 - 2abcd + b^2d^2 + a^2d^2 + 2abcd + b^2c^2 \\ &= a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2 \\ &= a^2(c^2 + d^2) + b^2(c^2 + d^2) \\ &= (a^2 + b^2)(c^2 + d^2) \\ &= N(s)N(t). \end{aligned}$$

■

Agora podemos esclarecer a questão das unidades de $\mathbb{Z}[i]$. Como uma primeira aplicação do Lema 1 .1, podemos determinar os inteiros de Gauss, que têm inversos multiplicativos em $\mathbb{Z}[i]$. A ideia é aplicar normas para reduzir a questão a inversibilidade em $\mathbb{Z}$.

Corolário 1.1 *Os únicos inteiros de Gauss que são inversíveis em* $\mathbb{Z}[i]$ *são* ± 1 *e* $\pm i$.

Prova. Podemos perceber que ± 1 e $\pm i$ têm inversas em $\mathbb{Z}[i]$. Onde 1 e -1 são a sua própria inversa e i e $-i$ são inversos um do outro como vimos anteriormente. Suponha que $\alpha \in \mathbb{Z}[i]$ seja inversível, digamos $\alpha \cdot \beta = 1$, para algum $\beta \in \mathbb{Z}[i]$. Queremos mostrar que $\alpha \in \{\pm 1, \pm i\}$. Tomando a norma de ambos os lados da equação $\alpha \cdot \beta = 1$, encontramos $N(\alpha)N(\beta) = 1$. Esta é uma equação em $\mathbb{Z}$, então sabemos que $N(\alpha) = \pm 1$. Uma vez que a norma não tem valores negativos, $N(\alpha) = 1$. Considere $\alpha = a + bi$, temos $a^2 + b^2 = 1$, e as soluções inteiras nos mostra quatro valores para $\alpha = \pm 1, \pm i$. ■

A norma de cada inteiro de Gauss é um número inteiro não-negativo, mas não é verdade que todo inteiro não-negativo é uma norma. De fato, as normas são os inteiros da forma $a^2 + b^2$, e a recíproca não é verdadeira pois existe número inteiro positivo que não é a soma de dois quadrados.

Lema 1.2 *Para todos os números inteiros de Gauss* s *e* t, *com* $t \neq 0$, *temos que* $N\left(\frac{s}{t}\right) = \frac{N(s)}{N(t)}$.

Prova. Vamos considerar que $s = a + bi \Rightarrow N(s) = a^2 + b^2$ e $t = c + di \Rightarrow N(t) = c^2 + d^2$. Nota-se que: $\frac{s}{t} = \frac{(a+bi)}{(c+di)} = \frac{(a+bi)}{(c+di)} \cdot \frac{(c-di)}{(c-di)} = \left(\frac{ac+db}{c^2+d^2}\right) + \left(\frac{bc-ad}{c^2+d^2}\right) i$.

Utilizando a álgebra:

$$\begin{aligned} N\left(\frac{s}{t}\right) &= \left(\frac{ac+db}{c^2+d^2}\right)^2 + \left(\frac{bc-ad}{c^2+d^2}\right)^2 \\ &= \left(\frac{a^2c^2+2abcd+d^2b^2+b^2c^2-2abcd+a^2d^2}{(c^2+d^2)^2}\right) \\ &= \left(\frac{a^2c^2+d^2b^2+b^2c^2+a^2d^2}{(c^2+d^2)^2}\right) \\ &= \left(\frac{a^2(c^2+d^2)+b^2(c^2+d^2)}{(c^2+d^2)^2}\right) \\ &= \left(\frac{a^2+b^2}{c^2+d^2}\right) \\ &= \frac{N(s)}{N(t)}. \end{aligned}$$

■

1.2.2 Divisibilidade

O Lema acima pode parecer sem importância, mas $\frac{N(s)}{N(t)}$ é um importante problema. Dados inteiros de Gauss s e t, será que $\frac{s}{t}$ também é um inteiro Gaussiano? A resposta é simples: às vezes. Nem todas essas divisões produzem um número inteiro de Gauss, e como sempre a divisão por zero é proibida.

Tomando $\alpha = (57 - 11i)$ podemos encontrar um número $\beta = (a + bi)$ para $\beta \in \mathbb{Z}[i]$, onde quociente da divisão entre α e β, não pertence ao conjunto dos números inteiros Gaussianos. Por exemplo, $\frac{(57-11i)}{(14+3i)} = 3,731 - 1,585i$, considerando três casas decimais, claramente que o quociente não pertence $\mathbb{Z}[i]$. Vamos agora encontrar um inteiro de Gauss $\beta = (a + bi)$ que divide $\alpha = (57 - 11i)$ com quociente sendo um número inteiro de Gauss. Percebemos que a divisão tem a mesma definição nos números inteiros:

Definição 3 *Dizemos que o inteiro de Gauss $(a + bi)$ divide o inteiro de Gauss $(c + di)$ se, e somente se, podemos encontrar um inteiro de Gauss $(e + fi)$ tal que $(c + di) = (a + bi)(e + fi)$. Se $(a + bi)$ divide $(c + di)$, utilizamos a notação $(a + bi) \mid (c + di)$.*

Exemplo 1 *Vejamos* $(7-25i)$. *Temos:*

$$\begin{aligned}(7-25i)\cdot(a+bi) &= (57-11i)\\ 7a+7bi-25ai-25bi^2 &= (57-11i)\\ (7a+25b)+(7b-25a)i &= (57-11i)\end{aligned}$$

Vamos formar um sistema: $\begin{cases} 7a+25b=57 \\ -25a+7b=-11 \end{cases} \Rightarrow a=1$ *e* $b=2$. $(1+2i)\in\mathbb{Z}[i]$.
Portanto, vimos que $\dfrac{(57-11i)}{(7-25i)}=1+2i$.
Logo, $(7-25i)\mid(57-11i)$ *e* $(1+2i)\mid(57-11i)$. $\diamond$

Exemplo 2 *Então* $(14+3i)\nmid(57-11i)$, *pois*

$$\begin{aligned}(14+3i)(a+bi) &= (57-11i)\\ 14a+14bi+3ai+3bi^2 &= (57-11i)\\ (14a-3b)+(14b+3a)i &= (57-11i)\end{aligned}$$

Vamos formar um sistema: $\begin{cases} 14a-3b=57 \\ 3a+14b=-11 \end{cases} \Rightarrow a=\dfrac{153}{41}$ *e* $b=-\dfrac{65}{41}$.

$\left(\dfrac{153}{41}-\dfrac{65}{41}i\right)\notin\mathbb{Z}[i]$. $\diamond$

Proposição 1 *O inteiro de Gauss* $\alpha=a+bi$ *é divisível por um número inteiro* c *se, e somente se,* $c\mid a$ *e* $c\mid b$ *em* $\mathbb{Z}$.

Prova. Tome $c\mid(a+bi)$ em $\mathbb{Z}[i]$ é igual $a+bi=c\cdot(m+ni)$ para qualquer $m,n\in\mathbb{Z}$ que é equivalente $a=cm$ e $b=cn$, ou $c\mid a$ e $c\mid b$. ■

Tomando $b=0$ no Proposição 1 nos diz que a divisibilidade entre inteiros comuns não muda quando se trabalha em $\mathbb{Z}[i]$: para $a,c\in\mathbb{Z}$, então $c\mid a$ em $\mathbb{Z}[i]$ se, e somente se, $c\mid a$ em $\mathbb{Z}$. No entanto, isso não significa que outros aspectos de $\mathbb{Z}$ permanecem o mesmo para $\mathbb{Z}[i]$. Por exemplo, veremos que alguns primos em $\mathbb{Z}$ não são primo em $\mathbb{Z}[i]$. A multiplicatividade da norma transforma as relações de divisibilidade em $\mathbb{Z}[i]$ em relações de divisibilidade em $\mathbb{Z}$.

Proposição 2 *Para* α,β *em* $\mathbb{Z}[i]$, *se* $\beta\mid\alpha$ *em* $\mathbb{Z}[i]$, *então* $N(\beta)\mid N(\alpha)$ *em* $\mathbb{Z}$.

Prova. Considere $\alpha=\beta\cdot\gamma$ para $\mathbb{Z}[i]$. Tomando a norma de ambos os lados, temos que: $N(\alpha)=N(\beta)\cdot N(\gamma)\Rightarrow N(\beta)\mid N(\alpha)$. ■

Corolário 1.2 *Um inteiro de Gauss tem norma par se, e somente se, ele é um múltiplo de* $(1+i)$.

Prova. Como $N(1+i)=2$, qualquer múltiplo de $(1+i)$ tem norma par. Por outro lado, suponha que $(a+bi)$ tem norma par. Então $a^2+b^2 \equiv 0 \pmod 2$. Analisando os casos:

i - Para a sendo um número par e b sendo um número ímpar. Temos que: $a=2m$ e $b=2n+1$, onde $m,n \in \mathbb{Z}$, então:

$$(2m)^2+(2n+1)^2 \equiv 1 \pmod 2.$$

ii - Para a e b ambos números pares. Temos: $a=2m$ e $b=2n$, onde $m,n \in \mathbb{Z}$, então:

$$(2m)^2+(2n)^2 \equiv 0 \pmod 2.$$

iii - Para a e b ambos números ímpares. Temos que : $a=2m+1$ e $b=2n-1$, onde $m,n \in \mathbb{Z}$, então:

$$\begin{aligned}(2m+1)^2+(2n-1)^2 &\equiv 0 \pmod 2.\\ m-n &\equiv 0 \pmod 2.\\ m &\equiv n \pmod 2.\end{aligned}$$

Portanto $a \equiv b \pmod 2$.
Considere $a+bi=(1+i)\cdot(u+vi)$, para alguns $u,v \in \mathbb{Z}$. Temos que:

$$\begin{aligned}a+bi &= u+vi+ui+vi^2\\ &= (u-v)+(u+v)i\end{aligned}$$

Vamos formar um sistema :$\begin{cases} u-v=a \\ u+v=b \end{cases} \Rightarrow u=\dfrac{b+a}{2}$ e $v=\dfrac{b-a}{2}$.
Temos que u e v são números inteiros desde que $a \equiv b \pmod 2$. Assim, $(1+i) \mid (a+bi)$ sendo a e b ambos pares ou ambos ímpares. ■

Exemplo 3 $N(1+3i)=1^2+3^2=10 \equiv 0$ *(mod 2), temos que* $(1+i) \mid (1+3i)$, *ou seja,* $(1+3i)=(1+i)(2+i)$.◇

Exemplo 4 *$N(1+2i) = 1^2 + 2^2 = 5 \equiv 1$ (mod 2), temos que $(1+i) \nmid (1+2i)$, ou seja, $(1+2i)$ não é múltiplo de $(1+i)$.* $\diamond$

Exemplo 5 *$N(2+6i) = 2^2 + 6^2 = 40 \equiv 0$ (mod 2), temos que $(1+i) \mid (2+6i)$, ou seja, $(2+6i) = (1+i)(4+2i)$.*$\diamond$

A Proposição 2 é importante para mostrar de uma forma rápida e prática como verificar se o inteiro de Gauss não é divisível por outro inteiro de Gauss. Transformar um problema de divisibilidade em $\mathbb{Z}[i]$ em $\mathbb{Z}$, tem um apelo óbvio, uma vez que é mais confortável trabalhar com a divisibilidade em $\mathbb{Z}$.

A recíproca nem sempre é verdadeira. Vejamos, por exemplo para $\alpha = (14 + 3i)$ e $\beta = (4 + 5i)$. Temos que $N(\beta) = 4^2 + 5^2 = 41$ e $N(\alpha) = 14^2 + 3^2 = 205 = 41 \cdot 5$, então $N(\beta) \mid N(\alpha)$, em $\mathbb{Z}$, pórem $(4 + 5i) \nmid (14 + 3i)$.

Em $\mathbb{Z}$, se $|m| = |n|$, então $m = \pm n$, ou seja, m e n são associados. Em $\mathbb{Z}[i]$ é falso: pois se $N(\alpha) = N(\beta)$ não significa que seja verdade que α e β são múltiplos unitários entre si. Considere $(4+5i)$ e $(4-5i)$. Temos $N(4-5i) = N(4+5i) = 41$, mas os múltiplos unitários de $(4 + 5i)$ são:

(a) $(4 + 5i) \cdot 1 = 4 + 5i$

(b) $(4 + 5i) \cdot (-1) = -4 - 5i$

(c) $(4 + 5i) \cdot i = 4i - 5 = -5 + 4i$

(d) $(4 + 5i) \cdot (-i) = -4i + 5 = 5 - 4i$

O número $(4-5i)$ não está nesta lista, então $(4+5i)$ e $(4-5i)$ não são múltiplos unitários. Iremos ver mais tarde que $(4 + 5i)$ e $(4 - 5i)$ são ainda relativamente primos em $\mathbb{Z}[i]$. Em suma, tomar a norma em $\mathbb{Z}[i]$ é um passo mais drástico do que a remoção de um sinal em um número inteiro.

1.2.3 O Teorema da Divisão

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

Teorema 4 *(Teorema da Divisão). Para $\alpha, \beta \in \mathbb{Z}[i]$ com $\beta \neq 0$, existem $\gamma, \delta \in \mathbb{Z}[i]$ de tal forma que $\alpha = \beta\gamma + \delta$ e $\delta > 0$ ou $N(\delta) < N(\beta)$. Na verdade, podemos escolher δ de tal sorte que $N(\delta) \leqslant \dfrac{N(\beta)}{2}$.*

Os números dos γ e δ são o quociente e resto, respectivamente, e o resto é limitado (de acordo com a sua norma) pelo tamanho do β que representa o divisor.

Antes de provar o Teorema 4, notamos que há uma sutileza na tentativa de calcular γ e δ. Isto pode ser melhor compreendido por meio do seguinte exemplo.

Exemplo 6 *Considere* $\alpha = 27-23i$ *e* $\beta = 8+i \Rightarrow N(\beta) = 8^2+1^2 = 65$. *Queremos escrever* $\alpha = \beta\gamma + \delta$ *com* $N(\delta) < 65$.

$$(27-23i) = (8+i)\cdot(a+bi) \Rightarrow a = \frac{193}{65} \text{ e } b = -\frac{211}{65}$$

Temos que: $\frac{193}{65} = 2,969\ldots$ *e* $-\frac{211}{65} = -3,246\ldots$. *Como* a *e* $b \notin \mathbb{Z}$, *então vamos considerar o seu inteiro e temos que* $\gamma = 2-3i$. *No entanto,* $\alpha = \beta\gamma + \delta \Rightarrow$

$$\begin{aligned} \delta &= \alpha - \beta\gamma \\ &= (27-23i) - (8+i)(2-3i) \\ &= (27-23i) - (16+2i-24i+3) \\ &= 8-i. \end{aligned}$$

Como $\delta = 8-i \Rightarrow N(8-i) = 8^2+1^2 = 65 = N(\beta)$. $\diamond$

O ideal é que a norma do resto da divisão seja inferior a norma do divisor. Assim, a nossa escolha para γ e δ não é desejável. Para corrigir a nossa abordagem, temos que pensar cuidadosamente sobre a nossa forma de substituir $\frac{193}{65} = 2,969\ldots$ e $-\frac{211}{65} = -3,246\ldots$ com números inteiros próximos. Note-se que $\frac{193}{65}$ e $-\frac{211}{65}$ estão mais próximo à direita de um número inteiro. Vamos usar o número inteiro mais próximo em vez de o maior inteiro, portanto, $\left(\frac{193}{65}\right)$ é mais próximo de 3 e $\left(-\frac{211}{65}\right)$ é mais próximo de -3, logo $\gamma = 3-3i$. Temos que :

$$\begin{aligned} \delta &= \alpha - \beta\gamma \\ &= (27-23i) - (8+i)(3-3i) \\ &= (27-23i) - (24+3i-24i+3) \\ &= -2i \end{aligned}$$

Como $\delta = -2i \Rightarrow N(\delta) < 65$. Então, nós usamos $\gamma = 3-3i$ e $\delta = -2i$. Escolhendo o número inteiro mais próximo, em vez do que o maior inteiro, também poderia ser feito em $\mathbb{Z}$.

Em verdade, o que estamos fazendo é tomando o menor inteiro maior do que alguém. Por exemplo, $\frac{34}{9} = 3,77\ldots$ está mais próximo de 4 do que de 3. Em relação a divisão com resto, isto corresponde a:

$$34 = 9 \cdot 4 - 2$$

ou

$$34 = 9 \cdot 3 + 7.$$

O resto da primeira equação é negativo, mas é menor em valor absoluto. O que encontramos aqui é o teorema da divisão modificada em $\mathbb{Z}$. No Teorema da divisão normalmente o resto não é negativo e é limitado superiormente por $|\beta|$.

Às vezes, o número pode estar no meio entre dois múltiplos de b, caso em que o quociente e o resto não são únicos, por exemplo, se $a = 27$ e $b = 6$, então existe um número equidistante entre $4b$ e $5b$:

$$27 = 6.4 + 3 \text{ e } 27 = 6.5 - 3.$$

Assim, temos duas escolhas de $r = 3$ ou $r = -3$. O teorema da divisão usual em $\mathbb{Z}$ tem um quociente e um resto único, mas a versão modificada não apresenta esta singularidade. Isto pode parecer uma calamidade, mas é exatamente o que precisamos para provar o teorema da divisão em $\mathbb{Z}[i]$ (Teorema 6). Após a prova, vamos apresentar mais exemplos.

Prova do Teorema 4: Considere $\alpha, \beta \in \mathbb{Z}[i]$, com $\beta \neq 0$. Queremos encontrar $\gamma, \delta \in \mathbb{Z}[i]$ tais que $\alpha = \beta\gamma + \delta$ e $N(\delta) \leq \frac{1}{2}N(\beta)$. Considerando que $\bar{\beta}$ é o conjugado de β. Temos que

$$\frac{\alpha}{\beta} = \frac{\alpha\bar{\beta}}{\beta\bar{\beta}} = \frac{\alpha\bar{\beta}}{N(\beta)} = \frac{m+ni}{N(\beta)} = \left(\frac{m}{N(\beta)}\right) + \left(\frac{n}{N(\beta)}\right) i. \tag{1.1}$$

Usando o teorema da divisão modificado em $\mathbb{Z}$, temos

$$m = N(\beta) \cdot q_1 + r_1 \text{ e } n = N(\beta) \cdot q_2 + r_2,$$

em que q_1 e q_2 estão em $\mathbb{Z}$ e $0 \leq |\ r_1\ |, |\ r_2\ | \leq \frac{1}{2}N(\beta)$. Substituindo m e n em (1.1), temos que

$$\begin{aligned} \frac{\alpha}{\beta} &= \frac{N(\beta)q_1 + r_1 + (N(\beta)q_2 + r_2)i}{N(\beta)} \\ &= q_1 + q_2 i + \frac{r_1 + r_2 i}{N(\beta)} \end{aligned}$$

donde

$$\alpha - \beta\gamma = \frac{r_1 + r_2 i}{\bar{\beta}}, \tag{1.2}$$

em que $\gamma = q_1 + q_2 i$. Considere $\delta = \alpha - \beta\gamma$.

Aplicando norma em ambos os lados de (1.2) e sabendo que $N(\beta) = N(\bar{\beta})$ obtemos

$$N(\alpha - \beta\gamma) = \frac{N(r_1 + r_2 i)}{N(\bar{\beta})} = \frac{r_1^2 + r_2^2}{N(\beta)}.$$

Sabemos que $0 \leq | r_1 |$ e $| r_2 | \leq \frac{1}{2}N(\beta)$, donde

$$N(\alpha - \beta\gamma) \leq \frac{(1/4)N(\beta)^2 + (1/4)N(\beta)^2}{N(\beta)} = \frac{1}{2}N(\beta).$$

■

Exemplo 7 *Considere* $\alpha = 11 + 10i$ *e* $\beta = 4 + i \Rightarrow N(\beta) = 4^2 + 1^2 = 17$. *Assim,*

$$\begin{aligned} \frac{\alpha}{\beta} &= \frac{\alpha\bar{\beta}}{N(\beta)} \\ &= \frac{(11 + 10i)(4 - i)}{17} \\ &= \frac{44 - 11i + 40i + 10}{17} \\ &= \frac{54 + 29i}{17}. \end{aligned}$$

Como $\frac{54}{17} = 3,1764\ldots$ *e* $\frac{29}{17} = 1,7058\ldots$, *temos* $\gamma = 3 + 2i$. *Então:*

$$\begin{aligned} \delta = \alpha - \beta\gamma &= (11 + 10i) - (4 + i)(3 + 2i) \\ &= (11 + 10i) - (12 + 8i + 3i - 2) \\ &= 1 - i. \end{aligned}$$

Por fim que $N(\delta) = 1^2 + (-1)^2 = 2 \leq \frac{1}{2}N(\beta)$. ⋄

Exemplo 8 *Considere* $\alpha = 41 + 24i$ *e* $\beta = 11 - 2i \Rightarrow N(\beta) = 11^2 + (-2)^2 = 125$.

Assim,

$$\begin{aligned}\frac{\alpha}{\beta} &= \frac{\alpha\bar{\beta}}{N(\beta)} \\ &= \frac{(41+24i)(11+2i)}{125} \\ &= \frac{451+82i+264i-48}{125} \\ &= \frac{403+346i}{125}.\end{aligned}$$

Como $\frac{403}{125} = 3,224\ldots$ *e* $\frac{346}{125} = 2,768\ldots$, *temos* $\gamma = 3+3i$. *Então:*

$$\begin{aligned}\delta = \alpha - \beta\gamma &= (41+24i) - (11-2i)(3+3i) \\ &= (41+24i) - (33+33i-6i+6) \\ &= 2-3i.\end{aligned}$$

Por fim que $N(\delta) = 2^2 + (-3)^2 = 13 \leq \frac{1}{2}N(\beta)$. $\diamond$

Há uma diferença interessante entre o teorema da divisão em $\mathbb{Z}[i]$ e o teorema da divisão em $\mathbb{Z}$, a saber, o quociente e o resto não são únicos em $\mathbb{Z}[i]$.

Exemplo 9 *Considere* $\alpha = 37+2i$ *e* $\beta = 11+2i \Rightarrow N(\beta) = 11^2+2^2 = 125$. *Calculamos:*

$$\begin{aligned}\frac{\alpha}{\beta} &= \frac{\alpha\bar{\beta}}{N(\beta)} \\ &= \frac{(37+2i)(11-2i)}{125} \\ &= \frac{407-74i+22i+4}{125} \\ &= \frac{411-52i}{125}.\end{aligned}$$

Como $\frac{411}{125} = 3,288\ldots$ *e* $-\frac{52}{125} = -0,416\ldots$, *temos:* $\gamma_1 = 3$, *considerando* $b = 0$ *e* $\gamma_2 = 3-i$, *considerando* $b = -1$. *Então para* $\gamma_1 = 3$, *temos*

$$\begin{aligned}\delta = \alpha - \beta\gamma &= (37+2i) - (11+2i)(3) \\ &= (37+2i) - 33 - 6i \\ &= 4-4i\end{aligned}$$

Note que $N(\delta) = 4^2 + (-4)^2 = 32 \leq \frac{1}{2}N(\beta)$.

Já para $\gamma_2 = 3 - i$. *temos*

$$\begin{aligned} \delta = \alpha - \beta\gamma &= (37 + 2i) - (11 + 2i)(3 - i) \\ &= (37 + 2i) - (33 + 6i - 11i + 2) \\ &= 2 + 7i \end{aligned}$$

Note que $N(\delta) = 2^2 + 7^2 = 53 \leq \frac{1}{2}N(\beta)$. *Concluimos que é verdade para* $\alpha = \beta \cdot 3 + (4 - 4i)$ *ou* $\alpha = \beta \cdot (3 - i) + (2 + 7i)$.$\diamond$

No exemplo anterior, o primeiro resultado não seria do nosso algoritmo da divisão em $\mathbb{Z}[i]$.

Vejamos abaixo um exemplo onde o algoritmo da divisão permite dois resultados diferentes.

Exemplo 10 *Considere* $\alpha = 1+8i$ *e* $\beta = 2-4i \Rightarrow N(\beta) = 2^2+(-4)^2 = 20$. *Assim,*

$$\begin{aligned} \frac{\alpha}{\beta} &= \frac{\alpha\bar{\beta}}{N(\beta)} \\ &= \frac{(1 + 8i)(2 + 4i)}{20} \\ &= \frac{2 + 4i + 16i - 32}{20} \\ &= \frac{-30 + 20i}{20} \\ &= \left(-\frac{3}{2}\right) + i. \end{aligned}$$

Como $-\frac{3}{2} = -1,5$ *podemos usar* $\gamma_1 = -2+i$ *ou* $\gamma_2 = -1+i$. *Então para* $\gamma_1 = -2+i$, *temos*

$$\begin{aligned} \delta = \alpha - \beta\gamma &= (1 + 8i) - (2 - 4i)(-2 + i) \\ &= (1 + 8i) - (-4 + 2i + 8i + 4) \\ &= 1 - 2i. \end{aligned}$$

Note que $N(\delta) = 1^2 + (-2)^2 = 5 \leq \frac{1}{2}N(\beta)$.

Já para $\gamma_2 = -1 + i$, *temos*

$$\begin{aligned} \delta = \alpha - \beta\gamma &= (1+8i) - (2-4i)(-1+i) \\ &= (1+8i) - (-2+2i+4i+4) \\ &= -1+2i. \end{aligned}$$

Note que $N(\delta) = (-1)^2 + 2^2 = 5 \leq \frac{1}{2}N(\beta)$. *Se escolhermos o* γ_1 *teremos* $\alpha = \beta \cdot (-2+i) + (1-2i)$, *e se escolhermos o* γ_2 *teremos* $\alpha = \beta \cdot (-1+i) + (-1+2i)$.$\diamond$

1.2.4 O Algoritmo de Euclides

Vamos definir o maior divisor comum em $\mathbb{Z}[i]$.

Definição 5 *Para* $\alpha \neq 0$ *e* $\beta \in \mathbb{Z}[i]$, *um maior divisor comum de* α *e* β *é divisor comum com norma máxima.*

Isto é análogo 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 $-\delta, i\delta$ e $-i\delta$. Talvez existam outros grandes divisores comuns, porém simplesmente não sabemos ainda. (Vamos descobrir no Corolário 4.7). Podemos falar de um máximo divisor comum, mas não é o maior divisor comum. A semelhante tecnicidade ocorreria em $\mathbb{Z}$ se definíssemos o maior divisor comum como um divisor comum com o maior valor absoluto, em vez de o maior divisor comum positivo.

Teorema 6 *(Algoritmo de Euclides). Tome* $\alpha, \beta \in \mathbb{Z}[i]$ *onde são diferente de zero. Aplicando repetidamente o teorema da divisão onde o resto é diferente de zero, teremos*

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

O último resto sendo 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.

Prova. A prova é análoga ao Algoritmo de Euclides em $\mathbb{Z}$. O raciocínio é a partir da primeira equação onde cada divisor comum de α e β divide pelo último resto (diferente de zero). Portanto, este último resto diferente de zero é um divisor comum, que é divisível por todos os outros. Por isso é um máximo divisor comum. ■

Definição 7 *Quando α e $\beta \in \mathbb{Z}[i]$ têm as unidades como máximo divisor comum, chamamos de relativamente primos, ou seja, primos entre si.*

Exemplo 11 *Calculamos um máximo divisor comum de $\alpha = 32+9i$ e $\beta = 4+11i$. Primeiro realizamos o teorema da divisão e, teremos $\gamma = 2-2i$ e $\delta = 2-5i$. Aplicamos o algoritmo de Euclides, encontramos*

$$\begin{aligned} 32+9i &= (4+11i)(2-2i)+(2-5i) \\ 4+11i &= (2-5i)(-2+i)+(3-i) \\ 2-5i &= (3-i)(1-i)-i \\ 3-i &= (-i)(1+3i)+0. \end{aligned}$$

O último resto diferente de zero é $(-i)$, então $mdc(32+9i, 4+11i) = -i$, são relativamente primos. ◇

Exemplo 12 *Mostrar que os conjugados $(4+5i)$ e $(4-5i)$, são relativamente primos em $\mathbb{Z}[i]$. Considere $\alpha = 4+5i$ e $\beta = 4-5i$, utilizando o teorema da divisão encontraremos $\gamma = i$ e $\delta = -(1-i)$, portanto temos que*

$$\begin{aligned} 4+5i &= (4-5i)i-(1-i) \\ 4-5i &= -(1-i)(-4)-i \\ -(1-i) &= -i(1+i)+0. \end{aligned}$$

O último resto diferente de zero é uma unidade, ou seja, $mdc(4+5i, 4-5i) = -i$, temos que $(4+5i)$ e $(4-5i)$ são relativamente primos.◇

Exemplo 13 *Vamos verificar o máximo divisor comum para $\alpha = 11+3i$ e $\beta = 1+8i$. Encontramos $\gamma = 1-i$ e $\delta = 2-4i$, então*

$$\begin{aligned} 11+3i &= (1+8i)(1-i)+(2-4i) \\ 1+8i &= (2-4i)(-1+i)+(-1+2i) \\ 2-4i &= (-1+2i)(-2)+0. \end{aligned}$$

O $mdc(11+3i, 1+8i) = -1+2i$. *Podemos encontrar uma forma diferente, e obter no último resto diferente de zero, assim*

$$\begin{aligned} 11+3i &= (1+8i)(1-i)+(2-4i) \\ 1+8i &= (2-4i)(-2+i)+(1-2i) \\ 2-4i &= (1-2i)2+0. \end{aligned}$$

Logo, $mdc(11+3i, 1+8i) = 1-2i$, *assim, sabemos que* $(1-2i) = (-1)(-1+2i)$. $\diamond$

Se ξ é o maior divisor comum de α e β, então $N(\xi) \mid N(\alpha)$ e $N(\xi) \mid N(\beta)$, de modo que $N(\xi) \mid (N(\alpha), N(\beta))$. No entanto, pode acontecer $N(\xi) < (N(\alpha), N(\beta))$. No exemplo anterior onde $\alpha = 4+5i$ e $\beta = 4-5i$ são primos entre si e, portanto, $N(\xi) = 1$, mas $N(\alpha) = N(\beta) = 41$. No exemplo onde $\alpha = 11+3i$ e $\beta = 1+8i \Rightarrow N(\alpha) = 11^2+3^2 = 130$ e $N(\beta) = 8^2+1^2 = 65$, tendo $mdc(130, 65) = 65$, e $mdc(\alpha, \beta) = -1+2i$, onde sua norma $N(-1+2i) = (-1)^2+2^2 = 5$.

Suponha $(N(\alpha), N(\beta)) = 1$. Então, qualquer divisor comum de α e β tem norma dividindo por 1, logo, sua norma deve ser 1 e, portanto, o divisor comum é uma unidade. Vimos que os inteiros Gaussianos com norma relativamente primos têm de ser primos entre si. A recíproca não é verdadeira, como mostra no exemplo $(4+5i)$ e $(4-5i)$.

Mas, em geral é necessário o algoritmo de Euclides em $\mathbb{Z}[i]$, a fim de calcular o maior divisor comum em $\mathbb{Z}[i]$.

Corolário 1.3 . *Para* $\alpha \neq 0$ *e* $\beta \in \mathbb{Z}[i]$, *vamos ter* δ *um máximo divisor comum produzido pelo Algoritmo de Euclides. Qualquer máximo divisor comum de* α *e* β *é um múltiplo unitário de* δ.

Prova. Vamos ter δ um máximo divisor comum de α e β. A partir da prova do algoritmo de Euclides, $\delta' \mid \delta$, considerando δ' é um divisor comum. Faça $\delta = \delta'\gamma$, assim temos que

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

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

1.2.5 O Teorema de Bézout

Dados inteiros a e b, não ambos nulos, exitem inteiros x e y tais que $ax + by = mdc(a, b)$. A mesma ideia funciona em $\mathbb{Z}[i]$.

Teorema 8 *(Teorema de Bézout). Seja α e β, ambos não nulos, então $mdc(\alpha, \beta) = \delta$. Então $\delta = \alpha x + \beta y$, para algum $x, y \in \mathbb{Z}[i]$.*

Prova. Considere o conjunto C sendo todas as combinações lineares de α e β e $n = \alpha x_0 + \beta y_0$, onde n é o menor elemento de C. Suponha, por absurdo, que $n \nmid \alpha$. Então $\alpha = nq + r$, com $0 < r < n$.

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

Então $r \in C$, pois $r > 0$ e $r < n$, onde n é o menor elemento de C, portanto, $n|\alpha$. Analogamente, $n|\beta$. Assim, n é o divisor comum de α e β. Vamos mostrar que $n = d$. De fato, pois se $d = mdc(\alpha, \beta)$, então

$$d \mid \alpha \Rightarrow \alpha = dq_1 \text{ e } d \mid \beta \Rightarrow \beta = dq_2.$$

Como $n = \alpha x_0 + \beta y_0 \Rightarrow n = d(q_1 x_0 + q_2 y_0) \Rightarrow d \mid n \Rightarrow d \leq n \Rightarrow d = n$. ■

Corolário 1.4 *Sendo α e β inteiros de Gauss, não ambos nulos, então são relativamente primos se, e somente se, podemos escrever*

$$1 = \alpha x + \beta y$$

para algum $x, y \in \mathbb{Z}[i]$.

Prova. ($\Rightarrow$): Se α e β são relativamente primos, então 1 é um máximo divisor comum de α e β. Portanto, podemos tomar $x, y \in \mathbb{Z}[i]$ tais que $1 = \alpha x + \beta y$ pelo teorema de Bézout.
($\Leftarrow$): Se $1 = \alpha x + \beta y$ para alguns $x, y \in \mathbb{Z}[i]$, então qualquer divisor comum de α e β é um divisor de 1, e portanto, é um múltiplo unitário, logo, temos que α e β são relativamente primos . ■

No **Exemplo 11** temos que $\alpha = 32 + 9i$ e $\beta = 4 + 11i$, que são relativamente primos, uma vez que o último resto diferente de zero é $(-i)$. Podemos inverter os

cálculos para expressar $(-i)$ como uma combinação de α e $\beta \in \mathbb{Z}[i]$.

Sabemos que: $\begin{cases} (2-5i) &= \alpha - \beta(2-2i) \\ (3-i) &= \beta - (2-5i)(-2+i) \end{cases}$ Temos que

$$\begin{aligned} -i &= (2-5i) - (3-i)(1-i) \\ &= (2-5i) - (\beta - (2-5i)(-2+i))(1-i) \\ &= (2-5i)(1+(-2+i)(1-i)) - \beta(1-i) \\ &= (2-5i)(3i) - \beta(1-i) \\ &= (\alpha - \beta(2-2i))(3i) - \alpha(1-i) \\ &= \alpha(3i) - \beta(7+5i) \end{aligned}$$

Multiplicando por (i) ambos os lados:

$$i \cdot (-i) = \alpha(3i) \cdot i - \beta(7+5i) \cdot i$$

$$1 = \alpha(-3) + \beta(5-7i).$$

Exemplo 14 *Verificamos que para $\alpha = 4+5i$ e $\beta = 4-5i$, são relativamente primos. Usando da substituição de volta, temos que*

$$\begin{aligned} -i &= (4-5i) - (-(1-i)) \cdot (-4) \\ &= (4-5i) - (4+5i-(4-5i)i) \cdot (-4) \\ &= (4+5i)(4) + (4-5i)(1-4i) \end{aligned}$$

e multiplicando i temos que:

$$\begin{aligned} i \cdot (-i) &= (4+5i) \cdot (4)i + (4-5i) \cdot (1-4i)i \\ 1 &= (4+5i)(4i) + (4-5i)(4+i). \diamond \end{aligned}$$

Vimos no **Exemplo 13** que $(-1+2i)$ é um máximo divisor comum de $\alpha = 11+3i$ e $\beta = 1+8i$. Podemos escrever como combinação linear de α e β, temos que

$$\begin{aligned} -1+2i &= 1+8i - (2-4i)(-1+i) \\ &= 1+8i - (11+3i-(1+8i)(1-i))(-1+i) \\ &= (11+3i)(1-i) + (1+8i)(1+(1-i)(-1+i)) \\ &= (11+3i)(1-i) + (1+8i)(1+2i) \\ &= \alpha(1-i) + \beta(1+2i). \end{aligned}$$

Exemplo 15 *Seja* $\alpha = 10 + 91i$ *e* $\beta = 7 + 3i$. *Pelo algoritmo de Euclides, temos*

$$\begin{aligned} \alpha &= \beta(6 + 11i) + 1 - 4i, \\ \beta &= (1 - 4i)(2i) - 1 + i, \\ 1 - 4i &= (-1 + i)(-3 + i) - 1, \\ -1 + i &= -1(1 - i) + 0. \end{aligned}$$

Temos que o último resto diferente de zero é (-1). *Logo* α *e* β *são relativamente primos. Temos uma combinação linear de* α *e* β

$$\begin{aligned} -1 &= (1 - 4i) - (-1 + i)(-3 + i) \\ &= (1 - 4i) - [\beta - (1 - 4i)(2i)](-3 + i) \\ &= (1 - 4i)[1 + (2i)(-3 + i)] - \beta(-3 + i) \\ &= (1 - 4i)(-1 - 6i) + \beta(3 - i) \\ &= [\alpha - \beta(6 + 11i)](-1 - 6i) + \beta(3 - i) \\ &= \alpha(-1 - 6i) + \beta(-(6 + 11i)(-1 - 6i) + 3 - i) \\ &= \alpha(-1 - 6i) + \beta(-57 + 46i). \end{aligned}$$

Podemos escrever (-1) *como uma combinação de* α *e* β *em* $\mathbb{Z}[i]$, *multiplicando ambos os lados por* (-1), *teremos*

$$1 = \alpha(1 + 6i) + \beta(57 - 46i). \diamond$$

O exemplo acima mostra que $(10 + 91i)$ e $(7 + 3i)$ são relativamente primos em $\mathbb{Z}[i]$. Observe que suas normas $N(10+91i) = 10^2+91^2 = 8381 = 172 \cdot 29$ e $N(7+3i) = 7^2 + 3^2 = 58 = 2 \cdot 29$, têm um fator comum em $\mathbb{Z}$. Podemos perceber que os inteiros Gaussianos que são relativamente primos não têm normas relativamente primas em $\mathbb{Z}$, vamos efetuar a "fatoração de primo" $(10 + 91i)$ e $(7 + 3i)$:

$$(10 + 91i) = (1 - 4i) \cdot (4 + i) \cdot (5 + 2i) \text{ e } (7 + 3i) = (1 + i) \cdot (5 - 2i).$$

Agora podemos enterder porque isso é possível: os fatores $(5 + 2i)$ e $(5 - 2i)$ têm a mesma norma, mas eles são relativamente primos. Todas as conseqüências habituais do teorema de Bézout sobre $\mathbb{Z}$ são análogas em $\mathbb{Z}[i]$.

Corolário 1.5 *Suponha que* $\alpha \mid \beta\gamma$ *em* $\mathbb{Z}[i]$, *com* α *e* β *relativamente primos. Então* $\alpha \mid \gamma$.

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

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

Portanto, $\alpha \mid \gamma$. ■

Corolário 1.6 *Se $\alpha \mid \gamma$ e $\beta \mid \gamma$ em $\mathbb{Z}[i]$, com α e β relativamente primos, então $\alpha\beta \mid \gamma$.*

Prova. Sabemos que $mdc(\alpha, \beta) = 1 \Rightarrow \alpha x + \beta y = 1$, para $x, y \in \mathbb{Z}[i]$. Multiplicando γ em ambos os lados, teremos:

$$\gamma\alpha x + \gamma\beta y = \gamma.$$

E sabemos que: $\begin{cases} \alpha \mid \gamma \Rightarrow \gamma = \alpha w \text{ para } w \in \mathbb{Z}[i] \\ \beta \mid \gamma \Rightarrow \gamma = \beta k, \text{ para } k \in \mathbb{Z}[i]. \end{cases}$

$$\begin{aligned} \gamma &= \beta k\alpha x + \alpha w\beta y \\ &= (\alpha\beta)(kx) + (\alpha\beta)yw \\ &= (\alpha\beta)(kx + yw). \end{aligned}$$

Portanto, $\alpha\beta \mid \gamma$. ■

Corolário 1.7 *Para α, β, γ em $\mathbb{Z}[i]$, não nulos, α e β são relativamente primos para γ se, e somente se, $\alpha\beta$ é relativamente primo para γ.*

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

Temos $\begin{cases} \alpha x + \gamma y = 1 \\ \beta z + \gamma w = 1 \end{cases} \Rightarrow \begin{cases} \alpha x + \gamma y = 1 \cdot \beta \\ \beta z + \gamma w = 1 \end{cases} \Rightarrow \begin{cases} \alpha\beta x + \gamma\beta y = \beta \\ \beta z + \gamma w = 1 \end{cases}$

Substituindo β em $\beta z + \gamma w = 1$, teremos: $z(\alpha\beta x + \gamma\beta y) + \gamma w = 1$, então $(\alpha\beta)(zx) + \gamma(\beta yz) + \gamma w = 1 \Rightarrow (\alpha\beta)(zx) + \gamma(\beta yz + w) = 1$. Considere $r = zx$ e $s = (\beta yz + w)$, então, $\alpha\beta r + \gamma s = 1 \Rightarrow mdc(\alpha\beta, \gamma) = 1$.
($\Leftarrow$): Sabemos que $mdc(\alpha\beta, \gamma) = 1 \Rightarrow \alpha\beta r + \gamma s = 1$. Considere $x = \beta r$ e $y = s$, então, $\alpha x + \gamma y = 1 \Rightarrow mdc(\alpha, \gamma) = 1$ e considere $z = \alpha r$ e $w = s$, então, $\beta z + \gamma w = 1 \Rightarrow mdc(\beta, \gamma) = 1$. ■

1.2.6 Fatoração Única

Vamos definir os inteiros de Gauss compostos, e em seguida, provar fatoração única. Sabemos que pela Proposição 2, se $\beta \mid \alpha$, então $N(\beta) \mid N(\alpha)$. Dessa forma, $1 \leq N(\beta) \leq N(\alpha)$, para $\alpha \neq 0$.

Lema 1.3 *Se $\beta \mid \alpha$ e $N(\beta) = 1$ ou $N(\beta) = N(\alpha)$, então ou β é uma unidade ou é um múltiplo unitário de α .*

Prova. Se $\beta \mid \alpha$ e $N(\beta) = 1$, então $\beta = \pm 1$ ou $\beta = \pm i$. Se $\beta \mid \alpha$ e $N(\beta) = N(\alpha)$, temos que $\alpha = \beta\delta$. Aplicando a norma em ambos os lados, temos que $N(\alpha) = N(\beta)N(\delta)$ e sabemos que $N(\beta) = N(\alpha)$, portanto, $N(\delta) = 1$, então $\delta = \pm 1$ ou $\delta = \pm i$. Logo, $\beta = \pm\alpha$ ou $\beta = \pm i\alpha$. ∎

Quando $N(\alpha) > 1$, há sempre oito divisores de α : $\pm 1, \pm i, \pm\alpha$ e $\pm i\alpha$, esses fatores chamamos de triviais de α. Eles são análogos aos quatro fatores triviais ± 1 e $\pm n$ para qualquer $n \in \mathbb{Z}$, com $\mid n \mid > 1$. Qualquer outro fator de α é chamado de não trivial. Pelo Lema 10.1, os fatores não triviais de α são os fatores com norma estritamente entre 1 e $N(\alpha)$.

Definição 9 *Seja $\alpha \in \mathbb{Z}[i]$ com $N(\alpha) > 1$. Então, se existir um fator não trivial de α, então, é chamado de composto e se α só tem fatores triviais, então α é primo.*

Tome $\alpha = \beta\gamma$, com à condição de $1 < N(\beta) < N(\alpha) \Rightarrow N(\beta) > 1$ e $N(\gamma) > 1$. Para qualquer fatoração de α, em um produto de inteiros de Gauss com norma superior a 1, chamamos de fatoração não-trivial. Assim, um número inteiro de Gauss composto é aquele que admite uma fatoração não- trivial. Por exemplo, uma fatoração trivial de $(7+i)$ é $(1-7i)i$. Uma fatoração trivial de $(7+i)$ é $(1-2i)(1+3i)$. Uma fatoração não-trivial de 5 é $(1 + 2i)(1 - 2i)$. O interessante é que o número 5 é primo em $\mathbb{Z}$, mas é composto em $\mathbb{Z}[i]$. O mesmo acontece com o número inteiro 2 que é composto em $\mathbb{Z}[i]$ podendo ser escrito na forma $(1 + i)(1 - i)$. No entanto, o número 3 é primo em $\mathbb{Z}[i]$, por isso alguns números primos em $\mathbb{Z}$ também são primos em $\mathbb{Z}[i]$.

Para mostrar que 3 é primo em $\mathbb{Z}[i]$, vamos argumentar por contradição. Considere que 3 é composto, então existe uma fatoração não trivial, logo $3 = \alpha\beta$. Aplicando a norma de ambos os lados, teremos: $9 = N(\alpha)N(\beta)$. Essa fatoração não é trivial, então $N(\alpha) > 1$ e $N(\beta) > 1$. Portanto $N(\alpha) = 3$. Tome $\alpha = a+bi \Rightarrow N(\alpha) = a^2+b^2 = 3$. Não existem números inteiros a e b que satisfaçam a equação, de modo temos uma contradição. Assim, 3 tem apenas fatoração trivial em $\mathbb{Z}[i]$, então 3 é primo em $\mathbb{Z}[i]$. Vamos ver mais adiante que para qualquer $p \in \mathbb{Z}^+$ se tivermos $p \equiv 3 \pmod 4$, então p também será primo em $\mathbb{Z}[i]$.

A melhor maneira para identificar os primos de Gauss é através de comparação com os números primos em $\mathbb{Z}$. Outro modo de encontrar primos em $\mathbb{Z}[i]$ é utilizando a norma, a partir dos números primos em $\mathbb{Z}$. Não é preciso utilizar a fatoração única em $\mathbb{Z}[i]$ para identificar primos Gaussianos.

Teorema 10 *Se a norma de um inteiro de Gauss é primo em* $\mathbb{Z}$*, então o inteiro Gaussiano é primo em* $\mathbb{Z}[i]$.

Prova. Tome $\alpha \in \mathbb{Z}[i]$ e p primo em $\mathbb{Z}^+$, com $N(\alpha) = p$. Vamos mostrar que α só tem fatores triviais (isto é, seus fatores têm norma 1 ou $N(\alpha)$), então α é primo em $\mathbb{Z}[i]$. Considere qualquer fatoração de $\alpha \in \mathbb{Z}[i]$, então $\alpha = \beta\delta$. Aplicando a norma, temos que $p = N(\beta)N(\delta)$, onde é uma equação em números inteiros positivos, e p é primo em $\mathbb{Z}^+$, por isso, $N(\beta) = 1$ ou $N(\delta) = 1$. Portanto, β ou δ é uma unidade, de modo que α não admite fatores não triviais. Assim, α é primo. ■

A recíproca do Teorema 10 é falsa, pois existem primos Gaussianos cuja a norma não é um primo em $\mathbb{Z}$. Por exemplo, o número 3 tem norma 9, mas sabemos que 3 é primo em $\mathbb{Z}[i]$.

Iremos dar mais ênfase sobre primos Gaussianos no próximo capítulo. Já sabemos o suficiente sobre números primos de Gauss, para voltar a nossa atenção para fatoração única. A existência de uma fatoração será provada por um argumento similar à prova de fatoração em $\mathbb{Z}$. Primeiro vamos estabelecer a existência de uma fatoração, depois vamos tratar a sua unicidade.

Teorema 11 *Seja* $\alpha \in \mathbb{Z}[i]$*, com* $N(\alpha) > 1$*. Então* α *pode ser escrito como um produto de números primos em* $\mathbb{Z}[i]$.

Prova. Por indução em $N(\alpha)$. Suponha que $N(\alpha) = 2$. Isso significa que $\alpha = \pm 1 \pm i$, portanto, α é primo pelo Teorema 10.
Agora vamos supor $n \geq 3$ e $1 < N(\alpha) \leq n$, onde n é um produto de números primos em $\mathbb{Z}[i]$. Queremos mostrar que todo inteiro Gaussiano com a norma n é um produto de números primos em $\mathbb{Z}[i]$. Se não houver inteiros de Gauss com norma n, então não há nada a provar. Assim, podemos supor que há inteiros de Gauss com norma n. Se temos um número inteiro de Gauss α com a norma n, que é composto, então podemos escrever $\alpha = \beta\gamma$, onde $N(\beta), N(\gamma) < N(\alpha) = n$. Por hipótese indutiva, β e γ são produtos de primos em $\mathbb{Z}[i]$. Portanto, α também é um produto de primos em $\mathbb{Z}[i]$. ■

Tendo estabelecido a existência de fatoração de primos em $\mathbb{Z}[i]$, vejamos agora a unicidade.

Lema 1.4 *Sejam* π *um primo em* $\mathbb{Z}[i]$ *e* $\alpha_1, \alpha_2, \ldots, \alpha_r \in \mathbb{Z}[i]$ *se* $\pi \mid \alpha_1\alpha_2 \ldots \alpha_r$*, então* π *divide algum* α_j.

Prova. Vamos usar indução sobre π. Se $r = 2$, então, seja $\pi \mid \alpha_1\alpha_2$. Suponha que $\pi \nmid \alpha_1$. Isto implica π e α_1 são relativamente primos. De fato, $mdc(\pi, \alpha_1)$ é um

múltiplo unitário de π, pois π é primo e tem divisores triviais. Isto implicaria $\pi \mid \alpha_1$, o que não é o caso. Agora que sabemos que π e α_1 são relativamente primos, então $\pi \mid \alpha_2$. ■

Podemos escrever $5 = (1+2i)(1-2i) = (2-i)(2+i)$. Os fatores são todos primos em $\mathbb{Z}[i]$, pois a norma deles é um número primo em $\mathbb{Z}$. Podemos fazer um jogo entre as duas fatorações, através dos múltiplos unitários, por exemplo: $(1+2i) = (2-i)i$ e $(1-2i) = (2+i)(-i)$. Na verdade, isso também pode acontecer em $\mathbb{Z}$, por exemplo: $6 = 2 \cdot 3 = (-2) \cdot (-3)$.

Este é um exemplo de fatoração não exclusiva de $\mathbb{Z}$, uma vez que podemos combinar outros fatores. Questões de sinal são evitadas em $\mathbb{Z}$, concentrando a atenção em números inteiros positivos e apenas primos positivos. Aceitamos a ambiguidade dos múltiplos unitários em nossa fatoração de primos. Isso explica a importância das unidades na fatoração única para $\mathbb{Z}[i]$.

Teorema 12 *(Fatoração Única). Qualquer $\alpha \in \mathbb{Z}[i]$, com $N(\alpha) > 1$, tem uma fatoração única em primos no seguinte sentido: se*

$$\alpha = \pi_1\pi_2 \cdots \pi_r = \pi_1'\pi_2' \cdots \pi_s',$$

em que $\pi_i's$ e $\pi_j's$ são primos em $\mathbb{Z}[i]$, então $r = s$ e depois de uma adequada organização para cada π_i é um múltiplo unitário de π_i'.

Prova. No Teorema 11 mostra cada $\alpha \in \mathbb{Z}[i]$, com $N(\alpha) > 1$, tem uma fatoração. Quando α é primo, sua fatoração é obviamente única. Agora vamos mostrar a unicidade, em geral, por indução em $N(\alpha)$. Tome $N(\alpha) = 2$, já foi estabelecido $\alpha = \pm 1 \pm i$. Agora suponha que $n \geq 3$ e $1 < N(\alpha) < n$ com α tendo uma fatoração única. Podemos supor que há inteiros de Gauss com a norma n (caso contrário, não há nada a verificar), e só temos de concentrar a atenção sobre α composto com a norma n. Considere duas fatorações de primos de α como na demonstração do teorema. Seja $\pi_1 \mid \alpha$, podemos escrever:

$$\pi_1 \mid \pi_1'\pi_2' \cdots \pi_s'.$$

Pelo Lema 1.3, $\pi_1 \mid \pi_j'$, para algum j. Podemos supor que $j = 1$, ou seja, $\pi_1 \mid \pi_1'$. Os únicos fatores não unitários de π_1' são múltiplos unitários de π_1', então $\pi_1 = u\pi_1'$ para alguma unidade $u \in \{\pm 1, \pm i\}$. Observando as duas fatorações de α :

$$\alpha = u\pi_1'\pi_2 \cdots \pi_r = \pi_1'\pi_2' \cdots \pi_s',$$

Cancelando π_1' em ambos os lados, temos:

$$u\pi_2 \cdots \pi_r = \pi_2' \cdots \pi_s', \tag{1.3}$$

sendo $\beta = \pi_2' \cdots \pi_s'$, então $N(\beta) = N(\alpha)/N(\pi_1') < N(\alpha)$.
Embora u é uma unidade, e $u\pi_2$ é um produto sobre o lado esquerdo de (1.2), ele é realmente um primo, de modo (1.2) têm duas fatorações de primos de β, com $(r-1)$ primos do lado esquerdo e $(s-1)$ primos do lado direito. 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 $u\pi_2$ e π_2' são múltiplos unitários π_i, π_i' são múltiplos unitários para $i > 2$. Seja $u\pi_2$ e π_2' são múltiplos unitários,π_2 e π_2' são múltiplos unitários, de modo que vemos todos os π_i é um múltiplo unitário de π_i' e a prova está completa. ■

Exemplo 16 *Vamos ilustrar a fatoração única de* $(3+4i)$. *Sabemos que* $N(3+4i) = 25 = 5 \cdot 5$. *Sabemos que* $(3+4i)$ *têm um fator não trivial onde a norma é 5, como* $5 = (1+2i)(1-2i)$, *então vamos considerar* $\alpha = 1+2i$ *e* $\beta = 1-2i$. *Assim, temos as seguintes possibilidades:*

(a) $\alpha \cdot \alpha = (1+2i)(1+2i) = -3+4i$

(b) $\alpha \cdot \beta = (1+2i)(1-2i) = 5$

(c) $\beta \cdot \beta = (1-2i)(1-2i) = -3-4i$.

Analizando (c), multiplicamos por (-1) *temos que:*

$$3+4i = -(1-2i)(1-2i) = -(1-2i)^2.$$

A fatoração de $(3+4i)$ *é* $-(1-2i)^2$. ◇

Vamos encontrar a fatoração de $(2319 + 1694i)$? Sua norma é 8247397, cuja fatoração em $\mathbb{Z}$ é $8247397 = 17 \cdot 29 \cdot 16729$.

Vamos observar os inteiros de Gauss com a norma $17, 29$ e 16729 e, em seguida, tentar multiplicá-las em conjunto para obter $(2.319 + 1694i)$. Vamos representar os números $17, 29$ e 16.729 na soma de dois quadrados:
$17 = 1^2 + 4^2$
$29 = 2^2 + 5^2$
$16729 = 40^2 + 123^2$.

Assim podemos fatorar em primos gaussianos:
$17 = (1+4i)(1-4i)$

$29 = (2 + 5i)(2 - 5i)$
$16729 = (40 + 123i)(40 - 123i)$.

Os inteiros de Gauss são primos pois suas normas são primos em $\mathbb{Z}$. Vamos escolher um fator de cada produto e multiplicá-los juntos. Temos 8 combinações possíveis, mas escolhemos a seguinte:

$$(1 + 4i)(2 + 5i)(40 + 123i) = -2319 - 1694i.$$

Portanto, uma fatoração de $(2319 + 1694i)$ é $-(1 + 4i)(2 + 5i)(40 + 123i)$.

Capítulo 2

Números Primos Gaussianos

No Capítulo anterior já definimos os primos Gaussianos, veja definição 9. Neste Capítulo, vamos estudar mais detalhadamente os primos em $\mathbb{Z}[i]$, suas propriedades, teoremas, curiosidades e exemplos. Os professores de matemática poderão trabalhar em sala de aula nas turmas finais do ensino médio. As referências utilizadas para elaboração deste capítulo foram BUTLER [2] , CONRAD [3], FOSSA [5] e WALL [9].

Os primos de Gauss possuem 8 divisores. Sendo $\gamma \in \mathbb{Z}[i]$ dizemos que γ será primo de Gauss se, e somente se, os únicos inteiros de Gauss que dividem γ são:

$$1,\ -1,\ i,\ -i,\ \gamma,\ -\gamma,\ \gamma i \text{ e } -\gamma i.$$

Com 8 divisores parecem bastante inicialmente, pois, os primos em $\mathbb{Z}$ têm o menor número possível de divisores. Pórem, os primos Gaussianos têm nada menos que oito fatores, e apesar de parecer um absurdo, isso está correto, pois além das quatro unidades, cada inteiro de Gauss tem mais quatro divisores, justamente os múltiplos unitários de γ.

Exemplo 17 *Considere* $\alpha = (1+2i)$, *onde* $N(\alpha) = 5$, *então* α *é primo. Vamos identificar todos os divisores de* α :

- $(1+2i) = 1 \cdot (1+2i)$
- $(1+2i) = (-1) \cdot (-1-2i)$
- $(1+2i) = i \cdot (2-i)$
- $(1+2i) = (-i) \cdot (-2+i)$

- $(1+2i) = (1+2i) \cdot 1$
- $(1+2i) = (-1-2i) \cdot (-1)$
- $(1+2i) = (1+2i)i \cdot (-i)$
- $(1+2i) = (-1-2i)i \cdot i \diamond$

Agora que identificamos os requisitos para os primos Gaussianos, vamos responder as seguintes perguntas:

1 - Todos os números primos de $\mathbb{Z}$ também serão primos em $\mathbb{Z}[i]$?

A resposta é: não.

O exemplo mais fácil é o menor primo em $\mathbb{Z}$, o número 2 que tem os seguintes fatores: $(1+i)(1-i)$, e por isso não é primo.

2 - Será que todos os números inteiros Gaussianos podem ser escritos de maneira única, a menos da unidade, como produto de primos de Gauss?

A resposta é: não.

Por exemplo, o número 2 pode ser escrito como produto dos seguintes fatores:

$$\begin{cases} 2 &= (1+i)(1-i) \\ 2 &= (-1+i)(-1-i) \end{cases}$$

Mas temos que ter a certeza que os fatores acima são primos. Sabemos que se $N(\alpha)$ é primo em $\mathbb{Z}$, então α é primo Gaussiano. Logo, $N(1+i) = N(1-i) = N(-1+i) = N(-1-i) = 2 \Rightarrow (1+i),\ (1-i),\ (-1+i)$ e $(-1-i)$ são primos em $\mathbb{Z}[i]$, logo, não existem divisores únicos.

Vamos observar a fatoração de um primo inteiro ímpar, o número 3, pois é possível verificar todas as combinações dos produtos entre números Gaussianos que o resultado seja 3.

Pelo Lema 1.1 sabemos que, se α e β são dois fatores não unitários de 3, então:

$$N(\alpha)N(\beta) = N(\alpha\beta) = N(3).$$

Tome $\alpha = a + bi$ e $\beta = c + di$, teremos:

$$(a^2 + b^2)(c^2 + d^2) = 9.$$

Sabemos que os fatores não são unidades, então,

$$(a^2 + b^2) \neq 1 \text{ e } (c^2 + d^2) \neq 1.$$

Como $9 = 3^2 \Rightarrow a^2 + b^2 = 3$ e $c^2 + d^2 = 3$.

Fazendo uma reflexão iremos perceber que não têm soluções inteiras, ou seja, 3 não tem fatores inteiros de Gauss, exceto para as unidades e os múltiplos unitários de si mesmo. Então 3 é primo de Gauss. O que acontece para que 3 seja primo de Gauss e 2 não seja? Vamos fazer a mesma abordagem para o número 2. Obtemos as duas equações abaixo:

$$a^2 + b^2 = 2 \text{ e } c^2 + d^2 = 2.$$

Essas equações têm soluções, ou seja, pode ser qualquer uma dessas combinações para $(a, b) = (\pm 1, \pm 1)$ e $(c, d) = (\pm 1, \pm 1)$, assim, garantimos que$(a+bi)\cdot(c+di) = 2$. Assim se quisermos fatorar um número inteiro n em inteiros de Gauss então primeiro vamos fatorar sua norma, $N(n) = XY$, com $X \neq 1$ e $Y \neq 1$. Podemos sempre fazer isso desde que $N(n) = n^2$, por isso, vai ter pelo menos dois (não necessariamente distintos) fatores não unitários. Então, vamos resolver as equações:

$$a^2 + b^2 = X \text{ e } c^2 + d^2 = Y.$$

Esse raciocínio é válido para qualquer inteiros de Gauss. Primeiro aplicamos a norma do número e transformamos em um produtos, por exemplo, $N(\gamma) = UV$, então podemos resolver as equações:

$$a^2 + b^2 = U \text{ e } c^2 + d^2 = V.$$

Exemplo 18 $N(57 - 11i) = 57^2 + 11^2 = 3370 = 10 \cdot 337$, *temos que:*

$$a^2 + b^2 = 10 \text{ e } c^2 + d^2 = 337.$$

Existem várias soluções, entre elas $(a, b) = (3, 1)$ *e* $(c, d) = (16, -9)$ *e, consequentemente,* $(57 - 11i) = (3 + i) \cdot (16 - 9i)$. $\diamond$

Esta abordagem mostrou que se a norma de um inteiro Gaussiano é um número primo, então o tal inteiro Gaussiano é primo. Isto é simplesmente porque se $N(\gamma) = p = 1 \cdot p$, para p primo, então sempre teremos uma unidade como fator.

Lema 2.1 *Seja* π *um primo em* $\mathbb{Z}[i]$. *Para algum primo* p *em* $\mathbb{Z}^+, \pi \mid p$.

Prova. Note que π divide sua norma: $N(\pi) = \pi\bar{\pi}$, então $\pi \mid N(\pi)$ em $\mathbb{Z}[i]$. Com $N(\pi) > 1$, escrevemos $N(\pi)$ como um produto de primos em $\mathbb{Z}^+$:

$$N(\pi) = p_1 p_2 \cdots p_r.$$

Como $\pi \mid N(\pi)$, em $\mathbb{Z}[i]$, e π é primo em $\mathbb{Z}[i]$, devemos ter $\pi \mid p_j$ para algum j pelo Lema 1.3. ■

O Lema anterior nos diz que os fatores primos em $\mathbb{Z}[i]$ dos números primos inteiros positivos vai mostrar todos os números primos gaussianos. Fatorando os primos Gaussianos dos três primeiros números primos:

$$\begin{cases} 2 &= (1+i)(1-i) \\ 3 &= 3 \\ 5 &= (1+2i)(1-2i) \end{cases}$$

Utilizando a fatoração única, os múltiplos unitários de $(1+2i)$ e $(1-2i)$ teremos os seguintes números primos gaussianos:

$$\begin{cases} (1+2i)\cdot 1 &= (1+2i) \\ (1+2i)\cdot(-1) &= (-1-2i) \\ (1+2i)\cdot(i) &= (-2+i) \\ (1+2i)\cdot(-i) &= (2-i) \end{cases} \quad \begin{cases} (1-2i)\cdot 1 &= (1-2i) \\ (1-2i)\cdot(-1) &= (-1+2i) \\ (1-2i)\cdot(i) &= (2+i) \\ (1-2i)\cdot(-i) &= (-2-i) \end{cases}$$

Esses oito números são realmente os múltiplos unitários de $(1+2i)$ e $(1-2i)$.

Teorema 13 *Um primo p em $\mathbb{Z}^+$ é composto em $\mathbb{Z}[i]$ se, e somente se, é uma soma de dois quadrados.*

Prova. ($\Rightarrow$): Se p é primo em $\mathbb{Z}^+$ e composto em $\mathbb{Z}[i]$, então existe uma fatoração não trivial, tome $p = \alpha\beta$. Em seguida, aplicando a norma em ambos os lados, teremos $p^2 = N(\alpha)N(\beta)$. Como a fatoração de p não trivial, e $p > 0$, temos que $N(\alpha) = p$. Considere $\alpha = a + bi \Rightarrow p = a^2 + b^2$.
($\Leftarrow$): Suponha que p é primo em $\mathbb{Z}^+$ e é uma soma de dois quadrados. Então temos que $p = a^2 + b^2$. Logo, em $\mathbb{Z}[i]$, temos a fatoração não trivial, $p = (a+bi)(a-bi)$, então p é composto em $\mathbb{Z}[i]$. ■

Os cinco primeiros números primos em $\mathbb{Z}^+$, que têm a somas de dois quadrados são:

$$\begin{cases} 2 &= 1^2 + 1^2 \\ 5 &= 1^2 + 2^2 \\ 13 &= 2^2 + 3^2 \\ 17 &= 1^2 + 4^2 \\ 29 &= 2^2 + 5^2 \end{cases}$$

Portanto, cada um desses números primos é composto em $\mathbb{Z}[i]$, ou seja, $29 = (2+5i)(2-5i)$. Este é uma fatoração de primo de Gauss, uma vez que os fatores têm norma primo (e, portanto, são primos em $\mathbb{Z}[i]$). Já fatoração de 2 é especial, pois seus fatores primos são múltiplos unitários entre si, onde $(1-i) = (-i)(1+i)$. Em outras palavras,

$$2 = (-i)(1+i)^2.$$

Corolário 2.1 *Se p é primo em $\mathbb{Z}^+$ e composto em $\mathbb{Z}[i]$, sendo $p \neq 2$, então os múltiplos unitários de p tem exatamente dois fatores primos de Gauss que são conjugados e possuem norma p.*

Prova. Pelo Teorema 13, quando p é composto temos que:

$$p = a^2 + b^2 = (a+bi) \cdot (a-bi)$$

em alguns $a, b \in \mathbb{Z}$. Considere $(a+bi)$ e $(a-bi)$ com norma p primo, sendo primos em $\mathbb{Z}[i]$. Vamos analisar como sendo os múltiplos unitários e chegaremos a seguinte conclusão:

(a) Se $a+bi = (a-bi) \cdot 1$, então $b = 0$ e $p = a^2$, o que é uma contradição.

(b) Se $a+bi = (a-bi) \cdot (-1) = -(a-bi)$, então $a = 0$, temos uma contradição novamente.

(c) Se $a+bi = (a-bi) \cdot i = b+ai$, então $b = a$ e $p = a^2 + a^2 = 2a^2$, contradição.

(d) Se $a+bi = (a-bi) \cdot (-i) = -b-ai$, mais uma vez implica contradição $p = 2a^2$.

Logo, terá dois fatores primos Gaussianos. ∎

Corolário 2.2 *Se p é primo em $\mathbb{Z}^+$ e satisfaz $p \equiv 3$ (mod 4), então p não é uma soma de dois quadrados ($p \neq a^2 + b^2$) em $\mathbb{Z}$ e logo p será primo em $\mathbb{Z}[i]$.*

Prova. Sabemos que $p^2 \equiv 0$ ou $1 \pmod 4$, então teremos para:

$$\begin{cases} a^2 + b^2 \equiv 0 \pmod 4, \text{ para } (a,b) = (0,0) \\ a^2 + b^2 \equiv 2 \pmod 4, \text{ para } (a,b) = (1,1) \\ a^2 + b^2 \equiv 1 \pmod 4, \text{ para } (a,b) = (0,1) \text{ ou } (a,b) = (1,0) \end{cases}$$

Portanto, $p \neq a^2 + b^2$, para $p \equiv 3 \pmod 4$. ∎

Quando p primo em $\mathbb{Z}^+$ e satisfaz $p \equiv 1 \pmod 4$, podemos escrever esses primos como a soma de dois quadrados, de modo que são compostos em $\mathbb{Z}[i]$ pelo Teorema 16.

Teorema 14 *Seja p primo em $\mathbb{Z}^+$. As seguintes condições são equivalentes:*

(1) $p = 2$ ou $p \equiv 1$ (mod 4),

(2) A congruência $x^2 \equiv -1$ (mod p) tem uma solução.

(3) $p = a^2 + b^2$, por algum $a, b \in \mathbb{Z}$.

Prova. Mostraremos inicialmente que (3) implica (1): se $p = a^2+b^2$, por algum $a, b \in \mathbb{Z}$. Como $x^2 \equiv 0$ ou 1 (mod 4), para qualquer x inteiro, temos que $a^2 + b^2 \equiv 0$ ou 1 ou 2 (mod 4). Para $a^2 + b^2 \equiv 0$ (mod 4) é impossível já que p é primo. Para $a^2 + b^2 \equiv 2$ (mod 4) só acontece para $p = 2$, pois p será par. Portanto, caso $p \neq 2$, só nos resta $a^2+b^2 \equiv 1$ (mod 4) o que demonstra que (3) $\Rightarrow$ (1). Para mostrar (1) implica (2), podemos tomar $p \neq 2$. Considere a fatoração

$$T^{(p-1)} - 1 \quad = \quad (T^{(p-1)/2)} - 1)(T^{(p-1)/2} + 1) \tag{2.1}$$

com coeficientes (mod p). Sabemos que um polinômio de grau d não tem mais do que d raízes (mod p). Aplicando o Pequeno Teorema de Fermat no lado esquerdo de (2.1), temos que $T^{(p-1)} - 1 \equiv 0$ (mod p), logo, $T \in \{1, 2, \ldots, p-1\}$ soluções, temos que $(T^{(p-1)/2)} - 1)(T^{(p-1)/2} + 1) \equiv 0$ (mod p), como $p-1 \equiv 0$ (mod 4), então $\left(\frac{p-1}{2}\right) = 2k$ para $k \in \mathbb{Z}$, logo, $\left(\frac{p-1}{2}\right)$ sempre será par, e temos que $T \in \{1, 2, \ldots, p-1\}$, então, $(T^{(p-1)/2} + 1)$ terá a metade das soluções de T, então considere que $\exists c \in \{1, 2, \ldots, p-1\}$ tal que $c^{(p-1)/2)} + 1 \equiv 0$ (mod p) $\Rightarrow c^{2k} \equiv -1$ (mod p) $\Rightarrow (c^k)^2 \equiv -1$ (mod p) $\equiv 3$ (mod 4), temos que $x = c^k$, logo, $x^2 \equiv -1$ (mod p), o que demonstra que (1) $\Rightarrow$ (2). Para mostrar que (2) implica (3), vamos mostrar que (2) implica p, onde é composto em $\mathbb{Z}[i]$. Sabemos que o Teorema 15 diz que $p = a^2 + b^2$. Vamos observar a congruência em (2) como uma relação divisibilidade em $\mathbb{Z}$. Quando $x^2 \equiv -1$ (mod p) para algum $x \in \mathbb{Z}$, temos que $x^2+1 \equiv 0$ (mod p), então, $p|(x^2+1)$ em $\mathbb{Z}$. Agora, considere este divisibilidade em $\mathbb{Z}[i]$, onde $x^2 + 1 = (x - i)(x + i)$, logo, podemos ter a seguinte fatoração de $x^2 + 1$:

$$p \quad | \quad (x + i)(x - i). \tag{2.2}$$

Vamos mostrar que p é composto em $\mathbb{Z}[i]$, argumentando por contradição. Se p é um número primo de Gauss, em (2.2), temos que $p|(x+i)$ ou $p|(x-i)$ em $\mathbb{Z}[i]$. Portanto, existe algum inteiro Gaussiano $(m+ni)$ que satisfaça $p(m+ni) = x \pm i$. Mas vamos observar a parte imaginária: $pn = \pm 1$. Isso é impossível! Temos uma contradição, o que prova que p é composto em $\mathbb{Z}[i]$, ou seja, p é uma soma de dois quadrados pelo Teorema 13, assim, (2) $\Rightarrow$ (3). ∎

Podemos resumir a fatoração de números primos em $\mathbb{Z}^+$ em fatores de primos de Gauss.

Exemplo 19 *O número 61 é primo em* $\mathbb{Z}^+$ *e satisfaz* $61 \equiv 1$ *(mod 4), então 61 tem dois fatores primos de Gauss. Uma vez que* $61 = 5^2 + 6^2 \Rightarrow 61 = (5+6i)(5-6i)$. $\diamond$

Teorema 15 *Cada primo em* $\mathbb{Z}[i]$ *é um múltiplo unitário de um dos seguintes números primos:*

(i) $(1+i)$

(ii) π *ou* $\bar{\pi}$, *onde* $N(\pi) = p$ *é primo em* $\mathbb{Z}^+$, *com* $p \equiv 1$ *(mod 4).*

(iii) p, *onde* p *é primo em* $\mathbb{Z}^+$, *com* $p \equiv 3$ *(mod 4).*

Prova. No item (i) e (ii) não é necessário mostrar que são primos em $\mathbb{Z}[i]$ pois a norma é primo em $\mathbb{Z}$. Para p primo em $\mathbb{Z}[i]$, então $p \equiv 3 \pmod 4$, logo, temos que $N(p) = p \cdot \bar{p} = p^2$, então, para todo p, primo de Gauss, cuja a norma não é primo em $\mathbb{Z}^+$. ■

Os primos de Gauss têm norma p ou p^2, onde p é primo e $p \in \mathbb{Z}^+$. Em particular, o número primo de Gauss é diferente de $(1+i)$ e seus múltiplos unitários têm uma norma ímpar. Assim, o número inteiro de Gauss, que não é divisível por $(1+i)$ tem norma ímpar, portanto, qualquer número inteiro de Gauss com uma norma par deve ser divisível por $(1+i)$. Isso já foi visto no Corolário 1.2. De um ponto de vista mais elevado, em relação a fatoração única em $\mathbb{Z}[i]$: pois o Corolário 1.2 é verdade, porque todo inteiro Gaussiano com a norma maior que 1 é um produto de números primos de Gauss e $(1+i)$ é o único primo Gaussiano com múltiplo unitário.

Teorema 16 *Um número inteiro maior do que 1 é uma soma de dois quadrados exatamente quando todos os primos p, com* $p \equiv 3$ *(mod 4), de sua fatoração ocorrem com a multiplicidade par.*

Prova. Primeiro vamos mostrar que um inteiro que tem multiplicidade par em seus fatores primos que são congruentes a 3 (mod 4), pode ser escrito como uma soma de dois quadrados. Sabemos que somas de dois quadrados são fechados para multiplicação. Qualquer primo $p \equiv 1 \pmod 4$ é uma soma de dois quadrados, pelo Teorema 13. Enquanto, um primo $p \equiv 3 \pmod 4$ não é uma soma de dois quadrados. Se $p \equiv 3 \pmod 4$ então $p^2 \equiv 1 \pmod 4$ e portanto $p^{2k} \equiv 1 \pmod 4$ para $\forall k \in \mathbb{N}$. Assim, como as potências dos primos $\equiv 3 \pmod 4$ são pares, temos o resultado. ■

Exemplo 20 *O número* $35 = 5 \cdot 7$ *tem apenas um fator primo que satisfaz* $p \equiv 3$ *(mod 4). Esse fator aparece com multiplicidade 1, então 35 não é uma soma de dois quadrados. Nem é* $5^k \cdot 7^w$ *para qualquer expoente ímpar* $w > 0$. *Mas para* $w = 2$, *temos que* $5 \cdot 7^2 = 245$ *é uma soma de dois quadrados:* $245 = 7^2 + 14^2$. $\diamond$

Portanto, vimos que os números primos em $\mathbb{Z}[i]$ são:

(1) O primo $(1+i)$ e seus múltiplos unitários.

(2) Os primos p em $\mathbb{Z}$ tal que $p \equiv 3 \pmod 4$ e seus múltiplos unitários.

(3) Para cada primo p em $\mathbb{Z}^+$ tal que $p \equiv 1 \pmod 4$, sendo $p = a^2 + b^2$, teremos $(a+bi)$ e $(a-bi)$ os primos em $\mathbb{Z}[i]$ e seus múltiplos unitários.

Capítulo 3

Atividades com os números Primos Gaussianos em sala de aula

Neste Capítulo elaboramos três atividades envolvendo os números inteiros Gaussianos, com aplicações de teoremas e intenções de desenvolver, exercitar, fixar e aprofundar os conteúdos matemáticos. As atividades servem como sugestões para o Professor de Matemática aplicar em sala de aula na 3ª série do ensino médio.

3.1 Atividade 1 - Apresentação dos inteiros Gaussianos

Podemos definir os inteiros de Gauss como subconjunto dos números complexos escrito na forma: $\alpha = a + bi$, onde $a, b \in \mathbb{Z}$. Vejamos alguns exemplos:

(a) $\alpha = 3 - 2i$, pois $a = 3$ *e* $b = -2$.

(b) $\alpha = -5 + i$, pois $a = -5$ *e* $b = 1$.

(c) $\alpha = -4$, pois $a = -4$ *e* $b = 0$.

(d) $\alpha = i$, pois $a = 0$ *e* $b = 1$.

Nesta atividade, vamos identificar os números inteiros Gaussianos, através de questões que necesitam dos conhecimentos dos números complexos e suas operações.

Atividade

Seja os números complexos $\alpha = a + 6i$ e $\beta = 18 + bi$. Sabendo que $(\alpha + \beta)$ é um número real e $\alpha \cdot \beta$ é um número imaginário puro, responda:

(a) Encontre os valores de a e b tais que α e β sejam inteiros Gaussianos.

(b) Calcule $(\alpha + \beta)$ e $\alpha \cdot \beta$

(c) Verifique se $\alpha | \beta$

Objetivo Geral

Reconhecer os números inteiros de Gauss, a partir dos números complexos.

Objetivos Específicos

- Estudar sobre dos números complexos, $\mathbb{C}$;
- Definir os números inteiros de Gauss, $\mathbb{Z}[i]$;
- Identificar os números inteiros Gaussianos;
- Aplicar as operações de adição e multiplicação.

Público Alvo

Estudantes da 3ª série do ensino médio, segundo os Parâmetros Curriculares Nacionais (PCN).

Pré-Requisitos

Os alunos deverão conhecer o conjuntos dos números inteiros e seu subconjunto inteiros positivos $\mathbb{Z}^+$, ter o conhecimento da definição de números complexos, ou seja, a representação $i^2 = -1$ e as principais operações entre eles.

Materiais

Os materiais utilizados essa atividade são lápis, borracha e a folha contendo a atividade.

Recomendações Metodológicas

Esta atividade será aplicada em sala de aula após a apresentação dos números complexos e a definição dos números inteiros de Gauss. Os estudantes responderão a atividade em dupla e, posteriormente, irão debater os resultados obtidos com toda a turma. Ao final do debate, o professor apresentará as respostas detalhadamente ou soliticar que os próprios alunos respondam no quadro.

Dificuldades Previstas

Esta atividade requer conhecimentos prévio sobre os números complexos, ou seja, se por algum motivo o aluno não absorveu esses conhecimentos a atividade será encarada com dificuldades. Dessa forma, ao perceber essas dificuldades o docente deverar dar uma atenção especial a este aluno.

Possíveis continuações ou desdobramentos

O professor poderá criar outras atividades envolvendo os números inteiros Gaussianos.

3.2 Atividade 2 - Identificação dos números primos em $\mathbb{Z}[i]$

Sendo p um número primo em $\mathbb{Z}[i]$, então vimos que existem apenas os seguintes fatores:

$$1,\ -1,\ i,\ -i,\ p,\ -p,\ pi \text{ e } -pi.$$

E sabemos que o número primo Gaussiano não pode ser escrito como a soma de dois quadrados e que pelo Teorema 10, se a norma de um inteiro de Gauss é primo em $\mathbb{Z}$, então o inteiro Gaussiano é primo em $\mathbb{Z}[i]$. Vejamos alguns exemplos:

(a) $N(1+2i) = 5$, pois 5 é primo em $\mathbb{Z} \Rightarrow (1+2i)$ é primo em $\mathbb{Z}[i]$.

(b) $N(5+2i) = 29$, pois 29 é primo em $\mathbb{Z} \Rightarrow (5+2i)$ é primo em $\mathbb{Z}[i]$.

(c) $N(10-i) = 101$, pois 101 é primo em $\mathbb{Z} \Rightarrow (10-i)$ é primo em $\mathbb{Z}[i]$.

(d) $N(3+5i) = 34$, pois 34 não é primo em $\mathbb{Z} \Rightarrow (3+5i)$ não é primo em $\mathbb{Z}[i]$.

Nessa atividade, vamos estudar como identificar os primos Gaussianos, utilizando os teoremas e as propriedades já vistos inicialmente.

Atividade

Determine quais dos seguintes inteiros de Gauss, são primos Gaussianos.

(a)$(1+3i)$ (b)$(3+4i)$ (c)$(14-5i)$ (d)$(-1+4i)$

Objetivo Geral

Descobrir a existência dos números primos Gaussianos.

Objetivos Específicos

- Saber a definição dos primos Gaussianos;
- Identificar os números primos Gaussianos;
- Estimular a curiosidade da descoberta dos primos Gaussianos.

Público Alvo

Estudantes da 3ª série do ensino médio, segundo os Parâmetros Curriculares Nacionais (PCN).

Pré-Requisitos

Será necessário a resolução da atividade anterior. Os alunos deverão saber a definição de números primos em $\mathbb{Z}^+$, conhecer os números complexos e saber identificar os números inteiros Gaussianos.

Materiais

Os materiais utilizados essa atividade são lápis, borracha e a folha contendo a atividade.

Recomendações Metodológicas

Esta atividade será aplicada em sala de aula após a definição dos inteiros de Gauss. Os estudantes responderão a atividade em dupla e, posteriormente, irão debater os resultados obtidos com toda a turma. Ao final do debate, o professor apresentará as respostas detalhadamente ou solitará que os próprios alunos respondam no quadro.

Dificuldades Previstas

Esta atividade requer conhecimentos prévios, assim, se por algum motivo o aluno não absorveu esses conhecimentos a atividade será encarada com dificuldades. Dessa forma, ao perceber essas dificuldades o docente deverar dar uma atenção especial a este aluno.

Possíveis continuações ou desdobramentos

O professor poderá criar outras atividades aplicando os números primos Gaussianos.

3.3 Atividade 3 - Relacionar os primos inteiros e primos Gaussianos

Nessa atividade, vamos fazer uma comparação entre os primos inteiros positivos, onde $p > 2$ e os primos Gaussianos, e encontrar uma característica comum entre os primos em $\mathbb{Z}^+$ que também são primos em $\mathbb{Z}[i]$.

Atividade

Vamos descobrir uma relação que indica quais números primos inteiros positivos também são primos Gaussianos.

- Para $p = 3$, vamos aplicar a norma, pois $N(p) = p^2 = (a + bi)(c + di)$, então:

$$N(3) = 9 = 3 \cdot 3 \Rightarrow (a + bi) = 3 \text{ e } (c + di) = 3.$$

  Não podemos escrever 3 como produto de dois números inteiros Gaussianos. Logo, **3 é primo Gaussiano**.

- Para $p = 5$, vamos aplicar a norma, pois $N(p) = p^2 = (a + bi)(c + di)$, então:

$$N(5) = 25 = 5 \cdot 5 \Rightarrow (a + bi) = 5 \text{ e } (c + di) = 5.$$

  Daí, $(a, b) = (\pm 2, \pm 1)$ e $(c, d) = (\pm 2, \pm 1)$. Assim, podemos escrever 5 como produto de dois números inteiros Gaussianos,

$$(2 - i)(2 + i) = 5.$$

  Logo, **5 não é primo Gaussiano**.

- Para $p = 7$, vamos aplicar a norma, pois $N(p) = p^2 = (a + bi)(c + di)$, então:

$$N(7) = 49 = 7 \cdot 7 \Rightarrow (a + bi) = 7 \text{ e } (c + di) = 7.$$

  Assim, não podemos escrever 7 como produto de dois números inteiros Gaussianos, donde concluimos que **7 é primo Gaussiano**.

- Para $p = 11$, vamos aplicar a norma, pois $N(p) = p^2 = (a + bi)(c + di)$, então:

$$N(11) = 121 = 11 \cdot 11 \Rightarrow (a + bi) = 11 \text{ e } (c + di) = 11.$$

  Assim, não podemos escrever 11 como produto de dois números inteiros Gaussianos, logo, **11 é primo Gaussiano**.

- Para $p = 13$, vamos aplicar a norma, pois $N(p) = p^2 = (a+bi)(c+di)$, então:

$$N(13) = 169 = 13 \cdot 13 \Rightarrow (a+bi) = 13 \text{ e } (c+di) = 13.$$

Daí, $(a,b) = (\pm 2, \pm 3)$ e $(c,d) = (\pm 2, \pm 3)$. Assim, podemos escrever 13 como produto de dois números inteiros Gaussianos.

$$(2+3i)(2-3i) = 13.$$

Logo, **13 não é primo Gaussiano**.

- Para $p = 17$, vamos aplicar a norma, pois $N(p) = p^2 = (a+bi)(c+di)$, então:

$$N(17) = 289 = 17 \cdot 17 \Rightarrow (a+bi) = 17 \text{ e } (c+di) = 17.$$

Daí, $(a,b) = (\pm 1, \pm 4)$ e $(c,d) = (\pm 1, \pm 4)$. Assim, podemos escrever 17 como produto de dois números inteiros Gaussianos.

$$(2-4i)(2+4i) = 17.$$

Logo, **17 não é primo Gaussiano**.

- Para $p = 19$, vamos aplicar a norma, pois $N(p) = p^2 = (a+bi)(c+di)$, então:

$$N(19) = 361 = 19 \cdot 19 \Rightarrow (a+bi) = 19 \text{ e } (c+di) = 19.$$

Assim, não podemos escrever 19 como produto de dois números inteiros Gaussianos, donde concluimos que **19 é primo Gaussiano**.

- Para $p = 23$, vamos aplicar a norma, pois $N(p) = p^2 = (a+bi)(c+di)$, então:

$$N(23) = 529 = 23 \cdot 23 \Rightarrow (a+bi) = 23 \text{ e } (c+di) = 23.$$

Assim, não podemos escrever 23 como produto de dois números inteiros Gaussianos, donde concluimos que **23 é primo Gaussiano**.

Objetivo Geral

Descobrir a relação entre os primos inteiros positivos e primos Gaussianos.

Objetivos Específicos

- Desenvolver habilidade nas operações dos conjuntos dos números complexos;
- Utilizar o raciocinio lógico nos cálculos de combinações dos resultados para $p = a^2 + b^2$, onde p é primo em $\mathbb{Z}^+$.

Público Alvo

Estudantes da 3ª série do ensino médio, segundo os Parâmetros Curriculares Nacionais (PCN).

Pré-Requisitos

Os alunos deverão saber a definição de números primos em $\mathbb{Z}^+$, e saber identificar os números inteiros gaussianos.

Materiais

Os materiais utilizados essa atividade são lápis, borracha e a folha contendo a atividade.

Recomendações Metodológicas

Esta atividade será aplicada em sala de aula após a definição dos inteiros de Gauss. Os estudantes responderão a atividade em dupla e, posteriormente, irão debater os resultados obtidos com toda a turma. Ao final do debate, o professor apresentará as respostas detalhadamente ou solitará que os próprios alunos respondam no quadro.

Dificuldades Previstas

Esta atividade requer conhecimentos prévios, assim, se por algum motivo o aluno não absorveu esses conhecimentos a atividade será encarada com dificuldades. Dessa forma, ao perceber essas dificuldades o docente deverar dar uma atenção especial a este aluno.

Possíveis continuações ou desdobramentos

O professor poderá criar outras atividades aplicando os números primos Gaussianos.

Capítulo 4

Soluções das atividades propostas

4.1 Solução da Atividade 1

Consideremos os números complexos $\alpha = a + 6i$ e $\beta = 18 + bi$. Sabendo que $(\alpha + \beta)$ é um número real e $\alpha \cdot \beta$ é um número imaginário puro, responda:

(a) Encontre os valores de a e b tais que α e β sejam inteiros Gaussianos.

Solução: Sendo $\alpha = a + 6i$ e $\beta = 18 + bi$, aplicando as operações dos números complexos, temos que $\alpha + \beta = x + 0 \cdot i$, com $x \in \mathbb{Z}$. Assim,

$$\begin{aligned} (a + 6i) + (18 + bi) &= x + 0 \cdot i \\ (a + 18) + (6 + b)i &= x + 0 \cdot i \end{aligned}$$

Vamos formar um sistema: $\begin{cases} a + 18 = x \\ 6 + b = 0 \end{cases} \Rightarrow b = -6.$

Para determinarmos o valor de a, temos que $\alpha \cdot \beta = 0 \cdot + yi$, com $y \in \mathbb{Z}$. Assim,

$$\begin{aligned} (a + 6i)(18 + bi) &= 0 + y \cdot i \\ 18a + abi + 108i - 6b &= 0 + y \cdot i \end{aligned}$$

Como $b = -6$, substituindo, teremos que:

$$\begin{aligned} 18a - 6ai + 108i + 36 &= 0 + y \cdot i \\ (18a + 36) + (-6a + 108)i &= 0 + y \cdot i \end{aligned}$$

Vamos formar um sistema: $\begin{cases} 18a + 36 = 0 \\ 6a + 108 = y \end{cases} \Rightarrow a = -2.$

Logo, $a = -2$ e $b = -6 \Rightarrow \begin{cases} \alpha = -2 + 6i \\ \beta = 18 - 6i \end{cases}$ então α e $\beta \in \mathbb{Z}[i]$.

(b) Calcule $(\alpha + \beta)$ e $\alpha \cdot \beta$.

Solução: Como vimos em (a), $\alpha + \beta = x$ e $\alpha \cdot \beta = yi$ onde $x, y \in \mathbb{Z}$, então:

$$\begin{cases} a + 18 = x \\ (-6a + 108) = y \end{cases}$$

Logo, $x = 16 \Rightarrow \alpha + \beta = 16$ e $y = 120 \Rightarrow \alpha\beta = 120i$.

(c) Verifique se $\alpha | \beta$.

Solução: Sabemos que $\beta = \alpha \cdot \gamma$, considere $\gamma = (c + di)$, para $c, d \in \mathbb{Z}$, assim,

$$\begin{aligned} (-2 + 6i) \cdot (c + di) &= (18 - 6i) \\ -2c - 2di + 6ci - 6d &= (18 - 6i) \\ (-2c - 6d) + (6c - 2d)i &= (18 - 6i) \end{aligned}$$

Vamos formar um sistema : $\begin{cases} -2c - 6d = 18 \\ 6c - 2d = -6 \end{cases} \Rightarrow a = -\dfrac{72}{40}$ e $b = -\dfrac{96}{40}$.

$\left(-\dfrac{72}{40} - \dfrac{96}{40}i\right) \notin \mathbb{Z}[i]$.

Logo, $\alpha \nmid \beta$.

4.2 Solução da Atividade 2

Determine quais dos seguintes inteiros de Gauss, são primos Gaussianos.

(a) $(1+3i)$

Solução: Vamos analisar a norma de $(1+3i)$, então temos que $N(1+3i) = 10$. Como 10 não é primo em $\mathbb{Z}$, então pelo resultado, $(1+3i)$ não é primo em $\mathbb{Z}[i]$. Vamos tentar escrever $(1+3i)$ como o produto de dois números inteiros Gaussianos. Considerando $N(\alpha) = (a+bi)(c+di)$ para $a, b, c, d \in \mathbb{Z}$.

Como $N(1+3i) = 1^2 + 3^2 = 10 = 2 \cdot 5$, temos que

$$\begin{cases} a^2 + b^2 = 2 \\ c^2 + d^2 = 5 \end{cases}$$

Estes têm várias soluções, entre elas $(a, b) = (1, 1)$ e $(c, d) = (2, 1)$ e, conseqüentemente, podemos escrever $(1+3i) = (1+i) \cdot (2+i)$.

(b) $(3+4i)$

Solução: Vamos analisar a norma de $(3+4i)$, então temos que $N(3+4i) = 25$. Como 25 não é primo em $\mathbb{Z}$, então pelo resultado, $(3+4i)$ não é primo em $\mathbb{Z}[i]$. Vamos tentar escrever $(3+4i)$ como o produto de dois números inteiros Gaussianos. Considerando $N(\alpha) = (a+bi)(c+di)$ para $a, b, c, d \in \mathbb{Z}$.

Como $N(3+4i) = 3^2 + 4^2 = 25 = 5 \cdot 5$, assim temos que

$$\begin{cases} a^2 + b^2 = 5 \\ c^2 + d^2 = 5 \end{cases}$$

Estes têm várias soluções, entre elas $(a, b) = (2, 1)$ e $(c, d) = (2, 1)$ e, conseqüentemente, podemos escrever $(3+4i) = (2+i) \cdot (2+i)$.

(c) $(14-5i)$

Solução: Vamos analisar a norma de $(14-5i)$, então temos que $N(14-5i) = 221$. Como 221 não é primo em $\mathbb{Z}$, então pelo resultado, $(14-5i)$ não é primo em $\mathbb{Z}[i]$.

Vamos tentar escrever $(14-5i)$ como o produto de dois números inteiros Gaussianos. Considerando $N(\alpha) = (a+bi)(c+di)$ para $a, b, c, d \in \mathbb{Z}$.

Como $N(14-5i) = 14^2 + (-5)^2 = 221 = 13 \cdot 17$ assim temos que

$$\begin{cases} a^2 + b^2 = 13 \\ c^2 + d^2 = 17 \end{cases}$$

Estes têm várias soluções, entre elas $(a, b) = (3, 2)$ e $(c, d) = (1, -4)$ e, conseqüentemente, podemos escrever $(14 - 5i) = (3 + 2i) \cdot (1 - 4i)$.

(d) $(-1 + 4i)$

Solução: Vamos analisar a norma de $(-1 + 4i)$, então temos que $N(-1 + 4i) = 17$. Como 17 é primo em $\mathbb{Z}$, então pelo resultado, $(3 + 4i)$ é primo em $\mathbb{Z}[i]$. Não existem o produto de dois números inteiros Gaussianos.

4.3 Solução da Atividade 3

Vamos descobrir uma relação que indica quais números primos inteiros positivos, para $p > 2$ também são primos Gaussianos.

Temos que:

Primo em $\mathbb{Z}$	Sentença	$p \equiv 1$ ou $3 \pmod 4$	Primo em $\mathbb{Z}[i]$	$p = (a+bi)(c+di)$
3	$3 = 4 \cdot 0 + 3$	$p \equiv 3 \pmod 4$	Sim	Não Existe
5	$5 = 4 \cdot 1 + 1$	$p \equiv 1 \pmod 4$	Não	$5 = (2-i)(2+i)$
7	$7 = 4 \cdot 1 + 3$	$p \equiv 3 \pmod 4$	Sim	Não Existe
11	$11 = 4 \cdot 2 + 3$	$p \equiv 3 \pmod 4$	Sim	Não Existe
13	$13 = 4 \cdot 3 + 1$	$p \equiv 1 \pmod 4$	Não	$13 = (2+3i)(2-3i)$
17	$17 = 4 \cdot 4 + 1$	$p \equiv 1 \pmod 4$	Não	$17 = (1-4i)(1+4i)$
19	$19 = 4 \cdot 4 + 3$	$p \equiv 3 \pmod 4$	Sim	Não Existe
23	$23 = 4 \cdot 5 + 3$	$p \equiv 3 \pmod 4$	Sim	Não Existe
29	$29 = 4 \cdot 7 + 1$	$p \equiv 1 \pmod 4$	Não	$29 = (2+5i)(2-5i)$
⋮	⋮	⋮	⋮	⋮
97	$97 = 4 \cdot 24 + 1$	$p \equiv 1 \pmod 4$	Não	$97 = (9+2i)(9-2i)$
⋮	⋮	⋮	⋮	⋮

Tabela 4.1: Tabela de Comparação

Então chegamos a conclusão que para todos os primos em $\mathbb{Z}^+$ escrito da forma $(4n+3)$ também é primo em $\mathbb{Z}[i]$.

Notações e Símbolos

Símbolo	Descrição
$\mathbb{C}$	Conjuntos dos números complexos
$\mathbb{Z}$	Conjuntos dos números inteiros
$\mathbb{Z}[i]$	Conjuntos dos números inteiros de Gauss
$\mathbb{Z}^+$	Conjuntos dos números inteiros positivos
α	Alfa
β	Beta
γ	Gama
δ	Delta
π	Pi
$\in$	Pertence
$\notin$	Não pertence
$\neq$	Diferente
$\equiv$	Congruente
$>$	Maior
$<$	Menor
$\geq$	Maior ou Igual
$\leq$	Menor ou Igual
$\mid$	Divide
$\nmid$	Não divide
$\exists$	Existe
$\nexists$	Não existe
$\forall$	Qualquer
$\Rightarrow$	Implica que
$\Leftrightarrow$	Se, somente se

Apêndice

Conjunto dos Números Complexos

O fato de um número negativo não ter raiz quadrada não parece ser problema para os matemáticos que se depararam com esta questão, até a concepção do modelo dos números complexos. O conjunto dos números complexos, denotado por $\mathbb{C}$, contém o conjunto dos números reais. Apresentando as operações de adição e multiplicação obtidas por extensão das operações de mesma denominação nos números reais, tem uma estrutura algébrica sendo que esse fechamento consiste na propriedade que tem o conjunto de possuir todas as soluções de qualquer equação polinomial com coeficientes naquele mesmo conjunto (no caso, o conjunto dos complexos).

Um número complexo é um número z que pode ser escrito na forma $z = x + iy$, em que x e y são números reais e onde i chamamos de unidade imaginária. Esta tem a propriedade $i^2 = -1$, sendo que x e y são chamados respectivamente parte real e parte imaginária de z. O plano complexo, também chamado de plano de Argand-Gauss é uma representação geométrica do conjunto dos números complexos. Da mesma forma como a cada ponto da reta está associado um número real, o plano complexo associa biunivocamente o ponto (x, y) do plano ao número complexo $x+yi$. Esta associação conduz a pelo menos duas formas de representar um número complexo:

1. Forma Retangular ou Cartesiana:

$$Z = (x, y) = x + iy$$

2. Forma Polar:

$$Z = r(\cos\theta + i\sin\theta)$$

Operações Elementares

O conjunto dos números complexos é um corpo. Portanto, é fechado sobre as operações de adição e multiplicação, além de possuir a propriedade de que todo elemento não-nulo do conjunto possui um inverso multiplicativo. Todas as operações do corpo podem ser performadas através das propriedades associativa, comutativa e distributiva, levando em consideração a identidade $i^2 = -1$.

Sejam z e w dois números complexos dados por $z = (a, b)$ e $w = (c, d)$ então definem-se as relações e operações elementares tal como segue:

1. Identidade: $z = w \Leftrightarrow a = b$ e $c = d$
2. Soma: $z + w = w + z = (a + bi) + (c + di) = (a + c) + (b + d)i$
3. Produto: $z.w = w.z = (a + bi)(c + di) = (ac - bd) + (bc + ad)i$
4. conjugado: $\overline{z} = a - bi$, onde $\overline{z}$ denota o conjugado de z. O conjugado de um número complexo é seu simétrico no plano complexo em relação ao eixo real. A soma e o produto de um número complexo com seu conjugado tem parte imaginária nula.
5. Soma de um Complexo pelo seu Conjugado: $z + \overline{z} = (a + bi) + (a - bi) = 2a$.
6. Produto de um Complexo pelo seu Conjugado: $z.\overline{z} = (a+bi)(a-bi) = a^2+b^2$.

Referências Bibliográficas

[1] Boyer, C. B. *História da Matemática*, Terceira Edição, São Paulo: Blucher.(2010).

[2] Butler, L. A. *A classification of Gaussian Primes.*

[3] Conrad, K. *The Gaussian Integers.*

[4] Eves, H. *Introdução à História da Matemática*, Campinas, São Paulo: Editora da UNICAMP. (2004).

[5] Fossa, J.A. *Introdução à Teoria Elementar dos Números Primos*, Natal, Rio Grande do Norte: Editora Universitária. (2003).

[6] Fujiwara, G. *Inteiros de Gauss e Inteiros de Eisenstein*, Eureka! 14, Rio de Janeiro: SBM. (2002).

[7] Hefez, A. *Elementos da Aritmética*, Textos Universitários, Segunda Edição, Rio de Janeiro: SBM. (2006).

[8] Sidki, S. *Introdução a Teoria dos Números*, Rio de Janeiro: IMPA. (1975).

[9] Wall, E.S. *Teoria dos Números para Professores do Ensino Fundamental*, São Paulo: AMGH Editora. (2014)