UNIVERSIDADE FEDERAL DE SÃO CARLOS
CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA
DEPARTAMENTO DE MATEMÁTICA

RAPHAEL ELIAS TOLEDO FERREIRA

UMA INTRODUÇÃO AOS INTEIROS GAUSSIANOS

SÃO CARLOS
2021

RAPHAEL ELIAS TOLEDO FERREIRA

UMA INTRODUÇÃO AOS INTEIROS GAUSSIANOS

Monografia apresentada ao Curso de Licenciatura em Matemática da Universidade Federal de São Carlos.

Orientador: Prof. Dr. Wladimir Seixas

SÃO CARLOS
2021

Ferreira, Raphael Elias Toledo

Uma introdução aos inteiros gaussianos / Raphael Elias Toledo Ferreira -- 2021.
90f.

TCC (Graduação) - Universidade Federal de São Carlos, campus São Carlos, São Carlos
Orientador (a): Wladimir Seixas
Banca Examinadora: João Carlos Vieira Sampaio, Luciene Nogueira Bertoncello
Bibliografia

1. Axiomas de Peano. 2. Teoria dos números. 3. Inteiros gaussianos. I. Ferreira, Raphael Elias Toledo. II. Título.

Ficha catalográfica desenvolvida pela Secretaria Geral de Informática (SIn)

DADOS FORNECIDOS PELO AUTOR

Bibliotecário responsável: Ronildo Santos Prado - CRB/8 7325

FUNDAÇÃO UNIVERSIDADE FEDERAL DE SÃO CARLOS

COORDENAÇÃO DOS CURSOS DE GRADUAÇÃO EM MATEMÁTICA - CCM/CCET
Rod. Washington Luís km 235 - SP-310, s/n - Bairro Monjolinho, São Carlos/SP, CEP 13565-905
Telefone: (16) 33518221 - http://www.ufscar.br

DP-TCC-FA nº 29/2021/CCM/CCET

Graduação: Defesa Pública de Trabalho de Conclusão de Curso

Folha Aprovação (GDP-TCC-FA)

FOLHA DE APROVAÇÃO

RAPHAEL ELIAS TOLEDO FERREIRA

UMA INTRODUÇÃO AOS INTEIROS GAUSSIANOS

Trabalho de Conclusão de Curso

Universidade Federal de São Carlos – Campus São Carlos

São Carlos, 25 de novembro de 2021

ASSINATURAS E CIÊNCIAS

Cargo/Função	Nome Completo
Orientador	Wladimir Seixas
Membro da Banca 1	João Carlos Vieira Sampaio
Membro da Banca 2	Luciene Nogueira Bertoncello

Documento assinado eletronicamente por **Wladimir Seixas**, **Professor(a) do Magistério Superior**, em 30/11/2021, às 15:26, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Luciene Nogueira Bertoncello**, **Professor(a) Adjunto(a)**, em 30/11/2021, às 18:14, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Joao Carlos Vieira Sampaio**, **Professor(a) do Magistério Superior**, em 30/11/2021, às 19:16, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.ufscar.br/autenticacao, informando o código verificador **0546177** e o código CRC **776CC009**.

AGRADECIMENTOS

Gostaria de agradecer a todos que me ajudaram nessa jornada: Deus, meus pais, meus avós, e tantos outros familiares. Também agradeço ao meu orientador, professores e colegas, que compartilharam seu conhecimento e entusiasmo pela Matemática.

RESUMO

Esta monografia apresenta os princípios da teoria dos números, estabelecendo de maneira formal fatos aritméticos importantes que caracterizam sistemas em questão. Procurou desenvolver a teoria de maneira axiomática, desde os princípios de conjuntos, que constituem a ferramenta principal para o rigor matemático. Ainda, o presente texto faz uma exposição de diferentes domínios de integridade, que apresentam muitas semelhanças, embora para cada um desses existam considerações e cuidados específicos a se fazer. A partir desse desenvolvimento de sistemas análogos ao conjunto dos números inteiros, é possível contemplar uma série de fatos e estruturas interessantes, bem como promover um bom entendimento de propriedades convenientes para serem trabalhadas em mais contextos. O texto também aborda o conjunto dos inteiros gaussianos, que ainda não é tão frequentemente trabalhado, mas apresenta um potencial interessante para se estudar os números inteiros.

Palavras-chave: Conjuntos sucessores. Axiomas de Peano. Teoria dos números. Inteiros gaussianos.

ABSTRACT

This monograph presents the principles of number theory, formally establishing important arithmetic facts that characterize the systems in question. It sought to develop theory in an axiomatic way, from the principles of sets, which constitute the main tool for mathematical rigor. Furthermore, this text presents different domains of integrity, which have many similarities, although for each of these there are specific considerations and precautions to be taken. From this development of systems analogous to the set of whole numbers, it is possible to contemplate a series of interesting facts and structures, as well as to promote a good understanding of properties suitable to be worked on in more contexts. The text also deals with the set of Gaussian integers, which is still not so often worked on, but presents an interesting potential for studying integers.

Keywords: Successor sets. Peano Axioms. Number theory. Gaussian integers.

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

A compreensão da lógica e da estrutura de um determinado sistema, passa muitas vezes pela comparação. De forma curiosa, o sistema dos números naturais pode ser utilizado para construir outros que preservam suas propriedades, com certas variações. A partir da análise da essência do que é preservado, podemos contemplar as ideias centrais da lógica desse sistema. Ainda, é possível estender um sistema com mais propriedades e facilitar a exposição de determinados fatos.

O presente trabalho procurou examinar de forma minuciosa as propriedades de cada sistema, fazendo uma exposição organizada e cuidadosa do desenvolvimento da teoria. Também foi dada maior atenção aos fatos mais importantes que dizem respeito a esses similares sistemas discretos.

Como um dos elementos que mais nos atrai à matemática é a exposição axiomática, procuramos desenvolver os conceitos desde à fundamentação lógica com conjuntos. A base utilizada foi a teoria dos conjuntos exposta em *Naive Set Theory* (HALMOS, 1998). A partir dessa referência, podemos estabelecer um fundamento bastante sólido para o formalismo.

Com efeito, a predileção deste trabalho foi trazer resultados centrais da teoria dos números da maneira mais didática e adequadamente formal possível, até chegarmos ao estudo dos números inteiros gaussianos. E fazer isso com uma discussão que trouxesse, de forma ampla, organização, significado, e contemplação aos elementos, mesmo que esses possam ser, às vezes, considerados “mais simples”.

Os inteiros gaussianos se mostram um objeto interessante para o estudo por formarem um domínio de integridade e apresentarem muitas semelhanças com a estrutura de inteiros, sendo inclusive possível decompô-los em fatores irredutíveis de uma forma única em certo sentido. A importância desse assunto se verifica por exemplo com a abordagem do mesmo na dissertação de Batista (2019), *A Teoria Elementar dos Inteiros de Gauss*.

2 O CONJUNTO DOS NÚMEROS NATURAIS

Começaremos nosso estudo a partir da construção dos Axiomas de Peano. A construção a seguir é exposta em *Naive Set Theory* (HALMOS, 1998). Faremos essa abordagem porque ela oferece uma boa compreensão a respeito do método axiomático, e também porque fornece um bom entendimento do Princípio da Indução Finita, esclarecendo significativamente o porquê deste princípio ser considerado um axioma; e como pensar situações mais gerais para as quais tal premissa não vale. Dessa forma, por meio de uma série de construções, seguiremos com a dedução dos Princípios de Peano.

Definição 2.1. Definimos **0**, **zero**, como o conjunto vazio. $0 = \{\}$.

Definição 2.2. Seja C um conjunto. Definimos $\boldsymbol{C^+}$, **o sucessor de C**, por: $C^+ = C \cup \{C\}$.

Exemplo 2.1.

a) Se $V = \{a, b\}$, então $V^+ = \{a, b, \{a, b\}\}$

b) $0^+ = 0 \cup \{0\} = \{\} \cup \{\{\}\} = \{\{\}\}$

Adiantando a exposição, os números naturais serão conjuntos específicos. E o conjunto dos Naturais será o agrupamento desses conjuntos específicos. Então, observamos que a definição de sucessor de um conjunto permite que falemos de sucessores de coisas que não são números, ou seja, de conjuntos que não são esses específicos. Afinal, não esperamos que todos os conjuntos sejam números. Entretanto, apesar do conceito sucessor ser definido em um contexto mais amplo, esse seria mais importante para a construção dos Naturais.

Axioma 2.1*[Axioma do Infinito] Existe um conjunto ao qual pertence o sucessor de cada um de seus elementos e o zero.*

Definição 2.3. Um conjunto com a propriedade acima é um **conjunto de sucessão**.

Proposição 2.1. *A interseção de qualquer família de conjuntos de sucessão é um conjunto de sucessão.*

Demonstração. Seja F uma família de conjuntos de sucessão. Naturalmente, $0 \in \bigcap F$. Por outro lado, $x \in \bigcap F$ implica $x \in C$ para todo $C \in F$. Logo, $x^+ \in C$, para todo $C \in F$, pois são conjuntos de sucessão. Portanto, $x^+ \in \bigcap F$, e assim $\bigcap F$ é um conjunto de sucessão. □

Consideramos um conjunto de sucessão A, que existe pelo Axioma 2.1. Então a interseção da família de todos os conjuntos de sucessão contidos em A é um conjunto de sucessão. Definimos assim o conjunto dos naturais.

Definição 2.4. Seja A um conjunto de sucessão. Definimos $\mathbb{N}$, **o conjunto dos números naturais**, por $\mathbb{N} = \bigcap K$, em que $K = \{X \subset A \mid X \text{ é um conjunto de sucessão}\}$.

Dessa forma, $\mathbb{N}$ é um conjunto de sucessão, e um **número natural** é um elemento desse conjunto. Temos assim, dois princípios de Peano garantidos. Isto é, duas propriedades que dizem respeito a $\mathbb{N}$. A saber,

a) $0 \in \mathbb{N}$ e

b) para todo $x \in \mathbb{N}$ temos que $x^+ \in \mathbb{N}$.

O próximo teorema, da **minimalidade** de $\mathbb{N}$, terá como consequência o Princípio da Indução Finita (PIF) expresso na linguagem da teoria de conjuntos, que apresenta uma formalidade conveniente.

Teorema 2.1. *(Minimalidade de $\mathbb{N}$) Seja B um conjunto de sucessão qualquer. Então $\mathbb{N} \subset B$.*

Demonstração. Consideramos A da Definição 2.4. Temos que $A \cap B \subset A$. Mas $A \cap B$ é um conjunto de sucessão pela Proposição 2.1, e $\mathbb{N}$ é a interseção de todos os conjuntos de sucessão contidos em A. Assim, temos $\mathbb{N} \subset A \cap B$ e portanto $\mathbb{N} \subset B$. □

Teorema 2.2 (Princípio da Indução Finita)**.** *Seja $S \subset \mathbb{N}$ tal que $0 \in S$ e que para todo $x \in S$ temos que $x^+ \in S$. Então $S = \mathbb{N}$.*

Demonstração. Como S é um conjunto de sucessão, pelo Teorema 2.1, $\mathbb{N} \subset S$. Logo, $S \subset \mathbb{N}$ implica $S = \mathbb{N}$. □

Seguindo a mesma linha e adotando essas estruturas, restam dois fatos para completar os cinco princípios. Primeiro devemos verificar que para todo $n \in \mathbb{N}$ segue que $n^+ \neq 0$. Depois precisamos argumentar que para todo $n, m \in \mathbb{N}$ temos que $n \neq m \Rightarrow n^+ \neq m^+$.

Teorema 2.3. *O zero não é sucessor de número algum.*

Demonstração. Verificamos a afirmação pois, para qualquer conjunto sucessor, $n \in n^+$. Se $n^+ = 0$ temos um absurdo. Portanto $n^+ \neq 0$. □

Observamos que no teorema já utilizamos o artigo definido para falar d**o** zero, mas não estamos falando no sentido de que ele é o único elemento neutro da adição. A unicidade do elemento zero é garantida pela Teoria dos Conjuntos, com o Axioma da Extensão. O zero é o conjunto vazio, que é único. Estamos apenas renomeando o mesmo e o pensando de forma diferente, como número. Por outro lado, para demonstrar a injetividade, precisamos de dois fatos auxiliares.

Proposição 2.2. *Nenhum número natural está contido em algum de seus elementos. De outro modo, para todo $n \in \mathbb{N}$ segue que $x \in n \Rightarrow n \not\subset x$.*

Demonstração. Demonstramos esta afirmação utilizando o Princípio da Indução Finita (PIF). Seja S o conjunto dos números naturais que não estão contidos em algum de seus elementos. $0 \in S$, pois $0 \in \mathbb{N}$ e não tem elementos para estar contido em algum deles. Suponhamos então que $n \in S$. O sucessor de n, n^+, não pode estar contido em n, pois caso estivesse teríamos $n \in n$. Como $n \subset n$, teríamos n contido em um de seus elementos. Por outro lado, $x \in n$ implica $n \not\subset x$, e como $n \subset n^+$, $n^+ \not\subset x$. Logo, n^+ não pode estar contido em algum de seus elementos, o que implica $n^+ \in S$. E portanto $S = \mathbb{N}$. □

Proposição 2.3. *Todo elemento de um número natural é subconjunto desse número. De outro modo, para todo $n \in \mathbb{N}$ segue que $x \in n \Rightarrow x \subset n$.*

Demonstração. Utilizamos novamente o PIF. Seja S o conjunto dos números naturais que têm todos seus elementos como subconjuntos. $0 \in S$ por argumento de vacuidade: todo elemento de 0 está contido em 0. Suponhamos que $n \in S$. Sabemos que $x \in n^+$ significa que $x = n$ ou $x \in n$. Se $x = n$, naturalmente, $x \subset n^+$. Por outro lado, $x \in n$ implica $x \subset n$, pois $n \in S$, que implica $x \subset n^+$. Logo, $n^+ \in S$ e $S = \mathbb{N}$. □

Assim, podemos demonstrar o seguinte.

Teorema 2.4 (Injetividade da sucessão)**.** *São diferentes os sucessores de dois naturais diferentes. De outro modo, para todo $n, m \in \mathbb{N}$ temos que $n \neq m \Rightarrow n^+ \neq m^+$. Mais ainda, para todo $n, m \in \mathbb{N}$ segue que se $n^+ = m^+ \Rightarrow n = m$.*

Demonstração. Suponhamos $n^+ = m^+$. Então, como $n \in n^+$, temos $n \in m^+$, o que implica $n \in m$ ou $n = m$. Pelo mesmo motivo, $m \in n$ ou $m = n$. Supondo $n \neq m$ temos $n \in m$ e $m \in n$, o que implica $n \in n$, pela Proposição 2.3. Mas então teríamos n sendo subconjunto de um de seus elementos, absurdo pela Proposição 2.2. Logo $n = m$. □

Percebemos que reduzimos os Axiomas de Peano apenas ao Axioma 2.1 da existência de um conjunto de sucessão. Deduzimos todas as outras afirmações pela Teoria de Conjuntos, o que é uma exposição bastante interessante, para percebermos o que faz do PIF ser de fato algo assumido. Podemos pensar em um conjunto de sucessão que não é o mínimo, e nesse caso, não valeria o PIF. Ademais, podemos pensar outros modelos em que não valem o axioma, como o conjunto dos reais ou o conjunto dos complexos, pois não temos o sucessor imediato. A reflexão sobre contextos nos quais não vale um princípio tem muita utilidade para compreendermos melhor o funcionamento desse princípio. Essa ideia foi bem desenvolvida quando se encontraram modelos para geometrias não euclidianas.

Faremos também uma abordagem do PIF como ferramenta para se definir uma função por recursividade. A utilidade do mesmo não está apenas em provar teoremas, mas também na definição de objetos com propriedades importantes.

Uma função por recursividade nos naturais, à princípio, não tem uma lei geral (por expressão) que toma um número natural e o leva em sua imagem (e não há garantia que tenha).

A recursividade aplica sucessivamente uma outra função definida em um conjunto X. A questão que se coloca é se tal procedimento pode de fato definir uma função dos naturais no conjunto X. O Teorema da Recursividade a seguir mostra que sim.

Teorema 2.5 (Recursividade)**.** *Sejam X um conjunto não vazio, e $a \in X$. E seja a função $f : X \to X$. Então existe uma função $u : \mathbb{N} \to X$ tal que $u(0) = a$ e também $u(n^+) = f(u(n))$.*

Demonstração. A demonstração se dá por construção, partindo-se do produto cartesiano de $\mathbb{N} \times X$. Sabemos que a função será um subconjunto desse produto cartesiano, um subconjunto de pares ordenados (sendo detalhista, isso seria o gráfico da função e precisaríamos também fixar posteriormente o contra-domínio, mas essa consideração não invalida o argumento). Tomamos então a coleção C de todos os subconjuntos A de $\mathbb{N} \times X$ tais que $(0, a) \in A$, e se $(n, x) \in A$ então $(n^+, f(x)) \in A$. O próprio produto cartesiano inicial possui essas propriedades, logo, a coleção C não é vazia. Assim, podemos fazer a interseção u de todos os conjuntos da coleção C. Por um argumento bem semelhante ao da Proposição 2.1 temos que u pertence a C. Assim, devemos provar apenas que u é uma função. O que deve ser provado é que se (n, x) e (n, y) pertencem u, então $x = y$. Para isso, é utilizado o PIF.

Seja S o conjunto de todos os naturais n tais que $(n, x) \in u$ para no máximo um x. Queremos provar que isso é verdade para todos os naturais. Logo, é conveniente provar que $0 \in S$ e $n^+ \in S$ sempre que $n \in S$; para então aplicar o PIF. Faremos isso várias vezes ao longo do texto, e isso indicará que estamos aplicando o princípio.

0 pertence a S. De fato, suponhamos que não pertencesse. Então $(0, b) \in u$ para algum $b \neq a$. Consideramos então o conjunto $u - \{(0, b)\}$. Esse conjunto ainda contém $(0, a)$, pois $a \neq b$. E se esse conjunto contém (n, x), também contém $(n^+, f(x))$, pois $n^+ \neq 0$ e o elemento removido não é $(n^+, f(x))$. Ocorreria então que o mesmo conjunto pertenceria à coleção C, mas isso não é possível pois u não poderia ser a interseção de todos os conjuntos de C. Logo $0 \in S$.

Suponhamos então que $n \in S$. Ou seja, existe apenas um x tal que $(n, x) \in u$. Como $(n, x) \in u$, temos que $(n^+, f(x)) \in u$. Perguntamos se n^+ pertence a S. Se não pertencesse, então teríamos $(n^+, y) \in u$ para algum $y \neq f(x)$. Consideramos então o conjunto $u - \{(n^+, y)\}$. Temos que $(0, a)$ pertence a tal conjunto. Se (m, t) pertence, então $(m^+, f(t))$ também pertence. Pois, se $m = n$ teremos tirado um elemento diferente de $(m^+, f(t)) = (n^+, f(x))$ e se $m \neq n$, temos $m^+ \neq n^+$ e teremos tirado um elemento diferente de $(m^+, f(t))$ também. Ou seja, o conjunto diminuído pertenceria a coleção C, o que novamente não é possível, pois de tal modo u não poderia ser a interseção de todos os conjuntos de C. Logo, temos um único elemento associado a n^+ e portanto $n^+ \in S$. Assim, $S = \mathbb{N}$ e u é de fato função. □

Quando se utiliza o Teorema 2.5 da recursividade para definir determinada função, temos uma **definição por indução**.

A partir de um determinado ponto no desenvolvimento de uma teoria, podemos encontrar um conjunto interessante de fatos que encapsulam de forma conveniente o que foi usado para demonstrar os mesmos. Ou seja, podemos partir de teoremas como se fossem axiomas e

nem precisamos utilizar procedimentos ou estruturas que antes o foram para as construções. É o caso dos Axiomas de Peano. Podemos utilizá-los sem voltar a pensar nos números como conjuntos, mas, simplesmente operando a aritmética. Há dois fatos ainda que apresentamos que abordam os conceitos mais primitivos do que os Axiomas de Peano. É interessante notar porque não conseguimos estudar tais fatos sob a luz apenas desses Axiomas. E posteriormente é interessante notar como conseguimos estudar outros fatos apenas com o novo ponto de partida. Vamos aos últimos teoremas deste capítulo.

Definição 2.5. Um conjunto é **transitivo** quando todo elemento dele está contido nele. De outro modo, A é transitivo quando, para todo x e y, se $x \in y$ e $y \in A$, temos que $x \in A$.

Vimos que todo natural é transitivo na Proposição 2.3. O próximo teorema diz respeito à transitividade do próprio conjunto $\mathbb{N}$.

Proposição 2.4. *O conjunto $\mathbb{N}$ dos números naturais é transitivo.*

Demonstração. Seja S o conjunto dos números naturais n tais que $n \in S \Rightarrow n \subset S$. Temos que $0 \in S$, pois zero, o próprio conjunto vazio, está contido em S, e curiosamente, a conclusão é a hipótese da implicação $0 \in S \Rightarrow 0 \subset S$. Suponhamos que $n \in S$. Então $n \subset S$ e $n \cup \{n\} \subset S$. Logo, $n^+ \subset S$, a implicação é também satisfeita de forma diferente e $n^+ \in S$. Assim, $S = \mathbb{N}$, e como S é transitivo por construção, $\mathbb{N}$ é transitivo. □

Proposição 2.5. *Se E é um subconjunto não vazio de um número natural, então existe um elemento $m \in E$ tal que para todo $k \in E$, com $k \neq m$, tem-se $m \in k$.*

Demonstração. Seja S o conjunto dos números naturais n tais que: para todo $E \subset n, E \neq \emptyset$, $\exists m \in E$ tal que $k \in E$ e $k \neq m \Rightarrow m \in k$. Por vacuidade, $0 \in S$. Se $n \in S$, tomamos $n^+ = n \cup \{n\}$. E os subconjuntos não vazios de n^+ serão os subconjuntos não vazios de n mais os subconjuntos de n aumentados com o elemento n. Para todos subconjuntos não vazios de n, aumentados ou não com o elemento n, tomamos o mesmo m, pois $m \in E \Rightarrow m \in n$. Para o conjunto vazio aumentado com o elemento n, basta tomarmos $m = n$, pois o fato se verifica por vacuidade. Logo, $n^+ \in S$ e $S = \mathbb{N}$. Portanto, todos os naturais possuem a propriedade que caracteriza S. □

3 OS AXIOMAS PARA O CONJUNTO DOS NÚMEROS NATURAIS

Os Axiomas de Giuseppe Peano[1] servem como ponto de partida importante para deduzir as propriedades básicas das operações com os números naturais (zero incluso). São elas: associatividade e comutatividade (adição e multiplicação), existência de elemento neutro para a soma, elemento neutro para o produto, distributividade, etc. Em essência, podemos estabelecer uma série de fatos aritméticos importantes a partir desses axiomas. Além de fatos sobre as operações aritméticas familiares, temos outros a respeito da função de sucessão. Alguns são estranhos por parecerem muito elementares; no entanto, não estão nos axiomas iniciais, logo não podem ser assumidos; devem ser provados. Utilizamos *The Construction of Number Systems* (KUMAR, 2011) como referência para este e o próximo capítulo.

Vamos então enunciar os Axiomas de Peano, que estabelecemos no capítulo anterior, e que nos será de grande utilidade.

Seja $\mathbb{N}$ o conjunto dos **números naturais**. Vamos supor que tal conjunto possui as seguintes propriedades.

Axioma 3.1 *Zero é um número natural, isto é,* $0 \in \mathbb{N}$

Axioma 3.2 *O sucessor* n^+ *de um número natural n é um número natural, ou seja,* $n \in \mathbb{N} \Rightarrow n^+ \in \mathbb{N}$

Axioma 3.3 *Zero não é sucessor de número algum, isto é, para todo* $n \in \mathbb{N} : 0 \neq n^+$

Axioma 3.4 *Números naturais diferentes têm sucessores diferentes, ou seja,* $\forall n, m \in \mathbb{N} : n \neq m \Rightarrow n^+ \neq m^+$

Axioma 3.5 *(Princípio da Indução Finita) Se* $S \subset \mathbb{N}$, $0 \in S$ *e* $n \in S \Rightarrow n^+ \in S$, *então* $S = \mathbb{N}$.

Observamos que os axiomas acima não foram apresentados na ordem em que foram deduzidos ou construídos, mas em uma ordem que é mais intuitiva de se estudar. Lembramos que todos esses se reduzem ao Axioma 2.1, e à Teoria dos Conjuntos.

Um breve comentário sobre o sentido de cada um dos axiomas. O primeiro axioma nos diz essencialmente que $\mathbb{N}$ é um conjunto não vazio. O segundo axioma nos informa algo sobre a função de sucessão, ou seja: seu domínio é $\mathbb{N}$, bem como seu contra-domínio. O conjunto $\mathbb{N}$ é fechado em relação ao operador unário de sucessão. O terceiro axioma nos permite concluirmos que a função de sucessão não é sobrejetiva. O quarto axioma, por sua vez, nos permite concluir que a função de sucessão é injetiva. Estas duas últimas constatações se relacionam ao conceito de conjunto infinito. Por fim, o quinto axioma possibilita estendermos as conclusões finitas sobre os elementos de $\mathbb{N}$ para uma conclusão geral, infinita enumerável.

[1] Giuseppe Peano (1858-1932), matemático italiano.

Agora deduziremos propriedades restritas de associatividade, comutatividade, distributividade, etc. Ou seja, aquelas com um número fixo e reduzido de termos. Passemos então a alguns fatos menores que merecem atenção.

Teorema 3.1. *Todo número natural n é diferente de seu sucessor n^+.*

Demonstração. Seja S o conjunto dos números naturais n tais que $n \neq n^+$. Podemos afirmar que $0 \neq 0^+$, pois 0 não é sucessor de número natural algum. Por outro lado, se $n \in S$, $n \neq n^+$, logo $n^+ \neq (n^+)^+$, pois não há dois naturais diferentes com o mesmo sucessor. Logo, $n^+ \in S$. Portanto, pelo Princípio da Indução, $S = \mathbb{N}$. □

Teorema 3.2. *Se $n \neq 0$, então $n = m^+$ para algum número natural m.*

Demonstração. Seja S o conjunto dos números naturais n tais que $n = 0$ ou $n = m^+$, para algum número natural m. É razoável que $0 \in S$. Então, seja $n \in S$. O sucessor de n, n^+, é um natural e $n^+ = k^+$, para algum número natural k, a saber o próprio n. Logo, $n^+ \in S$. Assim, $S = \mathbb{N}$. Portanto, se n é um natural $\neq 0$, $n \in S$, porque ainda é um natural. O que implica que n é sucessor de algum número, pois o outro lado da disjunção na definição de S (= 0) não pode ocorrer. □

Estabelecidos esses fatos, vamos então às definições das operações aritméticas, bem como à dedução de suas propriedades.

Definição 3.1. Definimos o operador binário de **adição**, **+**, da seguinte forma.

a) Para todo $n \in \mathbb{N}$ segue que $n + 0 = n$.

b) Para todo $n, m \in \mathbb{N}$ temos que $n + m^+ = (n + m)^+$.

Observamos que, devido ao Teorema 3.2, temos um número natural que é 0 ou é sucessor de algum número, ou seja, da forma m^+, para algum $m \in \mathbb{N}$. Portanto, a definição do operador acima de fato contempla todas as possibilidades para a soma $a + b$ de dois naturais a e b quaisquer.

Quanto ao fato de que no segundo item temos também uma soma do lado direito da equação, ocorre que recorreremos novamente à definição até chegarmos à soma $n + 0$. A demonstração de que o procedimento termina pode ser feita de maneira simples pelo PIF, embora deva ficar claro o que significa dizer "o procedimento termina". Significaria talvez que a expansão final da expressão tem tamanho finito (sendo um número natural)? Essas considerações aparentam ter um aspecto metamatemático (um fato que se afirma sobre as sentenças da teoria, e não uma proposição da teoria em si) que não cabe formalizar e aprofundar neste contexto, mas talvez deva-se mencionar por curiosidade lógica.

Proposição 3.1 (Elemento neutro da adição)**.** *Para qualquer $a \in \mathbb{N}$: $a + 0 = 0 + a = a$.*

Demonstração. Da definição, para qualquer $a \in \mathbb{N}$, $a + 0 = n$. Seja $S = \{x \in \mathbb{N} \mid 0 + x = x + 0\}$. Temos facilmente que $0 \in S$. E se $n \in S$ então $0 + n^+ = (0 + n)^+ = (n + 0)^+ = n^+ = n^+ + 0$. E assim $n^+ \in S$. Logo, $S = \mathbb{N}$, pelo PIF. E $a + 0 = 0 + a = a$, para $a \in \mathbb{N}$ qualquer. □

Proposição 3.2 (Associatividade da adição)**.** *Para quaisquer $a, b, c \in \mathbb{N}$: $(a + b) + c = a + (b + c)$.*

Demonstração. Consideramos um subconjunto S de $\mathbb{N}$ da seguinte forma. $S = \{z \in \mathbb{N} \mid \forall x, y \in \mathbb{N} : (x + y) + z = x + (y + z)\}$. Percebemos que $0 \in S$ pois $(x + y) + 0 = x + y = x + (y + 0)$. Por outro lado, se $n \in S$, temos que $(x + y) + n^+ = ((x + y) + n)^+ = (x + (y + n))^+ = x + (y + n)^+ = x + (y + n^+)$. Logo, $n^+ \in S$. Novamente, pelo PIF, para qualquer $z \in \mathbb{N}$ temos que para quaisquer $x, y \in \mathbb{N}$, ocorre a associatividade. Portanto, ocorre para quaisquer $x, y, z \in \mathbb{N}$. □

Proposição 3.3 (Comutatividade da Adição)**.** *Para quaisquer $a, b \in \mathbb{N}$: $a + b = b + a$.*

Demonstração. Consideramos um subconjunto S de $\mathbb{N}$ dado por $S = \{y \in \mathbb{N} \mid \forall x \in \mathbb{N} : x + y = y + x\}$. Já sabemos que $0 \in S$. Precisamos ainda verificar que $0^+ = 1 \in S$, ou seja, para todo $x \in \mathbb{N}$ temos $x + 1 = 1 + x$. Seja $T = \{x \in \mathbb{N} \mid x + 1 = 1 + x\}$. Já temos que $0 \in T$. Se $n \in T$, $n^+ + 1 = (n^+)^+ = (n + 1)^+ = (1 + n)^+ = 1 + n^+$. Logo, $T = \mathbb{N}$ e $1 \in S$. Por fim, suponhamos que $n \in S$. Então $x + n^+ = (x + n)^+ = (n + x)^+ = n + x^+ = n + (x + 1) = n + (1 + x) = (n + 1) + x = n^+ + x$. Assim, $n^+ \in S$. Concluímos que $S = \mathbb{N}$ e a propriedade comutativa vale para quaisquer $x, y \in \mathbb{N}$. □

Proposição 3.4 (Cancelamento da adição)**.** *Para quaisquer $a, b, c \in \mathbb{N}$: $b + a = c + a \Rightarrow b = c$, e $a + b = a + c \Rightarrow b = c$.*

Demonstração. Consideramos um subconjunto S de $\mathbb{N}$ dado por $S = \{x \in \mathbb{N} \mid \forall y, z \in \mathbb{N} : y + x = z + x \Rightarrow y = z\}$. Por verificação, $0 \in S$. Por outro lado, se $n \in S$ então $y + n^+ = z + n^+ \Rightarrow (y + n)^+ = (z + n)^+$. Pelo Axioma 3.4, $y + n = z + n$. Pela hipótese de indução, $y = z$. Logo, $n^+ \in S$, $S = \mathbb{N}$ e vale o cancelamento da adição. Da propriedade comutativa temos o segundo cancelamento. □

Proposição 3.5 (Existência e unicidade do elemento neutro da adição)**.** *Existe $x \in \mathbb{N}$ tal que para todo $a \in \mathbb{N}$ temos que $a + x = x + a = a$. Ademais, tal x é único.*

Demonstração. Do que foi abordado anteriormente, 0 é tal elemento. Se, por outro lado, $a + x = a = a + 0$, do cancelamento da adição, $x = 0$. De outra maneira, se x é elemento neutro da adição, então $x = x + 0 = 0 + x = 0$, que é uma demonstração usual. □

Neste momento, convém a introdução de relações que estabelecem a **ordem** no conjunto dos números naturais. Assim como a dedução das propriedades mais importantes, que dizem respeito ao ordenamento. Temos aqui dois tipos de ordem, que se dividem essencialmente em: a ordem estrita, que não admite reflexividade de nenhum elemento; e a ordem comum, que é reflexiva para todos os elementos. Há também outra diferença a ser considerada. Na ordem estrita, convém definir a anti-simetria dizendo que não há nenhum par de elementos

x, y tal que simultaneamente xRy e yRx (nesta notação xRy significa $(x, y) \in R$). Na ordem comum, convém definir anti-simetria dizendo que quando há um par de elementos x, y tal que simultaneamente $xR'y$ e $yR'x$, então $x = y$. A razão disso é que a ordem comum é reflexiva e por isso admite tal par. Neste contexto, as ordens estudadas são totais, ou seja, admitem a comparação de quaisquer dois elementos, que no caso são números naturais. A ordem estrita estará relacionada com a expressão "menor do que", e a ordem comum, por outro lado, com a expressão "menor do que ou igual a".

Definição 3.2. Sejam $n, m \in \mathbb{N}$. Dizemos que n **é menor do que** m, escrevemos $n < m$, se existe $k \in \mathbb{N}$, tal que $m = n + k^+$. Analogamente, n **é menor ou igual a** m, escrevemos $n \leq m$, se existe $k \in \mathbb{N}$ tal que $m = n + k$, ou seja, se $n < m$ ou $m = n + 0 = n$.

Definição 3.3. Sejam $n, m \in \mathbb{N}$. Dizemos que m **é maior do que** n, escrevemos $m > n$, se $n < m$. Analogamente, m **é maior ou igual a** n, escrevemos $m \geq n$, se $n \leq m$.

Teorema 3.3 (Anti-reflexividade)**.** *Para qualquer $a \in \mathbb{N}$ segue que a não é menor que a e escrevemos $a \not< a$. De outra forma, para quaisquer $a, k \in \mathbb{N}$ temos que $a \neq a + k^+$.*

Demonstração. Seja $S \subset \mathbb{N}$ com $S = \{y \in \mathbb{N} \mid \forall x \in \mathbb{N} : x \neq x + y^+\}$. Por verificação temos que $0 \in S$, uma vez que nenhum número é igual a seu sucessor, do Teorema 3.1. Suponhamos que $n \in S$, ou seja $\forall x \in \mathbb{N} : x \neq x + n^+$. Temos de pensar agora o caso n^+. Consideramos então $T \subset \mathbb{N}$ tal que $T = \{m \in \mathbb{N} \mid m \neq m + n^{++}\}$. Verificamos que $0 \in T$, pois 0 não é sucessor de número natural algum. Por outro lado, se $j \in T$ então suponhamos que j^+ não pertencesse a T, que fosse o caso de $j^+ = j^+ + n^{++}$. Assim, $j^+ = (j^+ + n^+)^+$, que implica $j = j^+ + n^+$, pelo Axioma 3.4. Então $j = (j + 1) + n^+ \Rightarrow j = j + (1 + n^+) \Rightarrow j = j + (n^+ + 1) \Rightarrow j = j + n^{++}$. O que contradiz o que havíamos suposto sobre j. Logo, $j^+ \in T$ e $T = \mathbb{N}$. Assim, $n^+ \in S$, $S = \mathbb{N}$ e a anti-reflexividade vale para todo número natural. □

Teorema 3.4 (Transitividade)**.** *Para quaisquer $a, b, c \in \mathbb{N}$ temos que se $a < b$ e $b < c$, então $a < c$.*

Demonstração. Sejam $x, y, z \in \mathbb{N}$, tais que $x < y$ e $y < z$. Então $z = y + k^+$ para algum $k \in \mathbb{N}$. Sabemos que $y = x + l^+$ para algum $l \in \mathbb{N}$. Logo, temos $z = y + k^+ = (x + l^+) + k^+ = x + (l^+ + k^+) = x + (l^+ + k)^+$ e assim $z = x + m^+$, para algum $m \in \mathbb{N}$. Portanto, $x < z$. □

Teorema 3.5 (Tricotomia)**.** *Para quaisquer $a, b \in \mathbb{N}$, uma e somente uma das possibilidades ocorre: $a < b$ ou $a = b$ ou $b < a$.*

Notação: $\veebar$ denota a disjunção exclusiva, isto é, $p \veebar q$ será falsa se ambas, p e q, forem verdadeiras ou falsas.

Demonstração. Primeiro, mostremos que apenas um desses casos pode ocorrer. Sejam $x, y \in \mathbb{N}$. Se $x < y$ então $y = x + k^+$, para algum $k \in \mathbb{N}$. Logo, não podemos ter $x = y$, pois contraria o

teorema 4.23 da anti-reflexividade. Por outro lado, $y < x$ também não é possível, pois teríamos $x = y + l^+$ para algum $l \in \mathbb{N}$ e então $x = (x + k^+) + l^+$, ou seja, $x = x + (k^+ + l)^+$, o que também contraria a anti-reflexividade. Por fim, se $x = y$ também não poderíamos ter as outras duas opções pelo mesmo motivo. E começando com a outra desigualdade temos um caso análogo ao primeiro. Logo, se uma das opções ocorre, as outras não ocorrem.

Para a segunda parte, consideramos o conjunto $S \subset \mathbb{N}$ com $S = \{x \in \mathbb{N} \mid \forall y \in \mathbb{N} : x < y \veebar x = y \veebar y < x\}$. $0 \in S$, pois $y = 0$ ou $y = u^+ = 0 + u^+$ e portanto $0 < y$. Suponhamos então $m \in S$. Temos três possibilidades: $y < m$ ou $m = y$ ou $m < y$. Consideremos primeiramente o caso $y < m$. Então, $m = y + k^+$, para algum $k \in \mathbb{N}$. Logo $m^+ = (y + k^+)^+ = y + k^{++}$, $y < m^+$, e $m^+ \in S$. A outra possibilidade é $m = y$ e então $m^+ = y^+ = y + 1$, e $y < m^+$, que implica também $m^+ \in S$. Por último, se $m < y$ então $y = m + k^+$ para algum $k \in \mathbb{N}$. Se $k = 0$, $y = m^+$ e $m^+ \in S$. Por outro lado, se $k = l^+$, e $y = m + l^{++}$, então $y = m + l^{++} = m + (l^+ + 1) = m + (1 + l^+) = (m + 1) + l^+ = m^+ + l^+$. Logo $m^+ < y$ e $m^+ \in S$. Assim $S = \mathbb{N}$, e a propriedade da tricotomia vale para todos os pares de números naturais. □

Teorema 3.6 (Anti-simetria)**.** *Para quaisquer $a, b \in \mathbb{N}$: não se tem que $a < b \wedge b < a$.*

Demonstração. A anti-simetria definida dessa forma é uma consequência direta do teorema anterior. Observamos o caso em que escolhemos o mesmo elemento, ou seja, $a = b$. □

Teorema 3.7 (Totalidade)**.** *Para quaisquer $a, b \in \mathbb{N}$ com $a \neq b$: obrigatoriamente $a < b \vee b < a$.*

Demonstração. A totalidade definida dessa forma também é uma consequência direta do que provamos. □

Faz mais sentido falar em anti-simetria aqui do que em totalidade. A anti-simetria ainda precisa ser mencionada como consequência. Mas a totalidade já seria a própria tricotomia. A totalidade é utilizada para se falar de ordens [formadas por relações] nas quais é possível comparar quaisquer dois elementos escolhidos ao acaso do conjunto. Nessa escolha arbitrária, consideramos ser possível tomar o mesmo elemento duas vezes. Se a ordem for uma ordem comum, podemos ainda comparar. Caso contrário, precisamos da relação de igualdade. Então, em uma ordem estrita, comumente utilizamos a relação de igual para conseguirmos totalidade e fica mais conveniente tratar apenas da tricotomia.

As propriedades para a outra relação, que determina ordem comum total, são listadas a seguir, sem contudo expor as demonstrações, pois elas são pequenas variações das demonstrações anteriores, usando k ao invés de k^+.

Teorema 3.8 (Reflexividade)**.** *Para qualquer $a \in \mathbb{N}$: $a \leq a$.*

Teorema 3.9 (Transitividade)**.** *Para quaisquer $a, b, c \in \mathbb{N}$: $a \leq b$ e $b \leq c \Rightarrow a \leq c$.*

Teorema 3.10 (Anti-simetria)**.** *Para quaisquer $a, b \in \mathbb{N}$: $a \leq b$ e $b \leq a \Rightarrow a = b$.*

Teorema 3.11 (Totalidade)**.** *Para quaisquer $a, b \in \mathbb{N}$: $a \leq b$ ou $b \leq a$.*

A relação de ordem é importante para aprofundarmos nossa compreensão do Princípio da Indução Finita, conhecendo outras versões para o mesmo, que são consideradas equivalentes. Partimos de uma axiomatização em que a formulação do PIF fica diretamente dependente dos princípios de conjuntos, e a partir dele construímos a ordem e deduzimos outros princípios, do Bom Ordenamento e da Indução Completa. Com a finalidade de demonstrar a dependência do PIF dos princípios seguintes seria necessário considerarmos o conceito de ordem primeiro, para então construirmos o axioma de maneira diferente. Ou seja, levantamos apenas o questionamento (sem contudo tentar responder): sob quais determinadas condições, as outras formulações são equivalentes ao Princípio da Indução Finita (sem usar aquilo que é feito por este)? Vamos a mais algumas definições para passar às formas alternativas.

Definição 3.4. Seja um conjunto S, com uma ordem comum $\leq$ definida no mesmo. Então, um elemento $m \in S$ é **mínimo** se, para qualquer $n \in S$, $m \leq n$.

Veremos no próximo teorema que um elemento mínimo é único, e portanto é **o** elemento mínimo.

Proposição 3.6 (Unicidade do elemento mínimo)**.** *Seja um conjunto S. Se S tem um elemento mínimo, então este é único.*

Demonstração. Seja um conjunto S e uma ordem comum $\leq$ em S. Sejam m, n elementos mínimos de S. Logo $m \leq n$ e $n \leq m$. Devido à anti-simetria $m = n$. Portanto, o elemento mínimo é único. □

Teorema 3.12 (Princípio do Bom Ordenamento - PBO)**.** *Seja $S \subset \mathbb{N}$, $S \neq \emptyset$. Então S, na ordem da relação menor ou igual, $\leq$, tem um elemento mínimo.*

Demonstração. Seja $T = \{x \in \mathbb{N} \mid x \in S \Rightarrow \exists m \in S : \forall s \in S : m \leq s\}$. Neste caso o conjunto S é variável. A estratégia é demonstrar que $T = \mathbb{N}$ para então utilizarmos o fato de que S tem um elemento. Isso implicará que este admite mínimo. Constatamos que $0 \in T$ por simples verificação, pois se $0 \in S$, S possuí elemento mínimo, já que $0 \leq s$ para qualquer $s \in \mathbb{N}$ e $S \subset \mathbb{N}$.

Por outro lado, suponha que $n \in T$. Suponhamos então que $n^+ \in S$. Se $n \in S$, S já admite mínimo; assim consideramos que $n \notin S$ e tomamos o conjunto $A = S \cup \{n\}$. Como $n \in T$ e $n \in A$, A admite elemento mínimo. Seja $a \in A$ o elemento mínimo de A. Podemos ter $a \neq n$ ou $a = n$. Se $a \neq n$, então $a \in S$. Como a é o mínimo de A, a é elemento mínimo de S e S admite mínimo. Consideramos por fim o caso $a = n$. Se $s \in S$, $n \leq s$. Mas $n \notin S$, então $n \neq s$, o que implica $n < s$. Logo, $s = n + k^+$ para algum natural k. O que implica que $s = n + (k + 1) = n + (1 + k) = (n + 1) + k = n^+ + k$, e $n^+ \leq s$. Logo n^+ é elemento mínimo de S, S admite mínimo, $T = \mathbb{N}$ e todo subconjunto não vazio de $\mathbb{N}$ admite mínimo. □

O próximo teorema é conhecido como Princípio da Indução Completa - PIC. Este princípio é equivalente ao Princípio da Indução Finita, no entanto, este faz uso do conceito de **menor**

que nos números naturais. Neste contexto, suas propriedades foram deduzidas por meio do PIF. Logo, o trabalho de constatar a equivalência de ambos deve tomar certo cuidado para não incorrer em circularidade. Ou seja, é estranho dizer que se pode obter primeiro do segundo, quando os conceitos do segundo são obtidos pelo primeiro. Ao mesmo tempo, lembramos que deduzimos o PIF de um ponto bastante elementar na Teoria de Conjuntos, e que envolve tomar a interseção de uma família de conjuntos de sucessão.

Se quisermos estabelecer a equivalência dos dois princípios, precisamos interromper no ponto que envolve tomar a interseção de uma família de conjuntos de sucessão e utilizar as propriedades de ordens, junto com o conceito de sucessão, que seria necessário pois está presente na hipótese do PIF. Lembramos que as ordens são relações e que as suas propriedades não dependem deste, mas podem ser admitidas: as características de (anti-)reflexividade, transitividade, anti-simetria, totalidade, etc. O Princípio do Bom Ordenamento de fato também é, sob determinadas condições, equivalente. Mas para este princípio também valem as mesmas considerações. Portanto, não apresentamos a dedução do PIF por meio dos outros, e não constatamos as equivalências. Elas não fazem falta em si na prática. Esse comentário seria apenas para mencionar algo que pode merecer atenção. Por fim, a demonstração abaixo utiliza o PBO.

Teorema 3.13 (Princípio da Indução Completa - PIC)**.** *Seja* $S \subset \mathbb{N}$ *tal que* $0 \in S$ *e* $\forall n \in \mathbb{N} : (\forall k < n : k \in S) \rightarrow n \in S$*. Então* $S = \mathbb{N}$*.*

Demonstração. Seja $T = \{n \in \mathbb{N} \mid n \notin S\}$. Dessa vez, a estratégia é mostrar que $T = \emptyset$. Vamos supor que T não é vazio e seja m o elemento mínimo de T, garantido pelo Teorema 3.12. Como $0 \in S$, temos que $0 \notin T$. Logo, $0 < m$. Como m é mínimo, se $k < m$ então $k \notin T$, e assim $k \in S$. Pela segunda hipótese, então $m \in S$. Mas isso é uma contradição, pois T é o complementar de S em relação ao conjunto $\mathbb{N}$. Portanto $T = \emptyset$ e $S = \mathbb{N}$. □

Uma vez desenvolvido o conceito de ordem com a relação "menor ou igual a", é possível introduzir o conceito de subtração no conjunto dos números naturais. Antes, passamos brevemente pela ideia de **antecessor**. Então, dados $m, n \in \mathbb{N}$, definimos $m - n$ desde que tenhamos $n \leq m$. Portanto, axiomaticamente, a ordem comum total construída com a soma (existe k tal que $m = n + k$) precede a subtração.

De modo semelhante, precisamos introduzir o conceito de ordem com a divisibilidade para abordar a divisão. A divisibilidade (relação de ordem comum parcial, pois há pares de elementos em que nenhum é divisível por outro), com efeito, é definida com a multiplicação. Dados $m, n \in \mathbb{N}$, podemos definir a divisão m/n desde que tenhamos $n \mid m$, ou seja, desde que existe $q \in \mathbb{N}$ tal que $m = n \times q$.

Esse caminho também é interessante, e deve nos fornecer ferramentas formais convenientes futuramente.

Definição 3.5. Seja $m \in \mathbb{N}$ tal que $m = n^+$ para algum $n \in \mathbb{N}$. Definimos $m^- = n$, **o antecessor de** m, como o número cujo sucessor é m.

Já sabemos que o antecessor é único pelo Axioma 3.4. Ou seja, se $m = j^+$ e $m = k^+$, temos $j^+ = k^+$, que implica $j = k$. Portanto, o antecessor está bem definido. Ademais pela definição o zero não possuirá antecessor, pois 0 não é tal que $0 = n^+$ para algum $n \in \mathbb{N}$.

Definição 3.6. Sejam $a, b \in \mathbb{N}$ com $b \leq a$. Então, pela definição de $\leq$, existe $k \in \mathbb{N}$ tal que $a = b + k$. Ademais, tal k é único, pois $a = b + p$ e $a = b + k \Rightarrow b + p = b + k \Rightarrow p = k$. Portanto, podemos considerar uma função, chamada **subtração**, $- : X \to \mathbb{N}$, em que $X \subset \mathbb{N} \times \mathbb{N}$, com $X = \{(a, b) \in \mathbb{N} \times \mathbb{N} \mid b \leq a\}$, e $a - b = k$ tal que $a = b + k$.

Essencialmente isso nos dá o fato de que $b + (a - b) = (a - b) + b = a$. Interessante notar também que $b \leq a + b$ e portanto podemos fazer $(a + b) - b$. E $(a + b) - b = l$ tal que $b + l = a + b$. Logo $l = a$, pelo cancelamento. Ou seja, quando $b \leq a$, $(a - b) + b = (a + b) - b = a$. Intuitivamente, sabemos de fato que a subtração de b é a operação oposta à adição de b, e a ordem em que são realizadas não importa, dentro das situações em que é possível as duas ordens. Descontam-se os efeitos contrários. Seguindo a mesma disposição de tentar relacionar os fatos de modo abrangente, podemos abordar esse operador no contexto de estrutura associativa, comutativa, de cancelamento ou distributiva.

Proposição 3.7 (Elemento neutro da subtração)**.** *Para qualquer $a \in \mathbb{N}$: $0 \leq a$ e portanto $a - 0$ está definido com $a - 0 = a$.*

Demonstração. Temos que $a = 0 + a$, e assim $0 \leq a$ e $a - 0 = k$ tal que $0 + k = a$. Portanto, $a - 0 = a$. Tanto a adição quanto a subtração por zero não alteram o resultado. □

Proposição 3.8 (Associatividade na subtração)**.** *Para quaisquer $a, b, c \in \mathbb{N}$: se $c \leq b$, $(a + b) - c = a + (b - c)$.*

Demonstração. Se $c \leq b$, então $c + (b - c) = (b - c) + c = b$. O que implica $a + ((b - c) + c) = a + b$ e segue que $(a + (b - c)) + c = a + b$. Como $b \leq a + b$, então $c \leq a + b$. Assim, $(a + b) - c$ está definido e temos $((a + (b - c)) + c) - c = (a + b) - c$. Portanto $a + (b - c) = (a + b) - c$. □

Proposição 3.9 (Comutatividade na subtração)**.** *Para quaisquer $a, b, c \in \mathbb{N}$: se $c \leq a$, $(a + b) - c = (a - c) + b$.*

Demonstração. Se $c \leq a$, como $a \leq a + b$, então $c \leq a + b$. Temos então que $c + (a - c) = (a - c) + c = a$. Assim, $((a - c) + c) + b = a + b$, o que implica $(((a - c) + b) + c) - c = (a + b) - c$. Portanto $(a - c) + b = (a + b) - c$. □

Essas duas últimas propriedades nos sugerem algo que ficará mais claro e simples quando estivermos lidando com números inteiros: que a subtração é de algum modo um operador tão associativo e comutativo quanto a adição. O "cálculo dos efeitos" de cada termo pode ser considerado (simplificação da expressão) a qualquer momento. Ao se lidar com os números naturais, as condições limitam a manipulação algébrica. Nos números inteiros, com

efeito, não será necessário se preocupar com certos requisitos. O mesmo ocorre, considerando a divisão, ao passarmos dos números inteiros para os números racionais, ou dos números naturais para os números racionais não negativos.

Proposição 3.10 (Cancelamento da subtração I)**.** *Para quaisquer* $a, b, c \in \mathbb{N}$*: se* $a \leq b$ *e* $a \leq c$*, então* $b - a = c - a \Rightarrow b = c$*.*

Demonstração. Se $a \leq b$ e $a \leq c$, estão definidas as subtrações na hipótese. Desse modo, $a + (b - a) = (b - a) + a = b$ e ao mesmo tempo $a + (c - a) = (c - a) + a = c$. Mas então $b - a = c - a \Rightarrow b = (b - a) + a = (c - a) + a = c$, e portanto $b = c$ e vale o cancelamento da subtração. □

Proposição 3.11 (Cancelamento da Subtração II)**.** *Para quaisquer* $a, b, c \in \mathbb{N}$*: se* $a \leq b$ *e* $c \leq b$*, então* $b - a = b - c \Rightarrow a = c$*.*

Demonstração. Se $a \leq b$ e $c \leq b$, estão definidas as subtrações na hipótese. E, desse modo, $a + (b - a) = (b - a) + a = b$ e ao mesmo tempo $c + (b - c) = (b - c) + c = b$. Mas então $(b - a) + a = (b - c) + c \Rightarrow (b - a) + a = (b - a) + c$. Assim, do cancelamento da adição, $a = c$ e vale a propriedade. □

Proposição 3.12 (Neutro da subtração é único)**.** *Existe* $x \in \mathbb{N}$ *tal que* $\forall a \in \mathbb{N} : a - x = a$*. Ademais, tal* x *é único.*

Demonstração. Já sabemos que 0 é um elemento com tal propriedade. Temos $(a - x) + x = a$. Se, por outro lado, $a - x = a$, então $a + x = a$ e da unicidade do neutro da soma, $x = 0$. □

Proposição 3.13 (Distributividade da subtração)**.** *Para quaisquer* $a, b, c \in \mathbb{N}$*: se* $b + c \leq a$*, então* $a - (b + c) = (a - b) - c$*.*

Demonstração. Se $b + c \leq a$, então $a = (b + c) + k$, para algum $k \in \mathbb{N}$. E está definida a subtração $a - (b + c) = k$. Ao mesmo tempo, se $a = b + (c + k)$, $b \leq a$ e está definida a subtração $a - b$. Também $a - b = c + k$. Logo $c \leq a - b$ e está definida a subtração $(a - b) - c$, igual a k. Portanto, $a - (b + c) = (a - b) - c$. □

Vamos definir então o operador de multiplicação. E desenvolver suas propriedades mais importantes. Notemos que nas expressões mistas interpretamos a precedência da multiplicação sobre a adição e subtração.

Definição 3.7. Definimos o operador binário de **multiplicação**, $\times$, da seguinte forma.

a) Para todo $n \in \mathbb{N}$ temos que $n \times 0 = 0$

b) Para todo $n, m \in \mathbb{N}$ temos que $n \times m^+ = n \times m + n$

As mesmas considerações feitas para a definição da adição valem aqui. Devido ao Teorema 3.2 temos que um número é 0 ou da forma m^+, para algum $m \in \mathbb{N}$. Assim, a definição do operador acima contempla todas as possibilidades para a multiplicação $a \times b$ de dois naturais a e b quaisquer. E podemos demonstrar retoricamente por PIF que o procedimento termina: termina para 0, e se termina para n, basta aplicar a definição e verificar que termina para n^+.

Proposição 3.14 (Distributividade da multiplicação em relação à adição)**.** *Para quaisquer $a, b, c \in \mathbb{N}$: $a \times (b + c) = a \times b + a \times c$ e $(b + c) \times a = b \times a + c \times a$.*

Demonstração. Seja $S \subset \mathbb{N}$ com $S = \{z \in \mathbb{N} \mid \forall x, y \in \mathbb{N} : x \times (y+z) = x \times y + x \times z\}$. Verificamos que $0 \in S$, pois $x \times (y+0) = x \times y = x \times y + 0 = x \times y + x \times 0$. Por outro lado, suponhamos que $n \in S$. Então, $x \times (y+n^+) = x \times (y+n)^+ = x \times (y+n) + x = (x \times y + x \times n) + x = x \times y + (x \times n + x) = x \times y + (x \times n^+)$. Então $n^+ \in S$, $S = \mathbb{N}$ e a propriedade distributiva à esquerda vale.

Seja então $S' \subset \mathbb{N}$ com $S' = \{x \in \mathbb{N} \mid \forall y, z \in \mathbb{N} : (y+z) \times x = y \times x + z \times x\}$. Verificamos que $0 \in S'$, pois $(y + z) \times 0 = 0 = 0 + 0 = y \times 0 + z \times 0$. Por outro lado, suponhamos que $n \in S'$. Então, $(y+z) \times (n^+) = (y+z) \times n + (y+z) = (y \times n + z \times n) + (y+z) = ((y \times n + z \times n) + y) + z = (y \times n + (z \times n + y)) + z = (y \times n + (y + z \times n)) + z = ((y \times n + y) + z \times n) + z = (y \times n + y) + (z \times n + z) = y \times n^+ + z \times n^+$. Então $n^+ \in S'$, $S' = \mathbb{N}$ e a propriedade distributiva à direita vale. □

Proposição 3.15 (Distributividade da multiplicação em relação à subtração)**.** *Para quaisquer $a, b, c \in \mathbb{N}$: se $c \leq b$, $a \times (b - c) = a \times b - a \times c$ e $(b - c) \times a = b \times a - c \times a$.*

Demonstração. Se $c \leq b$, temos $(b - c) + c = c + (b - c) = b$. Assim, $a \times ((b - c) + c) = a \times b$ e segue que $a \times (b - c) + a \times c = a \times b$. Temos $a \times c \leq a \times b$ e ao mesmo tempo $a \times b - a \times c = k$ tal que $a \times c + k = a \times b$. Portanto, $k = a \times (b - c) = a \times b - a \times c$ e vale a distributiva à esquerda. Para a distributiva à direita basta utilizarmos a distributiva à esquerda com a comutatividade da multiplicação. □

Proposição 3.16 (Elemento neutro da multiplicação)**.** *Para qualquer $a \in \mathbb{N}$: $a \times 1 = 1 \times a = a$.*

Demonstração. Pela definição de multiplicação, verificamos que, para qualquer $x \in \mathbb{N}$, $x \times 1 = x \times 0^+ = x \times 0 + x = x$. Seja $S \subset \mathbb{N}$ com $S = \{x \in \mathbb{N} \mid x \times 1 = 1 \times x\}$. Verificamos que $0 \in S$, pois $0 \times 1 = 0 \times 0^+ = 0 \times 0 + 0 = 0 = 1 \times 0$. Por outro lado, se $n \in S$, então $n^+ \times 1 = n^+ \times 0 + n^+ = n^+ = n + 1 = 1 \times n + 1 \times 1 = 1 \times (n + 1) = 1 \times n^+$. Logo $n^+ \in S$, $S = \mathbb{N}$ e a propriedade vale. □

Proposição 3.17 (Associatividade da multiplicação)**.** *Para quaisquer $a, b, c \in \mathbb{N}$: $(a \times b) \times c = a \times (b \times c)$.*

Demonstração. Seja $S \subset \mathbb{N}$ com $S = \{z \in \mathbb{N} \mid \forall x, y \in \mathbb{N} : (x \times y) \times z = x \times (y \times z)\}$. Verificamos que $0 \in S$. Por outro lado, se $n \in S$, temos que $(x \times y) \times n^+ = (x \times y) \times n + x \times y = x \times (y \times n) + x \times y = x \times (y \times n + y) = x \times (y \times n^+)$. Logo, $n^+ \in S$, $S = \mathbb{N}$ e vale a associatividade do produto. □

Proposição 3.18 (Comutatividade da multiplicação)**.** *Para quaisquer* $a, b \in \mathbb{N}$*:* $a \times b = b \times a$*.*

Demonstração. Seja $S \subset \mathbb{N}$ com $S = \{y \in \mathbb{N} \mid \forall x \in \mathbb{N} : x \times y = y \times x\}$. Verificamos primeiro que $0 \in S$. Para isso, seja $T \subset \mathbb{N}$ com $T = \{x \in \mathbb{N} \mid x \times 0 = 0 \times x\}$. Verificamos de forma simples que $0 \in T$. Por outro lado, se $n \in T$, então $0 \times n^+ = 0 \times (n+1) = 0 \times n + 0 \times 1 = n \times 0 + 0 = 0 = n^+ \times 0$. Logo, $n^+ \in T$, $T = \mathbb{N}$ e $0 \in S$. Por outro lado, se $n \in S$, temos que $x \times n^+ = x \times n + x = n \times x + 1 \times x = (n+1) \times x = n^+ \times x$. Portanto, $n^+ \in S$, $S = \mathbb{N}$ e vale a comutativa da multiplicação. □

Proposição 3.19 (Cancelamento da multiplicação)**.** *Para quaisquer* $a, b, c \in \mathbb{N}$*:* $b \times a^+ = c \times a^+ \Rightarrow b = c$*.*

Demonstração. Observamos que podemos cancelar um termo a^+, que, por ser sucessor de algum número, é diferente de 0. Se fosse 0 não valeria a lei do cancelamento, pois poderíamos considerar dois números diferentes e o produto deles por 0 seriam ambos iguais a 0.

Vamos induzir em b. Seja então $S = \{y \in \mathbb{N} \mid \forall x, z \in \mathbb{N} : y \times x^+ = z \times x^+ \Rightarrow y = z\}$. Para $y = 0$ teremos $0 = 0 \times x^+ = z \times x^+$. Se $z \neq 0$, então teríamos $z = q^+$ para algum $q \in \mathbb{N}$. Segue que $0 = q^+ \times x^+ = q^+ \times x + q^+ = (q^+ \times x + q)^+$, mas então 0 seria sucessor de algum número, o que não é possível. Portanto $y = z = 0$.

Por outro lado, suponhamos que $n \in S$. Desse modo, se $n^+ \times x^+ = z \times x^+$ temos que $z \neq 0$, pois $n^+ \times x^+ = n^+ \times x + n^+ = (n^+ \times x + n)^+ \neq 0$. Logo, $z = p^+$ para algum $p \in \mathbb{N}$. Assim, $n^+ \times x^+ = p^+ \times x^+ \Rightarrow n \times x^+ + x^+ = p \times x^+ + x^+ \Rightarrow n \times x^+ = p \times x^+$ que pela hipótese de indução nos dá $n = p$ e implica em $n^+ = p^+$. Desse modo, $n^+ = z$, e $n^+ \in S$. Portanto, $S = \mathbb{N}$ e vale o cancelamento da multiplicação. □

Proposição 3.20 (Elementos não nulos)**.** *Para quaisquer* $a, b \in \mathbb{N}$*:* $a^+ \times b^+ \neq 0$*.*

Demonstração. Isso já foi demonstrado anteriormente, mas deixamos explicitado aqui. $a^+ \times b^+ = a^+ \times b + a^+ = (a^+ \times b + a)^+ \neq 0$, pois 0 não é sucessor de número natural algum. □

Esse fato nos dá portanto que $x \times y = 0$ implica $x = 0$ ou $y = 0$, pois caso contrário teríamos o resultado diferente de zero. Essa propriedade é requisito para denominarmos um anel como **domínio de integridade**. $\mathbb{N}$ não é um anel, pois não tem elemento oposto, mas apresenta também esse aspecto de integridade.

Por último, concluímos que o elemento neutro da multiplicação é único.

Proposição 3.21 (Neutro da multiplicação é único)**.** *Existe* $x \in \mathbb{N}$ *tal que para todo* $a \in \mathbb{N}$ *:* $a \times x = x \times a = a$*. Ademais, tal* x *é único.*

Demonstração. Pelo que foi apresentado, o elemento 1 possui tal propriedade. Se, por outro lado, $a \times x = a$, para qualquer $a \in \mathbb{N}$, então particularmente $k^+ \times x = k^+ = k^+ \times 1$. Da propriedade do cancelamento da multiplicação temos $x = 1$. Poderíamos ter procedido da maneira usual. Se 1 e $1'$ são elementos com tal propriedade, então $1' = 1' \times 1 = 1 \times 1' = 1$. □

Prosseguimos com a definição de divisibilidade, estudo das respectivas propriedades de ordem comum parcial e então com a definição do operador divisão e a demonstração de seus teoremas.

Definição 3.8. Sejam $a, b \in \mathbb{N}$. Dizemos que b **divide** a, escrevemos $b \mid a$, se existe $q \in \mathbb{N}$, tal que $a = b \times q$.

Definição 3.9. Sejam $a, b \in \mathbb{N}$. Dizemos que a **é divisível por** b, ou a **é múltiplo de** b, se $b \mid a$. Não há notação para tal ordem invertida.

Teorema 3.14 (Reflexividade)**.** *Para qualquer $a \in \mathbb{N}$: $a \mid a$.*

Demonstração. Temos que, para qualquer $a \in \mathbb{N}$: $a = a \times 1$. Portanto, $a \mid a$. □

Teorema 3.15 (Transitividade)**.** *Para quaisquer $a, b, c \in \mathbb{N}$: $a \mid b$ e $b \mid c \Rightarrow a \mid c$.*

Demonstração. Se $a \mid b$ e $b \mid c$ temos que $c = b \times q'$ e $b = a \times q$ para determinados $q, q' \in \mathbb{N}$. Logo, $c = (a \times q) \times q' = a \times (q \times q')$ e assim $c = a \times k$ para algum $k \in \mathbb{N}$. Portanto, $a \mid c$ e a divisibilidade é uma relação transitiva. □

Teorema 3.16 (Limitação)**.** *Para quaisquer $a, b \in \mathbb{N}$: se $b \mid a$, então $a = 0$ ou $b \leq a$. De outra forma, sabemos que para qualquer $b \in \mathbb{N}$, $b \mid 0$. Por outro lado, se $b \mid a^+$, então $b \leq a^+$. Ademais, neste caso $b \neq 0$.*

Demonstração. Demonstremos a segunda forma. Se $b \mid a^+$, então $a^+ = b \times q$ para algum $q \in \mathbb{N}$. Mas b e q devem ser diferentes de zero, pois caso contrário teríamos $a^+ = 0$. Portanto, $a^+ = b \times k^+$ para algum $k \in \mathbb{N}$. Logo, $a^+ = b \times k + b$ e temos então que $a^+ = b + l$, para algum $l \in \mathbb{N}$. Ou seja, $b \leq a^+$ e vale a propriedade da limitação. □

Teorema 3.17 (Anti-simetria)**.** *Para quaisquer $a, b \in \mathbb{N}$: se $a \mid b$ e $b \mid a$ então $a = b$.*

Demonstração. Se $a \mid b$ e $b \mid a$, temos três possibilidades. Se ambos são 0, o teorema se verifica. A situação em que apenas um dos dois é zero não é possível, pois teríamos $k^+ \mid 0$ e $0 \mid k^+$, ou seja $k^+ = 0 \times q = 0$, para algum $q \in \mathbb{N}$. Por último, se ambos $\neq 0$. Como $a \mid b$ e $b \mid a$, segue que $a \leq b$ e $b \leq a$, e portanto $a = b$. Vale a propriedade de anti-simetria para a relação de divisibilidade. □

Teorema 3.18 (Não totalidade)**.** *Não se tem para quaisquer $a, b \in \mathbb{N}$: $a \mid b$ ou $b \mid a$.*

O teorema 4.19 pode ser verificado através de um contra-exemplo. Consideramos o par 2 e 3. Pela limitação, $3 \nmid 2$. Por outro lado, $2 \nmid 3$, pois: $2 \times 0 = 0$, $2 \times 1 = 2$, $2 \times 2 = 2 \times 1 + 2 = 2 + 1^+ = (2 + 1)^+ \neq 3$. Naturalmente, $2 \times 3 = 3$ implicaria $2 = 1$, pelo cancelamento da multiplicação, e portanto não é possível. Não há mais possibilidades de quocientes, pois outras alternativas não são menores ou iguais a 3. Se números maiores fossem quocientes, também dividiriam o 3, o que não é possível pelo teorema da limitação.

Está verificado então que a divisibilidade é uma relação de ordem comum não total no conjunto dos naturais. Um importante fato da divisibilidade, agora fora do campo das propriedades de ordem, é a divisibilidade da combinação linear. Vamos constatar a mesma, que poderá vir a ser útil futuramente.

Teorema 3.19. *Para quaisquer $a, b, c \in \mathbb{N}$: se $a \mid b$ e $a \mid c$, então para quaisquer $x, y \in \mathbb{N}$: $a \mid (b \times x + c \times y)$.*

Demonstração. Esse fato decorre diretamente da distributiva e associativa. Se $a \mid b$ e $a \mid c$, então $b = a \times q$ e $c = a \times q'$, com $q, q' \in \mathbb{N}$. Logo $b \times x + c \times y = (a \times q) \times x + (a \times q') \times y = ... = a \times (q \times x + q' \times y)$ e portanto $b \times x + c \times y = a \times k$, para algum $k \in \mathbb{N}$ e $a \mid (b \times x + c \times y)$. □

Passamos assim à definição do operador de divisão e ao estudo de suas propriedades. Sejam $a, b \in \mathbb{N}$ com $b \mid a$ e $b \neq 0$. Então, pela definição de divisibilidade, existe $q \in \mathbb{N}$ tal que $a = b \times q$. Se fosse o caso $b = 0$, então $a = 0$ e $a = b \times q$ se verificaria para qualquer natural q. Mas como $b \neq 0$ o q é único, pois $a = b \times p$ e $a = b \times q \Rightarrow b \times p = b \times q \Rightarrow p = q$, pelo cancelamento da multiplicação.

Definição 3.10. Sejam $a, b \in \mathbb{N}$ com $b \mid a$ e $b \neq 0$. Definimos o operador binário, chamado **divisão**, $/ : X \to \mathbb{N}$, em que $X \subset \mathbb{N} \times \mathbb{N}$, com $X = \{(a, b) \in \mathbb{N} \times \mathbb{N} \mid b \neq 0 \text{ e } b \mid a\}$, e $a/b = q$ tal que $a = b \times q$.

Analogamente à subtração, temos $b \times (a/b) = (a/b) \times b = a$. Observamos também que $b \mid a \times b$ e portanto podemos fazer $(a \times b)/b$. E $(a \times b)/b = l$ tal que $b \times l = a \times b$. Logo $l = a$, pelo cancelamento, pois $b \neq 0$. Ou seja, quando $b \mid a$, $(a/b) \times b = (a \times b)/b = a$. Intuitivamente, sabemos que a divisão por b é a operação oposta à multiplicação por b e a ordem em que são realizadas não importa, dentro das situações em que é possível as duas ordens. Descontam-se os efeitos contrários. Também abordamos esse operador no contexto de estrutura associativa, comutativa, de cancelamento ou distributiva. Temos então as propriedades da divisão, que são obtidas de forma muito análoga àquela feita na subtração.

Proposição 3.22 (Elemento neutro da divisão)**.** *Para qualquer $a \in \mathbb{N}$: $1 \mid a$ e portanto $a/1$ está definido. E $a/1 = a$.*

Demonstração. Temos que $a = 1 \times a$, e assim $1 \mid a$ e $a/1 = k$ tal que $1 \times k = a$. Portanto, $a/1 = a$. E tanto a multiplicação quanto a divisão por 1 não alteram o resultado. □

Proposição 3.23 (Associatividade na divisão)**.** *Para quaisquer $a, b, c \in \mathbb{N}$, $c \neq 0$: se $c \mid b$, então $(a \times b)/c = a \times (b/c)$.*

Demonstração. Se $c \neq 0$ e $c \mid b$, então $c \times (b/c) = (b/c) \times c = b$. O que implica $a \times ((b/c) \times c) = a \times b$ e portanto $(a \times (b/c)) \times c = a \times b$. Como $b \mid a \times b$, temos que $c \mid a \times b$. Assim, $(a \times b)/c$ está definido e temos $((a \times (b/c)) \times c)/c = (a \times b)/c$. Portanto, $a \times (b/c) = (a \times b)/c$. □

Proposição 3.24 (Comutatividade na divisão)**.** *Para quaisquer* $a, b, c \in \mathbb{N}$*,* $c \neq 0$*: se* $c \mid a$*,* $(a \times b)/c = (a/c) \times b$*.*

Demonstração. Se $c \mid a$, como $a \mid a \times b$, então $c \mid a \times b$. Como $c \neq 0$, a divisão por c está definida, e temos então que $c \times (a/c) = (a/c) \times c = a$. E assim $((a/c) \times c) \times b = a \times b$, o que implica $(((a/c) \times b) \times c)/c = (a \times b)/c$. Portanto, $(a/c) \times b = (a \times b)/c$. □

Proposição 3.25 (Cancelamento da divisão - I)**.** *Para quaisquer* $a, b, c \in \mathbb{N}$*: se* $a \neq 0$*,* $a \mid b$ *e* $a \mid c$*, então* $b/a = c/a \Rightarrow b = c$*.*

Demonstração. Se $a \neq 0$, $a \mid b$ e $a \mid c$, estão definidas as divisões na hipótese. Desse modo, $a \times (b/a) = (b/a) \times a = b$ e ao mesmo tempo $a \times (c/a) = (c/a) \times a = c$. Então, $b/a = c/a \Rightarrow b = (b/a) \times a = (c/a) \times a = c$, e portanto $b = c$ e vale o cancelamento da divisão. □

Proposição 3.26 (Cancelamento da Divisão - II)**.** *Para quaisquer* $a, b, c \in \mathbb{N}$*: se* $a \mid c^+$ *e* $b \mid c^+$*, então* $c^+/a = c^+/b \Rightarrow a = b$*.*

Demonstração. Se $a \mid c^+$ e $b \mid c^+$, então $a, b \neq 0$ (caso contrário absurdo) e as divisões da hipótese estão definidas. Ademais, $c^+ = (c^+/a) \times a = (c^+/b) \times b \Rightarrow (c^+/a) \times a = (c^+/a) \times b$. Como $c^+/a \neq 0$ (caso contrário teríamos $c^+ = 0$), temos $a = b$, pelo cancelamento da multiplicação. □

Proposição 3.27 (Neutro da divisão é único)**.** *Temos que* $\exists x \in \mathbb{N} : \forall a \in \mathbb{N} : a/x = a$*. Ademais, tal* x *é único.*

Demonstração. Pelo que foi apresentado, 1 possui tal propriedade. Por outro lado, $a/x = a = a/1$, para qualquer $a \in \mathbb{N}$, então particularmente $k^+/x = k^+/1$. Do Teorema 3.26 segue que $x = 1$. □

Proposição 3.28 (Distributividade da divisão em relação à adição)**.** *Para quaisquer* $a, b, c \in \mathbb{N}$*: se* $a \neq 0$*,* $a \mid b$ *e* $a \mid c$*. Então,* $a \mid (b + c)$ *e* $(b + c)/a = b/a + c/a$*.*

Demonstração. Se $a \neq 0$, $a \mid b$ e $a \mid c$, então estão definidas as divisões b/a e c/a. Pelo Teorema 5.8, $a \mid (b + c)$ e está definida a divisão $(b + c)/a$. De modo que $((b + c)/a) \times a = a \times ((b + c)/a) = (b + c) = (b/a) \times a + (c/a) \times a$. Logo $((b + c)/a) \times a = (b/a + c/a) \times a$. Como $a \neq 0$, vale o cancelamento da multiplicação. Portanto, $(b + c)/a = b/a + c/a$, e vale a distributiva da divisão. □

Proposição 3.29 (Distributividade da divisão em relação à subtração)**.** *Para quaisquer* $a, b, c \in \mathbb{N}$*: se* $a \neq 0$*,* $a \mid b$*,* $a \mid c$*, e* $c \leq b$*, então,* $a \mid (b - c)$ *e* $(b - c)/a = b/a - c/a$*.*

Demonstração. Se $a \neq 0$, $a \mid b$ e $a \mid c$, temos as duas divisões b/a e c/a definidas. Como $c \leq b$ podemos definir $b - c$. Mas $b - c = a \times (b/a) - a \times (c/a)$. Desse modo, pela segunda distributiva da multiplicação. $a \times (b/a - c/a) = b - c$ e temos que $a \mid (b - c)$, com $(b - c)/a = q$ tal que $a \times q = (b - c) = a \times (b/a - c/a)$. Portanto, pelo cancelamento, $q = (b/a - c/a)$, ou seja, $(b - c)/a = b/a - c/a$ e a propriedade se verifica. □

Outra função que é bastante conveniente estudarmos, junto com as suas propriedades, é a potenciação. No contexto dos números naturais esse operador não possui o inconveniente da definição condicionada (utilizamos uma estratégia para contornar um caso), como ocorre com a subtração e a divisão. Suas propriedades são bastante importantes para uma série de cálculos futuros. Na realidade, devem ser estudadas posteriormente no contexto mais amplo de outros conjuntos numéricos. Ocorre que neste contexto já se manifestam os padrões característicos. Vamos então à definição, interpretando a precedência da potenciação sobre a multiplicação (e sobre a divisão).

Definição 3.11. Definimos o operador binário de **potenciação**, escrevemos $\widehat{\ }$, da seguinte forma.

a) Para todo $n \in \mathbb{N} : 0\widehat{\ }n^+ = 0$

b) Para todo $n \in \mathbb{N} : n^+\widehat{\ }0 = 1$

c) Para todo $n, m \in \mathbb{N} : n^+\widehat{\ }m^+ = n^+\widehat{\ }m \times n^+$

Verificamos que o operador está definido para todos os pares a, b de naturais, exceto $(0, 0)$. Observamos que não conseguimos obter o caso $0\widehat{\ }0$ da definição. Pela primeira condição, temos o operador definido para todos os pares de naturais em que o primeiro termo, a **base**, é igual a zero e o segundo, o **expoente**, é diferente de zero. Pela segunda condição, temos o operador definido para todos os pares de naturais em que o expoente é zero e a base é diferente de zero. E pela terceira condição, está definido para todos os pares de naturais em que a base e o expoente são diferentes de zero. O terceiro item é aplicado sucessivamente até chegarmos na situação do segundo. Quando começamos na situação do primeiro, o resultado já é aferido como 0, e não precisa aplicar recorrência.

Proposição 3.30. *(Elemento neutro da potenciação) Para qualquer $a \in \mathbb{N}$: $a\widehat{\ }1 = a$.*

Demonstração. Se $a = 0$, temos do primeiro item da definição que $0\widehat{\ }n^+ = 0$, para qualquer $n \in \mathbb{N}$, e em particular para $n = 0$. Portanto $0\widehat{\ }1 = 0$. Se $a = k^+$ para algum $k \in \mathbb{N}$, caímos no terceiro item e $k^+\widehat{\ }0^+ = k^+\widehat{\ }0 \times k^+ = 1 \times k^+ = k^+$, utilizando o segundo item. □

Proposição 3.31. *Para qualquer $a \in \mathbb{N}$: $1\widehat{\ }a = 1$.*

Demonstração. Seja $S = \{x \in \mathbb{N} \mid 1\widehat{\ }x = 1\}$. Verifica-se que $0 \in S$ da definição; e também que $1 \in S$. Por outro lado, se $n \in S$, então $1\widehat{\ }n^+ = 1\widehat{\ }n \times 1 = 1 \times 1 = 1$. Portanto, $n^+ \in S$, $S = \mathbb{N}$. E a propriedade vale para todos os naturais. □

Proposição 3.32 (Potenciação não é associativa)**.** *Não se tem que para quaisquer $a, b, c \in \mathbb{N}$: $(a\widehat{\ }b)\widehat{\ }c = a\widehat{\ }(b\widehat{\ }c)$.*

Não é difícil verificar tal fato informalmente. Vamos procurar um exemplo para ser desenvolvido. Consideremos então $(2\hat{}1)\hat{}2$ e $2\hat{}(1\hat{}2)$. Temos que $(2\hat{}1)\hat{}2 = 2\hat{}2 = 2\hat{}1 \times 2 = 2 \times 2 = 2 + 2 = 4$. Por outro lado $2\hat{}(1\hat{}2) = 2\hat{}1 = 2$. Logo $(2\hat{}1)\hat{}2 \neq 2\hat{}(1\hat{}2)$. Portanto, a propriedade associativa não vale.

Proposição 3.33 (Potenciação não é Comutativa)**.** *Não se tem que para quaisquer $a, b \in \mathbb{N}$: $a\hat{}b = b\hat{}a$.*

Consideremos um contraexemplo: $1\hat{}0 = 1 \neq 0 = 0\hat{}1$. Segue que não vale a comutatividade.

Proposição 3.34. *Para quaisquer $a, b \in \mathbb{N}$: $a\hat{}b = 0 \Rightarrow a = 0$.*

Demonstração. Provamos a contrapositiva. Se $a \neq 0$, $a = k^+$ para algum $k \in \mathbb{N}$. Então seja $S = \{x \in \mathbb{N} \mid k^+\hat{}x \neq 0\}$. Temos que $0 \in S$, pois $k^+\hat{}0 = 1$, da definição. Por outro lado, se $n \in S$, $k^+\hat{}n = p^+$ para algum $p \in \mathbb{N}$ e consideramos $k^+\hat{}n^+$. Temos que $k^+\hat{}n^+ = k^+\hat{}n \times k^+ = p^+ \times k^+ \neq 0$, da Proposição 3.20. Portanto, $a \neq 0 \Rightarrow a\hat{}b \neq 0$, para qualquer $b \in \mathbb{N}$. □

Proposição 3.35 (Distributiva da multiplicação para a base)**.** *Para quaisquer $a, b, c \in \mathbb{N}$: se $a \neq 0$ ou $b, c \neq 0$, então $a\hat{}(b + c) = a\hat{}b \times a\hat{}c$.*

Demonstração. Se $a = 0$, mas $b = p^+$ e $c = q^+$, a propriedade se verifica pois $0\hat{}(p^+ + q^+) = 0\hat{}(p^+ + q)^+ = 0 = 0\hat{}p^+ \times 0\hat{}q^+$. Consideramos o caso em que a base é diferente de 0. Seja $S = \{z \in \mathbb{N} \mid \forall x, y \in \mathbb{N} : x^+\hat{}(y + z) = x^+\hat{}y \times x^+\hat{}z\}$. Por verificação, temos que $0 \in S$. Se, por outro lado, $n \in S$, então $x^+\hat{}(y + n^+) = x^+\hat{}(y + (n + 1)) = x^+\hat{}(y + (1 + n)) = x^+\hat{}((y + 1) + n) = x^+\hat{}(y^+ + n) = x^+\hat{}y^+ \times x^+\hat{}n = (x^+\hat{}y \times x^+) \times x^+\hat{}n = x^+\hat{}y \times x^+\hat{}n^+$. Logo, $n^+ \in S$, $S = \mathbb{N}$ e temos a regra "conserva a base, soma os expoentes". □

Proposição 3.36 (Distributiva da divisão para a base)**.** *Para quaisquer $a, b, c \in \mathbb{N}$ com $c \leq b$: se $a \neq 0$, então $a\hat{}(b - c) = a\hat{}b / a\hat{}c$.*

Demonstração. Seja $S = \{y \in \mathbb{N} \mid \forall x, z \in \mathbb{N} \text{ com } z \leq y : x^+\hat{}(y - z) = x^+\hat{}y / x^+\hat{}z\}$. Por verificação, temos que $0 \in S$. Se, por outro lado, $n \in S$, então consideramos $x^+\hat{}(n^+ - z)$. Temos três possibilidades para $z \leq n^+$. Se $z = 0$, temos $z \leq n^+$, e portanto a subtração fica definida e também a propriedade se verifica. Se $z = n^+$, temos $x^+\hat{}0 = 1 = q/q = x^+\hat{}n^+ / x^+\hat{}z$. Por outro lado, se $z = t^+$ e $z < n^+$, temos que $n^+ = z + e^+$ para algum $e \in \mathbb{N}$. Assim, $n^+ = (z + e)^+$, $n = z + e$ e logo $z \leq n$. Devemos ter $z - 1$ definido, pois $z = t + 1$; e $z - 1 \leq n$, pois $n = (z - 1) + 1 + e$. Ao mesmo tempo, $(n + 1) - z = n - (z - 1)$. Logo $x^+\hat{}(n^+ - z) = x^+\hat{}(n - (z - 1)) = x^+\hat{}n / x^+\hat{}(z - 1) = (x^+\hat{}n \times x^+) / (x^+\hat{}(z - 1) \times x^+) = (x^+\hat{}n^+) / (x^+\hat{}z)$. Portanto, $n^+ \in S$, $S = \mathbb{N}$ e temos a regra "conserva a base, subtrai os expoentes". □

Proposição 3.37 (Potência de potência)**.** *Para quaisquer $a, b, c \in \mathbb{N}$: se $a \neq 0$ ou $b, c \neq 0$, então $(a\hat{}b)\hat{}c = a\hat{}(b \times c)$.*

Demonstração. Se $a = 0$, mas $b = p^+$ e $c = q^+$, temos $(0\hat{}p^+)\hat{}q^+ = 0\hat{}q^+ = 0 = 0\hat{}(p^+ \times q^+)$. Em contrapartida, se $a \neq 0$, consideramos então o conjunto $S = \{z \in \mathbb{N} \mid \forall x, y \in \mathbb{N} : (x^+\hat{}y)\hat{}z = x^+\hat{}(y \times z)\}$. Por verificação $0 \in S$, pois $(x^+\hat{}y)\hat{}0 = 1 = x^+\hat{}(y \times 0)$. Por outro lado, se $n \in S$, $(x^+\hat{}y)\hat{}n^+ = (x^+\hat{}y)\hat{}n \times (x^+\hat{}y) = x^+\hat{}(y \times n) \times (x^+\hat{}y) = x^+\hat{}(y \times n + y) = x^+\hat{}(y \times n^+)$. Portanto, temos a regra "conserva a base, multiplica os expoentes". □

Proposição 3.38 (Distributiva da multiplicação do expoente)**.** *Para quaisquer $a, b, c \in \mathbb{N}$: se $a \neq 0$ ou $b, c \neq 0$, então $(b \times c)\hat{}a = b\hat{}a \times c\hat{}a$.*

Demonstração. Se $a = 0$, mas $b = p^+$ e $c = q^+$, temos que a propriedade se verifica. Por outro lado, consideramos o caso $a \neq 0$. Seja $S = \{x \in \mathbb{N} \mid \forall y, z \in \mathbb{N} : (y \times z)\hat{}x^+ = y\hat{}x^+ \times z\hat{}x^+\}$. Verificamos que $0 \in S$. Em contrapartida, se $n \in S$, então $(y \times z)\hat{}n^{++} = (y \times z)\hat{}n^+ \times (y \times z) = (y\hat{}n^+ \times z\hat{}n^+) \times (y \times z) = (y\hat{}n^+ \times y) \times (z\hat{}n^+ \times z) = y\hat{}n^{++} \times z\hat{}n^{++}$. Portanto, $n^+ \in S$, $S = \mathbb{N}$ e vale a propriedade. □

Proposição 3.39 (Distributiva da divisão do expoente)**.** *Para quaisquer $a, b, c \in \mathbb{N}$: se $c \neq 0$, $c \mid b$ e ($a \neq 0$ ou $b \neq 0$), então $(b/c)\hat{}a = b\hat{}a/c\hat{}a$.*

Demonstração. Se $a = 0$, mas $b = p^+$, e $c \neq 0$ com $c \mid b$, temos que a divisão da hipótese está definida, é diferente de 0 e a propriedade se verifica. Por outro lado, consideramos o caso $a \neq 0$. Então, seja $S = \{x \in \mathbb{N} \mid \forall y, z \in \mathbb{N} \text{ com } z \neq 0 \ \wedge \ z \mid y : (y/z)\hat{}x^+ = y\hat{}x^+/z\hat{}x^+\}$. Verificamos que $0 \in S$. Em contrapartida, se $n \in S$, então $(y/z)\hat{}n^{++} = (y/z)\hat{}n^+ \times (y/z) = (y\hat{}n^+/z\hat{}n^+) \times (y/z) = r \times s$, com $r = y\hat{}n^+/z\hat{}n^+$ e $s = (y/z)$. Mas $(r \times z\hat{}n^+) \times (s \times z) = (r \times s) \times (z\hat{}n^{++}) = y\hat{}n^{++}$. Logo, $z\hat{}n^{++} \mid y\hat{}n^{++}$, $z \neq 0 \Rightarrow z\hat{}n^{++} \neq 0$ e podemos fazer a divisão $y\hat{}n^{++}/z\hat{}n^{++} = r \times s$. Assim, $y\hat{}n^{++}/z\hat{}n^{++} = (y/z)\hat{}n^{++}$. Portanto, $n^+ \in S$, $S = \mathbb{N}$ e vale a propriedade. □

Proposição 3.40 (Cancelamento da potenciação - I)**.** *Para quaisquer $a, b, c \in \mathbb{N}$: $a^{++}\hat{}b = a^{++}\hat{}c \Rightarrow b = c$.*

Demonstração. Se $a^{++}\hat{}b = a^{++}\hat{}c$, suponhamos que $b \neq c$. Então, segue do Teorema 4.26 que $b < c$ ou $c < b$. Os dois casos são logicamente idênticos, sendo assim basta fazer um deles. Supomos que $b < c$ e assim $c = b + k^+$ para algum $k \in \mathbb{N}$. Temos dessa forma $a^{++}\hat{}b = a^{++}\hat{}c = a^{++}\hat{}(b + k^+) = a^{++}\hat{}b \times a^{++}\hat{}k^+$. Logo, como $a^{++}\hat{}b \neq 0$, da Proposição 3.34, temos que $1 = a^{++}\hat{}k^+$ pelo cancelamento da multiplicação. Então $1 = a^{++}\hat{}k \times a^{++} = a^{++}\hat{}k \times a^+ + a^{++}\hat{}k$. Também pela Proposição 3.34, $a^{++}\hat{}k = p^+$, para algum $p \in \mathbb{N}$. Assim, $0^+ = p^+ \times a^+ + p^+ = q^+ + p^+ = (p + q)^{++}$, para algum $q \in \mathbb{N}$, pela Proposição 3.20. Temos assim um absurdo, pois ficamos com $0 = (p + q)^+$. De modo que $b \not< c$. Pelo mesmo tipo de argumento $c \not< b$. Portanto, $b = c$ e vale a propriedade. □

Proposição 3.41 (Cancelamento da potenciação - II)**.** *Para quaisquer $a, b, c \in \mathbb{N}$: $a\hat{}c^+ = b\hat{}c^+ \Rightarrow a = b$.*

Demonstração. Seja $S = \{z \in \mathbb{N} \mid \forall x, y \in \mathbb{N} : x < y \rightarrow x\hat{}z^+ < y\hat{}z^+\}$. Verificamos que $0 \in S$. Por outro lado, se $n \in S$, suponhamos que $x < y$. Então $x\hat{}n^+ < y\hat{}n^+$. Usaremos que para quaisquer $a, b, c, d \in \mathbb{N}$: $a < b$ e $c < d \Rightarrow a \times c < b \times d$, que decorre de outra propriedade provada posteriormente. Logo, $x\hat{}n^+ \times x < y\hat{}n^+ \times y$ e $x\hat{}n^{++} < y\hat{}n^{++}$. Assim, $n^+ \in S$ e $S = \mathbb{N}$. Desse modo, $a \neq b$ implica $a < b \veebar b < a$, que implica, para qualquer $c \in \mathbb{N}$, $a\hat{}c^+ < b\hat{}c^+ \veebar b\hat{}c^+ < a\hat{}c^+$, ou seja, $a\hat{}c^+ \neq b\hat{}c^+$. Obtemos assim a contrapositiva do que queríamos provar. Portanto, vale a propriedade. □

Utilizamos um fato ainda não demonstrado devido à preferência de se agrupar as propriedades semanticamente próximas. Deixamos junto aquilo que faz mais sentido. Naturalmente, seria mais bonito respeitar a ordem de requisitos das demonstrações, mas também é difícil abandonar o significado interessante que se obtém com a utilização da ordem na justificativa para as duas propriedades do cancelamento. Estamos utilizando o fato de que as funções são estritamente crescentes (tanto para a base como para o expoente), o que implica a injetividade.

Passamos agora ao estudo da radiciação, na forma geral, e a demonstração de suas propriedades. Após isso, investigaremos as compatibilidades de ordem e concluímos o capítulo. Passemos a definição de raiz n-ésima.

Definição 3.12. Sejam $b, n \in \mathbb{N}$, com $n \neq 0$. Se $b = a\hat{}n$, para algum $a \in \mathbb{N}$ podemos definir **raiz $n-$ésima de** b, escreve-se $\sqrt[n]{b}$, como $\sqrt[n]{b} = r$ tal que $r\hat{}n = b$.

Sabemos da Proposição 3.41 (como $n \neq 0$) que $a\hat{}n = r\hat{}n \Rightarrow a = r$ e desse modo tal r é único. Portanto, temos a operação bem definida. Assim, a raiz é um operador binário $\sqrt{\ } : S \rightarrow \mathbb{N}$, em que $S \subset \mathbb{N} \times \mathbb{N}$ com $S = \{(b, n) \in \mathbb{N} \times \mathbb{N} \mid b = a\hat{}n$, para algum $a \in \mathbb{N}\}$.

Da definição temos que $(\sqrt[n]{b})\hat{}n = b$. Vamos então às propriedades do operador de radiciação.

Proposição 3.42 (Distributividade da radiciação em relação à multiplicação)**.** *Para quaisquer $a, b, n \in \mathbb{N}$, com $n \neq 0$: se $a = p\hat{}n$ e $b = q\hat{}n$, então $\sqrt[n]{a \times b} = \sqrt[n]{a} \times \sqrt[n]{b}$.*

Demonstração. Se $n \neq 0$, $a = p\hat{}n$ e $b = q\hat{}n$, para determinados $p, q \in \mathbb{N}$. Então, as raízes do lado direito estão definidas e $\sqrt[n]{a} = p$, $\sqrt[n]{b} = q$. Ademais, utilizando a distributiva da potenciação, $(\sqrt[n]{a} \times \sqrt[n]{b})\hat{}n = (\sqrt[n]{a}\hat{}n \times \sqrt[n]{b}\hat{}n) = a \times b$. Logo, existe $r \in \mathbb{N}$ $(r = \sqrt[n]{a} \times \sqrt[n]{b})$ tal que $r\hat{}n = a \times b$. Assim a raiz $\sqrt[n]{a \times b}$ está definida e é igual a r. Portanto, $\sqrt[n]{a \times b} = (\sqrt[n]{a} \times \sqrt[n]{b})$ e vale a propriedade. □

Proposição 3.43 (Distributividade da radiciação em relação à divisão)**.** *Para quaisquer $a, b, n \in \mathbb{N}$, com $b, n \neq 0$: se $a = p\hat{}n$, $b = q\hat{}n$ e $b \mid a$, então $\sqrt[n]{a/b} = \sqrt[n]{a}/\sqrt[n]{b}$.*

Demonstração. Se $b, n \neq 0$, $a = p\hat{}n$ e $b = q\hat{}n$, para determinados $p, q \in \mathbb{N}$. Então, as raízes do lado direito estão definidas, $\sqrt[n]{a} = p$, e $\sqrt[n]{b} = q$. Temos também que $\sqrt[n]{b} \neq 0$ pois caso contrário, como $(\sqrt[n]{b})\hat{}n = b$, teríamos $b = 0$. Mas ainda precisamos garantir que $\sqrt[n]{b} \mid \sqrt[n]{a}$. Supomos que isso seja verdade, pois a demonstração demanda o lema de Euclides.

Assim assumimos que a divisão à direita está definida e utilizamos a distributiva da potenciação, $(\sqrt[n]{a}/\sqrt[n]{b})\hat{}n = (\sqrt[n]{a\hat{}n}/\sqrt[n]{b\hat{}n}) = a/b$. Logo, existe $r \in \mathbb{N}$ ($r = \sqrt[n]{a}/\sqrt[n]{b}$) tal que $r\hat{}n = a/b$. Assim a raiz $\sqrt[n]{a/b}$ está definida e é $= r$. Portanto, $\sqrt[n]{a/b} = (\sqrt[n]{a}/\sqrt[n]{b})$ e vale a propriedade. □

Proposição 3.44. *Raiz de raiz] Para quaisquer $a, m, n \in \mathbb{N}$, com $m, n \neq 0$: se $a = p\hat{}(m \times n)$, para algum $p \in \mathbb{N}$ então $\sqrt[m]{\sqrt[n]{a}} = \sqrt[n]{\sqrt[m]{a}} = \sqrt[m\times n]{a}$.*

Demonstração. Se $a = p\hat{}(m \times n)$ então está definida a raiz à direita da equação. Também, $a = p\hat{}(m \times n) = (p\hat{}n)\hat{}m = (p\hat{}m)\hat{}n$. Portanto, temos $\sqrt[m]{\sqrt[n]{a}} = \sqrt[m]{\sqrt[n]{(p\hat{}m)\hat{}n}} = \sqrt[m]{p\hat{}m} = p = \sqrt[n]{p\hat{}n} = \sqrt[n]{\sqrt[m]{(p\hat{}m)\hat{}n}} = \sqrt[n]{\sqrt[m]{a}}$. □

As propriedades de compatibilidades para $<$ (as compatibilidades para $\leq$ ficam estabelecidas imediatamente, pois os casos de $=$ se verificam), bem como para divisibilidade e finalizamos este capítulo serão dadas pelas proposições a seguir.

Proposição 3.45 (Compatibilidade $<$ e adição)**.** *Para quaisquer $a, b, k \in \mathbb{N}$: se $a < b$ então $a + k < b + k$.*

Demonstração. Se $a < b$, então $b = a + p^+$ para algum $p \in \mathbb{N}$. Logo, $k + b = (k + a) + p^+$, ou seja, $b + k = (a + k) + p^+$, e também ficamos com $a + k < b + k$. □

Proposição 3.46 (Compatibilidade $<$ e subtração)**.** *Para quaisquer $a, b, k \in \mathbb{N}$: se $k \leq a$ e $a < b$ então $a - k < b - k$.*

Demonstração. Se $a < b$ e $k \leq a$, então $b = a + p^+$ para algum $p \in \mathbb{N}$, e $a = k + q$, para algum $q \in \mathbb{N}$. Assim, $b = k + (q + p)^+$ e $k < b$, o que implica $k \leq b$. Então $a - k$ e $b - k$ estão definidos. Se fosse o caso que $a - k = b - k$ teríamos $(a - k) + k = a = b = (b - k) + k$, impossível. Se tivéssemos $b - k < a - k$, da propriedade anterior teríamos $(b - k) + k = b < a = (a - k) + k$, também impossível. Portanto, da tricotomia a única alternativa adequada é $a - k < b - k$. □

Proposição 3.47 (Compatibilidade $<$ e produto)**.** *Para quaisquer $a, b, k \in \mathbb{N}$: se $a < b$ então $a \times k^+ < b \times k^+$.*

Demonstração. Seja $S = \{z \in \mathbb{N} \mid \forall x, y \in \mathbb{N} : x < y \Rightarrow x \times z^+ < y \times z^+\}$ Por verificação, $0 \in S$. Por outro lado, se $n \in S$, suponhamos $x < y$. Logo $x \times n^+ < y \times n^+$ e $y \times n^+ = x \times n^+ + p^+$ para algum $p \in \mathbb{N}$. Como $x < y$, podemos somar os valores iguais dos dois lados da desigualdade. Assim, $x + x \times n^+ + p^+ < y + y \times n^+$ e obtemos com $x \times n^{++} + p^+ < y \times n^{++}$. Mas também ocorre que $x \times n^{++} < x \times n^{++} + p^+$. Portanto, $x \times n^{++} < y \times n^{++}$, $n^+ \in S$, $S = \mathbb{N}$ e vale a compatibilidade com o produto. □

Proposição 3.48 (Compatibilidade $<$ e divisão)**.** *Para quaisquer $a, b, k \in \mathbb{N}$ com $k \neq 0$: se $k \mid a, b$ e $a < b$ então $a/k < b/k$.*

Demonstração. Se $k \neq 0$, $k \mid a$ e $k \mid b$, então a/k e b/k estão definidos. Se fosse o caso que $a/k = b/k$ teríamos $(a/k) \times k = a = b = (b/k) \times k$, impossível. E se tivéssemos $b/k < a/k$, da propriedade anterior teríamos $(b/k) \times k = b < a = (a/k) \times k$, também impossível. Portanto, da tricotomia a única alternativa adequada é $a/k < b/k$. □

Proposição 3.49 (Compatibilidade $<$ e potenciação)**.** *Para quaisquer $a, b, k \in \mathbb{N}$: se $a < b$ então $a^{\frown}k^{+} < b^{\frown}k^{+}$.*

Demonstração. Se $a = 0$, temos que $b \neq 0$ e $a^{\frown}k^{+} = 0 < b^{\frown}k^{+} \neq 0$. Consideramos o caso em que $a = x^{+} \neq 0$. Seja $S = \{z \in \mathbb{N} \mid \forall x, y \in \mathbb{N} : x^{+} < y \Rightarrow x^{+\frown}z^{+} < y^{\frown}z^{+}\}$ Por verificação, $0 \in S$. Por outro lado, se $n \in S$, suponhamos $x^{+} < y$. Logo $x^{+\frown}n^{+} < y^{\frown}n^{+}$. Assim, $x^{+\frown}n^{+} \times y < y^{\frown}n^{+} \times y$, pois $y \neq 0$. Como $x^{+\frown}n^{+} \neq 0$ e $x^{+} < y$, então $x^{+\frown}n^{+} \times x^{+} < x^{+\frown}n^{+} \times y$. Desse modo, $x^{+\frown}n^{++} < y^{\frown}n^{++}$. Portanto, $n^{+} \in S$, $S = \mathbb{N}$ e a propriedade se verifica. □

Proposição 3.50 (Compatibilidade $<$ e radiciação)**.** *Para quaisquer $a, b, k \in \mathbb{N}$ com $k \neq 0$, $a = p^{\frown}k$ e $a = q^{\frown}k$: se $a < b$ então $\sqrt[k]{a} < \sqrt[k]{b}$.*

Demonstração. Se $k \neq 0$, $a = p^{\frown}k$ e $b = q^{\frown}k$, então $\sqrt[k]{a}$ e $\sqrt[k]{b}$ estão definidos. Se fosse o caso que $\sqrt[k]{a} = \sqrt[k]{b}$ teríamos $\sqrt[k]{a}^{\frown}k = a = b = \sqrt[k]{b}^{\frown}k$, impossível. E se tivéssemos $\sqrt[k]{b} < \sqrt[k]{a}$, da propriedade anterior teríamos $\sqrt[k]{b}^{\frown}k = b < a = \sqrt[k]{a}^{\frown}k$, também impossível. Portanto, da tricotomia a única alternativa adequada é $\sqrt[k]{a} < \sqrt[k]{b}$. □

Interessante observar que podemos pensar as compatibilidades também no contexto da ordem comum parcial estabelecida com a relação de divisibilidade. Verifiquemos quais operações apresentam a compatibilidade e quais não apresentam.

Proposição 3.51 (Incompatibilidade $\mid$ e adição)**.** *Não se tem que para quaisquer $a, b, k \in \mathbb{N}$: se $a \mid b$ então $a + k \mid b + k$.*

Consideremos o caso particular com os números 1 e 2. Sabemos que $1 \mid 2$, mas $2 \nmid 3$, como já foi verificado.

Proposição 3.52 (Incompatibilidade $\mid$ e subtração)**.** *Não se tem que para quaisquer $a, b, k \in \mathbb{N}$: se $k \leq a, b$ e $a \mid b$ então $a - k \mid b - k$.*

Consideramos o caso particular com os números 1 e 2. $1 \mid 2$, mas $1 - 1 = 0 \nmid 1 = 2 - 1$. Lembramos que nenhuma divisão por zero está definida, mas a divisibilidade sim, e o único número divisível por 0 é ele mesmo. Esse caso não é muito significativo mas é o mais fácil de encaixar na formalidade.

O próximo caso seria com os números 3 e $6 = 3^{+++} = (3 + 0)^{+++} = 3 + 3 = 3 \times 2$. Temos que $3 \mid 6$, mas $2 \nmid 5$, pois $2 \times 1 = 2$ $2 \times 2 = 2^{++}$, $2 \times 3 = 2^{++++} = 5^{+}$, e a possibilidade 4 para quociente também seria maior do que 5 e portanto $\neq 5$. Pelo cálculo aritmético, a verificação é trivial. A proposta entretanto é verificar pelas definições. Por isso tomamos os menores casos possíveis.

Proposição 3.53 (Compatibilidade $\mid$ e produto)**.** *Para quaisquer $a, b, k \in \mathbb{N}$: se $a \mid b$ então $a \times k \mid b \times k$.*

Demonstração. Se $a \mid b$, então $b = a \times p$ para algum $p \in \mathbb{N}$. Logo, $k \times b = k \times (a \times p)$, ou seja, $b \times k = (a \times k) \times p$, e também ficamos com $a \times k \mid b \times k$. □

Proposição 3.54 (Compatibilidade $\mid$ e divisão)**.** *Para quaisquer $a, b, k \in \mathbb{N}$ com $k \neq 0$: se $k \mid a, b$ e $a \mid b$ então $a/k \mid b/k$.*

Demonstração. Se $k \neq 0$ e $k \mid a, b$, as divisões a/k e b/k estão definidas. Ademais, como $b \mid a$, $b = a \times p$ para algum $p \in \mathbb{N}$. Logo, $(b/k) \times k = ((a/k) \times k) \times p$ e $(b/k) \times k = ((a/k) \times p) \times k$. Assim, como $k \neq 0$, $(b/k) = (a/k) \times p$, temos que $a/k \mid b/k$. Naturalmente, se $a \neq 0$, b/a está definido e $b/a = (b/k)/(a/k)$ o que nos fornece uma ferramenta para simplificar divisões, passando para cálculo com números menores. □

Proposição 3.55 (Compatibilidade $\mid$ e potenciação)**.** *Para quaisquer $a, b, k \in \mathbb{N}$: se $a \mid b$ então $a \hat{} k^+ \mid b \hat{} k^+$. Ademais, se $b \neq 0$, $a \hat{} 0 = 1 \mid 1 = b \hat{} 0$.*

Demonstração. Seja $S = \{z \in \mathbb{N} \mid \forall x, y \in \mathbb{N} : x \mid y \Rightarrow x \hat{} z^+ \mid y \hat{} z^+\}$ Por verificação, $0 \in S$. Por outro lado, se $n \in S$, suponhamos $x \mid y$. Logo $x \hat{} n^+ \mid y \hat{} n^+$ e $y \hat{} n^+ = x \hat{} n^+ \times p$ para algum $p \in \mathbb{N}$. Como $x \mid y$, podemos multiplicar valores iguais dos dois lados da inequação. Assim, $x \times (x \hat{} n^+ \times p) \mid y \times (y \hat{} n^+)$ e ficamos com $x \hat{} n^{++} \times p \mid y \hat{} n^{++}$. Mas também ocorre que $x \hat{} n^{++} \mid x \hat{} n^{++} \times p$ e portanto $x \hat{} n^{++} \mid y \hat{} n^{++}$. Desse modo, $n^+ \in S$, $S = \mathbb{N}$ e vale a compatibilidade com o produto. □

Proposição 3.56 (Compatibilidade $\mid$ e radiciação)**.** *Para quaisquer $a, b, k \in \mathbb{N}$ com $k \neq 0$, $a = p \hat{} k$ e $a = q \hat{} k$: se $a \mid b$ então $\sqrt[k]{a} \mid \sqrt[k]{b}$.*

Esta última compatibilidade foi utilizada na Proposição 3.43 e não será demonstrada por exigir que tenhamos desenvolvido o lema de Euclides.

O objetivo deste capítulo foi relacionar aquilo que é o mais básico e que utilizamos com frequência. Isso foi feito também de modo que as propriedades aparecessem em uma ordem organizada. A partir de um determinado momento, aqueles fatos que se sugerem imediatamente após outros acabam por exigir uma maior profundidade teórica que a esperada. Isso ocorreu com a Proposição 3.41, que utilizou uma consequência da Proposição 3.47; e com a Proposição **??**, que é necessária também na Proposição 3.56. Passamos à construção dos axiomas para a aritmética dos inteiros, que é mais abrangente que a dos naturais. A partir desses, fazemos um estudo menos extenso como foi feito neste capítulo.

4 A CONSTRUÇÃO DOS NÚMEROS INTEIROS

Neste capítulo iremos fazer apenas a construção dos axiomas principais do conjunto $\mathbb{Z}$, que o fazem domínio de integridade, uma estrutura algébrica que pode ser estudada de forma abstrata. Também introduziremos uma relação que é uma ordem denominada "compatível com a estrutura de anel". Para isso, utilizaremos a construção tradicional de conjuntos de equivalência em pares ordenados de naturais.

Consideremos $\mathbb{N} \times \mathbb{N}$ o produto cartesiano do conjunto dos números naturais, ou seja, o conjunto de pares ordenados (a, b) com $a, b \in \mathbb{N}$. Seja $\sim$ uma relação nesse conjunto definida por $(a, b) \sim (c, d) \Leftrightarrow a + d = b + c$. Caso $a > b$, tal condição, se traduz essencialmente no fato $a - b = c - d$. Se $b > a$, a condição se traduz em $b - a = d - c$. Nesse caso, trabalharemos apenas com a adição.

Proposição 4.1. *A relação acima criada é uma relação de equivalência. Ou seja, é transitiva, simétrica e reflexiva.*

Demonstração. Começamos pela transitividade. Sejam (a, b), (c, d) e (e, f) pares ordenados de naturais, com $(a, b) \sim (c, d)$ e $(c, d) \sim (e, f)$. Então $(a + d) = (b + c)$ e $(c + f) = (d + e)$. Logo, adicionando termo a termo ficamos com

$$(a + d) + (c + f) = (b + c) + (d + e) \Rightarrow (a + d) + (f + c) = (b + c) + (e + d) \Rightarrow$$

$$((a + d) + f) + c = ((b + c) + e) + d \Rightarrow (a + (d + f)) + c = (b + (c + e)) + d \Rightarrow$$

$$(a + (f + d)) + c = (b + (e + c)) + d \Rightarrow ((a + f) + d) + c = ((b + e) + c) + d \Rightarrow$$

$$(a + f) + (d + c) = (b + e) + (c + d) \Rightarrow (a + f) + (c + d) = (b + e) + (c + d) \Rightarrow (a + f) = (b + e).$$

Portanto, $(a, b) \sim (e, f)$.

A simetria se verifica facilmente. Se $(a, b) \sim (c, d)$ então $(a + d) = (b + c) \Rightarrow (c + b) = (d + a) \Rightarrow (c, d) \sim (a, b)$.

A propriedade reflexiva, finalmente, também decorre da comutatividade da adição. $(a, b) \sim (a, b)$ pois $(a + b) = (b + a)$. □

Vamos agora mostrar como $\mathbb{Z}$ pode ser compreendido como o conjunto de classes de equivalência de tal relação em $\mathbb{N} \times \mathbb{N}$. Definimos a adição da seguinte forma.

Sejam $A, B \in \mathbb{Z}$. A e B são subconjuntos não vazios de $\mathbb{N} \times \mathbb{N}$. Consideramos, os elementos $(a, b) \in A$ e $(c, d) \in B$. Denotamos a classe de equivalência A por $[(a, b)]$ e B por $[(c, d)]$. Definimos a soma de A e B por

$$A \oplus B = [(a + c, b + d)].$$

Precisamos verificar se a adição definida de $A, B \in \mathbb{Z}$ está bem definida. Ou seja, se essa

soma é de fato uma função de $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$. Para isso, precisamos que a soma seja independente dos representantes de classe de A e B. Mais especificamente, queremos que se $(a, b) \sim (a', b')$ e $(c, d) \sim (c', d')$ então $(a + c, b + d) \sim (a' + c', b' + d')$. Constatemos isso.

Teorema 4.1 (Adição é bem definida)**.** *Sejam $A, B \in \mathbb{Z}$, com $A = [(a, b)]$ e $B = [(c, d)]$. A operação $\oplus : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, está bem definida pela expressão $A \oplus B = [(a, b)] \oplus [(c, d)] = [(a + c, b + d)]$.*

Demonstração. Se $A = [(a, b)]$ e ao mesmo tempo $A = [(a', b')]$, então $(a, b) \sim (a', b')$. Por outro lado, se $B = [(c, d)]$ e ao mesmo tempo $B = [(c', d')]$, então $(c, d) \sim (c', d')$. Temos assim $a+b' = b+a'$ e $c+d' = d+c'$. O que implica $(a+b')+(c+d') = (b+a')+(d+c') \Rightarrow (a+c)+(b'+d') = (b + d) + (a' + c') \Rightarrow (a + c, b + d) \sim (a' + c', b' + d')$. E a escolha dos representantes de classe não interfere no resultado. Portanto, a adição está bem definida. □

Definimos a multiplicação, por sua vez, da seguinte forma.

Definição 4.1. Sejam $A, B \in \mathbb{Z}$. A e B são subconjuntos não vazios de $\mathbb{N} \times \mathbb{N}$. Então, tomamos os elementos $(a, b) \in A$ e $(c, d) \in B$. Podemos denotar a classe de equivalência A por $[(a, b)]$ e naturalmente, B por $[(c, d)]$. Queremos definir a multiplicação de A e B por $A \otimes B = [(ac + bd, ad + bc)]$

Observamos que, curiosamente, essa expressão é quase idêntica à multiplicação de números complexos, que será vista adiante. Precisamos também verificar se o produto assim expresso de $A, B \in \mathbb{Z}$ está bem definido [1]. Constatemos isso.

Teorema 4.2. *(Multiplicação é Bem Definida) Sejam $A, B \in \mathbb{Z}$ Com $A = [(a, b)]$ e $B = [(c, d)]$. A operação $\otimes : \mathbb{Z} \to \mathbb{Z}$, está bem definida pela expressão $A \otimes B = [(a, b)] \otimes [(c, d)] = [(ac + bd, ad + bc)]$.*

Demonstração. Se $A = [(a, b)]$ e ao mesmo tempo $A = [(a', b')]$, então $(a, b) \sim (a', b')$. Por outro lado, se $B = [(c, d)]$ e ao mesmo tempo $B = [(c', d')]$, então $(c, d) \sim (c', d')$. Temos então $a+b' = b+a'$ e $c+d' = d+c'$. Cabe uma breve explicação para o cálculo abaixo. Essencialmente, estamos trocando os termos se multiplicando. No início, para cada troca que queremos realizar no parênteses maior à esquerda, somamos um termo no parênteses maior à direita. E assim procedemos para cada termo. No final, conseguimos transformar a soma que tínhamos na soma pretendida sem alterar o termo maior à direita. E ficamos com a igualdade pretendida. Os passos intermediários de associatividade são omitidos por gerarem um detalhismo desnecessário para entender a ideia central. Calculamos

$$\begin{aligned}(ac + bd + a'd' + b'c') + (a'c + b'c + a'd + b'd) = \\ &= (a + b')c + (b + a')d + a'(c + d') + b'(d + c') \\ &= (b + a')c + (a + b')d + a'(d + c') + b'(c + d')\end{aligned}$$

[1] A demonstração foi baseada em: <https://proofwiki.org/wiki/Integer_Multiplication_is_Well-Defined>. Acesso em 5 de nov. de 2021.

pois $a + b' = b + a'$, $c + d' = d + c'$ Segue que

$$\begin{aligned}(ac + bd + a'd' + b'c') + (a'c + b'c + a'd + b'd) &= \\ &= bc + a'c + b'd + ad + a'd + a'c' + b'c + b'd' \\ &= (ad + bc + a'c' + b'd') + (a'c + b'c + a'd + b'd).\end{aligned}$$

Logo,

$$(ac + bd + a'd' + b'c') = (ad + bc + a'c' + b'd')$$

e

$$[(ac + bd, ad + bc)] = [(a'c' + b'd', a'd' + b'c')].$$

Deste modo, a escolha dos representantes de classe não interfere no resultado. Portanto, a multiplicação está bem definida. □

Devemos estabelecer as propriedades mais importantes das operações com inteiros: associatividade, comutatividade, cancelamento, distributividade, elemento neutro etc. Muitas das propriedades têm a mesma forma daquelas já estabelecidas para o contexto dos números naturais. Por simplicidade, não iremos utilizar os símbolos $\oplus$ e $\otimes$. Lembremos apenas qual é a operação que estamos expressando pelo contexto.

Proposição 4.2 (Elemento neutro da adição)**.** *Existe um elemento neutro da adição. Ademais, este elemento neutro é único.*

Demonstração. Seja $0 \in \mathbb{Z}$ definido como $0 = [(x, x)]$, para algum $x \in \mathbb{N}$. Então, para qualquer $A \in \mathbb{Z}$: $A + 0 = 0 + A = A$. Seja $A = [(a, b)]$, com $a, b \in \mathbb{N}$. Temos então que $A+0 = [(a, b)]+[(x, x)] = [(a+x, b+x)] = [(x+a, x+b)] = 0+A$. Por outro lado, $(a, b) \sim (a+x, b+x)$, pois $a + (b + x) = (a + b) + x = (b + a) + x = b + (a + x)$. Assim, $A + 0 = A$. Vale mencionar que $(x, x) \sim (0, 0)$. Para a unicidade, seja $0'$ tal que $A + 0' = 0' + A = A$, também para qualquer A. Então, em particular $0' = 0' + 0 = 0 + 0' = 0$. Logo, $0' = 0$, o que significa que o elemento neutro é único. □

Proposição 4.3 (Associatividade da adição)**.** *Para quaisquer $A, B, C \in \mathbb{Z}$: $(A+B)+C = A+(B+C)$.*

Demonstração. Sejam $A = [(a, b)]$, $B = [(c, d)]$ e $C = [(e, f)]$, com $a, b, c, d, e, f \in \mathbb{N}$. Temos então que $(A+B)+C = ([(a, b)]+[(c, d)])+[(e, f)] = [(a+c, b+d)]+[(e, f)] = [((a+c)+e, (b+d)+f)] = [a + (c + e), b + (d + f)] = [(a, b)] + [(c + e, d + f)] = [(a, b)] + ([(c, d)] + [(e, f)]) = A + (B + C)$. Assim, $(A + B) + C = A + (B + C)$ e vale a propriedade. □

Proposição 4.4 (Comutatividade da adição)**.** *Para quaisquer $A, B \in \mathbb{Z}$: $A + B = B + A$.*

Demonstração. Sejam $A = [(a, b)]$, $B = [(c, d)]$, com $a, b, c, d \in \mathbb{N}$. Temos então que $A + B = [(a, b)] + [(c, d)] = [(a + c, b + d)] = [(c + a, d + b)] = [(c, d)] + [(a, b)]$. Assim, $A + B = B + A$ e vale a propriedade. □

Proposição 4.5 (Cancelamento da adição)**.** *Para quaisquer $A, B, C \in \mathbb{Z}$: $B+A = C+A \Rightarrow B = C$.*

Demonstração. Sejam $A = [(a, b)]$, $B = [(c, d)]$ e $C = [(e, f)]$, com $a, b, c, d, e, f \in \mathbb{N}$. Suponhamos então que $B+A = C+A$. Assim, $[(c, d)]+[(a, b)] = [(e, f)]+[(a, b)] \Rightarrow [(c+a, d+b)] = [(e+a, f+b)] \Rightarrow (c+a)+(f+b) = (d+b)+(e+a) \Rightarrow (c+f)+(a+b) = (d+e)+(a+b) \Rightarrow c+f = d+e \Rightarrow (c, d) \sim (e, f)$. E portanto $B = C$ e vale a propriedade. □

Esta última propriedade poderia ser obtida também do elemento oposto da adição com a associatividade. Desta forma, não precisa ser um axioma na caracterização de domínio de integridade.

Proposição 4.6 (Elemento oposto da adição)**.** *Para qualquer $A \in \mathbb{Z}$, existe $B \in \mathbb{Z}$ tal que $A + B = B + A = 0$. Ademais, se B' também é tal que $A + B' = B' + A = 0$. Então $B' = B$. Ou seja, B é único, para cada A.*

Demonstração. Sejam $A = [(a, b)]$, com $a, b \in \mathbb{N}$ e $B = [(b, a)]$. Então $A + B = [(a, b)] + [(b, a)] = [(a + b, b + a)] = [(b + a, a + b)] = B + A$. Como $[(x, x)] = [(0, 0)]$, temos $A + B = B + A = 0$. Para a unicidade, seja B' tal que $A + B' = 0$. Então, em particular $B' = B' + 0 = B' + (A + B) = (B' + A) + B = 0 + B = B$. Logo $B' = B$, o que significa que o oposto é único para cada elemento. Observamos que a unicidade aqui também não precisou se preocupar com a natureza interna do número inteiro, como par ordenado de naturais. □

Expomos agora as propriedades da multiplicação.

Proposição 4.7 (Associatividade da multiplicação)**.** *Para quaisquer $A, B, C \in \mathbb{Z}$: $(A \times B) \times C = A \times (B \times C)$.*

Demonstração. Sejam $A = [(a, b)]$, $B = [(c, d)]$ e $C = [(e, f)]$, com $a, b, c, d, e, f \in \mathbb{N}$. Segue que

$$
\begin{aligned}
(A \times B) \times C &= (([(a, b)] \times [(c, d)]) \times [(e, f)]) \\
&= (([ac + bd, ad + bc]) \times ([e, f])) \\
&= ([((ac + bd)e + (ad + bc)f, (ac + bd)f + (ad + bc)e)]) \\
&= ([(ace + bde + adf + bcf, acf + bdf + ade + bce)]) \\
&= ([(ace + adf + bcf + bde, acf + ade + bce + bdf)]) \\
&= ([(a(ce + df) + b(cf + de), a(cf + de) + b(ce + df))]) \\
&= ([(a, b)]x[(ce + df, cf + de)]) \\
&= ([(a, b)]x(([c, d])x([e, f]))) \\
&= A \times (B \times C)
\end{aligned}
$$

Portanto, a propriedade é válida. □

Proposição 4.8 (Comutatividade da multiplicação)**.** *Para quaisquer* $A, B \in \mathbb{Z}$*:* $A \times B = B \times A$*.*

Demonstração. Sejam $A = [(a, b)]$, $B = [(c, d)]$, com $a, b, c, d \in \mathbb{N}$. Temos então que $A \times B = [(a, b)] \times [(c, d)] = [(ac + bd, ad + bc)] = [(ca + db, cb + da)] = B \times A$. Assim, $A \times B = B \times A$ e vale a propriedade[2]. □

Proposição 4.9 (Elemento neutro da multiplicação)**.** *Existe um neutro da multiplicação. Seja* $\mathbb{1} \in \mathbb{Z}$ *definido como* $\mathbb{1} = [(x^+, x)]$*, para algum* $x \in \mathbb{N}$*. Então. para qualquer* $A \in \mathbb{Z}$*:* $A \times \mathbb{1} = \mathbb{1} \times A = A$*.*

Demonstração. Seja $A = [(a, b)]$, com $a, b \in \mathbb{N}$. Temos então que (usando primeiro a comutatividade) $\mathbb{1} \times A = A \times \mathbb{1} = [(a, b)] \times [(x^+, x)] = [(ax^+ + bx, ax + bx^+)] = [(ax + bx + a, ax + bx + b)] = [(a, b)]$. Assim, $A \times \mathbb{1} = A$ e vale a propriedade. Vale mencionar que $(x^+, x) = (x + 1, x) \sim (1, 0)$. □

Proposição 4.10 (Propriedade distributiva)**.** *Para quaisquer* $A, B, C \in \mathbb{Z}$*:* $A \times (B + C) = A \times B + A \times C$ *e* $(B + C) \times A = B \times A + C \times A$*.*

Até aqui, temos as propriedades que mostram que $(\mathbb{Z}, \oplus, \otimes)$ é anel comutativo com unidade.

Demonstração. Sejam $A = [(a, b)]$, $B = [(c, d)]$ e $C = [(e, f)]$, com $a, b, c, d, e, f \in \mathbb{N}$. Temos então que $A \times (B + C) = [(a, b)] \times ([(c, d)] + [(e, f)]) = [(a, b)] \times [(c + e, d + f)] = [a(c + e) + b(d + f), a(d + f) + b(c + e)] = [(ac + ae + bd + bf, ad + af + bc + be)] = [(ac + bd, ad + bc)] + [(ae + bf, af + be)] = [(a, b)] \times [(c, d)] + [(a, b)] \times [(e, f)] = A \times B + A \times C$. Logo, $A \times (B + C) = A \times B + A \times C$, e vale a distributividade à esquerda. Para a distributividade à direita basta usarmos a propriedade comutatividade. □

Proposição 4.11 (Cancelamento da multiplicação)**.** *Para quaisquer* $A, B, C \in \mathbb{Z}$ *com* $A \neq 0$*:* $B \times A = C \times A \Rightarrow B = C$*.*

Demonstração. Sejam $A, B, C \in \mathbb{Z}$, com $A \neq 0$. Seja $A = [(a, b)]$. por hipótese, $A \neq 0 = [(x, x)]$ para algum $x \in \mathbb{N}$. Logo, $a \neq b$ e temos que $a < b$ ou $b < a$. Suponhamos que $b < a$. O outro caso será análogo. Então, $a = b + k^+$, para algum $k \in \mathbb{N}$. Temos $(a, b) \sim (k^+, 0)$, pois $a + 0 = b + k^+$. Logo, $A = [(k^+, 0)]$. Se $B \times A = C \times A$. Somando $-C \times A$ dos dois membro da inequação, obtemos $B \times A + -C \times A = C \times A + -C \times A \Rightarrow (B + -C) \times A = (C + -C) \times A = 0$ Logo, $(B + -C) \times A = 0$. Denotando $B - C$ de $[(p, q)]$ segue que $[(pk^+, qk^+)] = [(0, 0)]$. Ou seja, $pk^+ + 0 = qk^+ + 0 \Rightarrow pk^+ = qk^+ \Rightarrow p = q$, pelo cancelamento da multiplicação em $\mathbb{N}$. Mas então $B + -C = 0 \Rightarrow (B + -C) + C = C \Rightarrow B + (-C + C) = C \Rightarrow B = C$. Portanto, vale o cancelamento da multiplicação. O cancelamento de termo não nulo multiplicando à esquerda é obtido pela comutatividade[3]. □

[2] A demonstração foi baseada em <https://proofwiki.org/wiki/Integer_Multiplication_is_Commutative>. Acesso em: 5 nov. 2021.

[3] A demonstração foi baseada em <https://proofwiki.org/wiki/Non-Zero_Integers_are_Cancellable_for_Multiplication>. Acesso em: 5 nov. 2021.

As próximas três proposições são demonstradas sem utilizar da estrutura interna do conjunto dos números inteiros. Logo, não precisariam ter sido provadas neste capítulo, em que o objetivo é estabelecer os axiomas. No entanto, desfavorece o domínio do conteúdo distanciar esses fatos dos teoremas anteriores. Observamos que é possível provar o domínio de integridade pela estrutura interna e então usar este resultado para provar o cancelamento.

Proposição 4.12 (Unicidade do elemento neutro da multiplicação)**.** *Se $A, B \in \mathbb{Z}$, $A \neq 0$ e B é tal que $A \times B = A$, então $B = \mathbb{1}$.*

Demonstração. De fato, $A \times B = A \Rightarrow A \times B = A \times \mathbb{1} \Rightarrow B \times A = \mathbb{1} \times A \Rightarrow B = \mathbb{1}$, pela propriedade do cancelamento. □

Proposição 4.13 (Multiplicação por elemento neutro da adição)**.** *Para qualquer $A \in \mathbb{Z}$, $A \times 0 = 0 \times A = 0$.*

Demonstração. Temos que $A \times 0 = A \times (0 + 0) = A \times 0 + A \times 0$. Assim, $A \times 0 = A \times 0 + A \times 0$. Seja $B \in \mathbb{Z}$ o elemento oposto a $A \times 0$. Então $A \times 0 + B = (A \times 0 + A \times 0) + B = A \times 0 + (A \times 0 + B)$ e logo $0 = A \times 0$. Portanto, vale a propriedade para qualquer $A \in \mathbb{Z}$. □

Com a próxima propriedade teremos um domínio.

Proposição 4.14 (Domínio de integridade)**.** *Sejam $A, B \in \mathbb{Z}$ tais que $A \times B = 0$. Então $A = 0$ ou $B = 0$.*

Demonstração. Se $A = 0$ não há nada a fazer. Suponhamos então que $A \neq 0$. Logo, $A \times B = A \times 0$. Como A não é nulo, podemos aplicar a lei do cancelamento. Assim, $B = 0$. Portanto, $\mathbb{Z}$ é domínio de integridade. □

Das últimas proposições, se $A \neq 0$ e $B \neq 0$, então $A \times B \neq 0$. Isso significa essencialmente que se multiplicamos elementos não nulos não podemos ter o resultado nulo. Se $B \neq \mathbb{1}$, $A \times B \neq A$, desde que A não seja nulo. Ou seja, qualquer multiplicador $\neq \mathbb{1}$ "muda" o outro operando (não nulo).

O próximo resultado diz respeito à noção intuitiva que temos da inclusão dos números naturais no conjunto dos números inteiros. De forma intuitiva seria a compreensão de que se ignorarmos os números com sinal negativo, obtemos apenas os números naturais. De forma mais aprofundada, podemos encontrar um subconjunto das classes de equivalência que tem estrutura equivalente a do conjunto dos números naturais.

Proposição 4.15 (Imersão dos números naturais no conjunto dos números inteiros)**.** *Seja $f : \mathbb{N} \to \mathbb{Z}$ tal que $f(k) = [(a + k, a)]$ para algum $a \in \mathbb{N}$. Então*

a) f é injetiva,

b) $f(b + c) = f(b) + f(c)$ e

c) $f(b \times c) = f(b) \times f(c)$.

Demonstração. Sejam $x, y \in \mathbb{N}$ com $x \neq y$. Então $f(x) = [(a + x, a)]$ e $f(y) = [(a + y, a)]$. Suponhamos que $f(x) = f(y) \Leftrightarrow [(a + x, a)] = [(a + y, a)] \Rightarrow a + x + a = a + a + y \Rightarrow x = y$. Mas isso contraria a hipótese e portanto $f(x) \neq f(y)$. Logo, a função é injetiva. Por outro lado, $f(b+c) = [(a+(b+c), a)] = [(a+b, a)]+[c, 0] = [(a+b, a)]+[(a+c, a)] = f(b)+f(c)$. Temos também que, $f(b \times c) = [(a+(b \times c), a)] = [(b \times c, 0)] = [(b, 0)] \times [(c, 0)] = [(a+b, a)] \times [(a+c, a)] = f(b) \times f(c)$. Obtemos um mergulho da estrutura do conjunto dos números naturais na estrutura do conjunto dos números inteiros. □

Prosseguimos agora com o desenvolvimento dos conceitos de ordem estrita e ordem comum para o conjunto dos números inteiros, estabelecendo as mesmas propriedades vistas anteriormente. Ou seja, para ordem estrita: anti-reflexividade, transitividade, tricotomia, anti-simetria e totalidade. E para ordem comum: reflexividade, transitividade, simetria e totalidade. Continuamos então com as definições construtivas.

Definição 4.2. Sejam $A, B \in \mathbb{Z}$, com $A = [(a, b)]$ e $B = [(c, d)]$. Dizemos que A **é menor do que** B, escrevemos $A < B$, se $a + d < b + c$. Dizemos que A **é menor ou igual a** B, escrevemos $A \leq B$, se $a + d \leq b + c$. Ou seja se $A < B$ ou $A = B$.

Proposição 4.16 (Bem definida)**.** *A relação de ordem estrita é bem definida. Ou seja, se* $A = [(a, b)] = [(a', b')]$, $B = [(c, d)] = [(c', d')]$ *e* $a + d < b + c$, *então* $a' + d' < b' + c'$.

Demonstração. Sejam $A = [(a, b)] = [(a', b')]$, $B = [(c, d)] = [(c', d')]$ tais que $a+d < b+c$. Então, existe $k \in \mathbb{N}$ tal que $b + c = (a + d) + k^+$. Somando $a' + d'$ a ambas os lados da desigualdade e rearranjando obtemos que $(a' + b) + (c + d') = (a' + d') + (a + d) + k^+ \Rightarrow (a + b') + (c' + d) = (a'+d')+(a+d)+k^+ \Rightarrow (b'+c')+(a+d) = (a'+d')+k^+ +(a+d) \Rightarrow b'+c' = (a'+d')+k^+ \Rightarrow a'+d' < b'+c'$. Logo, a expressão para a relação de ordem independe dos representantes de classe, e portanto a relação está bem definida. □

Proposição 4.17 (Anti-reflexividade)**.** *Para qualquer* $A \in \mathbb{Z}$: $A \not< A$. *De outra forma, para quaisquer* $a, b, k \in \mathbb{N}$, $a + b \neq (b + a) + k^+$.

Demonstração. A anti-reflexividade no conjunto dos números inteiros é uma consequência direta da anti-reflexividade no conjunto dos números naturais. Para isso, basta fazermos $a+b = b+a = p$ e já sabemos que $p \neq p + k^+$, para qualquer $k \in \mathbb{N}$. □

Proposição 4.18 (Transitividade)**.** *Para quaisquer* $A, B, C \in \mathbb{Z}$: $A < B$ *e* $B < C \Rightarrow A < C$.

Demonstração. Sejam $A = [(a, b)]$, $B = [(c, d)]$ e $C = [(e, f)]$, com $a, b, c, d, e, f \in \mathbb{N}$. Se $A < B$ e $B < C$, então $a + d < b + c$ e $c + f < d + e$. Assim, existem $p, q \in \mathbb{N}$ tais que $b + c = (a + d) + p^+$ e $d + e = (c + f) + q^+$. Somando e na primeira equação e rearranjando os termos, obtemos $(b+e)+c = (d+e)+a+p^+ \Rightarrow (b+e)+c = (c+f)+q^+ +a+p^+ \Rightarrow (b+e)+c = (a+f)+q^+ +p^+ +c \Rightarrow b + e = (a + f) + (q^+ + p)^+$ Logo, $b + e = (a + f) + r^+$, para algum $r \in \mathbb{N}$, $a + f < b + e$, $A < C$ e vale a transitividade. □

Proposição 4.19 (Tricotomia)**.** *Para quaisquer $A, B \in \mathbb{Z}$: obrigatoriamente $A < B \veebar A = B \veebar B < A$.*

Demonstração. Sejam $A = [(a, b)]$, $B = [(c, d)]$, com $a, b, c, d \in \mathbb{N}$. $A < B$ por definição é $a + d < b + c$. $A = B$ por sua vez é $a + d = b + c$. E $B < A$ por fim é $b + c < a + d$. Mas, pela tricotomia no conjunto dos números naturais, temos exatamente essas três possibilidades. Logo, também devemos ter a tricotomia no conjunto dos números inteiros, já que cada sentença no conjunto dos números naturais pode ser substituída pela equivalente no teorema. □

Proposição 4.20 (Anti-simetria)**.** *Para quaisquer $A, B \in \mathbb{Z}$: não se tem simultaneamente que $A < B$ e $B < A$.*

Demonstração. A anti-simetria definida dessa forma é uma consequência direta do Teorema 4.19. □

Proposição 4.21 (Totalidade)**.** *Para quaisquer $A, B \in \mathbb{Z}$ com $A \neq B$: obrigatoriamente $A < B \vee B < A$.*

Demonstração. A totalidade definida dessa forma também é uma consequência direta do que já provamos anteriormente. □

Da tricotomia, sabemos que para qualquer $A \in \mathbb{Z}$ teremos, em particular, $A < 0 \veebar A = 0 \veebar A > 0$. Considerando $A = [(a, b)]$, teremos $A < 0 \Leftrightarrow a + 0 < b + 0$, ou seja $a < b$. Por outro lado, $A = 0 \Leftrightarrow a + 0 = b + 0$, ou $a = b$. E por fim, $A > 0 \Leftrightarrow b + 0 < a + 0$, ou seja, $a > b$. Quando $A < 0$, dizemos que A é **negativo**; $A > 0$, dizemos que A é **positivo**; $A = 0$, dizemos que A é **nulo**. Observamos que agora temos elementos com uma propriedade que não ocorria com os números naturais, isto é, elementos menores do que zero, na nova relação de ordem.

Uma vez estabelecidas as propriedades para ordem estrita, enunciamos as propriedades para ordem comum, sem contudo demonstrá-las, pois são essencialmente análogas as anteriores, salvo a diferença de se usar k no lugar de k^+, e na última, simplesmente usamos a totalidade na comparação de naturais.

Proposição 4.22 (Bem definida)**.** *A relação de ordem comum expressa está bem definida. Ou seja, se $A = [(a, b)] = [(a', b')]$, $B = [(c, d)] = [(c', d')]$ e $a + d \leq b + c$, então $a' + d' \leq b' + c'$.*

Proposição 4.23 (Reflexividade)**.** *Para qualquer $A \in \mathbb{Z}$: $A \leq A$.*

Proposição 4.24 (Transitividade)**.** *Para quaisquer $A, B, C \in \mathbb{Z}$: $A \leq B$ e $B \leq C \Rightarrow A \leq C$.*

Proposição 4.25 (Anti-simetria)**.** *Para quaisquer $A, B \in \mathbb{Z}$: se $A \leq B$ e $B \leq A$, então $A = B$.*

Proposição 4.26 (Totalidade)**.** *Para quaisquer $A, B \in \mathbb{Z}$: obrigatoriamente $A \leq B \vee B \leq A$.*

Da totalidade, sabemos que para qualquer $A \in \mathbb{Z}$ teremos, em particular, $A \leq 0 \vee A \geq 0$. Considerando $A = [(a, b)]$, teremos $A \leq 0 \Leftrightarrow a + 0 \leq b + 0$, ou seja $a \leq b$. Por outro lado, $A \geq 0 \Leftrightarrow b + 0 \leq a + 0$, ou seja, $a \geq b$. Quando: $A \leq 0$, dizemos que A é **não positivo**; $A \geq 0$, dizemos que A é **não negativo**.

Para completar as propriedades de domínio de integridade e passar por todos os axiomas que para essa estrutura de pares ordenados de números naturais, devemos contemplar as compatibilidades de $<$ com as operações de soma e multiplicação. Após isso, é pouco provável que necessitemos retornar ao tratamento construtivo que já foi feito. Provemos esses dois fatos, portanto.

Teorema 4.3 (Compatibilidade de $<$ com a operação de adição)**.** *Para quaisquer $A, B, C \in \mathbb{Z}$: $A < B \Rightarrow A + C < B + C$.*

Demonstração. Sejam $A = [(a, b)]$, $B = [(c, d)]$, $C = [(e, f)]$ com $a, b, c, d, e, f \in \mathbb{N}$. Se $A < B$, então $a + d < b + c \Rightarrow (a + e) + (d + f) < (b + f) + (c + e) \Rightarrow [(a + e), (b + f)] < [(c + e), (d + f)] \Rightarrow A + C < B + C$. Portanto, temos a compatibilidade de $<$ com a adição. □

Teorema 4.4 (Compatibilidade de $<$ com a operação de multiplicação)**.** *Para quaisquer $A, B, C \in \mathbb{Z}$: se $0 < B$, então $A < C \Rightarrow A \times B < C \times B$.*

Demonstração. Sejam $A = [(a, b)]$, $B = [(k^+, 0)]$, $C = [(e, f)]$ com $a, b, e, f, k \in \mathbb{N}$. Por simples cálculo, sabemos que B é da forma apresentada. Assim, $A < C \Rightarrow a + f < b + e$. E, da compatibilidade de $<$ no conjunto dos números naturais com a multiplicação, $(a + f) \times k^+ < (b + e) \times k^+ \Rightarrow a \times k^+ + f \times k^+ < b \times k^+ + e \times k^+ \Rightarrow [(a \times k^+, b \times k^+)] < [(e \times k^+, f \times k^+)] \Rightarrow A \times B < C \times B$. Portanto, temos a compatibilidade de $<$ com a multiplicação. □

As seguintes compatibilidades, de $\leq$, também se verificam e as demonstrações são análogas.

Teorema 4.5 (Compatibilidade de $\leq$ com a operação de adição)**.** *Para quaisquer $A, B, C \in \mathbb{Z}$: $A \leq B \Rightarrow A + C \leq B + C$.*

Teorema 4.6 (Compatibilidade de $\leq$ com a operação de multiplicação)**.** *Para quaisquer $A, B, C \in \mathbb{Z}$: se $0 < B$, então $A \leq C \Rightarrow A \times B \leq C \times B$.*

Para concluir, devemos agora apenas estabelecer o Princípio do Bom Ordenamento para o caso de subconjuntos de números inteiros. Neste contexto, devemos exigir que o subconjunto seja limitado inferiormente.

Teorema 4.7 (Princípio do Bom Ordenamento para números inteiros)**.** *Seja $S \subset \mathbb{Z}$ tal que existe $i \in \mathbb{Z}$ de modo que para todo $s \in S$, $i < s$. Então existe $m \in S$ tal que $m \leq s$ para todo $s \in S$.*

Demonstração. Faremos um esboço da demonstração. Por questão de simplicidade iremos considerar os representantes de classe que têm 0 em ao menos uma das ordenadas. Assim, as

classes são do tipo $[(a,0)]$, $[(0,0)]$ e $[(0,b)]$, com $a,b \in \mathbb{N}$ e $a,b \neq 0$. Sabemos que números inteiros do primeiro tipo são os números positivos, $[(0,0)]$ é o 0, e os números inteiros do terceiro tipo são os números negativos. Se tomarmos o limite inferior como sendo $[(0,0)]$ ou um número positivo, S será formado por números positivos e devido ao mergulho dos números naturais nesses, temos que S terá o menor elemento (pois teremos um $S' \subset \mathbb{N}$ correspondente a S que terá o menor elemento). Caso o limite inferior seja um número negativo, digamos $[(0,b)]$, temos duas possibilidades: S formado apenas por números positivos, e o caso já foi abordado; ou existe $n \in S$ tal que n é negativo. O conjunto de valores negativos de S é finito. Logo, certamente terá o menor elemento na ordem total. Seja $[(0,r)]$ tal elemento, com $r \in \mathbb{N}$, $r \neq 0$. Temos que $[(0,r)] < [(0,0)]$ e $[(0,r)] < [(a,0)]$. Ou seja, tal elemento é menor que 0 ou qualquer número positivo. Assim, deve ser menor ou igual a qualquer elemento negativo pertencente a S ou possíveis elementos positivos de S. Portanto, é o elemento mínimo de S. □

Teorema 4.8. *Seja $S \subset \mathbb{Z}$ tal que existe $j \in \mathbb{Z}$ de modo que para todo $s \in S$, $j > s$. Então existe $m \in S$ tal que $m \geq s$ para todo $s \in S$.*

Demonstração. Este teorema pode ser verificado aplicando-se o Teorema 4.7 para o conjunto $-S$ dos números inteiros opostos aos elementos de S. Esse conjunto será limitado inferiormente, por $-j$ e portanto terá o elemento mínimo, cujo oposto, em S, é o elemento máximo. □

5 TEORIA ELEMENTAR DOS NÚMEROS

Começamos este capítulo com a definição da estrutura algébrica principal na teoria dos números.

Definição 5.1. Seja C um conjunto não vazio. Sejam $+ : C \times C \to C$ e $\times : C \times C \to C$ operadores binários, que denominaremos **adição** e **multiplicação**, respectivamente[1] Mais ainda, são válidas as seguintes propriedades:

Propriedades da adição:

a) Associatividade da adição: $\forall a, b, c \in C : (a + b) + c = a + (b + c)$

b) Comutatividade da adição: $\forall a, b \in C : a + b = b + a$

c) Existência de elemento neutro para a adição: $\exists x \in C : \forall a \in C : a + x = a$ Denotamos um elemento com essa propriedade por "0". Outros elementos com a propriedade podem ser denotados pelo símbolo anterior com um sobrescrito.

d) Existência de elemento oposto para a adição: $\forall a \in C : \exists x \in C : a + x = 0$ Se "a" denota um elemento de C, então podemos usar "a'" e "a''" para denotar elementos que somados com a resultam em um elemento neutro.

Propriedades da multiplicação:

a) Associatividade da multiplicação: $\forall a, b, c \in C : (a \times b) \times c = a \times (b \times c)$

b) Comutatividade da multiplicação: $\forall a, b \in C : a \times b = b \times a$

c) Existência de elemento neutro para a multiplicação: $\exists x \in C : \forall a \in C : a \times x = a$. Denotamos um elemento com essa propriedade por "1". Outros elementos com a propriedade podem ser denotados pelo símbolo anterior com um sobrescrito.

d) Distributividade do multiplicação sobre a adição: $\forall a, b, c \in C : c \times (a + b) = c \times a + c \times b$

Domínio de Integridade: $\forall a, b \in C : a \times b = 0 \Rightarrow a = 0 \vee b = 0$

Nessas condições, a estrutura $(C, +, \times)$ será denominada **domínio de integridade**, ou simplesmente **domínio**.

[1] Escrevemos familiarmente "$a + b$" em vez de "$+(a, b)$", "$a \times b$" no lugar de "$\times(a, b)$". Nas expressões, as operações entre parênteses são realizadas primeiro, e é assumida a precedência da multiplicação relativamente à adição. Esta é uma consideração que diz respeito somente à escrita e à interpretação das expressões e não à estrutura em si que é criada com os axiomas.

Portanto, $(\mathbb{Z}, +, \times)$ é um domínio de integridade considerando + e $\times$ como as operações usuais de adição e multiplicação. Também denotaremos a multiplicação pela concatenação de variáveis. Assim, por exemplo: $ab = a \times b$. A ordem definida no capítulo anterior é compatível com a estrutura de domínio de integridade do conjunto dos números inteiros [2] e vale também o Princípio do Bom Ordenamento. Observamos que os axiomas não foram dispostos na ordem em que foram deduzidos (no contexto anterior, eram teoremas), porém, em uma outra mais intuitiva de se estudar, o que também foi feito no capítulo 2.

Sabemos de resultados imediatos desses axiomas que o elemento neutro será único, e portanto poderá ser denotado unicamente por "0" sem nenhum outro marcador. Sabemos também da unicidade do elemento oposto para cada elemento de C, e com isso definimos um operador unário $- : C \to C$ que leva a em $-a$, o oposto de a. Observamos que escrevemos $-a$ em vez de $-(a)$, como feito anteriormente. Supomos a precedência desse operador unário em relação aos outros operadores. Novamente, essa é uma consideração sintática e que influencia a interpretação das expressões e não diz respeito aos axiomas. Poderíamos, por outro lado, não utilizar as expressões sintéticas que se valem da regra do PEMDAS (Parênteses, Expoente, Multiplicação/Divisão, Adição/Subtração) para escrever os mesmos axiomas. Ou seja, escrevendo os operadores explicitamente com a linguagem de funções. Mas esse estilo é desajeitado e incômodo para o contexto de cálculos.

Muitos fatos podem ser obtidos dessa estrutura. Essencialmente, a partir de várias propriedades importantes do conjunto dos números inteiros, buscaríamos aquelas que traduzam a real natureza desses objetos, formando um conjunto mínimo que permite deduzirmos todas as outras. No entanto, essas propriedades, sendo meticulosamente aplicadas em alguma expressão (precisa), levariam a numerosos passos para se efetuar ou simplificar uma conta. Ocorre que na efetivação de cálculos pensamos uma adição como uma operação que admite uma quantidade arbitrária de parcelas (assim como o produto) e não apenas duas. A única coisa que importaria é a ordem, e podemos omitir os parênteses. E na realidade, sequer a ordem importa, devido à comutatividade.

Para justificar a não exposição dos numerosos passos intermediários relativos a trocas simples de parênteses e a trocas de termos adjacentes em uma expressão, à titulo de curiosidade, poderíamos definir as operações de anel de modo a possibilitar a aplicação usual que fazemos delas. Precisaríamos utilizar polinômios e isso seria cansativo. Dessa forma, iremos partir essencialmente de um esquema axiomático bem mais forte, que pode ser deduzido das propriedades mais simples. No entanto, tal dedução não será feita pois é demasiadamente trabalhosa; e em última análise, envolve a aplicação das propriedades associativas e comutativas simples também nos operadores lógicos, o que aumenta ainda mais o esforço de formalização. Seria um tanto estranho realizar uma demonstração de forma textual, que se vale exatamente dessa super-estrutura que permite uma ampla associatividade e comutatividade nos operadores

[2] Para este tópico foi consultado: <https://proofwiki.org/wiki/Definition:Ordering_Compatible_with_Ring_Structure>. Acesso em: 10 nov. 2021.

lógicos, para se provar a mesma estrutura no escopo aritmético.

A intenção desses comentários é endereçar um incômodo com passos que podem ser considerados longos para o formalismo. E embora fosse interessante buscar esse grau de arranjo lógico, foge do escopo do trabalho.

Começamos, enfim, a abordar a Teoria dos Números usual. Dessa forma, não iremos demonstrar propriedades aritméticas elementares como fizemos no caso do conjunto dos números naturais. As considerações são bem mais extensas, pois temos mais possibilidades devido aos negativos. Ressaltaremos, sem provar, fatos relativos ao estudo da divisibilidade/divisão, que também será o foco no estudo dos números inteiros gaussianos. É preciso, contudo, passar rapidamente por algumas proposições a respeito do módulo e multiplicação por oposto, abordadas em *Números: uma Introdução à Matemática* (MILLIES; COELHO, 2001), cujas demonstrações são fornecidas.

Definição 5.2. Seja $a \in \mathbb{Z}$. Chamamos de **módulo** de a, escrevemos $|a|$, a função definida da seguinte forma. $|.| : \mathbb{Z} \to \mathbb{Z}$ e temos que:

$$|a| = \begin{cases} a, & \text{se } a \geq 0 \\ -a, & \text{se } a < 0 \end{cases}$$

Seguem as propriedades básicas de módulo.

Proposição 5.1. *Para qualquer $a \in \mathbb{Z}$: $|a| \geq 0$.*

Demonstração. De fato, temos ou $a \geq 0 \Rightarrow |a| = a \geq 0$ ou $a < 0 \Rightarrow |a| = -a > 0$. Constatamos que o operador unário de módulo assume apenas valores não negativos. □

Proposição 5.2. *Para qualquer $a \in \mathbb{Z}$: $|a| = 0 \Leftrightarrow a = 0$.*

Demonstração.
[$\Leftarrow$] $a = 0 \Rightarrow a \geq 0 \Rightarrow |a| = a = 0$.
[$\Rightarrow$] Separamos por casos. $a < 0 \Rightarrow |a| = -a > 0 \Rightarrow a \neq 0$. Por outro lado, $a > 0 \Rightarrow |a| = a > 0 \Rightarrow a \neq 0$. Assim, resta-nos apenas $a = 0$. Neste caso, $|a| = a = 0$. □

Proposição 5.3. *Para qualquer $a \in \mathbb{Z}$: $-|a| \leq a \leq |a|$.*

Demonstração. As demonstrações de módulo sempre seguem a mesma lógica de divisão por casos, devido à definição do operador. Primeiro, observamos o seguinte. Se $a > 0$, então $-|a| < 0 < |a| \Rightarrow -|a| \leq 0 \leq |a|$. Se $a = 0$, então $|a| = 0 = -|a| \Rightarrow -|a| \leq 0 \leq |a|$. Se $a < 0$, então $-|a| < 0 < |a| \Rightarrow -|a| \leq 0 \leq |a|$. Ou seja, $-|a| \leq 0 \leq |a|$ e em todo caso temos $-|a| \leq |a|$. Ao mesmo tempo $|a| = a \vee |a| = -a$. Assim, $a = |a| \vee a = -|a|$. Portanto, $-|a| \leq a \leq |a|$ □

Proposição 5.4. *Para qualquer $a \in \mathbb{Z}$: $|-a| = |a|$.*

Demonstração. Primeiramente $a > 0 \Rightarrow -a < 0$. Assim, $|a| = a$, $|-a| = -(-a) = a$ e $|a| = |-a|$. Por outro lado $a = 0 \Rightarrow -a = 0 \Rightarrow |a| = |-a|$. Por fim, $a < 0 \Rightarrow -a > 0$. Logo, $|a| = -a$, $|-a| = -a$ e $|a| = |-a|$. □

Proposição 5.5. *Para quaisquer $a, b \in \mathbb{Z}$: $|ab| = |a| \times |b|$.*

Demonstração. Se $a = 0$ ou $b = 0$, a afirmação se verifica. Suponhamos então ambos diferentes de 0. Se $a > 0$ e $b > 0$, então $ab > 0$ e $|ab| = ab = |a| \times |b|$. Se $a < 0$ e $b < 0$, então $-a > 0$ e $-b > 0$, o que implica $-a \times -b = a \times b > 0$ e $|ab| = ab = -a \times -b = |a| \times |b|$. Por fim, se $a > 0$ e $b < 0$, temos $-b > 0$ e $a(-b) = -(ab) > 0$, logo $|ab| = |-(ab)| = -(ab) = a(-b) = |a| \times |b|$. O caso $a < 0$ e $b > 0$ é análogo. □

Na proposição anterior, utilizamos a regra dos sinais na multiplicação, que será apresentada mais adiante. O módulo é uma função importante, pois fornece a noção intuitiva de "medida do tamanho do número". O tamanho é aferido de maneira diferente nos outros contextos que iremos estudar.

Uma propriedade importante do módulo é a desigualdade que demonstramos a seguir.

Proposição 5.6 (Desigualdade triangular)**.** *Para quaisquer $a, b \in \mathbb{Z}$: $|a + b| \leq |a| + |b|$.*

Demonstração. Para demonstrar essa proposição mais facilmente, façamos uso da infraestrutura dos inteiros, pois a explicação deste fato é mais simples falando do modo elementar como se adicionam tais números. Se $a = 0$ ou $b = 0$, o resultado é imediato. Então, se ambos os elementos forem positivos, teremos como resultado outro número positivo de módulo igual à soma dos outros dois módulos. Sejam $a, b \in \mathbb{N}$ com $a, b \neq 0$. $[(a, 0)] + [(b, 0)] = [(a + b, 0)]$ e $|[(a+b, 0)]| = a+b$. Se ambos forem negativos, teremos como resultado outro número negativo de módulo igual a soma dos outros dois módulos. $[(0, a)] + [(0, b)] = [(0, a + b)]$ e $|[(0, a + b)]| = a + b$. Suponhamos que um dos números seja positivo e o outro seja negativo. Então temos uma soma do tipo $[(a, 0)] + [(0, b)] = [(a, b)]$. Temos dois casos, como estudado na matemática básica: $a < b$ ou $b < a$. No primeiro caso, consideramos $[(0, b - a)]$ como representante de classe e no segundo $[(a - b, 0)]$. Em ambos o módulo ($b - a < b$ ou $a - b < a$) será menor que $a + b$. Aqui representamos o módulo como um número natural, mas precisamente seria um inteiro com a segunda ordenada zero. □

Estudamos agora os aspectos relativos à divisão. Começamos pela relação de divisibilidade. Consideremos um número inteiro como par ordenado para que fiquem mais fáceis as seguintes considerações.

Agora faz-se necessário pensar a multiplicação por números negativos. Quando um dos fatores é nulo, temos um resultado nulo, independente do outro fator. Quando os dois fatores são positivos, permanecemos (em certo sentido) no domínio dos naturais. Ou seja, a multiplicação dos inteiros restrita aos Naturais é a multiplicação dos Naturais. Quando um dos fatores é negativo e o outro positivo, passamos ao domínio dos negativos, sendo o módulo do resultado

o mesmo que obteríamos caso multiplicássemos fatores positivos com os mesmos módulos. Quando os dois fatores são negativos, o resultado é positivo, sendo o módulo do resultado o mesmo que obteríamos caso multiplicássemos fatores positivos com os mesmos módulos.

A regra dos sinais a seguir abrange tais considerações; porém, diz respeito à oposição.

Proposição 5.7 (Regra dos sinais)**.** *Para quaisquer* $a, b \in \mathbb{Z}$*:* $-(-a) = a$*,* $(-a)b = -(ab) = a(-b)$*, e* $(-a)(-b) = ab$*.*

Demonstração. Temos que $-(-a) = -(-a)+0 = -(-a)+(-a+a) = (-(-a)+-a)+a = 0+a = a$. Por outro lado $(-a)b = (-a)b+0 = (-a)b+(ab+-(ab)) = ((-a)b+ab)+-(ab) = ((-a+a)b+-(ab) = 0b + -(ab) = -(ab)$. Analogamente para $a(-b)$. Usando as afirmações anteriores, segue que $(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$. □

Passamos então à divisibilidade, que é abordada da mesma forma que fizemos no conjunto dos números naturais.

Definição 5.3. Sejam $a, b \in \mathbb{Z}$. Dizemos que b **divide** a, escrevemos $b \mid a$, se existe $q \in \mathbb{Z}$, tal que $a = b \times q$.

Definição 5.4. Sejam $a, b \in \mathbb{Z}$. Dizemos que a **é divisível por** b, ou a **é múltiplo de** b, se $b \mid a$. Não há notação para tal ordem invertida.

As propriedades de divisibilidade vistas para o conjunto dos números naturais serão as mesmas para o conjunto dos números inteiros. Devemos considerar os múltiplos tanto “à esquerda” quanto “à direita” do zero, intuitivamente pensados na reta. Retomamos os teoremas de divisibilidade, provados para os números naturais, agora para o escopo dos números inteiros. As demonstrações não são feitas pois envolvem apenas alguns ajustes dos raciocínios, ou mesmo nenhum.

Teorema 5.1 (Reflexividade)**.** *Para qualquer* $a \in \mathbb{Z}$*:* $a \mid a$*.*

Teorema 5.2 (Transitividade)**.** *Para quaisquer* $a, b, c \in \mathbb{Z}$*:* $a \mid b \ \ e \ \ b \mid c \Rightarrow a \mid c$*.*

Teorema 5.3 (Limitação)**.** *Para quaisquer* $a, b \in \mathbb{Z}$*: se* $b \mid a$*, então* $a = 0$ *ou* $-|a| \leq b \leq |a|$*. De outra forma, sabemos que para qualquer* $b \in \mathbb{Z}$*,* $b \mid 0$*. Por outro lado, se* $b \mid a \neq 0$*, então* $-|a| \leq b \leq |a|$*. Ademais, neste caso* $b \neq 0$*.*

Teorema 5.4 (Anti-simetria)**.** *Para quaisquer* $a, b \in \mathbb{Z}$*: se* $a \mid b \ \ e \ \ b \mid a$ *então* $a = b \ \vee \ a = -b$*.*

Teorema 5.5 (Não totalidade)**.** *Não se tem que para quaisquer* $a, b \in \mathbb{Z}$*, obrigatoriamente:* $a \mid b$ *ou* $b \mid a$*.*

Estabelecemos então que a divisibilidade é uma relação de ordem comum não total no conjunto dos números inteiros. Também temos nos números inteiros a divisibilidade da combinação linear.

Teorema 5.6. *Para quaisquer $a, b, c \in \mathbb{Z}$: se $a \mid b$ e $a \mid c$, então, para quaisquer $x, y \in \mathbb{Z}$: $a \mid (b \times x + c \times y)$.*

Por fim, retomamos a operação de divisão e as mesmas propriedades no caso dos inteiros.

Definição 5.5. Sejam $a, b \in \mathbb{Z}$, com $b \mid a$ e $b \neq 0$. Então, pela definição de divisibilidade, existe $q \in \mathbb{Z}$ tal que $a = b \times q$.

Observamos que se $b = 0$, então $a = 0$ e $a = b \times q$ se verifica para qualquer número inteiro q. Mas como $b \neq 0$, o q é único, pois $a = b \times p$ e $a = b \times q \Rightarrow b \times p = b \times q \Rightarrow p = q$, pelo cancelamento da multiplicação. Portanto, podemos considerar um operador binário, chamado **divisão**, $/ : X \to \mathbb{Z}$, em que $X \subset \mathbb{Z} \times \mathbb{Z}$, com $X = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid b \neq 0 \text{ e } b \mid a\}$, e $a/b = q$ tal que $a = b \times q$.

Proposição 5.8 (Elemento neutro da divisão)**.** *Para qualquer $a \in \mathbb{Z}$: $1 \mid a$ e portanto $a/1$ está definido. Além disso, $a/1 = a$.*

Proposição 5.9 (Associatividade na divisão)**.** *Para quaisquer $a, b, c \in \mathbb{Z}$, $c \neq 0$: se $c \mid b$, então $(a \times b)/c = a \times (b/c)$.*

Proposição 5.10 (Comutatividade na divisão)**.** *Para quaisquer $a, b, c \in \mathbb{Z}$, $c \neq 0$: se $c \mid a$, $(a \times b)/c = (a/c) \times b$.*

Proposição 5.11 (Cancelamento da divisão - I)**.** *Para quaisquer $a, b, c \in \mathbb{Z}$, $a \neq 0$: se $a \mid b$ e $a \mid c$, então $b/a = c/a \Rightarrow b = c$.*

Proposição 5.12 (Cancelamento da divisão - II)**.** *Para quaisquer $a, b, c \in \mathbb{Z}$, $a, b, c \neq 0$: se $a \mid c$ e $b \mid c$, então $c/a = c/b \Rightarrow a = b$.*

Proposição 5.13 (Neutro da divisão)**.** *Temos que $\exists x \in \mathbb{Z} : \forall a \in \mathbb{Z} : a/x = a$. Ademais, tal x é único.*

Proposição 5.14 (Distributividade da divisão em relação à adição)**.** *Para quaisquer $a, b, c \in \mathbb{Z}$, $a \neq 0$: se $a \mid b$ e $a \mid c$, então $a \mid (b + c)$ e $(b + c)/a = b/a + c/a$.*

Proposição 5.15 (Distributividade da divisão em relação à subtração)**.** *Para quaisquer $a, b, c \in \mathbb{Z}$, $a \neq 0$: se $a \mid b$ e $a \mid c$, então $a \mid (b - c)$ e $(b - c)/a = b/a - c/a$.*

Observamos que a subtração no conjunto dos números inteiros pode ser definida com o auxílio do operador unário de oposição ou da mesma forma que foi feita para os números naturais, porém agora sem a necessidade de se colocar a condição de um número maior do que outro.

É possível verificar também, com alguns ajustes, as compatibilidades da divisibilidade. As duas incompatibilidades abaixo podem ser demonstradas com exemplos no caso dos números

naturais, e portanto a prova é praticamente a mesma para os números inteiros. As compatibilidades com produto e divisão são demonstradas essencialmente de forma algébrica e portanto a reformulação é pequena. Já no caso da potenciação requer-se maior ajuste, por utilizar o Princípio de Indução Finita (PIF). A definição da potência nos números inteiros exige restrições para não entrarmos no contexto das frações.

Proposição 5.16 (Incompatibilidade $\mid$ e adição)**.** *Não se tem que para quaisquer* $a, b, k \in \mathbb{Z}$*: se* $a \mid b$ *então* $a + k \mid b + k$*.*

Proposição 5.17 (Incompatibilidade $\mid$ e subtração)**.** *Não se tem que para quaisquer* $a, b, k \in \mathbb{Z}$*: se* $a \mid b$ *então* $a - k \mid b - k$*.*

Proposição 5.18 (Compatibilidade $\mid$ e produto)**.** *Para quaisquer* $a, b, k \in \mathbb{Z}$*: se* $a \mid b$ *então* $a \times k \mid b \times k$*.*

Proposição 5.19 (Compatibilidade $\mid$ e divisão)**.** *Para quaisquer* $a, b, k \in \mathbb{Z}$ *com* $k \neq 0$*: se* $k \mid a, b$ *e* $a \mid b$ *então* $a/k \mid b/k$*.*

Proposição 5.20 (Compatibilidade $\mid$ e potenciação)**.** *Para quaisquer* $a, b \in \mathbb{Z}$ *e* $k \in \mathbb{N}$*: se* $a \mid b$ *então* $a\hat{}k^+ \mid b\hat{}k^+$*. Ademais, se* $b \neq 0$ *e supondo que* $a \mid b$*, temos que* $a \neq 0$ *e poderemos fazer* $a\hat{}0$*; então* $a\hat{}0 = 1 \mid 1 = b\hat{}0$*.*

A essência do conceito de divisão permanece quando passamos para o conjunto dos números inteiros. No capítulo 2 tivemos o foco na aritmética números naturais, e retomamos alguns daqueles resultados novamente com certas alterações para os números inteiros. Teoremas do capítulo 2 foram utilizados para construir o domínio de integridade dos números inteiros no capítulo 4, com uma ordem compatível com a estrutura e que determina também um bom ordenamento. O foco e o desenvolvimento deste capítulo se dá com o estudo da divisão. Alguns pormenores aritméticos foram levantados, mas não procuramos nos alongar com o formalismo aqui, embora também fosse importante relacionar todas as propriedades básicas e procurar prová-las. Continuamos apresentando um conjunto de fatos da divisão que será comparado à frente com outro no contexto dos inteiros gaussianos. Vamos à algumas definições.

Definição 5.6. Sejam $a, b \in \mathbb{Z}$, $b \neq 0$, e seja o conjunto $S = \{k \times b \leq a \mid k \in \mathbb{Z}\}$, dos múltiplos de b menores ou iguais a a. Como esse conjunto é limitado superiormente, ele possui o maior elemento, digamos $q \times b$. Temos então $q \times b \leq a < q \times b + |b| \Rightarrow 0 \leq a - q \times b < |b|$. Chamamos o valor q de **quociente** e $r = a - q \times b$ de **resto**. Temos esses valores unicamente determinados. Denominamos **divisão euclidiana** de a por b o processo de encontrar q e r tais que $a = q \times b + r$ e $0 \leq r < |b|$.

A definição 5.6 também poderia ser apresentada antes como um teorema. Múltiplos e divisores são importantes na Teoria dos Números. Os múltiplos de um número diferente de 0 são infinitos. E no contexto dos números inteiros são ilimitados superiormente e inferiormente.

Ainda, podemos considerar os múltiplos de dois números. Nessas duas listagens, com toda certeza existirão múltiplos comuns aos dois (além do 0), pois multiplicando um pelo outro já obtemos um múltiplo comum. O conjunto de múltiplos comuns também será infinito, bastando entender que podemos tomar os múltiplos de um múltiplo comum e temos a infinidade. E ainda se considerarmos os múltiplos comuns positivos, esse conjunto é limitado inferiormente e portanto possui menor elemento.

Definimos então o conjunto de divisores de um número não nulo. Pelo que vimos, esse conjunto é finito, pois os possíveis divisores estão compreendidos entre o módulo do número e o oposto do módulo. O 1 sempre será divisor de um número. Assim, podemos tomar dois números e listar seus divisores, e dessas duas listas relacionar aqueles comuns e positivos. A lista dos divisores comuns positivos, por sua vez, é finita (para isso exigimos apenas que um dos números seja diferente de 0) e não vazia, pois contempla o 1. Logo, entre os divisores comuns positivos teremos o maior.

As considerações feitas motivam as definições a seguir de menor múltiplo comum (mmc) e maior divisor comum (mdc). Passemos a elas.

Definição 5.7. Sejam $a, b \in \mathbb{Z}$, ambos não nulos. Denominamos **mínimo múltiplo comum**, ou **menor múltiplo comum**, de a e b, denotamos por $mmc(a, b)$, o menor inteiro positivo que é múltiplo de a e b.

Definição 5.8. Sejam $a, b \in \mathbb{Z}$, não sendo ambos nulos. Denominamos **máximo divisor comum**, ou **maior divisor comum**, de a e b, denotamos por $mdc(a, b)$, o maior inteiro que é divisor de a e b.

O procedimento descrito a seguir, denominado algoritmo de Euclides, nos permite encontrar o máximo divisor comum por meio da realização de divisões euclidianas sucessivas. Os estudos que seguem são tirados do texto *Teoria dos Números: Passeio com Primos e Outros Números Familiares pelo Mundo Inteiro* (MARTINEZ et al., 2009).

Sejam $a_1, a_2 \in \mathbb{Z}$, não sendo ambos nulos. Se $a_2 = 0$, temos $a_1 \neq 0$, e $mdc(a_1, a_2) = |a_1|$, pois como todo inteiro divide 0, o maior divisor entre os dois será o maior divisor de a_1, que está definido e é justamente $|a_1|$. Se $a_1 = 0$ a situação é análoga. Supomos então que $a_1, a_2 \neq 0$ e que $a_1 \geq a_2$, sem perda de generalidade. Podemos efetuar a divisão euclidiana de a_1 por a_2 e encontrar os únicos quociente q_1 e resto a_3 ($0 \leq a_3 < |a_2|$) que satisfazem a expressão $a_1 = q_1 \times a_2 + a_3$. Se $a_3 = 0$, temos que $mdc(a_1, a_2) = |a_2|$. Caso contrário, efetuamos a divisão euclidiana de a_2 por a_3, ambos diferentes de 0, e encontramos os únicos quociente q_2 e resto a_4 ($0 \leq a_4 < |a_3|$) que satisfazem a expressão $a_2 = q_2 \times a_3 + a_4$. Em geral, se $a_i, a_{i+1} \neq 0$, realizamos a divisão de a_i por a_{i+1} e encontramos os únicos quociente q_i e resto a_{i+2} ($0 \leq a_{i+2} < |a_{i+1}|$) tais que $a_i = q_i \times a_{i+1} + a_{i+2}$.

Teorema 5.7 (Algoritmo de Euclides)**.** *Temos que os valores da sequência finita a_n sempre decrescem e o termo final deve ser* 0*. Nesse processo, o módulo do último valor de a_n diferente de* 0 *é o $mdc(a_1, a_2)$.*

Demonstração. Temos, na divisão euclidiana de a por b: $a = q \times b + r$ e $0 \leq r < |b|$. Os divisores comuns a b e a também dividem r, mesmo para $r = 0$ (se u é divisor comum, $r = a - q \times b = x \times u - q \times (y \times u) = (x - q \times y) \times u$). Logo, dividem b e r. Por outro lado, os divisores comuns a b e r também dividem a, e portanto dividem b e a. Logo, o conjunto de divisores comuns de b e a e o conjunto de divisores comuns de b e r é o mesmo. Então o maior elemento é o mesmo. No algoritmo, isso ocorre para cada nova divisão efetuada e portanto o conjunto dos divisores comuns é preservado e junto é preservado o maior divisor comum. Caso o resto seja zero, o maior divisor comum será o módulo do divisor, uma vez que o maior divisor comum entre um número $k \neq 0$ e 0 é de fato $|k|$. Quando o resto se torna 0, o *mdc* fica evidente, sendo relativo aos dois elementos do início. □

O teorema a seguir é muito importante para diversos resultados na Teoria Elementar dos Números.

Teorema 5.8 (Bachet-Bezout)**.** *Sejam $a, b \in \mathbb{Z}$, não simultaneamente nulos. Então, existem $x, y \in \mathbb{Z}$ tais que $ax + by = mdc(a, b)$.*

Demonstração. Seja $S = \{ax + by > 0 \mid x, y \in \mathbb{Z}\}$ o conjunto das combinações $\mathbb{Z}$-lineares positivas de a e b. S é não vazio e pelo Princípio do Bom Ordenamento esse conjunto possui o menor elemento. Seja $d = ax_0 + by_0$ o menor elemento de S. Todo divisor comum a b e a deve dividir qualquer elemento de S, logo deve dividir d. Portanto, $mdc(a, b) \mid d \Rightarrow mdc(a, b) \leq d$. Por outro lado, d divide todo elemento de S. Pois seja $m = ax + by$ um elemento de S. Temos da divisão euclidiana de m por d: $m = qd + r$ com $0 \leq r < d$. E $r = m - qd = ax + by - qax_0 - qby_0 = a(x - qx_0) + b(y - qy_0)$. Mas então r é uma combinação $\mathbb{Z}$ linear de a, b. Se $r \neq 0$, seria o menor elemento de S, o que contraria a suposição. Logo, $r = 0$ e $d \mid m$. Assim d divide qualquer elemento de S. Em particular, $d \mid a$ e $d \mid b$. Segue então que d é divisor comum a b e a e portanto $d \leq mdc(a, b)$. Como $mdc(a, b) \leq d$ e $d \leq mdc(a, b)$, concluímos $d = mdc(a, b)$. □

Uma importante consequência do teorema 5.8 é a seguinte.

Proposição 5.21 (Lema de Euclides)**.** *Sejam $a, b, c \in \mathbb{Z}$. Se $a \mid bc$ e $mdc(a, b) = 1$, então $a \mid c$.*

Demonstração. Temos pelo teorema anterior que $ax_0 + by_0 = 1$, para determinados $x_0, y_0 \in \mathbb{Z}$. Segue que $cax_0 + cby_0 = c$. Como $a \mid ca$ e $a \mid cb$, temos que a divide o lado esquerdo da equação. Portanto, $a \mid c$. □

Passamos então à definição de primo, que será necessária para a abordagem das próximas proposições.

Definição 5.9. Denominamos um número $p > 1$ **primo** caso seus únicos divisores positivos sejam 1 e p. Ou seja, caso p não possa ser fatorado em inteiros positivos m, n, com $1 < m, n < p$.

Proposição 5.22. *Seja p um número primo e sejam $a_1, a_2, ..., a_m \in \mathbb{Z}$. Se $p \mid a_1 \times a_2 \times ... \times a_m \in \mathbb{Z}$, então $p \mid a_i$, para algum $i \in \{1, 2, ..., m\}$.*

Demonstração. Consideramos primeiro o produto $a_1 \times a_2$ e supomos que $p \mid a_1 \times a_2$. Se $p \mid a_1$, o enunciado é satisfeito. Se $p \nmid a_1$, o único divisor comum positivo entre ambos é 1, e portanto é o máximo divisor comum. Do lema 6.4 $p \mid a_2$. Para o caso com m termos, podemos aplicar uma Indução Finita e obter o resultado. □

Relacionaremos a seguir uma série de fatos elementares que são necessários em demonstrações nesta parte da teoria.

Proposição 5.23. *Sejam $a, p \in \mathbb{Z}$, com p primo. Então, $mdc(a, p) = 1$ ou $mdc(a, p) = p$.*

Demonstração. A afirmação é bastante razoável, pois os únicos divisores positivos de p são 1 e ele mesmo. Logo, essas são as únicas possibilidades para máximo divisor comum. □

Proposição 5.24. *Para quaisquer $a, b, k \in \mathbb{Z}$, a, b não ambos nulos: $mdc(a, b) = mdc(a - kb, b)$.*

Demonstração. Sejam $a, b, k \in \mathbb{Z}$, com a, b não ambos nulos. Um divisor comum de b e a também divide $a - kb$, logo é divisor comum de b e $a - kb$. Por outro lado, um divisor comum de b e $a - kb = n$ também divide a, logo é divisor comum de b e a. Portanto, os dois conjunto de divisores comuns são iguais, e da mesma forma o maior divisor comum é igual. □

Proposição 5.25. *Para quaisquer $a, b, c \in \mathbb{Z}$, com $b \neq 0$ ou $c \neq 0$: se $a \mid c$, então $mdc(a, b) \mid mdc(b, c)$.*

Demonstração. Temos que $mdc(a, b) \mid a$. Logo, $a \mid c$ implicará $mdc(a, b) \mid c$. Ao mesmo tempo, $mdc(a, b) \mid b$. Assim, $mdc(a, b) \mid b, c$. Pelo teorema de Bachet-Bézout, todo divisor comum deve dividir o maior divisor comum. Portanto, $mdc(a, b) \mid mdc(b, c)$. □

Proposição 5.26. *Para quaisquer $a, b, c \in \mathbb{Z}$: se $mdc(a, b) = 1$, então $mdc(c, b) = mdc(ac, b)$.*

Demonstração. Temos que $mdc(c, b)$ divide c e b, desta forma divide ac e b, e divide $mdc(ac, b)$. Por outro lado, como $mdc(a, b) = 1$, temos $av + bw = 1$, para determinados $v, w \in \mathbb{Z}$. Assim, $acv + bcw = c$. Logo, $mdc(ac, b)$ divide c, divide c e b, e portanto divide $mdc(c, b)$. Concluímos nessas condições que $mdc(c, b) = mdc(ac, b)$. □

É interessante ressaltar mais um fato sobre *mmc* e *mdc* de dois inteiros não nulos.

Teorema 5.9. *Para quaisquer $a, b \in \mathbb{N}$, $a, b \neq 0$: $mdc(a, b) \times mmc(a, b) = a \times b$.*

Demonstração. Seja $d = mdc(a, b)$. Logo, $av + bw = d$ para determinados $v, w \in \mathbb{Z}$. Mas $a = a_1 \times d$ e $b = b_1 \times d$. Assim, $a_1 dv + b_1 dw = d \Rightarrow a_1 v + b_1 w = 1$ e $mdc(a_1, b_1) = 1$. Seja $m = mmc(a, b)$. Como m é múltiplo de a, $m = ai$ para algum $i \in \mathbb{N}$. Ao mesmo tempo, $m = bj$ para algum $j \in \mathbb{N}$. Então $b_1 dj = a_1 di \Rightarrow b_1 j = a_1 i \Rightarrow b_1 \mid a_1 i$. Como $mdc(a_1, b_1) = 1$, temos da proposição 6.4 que $b_1 \mid i$. $m = a_1 di$ deve ser o menor inteiro positivo divisível por $b = b_1 d$. Assim $a_1 i$ deve ser o menor inteiro positivo divisível por b_1. E como $b_1 \mid i$, i deve ser o menor inteiro positivo divisível por b_1. Portanto, $i = b_1$, $mmc(a, b) = b_1 a \Rightarrow mdc(a, b) \times mmc(a, b) = db_1 a = ba$. □

As considerações feitas até o momento permitem provar o Teorema Fundamental da Aritmética. Esse teorema é importante pois todo inteiro pode ser expresso pelos seus fatores primos acompanhados de um sinal, e tal caracterização traz informação relevante para o estudo dos números.

Teorema 5.10 (Teorema Fundamental da Aritmética)**.** *Seja $n \in \mathbb{Z}$, com $n \geq 2$. Então n pode ser expresso em um único produto de primos, a menos da ordem desses fatores. Ou seja $n = p_1 \times ... \times p_v$, com $p_1, ..., p_v$ primos, $v \geq 1$ e $p_1 \leq ... \leq p_v$. E caso $n = q_1 \times ... \times q_w$, com $q_1, ..., q_w$ primos, $w \geq 1$ e $q_1 \leq ... \leq q_w$, temos $w = v$ e $q_1 = p_1, ..., q_v = p_v$.*

Demonstração. Utilizaremos o Princípio da Indução Completa para provarmos o teorema. Seja $S = \{n \in \mathbb{N} \mid n \text{ é um produto de fatores primos } \vee \ n = 0 \ \vee \ n = 1\}$. Temos que $0, 1 \in S$. Consideremos então $n > 1$. Suponhamos que $(\forall k < n : k \in S)$. Se n não pode ser decomposto em dois fatores $1 < a, b < n$, então n em si é primo, é produto de um fator primo e $n \in S$. Caso n possa ser decomposto em fatores a, b menores que ele e maiores que 1, como $(\forall k < n : k \in S)$, temos $a, b \in S$. Como $a, b > 1$, são eles produtos de fatores primos. Logo, $n = a \times b$ é um produto de fatores primos e $n \in S$. Ou seja, $S = \mathbb{N}$. Todo número ≥ 2 é um produto de fatores primos.

Para a unicidade, supomos por absurdo que n possui duas fatorações diferentes em primos.

$$n = p_1 \times ... \times p_v = q_1 \times ... \times q_w$$

Com $p_1 \leq ... \leq p_v$, $q_1 \leq ... \leq q_w$. Tomamos n o menor natural possível de ser decomposto em dois diferentes produtos de primos (PBO). Temos que $p_1 \mid q_1 \times ... \times q_w$ e assim $p_1 \mid q_i$ para algum $1 \leq i \leq w$. Logo, $p_1 = q_i$, pois q_i é primo. Portanto, $p_1 \geq q_1$. Analogamente, $q_1 \geq p_1$ e concluímos $p_1 = q_1$. Pelo cancelamento da multiplicação temos $m = n/p_1 = n/q_1$. Mas m admite fatoração única, pela minimalidade do n. Logo $w = v$, e $p_j = q_j$, para $1 \leq i \leq v$. Portanto, n admite fatoração única, o que devemos admitir para não incorrermos em contradição. □

Uma importante constatação no estudo de primos é saber que não há uma lista finita de tais números. O teorema de Euclides nos apresenta isso.

Teorema 5.11. *Seja $S = \{n \in \mathbb{Z} \mid n \text{ é primo}\}$. Temos que S não é finito.*

Demonstração. Suponhamos por absurdo que S fosse finito. Teríamos uma lista $p_1, ...p_k$ de todos os primos. Devemos verificar que isso não pode ser o caso. Façamos o produto de todos os primos dessa lista e adicionemos uma unidade. O número $u = p_1 \times ... \times p_k + 1$ não é divisível por nenhum dos primos da lista. Mas pelo teorema anterior, todo número é possível de ser decomposto em fatores primos. Temos duas possibilidades. Ou u em si é primo e não estava na lista original, e concluímos que a lista finita de todos os primos não pode existir. Ou u pode ser decomposto em fatores primos, mas como u não é divisível por nenhum fator da lista original,

pois na divisão euclidiana deixa resto 1, u deve ser decomposto em primos que não estão na lista. E chegamos à mesma conclusão que a lista finita não pode existir. Portanto, o conjunto S não pode ser finito. □

Passamos então a aritmética modular nos inteiros. Começamos com a definição de congruência e a partir dela deduzimos suas propriedades mais importantes. A aritmética modular também estará presente nos Inteiros Gaussianos. A intuição e algumas propriedades para tal contexto variam um pouco, mas a essência permanece. Este estudo é bastante útil para a compreensão da divisibilidade e do comportamento do resto com determinadas operações.

Definição 5.10. Sejam $a, b, c \in \mathbb{Z}$, com $c \neq 0$. Então a **é congruente a** b **módulo** c, escrevemos $a \equiv b \ mod(c)$, caso $c \mid (a - b)$. Ou seja, caso a, b deixem o mesmo resto na divisão euclidiana por c. Não é conveniente deixar $c = 0$, embora tenhamos que $0 \mid 0$.

Exemplo 5.1.

a) $4 \equiv 2 \ mod(2)$

b) $2 \equiv 5 \ mod(3)$

c) $0 \equiv c \ mod(c)$, para qualquer $0 \neq c \in \mathbb{Z}$

d) $-1 \equiv c - 1 \ mod(c)$, para qualquer $0 \neq c \in \mathbb{Z}$

As propriedades a seguir nos dizem que a relação de congruência é uma relação de equivalência. Não por acaso o símbolo de equivalência é utilizado para denotar um número congruente a outro. Também podemos ler $a \equiv b \ mod(c)$ como a **é equivalente a** b **módulo** c.

Proposição 5.27 (Reflexividade)**.** *Para quaisquer $a, n \in \mathbb{Z}$, com $n \neq 0$: $a \equiv a \ mod(n)$.*

Demonstração. Temos, para todo $a, n \in \mathbb{Z}$ e $n \neq 0$, que $n \mid a - a = 0$. Portanto, vale a reflexividade para a congruência. □

Proposição 5.28 (Simetria)**.** *Para quaisquer $a, b, n \in \mathbb{Z}$, com $n \neq 0$: $a \equiv b \ mod(n) \Rightarrow b \equiv a \ mod(n)$.*

Demonstração. Pela definição de congruência, temos que $n \mid a - b$. Logo, $a - b = q \times n$, para algum $q \in \mathbb{Z}$. Então, $-(a - b) = -(q \times n) \Rightarrow b - a = -q \times n$. Portanto, $b \equiv a \ mod(n)$ e vale a simetria para a relação. □

Proposição 5.29 (Transitividade)**.** *Para quaisquer $a, b, c, n \in \mathbb{Z}$, com $n \neq 0$: $a \equiv b \ mod(n)$ e $b \equiv c \ mod(n) \Rightarrow a \equiv c \ mod(n)$.*

Demonstração. Segue da hipótese que $n \mid a - b$ e $n \mid b - c$. Logo, $a - b = vn$ para algum $v \in \mathbb{Z}$ e $b - c = wn$ para algum $w \in \mathbb{Z}$. Assim, $a - b + b - c = vn + wn \Rightarrow a - c = (v + w)n$ e $n \mid a - c$. Portanto, $a \equiv c \ mod(n)$ e vale a transitividade para a congruência. □

Para a relação de congruência, também temos a compatibilidade com a adição, a subtração, o produto, e a potência. Ademais, há a lei do cancelamento.

Proposição 5.30 (Compatibilidade $\equiv$ e adição - I)**.** *Para quaisquer $a, b, c, d, n \in \mathbb{Z}$, com $n \neq 0$: $a \equiv b \ mod(n)$ e $c \equiv d \ mod(n) \Rightarrow a + c \equiv b + d \ mod(n)$.*

Demonstração. Temos que $n \mid a-b$ e $n \mid c-d$. Logo, $a-b = vn$ e $c-d = wn$ para determinados $v, w \in \mathbb{Z}$. Assim, $(a-b)+(c-d) = vn+wn \Rightarrow (a+c)-(b+d) = (v+w)n \Rightarrow n \mid (a+c)-(b+d)$. Portanto, $a + c \equiv b + d \ mod(n)$ e temos a compatibilidade com a adição. □

Proposição 5.31 (Compatibilidade $\equiv$ e adição - II)**.** *Para quaisquer $a, b, c, n \in \mathbb{Z}$, com $n \neq 0$: $a \equiv b \ mod(n) \Rightarrow a + c \equiv b + c \ mod(n)$.*

Demonstração. Basta observarmos que $c \equiv c \ mod(n)$ e aplicarmos a compatibilidade anterior. □

Proposição 5.32 (Compatibilidade $\equiv$ e subtração - I)**.** *Para quaisquer $a, b, c, d, n \in \mathbb{Z}$, com $n \neq 0$: $a \equiv b \ mod(n)$ e $c \equiv d \ mod(n) \Rightarrow a - c \equiv b - d \ mod(n)$.*

Demonstração. Temos que $n \mid a-b$ e $n \mid c-d$. Logo, $a-b = vn$ e $c-d = wn$ para determinados $v, w \in \mathbb{Z}$. Assim, $(a-b)-(c-d) = vn-wn \Rightarrow (a-c)-(b-d) = (v-w)n \Rightarrow n \mid (a-c)-(b-d)$. Portanto, $a - c \equiv b - d \ mod(n)$ e temos a compatibilidade com a subtração. □

Proposição 5.33 (Compatibilidade $\equiv$ e subtração - II)**.** *Para quaisquer $a, b, c, n \in \mathbb{Z}$, com $n \neq 0$: $a \equiv b \ mod(n) \Rightarrow a - c \equiv b - c \ mod(n)$.*

Demonstração. Também para esta proposição, basta observarmos que $c \equiv c \ mod(n)$ e aplicarmos a compatibilidade anterior. □

Proposição 5.34 (Compatibilidade $\equiv$ e produto - I)**.** *Para quaisquer $a, b, c, d, n \in \mathbb{Z}$, com $n \neq 0$: $a \equiv b \ mod(n)$ e $c \equiv d \ mod(n) \Rightarrow ac \equiv bd \ mod(n)$.*

Demonstração. Se $n \mid (a-b)$, temos que $n \mid (a-b)c$. Por outro lado, se $n \mid (c-d)$, temos que $n \mid (c-d)b$. Concluímos que $n \mid (a-b)c + (c-d)b \Rightarrow n \mid ac - bd$. Portanto, $ac \equiv bd \ mod(n)$ e vale a compatibilidade com o produto. □

Proposição 5.35 (Compatibilidade $\equiv$ e produto - II)**.** *Para quaisquer $a, b, k, n \in \mathbb{Z}$, com $n \neq 0$: $a \equiv b \ mod(n) \Rightarrow ak \equiv bk \ mod(n)$.*

Demonstração. Novamente, para esta proposição basta observarmos que $k \equiv k \ mod(n)$ e aplicarmos a compatibilidade anterior. □

Proposição 5.36 (Compatibilidade $\equiv$ e potência)**.** *Para quaisquer $a, b, k, n \in \mathbb{Z}$, com $n \neq 0$, e $k > 0$: $a \equiv b \ mod(n) \Rightarrow a\hat{}k \equiv b\hat{}k \ mod(n)$.*

Demonstração. Basta "aplicarmos sucessivamente" a primeira compatibilidade do produto obtida. Então, $a \equiv b\ mod(n)$ e $a \equiv b\ mod(n) \Rightarrow a \equiv b\ mod(n)$ e $a\hat{}2 \equiv b\hat{}2\ mod(n) \Rightarrow a \equiv b\ mod(n)$ e $a\hat{}3 \equiv b\hat{}3\ mod(n) \Rightarrow ...\ a\hat{}k \equiv b\hat{}k\ mod(n)$. Naturalmente, obtemos a afirmação válida para $k > 0$ utilizando o Princípio da Indução Finita. □

Proposição 5.37 (Lei do cancelamento)**.** *Para quaisquer* $a, b, k, n \in \mathbb{Z}$*, com* $n \neq 0$*: se* $mdc(k, n) = 1$ *então* $ak \equiv bk\ mod(n) \Rightarrow a \equiv b\ mod(n)$*.*

Demonstração. Temos que $n \mid ak - bk$, logo $n \mid (a - b)k$. Mas como $mdc(k, n) = 1$, obtemos que $n \mid (a - b)$ e portanto $a \equiv b\ mod(n)$. □

Alguns comentários para introduzir o conceito de Anel de Inteiros Módulo n. Como já abordamos, a relação de congruência é uma relação de equivalência, ou seja, reflexiva, simétrica e transitiva. Relações de equivalência em um certo conjunto $A \neq \emptyset$ determinam uma partição no mesmo: uma coleção de conjuntos $\neq \emptyset$ dois a dois disjuntos que unidos totalizam A. De fato, reciprocamente, uma partição em um conjunto também determina uma relação de equivalência.

Consideremos a partição dos inteiros formada pelos seguintes conjuntos. Seja $n \neq 0$. Sejam os conjuntos

$$\overline{x} = \{y \in \mathbb{Z} \mid y \equiv x\ mod(n)\}$$

Nessas condições, o conjunto $\{\overline{x} \mid x \in \mathbb{Z}\}$ é chamado de **Anel de Inteiros Módulo** n, que denotaremos por $\mathbb{Z}/n$. Tenhamos em mente que $\overline{a} = \overline{b} \Leftrightarrow a \equiv b\ mod(n) \Leftrightarrow a$ e b deixam o mesmo resto na divisão por n. Definimos operações com as classes de equivalência da seguinte forma. O módulo do qual estaremos tratando futuramente ficará subentendido pelo contexto.

$$\begin{cases} \overline{a} + \overline{b} & = \overline{a + b} \\ \overline{a} - \overline{b} & = \overline{a - b} \\ \overline{a} \times \overline{b} & = \overline{a \times b} \end{cases}.$$

A partir das compatibilidades demonstradas, verificamos sem dificuldade que as operações estão bem definidas pois não dependem dos representantes de classe. De fato, se a, a', b, b' são inteiros tais que $a \equiv a'\ mod(n)$ e $b \equiv b'\ mod(n)$, então $\overline{a + b} = \overline{a' + b'}$, $\overline{a - b} = \overline{a' - b'}$ e $\overline{a \times b} = \overline{a' \times b'}$

Um elemento é dito **inversível** quando podemos multiplicá-lo por outro e obter o elemento neutro da multiplicação. Nos inteiros, os únicos elementos inversíveis são 1 e -1. No entanto, quando lidamos com tais classes de equivalência, teremos outros. Constatemos então o seguinte fato, que será importante para sabermos quando estamos lidando com elementos inversíveis no anel módulo n. Ele nos diz que um elemento a é inversível módulo n se, e somente se, entre n e a temos apenas 1 como divisor comum positivo.

Proposição 5.38. *Sejam $a, n \in \mathbb{Z}$ com $n > 0$. Então $\exists b \in \mathbb{Z}$: $ab \equiv 1\ mod(n)$ se e somente se $mdc(a, n) = 1$.*

Demonstração. Temos a seguinte sucessão de equivalências. Existe b tal que $ab \equiv 1\ mod(n)$ $\Leftrightarrow$ existe b tal que $n \mid ab - 1 \Leftrightarrow$ existe b tal que existe k tal que $ab - 1 = kn \Leftrightarrow$ existem b, k tais que $ab - nk = 1 \Leftrightarrow mdc(a, n) = 1$. □

Assim, dizemos que a **é inversível módulo** n quando $mdc(a, n) = 1$. E b é denominado **inverso multiplicativo de** a **módulo** n. Em termos de classes de congruência, $\overline{a} \times \overline{b} = \overline{1}$. A classe de congruência $\overline{1}$, com efeito, é a unidade para o anel módulo n, em correspondência ao fato de que 1 é a unidade nos inteiros. Ainda, se $ab \equiv ab' \equiv 1\ mod(n)$, temos que $b \equiv b \times 1 \equiv b(ab') \equiv (ba)b' \equiv 1 \times b' \equiv b' mod(n)$. Portanto, o inverso multiplicativo de $\overline{a}$ está bem definido, e podemos denotá-lo por $\overline{a}^{-1}$. Denotamos por $(\mathbb{Z}/n)^{\times}$ o subconjunto formado pelos elementos inversíveis de $\mathbb{Z}/n$. Quando todos os elementos de um anel comutativo são inversíveis (exceto 0) denominamos tal anel de **corpo**. O próximo teorema trata de tal fato.

Teorema 5.12. *O anel $\mathbb{Z}/n$ é um corpo se, e somente se, n é primo.*

Demonstração. $\mathbb{Z}/n$ é corpo equivale a afirmar que todos os seus elementos $\overline{a} \neq \overline{0}$ são inversíveis. Para isso, devemos ter $mdc(a, n) = 1$ para todo a, com $0 < a < n$, ou seja, n é primo. Neste caso e apenas neste, nenhum número a, com $1 < a < n$, divide n. Caso dividisse, o $mdc(a, n)$ seria diferente de 1, o que não atende a hipótese. □

Para concluirmos o estudo dos inversos no anel módulo n devemos abordar a função de Euler e os teoremas de Euler-Fermat. Vamos primeiro definir a função ϕ de Euler, utilizada para contar o número de elementos inversíveis de um anel módulo n.

Definição 5.11. Definimos a função ϕ de Euler da seguinte forma.
$\phi(n) = |(\mathbb{Z}/n)^{\times}|$

Queremos calcular ϕ no caso geral. Vamos considerar como representantes de classe os n números x tais que $0 \leq x < n$. Particularmente quando p é primo, $\phi(p) = p - 1$, pois temos p elementos e apenas $\overline{0} = \overline{p}$ não é inversível. E $\phi(p^k) = p^k - p^{k-1}$, pois $mdc(a, p^k) = 1$ se, e somente se, $p \nmid a$, e temos $(p^k)/p = p^{k-1}$ elementos divisíveis por p no intervalo $0 \leq a < p^k$. Retirando esses de p^k elementos obtemos $p^k - p^{k-1}$. Então sabemos calcular a função ϕ em qualquer potência de primos. Uma importante propriedade dessa função é a sua característica multiplicativa quando dois elementos m, n são **primos entre si**, ou seja, quando $mdc(m, n) = 1$. Esse é o caso entre quaisquer duas potências de primos diferentes. Assim, iremos poder calcular facilmente ϕ de qualquer número, após decompô-lo em potências de primos.

Proposição 5.39. *Para quaisquer $m, n \in \mathbb{N}$: $mdc(m, n) = 1 \Rightarrow \phi(mn) = \phi(m) \times \phi(n)$.*

Demonstração. Consideremos primeiro a matriz abaixo, com m linhas e n colunas.

$$\begin{bmatrix} 1 & 2 & ... & n \\ n+1 & n+2 & ... & 2n \\ \vdots & \vdots & \ddots & \vdots \\ (m-1)n+1 & (m-1)n+2 & ... & (m-1)n+n = mn \end{bmatrix} \tag{5.1}$$

Observamos que $mdc(in+j, n) = mdc(j, n)$, pelo argumento de conjuntos de divisores comuns iguais. Então ocorre que se apenas um número, denotado por $in+j$, em uma das colunas é primo com n, teremos $mdc(in+j, n) = mdc(j, n) = 1$ e então $mdc(kn+j, n) = mdc(j, n) = 1$ e qualquer outro número da mesma coluna será primo com n. Na primeira linha, podemos perceber que temos $\phi(n)$ colunas de elementos primos com n. Em contrapartida, em cada coluna (de primos com n ou não) devemos ter um conjunto completo de representantes de classe módulo m, e portanto devemos ter em cada coluna $\phi(m)$ elementos primos com m. Teremos todos os representantes de classe pois, por exemplo, considerando dois elementos da coluna j, temos $i_1 n+j \equiv i_2 n+j \ mod(m) \Rightarrow i_1 n+j-j \equiv i_2 n+j-j \ mod(m) \Rightarrow i_1 n \equiv i_2 n \ mod(m) \Rightarrow i_1 \equiv i_2 \ mod(m) \Rightarrow i_1 = i_2$, sendo o cancelamento devido a $mdc(m, n) = 1$. Assim, em cada uma de $\phi(n)$ colunas de primos com n teremos $\phi(m)$ elementos que também serão primos com m e portanto primos com mn. Lembrando que se $mdc(m, k) = 1$ e $mdc(n, k) = 1$, temos que $mdc(mn, k) = mdc(n, k) = 1$. A quantidade de números primos com mn portanto é $\phi(mn) = \phi(m)\phi(n)$. □

Se a forma fatorada de n em potências de primos distintos é $n = p_1^{a_1}...p_k^{a_k}$, calculamos $\phi(n) = \phi(\prod_{i=1}^{k} p_i^{a_i}) = \prod_{i=1}^{k} \phi(p_i^{a_i}) = \prod_{i=1}^{k} (p_i^{a_i} - p_i^{a_i-1}) = \prod_{i=1}^{k} p_i^{a_i}(1 - 1/p_i) = n\prod_{i=1}^{k}(1 - 1/p_i)$.

Passamos assim ao teorema de Euler-Fermat, o qual também terá uma versão para inteiros gaussianos.

Teorema 5.13 (Euler-Fermat)**.** *Para quaisquer $a, m \in \mathbb{Z}$: se $mdc(a, m) = 1$, então $a^{\phi(m)} \equiv 1 \ mod(m)$.*

Demonstração. Seja $\{r_1, ..., r_{\phi(m)}\}$ um sistema completo de inversíveis módulo m, isto é, dois a dois não congruentes entre si, representando todas as classes inversíveis no anel de inteiros módulo m. Seja a um número natural tal que $mdc(a, m) = 1$. Assim, $ar_1, ..., ar_{\phi(m)}$ é um sistema completo de inversíveis módulo m, pois $mdc(a, m) = 1 \ \wedge \ mdc(r_i, m) = 1 \Rightarrow mdc(ar_i, m) = mdc(r_i, m) = 1$ e também $ar_i \equiv ar_j \ mod(m)$ implica $r_i \equiv r_j \ mod(m)$, pelo cancelamento, e então $i = j$. Logo, devemos ter cada ar_v congruente a um r_w. Portanto $\prod_{i=1}^{\phi(m)}(ar_i) \equiv \prod_{i=1}^{\phi(m)}(r_i) \ mod(m) \Rightarrow a^{\phi(m)}\prod_{i=1}^{\phi(m)}(r_i) \equiv \prod_{i=1}^{\phi(m)}(r_i) \ mod(m)$. Como o produtório resultante é inversível módulo m, pois todos os fatores são inversíveis, podemos aplicar o cancelamento e obter $a^{\phi(m)} \equiv 1 \ mod(m)$. □

Assim, imediatamente obtemos o Pequeno Teorema de Fermat.

Teorema 5.14 (Pequeno Teorema de Fermat)**.** *Para quaisquer* $a, p \in \mathbb{Z}$*, com* p *primo:* $a^p \equiv a \ mod(p)$*.*

Demonstração. Se $p \mid a$ teremos apenas $0 \equiv 0 \ mod(p)$. Caso contrário, basta lembrarmos que $\phi(p) = p - 1$. Então, pelo teorema 5.13, como $mdc(a, p) = 1$, $a^{p-1} \equiv 1 \ mod(p)$. E utilizando a compatibilidade com a multiplicação, temos $a^p \equiv a \ mod(p)$. □

6 POLINÔMIOS EM UMA VARIÁVEL

Começamos um breve estudo de polinômios em uma variável em um contexto geral, e comparamos com os números inteiros. Para isso, utilizamos os conceitos de **anel comutativo** e **anel com unidade**. De fato, um domínio de integridade, como é o caso dos inteiros, deve ser um anel comutativo com unidade. Para tanto, além das propriedades de anel, pedimos que o operador de multiplicação seja comutativo, e que tenhamos o elemento neutro para o mesmo. Para os resultados significativos, será importante também que exista inverso (corpo). Assim, podemos por exemplo falar de anel de inteiros módulo n, racionais, etc.

Definição 6.1. Seja K um anel comutativo com unidade. Definimos $K[x]$ como o conjunto de expressões $f(x)$ da forma $a_0 + a_1x + a_2x^2 + ... + a_nx^n$, com $a_i \in K$. Chamaremos tais expressões de **polinômios** com coeficientes em K, e $K[x]$ (com operações de soma e produto que serão abordadas adiante) de **anel de polinômios** com coeficientes em K.

Denotaremos essas expressões da seguinte forma $f(x) = \sum_i a_i x^i$, em que o somatório é feito ao ∞ e apenas se indica a variável i que corre (determina os termos) a partir do valor 0. O maior índice j tal que $a_j \neq 0$ será denominado **grau**, *deg*, do polinômio. O coeficiente a_j por sua vez é chamado de **coeficiente líder**. Se o polinômio é nulo, estabelecemos o coeficiente líder = 0.

Consideremos agora outra expressão $g(x) = \sum_i b_i x^i$. Definimos a soma e o produto em $K[x]$ por: $f(x) + g(x) = \sum_i (a_i + b_i)x^i$ e $f(x) \times g(x) = \sum_k (c_k)x^k$, em que $c_k = \sum_{i+j=k} a_i b_j$. O somatório anterior denota a adição de certos produtos, em que índices somados resultam em k. Lembramos que $0 \leq i$ e $0 \leq j$. Ainda, $c_k \neq 0$ implica $i \leq deg(f(x))$ e $j \leq deg(g(x))$, portanto temos finitos $c_k \neq 0$ e permanecemos no contexto de polinômios.

O grau do polinômio nulo é definido como $-\infty$. O objetivo aqui é tornar válidas as seguintes afirmações, que para serem válidas também precisam que K seja domínio.

$$deg(f(x) + g(x)) \leq max\{deg(f(x)), deg(g(x)\}$$

$$deg(f(x) \times g(x)) = deg(f(x)) + deg(g(x))$$

Lembramos agora da definição formal e algébrica de polinômio, que conceitua tal objeto como uma sequência quase nula de coeficientes. A definição aqui parte das expressões já desenvolvidas quando consideramos a adição e a multiplicação para tais sequências e $x = (0, 1, 0, ...)$. Dessa forma, consideremos que o x acima não é um elemento de K, mas um símbolo formal que denota uma constante.

Destacamos a definição precursora. Não iremos verificar, mas os polinômios formam um anel, sob as condições mínimas exigidas para defini-los. Temos um domínio de integridade, caso

o anel seja um domínio; mas não um corpo, caso aquele seja um corpo. As próximas afirmações ajudam a entender a herança de propriedades.

Proposição 6.1. *Seja K um anel e $K[x]$ o anel de polinômios com coeficientes em K. Então K é comutativo $\iff$ $K[x]$ é comutativo.*

Demonstração. [$\Rightarrow$] Se K é um anel comutativo, $f(x) \times g(x) =$
$(\sum_{i+j=0} a_i b_j, \sum_{i+j=1} a_i b_j, ...) = (\sum_{i+j=0} b_j a_i, \sum_{i+j=1} b_j a_i, ...) = g(x) \times f(x)$.
[$\Leftarrow$] Se $f(x) \times g(x) = g(x) \times f(x)$ para quaisquer $f(x), g(x) \in K[x]$, em particular: $(a_0 b_0, 0, 0, ...) = (a_0, 0, 0, ...) \times (b_0, 0, 0, ...) = (b_0, 0, 0, ...) \times (a_0, 0, 0, ...) = (b_0 a_0, 0, 0, ...)$. Portanto, $a_0 b_0 = b_0 a_0$, para quaisquer $a_0, b_0 \in K$. □

Proposição 6.2. *Seja K um anel e $K[x]$ o anel de polinômios com coeficientes em K. Então K tem unidade $\iff$ $K[x]$ tem unidade.*

Demonstração. [$\Rightarrow$] Se K possui unidade, ela é única. Denotamos (usualmente) por 1. Então, $(a_0, a_1, a_2, ...) \times (1, 0, 0, ...) = (1, 0, 0, ...) \times (a_0, a_1, a_2, ...) = (1a_0, 1a_1, 1a_2, ...) = (a_0, a_1, a_2, ...)$, e temos a unidade para $K[x]$.
[$\Leftarrow$] Se $K[x]$ possui unidade, então $f(x) \times 1 = 1 \times f(x) = f(x)$ para qualquer $f(x) \in K[x]$, em particular $1 \times (a, 0, 0...) = (a, 0, 0, ...)$. Logo, $deg(1) = 0$ e podemos escrever $1 = (t, 0, 0, ...)$. Assim, $(ta, 0, 0, ...) = (at, 0, 0, ...) = (a, 0, 0, ..) \iff ta = at = a$, para qualquer $a \in K$. Ou seja $t = 1$, K possui unidade. □

Proposição 6.3. *Seja K um anel e $K[x]$ o anel de polinômios com coeficientes em K. Então K é domínio de integridade $\iff$ $K[x]$ é domínio de integridade.*

Demonstração. Para falarmos em domínio, já estamos supondo a unidade e a comutatividade. Portanto temos as expressões usuais para polinômios.
[$\Leftarrow$] Se $f(x)g(x) = 0 \Rightarrow f(x) = 0 \ \vee \ g(x) = 0$, em particular $a_0 b_0 \Rightarrow a_0 = 0 \ \vee \ b_0 = 0$.
[$\Rightarrow$] Se $f(x)g(x) = 0$, escrevemos $f(x) = a_0 + ... + a_v x^v$ e $g(x) = b_0 + ... + b_w x^w$. Supomos $f(x) \neq 0$. Então $(a_0 + ... + a_v x^v)(b_0 + ... + b_w x^w) = 0$ implica sucessivamente: $b_w = 0$, pois $c_{v+w} = a_v b_w = 0$; $b_{w-1} = 0$, pois $c_{v+w-1} = a_v b_{w-1} = 0$; ... $b_0 = 0$, pois $c_v = a_v b_0 = 0$. Portanto, $g(x) = 0$. □

Podemos utilizar essas expressões para construir as chamadas **funções polinomiais**. Cada polinômio $f(x) = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n$ define uma única função polinomial $f : K \to K$, $c \mapsto f(c) = a_0 + a_1 c + a_2 c^2 + ... + a_n c^n$. Contudo, mais de um polinômio pode determinar uma mesma função polinomial. Os objetos apresentados possuem natureza distinta e portanto não podemos confundi-los. Um bom exemplo de que não temos uma correspondência biunívoca entre polinômios e funções polinomiais é o seguinte.

Exemplo 6.1. Seja o polinômio $f(x) = x^p - x \in (\mathbb{Z}/p)[x]$. E considere a função polinomial que o mesmo define. Temos pelo Pequeno Teorema de Fermat que tal função se anula em todo $c \in (\mathbb{Z}/p)$. Mas o polinômio (expressão) apresentado é diferente de $n(x) = 0 \in (\mathbb{Z}/p)[x]$, que

determina a mesma função polinomial nula. Assim, no contexto de aritmética modular, faz ainda mais sentido separar os conceitos de polinômio e função polinomial.

Considerando-se $f(x) \in K[x]$, se temos um $c \in K$ tal que $f(c) = 0$, chamamos tal elemento de **zero** ou **raiz** de $f(x)$.

Para os polinômios, sob determinadas condições, temos situações análogas àquelas no contexto dos inteiros. Por exemplo, podemos citar aqui: a definição de divisibilidade; a divisão euclidiana; o máximo divisor comum; o algoritmo de Euclides; o teorema de Bachet-Bezout; o conceito de polinômios irredutíveis, em semelhança com primos; o lema de Euclides; a fatoração única; a aritmética modular. Passemos a abordagem desses elementos.

Definição 6.2. Sejam $a(x), b(x) \in K[x]$. Dizemos que $b(x)$ **divide** $a(x)$, escrevemos $b(x) \mid a(x)$, se existe $q(x) \in K[x]$, tal que $a(x) = b(x) \times q(x)$.

Passamos então à divisão euclidiana, que sai de maneira menos imediata.

Teorema 6.1 (Divisão euclidiana)**.** *Seja K um corpo. E sejam polinômios $f(x), g(x) \in K[x]$, com $g(x) \neq 0$. Então existem polinômios $q(x), r(x) \in K[x]$, denominados **quociente** e **resto** respectivamente, tais que $f(x) = g(x)q(x) + r(x)$ com $deg(r(x)) < deg(g(x))$. Ademais, tais polinômios são únicos.*

Demonstração. Tomamos $m = deg(f(x))$ e $n = deg(g(x))$. Primeiramente, se $n > m$ temos que $q(x) = 0$ e $r(x) = f(x)$ satisfazem a relação, e também são os únicos possíveis. De fato, qualquer $q(x) \neq 0$ multiplicando $g(x)$ resulta em um polinômio com grau $\geq n$ e somando com $r(x)$, cujo grau requisitamos que seja $< n$, devemos ter o lado direito com grau maior do que o lado esquerdo da equação, absurdo. Nas considerações a seguir, a unicidade é deixada para o final.

Podemos supor então que $m \geq n$. Partimos do caso $n = 0$ ($g(x) \neq 0 \Rightarrow n \geq 0$ já pelo enunciado). Se $m = n = 0$, então $f(x) = a_0 \neq 0$ e $g(x) = b_0 \neq 0$. Ou seja, os polinômios são apenas constantes não nulas (se tivéssemos $f(x) = 0$ voltaríamos ao caso $n > m$ já descartado). Assim, tomamos $q(x) = a_0/b_0$ e $r(x) = 0$. Lembrando que estamos em um corpo, e por isso temos a_0/b_0. Continuando, se $m \geq 1$, escrevemos $f(x) = a_m x^m + f'(x)$, com $a_m \neq 0$, $deg(f'(x)) < m$, e $g(x) = b_0 \neq 0$, igualmente. Consideramos então o polinômio $f(x) - (a_m/b_0)x^m g(x) = f'(x)$, que terá grau menor do que m. Supondo que todo polinômio de grau menor do que m pode ser expresso como no enunciado: $f(x) - (a_m/b_0)x^m g(x) = g(x)q(x) + r(x)$ com $deg(r(x)) < 0$); obtemos $f(x) = ((a_m/b_0)x^m + q(x))g(x) + r(x)$, o resto sendo o mesmo (= 0). Por indução, todo polinômio com grau $m \geq 0$ pode ser expresso como no enunciado, quando $n = 0$.

Supomos a seguinte

Hipótese de indução : *Para todo k, $0 \leq k < n$, temos que para todo $m \geq k$, se $deg(f(x)) = m$ e $deg(g(x)) = k$, então existem $q(x)$ e $r(x)$ tais que $f(x) = g(x)q(x) + r(x)$, com $deg(r(x)) < deg(g(x))$.*

Queremos obter que para todo $m \geq n$, se $deg(f(x)) = m$ e $deg(g(x)) = n$, então existem $q(x)$ e $r(x)$ tais que $f(x) = g(x)q(x) + r(x)$, com $deg(r(x)) < deg(g(x))$. Dentro da indução, precisamos realizar outra.

Consideremos assim o caso $m = n \neq 0$. Temos $f(x) = a_0 + a_1x + a_2x^2 + ... + a_mx^m$, e $g(x) = b_0 + b_1x + b_2x^2 + ... + b_mx^m$. Fazendo $q(x) = a_m/b_m$ e $f'(x) = f(x) - q(x)g(x)$, temos que $deg(f'(x)) < deg(f(x)) = deg(g(x))$ e desse modo teremos $q'(x)$ e $r'(x)$ tais que $f'(x) = q'(x)g(x) + r'(x)$, com $deg(r'(x)) < deg(g(x))$ (de fato, $q'(x) = 0$ e $r'(x) = f'(x)$. Portanto, $f(x) - q(x)g(x) = q'(x)g(x) + r'(x) \Rightarrow f(x) = (q(x) + q'(x))g(x) + r'(x)$.

Realizamos mais uma hipótese de indução. Supomos que para todo $0 \leq i < j$, temos que, se $deg(f(x)) = n + i$ e $deg(g(x)) = n$, então existem $q(x)$ e $r(x)$ tais que $f(x) = g(x)q(x) + r(x)$, com $deg(r(x)) < deg(g(x))$. Queremos obter que se $deg(f(x)) = n + j$ e $deg(g(x)) = n$, então existem $q(x)$ e $r(x)$ tais que $f(x) = g(x)q(x) + r(x)$, com $deg(r(x)) < deg(g(x))$.

Temos $f(x) = a_0 + a_1x + a_2x^2 + ... + a_{n+j}x^{n+j}$, e $g(x) = b_0 + b_1x + b_2x^2 + ... + b_nx^n$. Fazendo $v(x) = (a_{n+j}/b_n)x^j$ e $f'(x) = f(x) - v(x)g(x)$ temos que $deg(f'(x)) < deg(f(x))$ e portando $deg(f'(x)) = n + i$ para algum $0 \leq i < j$. Da hipótese de indução, temos $q'(x)$ e $r'(x)$ tais que $f'(x) = q'(x)g(x) + r'(x)$, com $deg(r'(x)) < deg(g(x))$. Portanto, $f(x) - v(x)g(x) = q'(x)g(x) + r'(x) \Rightarrow f(x) = (v(x) + q'(x))g(x) + r'(x)$, e determinamos $q(x) = v(x) + q'(x)$ e $r(x) = r'(x)$.

Logo, sem de fato precisar usar a hipótese de indução acima, induzimos no grau do divisor que vale para n. Ou seja não houve necessidade de usar que vale a divisão para todo grau de divisor $0 \leq k < n$. Provamos que vale para todo dividendo com grau $m \geq n$, pois no caso base apenas retornamos à situação em que o grau do divisor fica maior que o grau do dividendo.

Para a unicidade, suponhamos que dados $f(x)$ e $g(x)$ como na hipótese tenhamos $f(x) = q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_2(x)$, com $q_1(x) \neq q_2(x)$, $r_1(x) \neq r_2(x)$ e $deg(r_1(x)), deg(r_2(x)) < deg(g(x))$. Nesse caso, teríamos $r_1(x) - r_2(x) = (q_2(x) - q_1(x))g(x)$. Mas pela equação deveríamos obter $deg(r_1(x) - r_2(x)) \geq deg(g(x))$. No entanto, $deg(r_1(x) - r_2(x)) \leq max\{deg(r_1(x)), deg(r_2(x))\} \Rightarrow deg(r_1(x) - r_2(x)) < deg(g(X))$ e chegamos à contradição. Logo, $r_1(x) = r_2(x)$ e $q_1(x) = q_2(x)$. □

Como consequência direta do teorema 6.1 temos:

Corolário 6.1 (Teorema do resto)**.** *Seja K um corpo, $f(x) \in K[x]$ e $a \in K$. Então $x - a \mid f(x) \Leftrightarrow f(a) = 0$.*

Demonstração. Fazemos a divisão euclidiana do polinômio $f(x)$ por $x - a$. Como $deg(x - a) = 1$, o resto deverá ter grau menor do que 1 (0 ou $-\infty$). Assim, denotaremos o mesmo por um coeficiente r. Segue que $f(x) = q(x)(x-a)+r$. Se $(x-a) \mid f(x)$, então $f(x) = q(x)(x-a) \Rightarrow f(a) = 0$. Por outro lado, se $f(a) = 0$, então $0 = f(a) = q(a)(a - a) + r \Rightarrow r = 0$. □

Antes de passarmos à definição de máximo divisor comum entre dois polinômios, observamos o seguinte. Ao tentarmos definir tal conceito para polinômios de maneira semelhante ao

que fizemos para $\mathbb{Z}$, encontramos algumas diferenças. Primeiro, precisamos de um parâmetro para falarmos de "máximo", e a escolha razoável seria o grau. Devemos ainda fazer a suposição idêntica de que não temos ambos os termos nulos, caso contrário não existe um limite para maior grau de polinômio que divide 0. Mas basta termos um $f(x) \neq 0$ e certamente nenhum outro com grau maior que $deg(f(x))$ pode dividi-lo.

O maior grau possível de polinômio que divide $f(x)$ seria então, propriamente, $deg(f(x))$. De fato, existe um polinômio com tal grau que o divide ($f(x)$ por exemplo). Suponhamos $f(x) = q(x)f'(x)$, com $deg(f'(x)) = deg(f(x))$. Devemos ter assim $q(x) = c$, $0 \neq c \in K$. Então, $f(x) = cf'(x) \Leftrightarrow f'(x) = (1/c)f(x) \Leftrightarrow f'(x) = c'f(x)$ e temos que qualquer $f'(x)$ obtido ao se multiplicar $f(x)$ por uma constante $\neq 0$ deve dividir este último. Na realidade, se $g(x) \mid f(x)$, não necessariamente de mesmo grau, $f(x) = q(x)g(x) \Rightarrow f(x) = (1/c)q(x)cg(x)$ e qualquer múltiplo não nulo de $g(x)$ também divide $f(x)$. Isso nos motiva a padronizarmos e considerarmos os divisores **mônicos**, com coeficiente líder = 1, que podemos obter sem dificuldade a partir de polinômio dado.

Observamos que a lista de divisores mônicos de qualquer polinômio é não vazia, pois $d(x) = 1$ sempre é divisor, e portanto entre duas listas certamente haverá ao menos um em comum, como visto antes.

Temos apenas um ponto delicado a abordar. Se $d_1(x)$ é divisor de um polinômio $f(x)$, sabemos que qualquer múltiplo por uma constante também será. Porém, será o caso que quando dois polinômios $d_1(x)$ e $d_2(x)$ são divisores devemos ter que estes são múltiplos entre si por uma constante? Obviamente podemos ter polinômios de graus diferentes dividindo $f(x)$, então façamos a pergunta considerando que $d_1(x), d_2(x)$ possuem o mesmo grau. Se sim, seriam ambos múltiplos de um mesmo polinômio mônico. Então reformulemos mais uma vez. Será o caso que quando dois polinômios mônicos $d_1(x)$ e $d_2(x)$ de mesmo grau dividem $f(x)$, eles são o mesmo?

Tomando o exemplo $(x + 1)(x)(x - 1)$, temos três divisores mônicos de grau 1 (ou grau 2) e que não são iguais entre si. Portanto a resposta é não. Mas quando pedimos que $d_1(x)$ seja divisor mônico de maior grau de $f(x)$, pelo que foi mostrado anteriormente, teremos de fato a unicidade. Entretanto, quando pedimos que $d_1(x)$ seja divisor mônico de maior grau de $f(x)$ e $g(x)$, fica difícil garantirmos o mesmo. Para cada grau menor que do dividendo, podemos ter mais de um polinômio mônico divisor. Assim, é conveniente reformular a definição de máximo divisor comum.

Definição 6.3. Seja um corpo K e sejam $f(x), g(x) \in K[x]$, não sendo ambos nulos. Definimos um **máximo divisor comum** de $f(x)$ e $g(x)$ como um polinômio mônico de grau máximo que divide $f(x)$ e $g(x)$.

Com efeito, se $q(x)$ e $q'(x)$ são máximos divisores comuns de $f(x)$ e $g(x)$, temos $deg(q(x)) \geq deg(q'(x))$ e $deg(q'(x)) \geq deg(q(x))$. Assim, $deg(q(x)) = deg(q'(x))$. Vamos ao algoritmo de Euclides, que é análogo ao já estudado e nos dá um método para obter um máximo

divisor comum.

Seja um corpo K e sejam $f_1(x), f_2(x) \in K[x]$, não ambos nulos. E $a_1, a_2 \in K$, respectivamente, os coeficientes líderes de tais polinômios. Se $f_2(x) = 0$, temos $f_1(x) \neq 0$, e consideramos $(1/a_1)f_1(x)$ como um *mdc*. Se $f_1(x) = 0$ a situação é análoga. Supomos então que $f_1(x), f_2(x) \neq 0$ e que $deg(f_1(x)) \geq deg(f_2(x))$, sem perda de generalidade. Podemos efetuar a divisão euclidiana de $f_1(x)$ por $f_2(x)$ e encontrar os únicos quociente $q_1(x)$ e resto $f_3(x)$ ($deg(f_3(x)) < deg(f_2(x))$) que satisfazem a expressão $f_1(x) = q_1(x) \times f_2(x) + f_3(x)$. Se $f_3(x) = 0$, consideramos $(1/a_2)f_2(x)$ como um *mdc*. Caso contrário, efetuamos a divisão euclidiana de $f_2(x)$ por $f_3(x)$, ambos diferentes de 0, e encontramos os únicos quociente $q_2(x)$ e resto $f_4(x)$ ($deg(f_4(x)) < deg(f_3(x))$) que satisfazem a expressão $f_2(x) = q_2(x) \times f_3(x) + f_4(x)$. Em geral, se $f_i(x), f_{i+1}(x) \neq 0$, realizamos a divisão de $f_i(x)$ por $f_{i+1}(x)$ e encontramos os únicos quociente $q_i(x)$ e resto $f_{i+2}(x)$ ($deg(f_{i+2}(x)) < deg(f_{i+1}(x))$) tais que $f_i = q_i \times f_{i+1} + f_{i+2}$.

Teorema 6.2 (Algoritmo de Euclides)**.** *Temos que os valores da sequência finita* $deg(f_n(x))$ *sempre decrescem e o último termo deve ser* $-\infty$*. Nesse processo, se* $f_u(x)$ *é o último polinômio diferente de* 0 *podemos considerar* $(1/a_u)f_u(x)$ *como um mdc de* $f_1(x), f_2(x)$*.*

Demonstração. A demonstração é análoga ao dos números inteiros. Na divisão euclidiana de $f(x)$ por $g(x)$, temos: $f(x) = q(x) \times g(x) + r(x)$ e $deg(r(x)) < deg(g(x))$. Os polinômios divisores comuns a $g(x)$ e $f(x)$ também dividem $r(x)$, mesmo para $r(x) = 0$ (se $u(x)$ é divisor comum, $r(x) = f(x) - q(x) \times g(x) = a(x) \times u(x) - q(x) \times (b(x) \times u(x)) = (a(x) - q(x) \times b(x)) \times u(x)$). Logo, dividem $g(x)$ e $r(x)$. Por outro lado, os divisores comuns a $g(x)$ e $r(x)$ também dividem $f(x)$, e portanto dividem $g(x)$ e $f(x)$. Logo, o conjunto de divisores comuns de $g(x)$ e $f(x)$ e o conjunto de divisores comuns de $g(x)$ e $r(x)$ é o mesmo. Então os maiores elementos são o mesmo. No algoritmo, isso ocorre para cada nova divisão efetuada e portanto o conjunto dos divisores comuns é preservado e junto é preservado os maiores divisores comuns, de maior grau. Caso o resto seja zero, um maior divisor comum pode ser o polinômio mônico múltiplo do último divisor, sendo relativo aos dois elementos do início. □

Demonstraremos o Teorema de Bachet-Bezout de forma alternativa, que também poderia ter sido empregada anteriormente e fornece um método para resolver a equação do enunciado.

Teorema 6.3 (Bachet-Bezout)**.** *Seja um corpo* K *e sejam* $f(x), g(x) \in K[x]$ *polinômios não ambos nulos. Então existem* $m(x), n(x) \in K[x]$ *tais que* $f(x)m(x) + g(x)n(x) = d(x)$*, para algum* $d(x)$ *máximo divisor comum de* $f(x), g(x)$*.*

Demonstração. Para encontrar tais $m(x), n(x)$ utilizamos o algoritmo de Euclides anterior. Se um dos polinômios iniciais é nulo, basta construirmos o polinômio mônico que é múltiplo do outro. Supomos então que $f(x), g(x) \neq 0$ e $deg(f(x)) \geq deg(g(x))$, sem perda de generalidade. Assim, do algoritmo, consideramos $f(x) = f_1(x)$, $g(x) = f_2(x)$. Supomos $f_u(x)$ o último elemento não nulo da sequência de polinômios obtida com o algoritmo, e tomamos $d(x) = (1/a_u)f_u(x)$, em que a_u é

o coeficiente líder de $f_u(x)$. Omitimos o x abaixo.

$$
\begin{aligned}
f_1 &= q_1 \times f_2 + f_3 \\
f_2 &= q_2 \times f_3 + f_4 \\
f_3 &= q_3 \times f_4 + f_5 \\
&\vdots \\
f_{u-2} &= q_{u-2} \times f_{u-1} + f_u \\
f_{u-1} &= q_{u-1} \times f_u + 0
\end{aligned}
$$

O elemento f_3 da primeira equação é uma combinação $\mathbb{Z}[x]$-linear de f_1, f_2, bem como $f_2 = 0f_1 + f_2$. A cada nova equação, consideramos o segundo e o terceiro elementos da anterior, expressos como combinação $\mathbb{Z}[x]$-linear de f_1, f_2, e substituímos na atual, encontrando a expressão deste terceiro elemento como combinação $\mathbb{Z}[x]$-linear de f_1, f_2. Fazemos isso até a penúltima equação e obtemos a expressão de f_u como combinação $\mathbb{Z}[x]$-linear de f_1, f_2. Por fim, apenas multiplicamos tal equação por $1/a_u$, para obtermos $d(x)$, um *mdc*. □

Considerando as mesmas condições do enunciado; como temos $f(x)m(x) + g(x)n(x) = d(x)$, para determinados $m(x), n(x) \in K[x]$, qualquer divisor comum a $f(x)$ e $g(x)$ também dividirá $d(x)$. Em particular, os divisores com o maior grau possível também serão divisores para $d(x)$. Assim podemos tirar duas conclusões.

Primeiro que, como qualquer polinômio $d'(x)$ divisor de $f(x), g(x)$ também divide $d(x)$, se o grau de $d'(x)$ for máximo teremos (para algum $c \neq 0$) $d(x) = cd'(x) \Leftrightarrow d'(x) = (1/c)d(x) \Leftrightarrow d'(x) = c'd(x)$ e todo divisor comum de grau máximo é múltiplo do polinômio mônico. Logo, temos de fato a unicidade do máximo divisor comum.

Segundo que as combinações $\mathbb{Z}[x]$-lineares de $f(x), g(x)$ possuem uma "parada" para o grau não negativo mínimo que conseguem atingir (tal limite inferior para $deg(f(x)i(x) + g(x)j(x))$ é $deg(mdc(f(x), g(x)))$. De fato, no caso dos inteiros havia uma "parada" para o valor positivo mínimo: o *mdc*. Esse elemento não só é o mínimo possível como é o mínimo de fato, pelo Teorema de Bachet-Bezout. Observamos que podemos facilmente fazer $deg(f(x)g(x)+g(x)(-f(x))) = -\infty$; e $ab + b(-a) = 0$, no contexto dos inteiros.

Passamos à definição de polinômios irredutíveis, conceito que tem considerável semelhança com o conceito de números primos, estudados anteriormente.

Definição 6.4. Seja K um corpo e $f(x) \in K[x]$, com $deg(f(x)) \geq 1$ (ou seja, $deg(f(x)) \neq -\infty, 0$). Dizemos que $f(x)$ é **irredutível** em $K[x]$ se $f(x) = g(x)h(x)$ (com $g(x), h(x) \in K[x]$) implica $deg(g(x)) = deg(f(x))$ ou $deg(h(x)) = deg(f(x))$. Ou seja, $f(x)$ não pode ser decomposto em dois polinômios com graus estritamente menores que $deg(f(x))$

Por hipótese $deg(f(x)) \geq 1$, assim $f(x) \neq 0, c$, para qualquer $c \in K$. Logo, se $f(x) = g(x)h(x)$, temos ambos polinômios $\neq 0$, e é o caso de expressar $deg(f(x))$ como a soma de dois

naturais. Se não conseguimos $g(x), h(x)$ tais que $f(x) = g(x)h(x)$ e $0 < deg(g(x)), deg(h(x)) < deg(f(x))$, então $f(x)$ é irredutível. Como $deg(f(x)) = deg(g(x)) + deg(h(x))$, nesse caso teremos também um dos graus sendo 0. Vamos a alguns exemplos de polinômios irredutíveis.

Exemplo 6.2. a) Naturalmente, todo polinômio $f(x) \in K[x]$ de grau 1 é irredutível. Pois temos que as possibilidades são $deg(g(x)) = 0$ ou $= 1$. Nos dois casos, um dos fatores terá o mesmo grau que $f(x)$.

b) O polinômio $x^2 + 1$ é irredutível em $\mathbb{Z}[x]$, pois caso contrário seria escrito como produto de dois polinômios (de grau 1) mônicos com coeficientes inteiros, e teríamos raízes inteiras. Mas sabemos que tal polinômio sequer possui raízes reais. Da mesma forma, $x^2 + 1$ é irredutível em $\mathbb{R}[x]$. Porém $x^2 + 1 = (x + i)(x - i)$ e portanto é redutível em $\mathbb{C}[x]$.

Sendo K um corpo, e $K[x]$ o anel de polinômios com coeficientes em K, quando os únicos irredutíveis nesse contexto são os lineares mônicos (isto é, da forma $x - a$), diremos que o corpo é **algebricamente fechado**. Isso significa em essência que todo polinômio com coeficientes em K será em último caso expresso em produto de fatores lineares mônicos (e um fator escalar) e portanto suas raízes sempre estarão em K. Ressaltemos como isso é uma propriedade do corpo e não do anel de polinômios. Passemos a mais analogias com inteiros, agora devido ao Lema de Euclides. Por simplicidade denotamos também os polinômios por variáveis, por exemplo, f no lugar de $f(x)$.

Proposição 6.4 (Lema de Euclides)**.** *Seja um corpo K e sejam $f, g, h \in K[x]$. Se $f \mid gh$ e $mdc(f, g) = 1$, então $f \mid h$.*

Demonstração. Temos pelo teorema 6.3 que $fv + gw = 1$, para determinados $v, w \in K[x]$. Concluímos que $hfv + hgw = h$. Como $f \mid hf$ e $f \mid gh$, temos que f divide o lado esquerdo da equação. Portanto, $f \mid h$. □

Sendo K um corpo, e $p, a \in K[x]$, com p polinômio mônico irredutível, então $mdc(a, p) = 1$ ou $mdc(a, p) = p$, de maneira semelhante.

Proposição 6.5. *Seja K um corpo e $p \in K[x]$ um polinômio mônico irredutível e sejam $a_1, a_2, ..., a_m \in K[x]$. Se $p \mid a_1 \times a_2 \times ... \times a_m$, então $p \mid a_i$, para algum $i \in \{1, 2, ..., m\}$.*

Demonstração. A demonstração segue a mesma lógica de anteriormente. Consideramos primeiro o produto $a_1 \times a_2$ e supomos que $p \mid a_1 \times a_2$. Se $p \mid a_1$, o enunciado é satisfeito. Se $p \nmid a_1$, o único divisor comum mônico entre ambos é 1, e portanto é o máximo divisor comum. Da proposição 6.4 $p \mid a_2$. Para o caso com m termos, podemos aplicar uma Indução Finita e obter o resultado. □

E assim temos a fatoração única reformulada.

Teorema 6.4 (Fatoração única)**.** *Seja um corpo K e $f \in K[x]$ mônico, com $deg(f) \geq 1$. Então, f pode ser expresso em um único produto de polinômios irredutíveis mônicos, a menos da ordem desses fatores. Ou seja $f = p_1 \times ... \times p_v$, com $p_1, ..., p_v$ polinômios irredutíveis mônicos. Caso $g = q_1 \times ... \times q_w$, com $q_1, ..., q_w$ polinômios irredutíveis mônicos, temos $w = v$, e $q_i = p_{j(i)}$, em que j é uma permutação em $\{1, ..., v\}$.*

Demonstração. Utilizaremos o Princípio da Indução Completa para provarmos o teorema. Seja $S = \{n \in \mathbb{N} \mid$ todo polinômio mônico com grau n pode ser expresso em um produto de polinômios irredutíveis mônicos $\vee\ n = 0\}$. Temos que $0, 1 \in S$. Consideremos então $n > 1$. Suponhamos que $(\forall k < n : k \in S)$. Seja f um polinômio com grau n. Se f não pode ser decomposto em dois fatores a, b com $0 < deg(a), deg(b) < n$, então f em si é irredutível, é produto de um fator irredutível mônico e $f \in S$. Caso f possa ser decomposto em fatores a, b com $0 < deg(a), deg(b) < n$, como $(\forall k < n : k \in S)$, temos $deg(a), deg(b) \in S$. Como $deg(a), deg(b) > 0$, a, b são produtos como no enunciado. Logo, f é um produto de polinômios irredutíveis mônicos, e $n \in S$. Ou seja $S = \mathbb{N}$. E todo polinômio de grau ≥ 1 é um produto como no enunciado.

Para a unicidade, temos que um polinômio linear mônico pode ser expresso em um único produto como no enunciado, pois teremos apenas um fator linear (irredutível) mônico , e então $(x - a) = (x - b) \iff a = b$. Assim, supomos que um polinômio $f(x)$, com $deg(f(x)) = n$, possui duas fatorações, que podem ser diferentes à princípio, em etc.

$$f = p_1 \times ... \times p_v = q_1 \times ... \times q_w$$

Supomos que todo polinômio mônico de grau menor que n pode ser fatorado de maneira única, desconsiderando a ordem. Temos que $p_1 \mid q_1 \times ... \times q_w$ e assim $p_1 \mid q_i$ para algum $1 \leq i \leq w$. Sabemos que q_i é mônico e irredutível $p_1 = q_i$. Pelo cancelamento da multiplicação, uma vez que estamos em um domínio de integridade, temos $g = f/p_1 = f/q_i$. Mas g possui grau menor que f e portanto é escrito unicamente como no enunciado. Logo, $w = v$, e o produto da direita pode ser diferente apenas como permutação dos elementos da esquerda. Portanto, f admite fatoração única. Aplicamos a indução, e qualquer polinômio de grau arbitrário admite fatoração única. □

Pela fatoração única, concluímos que o número de divisores mônicos de um determinado polinômio é finito, obtidos por meio de todas as combinações possíveis de produto com os fatores mônicos irredutíveis. Temos apenas finitas combinações do tipo.

Terminamos abordando a aritmética modular com polinômios. As mesmas definições e propriedades são transferidas para este contexto de maneira razoável.

Definição 6.5. Seja um corpo K e sejam $f, g, h \in K[x]$, com $h \neq 0$. Então f **é congruente a** g **módulo** h, escrevemos $f \equiv g\ mod(h)$, caso $h \mid (f - g)$. Ou seja, caso f, g deixem o mesmo resto

na divisão euclidiana por h (falar no mesmo resto da divisão euclidiana exige que K seja um corpo, como feito no teorema da divisão euclidiana).

Temos que tal relação é de equivalência. As demonstrações são as mesmas (por estarmos em mesmo contexto de domínio de integridade e portanto foram omitidas.

Proposição 6.6 (Reflexividade)**.** *Para quaisquer $f, h \in K[x]$, com $h \neq 0$: $f \equiv f \ mod(h)$.*

Proposição 6.7 (Simetria)**.** *Para quaisquer $f, g, h \in K[x]$, com $h \neq 0$: $f \equiv g \ mod(h) \Rightarrow g \equiv f \ mod(h)$.*

Proposição 6.8 (Transitividade)**.** *Para quaisquer $e, f, g, h \in K[x]$, com $h \neq 0$: $e \equiv f \ mod(h)$ e $f \equiv g \ mod(h) \Rightarrow e \equiv g \ mod(h)$.*

Para a relação de congruência módulo h em polinômios também valem as compatibilidades e as demonstrações não diferem.

Proposição 6.9 (Compatibilidade $\equiv$ e adição - I)**.** *Para quaisquer $d, e, f, g, h \in K[x]$, com $h \neq 0$: $d \equiv e \ mod(h)$ e $f \equiv g \ mod(h) \Rightarrow d + f \equiv e + g \ mod(h)$.*

Proposição 6.10 (Compatibilidade $\equiv$ e adição - II)**.** *Para quaisquer $d, e, f, h \in K[x]$, com $h \neq 0$: $d \equiv e \ mod(h) \Rightarrow d + f \equiv e + f \ mod(h)$.*

Proposição 6.11 (Compatibilidade $\equiv$ e subtração - I)**.** *Para quaisquer $d, e, f, g, h \in K[x]$, com $h \neq 0$: $d \equiv e \ mod(h)$ e $f \equiv g \ mod(h) \Rightarrow d - f \equiv e - g \ mod(h)$.*

Proposição 6.12 (Compatibilidade $\equiv$ e subtração - II)**.** *Para quaisquer $d, e, f, h \in K[x]$, com $h \neq 0$: $d \equiv e \ mod(h) \Rightarrow d - f \equiv e - f \ mod(h)$.*

Proposição 6.13 (Compatibilidade $\equiv$ e produto - I)**.** *Para quaisquer $d, e, f, g, h \in K[x]$, com $h \neq 0$: $d \equiv e \ mod(h)$ e $f \equiv g \ mod(h) \Rightarrow df \equiv eg \ mod(h)$.*

Proposição 6.14 (Compatibilidade $\equiv$ e produto - II)**.** *Para quaisquer $d, e, f, h \in K[x]$, com $h \neq 0$: $d \equiv e \ mod(h) \Rightarrow df \equiv ef \ mod(h)$.*

Proposição 6.15 (Lei do cancelamento)**.** *Para quaisquer $d, e, f, h \in K[x]$, com $h \neq 0$: se $mdc(f, h) = 1$ então $df \equiv ef \ mod(h) \Rightarrow d \equiv e \ mod(h)$.*

Podemos considerar em $K[x]/h$, o anel de polinômios módulo h: as classes de equivalência de polinômios que deixam o mesmo resto na divisão por h. Definimos de forma semelhante a soma e o produto dessas classes de equivalência. Por fim apresentamos o resultado abaixo.

Teorema 6.5. *Seja um corpo K e $h \in K[x]$ um polinômio irredutível mônico. Então $K[x]/h$ é um corpo.*

Demonstração. Temos que o anel de polinômios módulo h é comutativo com unidade (não podemos ainda assegurar que seja domínio). Para que seja corpo, devemos ter $\overline{a} \neq \overline{0}$ inversível (estamos considerando os polinômios a não divisíveis por h). Como h é irredutível e mônico, podemos ter $mdc(a,h) = 1$ ou $mdc(a,h) = h$, mas esta última opção implica $\overline{a} \neq \overline{0}$. Logo, $am + hn = 1$ para determinados $m, n \in K[x]$. E portanto $am - 1 = -hn \Rightarrow am \equiv 1\ mod(h)$. Assim $\overline{a} \times \overline{m} = \overline{am} = \overline{1}$ e portanto $\overline{a}$ é invertível. □

Façamos um exemplo de corpo obtido dessa forma.

Exemplo 6.3. Consideremos o corpo $K = \mathbb{Z}/2$ e portanto $K[x]$ é o anel de polinômios com coeficientes em $\{\overline{0}, \overline{1}\}$. Dividindo tais polinômios por $p = \overline{1}x^2+\overline{1}x+\overline{1}$ (observamos que é irredutível, pois grau 2 e sem raízes em K), os restos possíveis podem ter grau $-\infty, 0, 1$, razoavelmente. Temos como opções de resto, portanto: $\overline{0}, \overline{1}, \overline{1}x, \overline{1}x+\overline{1}$. Logo, $K[x]/(\overline{1}x^2+\overline{1}x+\overline{1}) = \{\overline{0}, \overline{1}, \overline{x}, \overline{x+1}\}$, omitindo as sobrelinhas interiores. Dessa forma, temos um corpo pois: $(\overline{1}, \overline{0}, ...) \times (\overline{1}, \overline{0}, ...) = (\overline{1}, \overline{0}, ...)$; e $(\overline{0}, \overline{1}, \overline{0}, ...) \times (\overline{1}, \overline{1}, \overline{0}, ...) = (\overline{0}, \overline{1}, \overline{1}, 0, ...)$, com $(\overline{0}, \overline{1}, \overline{1}, 0, ...) = (\overline{1}, \overline{1}, \overline{1}, \overline{0}...) + (\overline{1}, \overline{0}, ...)$. Ou seja, o polinômio $\overline{1}x^2 + \overline{1}x$ dividido por $\overline{1}x^2 + \overline{1}x + \overline{1}$ deixa resto $\overline{1}$, e assim pertence à mesma classe de equivalência da unidade. Todos os elementos são inversíveis e portanto $K[x]/(\overline{1}x^2 + \overline{1}x + \overline{1})$ é corpo, como esperávamos.

Encerramos assim nosso estudo de polinômios, objetos com características próprias que devem ser investigadas com atenção. Os resultados apresentados são os mais relevantes para este trabalho e portanto passamos ao próximo assunto.

7 INTEIROS GAUSSIANOS

Continuamos agora investigando nosso último contexto análogo ao números inteiros. Nossa investigação é baseada em *The Gaussian Integers* (CONRAD, 2008). Inteiros Gaussianos é o conjunto $\mathbb{Z}_i = \{a + bi \mid a, b \in \mathbb{Z}\}$ munido com as operações usuais de adição e multiplicação. Aqui estamos assumindo o desenvolvimento dos números complexos e temos que $i^2 = -1$.

As propriedades aritméticas de que dispomos aqui são essencialmente as mesmas. Não é difícil provarmos que temos para a soma: associatividade, comutatividade, existência e unicidade do elemento neutro, existência e unicidade de elemento oposto, bem como cancelamento. Para o produto: associatividade, comutatividade, distributividade, existência e unicidade do elemento neutro, cancelamento e a propriedade de domínio.

Assim como no caso dos polinômios, iremos precisar de um parâmetro para falarmos em máximo divisor comum adiante, pois não temos uma relação de ordem nos gaussianos (complexos). Utilizaremos a norma (pertencente a $\mathbb{N}$). Esse será nosso comparativo, o qual poderemos usar para aplicar os Princípios de Indução, ou o Princípio do Bom Ordenamento, como foi feito anteriormente utilizando o grau.

Enquanto no âmbito dos inteiros pensávamos em números maiores ou menores que 0, nos gaussianos consideramos 4 quadrantes (no produto cartesiano, com um detalhe sobre os eixos), nos quais temos o caso de oposição, mas também estágios “intermediários” da oposição (pela multiplicação do fator i ou $-i$). Em vez de falar somente em positivos e negativos, na reta dos inteiros, agora seria conveniente pensarmos em 4 conjuntos específicos, que serão apresentados. Esses conjuntos são, de maneira semelhante ao caso de positivos e negativos, em certo sentido, “reflexos” um do outro.

Embora tenhamos o conjunto dos inteiros contido (imerso) nos conjunto dos gaussianos, temos de ter certo cuidado com a questão de imersão. Pois, por exemplo, 2 é *primo* em inteiros, porém $2 = (1 + i)(1 - i)$ não é primo nos gaussianos, como ficará melhor especificado adiante com a definição de “primo”.

Ademais, ressaltamos os seguintes pontos. A norma, que utilizaremos aqui para medir o tamanho dos números inteiros gaussianos, seria semelhante também ao módulo, no conjunto dos números inteiros: assume somente valores positivos, é multiplicativa, etc. Seguiremos agora estudando tal função de norma, divisibilidade, divisão euclidiana, máximo divisor comum, algoritmo de Euclides, Bachet-Bezout, primos, aritmética modular, etc.

Definição 7.1. Seja $\alpha = a + bi \in \mathbb{Z}_i$. Definimos sua norma como o produto de α e seu conjugado $\overline{\alpha}$. $N(\alpha) = \alpha\overline{\alpha} = (a + bi)(a - bi) = a^2 + b^2$.

Exemplo 7.1.

a) $N(1) = 1$

b) $N(1 + 2i) = 1^2 + 2^2 = 5$

c) $N(a) = a^2$, para qualquer inteiro a.

Observamos que não usamos a distância euclidiana para definir a norma de um número complexo, mas o quadrado da mesma. A razão disso é por querermos manipular números inteiros, e a norma definida assim será sempre um número natural, pois é soma de dois naturais. Com efeito, iremos relacionar a divisibilidade na norma com a divisibilidade em $\mathbb{Z}_i$, e isso nos será de grande ajuda. A seguinte proposição aborda a propriedade multiplicativa da norma.

Proposição 7.1 (Norma é multiplicativa)**.** *Para quaisquer* $\alpha, \beta \in \mathbb{Z}_i$*:* $N(\alpha\beta) = N(\alpha)N(\beta)$.

Demonstração. Seja $\alpha = a + bi$ e $\beta = c + di$. Temos $\alpha\beta = (ac - bd) + (ad + bc)i$. Assim, $N(\alpha\beta) = (ac - bd)^2 + (ad + bc)^2 = (a^2c^2 - 2abcd + b^2d^2) + (a^2d^2 + 2abcd + b^2c^2) = a^2(c^2 + d^2) + b^2(d^2 + c^2) = (a^2 + b^2)(c^2 + d^2) = N(\alpha)N(\beta)$. Portanto, $N(\alpha\beta) = N(\alpha)N(\beta)$. □

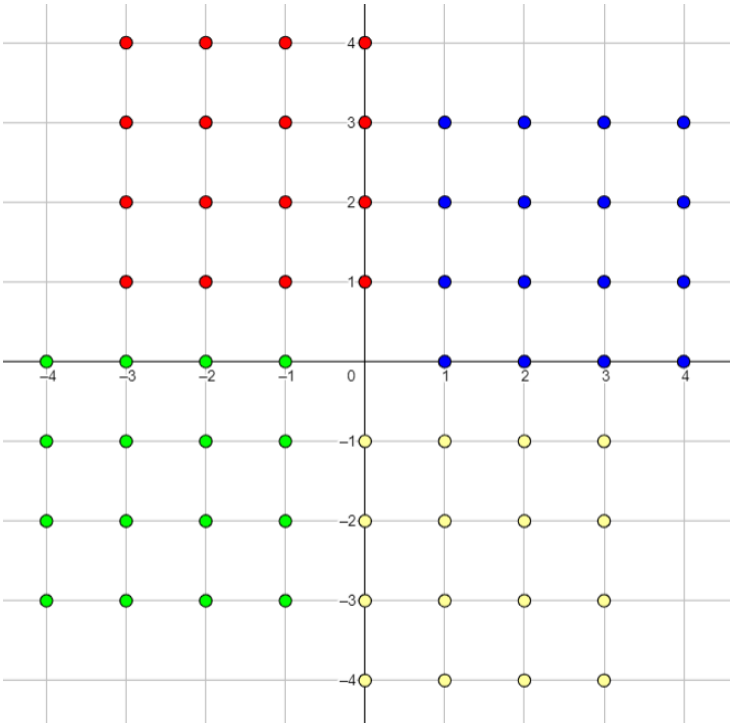
Os cálculos feitos anteriomente não precisaram supor $a, b, c, d \in \mathbb{Z}$. Os mesmos funcionam também para coeficientes reais. Uma primeira utilidade para essa proposição é encontrar quais são os elementos inversíveis em $\mathbb{Z}_i$. Nossa intuição diz que por lidarmos com coeficientes inteiros e por a norma ser multiplicativa, estamos limitados nesse aspecto. Esse é de fato o caso.

Proposição 7.2. *Os únicos gaussianos inversíveis são* ± 1 *e* $\pm i$.

Demonstração. De fato ± 1 e $\pm i$ são inversíveis. Por outro lado, se $\alpha \in \mathbb{Z}_i$ é inversível, então existe $\beta \in \mathbb{Z}_i$ tal que $\alpha\beta = 1$. Considerando a norma dos dois lados, $N(\alpha\beta) = N(\alpha)N(\beta) = 1$. Esta última equação por sua vez está nos inteiros e possui duas soluções. Mas como a norma não assume valores negativos, a nós importa apenas a solução positiva. Assim, $N(\alpha) = N(\beta) = 1$. Se $\alpha = a+bi$, então $N(\alpha) = a^2+b^2 = 1$. Portanto as soluções são $a = 0, b = \pm 1$ ou $a = \pm 1, b = 0$, ou seja, $\alpha = \pm 1$ ou $\alpha = \pm i$. □

Os elemento inversíveis de $\mathbb{Z}$ são ± 1, enquanto que os de $\mathbb{Z}_i$ são ± 1 e $\pm i$. Se por um lado podemos observar os inteiros tomando por base os positivos, multiplicados por um inversível (1 ou -1); por outro, também podemos compreender os elementos de $\mathbb{Z}_i$ tomando como base "o primeiro quadrante" ($a + bi$, com $a > 0$ e $b \geq 0$), multiplicados por um inversível. A Figura 3.1 ilustra como podemos obter os todos os pontos considerando o conjunto destacado em azul e multiplicando por 1, i, -1, $-i$.

Figura 7.1 – Quadrantes em Z_i.



Fonte: Elaborada pelo autor.

Passemos à divisibilidade em $\mathbb{Z}_i$, começando com a definição.

Definição 7.2. Sejam $a, b \in \mathbb{Z}_i$. Dizemos que b **divide** a, se existe $q \in \mathbb{Z}_i$ tal que $a = bq$.

Exemplo 7.2.

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

b) $i + 2i \mid 4 + 3i$, pois $2 = (1 + 2i)(2 - i)$

Para verificarmos se um inteiro gaussiano divide outro basta multiplicarmos o numerador e o denominador pelo conjugado do denominador. Consideramos então a parte real e a imaginária do resultado, e facilmente identificamos se tal número pertence a $\mathbb{Z}_i$.

Exemplo 7.3.

$$\frac{14 + 3i}{4 + 5i} = \frac{(14 + 3i)(4 - 5i)}{(4 + 5i)(4 - 5i)} = \frac{(56 + 15) + (12 - 70)i}{16 + 25} = \frac{71 - 58i}{41} = \frac{71}{41} - \frac{58i}{41}.$$

Certamente não temos a divisibilidade, pois o valor não está em $\mathbb{Z}_i$

A proposição seguinte trata da divisibilidade por um inteiro.

Proposição 7.3. *Sejam $a + bi \in \mathbb{Z}_i$ e $c \in \mathbb{Z} \subset \mathbb{Z}_i$. Então $c \mid a + bi$ se, e somente se, $c \mid a$ e $c \mid b$.*

Demonstração. Provamos por uma sucessão de equivalências. Se temos que $c \mid (a + bi)$, existe $(d + ei) \in \mathbb{Z}_i$ tal que $a + bi = c(d + ei) \iff a + bi = cd + cei \iff a = cd \wedge b = ce \iff c \mid a \wedge c \mid b$. □

Um aspecto que se mantém em $\mathbb{Z} \subset \mathbb{Z}_i$ é a divisibilidade (como já mencionamos, nem tudo é preservado, por exemplo o caso dos primos). Observamos que se a parte imaginária de α for zero, $c \mid \alpha$ nos complexos equivale a $c \mid \alpha$ nos inteiros. O teorema a seguir mostra a importância da multiplicatividade, que relaciona divisibilidade nos gaussianos com divisibilidade na norma.

Teorema 7.1. *Para quaisquer $\alpha\beta \in \mathbb{Z}_i$: se $\beta \mid \alpha$ no contexto dos inteiros gaussianos, então $N(\beta) \mid N(\alpha)$, no âmbito dos inteiros.*

Demonstração. Se $\beta \mid \alpha$, então existe $\theta \in \mathbb{Z}_i$ tal que $\alpha = \beta\theta$. Considerando a norma dos dois lados, $N(\alpha) = N(\beta\theta) = N(\beta)N(\theta)$. Mas isso significa que existe um inteiro a tal que $N(\alpha) = aN(\beta)$, ou seja, que $N(\beta) \mid N(\alpha)$ em $\mathbb{Z}$. □

O teorema 7.1 é interessante como uma maneira rápida para testar se um inteiro gaussiano pode dividir outro: a partir das normas de cada número considerado, se não houver divisibilidade entre as mesmas, não haverá entre os gaussianos respectivos. Portanto, a condição é necessária, mas não suficiente. Consideremos o exemplo 7.3, em que há divisibilidade entre as normas, pois $205 = 41 \times 5$, mas não entre os elementos, como foi desenvolvido. De todo modo, podemos sempre tentar realizar a divisão, como foi feito no mesmo exemplo, para verificar a divisibilidade.

Uma consideração a se fazer é que os múltiplos por inversíveis ($\alpha 1$, αi, $-\alpha$, e $-\alpha i$) de $\alpha \in \mathbb{Z}_i$ possuem a mesma norma. Mas a recíproca não se verifica. Não é verdade que $N(\alpha) = N(\beta) \Rightarrow \alpha = j\beta$ para algum j inversível. Consideremos por exemplo os números $1 + 2i$ e $1 - 2i$, de mesma norma, mas os múltiplos por inversíveis de $1 + 2i$ são $1 + 2i$, $-2 + i$, $-1 - 2i$, $2 - i$.

Não é difícil intuir tal fato considerando que os múltiplos por inversíveis são obtidos por rotações de 90^o na origem de vetor que representa um inteiro gaussiano; mas poderíamos tomar também reflexões na bissetriz dos quadrantes ímpares, que pode gerar outros de mesma norma. Assim, a norma faz equivaler um conjunto maior de elementos do que apenas os múltiplos por inversíveis.

O próximo assunto é a divisão euclidiana. Precisaremos retomar a divisão euclidiana nos números inteiros para continuarmos. Assim, provamos o teorema a seguir.

Teorema 7.2 (Divisão euclidiana modificada)**.** *Sejam $a, b \in \mathbb{Z}$, com $b \neq 0$. Então, existem $q, r \in \mathbb{Z}$, tais que $a = q \times b + r$ e $0 \leq |r| \leq |b|/2$.*

Demonstração. Pela divisão euclidiana, já obtemos q', r' tais que $a = bq' + r'$ e $0 \leq r' < |b|$. O múltiplo de b mais próximo de a não está a uma distância maior que $|b|/2$. Argumentamos.

Se $b > 0$ estamos tomando sempre q' o maior valor inteiro tal que $bq' \leq a$, ou seja, tal que $a - bq' \geq 0$. Consideramos então q' e $q' + 1$ como candidatos ao novo quociente q. Como

$$\begin{aligned}(a - bq') + (b(q' + 1) - a) = |b| : |b|/2 \leq (a - bq') < |b| \\ \Rightarrow |b| - |b|/2 \leq (a - bq') < |b| \\ \Rightarrow (|b| - (a - bq')) - |b|/2 \leq 0 < |b| - (a - bq') \\ \Rightarrow 0 < (b(q' + 1) - a) \leq |b|/2.\end{aligned}$$

Enquanto que

$$\begin{aligned}|b|/2 \leq (b(q' + 1) - a) < |b| \Rightarrow |b| - |b|/2 \leq (b(q' + 1) - a) < |b| \\ \Rightarrow (|b| - (b(q' + 1) - a)) - |b|/2 \leq 0 < |b| - (b(q' + 1) - a) \\ \Rightarrow 0 < (a - bq') \leq |b|/2.\end{aligned}$$

Por outro lado, se $b < 0$ estamos considerando sempre q' o menor valor inteiro tal que $bq' \leq a$, ou seja, tal que $a - bq' \geq 0$. Seja q' e $q' - 1$ como candidatos ao novo quociente q. Como

$$\begin{aligned}(a - bq') + (b(q' - 1) - a) = |b| : |b|/2 \leq (a - bq') < |b| \\ \Rightarrow |b| - |b|/2 \leq (a - bq') < |b| \\ \Rightarrow (|b| - (a - bq')) - |b|/2 \leq 0 < |b| - (a - bq') \\ \Rightarrow 0 < (b(q' - 1) - a) \leq |b|/2.\end{aligned}$$

Enquanto que

$$\begin{aligned}|b|/2 \leq (b(q' - 1) - a) < |b| \\ \Rightarrow |b| - |b|/2 \leq (b(q' - 1) - a) < |b| \\ \Rightarrow (|b| - (b(q' - 1) - a)) - |b|/2 \leq 0 < |b| - (b(q' - 1) - a) \\ \Rightarrow 0 < (a - bq') \leq |b|/2.\end{aligned}$$

Assim, $min\{|a - bq'|, |a - b(q' + 1)|\} \leq |b|/2$, quando $b > 0$. E $min\{|a - bq'|, |a - b(q' - 1)|\} \leq |b|/2$, quando $b < 0$. Em todo caso, é possível escolher q de modo a tornar a distância $|r| = |a - bq|$ de a a bq menor ou igual a $|b|/2$. □

Ressaltamos que agora não mais dispomos da unicidade em relação ao par (q, r), pois em determinados casos teremos $|r| = |b|/2$, o que implica $|a - bq'| = |a - b(q' + 1)|$ ou $|a - bq'| = |a - b(q' - 1)|$, a depender de b. Ou seja, a se situa no meio de dois múltiplos de b. Consequentemente, o teorema a seguir, de quociente e resto na divisão em $\mathbb{Z}_i$, também não nos fornece a unicidade, mas isso não será um problema. Mencionamos que, no cálculo de q, r em uma divisão entre inteiros gaussianos, precisamos tomar quociente com a aproximação ao

inteiro mais próximo, como feito no teorema anterior. Verificamos portanto o seguinte.

Teorema 7.3. *Para quaisquer $a, b \in \mathbb{Z}_i$, com $b \neq 0$: existem $q, r \in \mathbb{Z}_i$ tais que $a = bq + r$ e $N(r) \leq N(b)/2$, o que implica $N(r) < N(b)$.*

Demonstração. Sejam $a, b \in \mathbb{Z}_i$ com $b \neq 0$. Procedemos tentando efetuar a divisão inteira

$$\frac{a}{b} = \frac{a\overline{b}}{b\overline{b}} = \frac{a\overline{b}}{N(b)} = \frac{m+ni}{N(b)},$$

em que $a\overline{b} = m + ni$, para determinados $m, n \in \mathbb{Z}$. Utilizamos agora a divisão modificada de m, n por $N(b)$. Temos que existem $q_m, r_m, q_n, r_n \in \mathbb{Z}$ tais que $m = q_m N(b) + r_m$ e $n = q_n N(b) + r_n$, com $0 \leq |r_m|, |r_n| \leq N(b)/2$. Desse modo,

$$\frac{a}{b} = \frac{q_m N(b) + r_m + (q_n N(b) + r_n)i}{N(b)} = q_m + q_n i + \frac{r_m + r_n i}{N(b)}.$$

Logo,

$$a = b(q_m + q_n i) + b\frac{r_m + r_n i}{N(b)}.$$

Observamos que

$$b\frac{r_m + r_n i}{N(b)} = \frac{r_m + r_n i}{\overline{b}} = a - b(q_m + q_n i) \in \mathbb{Z}_i.$$

Consideramos $q = (q_m + q_n i)$ e $r = a - bq$. Basta verificarmos a propriedade de r. De fato, tomando as normas dos dois lados, $N(r) = N(a - bq) = (r_m^2 + r_n^2)/N(B)$. Usando as desigualdades, temos

$$\begin{aligned}
&r_m^2 \leq N^2(b)/4 \\
&r_n^2 \leq N^2(b)/4 \\
&r_m^2 + r_n^2 \leq N^2(b)/2 \Rightarrow \\
&r_m^2 + r_n^2/N(B) \leq N(b)/2
\end{aligned}$$

Logo, $N(r) \leq N(b)/2$. Com isso, estabelecemos a divisão euclidiana no contexto dos inteiros gaussianos. □

Façamos alguns exemplos para nos familiarizarmos com essa nova divisão. Primeiros efetuamos a operação em $\mathbb{Q}_i$ e então ajustamos coeficiente para inteiro mais próximo, tomamos a diferença como resto e conferimos a desigualdade com as normas.

Exemplo 7.4.

a) $(2+3i)/(2+2i) = (2+3i)(2-2i)/8 = (10+2i)/8 = 1,25+0,25i$. Assim, $(2+3i) = (2+2i)*1+i$. De fato $1 = N(i) \leq (1/2)N(2+2i) = 4$.

b) $(5+7i)/(2+2i) = (5+7i)(2-2i)/8 = (24+4i)/8 = 3+0,5i$. Assim, $(5+7i) = (2+2i)*3+(-1+i)$. De fato $2 = N(-1+i) \leq (1/2)N(2+2i) = 4$ ou $(5+7i) = (2+2i)*(3+i)+(1-i)$. De fato $2 = N(1-i) \leq (1/2)N(2+2i) = 4$. E exemplificamos como o quociente e o resto não são únicos.

Como ocorreu com os polinômios, podemos ter mais de um elemento com mesmo parâmetro (norma neste caso) dividindo outro. Por exemplo, sejam $a, b \in \mathbb{Z}_i$ tais que $b \mid a$. Então existe $q \in \mathbb{Z}_i$ tal que $a = bq = bi(-qi) = b(-1)(-q) = b(-i)(qi)$ e portanto $bi, b(-1), b(-i)$, de mesma norma, dividem a. Considerando-se isso, a definição de máximo divisor comum para inteiros gaussianos será semelhante a dos polinômios.

Se $a \in \mathbb{Z}_i$, $a \neq 0$, nenhum inteiro gaussiano b com $N(b) > N(a)$ divide a, pois $N(b) \nmid N(a)$. Assim, temos finitos divisores, e também podemos utilizar a norma como parâmetro para falarmos em máximos divisores comuns. Toda lista de divisores de um determinado inteiro gaussiano k é não vazia, pois $1, i, -1, -i \mid k$. Desse modo, podemos de fato sempre falar em máximo divisor comum entre dois gaussianos não ambos nulos. As considerações feitas justificam a definição a seguir.

Definição 7.3. Sejam $a, b \in \mathbb{Z}_i$, não sendo ambos nulos. Definimos um **máximo divisor comum** de a e b como um inteiro gaussiano de norma máxima que divide a e b.

Logo, se r, s são *mdc* entre a, b. $N(r) \geq N(s)$ e $N(s) \geq N(r)$. Portanto, $N(r) = N(s)$. Naturalmente, máximo divisor de apenas um gaussiano e terá norma = $N(e)$.

Como esperávamos, podemos aplicar o algoritmo de Euclides para encontrar um máximo divisor comum de $a, b \in \mathbb{Z}_i$.

Sejam $a_1, a_2 \in \mathbb{Z}_i$, não ambos nulos. Se $a_2 = 0$, temos $a_1 \neq 0$, e consideramos a_1 como um *mdc*. Se $a_1 = 0$ a situação é análoga. Supomos então que $a_1, a_2 \neq 0$ e que $N(a_1) \geq N(a_2)$, sem perda de generalidade. Podemos efetuar a divisão euclidiana de a_1 por a_2 e encontrar quociente q_1 e resto a_3 ($0 \leq N(a_3) < N(a_2)$) que satisfazem a expressão $a_1 = q_1 \times a_2 + a_3$. Se $a_3 = 0$, pegamos a_2 como um *mdc*. Caso contrário, efetuamos a divisão euclidiana de a_2 por a_3, ambos diferentes de 0, e encontramos quociente q_2 e resto a_4 ($0 \leq N(a_4) < N(a_3)$) que satisfazem a expressão $a_2 = q_2 \times a_3 + a_4$. Em geral, se $a_i, a_{i+1} \neq 0$, realizamos a divisão de a_i por a_{i+1} e encontramos quociente q_i e resto a_{i+2} ($0 \leq N(a_{i+2}) < N(a_{i+1})$) tais que $a_i = q_i \times a_{i+1} + a_{i+2}$.

Teorema 7.4 (Algoritmo de Euclides)**.** *Temos que os valores da sequência finita $N(a_n)$ sempre decrescem e o último termo deve ser* 0*. Nesse processo, se a_u é o último gaussiano diferente de* 0*, consideramos a_u como um mdc de a_1, a_2.*

Demonstração. Sejam $a, b \in \mathbb{Z}_i$. Temos, pela divisão euclidiana de a por b, que existem $q, r \in \mathbb{Z}_i$ tais que $a = bq + r$ e $0 \leq N(r) \leq (1/2)N(b) < N(b)$. Os divisores comuns a b e a também dividem r, mesmo para $r = 0$ (se u é divisor comum, $r = a - q \times b = x \times u - q \times (y \times u) = (x - q \times y) \times u$). Logo, dividem b e r. Por outro lado, os divisores comuns a b e r também dividem a, e portanto dividem b e a. Logo, o conjunto de divisores comuns de b e a e o

conjunto de divisores comuns de b e r é o mesmo. Então os elementos de maior norma são os mesmos. No algoritmo, isso ocorre para cada nova divisão efetuada e portanto o conjunto dos divisores comuns é preservado e junto são preservados os máximos divisores comuns. Caso o resto seja zero, um máximo divisor comum será o divisor (maior norma possível). Quando o resto se torna 0, um *mdc* fica evidente, sendo relativo aos dois elementos do início. □

Ao abordarmos *mdc*, procuramos um divisor cujo parâmetro comparativo seja máximo (existe aqui pelo PBO). Um fato que ainda precisamos argumentar, mas que é bem útil para entendermos a relação entre os divisores comuns é que estes sempre dividem um mdc. De modo que, isso nos indica que um *mdc* tem, de alguma forma, todos os divisores em sua composição. O fato a seguir nos será útil nesse sentido, e também para entender quais são todos os máximos divisores comuns. Passamos ao teorema de Bachet-Bezout, feita de forma análoga àquela dos polinômios.

Teorema 7.5 (Bachet-Bezout)**.** *Sejam $a, b \in \mathbb{Z}_i$ não ambos nulos. Então existem $m, n \in \mathbb{Z}_i$ tais que $am + bn = k$, para algum gaussiano k máximo divisor comum de a, b.*

Demonstração. Para encontrar tais m, n utilizamos o algoritmo de Euclides anterior. Se um dos elementos iniciais é nulo, o outro é um *mdc* e obtemos m, n sem dificuldade. Supomos então que $a, b \neq 0$ e $N(a) \geq N(b)$, sem perda de generalidade. Assim, do algoritmo, consideramos $a = a_1$, $b = a_2$. Supomos a_u o último elemento não nulo da sequência de inteiros gaussianos obtida com o algoritmo, e tomamos $k = a_u$.

$$
\begin{aligned}
a_1 &= q_1 \times a_2 + a_3 \\
a_2 &= q_2 \times a_3 + a_4 \\
a_3 &= q_3 \times a_4 + a_5 \\
&\vdots \\
a_{u-2} &= q_{u-2} \times a_{u-1} + a_u \\
a_{u-1} &= q_{u-1} \times a_u + 0
\end{aligned}
$$

O elemento a_3 da primeira equação é uma combinação $\mathbb{Z}_i$-linear de a_1, a_2, bem como $a_2 = 0a_1 + a_2$. A cada nova equação, consideramos o segundo e o terceiro elementos da anterior, expressos como combinação $\mathbb{Z}_i$-linear de a_1, a_2, e substituímos na atual, encontrando a expressão deste terceiro elemento como combinação $\mathbb{Z}_i$-linear de a_1, a_2. Fazemos isso até a penúltima equação e obtemos a expressão de $a_u = k$ (um *mdc*) como combinação $\mathbb{Z}_i$-linear de a_1, a_2. □

Já temos condições de descobrir quais são todos os máximos divisores comuns relativos a dois gaussianos a, b. Observamos que, pela expressão de Bachet-Bezout, todo divisor comum a b e a também divide k. Ou seja, todo divisor comum divide o máximo obtido aqui. Ocorre então que se p também é um *mdc*, $N(p) = N(k)$ e $k = pq$, para algum $q \in \mathbb{Z}_i$. Temos assim

que $N(k) = N(pq) = N(p)N(q) \Rightarrow N(q) = 1$. Temos $q = 1, i, -1, -i$. Portanto, todos os *mdc*'s são obtidos multiplicando-se um dos pelos inversíveis de $\mathbb{Z}_i$. Ademais, multiplicando a equação de Bachet-Bezout pelos inversíveis, obtemos as combinações $\mathbb{Z}_i$-lineares para todos máximos divisores comuns. Mas naturalmente, não podemos ter a equação para um inteiro gaussiano de norma menor que a máxima; caso contrário, como *mdc* deve dividir todas combinações, dividiria um elemento com norma menor, impossível.

Ao calcularmos um *mdc* de dois gaussianos a, b (i e 1, por exemplo) pode ocorrer de obtermos 1 (ou $i, -1, -i$). Desse modo, os máximos divisores comuns serão $1, i, -1, -i$, de norma = 1. Se esse for o caso, diremos que a, b são **primos entre si**, ou **coprimos**. Segue o resultado abaixo.

Proposição 7.4. *Para quaisquer $a, b \in \mathbb{Z}_i$, não ambos nulos: existem $m, n \in \mathbb{Z}_i$ tais que $am + bn = 1$ se e somente se a, b são primos entre si.*

Demonstração. Se são primos entre si, os *mdc*'s são $1, i, -1, -i$, e portanto temos a relação de Bachet-Bezout. Por outro lado, se $am + bn = 1$, para determinados $m, n \in \mathbb{Z}_i$, a norma dos divisores comuns é 1. Logo, os máximos só podem ser os inversíveis. □

Seguem os resultados análogos, consequências do teorema de Bachet-Bezout.

Teorema 7.6 (Lema de Euclides)**.** *Para quaisquer $a, b, c \in \mathbb{Z}_i$: se a, b são coprimos e $a \mid bc$, então $a \mid c$.*

Demonstração. Se a, b são coprimos, existem $m, n \in \mathbb{Z}_i$ tais que $am+bn = 1$. Assim, $cam+cbn = c$. Como $a \mid ca$ e $a \mid cb$, a divide o membro do lado esquerdo da equação. Portanto, $a \mid c$. □

Proposição 7.5. *Para quaisquer $a, b, c \in \mathbb{Z}_i$: se $a, b \mid c$ e a, b são coprimos, então $ab \mid c$.*

Demonstração. Se $a \mid c$, então $c = aq_1$ para algum $q_1 \in \mathbb{Z}_i$. Como a, b são coprimos, e $b \mid aq_1$, temos que $b \mid q_1$. Assim $q_1 = bq_2$, para algum $q_2 \in \mathbb{Z}_i$. Portanto, $c = abq_2$, e $ab \mid c$. □

Proposição 7.6. *Para quaisquer $a, b, c \in \mathbb{Z}_i$: a, c são coprimos e b, c são coprimos se, e somente se, ab, c são coprimos.*

Demonstração. [$\Rightarrow$] Se ab, c são coprimos, então $abm + cn = 1$ para determinados $m, n \in \mathbb{Z}_i$. E a equação já nos indica a, c coprimos e b, c coprimos.

[$\Leftarrow$] Se a, c coprimos e b, c coprimos $av + cw = 1$, $bv' + cw' = 1$. Multiplicando lado a lado: $abvv' + c(w'av + wbv' + cww') = 1$, e temos que ab, c são coprimos. □

Provamos mais fatos que havíamos feito para inteiros. Vamos assim à definição de primos neste contexto. Primeiro, apenas registramos formalmente algo que já consideramos antes.

Proposição 7.7. *Para quaisquer $a \in \mathbb{Z}_i$, com $a \neq 0$, os divisores de a com norma = 1 são os inversíveis, e com norma = $N(a)$ são os múltiplos por inversíveis de a.*

Demonstração. Se $N(b) = 1$, então $b \mid a$ e é um inversível. Por outro lado, se $b \mid a$ e $N(b) = N(a)$, então $a = bq$, para algum $q \in \mathbb{Z}_i$. $N(a) = N(bq) = N(b)N(q) \Rightarrow N(q) = 1$. E b é um múltiplo de a por inversível. □

Lembramos a consideração que já fizemos que existem mais elementos de norma = $N(a)$, que não são os múltiplos de a por inversíveis. Mas esses não dividem a, pela contra-positiva da proposição 7.7. Passamos à definição de primos em $\mathbb{Z}_i$.

Definição 7.4. Denominamos um número $p \in \mathbb{Z}_i$ **primo**, se $N(p) > 1$ e para todo $a \in \mathbb{Z}_i$: $a \mid p \Rightarrow N(a) = 1 \ \vee \ N(a) = N(p)$. Ou seja, caso p não possa ser decomposto em $v, w \in \mathbb{Z}_i$, com $1 < N(v), N(w) < N(p)$

Sejam $a, b, c \in \mathbb{Z}_i$. Chamamos a decomposição $c = ab$, com $1 < N(a), N(b) < N(p)$, de **fatoração não trivial** (**fatoração trivial**: $N(a) = 1$ ou $N(a) = N(c)$). Um primo, portanto, admite apenas fatoração trivial.

Embora nem todo primo em $\mathbb{Z}$ seja primo em $\mathbb{Z}_i$, temos uma condição suficiente muito útil para garantir a primalidade nos inteiros gaussianos.

Teorema 7.7. *Para qualquer $p \in \mathbb{Z}_i$: se $N(p)$ é primo em $\mathbb{Z}$, então p é primo em $\mathbb{Z}_i$.*

Demonstração. Seja $p \in \mathbb{Z}_i$ tal que $N(p)$ é primo em $\mathbb{Z}$. Sejam $a, b \in \mathbb{Z}_i$ tais que $p = ab$. Então $N(p) = N(a)N(b)$. Como $N(p)$ é primo, $N(a) = 1$ ou $N(a) = N(p)$, o que significa que p é primo em $\mathbb{Z}_i$. □

A recíproca não é verdadeira. Por exemplo, 3 é primo em $\mathbb{Z}_i$, mas sua norma não é primo em $\mathbb{Z}$.

Exemplo 7.5. 3 é primo em $\mathbb{Z}_i$. Suponhamos que não fosse. Então teríamos $a, b \in \mathbb{Z}_i$ tais que $ab = 3 \Rightarrow N(a)N(b) = 9$. Como $N(a), N(b)$ devem ser diferentes de 1, só nos resta $N(a) = N(b) = 3$. Escrevendo $a = m + ni$, temos $m^2 + n^2 = 3$, mas tal equação não tem solução nos inteiros.

Sejam $a, p \in \mathbb{Z}_i$, com p primo. Os únicos divisores de p tem norma 1 ou $N(p)$. Logo, se h é um *mdc* de a, p, então $N(h) = 1$ ou $N(h) = N(p)$. Passamos a seguinte proposição familiar.

Proposição 7.8. *Seja $p \in \mathbb{Z}_i$ primo e sejam $a_1, a_2, ..., a_m \in \mathbb{Z}_i$. Se $p \mid a_1 \times a_2 \times ... \times a_m$, então $p \mid a_i$, para algum $i \in \{1, 2, ..., m\}$.*

Demonstração. Consideramos primeiro o produto $a_1 \times a_2$ e supomos que $p \mid a_1 \times a_2$. Se $p \mid a_1$, o enunciado é satisfeito. Se $p \nmid a_1$, nenhum múltiplo de p por inversível divide a, e os únicos divisores comuns entre ambos têm norma 1, e portanto p, a são coprimos. Do lema de Euclides, $p \mid a_2$. Para o caso com m termos, podemos aplicar uma Indução Finita e obter o resultado. □

Passamos assim à fatoração dos inteiros gaussianos em primos.

Teorema 7.8 (Fatoração Única)**.** *Todo $a \in \mathbb{Z}_i$, com $N(a) > 1$ pode ser fatorado em um produto de primos em $\mathbb{Z}_i$. Ademais, a fatoração é única no sentido que: se $a = p_1 ... p_r = q_1 ... q_s$ (com p_i, q_j primos para i, j possíveis), então $r = s$ e todo q_j é um múltiplo por inversível de algum p_i.*

Demonstração. Como esperado, iremos realizar a indução completa na norma para provarmos o teorema. Seja $S = \{n \in \mathbb{N} \mid$ todo inteiro gaussiano com norma n pode ser expresso em um produto de primos em $\mathbb{Z}_i \ \vee n = 0 \ \vee \ n = 1\}$. Temos que $0, 1 \in S$. Também, $2 \in S$, pois a norma é um primo. Consideremos então $n > 2$. Suponhamos que $(\forall k < n : k \in S)$. E seja $a \in \mathbb{Z}_i$ com $N(a) = n$. Se a não pode ser decomposto em dois fatores b, c com $1 < N(b), N(c) < n$, então a em si é primo, é produto de um fator primo e $n \in S$. Caso a possa ser decomposto em fatores b, c com $1 < N(b), N(c) < n$, como $(\forall k < n : k \in S)$, temos $N(b), N(c) \in S$. Como $N(b), N(c) > 1$, b, c são produtos como no enunciado. Logo, $a = bc$ é um produto de primos, e $n \in S$. Ou seja, $S = \mathbb{N}$. Logo, todo inteiro gaussiano de noma ≥ 2 é um produto como no enunciado.

Para a unicidade, temos no caso base que todo inteiro gaussiano de norma igual a 2 é primo e portanto expresso de forma única, no sentido em questão. Assim, consideramos $n \geq 3$ e supomos que todo inteiro gaussiano g com $1 < N(g) < n$ é expresso unicamente como no enunciado. Seja $a \in \mathbb{Z}_i$ com $N(a) = n$. Se não tivermos inteiros gaussianos com norma $= n$ (nem todo natural é a soma de dois quadrados), não temos o que provar. Podemos supor então que existam gaussianos com norma $= n$. Assim, consideramos duas fatorações possíveis a princípio (que podem ser "iguais"): $a = p_1...p_r = q_1...q_s$. Temos que $p_1 \mid a$, logo $p_1 \mid q_j$, para algum j. Sem perda de generalidade, podemos supor $j = 1$, por uma questão de reordenamento. Como q_1 em si é primo, $q_1 = up_1$, para algum inversível u. Podemos cancelar p_1, e ficamos com $a/p_1 = p_2...p_r = uq_2...q_s = q_2'...q_s$. Obtemos um inteiro gaussiano de norma menor que n. Portanto, $s = r$, $q_j = v_j p_i$, e temos a fatoração única no sentido em questão para um inteiro gaussiano a qualquer de norma $= n$. Portanto, temos fatoração única para qualquer elemento de $\mathbb{Z}_i$. □

Temos facilmente a infinitude de primos em $\mathbb{Z}_i$ decorrendo da infinitude primos (normas) em $\mathbb{N}$. E por fim abordamos a aritmética modular em $\mathbb{Z}_i$. Começamos com a definição.

Definição 7.5. Sejam $a, b, c \in \mathbb{Z}_i$, com $c \neq 0$. Então a **é congruente a** b **módulo** c, escrevemos $a \equiv b \ mod(c)$, caso $c \mid (a - b)$.

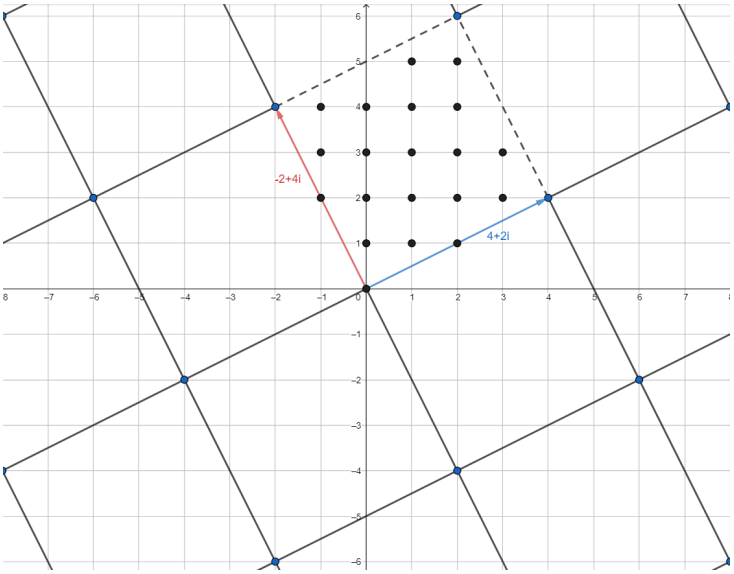
Como $\mathbb{Z}_i$ é um domínio de integridade, as propriedades de aritmética modular e as demonstrações são as mesmas. A relação se comporta bem para soma, diferença, produto, etc. Congruência módulo 0 significaria $a = b$, pois 0 divide apenas ele mesmo, então ignoramos esse caso.

Uma dúvida que surge é a respeito da não unicidade de quociente e resto. O que acontece nesses casos? Se $a = cq + r$ e $a = cq' + r'$, com $N(r), N(r') < N(c)$ ocorre que $cq+r = cq'+r' \Rightarrow r-r' = c(q'-q) \Rightarrow r \equiv r' \ mod(c)$. No caso dos inteiros, esta última congruência

iria implicar $r = r'$. Mas no caso dos inteiros gaussianos isso não se verifica. Consideremos por exemplo $1 \equiv -i \ mod(1+i)$. Com efeito se $a = cq + r$ e $b = cq' + r$, independentemente de outras igualdades, $a - cq = b - cq' \Rightarrow a - b = c(q - q') \Rightarrow a \equiv b \ mod(c)$. Ou seja, se temos pelo menos uma igualdade de resto, teremos a congruência. Mas não podemos afirmar que a congruência implica na igualdade de restos, razoavelmente, pois há mais possibilidades.

Vamos abordar agora uma maneira intuitiva de se compreender a congruência módulo $c = m + ni$ em $\mathbb{Z}_i$. Para isso, pensemos nos múltiplos gaussianos de c. $(m + ni)(v + wi) = v(m+ni) + w(-n+mi)$. Assim, podemos interpretar tais múltiplos como uma combinação $\mathbb{Z}$-linear de c e ci, este de mesmo módulo e perpendicular a c. Considerando essas combinações, estamos ladrilhando o plano com quadrados. Essas células nos ajudam a encontrar todas as diferentes classes de congruência módulo c. Para facilitar um pouco o trabalho com os conceitos, consideremos por exemplo $c = 4 + 2i$, cujos múltiplos são $m(4 + 2i) + n(-2 + 4i)$. Graficamente

Figura 7.2 – Exemplo $c = 4 + 2i$.



Fonte: Elaborado pelo autor.

Seja $b \in \mathbb{Z}_i$. Elementos congruentes a b módulo c podem ser obtidos ao nos deslocarmos (com o passo do módulo) nas direções dos vetores $(4 + 2i), (-2 + 4i)$. Observamos a célula quadrada de vértices $0, c, ci, c+ci$. Nesta célula, consideramos os *elementos internos*. Tomemos os pontos $A = 0 + c$ e $B = 0 + ci$. Os elementos internos da célula são os inteiros gaussianos que não estão sobre os segmentos orientados $A + ci$ ou $B + c$.

Nenhum dos internos é congruente a outro. Pois a diferença em qualquer par terá módulo $0 < N < N(c)$, e assim não é divisível por c. Ademais, se y é um interno, $y + kc + lci \equiv y \ mod(c)$, para quaisquer $k, l \in \mathbb{Z}$. Ou seja, elementos na mesma posição relativa das células são congruentes. Por outro lado, os internos representam todas as classes de equivalência, pois

cada elemento do plano é congruente a outro de norma menor que $N(c)$, o que compreende todas as posições relativas da célula.

Assim, utilizaremos os internos como um sistema completo de representantes de classes de equivalência módulo c, para qualquer $c \in \mathbb{Z}_i$, $c \neq 0$. Estudamos mais propriedades importantes da aritmética modular.

Proposição 7.9. *Seja $p \in \mathbb{Z}_i$, com p no mesmo contexto. E sejam $a, b \in \mathbb{Z}_i$ tais que $ab \equiv 0\ mod(p)$. Então $a \equiv 0\ mod(p)$ ou $b \equiv 0\ mod(p)$.*

Demonstração. Se $ab \equiv 0\ mod(p)$, por definição $p \mid ab$. Como p é primo, p divide um dos elementos, como foi provado no Lema de Euclides. □

Obtemos também o seguinte resultado feito nos inteiros.

Teorema 7.9. *Para quaisquer $a, b \in \mathbb{Z}_i$, com $b \neq 0$: $ax \equiv 1 mod(b)$ tem solução se, e somente se, a, b são primos entre si em $\mathbb{Z}_i$.*

Demonstração. A demonstração é a mesma sucessão de equivalências. Existe x tal que $ax \equiv 1\ mod(b) \Leftrightarrow$ existe x tal que $b \mid ax - 1 \Leftrightarrow$ existe x tal que existe y tal que $ax - 1 = yb \Leftrightarrow$ existem x, y tais que $ax - by = 1 \Leftrightarrow a, b$ são primos entre si. □

O fato a seguir não foi demonstrado nos contextos anteriores, e utiliza um resultado da álgebra.

Proposição 7.10. *Seja $p \in \mathbb{Z}_i$, com p primo gaussiano. Então, todo $a \in \mathbb{Z}_i$, $a \not\equiv 0\ mod(p)$, tem inverso multiplicativo módulo p, e qualquer congruência polinomial*

$$c_n x^n + c_{n-1} x^{n-1} + ... + c_1 x + c_0 \equiv 0\ mod(p)$$

em que $c_i \in \mathbb{Z}_i$, e $c_n \not\equiv 0\ mod(p)$, tem no máximo n soluções módulo p.

Demonstração. Temos que todo $a \in \mathbb{Z}_i$ não múltiplo de p é coprimo com este e, pelo teorema 7.9, tem inverso multiplicativo. Logo, $\mathbb{Z}_i/p$ é um corpo. O corolário segue do fato que um polinômio não têm mais raízes do que seu grau, no corpo em que está definido. □

Devemos ter uma preocupação para quais fatos permanecem de $\mathbb{Z}$ para $\mathbb{Z}_i$ (vice-versa), e quais se alteram. Pois, como já abordamos, os primos em $\mathbb{Z}$ nem sempre são primos em $\mathbb{Z}_i$. A relação de congruência módulo, por sua vez, não se altera do seguinte modo. Para quaisquer inteiros a, b, c: $a \equiv b\ mod(c)$ em $\mathbb{Z}$, se e somente se $a \equiv b\ mod(c)$ em $\mathbb{Z}_i$. Isso significa que quando $c \mid a - b$ em $\mathbb{Z}$, $c \mid a - b$ em $\mathbb{Z}_i$, razoavelmente. Por outro lado, quando $c \mid a - b$ em $\mathbb{Z}_i$, também temos $c \mid a - b$ em $\mathbb{Z}$. Esperamos que o quociente não seja complexo, caso contrário $a - b$ seria complexo. Logo, a propriedade se transfere sem dificuldades de $\mathbb{Z}_i$ para $\mathbb{Z}$.

Iremos agora tratar de mais dois assuntos para completar a comparação de inteiros gaussianos e inteiros. Vamos abordar a função ϕ de Euler e o pequeno teorema de Fermat. Mas

antes precisamos ter uma ideia de como calcular o número de classes de equivalência módulo $a \in \mathbb{Z}_i$, que denotamos por $n(a)$. Vamos a essa investigação, portanto; começando com o cálculo no caso de inteiros (contamos as diferentes classes de equivalência em $\mathbb{Z}_i$ de um inteiro).

Proposição 7.11. *Para qualquer $a \in \mathbb{Z}$, com $a \neq 0$: $n(a) = N(a) = a^2$.*

Demonstração. Seja um inteiro a. Já sabemos que os elementos internos na célula dos vetores a e ai formam um sistema completo de representantes módulo a. Portanto, temos a^2 (o número de quadrados na célula, sendo o mesmo que o número de pontos) diferentes classes de equivalência módulo a. Ou seja, $n(a) = N(a)$. □

Consideremos também o seguinte.

Proposição 7.12. *Para qualquer $a \in \mathbb{Z}_i$, com $a \neq 0$: $n(a) = n(\overline{a})$.*

Demonstração. Apenas observamos que (para $x, y \in \mathbb{Z}_i$): $x \equiv y \ mod(a) \iff a \mid (x-y) \iff x - y = qa \iff \overline{x-y} = \overline{qa} \iff \overline{x} - \overline{y} = \overline{q} \times \overline{a} \iff \overline{a} \mid \overline{x} - \overline{y} \iff \overline{x} \equiv \overline{y} \ mod(\overline{a})$. Dessa forma, cada diferente classe de equivalência módulo a corresponde a uma diferente classe de equivalência módulo $\overline{a}$, e reciprocamente. Ficamos com $n(a) \leq n(\overline{a})$ e $n(\overline{a}) \leq n(a)$, e portanto $n(a) = n(\overline{a})$. □

Temos também que a função n é multiplicativa.

Proposição 7.13. *Para quaisquer $a, b \in \mathbb{Z}_i$, $a, b \neq 0$. $n(ab) = n(a)n(b)$.*

Demonstração. Seja $\{m_1, ..., m_r\}$ um sistema completo de representantes módulo a; e $\{n_1, ..., n_s\}$ um sistema completo de representantes módulo b (naturalmente, $r = n(a)$, e $s = n(b)$). Seja então $c \in \mathbb{Z}_i$. Temos $c \equiv m_i \ mod(a)$ para determinado i, com $1 \leq i \leq r$. Assim, $c - m_i = ad$, para algum $d \in \mathbb{Z}_i$. Ao mesmo tempo, $d \equiv n_j \ mod(b)$, para determinado j, com $1 \leq j \leq s$, ou seja $d = bq + n_j$, para algum $q \in \mathbb{Z}_i$. Ficamos com $c = m_i + an_j + abq \equiv m_i + an_j \ mod(ab)$. Assim, todo inteiro gaussiano é equivalente a uma expressão do tipo. Temos $n(a) \times n(b)$ classes de equivalência possíveis. De fato são todas diferentes, pois supondo $m_{i'} + an_{j'} \equiv m_i + an_j \ mod(ab)$, devemos ter $(m_{i'} + an_{j'}) - (m_i + an_j) = abk \Rightarrow (m_{i'} - m_i) + a(n_{j'} - n_j) = aw \Rightarrow m_{i'} \equiv m_i \ mod(a) \Rightarrow i = i'$. Assim, $(m_{i'} - m_i) + a(n_{j'} - n_j) = abk \Rightarrow a(n_{j'} - n_j) = abk \Rightarrow (n_{j'} - n_j) = bk \Rightarrow n_{j'} \equiv n_j \ mod(b) \Rightarrow j = j'$. Portanto temos $n(a)n(b)$ classes de equivalência módulo ab. □

Por fim, com os três últimos fatos podemos demonstrar o resultado que pretendemos.

Teorema 7.10. *Para qualquer $a \in \mathbb{Z}_i$, com $a \neq 0$: $n(a) = N(a)$.*

Demonstração. Seja $a \in \mathbb{Z}_i$, com $a \neq 0$. A norma de a é um inteiro positivo. Logo, temos que $n(N(a)) = N^2(a)$. Ao mesmo tempo, $n(N(a)) = n(a\overline{a}) = n(a)n(\overline{a}) = n^2(a)$. Desse modo, $n^2(a) = N^2(a)$ e como ambas funções são positivas $n(a) = N(a)$. □

De forma semelhante, consideramos o anel de inteiros gaussianos módulo $a \in \mathbb{Z}_i$, o qual denotamos por $\mathbb{Z}_i/a$. Denotamos por $(\mathbb{Z}_i/a)^\times$ o subconjunto formado pelos elementos inversíveis de $\mathbb{Z}_i/a$. Se todos os elementos forem inversíveis, estamos em um corpo. A função ϕ de Euler é utilizada para contar o número de elementos inversíveis. Relembramos a definição.

Definição 7.6. Definimos a função ϕ de Euler da seguinte forma.

$$\phi(a) = |(\mathbb{Z}_i/a)^\times|.$$

Sabemos o número de inversíveis quando estamos em um anel de inteiros gaussianos módulo primo. Seja $p \in \mathbb{Z}_i$, com p primo em $\mathbb{Z}_i$. Assim, $\phi(p) = N(p) - 1$. Ademais, calculamos $\phi(p^k)$, tomando todos os elementos e retirando aqueles que são divisíveis por p. Com efeito, $n(p^k) = N(p^k) = N^k(p)$. Por outro lado, na célula de p^k teremos $N^{k-1}(p) = N^k(p)/N(p)$ mini-células, e em cada uma teremos um número divisível por p. Por que isso? Do mesmo modo que é possível pegar todos os representantes de classe naquela célula do vetor e seu ortogonal, podemos pegar os complexos da célula p e multiplicar cada um por valor conveniente $(1, i, -i, -1)$ que os colocará na célula p^k. Assim, temos novas mini-células p dentro da célula p^k. Em cada mini-célula temos apenas 1 múltiplo de p. O teorema seguinte adapta aquele feito nos inteiros e constata que a função ϕ é multiplicativa.

Proposição 7.14. *Para quaisquer $v, w \in \mathbb{Z}_i$: v, w coprimos $\Rightarrow \phi(vw) = \phi(v) \times \phi(w)$.*

Demonstração. Seja $\{m_1 = 1, ..., m_r = v\}$ um sistema completo de representantes módulo v; e $\{n_1 = 1, ..., n_s = w\}$ um sistema completo de representantes módulo w. Seja a matriz com a seguinte lei de formação $c_{ij} = n_j v + m_i$, com $1 \leq i \leq r = N(v)$ e $1 \leq j \leq s = N(w)$.

$$\begin{bmatrix} 1v+1 & 1v+m_2 & ... & 1v+v \\ n_2v+1 & n_2v+m_2 & ... & n_2v+v \\ \vdots & \vdots & \ddots & \vdots \\ wv+1 & wv+m_2 & ... & wv+v \end{bmatrix}$$

Denotemos o conjunto de máximos divisores comuns de $a, b \in \mathbb{Z}_i$ por $mdc(a, b)$. Observamos que $mdc(n_j v + m_i, v) = mdc(m_i, v)$, pois os conjuntos de divisores são iguais. Então ocorre que se apenas um número, denotado por $n_j v + m_i$, em uma das colunas é primo com v, teremos $mdc(n_j v + m_i, v) = mdc(m_i, v) = \{1, i, -1, -i\}$ e então $mdc(n_k v + m_i, v) = mdc(m_i, v) = \{1, i, -1, -i\}$ e qualquer outro número da mesma coluna será primo com v. Observando a primeira linha, podemos perceber que temos $\phi(v)$ colunas de elementos primos com v. Em contrapartida, em cada coluna (de primos com v ou não) devemos ter um conjunto completo de representantes de classe módulo w, e portanto devemos ter em cada coluna $\phi(w)$ elementos primos com w. Teremos todos os representantes de classe pois, por exemplo, considerando dois elementos da coluna m_i, temos $n_j v + m_i \equiv n_{j'} v + m_i \ mod(w) \Rightarrow n_j v + m_i - m_i \equiv n_{j'} v + m_i - m_i \ mod(w) \Rightarrow n_j v \equiv n_{j'} v \ mod(w) \Rightarrow n_j \equiv n_{j'} \ mod(w) \Rightarrow j = j'$, sendo o cancelamento pois v, w são coprimos.

Assim, em cada uma de $\phi(v)$ colunas de primos com v teremos $\phi(w)$ elementos que também serão primos com w e portanto primos com vw. Lembrando que se w, k são coprimos e v, k são coprimos, temos que wv, k são relativamente primos, pela proposição 7.6. A quantidade de números primos com vw portanto é $\phi(vw) = \phi(v)\phi(w)$. □

Por fim, temos o pequeno teorema de Fermat.

Teorema 7.11 (Pequeno Teorema de Fermat)**.** *Para quaisquer $a, p \in \mathbb{Z}_i$, com p inteiro gaussiano primo: se $a \not\equiv 0\ mod(p)$, então $a^{N(p)-1} \equiv 1\ mod(p)$.*

Demonstração. Seja $\{m_1, ..., m_r = p\}$ ($r = n(p) = N(p)$) um sistema completo de representantes módulo p e $\{m_1, ..., m_{r-1}\}$ um sistema completo de inversíveis módulo p. Como a é inversível módulo p, $am_1, ..., am_{r-1}$ é um sistema completo de inversíveis módulo p ($am_f \equiv am_g\ mod(p) \Rightarrow m_f \equiv m_g\ mod(p) \Rightarrow f = g$). Logo, devemos ter cada am_i congruente a um m_j. Multiplicando lado a lado ficamos com $m_1...m_{r-1} \equiv am_1...am_{r-1} = a^{r-1}m_1...m_{r-1}\ mod(p)$. Como cada m_k é inversível módulo p, cancelamos obtendo $a^{r-1} \equiv 1\ mod(p)$. Portanto, $a^{N(p)-1} \equiv 1\ mod(p)$. □

8 CONSIDERAÇÕES FINAIS

Esperamos ter abordado os diversos sistemas, com suas regras e características particulares, de maneira satisfatória para oferecer entendimento e familiaridade tanto com os fatos como com as técnicas. Destacamos como uma análise cuidadosa e simples pode oferecer um potencial didático, bem como uma satisfação ao estudarmos/explorarmos um assunto e sentirmos que não deixamos muitos detalhes incompletos.

REFERÊNCIAS

BATISTA, P. H. **A Teoria Elementar dos Inteiros de Gauss**. Dissertação (Mestrado Profissional em Rede Nacional) — Universidade Federal de Goiás, Instituto de Matemática e Estatística (IME), Goiânia●, 2019. Citado na página 8.

CONRAD, K. The gaussian integers. 2008. Disponível em: <https://kconrad.math.uconn.edu/blurbs/ugradnumthy/Zinotes.pdf>. Acesso em: 10 nov. 2021. Citado na página 73.

HALMOS, P. R. **Naive Set Theory**. New York: Springer Science Business Media, 1998. (Undergraduate Texts in Mathematics). Citado 2 vezes nas páginas 8 e 9.

KUMAR, N. The construction of number systems. 2011. Disponível em: <https://www.math.wustl.edu/~kumar/courses/310-2011/Peano.pdf>. Acesso em: 10 nov. 2021. Citado na página 14.

MARTINEZ, F. E. B. et al. **Teoria dos Números: um Passeio com Primos e Outros Números Familiares pelo Mundo Inteiro**. 3. ed. Rio de Janeiro: Livraria Virtual IMPA, 2009. Citado na página 52.

MILLIES, C.; COELHO, S. **Números: uma Introdução à Matemática**. 3. ed. São Paulo: EdUSP, 2001. Citado na página 47.