

Universidade Estadual de Maringá
Centro de Ciências Exatas
Departamento de Matemática
Mestrado Profissional em Matemática em Rede Nacional - PROFMAT

Soluções de Equações Diofantinas com Coeficientes nos Inteiros Gaussianos

por Vinícius Bomfim Cardoso

Orientador: Prof. Dr. Laerte Bemm

Maringá - PR

2020

Vinícius Bomfim Cardoso

**Soluções de Equações Diofantinas com
Coeficientes nos Inteiros Gaussianos**

Trabalho de conclusão de curso apresentado ao Programa de Mestrado Profissional em Matemática em Rede Nacional-PROFMAT do Departamento de Matemática, Centro de Ciências Exatas da Universidade Estadual de Maringá, como requisito parcial para obtenção de título de Mestre em Matemática.

Orientador: Prof.Dr.Laerte Bemm

Maringá - PR

2020

Dados Internacionais de Catalogação na Publicação (CIP)
(Biblioteca Setorial BSE-DMA-UEM, Maringá, PR, Brasil)

C268s	Cardoso, Vinicius Bomfim Soluções de equações diofantinas com coeficientes nos inteiros gaussianos / Vinicius Bomfim Cardoso. - Maringá, 2020. vi, 28 f. : il. color. Orientador: Prof. Dr. Laerte Bemm. Dissertação (mestrado) - Universidade Estadual de Maringá, Centro de Ciências Exatas, Departamento de Matemática, 2020. 1. Máximo divisor comum. 2. Equações diofantinas. 3. Inteiros gaussianos. 4. Domínios euclidianos. 5. Soluções em planilha eletrônica. I. Bemm, Laerte, orient. II. Universidade Estadual de Maringá. Centro de Ciências Exatas. Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT. III. Título. CDD 22.ed. 512.72
-------	--


Edilson Damasio CRB9-1.123

VINÍCIUS BOMFIM CARDOSO

SOLUÇÕES DE EQUAÇÕES DIOFANTINAS COM COEFICIENTES NOS INTEIROS GAUSSIANOS

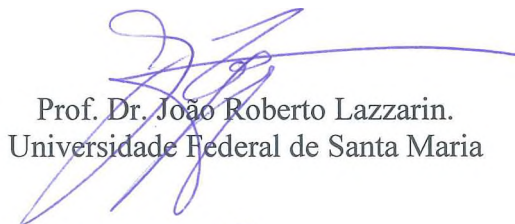
Dissertação apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional do Departamento de Matemática, Centro de Ciências Exatas da Universidade Estadual de Maringá, como parte dos requisitos necessários para a obtenção do título de Mestre em Matemática tendo a Comissão Julgadora composta pelos membros:

COMISSÃO JULGADORA:



Prof. Dr. Laerte Bemm

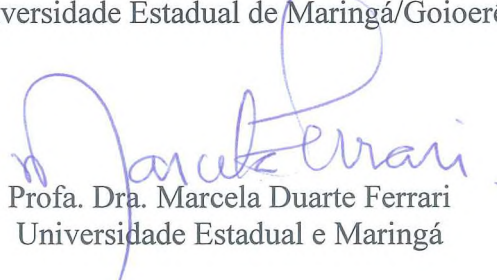
Universidade Estadual de Maringá (Orientador)



Prof. Dr. João Roberto Lazzarin.
Universidade Federal de Santa Maria



Prof. Dr. Edilson Soares Miranda
Universidade Estadual de Maringá/Goioerê



Prof. Dra. Marcela Duarte Ferrari
Universidade Estadual e Maringá

Aprovada em: 11 de março de 2020

Local de defesa: Auditório do DMA, Bloco F67, campus da Universidade Estadual de Maringá.

“Many who have had an opportunity of knowing any more about mathematics confuse it with arithmetic, and consider it an arid science. In reality, however, it is a science which requires a great amount of imagination.”

Sofia Kovalevskaya

Agradecimentos

Agradeço este trabalho, a Deus por ter me proporcionado todo estudo e criação deste trabalho da melhor forma possível.

Quero agradecer também aos meus pais Paulo e Geralda, pois me apoiaram e me incentivaram neste projeto desde o início. Quero agradecer também a minha esposa Érica, que também me incentivou, e me apoiou desde o momento em que entrou em minha vida.

Agradeço ao meu orientador Laerte Bemm, por ter me orientado e me guiado para que pudesse terminar este trabalho.

E um agradecimento especial a professora Ms. Priscila C. F. de Jesus por sua colaboração no desenvolvimento desse trabalho, em especial na elaboração dos algoritmos da Seção 5. Também agradeço por sua leitura minuciosa e sugestões relevantes ao texto final.

Resumo

Nesse trabalho estudamos condições necessárias e suficientes para que uma equação diofantina linear sobre um domínio euclidiano tenha solução. Apresentamos uma série de algoritmos (funções) que podem ser implementados em planilhas eletrônicas (por exemplo Libreoffice, Excel, etc), com o intuito de determinar (caso existam) soluções de equações diofantinas sobre $\mathbb{Z}[i]$.

Palavras-chave: Máximo Divisor Comum, Equações Diofantinas, Inteiros Gaussianos, Domínios Euclidianos, Soluções em Planilha Eletrônica.

Abstract

In this work we study necessary and sufficient conditions for a linear diophantine equation over an euclidean domain to have some solution. We present a series of algorithms (functions) that can be implemented in spreadsheets (for example Libreoffice, Excel, etc), in order to determine (if any) solutions for Diophantine equations over $\mathbb{Z}[i]$.

Key-words: Greatest Common Divisor, Diofantine Equations, Gaussian Integers, Euclidian Domains, Solutions on Spreadsheet.

Sumário

Introdução	1
1 Equações Diofantinas em Planilhas Eletrônicas	3
1 Máximo Divisor Comum em Domínios de Integridade	3
2 Domínios Euclidianos	5
3 Equações Diofantinas em Domínios Euclidianos	11
4 Aplicação: Equações Diofantinas sobre $\mathbb{Z}[i]$	13
5 Cálculos em $\mathbb{Z}[i]$ Através de Planilhas Eletrônicas	15
5.1 Divisão em $\mathbb{Z}[i]$	16
5.2 Cálculo do mdc em $\mathbb{Z}[i]$	17
5.3 Constantes de Bezout em $\mathbb{Z}[i]$	18
5.4 Soluções de Equações Diofantinas em $\mathbb{Z}[i]$	19
Conclusão	25
Referências Bibliográficas	27

Introdução

Equações lineares do tipo $aX + bY = c$, com $a, b, c \in \mathbb{Z}$ são comumente estudadas em disciplinas de Teoria dos Números nos cursos de graduação em Matemática. O interesse central no estudo dessas equações é encontrar soluções inteiras, ou seja, pares de números $x, y \in \mathbb{Z}$ tais que $ax + by = c$. Tais equações são chamadas *equações diofantinas* em homenagem a Diophanto de Alexandria (≈ 250 d. C.) que foi o primeiro a considerá-las. Quando estuda-se equações diofantinas, percebe-se que três coisas são cruciais e indispensáveis: divisibilidade, máximo divisor comum e algoritmo da divisão (em \mathbb{Z}). Como a determinação do máximo divisor comum de dois inteiros pode ser obtido através de sucessivas divisões (veja (HEFEZ, 2016) ou (MILIES, 2006)), podemos dizer que o algoritmo da divisão é essencial para o estudo dessas equações. Portanto, é mais conveniente estudá-las onde vale um tal algoritmo.

De fato, além de \mathbb{Z} , existem outros domínios de integridade onde vale um algoritmo da divisão. Tais domínios são chamados de euclidianos e há uma vasta literatura sobre eles (veja (ANDERSON, 2015) e (GATHEN, 2013), por exemplo). Mais ainda, no Teorema 4.10 de (GATHEN, 2013), os autores apresentam uma condição necessária e suficiente para que uma equação diofantina sobre um domínio euclidiano tenha solução. Nós apresentamos este teorema e sua prova no Teorema 3.2.

O ponto forte do estudo de equações diofantinas é que a maioria dos cálculos são algorítmicos e muitas vezes iterativos. O ponto fraco é que, em geral, tais cálculos são exaustivos e em grande quantidade. Por isso, é importante desenvolver modelos computacionais que possam ser implementados em computadores e que resolvam

tais equações. Em (DOS SANTOS, 2016), o autor implementa, para a plataforma *Android*, um aplicativo de resolução de equações diofantinas com coeficientes em \mathbb{Z} e em (SEMATIC SCHOLAR), o autor apresenta alguns algoritmos em linguagem de MATLAB para resolver equações diofantinas com coeficientes polinomiais.

Nesse trabalho apresentamos uma revisão bibliográfica sobre resolução de equações diofantinas sobre domínios euclidianos e desenvolvemos uma série de algoritmos que implementamos em planilhas eletrônicas do LibreOffice para determinarmos soluções de equações diofantinas sobre o domínio dos inteiros gaussianos $\mathbb{Z}[i]$. Para tanto, estruturamos a dissertação com apenas um capítulo dividido em 5 seções. Na Seção 1 definimos divisibilidade, máximo divisor comum e provamos o Lema de Euclides para domínios quaisquer. Na Seção 2 apresentamos uma prova algorítmica do Teorema de Bezout para domínios euclidianos e algumas consequências desse que serão utilizadas na Seção 3, onde apresentamos uma condição necessária e suficiente para que uma equação diofantina tenha solução. Na mesma seção, mostramos como determinar todas as soluções. Na Seção 4, aplicamos a teoria das seções anteriores para resolver equações diofantinas com coeficientes em $\mathbb{Z}[i]$. Na Seção 5 descrevemos uma série de algoritmos que implementamos numa planilha eletrônica do LibreOffice e que permitem obter o quociente e o resto da divisão de dois inteiros gaussianos; um máximo divisor comum de dois elementos de $\mathbb{Z}[i]$; as constantes de Bezout e as soluções de uma equação diofantina sobre $\mathbb{Z}[i]$. Finalizamos com uma breve conclusão.

Nesse momento vale ressaltar que os conceitos e resultados apresentados nas seções 1, 2 e 3 não são originais. Nós demonstramos a maioria dos resultados dessas seções por comodidade ao leitor e para deixar o trabalho o mais auto suficiente possível. Por outro lado, os algoritmos apresentados na Seção 5 são originais e acreditamos que o leitor não terá dificuldades em implementá-los.

Capítulo 1

Equações Diofantinas em Planilhas Eletrônicas

1 Máximo Divisor Comum em Domínios de Integridade

Esta seção é dedicada a fixarmos algumas notações, definições e resultados que são bem conhecidos e que usaremos no decorrer do trabalho. A menos que se mencione o contrário, A denotará um domínio de integridade, ou seja, um anel comutativo com identidade 1 em que o produto de elementos não nulos é não nulo. Para simplificar a nomenclatura, tais anéis serão chamados de domínios. Embora alguns conceitos que vamos estudar possam ser definidos para anéis em geral, nos interessa apenas os domínios.

Exemplo 1.1. *O anel dos inteiros \mathbb{Z} e o anel de polinômios sobre um corpo, com as operações usuais de adição e multiplicação são domínios;*

Exemplo 1.2. *O conjunto $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$, com as operações usuais de adição e multiplicação de números complexos é um domínio e é chamado de domínio dos inteiros gaussianos, em homenagem a C. F. Gauss, que foi o primeiro a considerar estes números para resolver problemas de Aritmética.*

1. MÁXIMO DIVISOR COMUM EM DOMÍNIOS DE INTEGRIDADE

Exemplo 1.3. Os conjuntos $\mathbb{Z}[\sqrt{\alpha}] = \{a + b\sqrt{\alpha} : a, b \in \mathbb{Z}\}$ (onde α é qualquer inteiro livre de quadrados) com as operações de adição e multiplicação definidas por

$$(a + b\sqrt{\alpha}) + (c + d\sqrt{\alpha}) = (a + b) + (c + d)\sqrt{\alpha}$$
$$(a + b\sqrt{\alpha})(c + d\sqrt{\alpha}) = (ac + \alpha bd) + (ad + bc)\sqrt{\alpha}.$$

Para $\alpha = -1$, temos $\mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[i]$. Para maiores detalhes, veja o Cap. 31 de (ANDERSON, 2015).

Definição 1.4. Sejam A um domínio e $a, b \in A$. Dizemos que a divide b (ou que a um divisor de b ou ainda b é um múltiplo de a) se existe $c \in A$ tal que $b = ac$. Nesse caso, escrevemos $a|b$.

Observação 1.5. Note que 0 apenas divide 0 . Além disso, por A ser domínio, segue facilmente que se $a|b$ e $a \neq 0$, então existe um único $c \in A$ tal que $b = ac$. Tal c é denotado por $\frac{b}{a}$.

A demonstração do próximo resultado será omitida por ser clássica.

Proposição 1.6. Sejam $a, b, c, d \in A$. Então:

- (i) $a|a$;
- (ii) Se $a|b$ e $b|c$, então $a|c$;
- (iii) Se $a|b$ e $c|d$ então $(ac)|(bd)$. Em particular, se $a|b$, então $ac|bc$;
- (iv) Se $a|b$ e $a|c$, então $a|(bs \pm ct)$ para quaisquer $s, t \in A$.

Definição 1.7. Sejam $a, b \in A^*$. Um elemento $d \in A^*$ é um máximo divisor comum (mdc) de a e b , se d satisfizer as seguintes propriedades:

- (i) $d|a$ e $d|b$;
- (ii) Se $d' \in A$ é tal que $d'|a$ e $d'|b$, então $d'|d$.

Pela definição anterior, em qualquer domínio A , $mdc(0, 0) = 0$ e $mdc(a, 0) = a$, para todo $a \in A$. Também, se $b|a$ em A , então $mdc(a, b) = b$. Outro ponto da definição

2. DOMÍNIOS EUCLIDIANOS

anterior que vale destaque é que ela não garante a existência tão pouco a unicidade de um mdc de dois elementos. Quando existir um mdc de quaisquer dois elementos, diremos que o domínio é com mdc . Por exemplo, \mathbb{Z} é um domínio com mdc (veja (HEFEZ, 2016) ou (MILIES, 2006)).

Observação 1.8. *Se d e d' são dois máximos divisores comuns de $a, b \in A$, então $d|d'$ e $d'|d$. Neste caso, existe $u \in \mathcal{U}(A)$ (conjunto dos elementos invertíveis de A) tal que $d' = du$. Ou seja, cada elemento da forma du , com $u \in \mathcal{U}(A)$, também é um mdc de a e b . Isto nos permite “escolher” um mdc de acordo com nossa conveniência. Em \mathbb{Z} , por exemplo, nós escolhemos o mdc entre a e b , como sendo positivo, mesmo sabendo que seu oposto também é um mdc . Para simplificar, denotamos qualquer mdc de a e b por $mdc(a, b)$. Assim, quando escrevemos $d = mdc(a, b)$, queremos dizer que d é um elemento de A que satisfaz a Definição 1.7. Quando $mdc(a, b) \in \mathcal{U}(A)$, ou equivalentemente, $mdc(a, b) = 1$, dizemos que a e b são coprimos ou primos entre si.*

Lema 1.9. (Lema de Euclides) *Sejam A um domínio e $a, b \in A$, tais que $a = bq + r$ para certos $q, r \in A$. Se $mdc(b, r)$ existe, então $mdc(a, b)$ existe e $mdc(a, b) = mdc(b, r)$.*

Demonstração:

Se existe $d = mdc(b, r)$, então existem $m, n \in A$ tal que $b = dm$ e $r = dn$. Assim, $a = (dm)q + dn = d(mq + n)$, isto é, $d|a$. Agora, se $d' \in A$ é tal que $d'|a$ e $d'|b$, então existem $a', b' \in A$ tais que, $a = d'a'$ e $b = d'b'$. Daí, $r = a - bq = d'(a' - b'q)$, o que implica, $d'|r$. Como $d = mdc(b, r)$, temos da Definição 1.7 que $d'|d$. Logo, $mdc(a, b)$ existe e $mdc(a, b) = d = mdc(b, r)$. \square

2 Domínios Euclidianos

Para os nossos propósitos, uma importante classe de domínios são os *domínios euclidianos*, i. é, aqueles que admitem um algoritmo da divisão.

2. DOMÍNIOS EUCLIDIANOS

Definição 2.1. *Seja A um domínio. Diremos que A é um domínio euclidiano, se existe uma função $\delta : A^* \rightarrow \mathbb{N}$ que satisfaz as seguintes propriedades:*

(i) $\forall a, b \in A^*$, se $b|a$, então $\delta(b) \leq \delta(a)$.

(ii) $\forall a, b \in A$ com $b \neq 0$, existem $q, r \in A$ tais que $a = bq + r$, com $r = 0$ ou $\delta(r) < \delta(b)$.

Nomenclatura 1. *No item (ii) da definição anterior, a é o dividendo, b é o divisor, q o quociente e r o resto. A função δ é denominada função norma.*

Exemplo 2.2. \mathbb{Z} é um domínio euclidiano com a função norma $\delta : \mathbb{Z}^* \rightarrow \mathbb{N}$ dada por $\delta(a) = |a|$.

Exemplo 2.3. Se \mathbb{K} é um corpo, então o anel de polinômios $\mathbb{K}[x]$ é um domínio euclidiano com a função norma $\delta : \mathbb{K}[x]^* \rightarrow \mathbb{N}$ dada por $\delta(p(x)) = \text{gr}(p(x))$ (grau de $p(x)$).

Exemplo 2.4. O domínio dos inteiros gaussianos $\mathbb{Z}[i]$ é euclidiano com a função norma $\delta : \mathbb{Z}[i]^* \rightarrow \mathbb{N}$ definida por $\delta(a + bi) = a^2 + b^2$. De fato, note que para quaisquer $z, w \in \mathbb{Z}[i]$, $\delta(zw) = \delta(z)\delta(w)$. Assim, se $z_1, z_2 \in \mathbb{Z}[i]^*$ são tais que $z_1|z_2$, então $z_2 = z_1z_3$ e daí $\delta(z_2) = \delta(z_1)\delta(z_3) \geq \delta(z_1)$. Isto mostra o item (i) da Definição 2.1. Para mostrar (ii), sejam $z_1, z_2 \in \mathbb{Z}[i]$ com $z_2 \neq 0$. Vamos mostrar que existem $q, r \in \mathbb{Z}[i]$ tais que $z_1 = qz_2 + r$ com $r = 0$ ou $\delta(r) < \delta(z_2)$. Com efeito, como $z_1, z_2 \in \mathbb{C}$, existem $\alpha, \beta \in \mathbb{Q}$ tais que $\frac{z_1}{z_2} = \alpha + \beta i$. Considere $m, n \in \mathbb{Z}$ tais que $|m - \alpha| \leq 0,5$ e $|n - \beta| \leq 0,5$. Então, $z_1 = z_2(\alpha + \beta i) = z_2(\alpha - m + m + \beta i - ni + ni) = z_2(m + ni) + z_2[(\alpha - m) + (\beta - n)i]$. Tomando $q = m + ni$ e $r = z_2[(\alpha - m) + (\beta - n)i]$, temos $z_1 = z_2q + r$. Mais ainda, como $m, n \in \mathbb{Z}$, segue que $q = m + ni \in \mathbb{Z}[i]$ e por consequência, $r = z_1 - z_2q \in \mathbb{Z}[i]$. Finalmente,

$$\delta(r) = \delta(z_2)[(\alpha - m)^2 + (\beta - n)^2] \leq \delta(z_2)(0,25 + 0,25) < \delta(z_2).$$

A seguir apresentamos o algoritmo da divisão de $\mathbb{Z}[i]$ de maneira sucinta.

2. DOMÍNIOS EUCLIDIANOS

Algoritmo 2.5. *Sejam $z_1 = x + yi, z_2 = a + bi \in \mathbb{Z}[i]$, com $z_2 \neq 0$.*

Passo 1. Calcular $\frac{z_1}{z_2} = \frac{xa + yb}{a^2 + b^2} + \frac{(ya - xb)}{a^2 + b^2}i$ e escrever $\alpha := \frac{xa + yb}{a^2 + b^2}$ e $\beta := \frac{ya - xb}{a^2 + b^2}$;

Passo 2. Tome $m, n \in \mathbb{Z}$ tais que $|m - \alpha| \leq 0,5$ e $|n - \beta| \leq 0,5$, ou seja, de modo que m e n estejam o mais próximo possível de α e β , respectivamente.

Resultado: *O quociente é $q = m + ni$ e o resto é $r = z_2[(\alpha - m) + (\beta - n)i]$.*

Observação 2.6. *Se A é um domínio euclidiano com norma δ , então para todo $a \in A^*$, $\delta(a) \geq 1$ e $\mathcal{U}(A) = \{a \in A^* : \delta(a) = \delta(1)\}$. Assim, por exemplo, temos que $\mathcal{U}(\mathbb{Z}) = \{1, -1\}$,*

$\mathcal{U}(\mathbb{Z}[i]) = \{1, -1, i, -i\}$ e $\mathcal{U}(\mathbb{K}[x]) = \mathbb{K}^$. Em particular, disso e da Observação 1.8, temos que se $a, b \in \mathbb{Z}[i]$ e $d = \text{mdc}(a, b)$, então $-d, di$ e $-di$ também são $\text{mdc}(a, b)$.*

Observação 2.7. *Note que todo domínio euclidiano é um domínio com mdc . De fato, sejam A um domínio euclidiano com norma δ e $a, b \in A$.*

Definimos $r_0 := a$ e $r_1 := b$. Existem $q_1, r_2 \in A$ tais que $r_0 = r_1q_1 + r_2$, com $r_2 = 0$ ou $\delta(r_2) < \delta(r_1)$.

Se $r_2 = 0$, então $r_1|r_0$ e temos $\text{mdc}(a, b) = \text{mcd}(r_0, r_1) = r_1$.

Se $r_2 \neq 0$, existem $q_2, r_3 \in A$ tais que $r_1 = r_2q_2 + r_3$, com $r_3 = 0$ ou $\delta(r_3) < \delta(r_2)$.

Se $r_3 = 0$, então $r_2|r_1$ e temos $\text{mdc}(a, b) = \text{mcd}(r_0, r_1) = \text{mdc}(r_1, r_2) = r_2$.

Se $r_3 \neq 0$, repetimos o processo.

Como $\delta(r_1) > \delta(r_2) > \delta(r_3) > \dots$ é uma sequência decrescente de números naturais, em algum momento obteremos um resto $r_n = 0$. Nesse caso, teremos $r_{n-2} = r_{n-1}q_{n-1}$, ou seja, $r_{n-1}|r_{n-2}$. Daí, $\text{mdc}(a, b) = \text{mdc}(r_0, r_1) = \text{mdc}(r_1, r_2) = \text{mdc}(r_2, r_3) = \dots = \text{mdc}(r_{n-2}, r_{n-1}) = r_{n-1}$.

A tabela a seguir representa um esquema prático para o cálculo de um $\text{mdc}(a, b)$. No momento em que numa das sucessivas divisões tivermos um resto $r_n = 0$, teremos $r_{n-1} = \text{mdc}(a, b)$.

Exemplo 2.8. *Pela tabela a seguir, temos $\text{mdc}(-72 + 56i, 25 - 33i) = 1 + i$.*

Exemplo 2.9. *Para $a = 1250 + 885i$ e $b = 720 + 256i \in \mathbb{Z}[i]$, temos:*

2. DOMÍNIOS EUCLIDIANOS

k	0	1	2	3	4	\dots	$n-2$	$n-1$	n
r_k	$r_0 = a$	$r_1 = b$	r_2	r_3	r_4	\dots	r_{n-2}	r_{n-1}	$r_n = 0$
q_k	—	q_1	q_2	q_3	q_4	\dots	q_{n-2}	q_{n-1}	—

Figura 1.1: $mdc(72 + 56i, 25 + 33i)$

k	0	1	2	3	4	5	6
r_k	$72+56i$	$25+33i$	$-11+15i$	$6-4i$	$-3+i$	$1+i$	0
q_k		$2-i$	$1-2i$	$-2+i$	$-2+i$	$-1+2i$	Acabou

Fonte: Os autores

Figura 1.2: $mdc(1250 + 885i, 720 + 256i)$

k	0	1	2	3	4	5	6	7	8	9	10
r_k	$1250+885i$	$720+256i$	$66-347i$	$26+124i$	$20+51i$	$-14+22i$	$-10+i$	4	$-2+i$	-1	0
q_k		$2+i$	$2i$	$-3-i$	2	$1-2i$	$2-2i$	-2	$-2-i$	$2-i$	Acabou

Fonte: Os autores

Logo, $mdc(1250 + 885i, 720 + 256i) = -1$, ou seja, $1250 + 885i$ e $720 + 256i$ são coprimos.

Teorema 2.10. (Teorema de Bezout) *Sejam A um domínio euclidiano e $a, b \in A$. Então, existem $s, t \in A$ (chamadas de constantes de Bezout) tais que $as + bt = mdc(a, b)$.*

Demonstração:

Faremos uma prova algorítmica e recursiva. Consideremos a notação (para restos e quocientes) e os cálculos feitos na Observação 2.7, bem como as seguintes fórmulas de recorrência:

$$s_0 = 1 \text{ e } t_0 = 0;$$

$$s_1 = 0 \text{ e } t_1 = 1;$$

$$s_k = s_{k-1}(-q_{k-1}) + s_{k-2} \text{ e } t_k = t_{k-1}(-q_{k-1}) + t_{k-2}, \quad \forall k \geq 2.$$

2. DOMÍNIOS EUCLIDIANOS

1. Se $r_2 = 0$, então $\text{mcd}(a, b) = r_1 = 0r_0 + 1r_1$. Neste caso, $s = 0$ e $t = 1$, i. é, $s = s_1$ e $t = t_1$.
2. Se $r_2 \neq 0$ e $r_3 = 0$, então $\text{mcd}(a, b) = r_2 = r_0 - q_1r_1$. Neste caso, $s = 1 = s_2$ e $t = -q_1 = t_2$.
3. Se $r_3 \neq 0$ e $r_4 = 0$ então $\text{mcd}(a, b) = r_3 = r_1 - q_2r_2 = r_1 - q_2(r_0 - q_1r_1) = -q_2r_0 + (1 + (-q_1)(-q_2))r_1$. Neste caso, $s = -q_2$ e $t = (-q_1)(-q_2) + 1$, ou seja, $s = s_2(-q_2) + s_1 = s_3$ e $t = t_2(-q_2) + t_1 = t_3$.
4. Se necessário, esse processo pode ser repetido e paramos quando $r_n = 0$. Daí obtemos $\text{mcd}(a, b) = r_{n-1} = as + bt$, onde $s = s_{n-2}(-q_{n-2}) + s_{n-3} = s_{n-1}$ e $t = t_{n-2}(-q_{n-2}) + t_{n-3} = t_{n-1}$. □

A demonstração anterior pode ser melhor visualizada numa tabela como a seguir.

k	0	1	2	...	k	...	$n-1$	n
r_k	$r_0 = a$	$r_1 = b$	r_2	...	r_k	...	r_{n-1}	$r_n = 0$
q_k	—	q_1	q_2	...	q_k	...	q_{n-1}	—
s_k	1	0	1	...	$s_{k-1}(-q_{k-1}) + s_{k-2}$...	$s_{n-2}(-q_{n-2}) + s_{n-3}$	—
t_k	0	1	$-q_1$...	$t_{k-1}(-q_{k-1}) + t_{k-2}$...	$t_{n-2}(-q_{n-2}) + t_{n-3}$	—

Exemplo 2.11. Em $\mathbb{Z}[i]$, consideremos $a = 132 + 88i$ e $b = 42 + 18i$. Pela tabela a seguir, temos que $\text{mcd}(132 + 88i, 42 + 18i) = 2 - 2i$ e as constantes de Bezout são $s = 4 + i$ e $t = -13 - 6i$.

2. DOMÍNIOS EUCLIDIANOS

Figura 1.3: mdc e constantes de Bezout para $132 + 88i$ e $42 + 18i$

k	0	1	2	3	4	5
r_k	$132+88i$	$42+18i$	$24-8i$	$10+2i$	$2-2i$	0
q_k		$3+i$	$1+i$	$2-i$	$2+3i$	Acabou
s_k	1	0	1	$-1-i$	$4+i$	Acabou
t_k	0	1	$-3-i$	$3+4i$	$-13-6i$	Acabou

Fonte: Os autores

Exemplo 2.12. Observe na tabela a seguir que o mdc de dois inteiros gaussianos pode ser um número inteiro e as constantes de Bezout não serem números inteiros.

Figura 1.4: mdc e constantes de bezout para $132 + 88i$ e $52 + 32i$

k	0	1	2	3	4	5	6
r_k	$132+88i$	$52+32i$	$-24-8i$	$12-8i$	$-4-4i$	4	0
q_k		3	$-2-i$	$-1-i$	$2i$	$-1-i$	Acabou
s_k	1	0	1	$2+i$	$2+3i$	$8-3i$	Acabou
t_k	0	1	-3	$-5-3i$	$-5-8i$	$-21+7i$	Acabou

Fonte: Os autores

Temos que $mdc(132 + 88i, 52 + 32i) = 4$ e as constantes de Bezout são $s = 8 - 3i$ e $t = -21 + 7i$.

Corolário 2.13. Sejam A um domínio euclidiano e $a, b, c \in A$. Então $mdc(ca, cb) = c \cdot mdc(a, b)$.

Demonstração:

Seja $d = mdc(a, b)$. Como $d|a$ e $d|b$, segue da Proposição 1.6(iii) que $cd|ac$ e $cd|bc$. Mais ainda, pelo Teorema de Bezout, existem $s, t \in A$ tais que $d = as + bt$. Daí, $cd = cas + cbt$. Agora, se $d' \in A$ é tal que $d'|ac$ e $d'|bc$, então pela Proposição 1.6(iv), $d'|acs + bcs = cd$. \square

3. EQUAÇÕES DIOFANTINAS EM DOMÍNIOS EUCLIDIANOS

Observação 2.14. *Sejam A um domínio euclidiano e $a, b \in A$ tais que*

$d = \text{mdc}(a, b) \neq 0$. Então $a = d \frac{a}{d}$ e $b = d \frac{b}{d}$ e pelo corolário anterior, $d = \text{mdc}(a, b) = \text{mdc}\left(d \frac{a}{d}, d \frac{b}{d}\right) = d \cdot \text{mdc}\left(\frac{a}{d}, \frac{b}{d}\right)$. Como A é domínio e $d \neq 0$, temos $\text{mdc}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Corolário 2.15. *Sejam A um domínio euclidiano e $a, b, c \in A$ tais que $\text{mdc}(a, b) = 1$ e $a|bc$, então $a|c$.*

Demonstração:

De fato, se $\text{mdc}(a, b) = 1$, então pelo Corolário 2.13 $\text{mdc}(ac, bc) = c$. Como $a|ac$ e $a|bc$, temos da Definição 1.7(ii) que $a|c$. \square

3 Equações Diofantinas em Domínios Euclidianos

Sejam A um domínio euclidiano e $a, b \in A$. Pelo que vimos na seção anterior, existem $s, t \in A$ tais que $as + bt = d$. Isso significa que a equação linear $aX + bY = \text{mdc}(a, b)$ tem solução em A . De modo mais geral, temos:

Definição 3.1. *Sejam A um domínio e $a, b, c \in A$ elementos não nulos. Uma equação do tipo*

$$aX + bY = c \tag{1.1}$$

é chamada de Equação Diofantina Linear sobre A nas variáveis X e Y . Os elementos a e b são chamados coeficientes e c de termo independente. Se existem $x, y \in A$ tais que $ax + by = c$, dizemos que (1.1) tem solução (em A).

Em cursos de Teoria dos Números, é comum se estudar equações diofantinas do tipo (1.1), com $a, b, c \in \mathbb{Z}$. Nosso objetivo nessa seção é estudar essas equações sobre um domínio euclidiano qualquer e aplicar esta teoria a equações com coeficientes em $\mathbb{Z}[i]$.

Proposição 3.2. *Sejam A um domínio euclidiano, $a, b, c \in A$ e $d = \text{mdc}(a, b) \neq 0$. Uma equação diofantina $aX + bY = c$ tem solução em A se e somente se $d|c$.*

3. EQUAÇÕES DIOFANTINAS EM DOMÍNIOS EUCLIDIANOS

Em particular, se a e b são coprimos, então para todo $c \in A$, $aX + bY = c$ tem solução em A .

Demonstração:

Suponhamos que $aX + bY = c$ tenha solução em A . Então, existirão $x, y \in A$ tais que $ax + by = c$. Como $d|a$ e $d|b$, segue da Proposição 1.6(iv) que $d|c$. Reciprocamente, se $d|c$ então, $c = d\frac{c}{d}$. Pelo Teorema de Bezout, existem $s, t \in A$, tais que $as + bt = d$. Multiplicando ambos os lados por $\frac{c}{d}$, obtemos $a\left(\frac{c}{d}s\right) + b\left(\frac{c}{d}t\right) = d\frac{c}{d} = c$, e a equação $aX + bY = c$ tem solução em A . \square

Note que podemos encontrar algoritmicamente uma solução de $aX + bY = c$, quando $d|c$. De fato, através de divisões sucessivas, podemos encontrar $s, t \in A$ tais que $as + bt = d$. Então, $x_0 = s\frac{c}{d}, y_0 = t\frac{c}{d}$ é uma solução em A , chamada uma *solução inicial*.

Teorema 3.3. *Sejam A um domínio euclidiano, $d = \text{mdc}(a, b) \neq 0$ e $aX + bY = c$ uma equação diofantina em A tal que $d|c$. Escrevendo $d = as + bt$, com $s, t \in A$, temos:*

1. $x_0 = \frac{c}{d}s, y_0 = \frac{c}{d}t$ é solução $aX + bY = c$;
2. Para todo $z \in A$, $x = x_0 + \frac{b}{d}z, y = y_0 - \frac{a}{d}z$ é solução de $aX + bY = c$;
3. Se x', y' é outra solução de $aX + bY = c$, então existe $z \in A$ tal que $x' = x_0 + \frac{b}{d}z, y' = y_0 - \frac{a}{d}z$.

Demonstração:

1. Segue da Proposição 3.2.
2. Substituindo $x = x_0 + \frac{b}{d}z, y = y_0 - \frac{a}{d}z$ na equação $aX + bY = c$, verificamos que é solução.
3. Sejam $x', y' \in A$ uma solução de $aX + bY = c$. Escrevemos $a_1 = \frac{a}{d}$ e $b_1 = \frac{b}{d}$.

4. APLICAÇÃO: EQUAÇÕES DIOFANTINAS SOBRE $\mathbb{Z}[I]$

Então

$$\begin{aligned}ax' + by' = ax_0 + by_0 &\Rightarrow a(x' - x_0) = b(y' - y_0) \\ &\Rightarrow da_1(x' - x_0) = db_1(y_0 - y') \\ &\Rightarrow a_1(x' - x_0) = b_1(y_0 - y'), \text{ pois } A \text{ é domínio} \\ &\Rightarrow b_1 | a_1(x' - x_0) \\ &\Rightarrow b_1 | (x' - x_0), \text{ pelo Corolário 2.15} \\ &\Rightarrow x' - x_0 = b_1z, \text{ para algum } z \in A \\ &\Rightarrow x' = x_0 + b_1z, \text{ para algum } z \in A.\end{aligned}$$

Substituindo $x' - x_0$ por b_1z em $a_1(x' - x_0) = b_1(y_0 - y')$ obtemos $a_1b_1z = b_1(y_0 - y')$, donde $y = y_0 - a_1z$, pois A é domínio. Logo, $x' = x_0 + \frac{b}{d}z$ e $y' = y_0 - \frac{a}{d}z$. \square

4 Aplicação: Equações Diofantinas sobre $\mathbb{Z}[i]$

Nesta seção, vamos aplicar a teoria que vimos anteriormente para estudar equações diofantinas sobre $\mathbb{Z}[i]$. Vejamos dois exemplos.

Exemplo 4.1. *Considere a equação $(52 + 32i)X + (25 + 15i)Y = 7 + i$. Neste caso, $a = r_0 = 52 + 32i$, $b = r_1 = 25 + 15i$ e $c = 7 + i$. Observando a tabela a seguir, vemos que $\text{mdc}(52 + 32i, 25 + 15i) = -1 - i$ e as constantes de Bezout são $s = s_4 = -8 + 5i$ e $t = t_4 = 10 - 17i$.*

4. APLICAÇÃO: EQUAÇÕES DIOFANTINAS SOBRE $\mathbb{Z}[I]$

Figura 1.5: mdc e constantes de Bezout para $52 + 32i$ e $25 + 15i$

k	0	1	2	3	4	5
r_k	$52+32i$	$15+25i$	$-3-3i$	$-2i$	$-1-i$	0
q_k		$2-i$	$-7-2i$	$1-i$	$1+i$	Acabou
s_k	1	0	1	$7+2i$	$-8+5i$	Acabou
t_k	0	1	$-2+i$	$-15+3i$	$10-17i$	Acabou

Fonte: Os autores

Agora, dividindo $c = 7 + i$ por $-1 - i = mdc(52 + 32i, 25 + 15i)$ obtemos o quociente $q = -4 + 3i$ e resto $r = 0$, ou seja, $-1 - i \mid 7 + i$. Logo, a equação diofantina dada tem solução e uma delas é $x_0 = \frac{c}{d}s = (-4 + 3i)(-8 + 5i) = 17 - 44i$ e $y_0 = \frac{c}{d}t = (-4 + 3i)(10 - 17i) = 11 + 98i$. As demais soluções são da forma $x_z = x_0 + \frac{c}{d}z = (17 - 44i) + (-42 + 10i)z$ e $y_z = y_0 - \frac{a}{d}z = (11 + 98i) + (20 + 5i)z$.

Exemplo 4.2. Vamos estudar a equação $(15 + 25i)X + (10 + 18i)Y = 5 - 5i$. A tabela seguir nos dá $mdc(15 + 25i, 10 + 18i) = 1 - i$ e constantes de Bezout são $s = s_4 = 5 - 2i$ e $t = t_4 = -7 + 3i$.

Figura 1.6: mdc e constantes de Bezout para $15 + 25i$ e $10 + 18i$

k	0	1	2	3	4	5
r_k	$15+25i$	$10+18i$	$5+7i$	$4i$	$1-i$	0
q_k		1	2	$2-i$	$-2+2i$	Acabou
s_k	1	0	1	-2	$5-2i$	Acabou
t_k	0	1	-1	3	$-7+3i$	Acabou

Fonte: Os autores

Como $1 - i \mid 5 - 5i$, a equação dada tem solução e uma delas é $x_0 = 5(5 - 2i) = 25 - 10i$ e $y_0 = 5(-7 + 3i) = -35 + 15i$. As demais soluções são da forma

5. CÁLCULOS EM $\mathbb{Z}[I]$ ATRAVÉS DE PLANILHAS ELETRÔNICAS

$x_z = (25 - 10i) + (-4 + 14i)z$ e $y_z = (-35 + 15i) + (5 - 20i)z$. Para $z = 1 + i$, obtemos $x_z = 7$ e $y_z = -10$. Logo, a equação $(15 + 25i)X + (10 + 18i)Y = 5 - 5i$ tem uma solução inteira.

5 Cálculos em $\mathbb{Z}[i]$ Através de Planilhas Eletrônicas

O algoritmo da divisão para inteiros gaussianos envolve diversos cálculos que podem nos levar a cometer erros e por consequência, não conseguirmos determinar o quociente e o resto corretamente. Como toda a teoria de equações diofantinas sobre domínios euclidianos depende basicamente do algoritmo da divisão, é de fundamental importância que tenhamos uma ferramenta que nos auxilie com os cálculos. Durante o desenvolvimento desse trabalho, as planilhas eletrônicas se mostraram bastante satisfatórias neste sentido. Isso se dá porque elas tem várias funções matemáticas que podem ser usadas para cálculos algébricos com números complexos, matrizes, etc. Em (LIBREOFFICE) encontra-se uma lista com várias funções pré-definidas do programa LibreOffice. Também há uma descrição e a sintaxe de cada função. Para acessar tais descrições, basta clicar no nome da função.

Para nós, a função “COMPLEXO” é uma das mais importantes. Ela converte um par ordenado de números reais em um número complexo. Sua sintaxe é: “COMPLEXO(NúmeroReal; INúm; Sufixo)”, onde a entrada “NúmeroReal” indica a parte real do número complexo e “INúm” indica a parte imaginária. A entrada “sufixo” pode ser deixada em branco. Portanto, se numa célula de uma planilha do LibreOffice escrevermos “=COMPLEXO(3;5)”, o retorno será o número complexo $3 + 5i$.

Nessa seção apresentamos uma gama de algoritmos que utilizam diversas funções pré-definidas do LibreOffice para criar novas funções. Como alguns destes algoritmos tem descrição muito longa (veja o Passo 4 do Algoritmo 5.1), o leitor poderá copiá-las da versão em PDF desse trabalho e colar numa planilha eletrônica. Para tanto, é preciso ficar atento a quatro coisas. Primeiro, o leitor deve copiar linha por linha de cada passo dos algoritmos e colar numa planilha eletrônica. Segundo, em alguns

5. CÁLCULOS EM $\mathbb{Z}[I]$ ATRAVÉS DE PLANILHAS ELETRÔNICAS

algoritmos (veja Passo 4 do Algoritmo 5.1) aparecerá a palavra “IMAGINÁRIO”. Ao copiar e colar, o resultado será “IMAGINARIO”, ou seja, o acento agudo do “A” não se manterá do PDF para o LibreOffice. Isso tem que ser corrigido manualmente pelo leitor na planilha. Terceiro, outro elemento que não se mantém são as palavras com aspas. No Algoritmo 5.1, por exemplo, aparece “Acabou”. Neste caso, o ato de copiar e colar do PDF para o LibreOffice não manterá as aspas de modo que o LibreOffice as reconheça. É preciso que o leitor apague as aspas copiadas e digite-as na planilha. Por último, é preciso garantir que não haja espaços nas fórmulas das planilhas LibreOffice.

5.1 Divisão em $\mathbb{Z}[i]$

Para determinar o quociente e o resto da divisão de dois elementos de $\mathbb{Z}[i]$ via uma planilha eletrônica, procedemos de acordo com o seguinte algoritmo:

Algoritmo 5.1.

Passo 1: Escolha $a = a_1 + a_2i$ e $b = b_1 + b_2i$ em $\mathbb{Z}[i]$, com $b \neq 0$ e abra uma planilha em branco;

Passo 2: Na célula B1 digite: =COMPLEXO(a_1 ; a_2)

Passo 3: Na célula C1 digite: =COMPLEXO(b_1 ; b_2)

Passo 4: Na célula C2 digite:

*=SE(C1=COMPLEXO(0;0);“Acabou”;COMPLEXO(SE(ABS(ARREDONDAR.PARA.BAIXO
(IMREAL(IMDIV(B1;C1)));0)-
IMREAL(IMDIV(B1;C1)))>0,5;ARREDONDAR.PARA.CIMA(IMREAL
(IMDIV(B1;C1)));0);ARREDONDAR.PARA.BAIXO(IMREAL(IMDIV(B1;C1)));0));SE
(ABS(ARREDONDAR.PARA.BAIXO(IMAGINÁRIO(IMDIV(B1;C1)));0)-
IMAGINÁRIO(IMDIV(B1;C1)))>0,5;ARREDONDAR.PARA.CIMA(IMAGINÁRIO
(IMDIV(B1;C1)));0);ARREDONDAR.PARA.BAIXO(IMAGINÁRIO(IMDIV(B1;C1)));0))))*

Passo 5: Na célula D1 digite: =IMSUBTR(B1;IMPROD(C2;C1))

5. CÁLCULOS EM $\mathbb{Z}[I]$ ATRAVÉS DE PLANILHAS ELETRÔNICAS

Resultado: As células C2 e D1 retornam, respectivamente, o quociente e o resto da divisão de a por b .

A figura a seguir ilustra o algoritmo anterior aplicado numa planilha eletrônica para $a = 75 + 41i$ e $b = 9 + 15i$. Obtemos o quociente $q = 4 - 2i$ e o resto é $r = 9 - i$.

Figura 1.7: Quociente e resto da divisão de $75 + 41i$ por $9 + 15i$

	A	B	C	D	E
1		75+41i	9+15i	9-i	
2			4-2i		
3					

Fonte: Os autores

A figura a seguir ilustra o contido na célula C2.

Figura 1.8: Função da célula C2

The screenshot shows a spreadsheet with the following data:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
1		75+41i	9+15i	9-i																
2			4-2i																	

The formula bar for cell C2 shows the following complex formula:

```
=SE(C1=COMPLEXO(0;0);"Acabou";COMPLEXO(SE(ABS(ARREDONDAR.PARA.BAIXO(IMREAL(IMDIV(B1;C1));0)-IMREAL(IMDIV(B1;C1)))>0,5;ARREDONDAR.PARA.CIMA(IMREAL(IMDIV(B1;C1));0);ARREDONDAR.PARA.BAIXO(IMREAL(IMDIV(B1;C1));0));SE(ABS(ARREDONDAR.PARA.BAIXO(IMAGINÁRIO(IMDIV(B1;C1));0)-IMAGINÁRIO(IMDIV(B1;C1)))>0,5;ARREDONDAR.PARA.CIMA(IMAGINÁRIO(IMDIV(B1;C1));0);ARREDONDAR.PARA.BAIXO(IMAGINÁRIO(IMDIV(B1;C1));0))))
```

Fonte: Os autores

5.2 Cálculo do mdc em $\mathbb{Z}[i]$

Pelo Teorema de Bezout, para determinarmos o *mdc* entre dois elementos de um domínio euclidiano, podemos aplicar o algoritmo da divisão sucessivas vezes até encontrarmos um resto igual a 0. O resto anterior será o *mdc* procurado. Portanto, podemos usar uma tabela do LibreOffice para determinar o *mdc* de quaisquer dois inteiros gaussianos a e b , aplicando o seguinte algoritmo:

5. CÁLCULOS EM $\mathbb{Z}[I]$ ATRAVÉS DE PLANILHAS ELETRÔNICAS

Algoritmo 5.2.

Passo 1: Escolha $a = a_1 + a_2i, b = b_1 + b_2i \in \mathbb{Z}[i]$ com $b \neq 0$ e aplique o Algoritmo 5.1;

Passo 2: Arraste a célula C2 sobre as células D2, E2, F2, G2, etc;

Passo 3: Arraste a célula D1 sobre as células E1, F1, G1, H1, etc.

Resultado: Quando alguma célula da linha 1 retornar zero, o mdc de a e b será o elemento da linha 1 imediatamente anterior a essa.

A figura a seguir mostra os cálculos que determinam $mdc(75+41i, 9+15i)$ utilizando os algoritmo anterior. As células em azul são os sucessivos restos, enquanto que as células em verde são os respectivos quocientes. Como a célula G1 retornou 0, temos o retorno da célula F1 é o $mdc(75 + 41i, 9 + 15i)$, ou seja, $mdc(75 + 41i, 9 + 15i) = 1 - i$.

Figura 1.9: Cálculo de $mdc(75 + 41i, 9 + 15i)$

	A	B	C	D	E	F	G
1		75+41i	9+15i	9-i	-2-2i	1-i	0
2			4-2i	1+2i	-2+2i	-2i	Acabou
3		1	0	1	-1-2i	-5-2i	Acabou
4		0	1	-4+2i	9+6i	26-4i	Acabou
5		7+i	1-i	0			
6			3+4i				

Fonte: Os autores

5.3 Constantes de Bezout em $\mathbb{Z}[i]$

O algoritmo a seguir nos mostra como é possível determinar através de uma tabela do LibreOffice as constantes Bezout para um par $a, b \in \mathbb{Z}[i]$, ou seja, $s, t \in \mathbb{Z}[i]$ tais que $as + bt = mdc(a, b)$. Para isso, utilizamos as fórmulas recursivas dadas na demonstração do Teorema de Bezout (ver Passos 4 e 5).

Algoritmo 5.3.

Passo 1: Escolha $a = a_1 + a_2i, b = b_1 + b_2i \in \mathbb{Z}[i]$ e aplique o Algoritmo 5.2;

Passo 2: Nas células B3 e C3 digite 1 e 0, respectivamente;

5. CÁLCULOS EM $\mathbb{Z}[I]$ ATRAVÉS DE PLANILHAS ELETRÔNICAS

Passo 3: Nas células B4 e C4 digite 0 e 1, respectivamente;

Passo 4: Na célula D3 digite: =SE(D1=COMPLEXO(0;0);"Acabou";IMSUBTR(B3; IMPROD(C2;C3)))

Passo 5: Na célula D4 digite: =SE(D1=COMPLEXO(0;0);"Acabou";IMSUBTR(B4; IMPROD(C2;C4)))

Passo 6: Arraste a célula D3 sobre as células E3, F3, G3, etc;

Passo 7: Arraste a célula D4 sobre as células E4, F4, G4, etc;

Resultado: Quando em alguma célula da linha 3 (linha 4) aparecer a palavra "Acabou", a célula imediatamente anterior será o valor de s (valor de t).

Na figura a seguir vemos como são obtidas as constantes de Bezout para $75 + 41i$ e $9 + 15i$. Temos que $s = -5 - 2i$ e $t = 26 - 4i$.

Figura 1.10: Constantes de Bezout para $75 + 41i$ e $9 + 15i$.

	A	B	C	D	E	F	G
1		$75+41i$	$9+15i$	$9-i$	$-2-2i$	$1-i$	0
2			$4-2i$	$1+2i$	$-2+2i$	$-2i$	Acabou
3		1	0	1	$-1-2i$	$-5-2i$	Acabou
4		0	1	$-4+2i$	$9+6i$	$26-4i$	Acabou
5		$7+i$	$1-i$	0			
6			$3+4i$				
7	s	$-5-2i$					
8	t	$26-4i$					

Fonte: Os autores

5.4 Soluções de Equações Diofantinas em $\mathbb{Z}[i]$

Consideremos uma equação diofantina $aX + bY = c$ com $a = a_1 + a_2i$, $b = b_1 + b_2i$ e $c = c_1 + c_2i$ em $\mathbb{Z}[i]$. Para determinarmos uma solução $x_0, y_0 \in \mathbb{Z}[i]$ através de uma planilha eletrônica, aplicamos o algoritmo a seguir.

Algoritmo 5.4.

Passo 1: Aplique o Algoritmo 5.3 para a e b ;

5. CÁLCULOS EM $\mathbb{Z}[I]$ ATRAVÉS DE PLANILHAS ELETRÔNICAS

Passo 2: Na célula B5 digite: =COMPLEXO(c_1 ; c_2)

Passo 3: Na célula C5 digite:

=SE(D1=COMPLEXO(0;0);IMPROD(1;C1);SE(E1=COMPLEXO(0;0);IMPROD(1;D1);
SE(F1=COMPLEXO(0;0);IMPROD(1;E1);SE(G1=COMPLEXO(0;0);IMPROD(1;F1);
SE(H1=COMPLEXO(0;0);IMPROD(1;G1);SE(I1=COMPLEXO(0;0);IMPROD(1;H1);
SE(J1=COMPLEXO(0;0);IMPROD(1;I1);SE(L1=COMPLEXO(0;0);IMPROD(1;K1);
SE(M1=COMPLEXO(0;0);IMPROD(1;L1);SE(N1=COMPLEXO(0;0);IMPROD(1;M1);
SE(O1=COMPLEXO(0;0);IMPROD(1;N1);SE(P1=COMPLEXO(0;0);IMPROD(1;O1);0))))))))))

Passo 4: Copie a célula C2 e cole-a na célula C6;

Passo 5: Copie a célula D1 e cole-a na célula D5;

Passo 6: Na célula B7 digite:

=SE(D3="Acabou";IMPROD(1;C3);SE(E3="Acabou";IMPROD(1;D3);
SE(F3="Acabou";IMPROD(1;E3);SE(G3="Acabou";IMPROD(1;F3);
SE(H3="Acabou";IMPROD(1;G3);SE(I3="Acabou";IMPROD(1;H3);
SE(K3="Acabou";IMPROD(1;J3);SE(L3="Acabou";IMPROD(1;K3);
SE(M3="Acabou";IMPROD(1;L3);SE(N3="Acabou";IMPROD(1;M3);
SE(O3="Acabou";IMPROD(1;N3);0))))))))))

Passo 7: Copie a célula B7 e cole-a na célula B8;

Passo 8: Na célula B9 digite: =SE(D5=COMPLEXO(0;0);IMPROD(C6;B7);"Eq. Sem Sol")

Passo 9: Na célula B10 digite: =SE(D5=COMPLEXO(0;0);IMPROD(C6;B8);"Eq. Sem Sol")

Resultado: Se nas células B9 e B10 aparecerem a expressão "Eq Sem Sol.", então a equação $aX + bY = c$ não tem solução. Caso contrário, os inteiros gaussianos que aparecem serão, respectivamente, soluções iniciais x_0 e y_0 da equação.

Observação 5.5. Cabe aqui explicar o que os passo do algoritmo anterior retornam.

- O passo 3 desloca o $\text{mdc}(a, b)$ da linha 1 para a célula C5.

5. CÁLCULOS EM $\mathbb{Z}[I]$ ATRAVÉS DE PLANILHAS ELETRÔNICAS

- Os passos 4 e 5 retornam, respectivamente, o quociente e o resto da divisão de c por $\text{mdc}(a, b)$.
- Os passos 6 e 7 deslocam as constantes de Bezout das linhas 3 e 4 para as células B7 e B8.
- Os passos 8 e 9 nos dão as soluções iniciais da equação, caso elas existam.
- O algoritmo identifica no passo 5 se o resto da divisão de c por $\text{mdc}(a, b)$ é igual ou diferente de 0. Caso tal resto não seja 0, o algoritmo fornece a resposta “Eq. Sem Sol.”, o que significa que a equação dada não tem solução.

Considere as equações $(75 + 41)X + (9 + 15i)Y = 7 + i$ e $(75 + 41)X + (9 + 15i)Y = 7 + 2i$. As próximas figuras mostram que a primeira equação tem solução $x_0 = -7 - 26i$, $y_0 = 94 + 92i$ e a segunda equação não tem solução.

Figura 1.11: $(75 + 41)X + (9 + 15i)Y = 7 + i$ tem solução

	A	B	C	D	E	F	G
1		75+41i	9+15i	9-i	-2-2i	1-i	0
2			4-2i	1+2i	-2+2i	-2i	Acabou
3		1	0	1	-1-2i	-5-2i	Acabou
4		0	1	-4+2i	9+6i	26-4i	Acabou
5		7+i	1-i	0			
6			3+4i				
7	s	-5-2i					
8	t	26-4i					
9	x_0	-7-26i					
10	y_0	94+92i					

Fonte: Os autores

5. CÁLCULOS EM $\mathbb{Z}[I]$ ATRAVÉS DE PLANILHAS ELETRÔNICAS

Figura 1.12: $(75 + 41)X + (9 + 15i)Y = 7 + 2i$ não tem solução

	A	B	C	D	E	F	G
1		75+41i	9+15i	9-i	-2-2i	1-i	0
2			4-2i	1+2i	-2+2i	-2i	Acabou
3		1	0	1	-1-2i	-5-2i	Acabou
4		0	1	-4+2i	9+6i	26-4i	Acabou
5		7+2i	1-i	1			
6			2+4i				
7	s	-5-2i					
8	t	26-4i					
9	x_0	q. Sem Sol.					
10	y_0	q. Sem Sol.					

Fonte: Os autores

O próximo algoritmo visa determinar outras soluções de $aX + bY = c$ via uma planilha eletrônica. Estas soluções são determinadas via as fórmulas dadas pelo Teorema 3.3(iii).

Algoritmo 5.6.

Passo 1: Aplique o Algoritmo 5.4 para equação $aX + bY = c$;

Passo 2: Na célula B11 digite:

=COMPLEXO(SE(ABS(ARREDONDAR.PARA.BAIXO(IMREAL(IMDIV(B1;C5));0)

IMREAL(IMDIV(B1;C5)))>0,5;ARREDONDAR.PARA.CIMA(IMREAL(IMDIV(B1;C5));0);

ARREDONDAR.PARA.BAIXO(IMREAL(IMDIV(B1;C5));0));SE(ABS

(ARREDONDAR.PARA.BAIXO(IMAGINÁRIO(IMDIV(B1;C5));0)-

IMAGINÁRIO(IMDIV(B1;C5)))>0,5;ARREDONDAR.PARA.CIMA

(IMAGINÁRIO(IMDIV(B1;C5));0);ARREDONDAR.PARA.BAIXO

(IMAGINÁRIO(IMDIV(B1;C5));0)))

Passo 3: Na célula B12 digite:

=COMPLEXO(SE(ABS(ARREDONDAR.PARA.BAIXO(IMREAL(IMDIV(C1;C5));0)

IMREAL(IMDIV(C1;C5)))>0,5;ARREDONDAR.PARA.CIMA(IMREAL(IMDIV(C1;C5));0);

5. CÁLCULOS EM $\mathbb{Z}[I]$ ATRAVÉS DE PLANILHAS ELETRÔNICAS

ARREDONDAR.PARA.BAIXO(IMREAL(IMDIV(C1;C5));0));SE(ABS
(ARREDONDAR.PARA.BAIXO(IMAGINÁRIO(IMDIV(C1;C5));0)-
IMAGINÁRIO(IMDIV(C1;C5)))>0,5;ARREDONDAR.PARA.CIMA
(IMAGINÁRIO
(IMDIV(C1;C5));0);ARREDONDAR.PARA.BAIXO(IMAGINÁRIO(IMDIV(C1;C5));0)))

Passo 4: Escolha um inteiro gaussiano $z = z_1 + z_2i$ e na célula B13 digite: =COMPLEXO($z_1; z_2$)

Passo 5: Na célula B14 digite: =IMSOMA(B9;IMPROD(B12;B13))

Passo 6: Na célula B15 digite: =IMSUBTR(B10;IMPROD(B11;B13))

Resultado: As células B14 e B15 retornam valores de x e y que são soluções de $aX + bY = c$.

Observação 5.7. No Algoritmo 5.6, os passos 2 e 3 calculam $\frac{a}{d}$ e $\frac{b}{d}$, respectivamente. Os passos 5 e 6 determinam, respectivamente, soluções $x = x_0 + \frac{b}{d}z$ e $y = y_0 - \frac{a}{d}z$ para cada $z \in \mathbb{Z}[i]$ que for digitado na célula B13.

Exemplo 5.8. A próxima figura mostra todos os algoritmos descritos nesta seção serem aplicados para a equação $(75 + 41i)X + (9 + 15i)Y = 7 + i$. Temos que $\text{mdc}(75 + 41i, 9 + 15i) = 1 - i$ e $1 - i \mid 7 + i$. Também, $x_0 = -7 - 26i$, $y_0 = 94 + 92i$, $\frac{a}{d} = 17 + 58i$ e $\frac{b}{d} = -3 + 12i$. Por fim, $x = -28 + 7i$ e $y = 101 - 99i$ são soluções obtidas a partir de $z = 3 + i$.

5. CÁLCULOS EM $\mathbb{Z}[I]$ ATRAVÉS DE PLANILHAS ELETRÔNICAS

Figura 1.13: Outra solução da equação $(75 + 41)X + (9 + 15i)Y = 7 + i$

	A	B	C	D	E	F	G
1		75+41i	9+15i	9-i	-2-2i	1-i	0
2			4-2i	1+2i	-2+2i	-2i	Acabou
3		1	0	1	-1-2i	-5-2i	Acabou
4		0	1	-4+2i	9+6i	26-4i	Acabou
5		7+i	1-i	0			
6			3+4i				
7	s	-5-2i					
8	t	26-4i					
9	x_0	-7-26i					
10	y_0	94+92i					
11	a/d	17+58i					
12	b/d	-3+12i					
13	z	3+i					
14	x	-28+7i					
15	y	101-99i					

Fonte: Os autores

Conclusão

Determinar um *mdc* entre dois elementos de um domínio qualquer pode ser trabalhoso. Isso se deve ao fato da definição de *mdc* não apresentar um possível candidato. Ela apenas diz que d é um *mdc* de a e b , se d é um divisor comum de a e b e qualquer outro divisor comum de a e b divide d . Pela Observação 2.7, quando estamos trabalhando com domínios euclidianos, isso fica um pouco mais fácil, porém, podemos ter dificuldades nos cálculos das sucessivas divisões. Por isso, um programa de computador que realize tais cálculos é crucial. O mesmo vale para determinarmos as constantes de Bezout e as soluções de equações diofantinas.

Nesse sentido, os algoritmos para $\mathbb{Z}[i]$ que apresentamos na Seção 5 são interessantes e muito práticos, pois eles podem ser aplicados praticamente em qualquer computador, *smartphone* ou *tablet* sem a necessidade do conhecimento de uma linguagem de programação específica. Basta ter instalado o *Office* ou o *LibreOffice* e seguir os passos apresentados nos algoritmos da Seção 5. Observamos que uma vez programada uma tabela conforme descrevemos anteriormente, só é preciso alterar as células B1, C1, B5 e B13 para determinar diferentes *mdc's* ou resolver diferentes equações diofantinas.

Durante o desenvolvimento desse trabalho, percebemos a falta de recursos computacionais simples, viáveis e assecíveis para a realização dos cálculos algébricos em $\mathbb{Z}[i]$ que necessitávamos. Com essa necessidade passamos considerar as planilhas do LibreOffice como uma possibilidade de ferramenta. Nós as escolhemos por vários motivos, dentre eles a facilidade de acesso e manuseio pelos usuários, bem como a existência de algumas funções pré-definidas, por exemplo, multiplicação, adição e

5. CÁLCULOS EM $\mathbb{Z}[I]$ ATRAVÉS DE PLANILHAS ELETRÔNICAS

subtração de números complexos. Por um lado, para nós o mais importante foi a programação da divisão euclidiana em $\mathbb{Z}[i]$. Por outro lado, como pode-se perceber no Passo 4 do Algoritmo 5.1, esta programação foi a mais difícil, pois envolve diversos comandos lógicos.

Nós acreditamos que um aplicativo de celular como aquele desenvolvido em (DOS SANTOS, 2016) seria muito mais atrativo. Porém, ele se limita a *smartphones* com sistema *Android*. Ressaltamos ainda que as planilhas que apresentamos também podem ser usadas para resolver equações diofantinas clássicas, ou seja, com coeficientes em \mathbb{Z} . Para tanto, basta zerar a parte imaginária dos coeficientes e termo independente da equação.

Esperamos que estudantes e professores de graduação e pós-graduação se inspirem em utilizar as planilhas do LibreOffice para outras atividades. Por exemplo, em (DE JESUS, 2018) os autores descrevem como tais planilhas podem ser úteis para o estudo de Geometria Analítica. Elas são viáveis para resolver sistemas lineares com poucas incógnitas através da Regra de Cramer, pois essa regra depende apenas de cálculos de determinantes e quociente de números reais, que podem ser realizados facilmente em uma planilha eletrônica. Além disso, acreditamos que equações diofantinas sobre outros domínios euclidianos do tipo $\mathbb{Z}[\alpha]$, como descritos no Exemplo 1.2, possam ser estudados com o auxílio de tabelas do LibreOffice.

Referências Bibliográficas

- [1] LIBREOFFICE. **Funções de suplemento (add-in), lista das funções de análise - parte 2**. Disponível em: <https://help.libreoffice.org/3.3/Calc/Add-in_Functions,_List_of_Analysis_Functions_Part_Two/pt-BR>. Acesso em 17 de março de 2020.
- [2] SEMANTIC SCHOLAR. **SOLUTION OF SIMPLE DIOPHANTINE EQUATIONS BY MEANS OF MATLAB**. Disponível em: <<https://www.semanticscholar.org/paper/SOLUTION-OF-SIMPLE-DIOPHANTINE-EQUATIONS-BY-MEANS/6ec1d1d98bb1044fb0683540474b3dadca04bfe0>>. Acesso em: 25 de setembro de 2019.
- [3] ANDERSON, M. e FEIL, T. **A First Course in Abstract Algebra: Rings, Groups and Fields**. 3ª Edição. New York: CRC Press, 2015.
- [4] GATHEN, J. V. Z. e GERHARD, J. **Modern Computer Algebra**. 3ª Edição. New York: Cambridge University Press, New York, 2013.
- [5] HEFEZ, A. **Aritmética**, 2ª Edição. Rio de Janeiro: SBM-Coleção PROFMAT, 2016.

- [6] MILIES, C. F. P. M. e COELHO, S. P. **Números**: Uma Introdução à Matemática. 3ª Edição 2 reimpr. São Paulo: Editora da USP, 2006.
- [7] DE JESUS, O. F. **O Uso de Planilhas do Excel Aplicadas a Tópicos de Geometria Analítica**. 2018, 243f. Dissertação (Matemática) – Universidade Federal de Goiás, Jataí, 2018.
- [8] DOS SANTOS, L. A. **Equações diofantinas lineares: um aplicativo para a resolução**. 2016, 65f. Trabalho de Conclusão de Curso (Licenciatura em Matemática) – Universidade Estadual Paulista, Guaratinguetá, 2016.